

---

# MSC-ED Authentication and Accounting Solution V1.0

---

# 1 Contents

1	Contents .....	1
2	Product Introduction .....	2-1
2.1	Overview .....	2-1
2.2	Product Model.....	2-2
2.3	Installation.....	2-3
2.4	Basic Capabilities and Restrictions .....	2-5
3	Routine Maintenance .....	3-9
3.1	Login .....	3-9
3.2	Upgrading the MSC-ED Card Version .....	3-10
3.3	Password Change and Recovery.....	3-11
3.3.1	Password Change .....	3-11
3.3.2	Password Recovery .....	3-11
3.4	Log Query .....	3-16
4	Common Functions and Basic Configuration .....	4-19
4.1	Deployment.....	4-19
4.2	RG-N18000 Configuration.....	4-19
4.2.1	Web Authentication Configuration .....	4-19
4.2.2	Enabling the Function of Adding the Portal Page to Favorites.....	4-21
4.2.3	IPFIX Configuration.....	4-21
4.2.4	No-traffic Detection Configuration.....	4-21
4.2.5	AP Load Balancing and Traffic Diversion .....	4-22
4.2.6	IPv6 Deployment.....	4-32
4.2.7	Clock Synchronization Configuration.....	4-32
4.2.8	Authentication Exemption .....	4-32
4.2.9	Portal Escape .....	4-33
4.2.10	RADIUS Escape.....	4-33
4.2.11	QR-code-based Access .....	4-34
4.2.12	Restart Protection.....	4-35
4.2.13	DHCP Support.....	4-36
4.2.14	Remote Authentication.....	4-36
4.2.15	PBR Configuration Reference from Other Vendors.....	4-39
4.2.16	Track Support for the RNS.....	4-41
4.2.17	Bypass.....	4-42
4.2.18	DHCP Support.....	4-43
4.2.19	IPoE.....	4-43
4.2.20	Intranet Authentication Without the MSC-ED Card .....	4-45
4.2.21	IP-Portal Mapping.....	4-46
4.3	MSC-ED Configuration.....	4-50
4.3.1	(Mandatory) Attack Prevention Configuration.....	4-50
4.3.2	(Mandatory) Access Mode and Interface Configuration .....	4-54
4.3.3	(Mandatory) RG-N18000 Correlation and IPFIX Configuration.....	4-58
4.3.4	(Mandatory) Clock Synchronization Configuration .....	4-60

---

4.3.5	URL Audit Configuration .....	4-62
4.3.6	Traffic Monitoring Configuration.....	4-63
4.4	SAM+ Support Configuration.....	4-66
4.4.1	(Mandatory) SAM+ Support Configuration.....	4-66
4.4.2	Billing Policy Configuration.....	4-67
4.4.3	SMP Server Configuration .....	4-70
4.4.4	Accounting Update .....	4-71
5	Typical Configuration .....	5-72
5.1	Overall Solution .....	5-72
5.1.1	Networking Mode .....	5-72
5.1.2	Functional Differences Between the Bridge Mode and Gateway Mode.....	5-75
5.2	Layer 2 Bridge Mode Configuration Case .....	5-76
5.2.1	General Configuration Template .....	5-76
5.2.2	Implementation Case of a Scientific Institute .....	5-80
5.3	Layer 3 Authentication Configuration Case.....	5-95
5.3.1	Precautions .....	5-95
5.3.2	Layer 3 Authentication and Limitations .....	5-95
5.3.3	Version Selection and Upgrade .....	5-96
5.3.4	Interconnection Address Design and Configuration .....	5-96
5.3.5	NTP Clock Synchronization Configuration.....	5-99
5.3.6	MSC-ED Card and RG-N18000 Correlation Configuration .....	5-100
5.3.7	PBR-based Traffic Diversion Configuration .....	5-100
5.3.8	Layer 3 Authentication Configuration.....	5-104

---

---

## 2 Product Introduction

### 2.1 Overview



The MSC-ED series is a multi-service card developed by Ruijie Networks for gateway-based authentication and accounting. It is applicable to the RG-N18000 series next-generation, cloud-based core switches, and supports exit authentication, traffic-based charging, URL audit, and flow control. It is the industry's first authentication and accounting module compatible with multiple switch-based deployment modes. The MSC-ED card supports bridge deployment and gateway deployment.

Bridge deployment supports the following forwarding mechanisms: bridge forwarding, sniffer, and software bypass, all of which require serial connection setup by the MSC-ED card. Bridge deployment requires the combined use of the MSC-ED and the RG-N18000.

Gateway deployment is applicable to Layer 3 networking and supports policy-based routing (PBR) and forwarding. In this deployment mode, the MSC-ED card supports Layer 3 Web authentication and remote authentication, but only the specified card version can be used.

Area	Product Name	Function	Version	Remarks
Dormitory area Office area Teaching area	Access, aggregation, and core switch	No functional change	All versions	The function of preventing unauthorized IP address configuration is supported (IP source grade+IP DHCP snooping).
	Wireless access point (AP)	Wireless forwarding channel	All versions	N/A

Area	Product Name	Function	Version	Remarks
Area between the network core and the egress	RG-N18000	Authentication, Authorization and Accounting (AAA)	N18000_RGOS 11.5 (1) B2	N/A
	MSC-ED card	Traffic-based charging	MSC_RGOS 11.1 (8) B1	N/A
Egress	Powercache	Hotspot caching and use of extranet resources on the intranet	All versions	N/A
	ACE	Bandwidth guarantee for key applications and users, traffic visualization, URL and IM logging, and accounting	All versions	N/A
	EG2000XE	Smart routing, multilink load balancing, domain name server (DNS), and network address translation (NAT)	All versions	N/A
Service area	SAM	AAA server	SAM+	N/A
	ePortal	Portal server	1.43 and later	N/A
	SNC	Whole-network topology management, VLAN management, and configuration management	2.28 and later	N/A
	eLog server	Behavior audit	N/A	N/A

## 2.2 Product Model

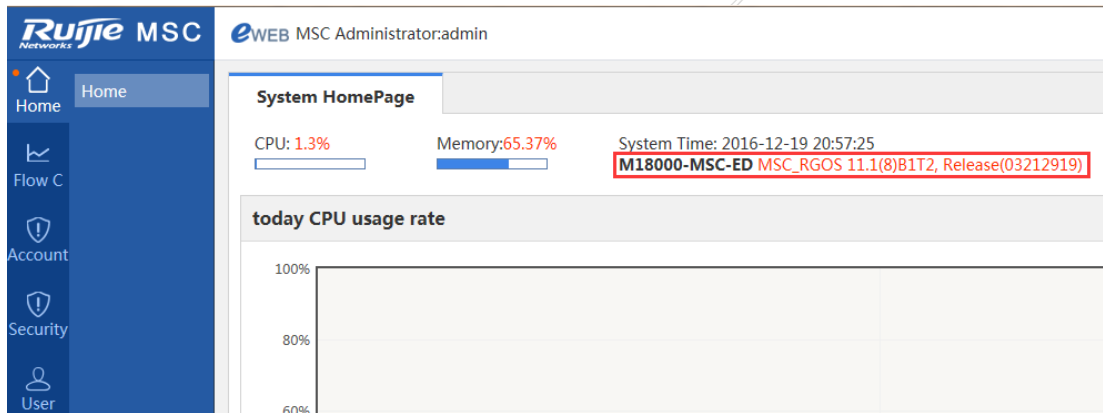
The product name of the authentication and accounting card is M18000-MSC-ED. The product version is displayed on the command-line interface (CLI) of the RG-N18000 chassis and the Web homepage of the MSC-ED card.

The following versions need to be specified: MSC-ED card version, RG-N18000 version, SAM+ version, and ePortal version.

Currently, the MSC-ED series has only the following model:

```
Ruijie#show ver
System description      : Ruijie Multi-Service CARD(M18000-MSC-ED) by Ruijie Networks.
System start time      : 2015-10-12 14:40:50
System uptime          : 0:00:28:32
System hardware version : 1.00
System software version : MSC_RGOS 11.1(8)B1
System patch number     : NA
System serial number    : 1234942570025
System boot version     : 1.3.8
Ruijie#
```

The model is displayed on the Web homepage of the MSC-ED card.



## 2.3 Installation

### I. Installing hardware

Note: For FE cards, line cards, and engine slots, only one slot has no filler panel installed in the standard configuration of a chassis before shipment. To insert cards into other slots, remove the filler panels. A filler panel must be installed in a slot without a card; otherwise, the heat dissipation of the device is affected.

1. Wear ESD wrist straps, and ensure that the ESD wrist straps are in good contact with the skin and they are properly grounded.
2. Remove the filler panel from a slot of the chassis.
3. Take a card out of the card box and hold the handle of the card with both hands. Horizontally hold and place cards when taking and transferring them. Do not knock the side connected to the backplane.



The hardware installation process for the MSC-ED card is similar to that for the RG-N18000 service card. For details, see the [N18000 Series Switch Hardware Installation Manual](#).

### II. Checking the hardware status

Connect to a power supply and check whether the device operates properly. (The checking process is similar to that for firewall cards.)

- Check that the card indicator is steady on green.
- Run the **show version slots** command and check that the card is properly recognized.

- Run the **show run** command and check that interfaces are loaded correctly in configuration.

### III. Checking the card loading status

```
N18007#sh ver slot
```

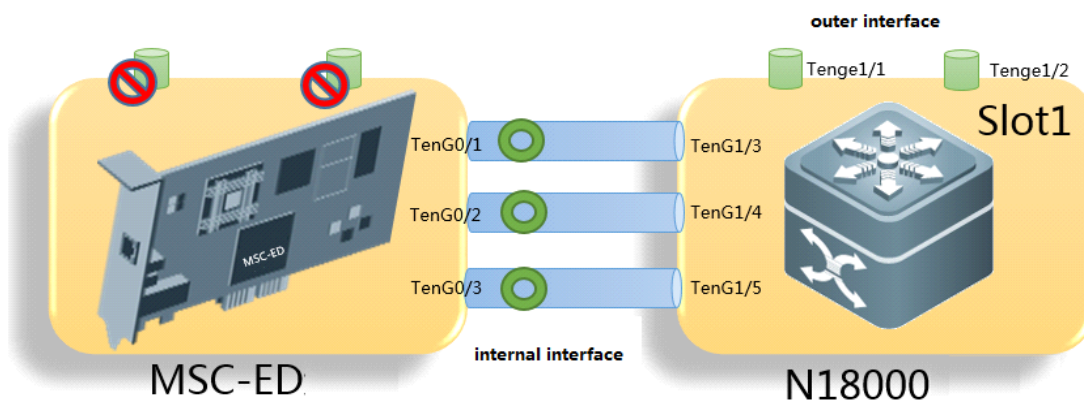
Dev	Slot	Port	Configured Module	Online Module	Software Status
1	1	0	none	none	none
1	2	7	M18000-MSC-ED	M18000-MSC-ED	ok
1	3	48	M18000-24GT20SFP4XS-ED	M18000-24GT20SFP4XS-ED	ok
1	4	44	M18000-24XS4QXS-DB	M18000-24XS4QXS-DB	ok
1	5	7	M18000-MSC-ED	M18000-MSC-ED	ok
1	M1	0	N/A	none	none
1	M2	0	N/A	M18007-CM II LITE	master

### IV. Checking the status of internal interfaces

```
N18007#sh int sta | in 1/2
```

Interface	Status	Vlan	Duplex	Speed	Type
TenGigabitEthernet 1/2/1	down	1	Unknown	Unknown	fiber
TenGigabitEthernet 1/2/2	down	1	Unknown	Unknown	fiber
TenGigabitEthernet 1/2/3	up	44	Full	10G	fiber
TenGigabitEthernet 1/2/4	up	44	Full	10G	fiber
TenGigabitEthernet 1/2/5	up	55	Full	10G	fiber
TenGigabitEthernet 1/2/6	down	1	Unknown	Unknown	fiber
TenGigabitEthernet 1/2/7	down	1	Unknown	Unknown	fiber

The external physical interfaces of the RG-N18000 card are Interface 1 and Interface 2; therefore, internal interfaces are numbered starting from 3, as shown in the following figure.



### V. Checking the software status

1. Correct version; 2. Clock synchronization completed; 3. Initial interface shutdown in bridge mode.

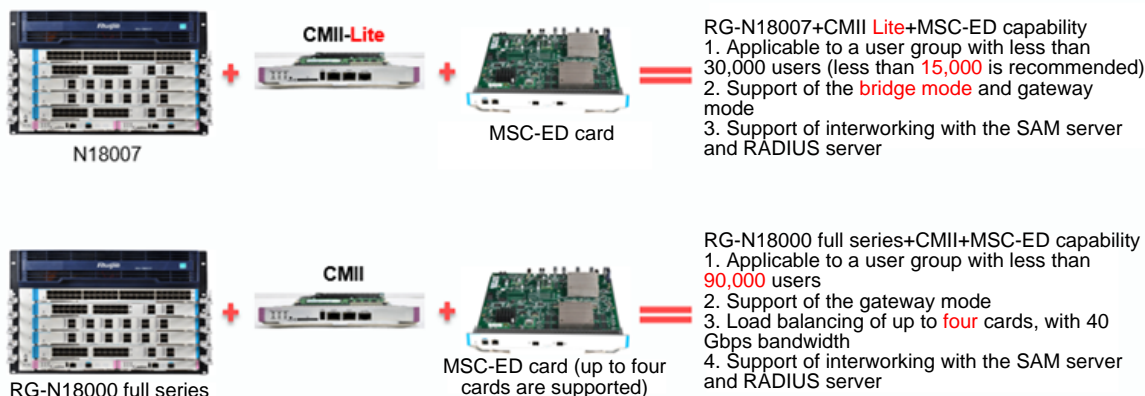
Connect a PC to the console port on the device panel and perform the following operations:

- Check that the software is loaded properly and CLI commands can be entered on the console.
- Run the **show version detail** CLI command to check whether the software version is correct.
- Check the clock and related settings. The MSC-ED card must be configured with a clock synchronization protocol. By default, a server on the Internet is used as the SNTP server. If the MSC-ED card cannot connect to the Internet, you are advised to change the IP address of the SNTP server to the IP address of the RG-N18000 and enable a clock synchronization protocol on the RG-N18000. Accounting and real-name auditing are accurate only when the RG-N18000, MSC-ED, and SAM server have consistent time.
- By default, the MSC-ED card adopts the bridge mode. The TenG0/1 and TenG0/2 interfaces that form a bridge are connected to the TenG1/3 and TenG1/4 interfaces of the RG-N18000. To avoid VLAN loops, configure traffic diversion on the TenG1/3 and TenG1/4 interfaces.

## 2.4 Basic Capabilities and Restrictions

The combined use of available products as is summarized as follows:

Product selection is based on two factors: traffic volume and user quantity.



Main Indicator	Metric	Value
Layer 3 authentication	IPv4 Web authentication performance	1,000 users per second
	Online terminal capacity	90,000 dual stack
	Online user information synchronization performance (SAM server and RG-N18000)	100,000 users within 15 minutes
	Authentication exemption configuration on the SAM server	Supported
	Mapping of one account to multiple terminals (wired and wireless)	Supported
	Web authentication client	Supported
	Layer 3 authentication deployment modes	Bypass and serial connection



Main Indicator	Metric	Value
	IP spoofing protection during accounting	Supported
Traffic-based charging	IPv4 forwarding performance of a single traffic exit authentication card	10 Gbps
	Centralized device connection, 40 Gbps per device	40 Gbps
	Traffic table creation performance per card	100,000 per second
	Traffic table capacity per card, IPv4	8,000,000
	Traffic table capacity per card, IPv6	1,000,000
Tiered charging	No decimal during segment charging	Integer
Openness	Standard RADIUS interworking	Supported
Reliability	RADIUS escape	Supported
	Portal escape	Supported
	Hot standby of the network access authentication card	Supported
	AP link backup to solve line card failures	Supported
Audit	Audit	30,000 concurrent terminals per card, 20,000/s performance per card

**Parallel comparison of product functions:**

	RG-N18000+MSC card	RSR77
Noise reduction	<p>The noise reduction performance is high, supporting instant page display under the 100,000/s noise condition.</p> <p>(1) When receiving a packet, the RG-N18000 includes a Java script in the packet to trigger redirection. The browser can recognize the Java script and trigger redirection. Because noise packets cannot be recognized, the packets are not redirected to the portal server, thus reducing the server burden.</p>	<p>The noise reduction performance is poor.</p> <p>(1) The RSR77 recognizes Web requests and non-Web requests, and also recognizes lightweight applications based on the User-Agent field in HTTP packets. The RSR77 distinguishes between Web HTTP request packets and non-Web HTTP request packets, and discards the HTTP packets from non-Web applications.</p>
Application scenario	<p>(1) Layer 2 access authentication and accounting</p> <p>(2) Layer 3 exit authentication and accounting</p>	Layer 3 exit authentication and accounting
Authentication method	Layer 2 Web authentication, Layer 3 Web authentication, and 1x authentication	Layer 3 Web authentication
Deployment scenario	<p>(1) Core deployment</p> <p>(2) Bypass deployment</p> <p>(3) Transparent deployment at the egress</p>	<p>(1) Bypass deployment</p> <p>(2) Layer 3 deployment at the egress</p>

	RG-N18000+MSC card	RSR77
Performance	90,000 online terminals; 512-byte and 40-Gbps forwarding bandwidth; no impact on forwarding bandwidth from configuration of accounting-free network segments; formal third-party certificates	90,000 online terminals; 40-Gbps forwarding bandwidth (bytes unknown); impact on forwarding bandwidth from configuration of accounting-free network segments
Perception-free authentication	Supported Layer 3 perception-free authentication under planning	Not supported

Flow control	Supported	Supported
Accounting principle	Based on duration or traffic	Based on duration or traffic
IP spoofing	Solved by DHCP support	Not solved
Active/Standby RADIUS	Supported	Unsupported
Traffic statistics precision	4M/4 minutes	10M/5 minutes
URL audit	Supported, with 80,000/s URL audit performance	Supported
User group bandwidth management	Supported	Supported
Guest authentication by QR code scan	Supported	Unsupported
Traffic classification	Eight types	Three types
Authentication exemption based on the source and destination IP addresses	Supported	Supported
Accounting exemption	Supported	Unsupported
Attack prevention	Overall attack prevention per user, which is enabled by default and does not affect performance	Overall attack prevention per user, which affects performance (It is recommended that this function be enabled only when an attack occurs.)
Architecture	Separation of authentication, accounting, and forwarding, which meets high performance requirements	Authentication, accounting, and forwarding implemented by cards
Reliability	(1) Bypass (2) AA deployment (3) RADIUS and portal escape (4) Multi-VSU feature	(1) RADIUS and portal escape
Openness	Support of SAM, free RADIUS, urban hotspot, Srun, and self-developed RADIUS	Support of only SAM
Cost	Relatively high	Relatively low

---

Egress	Egress deployment not supported	Support of egress deployment, NAT, and smart routing
Carrier solution	DSN disputes between multiple carriers for Web authentication	Supported

---

## 3 Routine Maintenance

### 3.1 Login

#### Web Login

Management interface: MGMT

Default management address: 192.168.1.1

Web login URL: <http://192.168.1.1>

Default account name and password: **admin** and **admin**

#### SSH Login

Default management address: 192.168.1.1

Management interface: MGMT

Default account name and password: **admin** and **admin**

Note: You are advised to log in over Web for the first time. After you configure the management interface address and the gateway in interface configuration mode, log in over SSH or telnet.

#### Telnet Login

Default management address: 192.168.1.1

Management interface: MGMT

By default, neither the VTY password nor the privileged password is set. You need to set the Web administrator password and the telnet password on the **System Settings** page.

Note: You are advised to log in over Web for the first time. After you configure the management interface address and the gateway in interface configuration, log in over SSH or telnet.

#### Console Login

Baud rate: 9,600

Data bits: 8

Parity check: none

Stop bit: 1

Data flow control: none

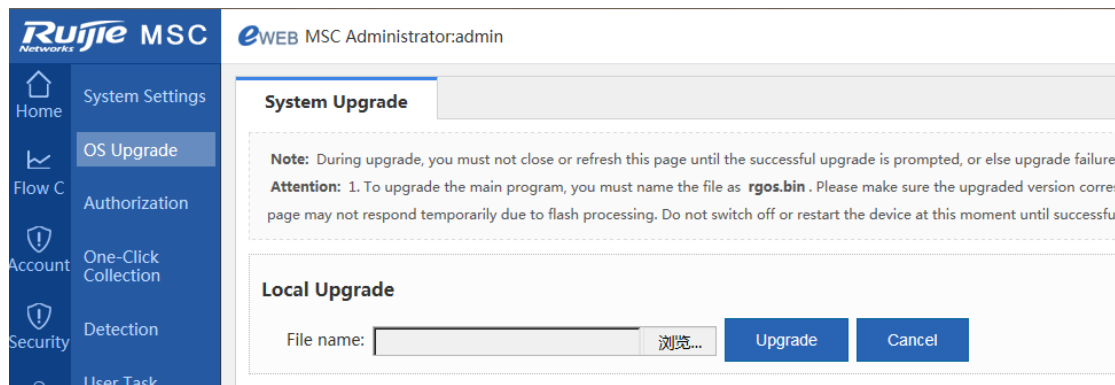
If your PC comes with HyperTerminal, the COM port is located beside the display interface on the back of the chassis. The COM port has nine pins. If you use a laptop without a COM port, connect a serial-to-USB cable.

The MSC-ED card has a console port on its front panel, and the port is marked with **console**.

## 3.2 Upgrading the MSC-ED Card Version

### I. (Recommended) Web-based upgrade

1. Log in to the Web management interface of the MSC-ED card from the intranet.
2. (Note) Change the name of the upgrade package to **rgos.bin**.
3. Click **System Upgrade** and select and upload the upgrade package used for local upgrade.
4. Wait until upgrade is successful. Do not perform any operations during the upgrade process.

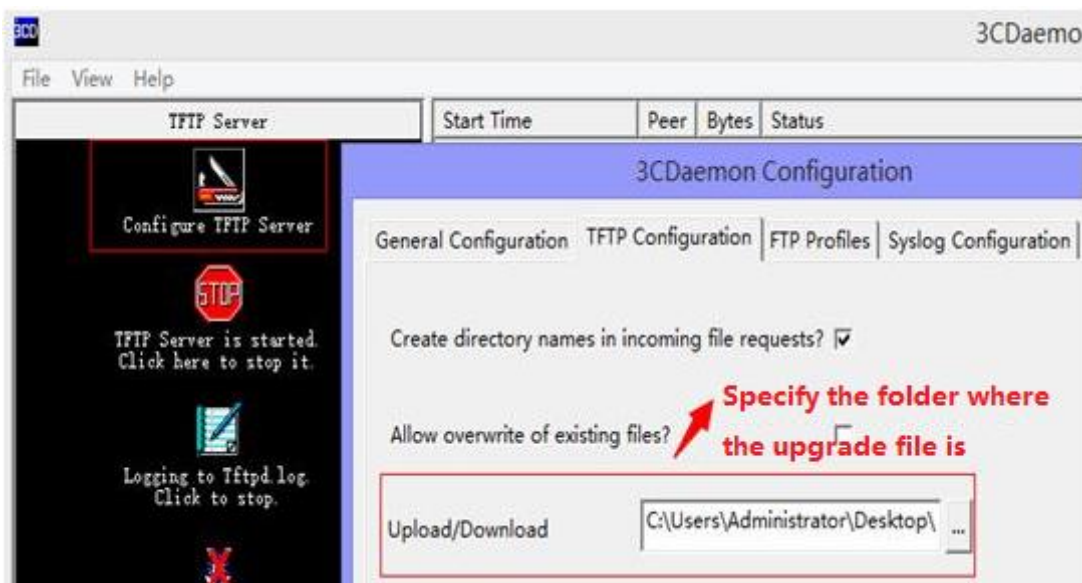


### II. Upgrade on CLI

1. Prepare the upgrade file and tool.

Change the name of the main program to be upgraded to **rgos.bin**. Use the 3C Daemon TFTP tool for CLI upgrade, due to the large size of the 11.X version.

2. Run 3C Daemon to start a TFTP server, and specify the location of the program to be upgraded.



Before upgrade, check Windows Firewall, antivirus software settings, and system security policies. Only one TFTP server can be started, otherwise, port conflict will occur.

3. Log in to the CLI.

Enter the upgrade command **upgrade download oob\_tftp://192.168.51.59/rgos.bin** (192.168.51.59 is the IP address of the PC)

Run the **show version** command on the CLI to display version information.

## 3.3 Password Change and Recovery

### 3.3.1 Password Change

Choose **Advance > System Settings > Change Password** to change your password.

The screenshot displays the Ruijie MSC eWEB Administrator interface. The top left shows the 'Ruijie MSC' logo and the user 'eWEB MSC Administrator:admin'. A navigation menu on the left includes 'Home', 'OS Upgrade', 'Flow C', 'Authorization', 'Account', 'One-Click Collection', 'Security', 'Detection', 'User Task', 'System Log', 'Network', 'System Report', and 'Advance'. The 'System Settings' menu item is highlighted. The main content area shows the 'Change Password' page with tabs for 'Change Password', 'Restart', 'Factory Default', 'Configuration Backup', and 'SysTi'. A note states: 'Note: The administrator has full permissions to configure and view settings. Tip: After you change the password, please log in again with the new password. The password cannot exceed 32 characters.' Below this, the 'Change Web Password' section shows 'User Name: admin', 'New Password:' and 'Confirm Password:' input fields with asterisks, and 'Save' and 'Clear' buttons. At the bottom, there is a link for 'Change Password for Authentication'.

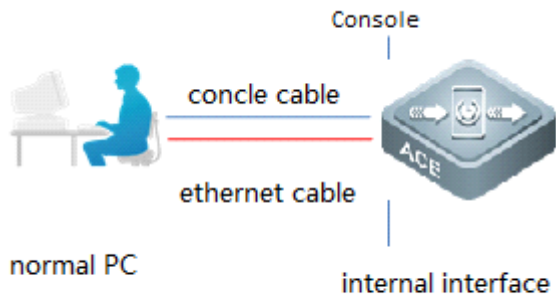
### 3.3.2 Password Recovery

#### I. Network Mode

If you are an administrator but forget the password and cannot log in to the MSC-ED card in Web mode, use a console cable to access the CTRL layer and recover your password. You need to save previous configurations before recovery.

If the configurations are unimportant, you can press the RESET button on the panel in the power-on state for 8s to reset the card to default settings. The default IP address is 192.168.1.1, and the default username and password are both **admin**.

#### II. Network Topology



### password recovery

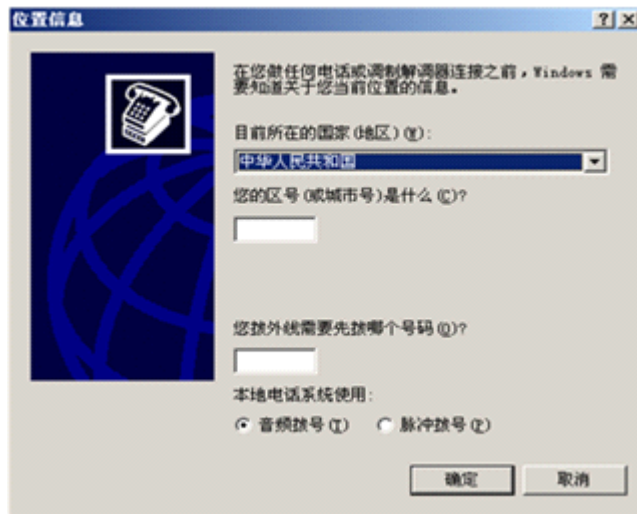
### III. Configuration Tips

1. If you need to save previous configurations, get a console cable ready for password recovery. Restart the device and recover the password at the Boot layer.
2. After the device is restarted, password recovery is completed at the Boot layer, which will cause a network interruption. Perform password recovery when the network can be disconnected.

### IV. Configuration Steps

- (1) Perform the following operations to recover your password:
  - a. Connect a console cable to the console port of the MSC-ED card, and connect a network cable to the internal network port of the ACE.
  - b. Configure the network device by using HyperTerminal.

Choose **Start > Programs > Accessories > Communication** to start the HyperTerminal program. (By default, Windows Server 2003 does not come with HyperTerminal, and you need to install HyperTerminal using the Add/Remove Programs tool in Control Panel.) The following dialog box is displayed when you use HyperTerminal for the first time.



Enter an area code (for example, 099) and click **OK**. The following dialog box is displayed.



Click **OK** to start HyperTerminal. Enter a name and click **OK**.



Select the COM port connected to the console cable for **Connect to**, and click **OK**.



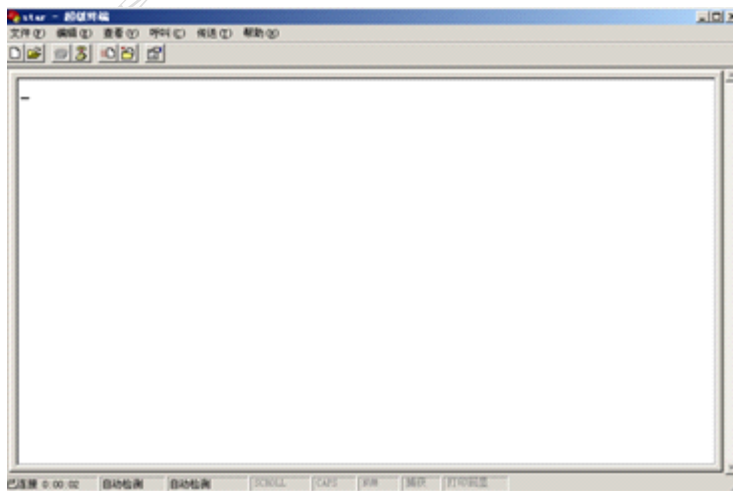
In the **COM Attributes** dialog box, click **Restore Defaults** then **OK**. The HyperTerminal configuration window is displayed, with the cursor blinking in the upper left corner.

**The default baud rate is 9,600.**





Press **Enter** to enter user mode (Ruijie>) on the network device.



- (2) Power off then on the device. Keep pressing the shortcut key **Ctrl+C** on the HyperTerminal interface until the main menu is displayed, as shown in the following figure.

```

Ruijie#reload
Reload system?(y/N)y
Ruijie#Sending all processes the TERM signal...
Sending all processes the KILL signal...
Unmounting /mnt/sata0 file systems...
/etc/rc.d/rc6.d/S99reboot: /etc/rc.d/rc6.d/S99reboot: 29: cannot create /proc/sysrq-trigger: Directory
[ 184.788594] Just a test! Event code: 1! System reboot now...%RG_LMK-0-REBOOT: Rebooting by job: busy

Boot 1.2.7-00374-g514b302 (Build time: Aug 18 2014 - 15:34:21)

DRAM: 4 GiB
NAND: 512 MiB
Flash: 8 MiB
SETMAC: Setmac operation was performed at 2014-09-17 17:17:55 (version: 11.0)
Press Ctrl+C to enter Boot Menu
Skipping PCIe port 0 BIST, reset not done. (port not configured)
Skipping PCIe port 1 BIST, in EP mode, can't tell if clocked.
BIST check passed.
EG2000G board revision major:1, minor:0
OCTEON CN6645-AAP pass 1.2, Core clock: 1100 MHz, IO clock: 750 MHz, DDR clock: 666 MHz (1332 Mhz data
Net: octeth0, octeth1, octeth2, octeth3, octeth4 [PRIME], octeth5, octeth6, octeth7
Entering simple UI....

===== 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
 6. Set backplane info
*****
Press a key to run the command:

```

press Ctrl+C repeatedly

(3) Press the shortcut key **Ctrl+Q** to open the U-Boot CLI, enter the **main\_config\_password\_clear** command, and press **Enter**. The device restarts automatically and enters its system without password input (the password does not need to be entered only at that time).

(4) Change the privileged password and the Web administrator password in device configuration mode as follows:

Set a new Web administrator password.

```

Ruijie#conf t
Ruijie(config)# webmaster level 0 username admin password admin //new username and password are
admin
Ruijie(config)#exit
Ruijie(config)# enable secret admin //enable password is admin
Ruijie#write //save the configuration

```

The new password takes effect after being saved. Restart is not required.

Because users are also authenticated on the console port when Web authentication is enabled, you need to change the password for user authentication; otherwise, you cannot log in to the console port after exit. To change the password, re-set the telnet login password on the Web management interface, or configure a telnet user and a password on the CLI.

```

Ruijie(config)#username admin password admin


```

---

Note: Do not exit the system before you change the password; otherwise, you need to input the old password to re-enter the system.

## V. Verification

Use the new password to log in to the MSC-ED card. The following figure shows the login page.



# MI8000-MSC-ED

Username:

password:

Language: English ▼

[Forget password?](#)

## 3.4 Log Query

1. Logs are stored in a flash drive directory

```

Ruijie#dir
Directory of flash:/
Number  Properties  Size           Time           Name
-----  -
1       drwx         224B          Thu Jan 1 08:00:53 1970  dm
2       -rwx        175.1k        Mon Sep 7 22:38:35 2015  syslog_3.txt
3       drwx         160B          Thu Jan 1 08:00:38 1970  rep
4       drwx         224B          Thu Jan 1 08:00:38 1970  var
5       drwx         160B          Thu Jan 1 08:00:53 1970  addr
6       drwx         440B          Thu Jan 1 08:00:58 1970  sync
7       -r--         95B           Thu Jan 1 08:00:19 1970  tmp_env.txt
8       -rwx         1.9M          Thu Jan 1 12:07:51 1970  syslog.txt
9       drwx         232B          Thu Jan 1 08:00:21 1970  security
10      -rw-         2.3M          Mon Sep 7 23:35:45 2015  dev_audit.db
11      -rw-         2.1k          Mon Sep 7 23:34:06 2015  config.text
12      -rw-         0B            Thu Jan 1 08:00:23 1970  user_task.db
13      -rw-         134.5k        Thu Jan 1 09:10:25 1970  rlog.elf
14      -rw-         188.3k        Thu Aug 27 11:37:27 2015  tech_vsd0_20150827113726.tar.gz
15      drwx         160B          Thu Jan 1 08:00:17 1970  user_task
16      -rwx         696B          Thu Jan 1 08:00:18 1970  httpd_cert.crt
17      -rwx         21B           Mon Sep 7 23:34:06 2015  syslog_rfc5424_flag.txt
18      drwx         352B          Thu Jan 1 08:00:27 1970  portal
19      -rw-         32.ok         Thu Jan 1 08:01:39 1970  user_diary.db
20      -rw-         4B            Mon Sep 7 14:23:01 2015  reload
21      drwx         160B          Thu Jan 1 08:00:53 1970  dm_tipc
22      drwx         304B          Mon Sep 7 17:36:29 2015  upgrade
23      drwx         240B          Thu Jan 1 08:00:07 1970  mode_mgmt
24      dr--         232B          Thu Jan 1 08:00:29 1970  sslvpn
25      drwx         304B          Thu Jan 1 08:12:09 1970  rg_l1cns
26      drwx         304B          Thu Jan 1 08:00:17 1970  syslog
27      drwx         160B          Thu Jan 1 08:00:52 1970  feedback
28      -rwx         887B          Thu Jan 1 08:00:18 1970  httpd_key.pem
29      -rwx         1.9M          Thu Jan 1 18:57:12 1970  syslog_1.txt
30      -rwx         1.9M          Tue Aug 18 18:51:39 2015  syslog_2.txt
15 files, 15 directories
281,903,104 bytes data total (276,070,400 bytes free)
536870912 bytes flash total (276,070,400 bytes free)

```

## 2. Display Logs

- (1) Run the **show logging** command to display logs.

```

ISK#sh logging
Syslog logging: enabled
Console logging: level debugging, 20639 messages logged
Monitor logging: level debugging, 0 messages logged
Buffer logging: level debugging, 20639 messages logged
File logging: level debugging, 20614 messages logged
File name:syslog.txt, size 128 Kbytes, have written 4 files
Standard format:false
Timestamp debug messages: datetime
Timestamp log messages: datetime
Sequence-number log messages: disable
Synname log messages: disable
Count log messages: disable
Trap logging: level notifications, 266 message lines logged,0 fail
Log Buffer (Total 1280000 Bytes): have written 1280000, Overwritten 251268
*Oct 30 05:49:38: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.6.153.61, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:49:40: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.7.153.78, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:49:42: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.6.153.85, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:49:42: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.8.86.141, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:49:44: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.9.86.181, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:49:44: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.8.86.175, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:49:46: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.6.153.119, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:49:48: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.7.153.136, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:49:50: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.6.153.148, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:49:52: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.7.153.165, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:49:54: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.7.153.180, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:49:56: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.9.153.214, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:49:58: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.6.153.206, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:50:00: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.9.87.41, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s
*Oct 30 05:50:02: NWEBAUTH-6-USER_ONLINE: User Online: IP 10.6.153.235, MAC 1414.4b22.2422, Port Ag3, Time-limit 0s, Flow-limit 0s

```

- (1) Run the **more flash:syslog\_1.txt** command to display the log information in the **syslog\_1.txt** file in the **dir** directory.

## 3. Copy Logs

---

(1) Copy logs over TFTP. (The TFTP service must be enabled on the PC. For example, the IP address of the PC is 192.168.1.1.)

```
copy flash:/syslog/syslog_XXX.text tftp://192.168.1.1/syslog_XXX.text //Connect the network cable of
the PC to the router interface, or:
copy flash:/syslog/syslog_XXX.text oob_tftp://192.168.1.1/syslog_XXX.text //Connect the network
cable to the MGMT interface on the global management mainboard.
```

**flash:/syslog/syslog\_XXX.text** is a sample path.

(2) Copy logs using a USB flash drive.

```
copy flash:/syslog/syslog_XXX.text usb0:sw1_m1.syslog_XXX.text //Connect a USB flash drive to the M1
management board of SW1.
```

---

## 4 Common Functions and Basic Configuration

### 4.1 Deployment

The deployment process involves the following functional components:

1. RG-N18000 chassis: data traffic diversion, authentication, and access to partial network resources before authentication
2. MSC-ED service card: accounting, flow control, and URL audit
3. Authentication and accounting system: authentication and account configuration

Precautions:

1. For proper recognition of the MSC-ED line card, use the correct switch version for the MSC-ED authentication solution.
2. Only the generic version of the MSC-ED authentication solution is available. If you need to use the MSC-ED line card in conjunction with the simplified network solution, contact the product TAC.
3. The MSC-ED authentication solution supports new features such as Layer 2/3 Web authentication and remote authentication. Do not use these features with the simplified network solution.

### 4.2 RG-N18000 Configuration

#### 4.2.1 Web Authentication Configuration

##### Working Principle

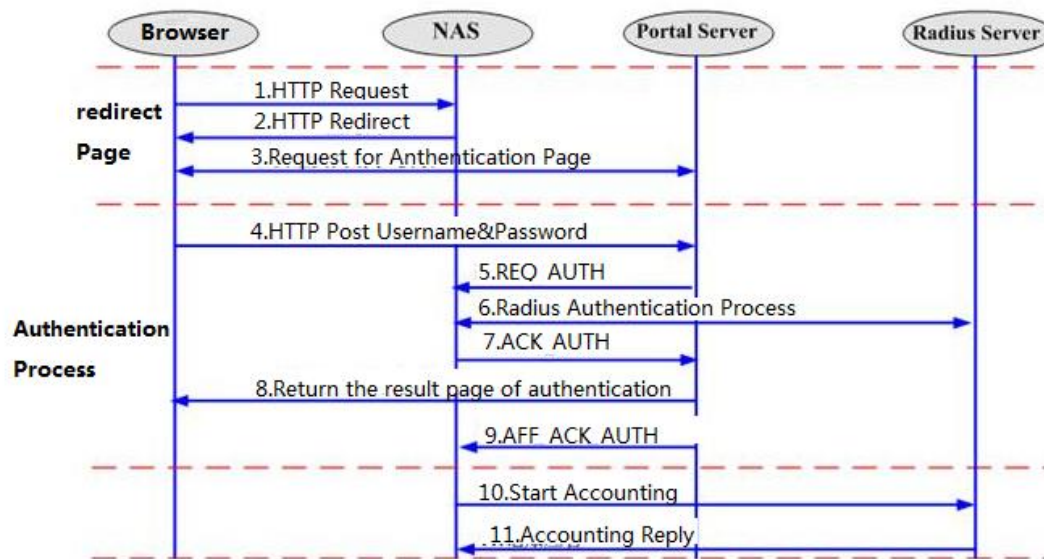
- A user opens the Internet Explorer and initiates an HTTP request for accessing a website.
- The network access server (NAS) intercepts the HTTP request and redirects the user to the portal server because the user was not authenticated before. The NAS adds related parameters to the portal URL. For parameter details, see the description of CHAP authentication.
- The portal server pushes the Web authentication page to the user.
- The user fills in an account name, password, and other information on the authentication page, and then submits the information to the portal server.
- The portal server submits the account name and password to the NAS in order to initiate authentication.
- The NAS sends the account name and password to the RADIUS server for authentication. The RADIUS server determines user validity based on the user information, and then returns the RADIUS access-accept/reject response to the NAS.
- The NAS returns the authentication result to the portal server.
- The portal server pushes a page containing the authentication result to the user.
- The portal server returns a response to the NAS to indicate the reception of the authentication result.
- The NAS sends a Start Accounting packet.

Remarks:

Web authentication acceleration supports direct access to the portal page for authentication. Redirection is not required.

Difference from the first-generation portal server: Authentication is jointly completed by the NAS and the RADIUS server, which effectively reduces the burden on the portal server.

Flowchart of packet exchange:



### Configuration Steps

```
aaa new-model //Enable AAA.
radius-server host 192.168.197.79 key ruijie //RADIUS authentication server
aaa authorization network default group radius //AAA configuration reference, which may vary according
to the actual service deployment.
aaa authentication web-auth default group radius //Enable Web authentication.
aaa accounting update periodic 20 //AAA configuration reference, which may vary according to the
actual service deployment.
aaa accounting update //AAA configuration reference, which may vary according to the actual service
deployment.
aaa accounting network default start-stop group radius //AAA configuration reference, which may vary
according to the actual service deployment.

web-auth template eportalv2 //Authentication temp
ip 192.168.197.79
url http://192.168.197.79:8080/eportal/index.jsp //Add the RG-N18000 to the portal server.
web-auth portal key ruijie //Configure a key for the portal server.
web-auth direct-host 49.209.88.101 //(Optional) Configure a list of users exempt from authentication.

interface range GigabitEthernet 0/2-3 //Enable Web authentication in interface configuration mode.
web-auth enable eportalv2 //Enable Web authentication in interface configuration mode.
```



---

Note: The Web authentication adopted by the MSC-ED traffic equipment room solution is different from that adopted by the campus network 3.0 solution.

The Web authentication adopted by the MSC-ED traffic equipment room solution supports the Layer 2 VLAN interface and the Layer 3 switch virtual interface (SVI), but does not support QinQ and Super VLAN.

## 4.2.2 Enabling the Function of Adding the Portal Page to Favorites

This function allows users to add the portal page to their Internet Explorer favorites and then click the portal link in the **Favorites** directory to perform authentication, removing the need to enter URLs in the address bar of the browser. The NAS port number for users with this function enabled is 0 on the **Operation > Online User** page of the SAM server.

### Configuration Reference

```
web-auth portal eportalv2
```

## 4.2.3 IPFIX Configuration

### Working Principle

IPFIX is used to update user traffic accounting information. It encapsulates the authentication information on the egress gateway as TCP packets according to the IPFIX-defined format and sends the packets to the configured server, which then updates the corresponding accounting information.

IPFIX transfers flow records as templates. Before sending flow records, IPFIX creates a template according to the record format and sends the template to the server. The template defines the attributes and length of the fields in the flow record. IPFIX defines hundreds of field attributes, and each attribute corresponds to an identifier used to indicate the meaning of the attribute. For example, an attribute marked by 8 indicates the source IP address. Upon receiving the template, the server determines the format of subsequent IPFIX flow records and parses these records according to the format.

If the RADIUS server is RG-SAM+, perform the following configuration. If the RADIUS server is not RG-SAM+, consult the background.

IPFIX configuration reference for RG-SAM+:

```
web-auth acct-method ipfix //Set the Web authentication and accounting mode to the IPFIX mode.  
ip auth-flow export destination 192.168.1.6 4739 //Upload traffic information to the SAM server.
```

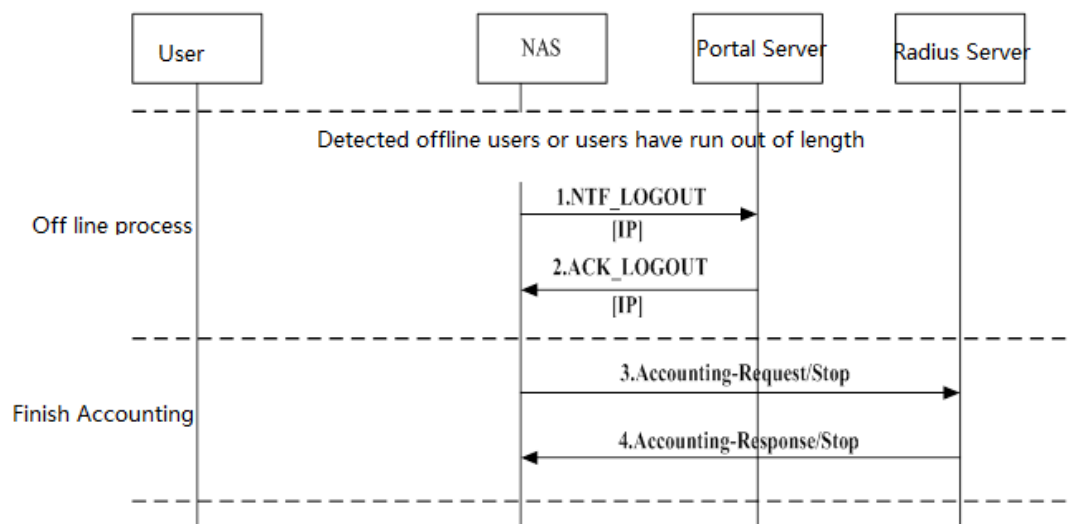
## 4.2.4 No-traffic Detection Configuration

### Mandatory

When an authenticated user goes offline abnormally (for example, the user disconnects the network cable or powers off the device) and then connects to the Internet in another dorm room, the user cannot perform authentication because the user is still in the online state.



Flowchart of no-traffic detection:



## Configuration Reference

You can set the period allowed for users to stay online with no traffic detected. Once a user is detected with no traffic during that period, the user is forced offline. The period determines how long the user has to wait in order to perform re-authentication after port migration. The configuration command is as follows:

**Offline-detect interval** xx (precise to minutes) **threshold** 0 (**threshold** is set to 0)

The MSC-ED solution supports no-traffic detection, but does not support low-traffic detection.

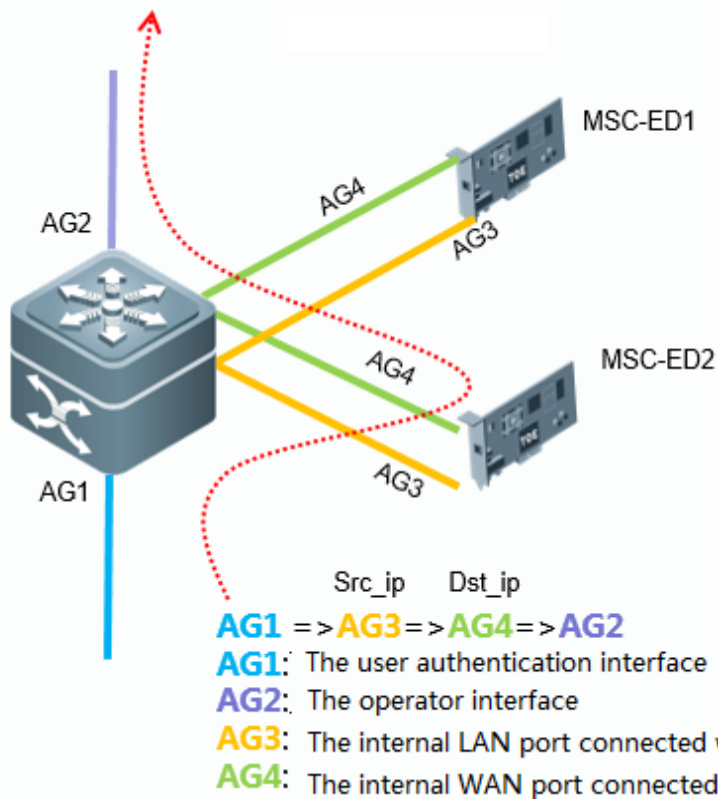
```
offline-detect interval 5 threshold 0
```

## 4.2.5 AP Load Balancing and Traffic Diversion

### 4.2.5.1 AP Load Balancing

You can connect two or more MSC-ED cards in AP binding mode according to deployment requirements.

You can configure an AP interface for load balancing and hot standby between the MSC-ED cards. In the following figure, an interface of MSC-ED1 and an interface of MSC-ED2 are configured to form AP3 and AP4 respectively. Users' uplink traffic (traffic from the user side to the Internet) is diverted to AP3, whereas users' downlink traffic (traffic from the Internet to the user side) is diverted to AP4. AP3 adopts an AP load balancing algorithm based on the source IP address, whereas AP4 adopts an AP load balancing algorithm based on the destination IP address. If the uplink traffic of users who use IP1 to access the extranet is distributed to MSC-ED1 (which implements load balancing based on the source IP address), the downlink traffic of those users is also distributed to MSC-ED1 using the key of the load balancing algorithm based on the destination IP address. Such a solution must ensure that the load balancing algorithm based on the source IP address and that based on the destination IP address are the same. When MSC-ED1 fails, services are switched over to MSC-ED2 to implement hot standby.



**Configuration description:**

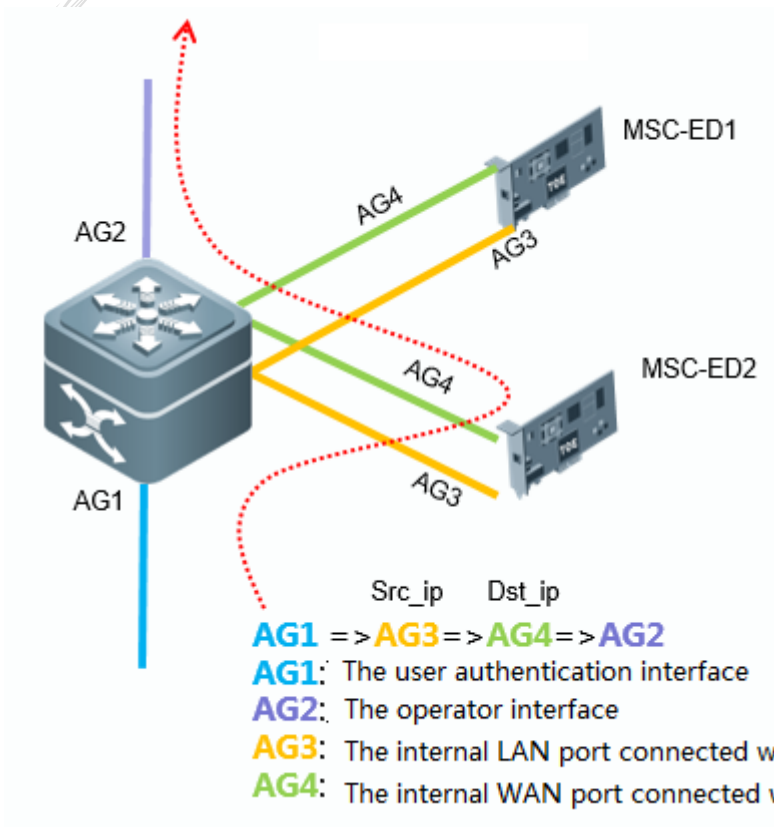
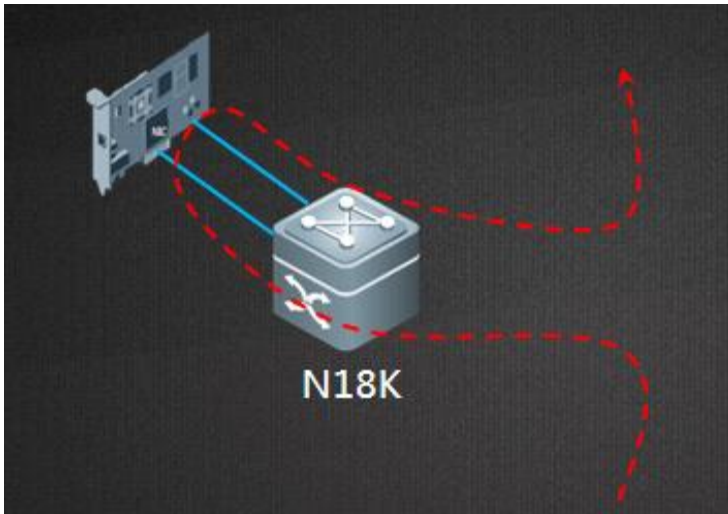
```
Ruijie(config)#int ag 3
Ruijie(config-if-AggregatePort 3)#sw a vlan 2
Ruijie(config-if-AggregatePort 3)#aggregateport load-balance src-ip (The MSC-ED cards implement load balancing for uplink traffic based on the source IP address.)
Ruijie(config)#int ag 4
Ruijie(config-if-AggregatePort 4)#sw a vlan 2
Ruijie(config-if-AggregatePort 4)# aggregateport load-balance dst-ip (The MSC-ED cards implement load balancing for downlink traffic (returned from the extranet) based on the destination IP address.)
Ruijie(config)# msc path vlan 2 dev-input Ag1 dev-output Ag2 msc-input Ag3 msc-output Ag4 //(Set the direction of traffic diversion.)
```

**4.2.5.2 Path-based Traffic Diversion (in Bridge Mode)**

**Path-based Traffic Diversion**

---

Traffic coming from the RG-N18000 is diverted to the MSC-ED card. Then the traffic is sent from another port of the MSC-ED card back to the RG-N18000 for forwarding, as shown in the following figure.



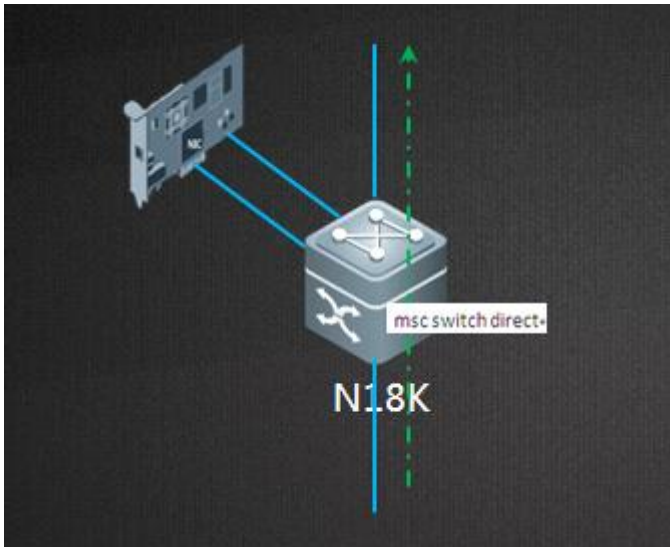
Configuration example:

```
msc path vlan 2000 dev-input ag1 dev-output ag2 msc-input ag 3 msc-output ag 4 // Traffic coming from the AG1 port of the RG-N18000 is diverted to the internal AG3 port of the MSC-ED card. Then the
```

traffic is sent from the AG4 internal port of the MSC-ED card to the AG2 port of the RG-N18000 for forwarding.

## Manual Bypass

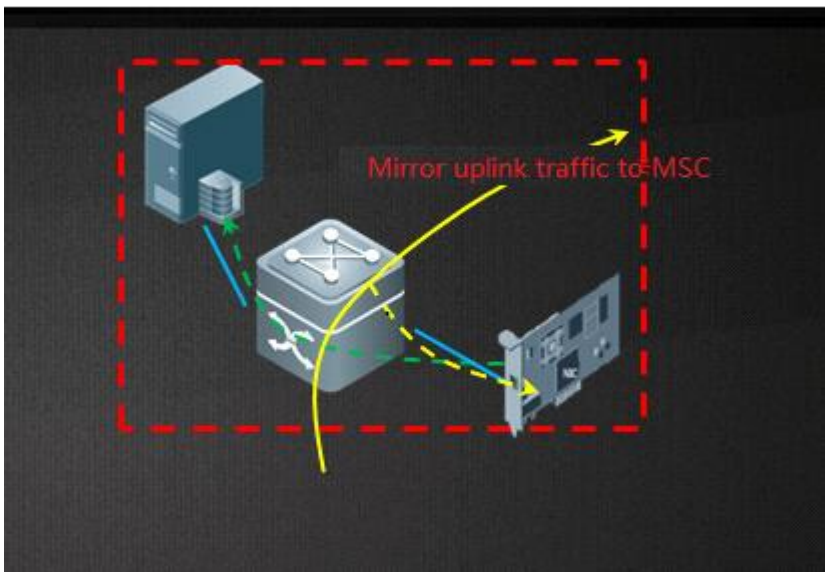
User traffic is forwarded directly by the RG-N18000 without entering the MSC-ED card, as shown in the following figure.



Configuration command: **msc switch direct**

You can use the **bypass enable obs force** command when the optical bypass switch (OBS) is deployed.

## Mirror-based Traffic Diversion



Mirror the uplink port of the RG-N18000 to the MSC-ED card, mirror the TX packets on the uplink port to internal Port 1 of the MSC-ED card, and mirror the RX packets on the uplink port to internal Port 2 of the MSC-ED card.

When the MSC-ED card fails, only accounting is affected.

Configure traffic diversion on the uplink and downlink ports of the RG-N18000.

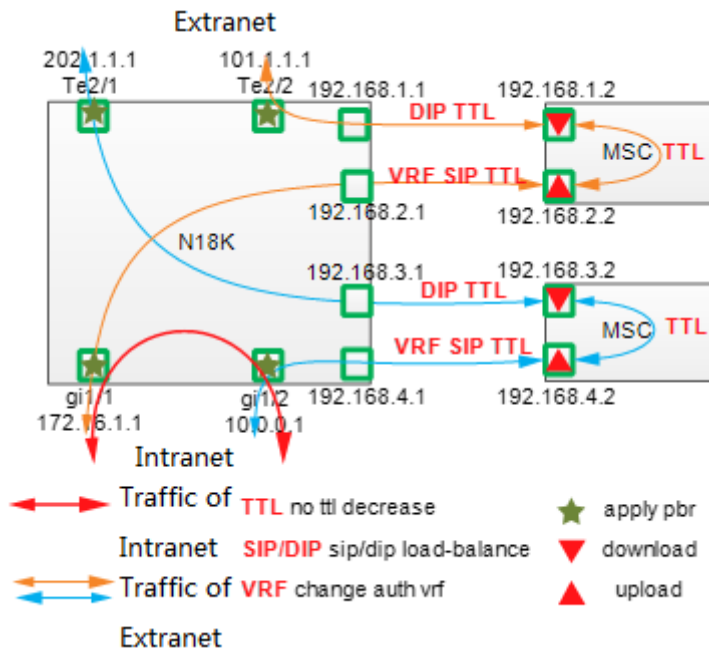
```
monitor session 1 destination interface AggregatePort 1 switch
monitor session 1 source interface GigabitEthernet 2/2/25 tx
monitor session 2 destination interface AggregatePort 2 switch
monitor session 2 source interface GigabitEthernet 2/2/25 rx
```

Configure port mirroring.

Remarks: 2/2/25 is the uplink port, and 2/2/23 is the downlink port.

### 4.2.5.3 PBR-based Traffic Diversion (in Gateway Mode)

The following figure shows the flowchart of PBR-based traffic diversion.



Ports connected between the MSC-ED card and the RG-N18000:

	18K VLAN	18K VLAN IP	18K-1 VSU:Port	18K-2 VSU:Port	MSC Port	MSC1 Port Ip	MSC2 Port Ip
Lan	10	10.10.10.1	Slot1/1/3	Slot2/1/3	T0/1	10.10.10.2	10.10.10.3
Wan	20	10.10.20.1	Slot1/1/4	Slot2/1/4	T0/2	10.10.20.2	10.10.20.3
MGMT	30	10.10.30.1	Slot1/1/5	Slot2/1/5	T0/3	10.10.30.2	10.10.30.3

Deployment logic:

1. Configure the device interconnection address.

- 
2. Configure an ACL for the network segments that require authentication.
  3. Design PBR.
  4. (Optional) Configure track support.
  5. Enable PBR and Web authentication in interface configuration mode.

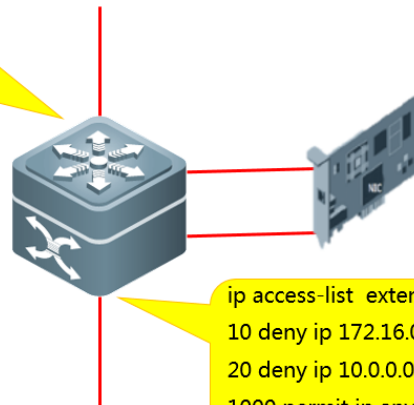
**Step 1: Configure the device interconnection address.**

To implement PBR-based traffic diversion, reconstruct the Layer 2 interfaces connected between the MSC-ED card and the RG-N18000 into Layer 3 interfaces.

**Step 2: Configure an ACL for network the segments that require authentication.**

Method 1:

```
ip access-list extended download
10 deny ip any 172.16.0.0 0.0.255.255
20 deny ip any 10.0.0.0 0.255.255.255
1000 permit ip any any
```

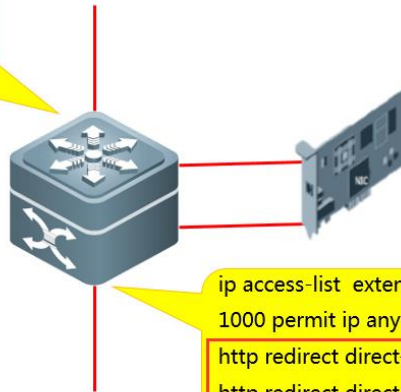


```
ip access-list extended upload
10 deny ip 172.16.0.0 0.0.255.255 any
20 deny ip 10.0.0.0 0.255.255.255 any
1000 permit ip any any
```

Filter marked user traffic to prevent accounting-free traffic from entering the MSC-ED card. pay attention to the marking direction. Clarify the source and destination of data traffic, and define **any** correctly for extranet access traffic and intranet access traffic.

Method 2:

```
ip access-list extended download
1000 permit ip any any
```

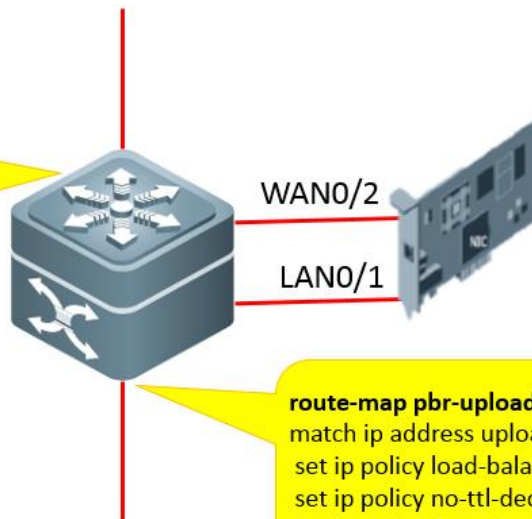


```
ip access-list extended upload
1000 permit ip any any
http redirect direct-site 10.0.0.0 255.0.0.0
http redirect direct-site 172.16.0.0 255.255.0.0
```

You can configure network segments to be exempt from authentication to protect the traffic defined with **any any** from anomalies. When traffic from authentication-free network segments enters the MSC-ED card, the traffic is transferred to the authentication-free VRF or is blocked.

### Step 3: Configure PBR-based traffic diversion on the ingress and egress of the RG-N18000.

```
route-map pbr-download permit 10
match ip address download
set ip policy load-balance dst-ip
set ip policy no-ttl-decrease
```



```
route-map pbr-upload permit 10
match ip address upload
set ip policy load-balance src-ip
set ip policy no-ttl-decrease
set ip policy I3-auth
```

#### Note:

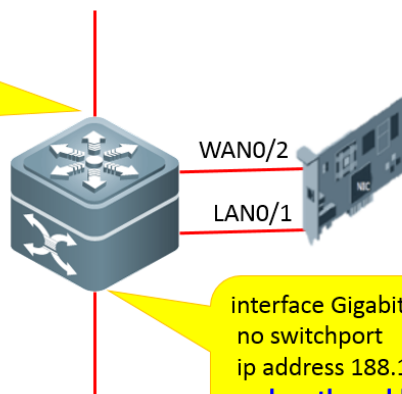
On the MSC-ED card, the WAN port is fixed to TenG0/2 and the LAN port is fixed to TenG0/1.

The **set ip policy no-ttl-decrease** command (mandatory) is used to disable the function of deducting the TTL hops of traffic entering the MSC-ED card.

The **set ip policy I3-auth** command (mandatory) is used to divert users exempt from authentication to the authentication-free VRF.

### Step 4: Configure PBR-based traffic diversion on the ingress and egress of the RG-N18000.

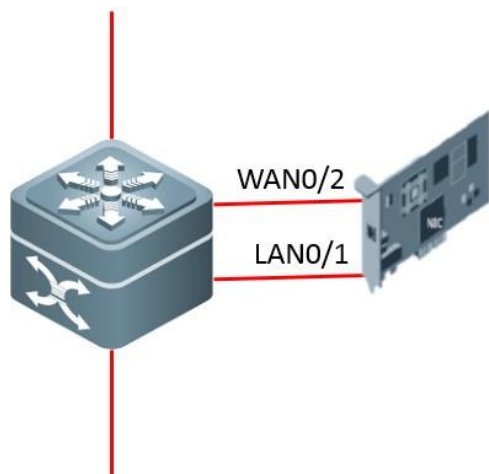
interface GigabitEthernet 9/1  
no switchport  
description link-to-server  
ip address 192.168.1.144 255.255.255.0  
ip policy route-map pbr-download



interface GigabitEthernet 9/5  
no switchport  
ip address 188.1.1.17 255.255.255.252  
web-auth enable eportalv2  
ip policy route-map pbr-upload

Note: This version supports Layer 3 Web authentication.

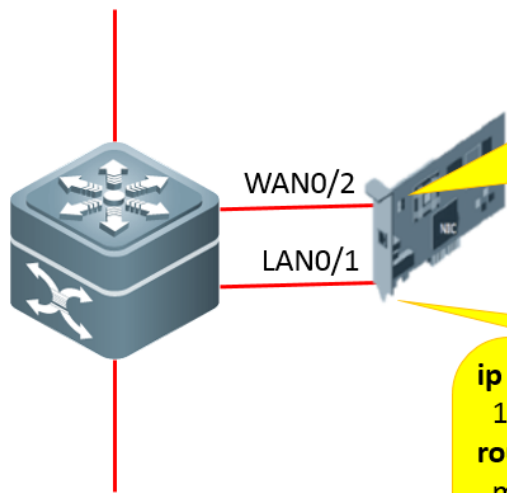
Step 5: Log in to the MSC-ED card and enable PBR-based traffic diversion.



MSC(config)#sys-mode gateway

Configure the MSC-ED card to enter gateway mode. Then the card restarts automatically.





```

ip access-list standard down
10 permit ip any any
route-map down permit 10
match ip address down
set ip next-hop 192.168.2.1
interface TenGigabitEthernet 0/2
ip address 192.168.1.2 255.255.255.0
ip policy route-map down

```

```

ip access-list extended up
100 permit ip any any
route-map up permit 10
match ip address up
set ip next-hop 192.168.1.1
interface TenGigabitEthernet 0/1
ip address 192.168.2.2 255.255.255.0
ip policy route-map up

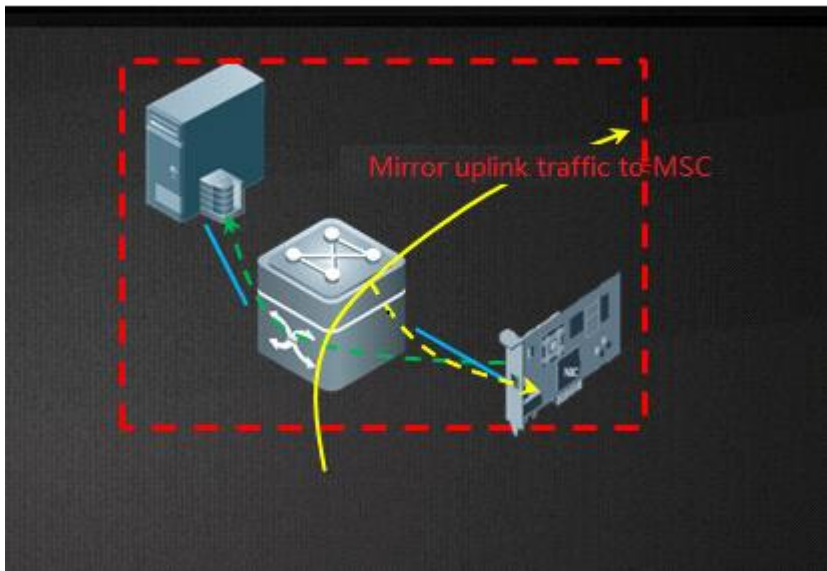
```

**Step 6: Configure track support.**

For details, see section 4.2.16 "Track Support for the RNS."



**4.2.5.4 Traffic Diversion Based on Port Mirroring**



---

Scenario description:

Mirror the uplink port of the RG-N18000 to the MSC-ED card, mirror the TX packets on the uplink port to internal Port 1 of the MSC-ED card, and mirror the RX packets on the uplink port to internal Port 2 of the MSC-ED card.

When the MSC-ED card fails, only accounting is affected.

Configuration example:

1. Mirror configuration: Configure TE 2/4/24 as the uplink port of the RG-N18000.

```
monitor session 1 destination interface AggregatePort 1 switch
monitor session 1 source interface TenGigabitEthernet 2/4/24 tx
monitor session 2 destination interface AggregatePort 2 switch
monitor session 2 source interface TenGigabitEthernet 2/4/24 rx
```

2. Configure the uplink and downlink ports of the RG-N18000.

```
interface GigabitEthernet 1/3/13
switchport access vlan 11
redirect destination interface TenGigabitEthernet 2/4/24 acl ipv4 in
web-auth enable eportalv2

interface TenGigabitEthernet 2/4/24
switchport access vlan 11
redirect destination interface GigabitEthernet 1/3/13 acl ipv4 in
```

Apply an ACL to the ports.

```
ip access-list extended ipv4
10 permit ip any any
```

3. Configure the internal ports of the MSC-ED card.

```
interface AggregatePort 1
aggregateport load-balance src-ip
switchport access vlan 222

interface AggregatePort 2
aggregateport load-balance dst-ip
switchport access vlan 333
```

---

## 4.2.6 IPv6 Deployment

### Mandatory

The IPv6 feature ensures normal forwarding of IPv6 data during the IPv4 authentication control process.

IPv6 can be deployed in strict, loose, or compatible mode.

#### [Deployment mode] [IPv4 packet forwarding rule] [IPv6 packet forwarding rule]

[Strict mode] [Packets compliant with the IPv4+MAC criteria are forwarded] [IPv6 packets are forwarded.]

[Loose mode] [Packets compliant with the IPv4+MAC criteria are forwarded] [All IPv6 packets are forwarded.]

#### Configuration command reference:

```
Ruijie(config)#address-bind ipv6-mode ?
looseIPv6 loose mode    (Recommend)
strictIPv6 strict mode  (default: strict) ;
```

## 4.2.7 Clock Synchronization Configuration

Clock synchronization must be configured for the MSC-ED card to maintain clock consistency with the background and thus ensure proper accounting.

Configure the time zones of the RG-N18000 and the MSC-ED card to be consistent. (The time zone of the MSC-ED card is managed by the SNTP server.)

Configuration example: **clock timezone dongba +8 0**

Configure NTP master on the RG-N18000.

Configuration example: **ntp master 8**

The RG-N18000 is the system time source and provides the NTP server to the MSC-ED card.

For other configurations, see section 4.3.4 "(Mandatory) Clock Synchronization."

## 4.2.8 Authentication Exemption

### Configuration Steps

1. Configure a list of authentication-free sites.

Configure a list of sites that users can access without authentication. A common application scenario is that users can download the Su client from a public resource site before authentication. To configure the IP addresses of authentication-free sites (straight-through sites), run the following command in global configuration mode:

#### http redirect direct-site

2. Configure authentication-free addresses.

Web authentication is implemented based on the port status (enabled or disabled). Some IP addresses can be accessed without authentication, for example, the IP addresses accessed by managers and the IP addresses of printers, hydroelectric

---

systems, and other public resources. To configure a list of authentication-free IP addresses or network segments, run the following command in global configuration mode:

#### web-auth direct-host

3. Configure a secure channel.

An ACL-based authentication-free mechanism can be configured globally or based on ports.

Deployment in global configuration mode:

```
ip access-list extended safe ( extended acl )
1 per ip host xxxx xxxxxx
security global access-group safe
```

## 4.2.9 Portal Escape

The roles that take part in the AAA process include users, the NAS, AAA server, and portal server. Users cannot access the Internet when the portal server cannot respond timely to users' authentication requests due to a failure. To address this problem, the RG-N18000 provides the portal escape function. The RG-N18000 monitors the performance of the portal server in real time. When the portal server fails, automatic configurations are made to allow new users to access the Internet without authentication while maintaining the network access of existing online users, providing favorable user experience.

#### Notes:

- The portal detection function must be configured when the escape function is used.
- If multiple portal servers are configured, the escape function takes effect only when none of the portal servers is available.
- The escape function is intended only for the portal server, not the RADIUS server.

#### Configuration commands:

```
safe web-auth portal-escape [nokick] // Command used to configure the portal escape function:
web-auth portal-check interval 3 retransmit 3 // Command used to configure the portal detection interval
and times:
```

#### Configuration description:

Configure the portal escape function if the continuity of critical services on the network needs to be maintained when the portal server fails. The portal detection function must be configured together with the portal escape function. When **nokick** is specified, users will not be forced offline when escape takes effect; when **nokick** is not specified, all users will be forced offline.

## 4.2.10 RADIUS Escape

The roles that take part in the AAA process include users, the NAS, AAA server, and portal server. Users cannot access the Internet when the portal server cannot respond timely to users' authentication requests due to a failure. To address this problem, the RG-N18000 provides the RADIUS escape function. The RG-N18000 monitors the performance of the RADIUS server in

real time. When the RADIUS server fails, automatic configurations are made to allow new users to access the Internet without authentication while maintaining the network access of existing online users, providing favorable user experience.

**Configuration command:**

```
radius-server host xxx.xxx.xxx.xxx test username ruijie key ruijie //ip address of SAM server
radius-server dead-criteria time 3 tries 3
web-auth radius-escape
```

**Configuration description:**

If the RADIUS server is unavailable, the authentication page is displayed when users attempt to access the extranet. Users can pass authentication using any account name and password.

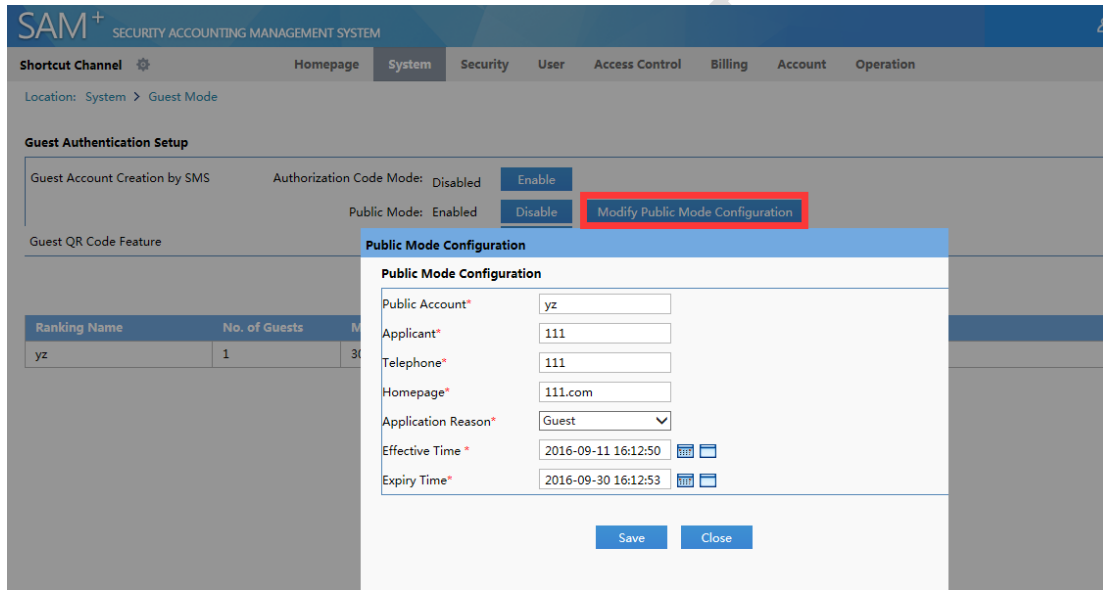
Ensure that the dead time of the RADIUS server is not 0.

### 4.2.11 QR-code-based Access

**QR code scan intended for guests**



**Configuring the guest QR code scan feature on the SAM+ server**



After Web authentication is enabled on the device, unauthenticated users cannot access network content. After authentication-free URLs are configured, the device permits the traffic of unauthenticated users that matches the configured URLs, allowing those users to access the URLs. Because the WeChat app and iPhones require server access, the QR code scan feature of the WeChat and iPhones do not support QR-code-based authentication. In the new solution, you can deploy a DNS relay on the RG-N18000 to permit traffic from the WeChat app and iPhones.

#### Configuration example:

```
N18K(config-if-GigabitEthernet 1/1)#dns-sniffer enable //Enable the DNS relay function on the uplink port.
N18K(config)#free-url weixin //Configure the WeChat server address as a straight-through address.
N18K(config)# free-url url captive.apple.com //Configure the iPhone server address as a straight-through address.
```

**Note: Because the Tencent server uses a unified address, after the WeChat server address is configured as a straight-through address, access to other Tencent services is also permitted without authentication.**

## 4.2.12 Restart Protection

### Working Principle

When the device is restarted, it generates large noises as many users perform authentication. The restart protection function is used to solve the authentication congestion problem of the authentication server during the restart process.

Enable restart protection for authentication based on different IP address segments. Configure the following authentication sequence: authenticate IP addresses ending with 0 to 7 (for example, x.x.x.0–x.x.x.7) -> authenticate IP addresses ending with 8 to 15. The authentication process proceeds to IP addresses ending with greater numbers. Users can pass authentication within 30 minutes, ensuring device performance and stability.

#### Configuration example:

```
Ruijie#conf
```

```
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)#auth-reboot protect
```

## 4.2.13 DHCP Support

### Working principle

The DHCP address release notification function is used to notify the RG-N18000 (deployed with the DHCP server) of DHCP address release, in order to force Web-authenticated users offline. This function is enabled by default.

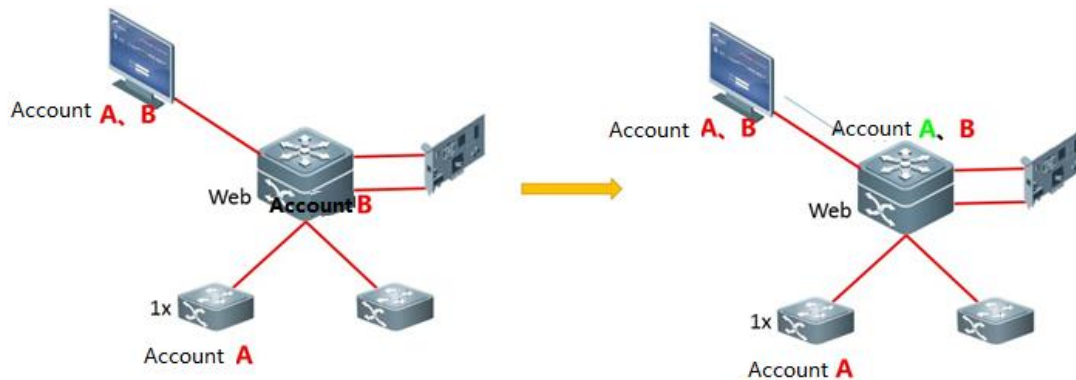
You can use the following command to disable this function.

Configuration example:

```
Ruijie#conf
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# web-auth dhcp-server check (enable by default, not recommend to disable this function)
```

## 4.2.14 Remote Authentication

Remote authentication is only applicable to the Layer 3 core. After users pass authentication on an access and aggregation switch, the SAM server synchronizes the users to the RG-N18000, which controls the users' access to the extranet and collects traffic statistics using the MSC-ED card.



### Configuration Steps

1. Configure the remote authentication server.

```
[no] remote-auth server host ipv4 [port port-num]
```

Configure the IP address and source port of the remote authentication server. The IP address must be an IPv4 address, and the source port is optional. If the source port is not configured, any port with the configured IP address can be connected to the device. If the source port is configured, a connection must be set up based on the specified IP address and port. Remote authentication is enabled after the IP address and source port are configured.

2. Configure remote authentication port control.

```
[no] remote-auth enable
```

After remote authentication is enabled, the gateway traffic of unauthenticated users is blocked. Remote authentication control must be configured on the port connected to users requiring remote authentication. After remote authentication control is enabled, the gateway traffic of all users is blocked. After a remote user passes authentication, a permit-access entry mapping the user's IP address is delivered. Remote authentication supports router interfaces (including AP router interfaces) and SVIs.

3. Configure the SAM server.

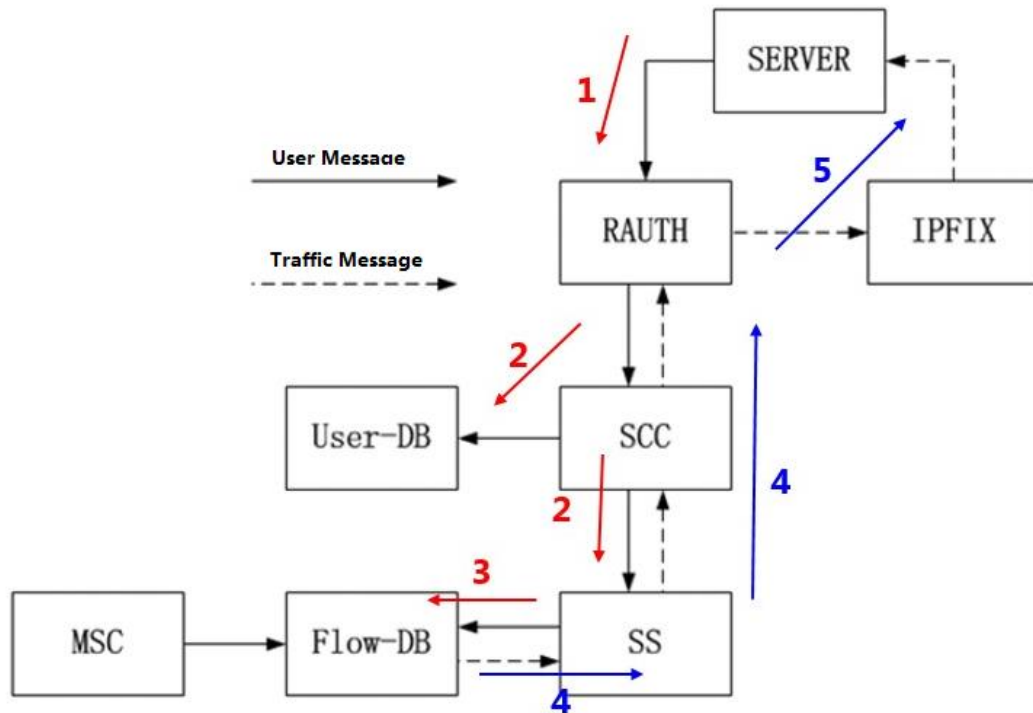
Select **Use Port 2009** when you add the RG-N18000 to the SAM server.

The screenshot shows the SAM+ configuration interface for a device. The page title is "SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM" with a user "admin" and "Logout" options. The navigation menu includes "Homepage", "System", "Security", "User", "Access Control", "Billing", "Account", and "Operation". The "System" tab is active, and the "Device" configuration page is displayed. The configuration fields are as follows:

Field	Value
Device IP Address*	172.29.100.1
Device Type*	Ruijie Switch
IP Type*	IPv4
Device Key*	ruijie
Model*	N18K
PPPoE Authentication	Please use comma or space to
IPOE+Web	Please use comma or space to
Domain	separate multiple domains
Authentication Domain	separate multiple domains
Community*	ruijie
MAC Address*	For trusted ARP binding application, MAC address must be filled
SNMP Proxy Port	If you do not fill in, the default port 161 will be adopted
DHCP Login Username	
DHCP Login Password	
Telnet Login Username	
Telnet Login Password	
Telnet Privileged	
Device Group*	default
Password	
Device Name	
Device Location	
Device Timeout (secs)*	3
Device Idle Time (secs)	
Device Feature	<input type="checkbox"/> Re-authentication <input type="checkbox"/> Account Update <input type="checkbox"/> Client Detection
Area	Please Select (Device IP(v4))
Web Authentication	<input type="checkbox"/> Select this to enable the web authentication for the
RG-ePortal	
Option	switch
Management Port	
Integration	
Description	
Port(1~65535)	
SU Version Check	<input checked="" type="checkbox"/> Enable (Applicable to authentication client + access switch authentication mode)
N18K Feature	<input checked="" type="checkbox"/> Layer Gateway Certification <input checked="" type="checkbox"/> Use Port 2009

Internal implementation logic of remote authentication





1. After related configuration is complete, the remote authentication component Remote-Auth (RAUTH) listens to TCP Port 2009 for server connection setup.
2. When RAUTH receives an online user record, it sets the user to SCC, which then adds the user to a user database (User-DB) and sets the user to the SS.
3. The SS permits the gateway traffic coming from the IP address and adds the user information to a flow database (Flow-DB). The MSC-ED card collects traffic statistics on the user based on the information provided by the flow database.
4. When the traffic threshold or the update period is reached, the SS sends traffic statistics to the SCC, which then transparently transmits the statistics to RAUTH.
5. RAUTH locates the online user based on the IP address in the traffic statistics, encapsulates the user information into an IPFIX message, and sends the message to the IPFIX, which then sends the user information to the server for accounting.

After modularization, the SS is integrated on the PD as an interface for receiving information from the PI (which provides services related to switch hardware).

The SCC is a component of the PI and functions as a security control center. The SCC delivers entries related to the PI's security functions.

#### **Message types of remote authentication during the packet capture process**

- #1 message: The server instructs the RG-N18000 to block the gateway traffic of a user (NULL).
- #2 message: The server notifies the RG-N18000 that a user is in arrears.
- #3 message: The server notifies the RG-N18000 that a user goes online.
- #4 message: The server notifies the RG-N18000 that a user goes offline.

- 
- #5 message: The server notifies the RG-N18000 that a user has no available duration.
  - #6 message: The server notifies the RG-N18000 that a user has no traffic (NULL).
  - #7 message: The RG-N18000 acknowledges a notification sent by the server.
  - #8 message: The server instructs the RG-N18000 to synchronize online users.
  - #9 message: the last packet during online user synchronization.
  - #10 message: heartbeat packet.
  - #11 message: The RG-N18000 notifies the server that a user's traffic quota has run out.

## 4.2.15 PBR Configuration Reference from Other Vendors

### PBR Logic

---

1. Identify routes.
2. Define a PBR template.
3. Invoke the template.

### Cisco PBR Configuration Reference

---

```
My3377(config)#access-list 10 permit 192.168.1.0 //Mark the traffic that needs to be diverted.
My3377(config)#access-list 20 permit 192.168.2.0 //Same as above.
My3377(config)#route-map nexthop permit 10 //Specify a name.
My3377(config-route-map)#match ip address 10 //Match with a list.
My3377(config-route-map)#set ip next-hop 192.168.100.1 //Configure a policy.
My3377(config-route-map)#exit
My3377(config)#route-map nexthop permit 20
My3377(config-route-map)#match ip address 20
My3377(config-route-map)#set ip next-hop 192.168.100.2 //Configure another policy.
My3377(config-route-map)#exit
My3377(config)#route-map nexthop permit 30
My3377(config)#int s2/1
My3377(config-if)#ip policy route-map nexthop //Invoke the policies in interface configuration mode.
My3377(config-if)#exit
```

### Huawei PBR Configuration Reference

---

1. Identify routes.

```
[Quidway] acl 3001
    [Quidway-acl-adv-3001] rule permit ip source 10.1.40.0 0.0.0.255 destination 10.1.40.0 0.0.0.255
//permit
[Quidway-acl-adv-3001] quit
```

2. Define a PBR template.

Configure traffic classification.

#Create traffic classification packets on the Quidway.

```
[Quidway] traffic classifier a
[Quidway-classifier-a] if-match acl 3001
[Quidway-classifier-a] quit
```

#Create Traffic Behavior A on the Quidway.

```
[Quidway-classifier-a] quit [Quidway] traffic behavior a
[Quidway-behavior-a] redirect ip-nexthop 10.1.99.5 //Redirect the traffic from Network Segment 40 to
the next hop address 10.1.99.5.
[Quidway-behavior-a] quit
```

#Create Traffic Policy A on the Quidway and bind traffic classification with Traffic Behavior A.

```
[Quidway] traffic policy a
[Quidway-trafficpolicy-a] classifier a behavior a
```

3. Invoke the template.

```
[Quidway] interface gigabitethernet 0/0/0
[Quidway-Gigabitethernet0/0/0] traffic-policy a inbound
[Quidway-Gigabitethernet0/0/0] quit
```

## ZTE PBR Configuration Reference

---

1. Identify routes.

```
acl extended number 100
rule 5 permit ip 10.50.0.0 0.0.3.255 0.0.0.0 255.255.255.255
```

2. Define a PBR template.

```
route-map name ZY permit 100
```

```
match ip address 100
set default ip next-hop 10.0.0.1
set default interface g7/5
set default interface g7/10
```

3. Invoke the template.

```
interface gei_7/5
ip policy route-map ZY
interface gei_7/10
ip policy route-map ZY
```

## 4.2.16 Track Support for the RNS

The phase 3 solution makes improvement to the RNS function, which can be used by PBR.

1. Monitor the directly connected interface of the MSC-ED card over ICMP echo.

```
ip rns 1 icmp-echo 192.168.1.2 timeout 6000
ip rns 2 icmp-echo 192.168.1.3 timeout 6000
ip rns 3 icmp-echo 192.168.1.4 timeout 6000
ip rns 4 icmp-echo 192.168.1.5 timeout 6000
```

2. Configure track support for the RNS.

```
track 100 rns-list 1
track 200 rns-list 2
track 300 rns-list 3
track 400 rns-list 4
```

3. Enable track support for the RNS.

```
route-map pbr-upload permit 10
set ip next-hop verify-availability 19.1.1.2 track 100
set ip next-hop verify-availability 19.1.1.3 track 200
set ip next-hop verify-availability 19.1.1.4 track 300
set ip next-hop verify-availability 19.1.1.5 track 400

route-map pbr-download permit 10
set ip next-hop verify-availability 19.1.2.2 track 100
set ip next-hop verify-availability 19.1.2.3 track 200
set ip next-hop verify-availability 19.1.2.4 track 300
```

```
set ip next-hop verify-availability 19.1.2.5 track 400
```

## 4.2.17 Bypass

### Working Principle

The bypass function of the OBS is used to transfer traffic to the bypass link so that traffic does not enter the switch connected to the OBS when the OBS transitions to the bypass state.

The straight-through bypass function of a switch is applicable in the environment where the switch is connected to the MSC-ED card, but not to the OBS. When the switch enters the bypass state, the traffic that otherwise enters the MSC-ED card is transferred to the straight-through path of the switch that is configured by the **msc path** command.

#### Bypass detection:

You can add multiple line cards to a detection group. When the bypass detection function detects that all line cards of the group are abnormal, it prompts that the detection group is abnormal.

You can configure multiple detection groups. When the bypass detection function detects that a group is abnormal, it switches to the bypass state. When the group is recovered, it switches back to the non-bypass state.

The bypass detection function allows you to associate the detected MSC-ED card with a track ID. You can configure track support for the RNS to detect the MSC-ED card and associate with the same track ID to configure bypass detection for the RNS.

#### Configuration example:

```
bypass enable obs          //Enable the bypass function of the OBS.
bypass enable switch-direct //Enable the straight-through bypass function of the switch.
bypass group 1 dev 1 slot 7
bypass group 2 dev 1 slot 6 track 6
bypass group 2 dev 1 slot 5 track 5 //Add the MSC-ED cards in Slot 5 and Slot 6 to Group 2.
ip rns 5 //Configure ICMP detection.
  icmp-echo 210.77.16.23
  frequency 6000
ip rns 6
  icmp-echo 210.77.16.22
  frequency 6000
ip rns schedule 5 start-time now life forever //Configure the scheduling method, start time, and time
to live (TTL) of an IP RNS test.
ip rns schedule 6 start-time now life forever
ip rns reaction-configuration 5 react allfail action-type Track //Configure the proactive threshold
monitoring and triggering mechanism for the IP RNS test.
ip rns reaction-configuration 6 react allfail action-type Track
track 5 rns 5
track 6 rns 6
```

---

## 4.2.18 DHCP Support

### Working Principle

The DHCP server is deployed on the RG-N18000 and sends notification messages to the RG-N18000. Web-authenticated users are forced offline when the DHCP address is released.

Configuration example

```
Ruijie#conf
Enter configuration commands, one per line. End with CNTL/Z.
Ruijie(config)# web-auth dhcp-server check
```

:

#### Note:

Because the **dhcp-guard** command configures rate limiting based on five MAC addresses by default, you need to make adjustments manually.

1. Check the threshold.

```
Ruijie#show nfpp dhcp-guard summary
(Format of column Rate-limit and Attack-threshold is per-src-ip/per-src-mac/per-port.)
Interface Status Isolate-period Rate-limit Attack-threshold
Global Enable 0-/5/1200 -/10/1500
Maximum count of monitored hosts: 20000
Monitor period: 600s
```

2. Change the threshold of **nfpp dhcp-guard Rate-limit per-src-mac** to that of **nfpp dhcp-guard Rate-limit per-port**.

Recommended configuration:

```
N18K #sh run | be nfpp
nfpp
dhcp-guard rate-limit per-src-mac 8000
dhcp-guard attack-threshold per-src-mac 8000
```

## 4.2.19 IPoE

### 4.2.19.1 IPoE Perception-free Authentication

#### Working Principle

When a user connects to the Internet for the first time, the user must perform Web authentication. After Layer 3 forwarding, the packet does not contain the MAC address of the user's terminal. Therefore, the MAC addresses of terminals must be obtained

---

by other means during initial authentication. After the DHCP monitoring function is enabled, all DHCP packets are copied to generate DHCP snooping entries. Then the DHCP snooping function is used to provide entry notifications.

The RG-N18000 learns the association between IP address and MAC address through DHCP snooping. When the Web authentication server generates user entries used for authentication, it needs to query the MAC addresses of terminals based on their IP addresses and encapsulate the MAC addresses used for authentication. (The server background can bind MAC addresses with usernames only after the server obtains the MAC addresses.)

When a user performs authentication by clicking the portal link in **Favorites**, the Web authentication server, after receiving a portal authentication request, obtains the user's MAC address based on the IP address contained in the request, in order to create a user entry.

When the user applies for DHCP upon subsequent access to the Internet, IPoE authentication is triggered, whereby the MAC address contained in the DHCP request is used as the username and password. After authentication, the Web authentication server delivers a route to permit the user entry.

Configuration example:

1. Run the **ip dhcp snooping monitor** command in global configuration mode.
2. Run the **ipoe-auth enable** command on the port configured with Web authentication control.
3. In the scenario where the gateway mode is used and the DHCP server is located on the RG-N18000, because the IPoE controlled port is different from the interface learned by DHCP snooping entries, you need to run the following command to configure interface binding for IPoE authentication:

**ipoe-auth binding source interface xxx destination interface yyy**

**source** indicates the interface learned by DHCP snooping, and **destination** indicates the IPoE controlled port.

**Note:**

IPoE perception-free authentication is only applicable in the scenario where the DHCP server is located on the RG-N18000 or the RG-N18000 is connected in the uplink direction.

**[Important] You can only configure an AAA method list when IPoE is implemented in Layer 3 scenarios, but you cannot configure dot1x.**

## 4.2.19.2 Escape Function

The escape function takes effect for IPoE users when the RADIUS server fails.

### Working Principle

- The test account of the RADIUS server can be configured on the RG-N18000 for server detection. The RG-N18000 triggers RADIUS escape when it detects that the RADIUS server is unreachable, or it cannot interact properly with the server. When new users trigger authentication, the RG-N18000 returns the successful result without password verification.
- When the RADIUS server is recovered, packet exchange using the test account is restored, allowing the RG-N18000 to determine that the RADIUS server is normal and disable the escape function.
- If the test account is not configured on the RG-N18000, the RG-N18000 determines whether the RADIUS server is abnormal according to the exchange of authentication packets. The RG-N18000 enables the escape function when it

---

detects that the RADIUS server is abnormal. However, when the RADIUS server is recovered, the RG-N18000 cannot restore the server status.

After you run the **ipoe-auth enable** command in interface configuration mode, run the **ipoe-auth critical** command to enable authorization for new authenticated users when the RADIUS server is unreachable.

In addition, run the **ipoe-auth critical recovery action reinitialize** command. If the escape function is enabled on a port, authenticated users on the port can access the Internet without re-authentication after the RADIUS server is recovered. The RG-N18000 initiates authentication only to users authenticated in escape mode during RADIUS server inaccessibility.

## 4.2.20 Intranet Authentication without the MSC-ED Card

The packet forwarding process for Layer 3 authentication with the MSC-ED card is as follows: After packets are transferred over the authentication VRF route, traffic is diverted to the MSC-ED card for accounting and traffic policy implementation; then the traffic is diverted to the RG-N18000 for forwarding over the VRF0 route.

1. When a packet enters the RG-N18000 over the authentication-enabled port and then is forwarded over the authentication VRF route, the RG-N18000 queries the host routing table over SIP. If the host routing table does not have a matching entry, the packet is matched with the FP entry. Then Web authentication is performed. After the user passes authentication, a SIP authentication routing entry is delivered to the routing table.
2. If the host routing table has a matching entry, the packet is matched with the FP entry and forwarded to the MSC-ED card for accounting and traffic policy implementation.
3. The MSC-ED card forwards the packet to the RG-N18000, which then forwards the packet over a regular route.

In the general education sector, authentication is required for access between different schools. Layer 3 authentication can be considered as intranet authentication, but such an authentication scenario does not have the MSC-ED card. For this reason, intranet authentication cannot be performed based on the traffic diversion mechanism applicable to the MSC-ED card. In this case, packet forwarding must be enabled for the authentication VRF route.

### Working Principle

1. When authenticated users access the extranet without the MSC-ED card, packets are forwarded to the extranet based on the default next hop specified by PBR.
2. After an intranet user passes authentication, the RG-N18000 delivers an authentication route prefixed with the user's IP address. The RG-N18000 queries the routing module to obtain the route's egress (next hop) and sets the complete route to the hardware. The route has a higher priority than the route with the default PBR-specified next hop.
3. When a user accesses an intranet, the packet is forwarded by matching an authentication route entry on the hardware.
4. Because packets are forwarded by matching authentication route entries during the intranet access authentication process when the MSC-ED card is not used, a CLI command is provided to determine whether to enable the RG-N18000 to change the forwarding mode from traffic diversion (when the MSC-ED card is used) to authentication routing.

Configuration example:

```
N18K(config)#auth-route forward
This operation will make smaller capacity and clear all users. Are you sure to continue? (Y/N)y
```



The following table lists the impact on the original solution after forwarding is enabled in authentication routing mode. (Only core scenarios are considered, and intranet access authentication is not required in transparent transmission mode.)

Scenario	Description	Result
Intranet access authentication not required MSC-ED card available	Extranet traffic is diverted to the MSC-ED card through PBR.	No impact Supported capacity: 10,000 online terminals You are advised to disable forwarding in authentication routing mode.
Forwarding during the intranet access authentication process MSC-ED card available	Extranet traffic and intranet traffic are diverted to the MSC-ED card through PBR. (The route specified by PBR has a higher forwarding priority than regular routes.)	No impact Supported capacity: 10,000 online terminals You are advised to disable forwarding in authentication routing mode.
Intranet access authentication not required MSC-ED card not available	Extranet traffic is forwarded to the next hop specified by PBR.	No impact Supported capacity: 10,000 online terminals You are advised to disable forwarding in authentication routing mode.
Forwarding during the intranet access authentication process MSC-ED card not available	Extranet traffic is forwarded to the default next hop specified by PBR. Intranet traffic is forwarded to the next hop.	Forwarding in authentication routing mode must be supported at Phase 4.

Evaluation of the impact on the original solution caused by forwarding in authentication routing mode.

**Note:**

The RG-N18000 supports 10,000 users during forwarding in authentication routing mode.



### 4.2.21 IP-Portal Mapping

The roles that take part in the AAA process include users, the NAS, AAA server, and Portal server. In the actual environment, authentication is enabled on a single interface but multiple portal servers are deployed due to server performance limit. Therefore, Layer 3 authentication supports the multi portal server feature. Packets are forcibly sent to the specified portal server according to users' SIP information, and the portal server pushes the Web authentication page to users. In this way, packets can be distributed to different portal servers, reducing the traffic burden on a single server.

---

**Implementation process:**

1. Configure a template for the Web authentication module and bind the template to the portal server and RADIUS authentication and accounting server. By default, the default RADIUS server is bound if you do not configure the server explicitly.
2. Bind SIP to the template ID for the Web authentication module. Different SIP records can be bound to the same template ID or different template IDs.
3. The Web authentication module delivers the SIP-template ID binding relationship to the SS module.
4. A user opens the Internet Explorer and initiates an HTTP request for accessing a website.
5. The NAS intercepts the HTTP request, and the SS registers the kernel packet reception/transmission interface and determines that authentication is enabled on the packet ingress. Because the user is not authenticated, the SS fills in the DSCP field of the packet with the corresponding template ID according to the SIP information of the packet, and forwards the packet to the Web authentication module of the NAS.
6. The Web authentication module determines that authentication is enabled on the port that receives the packet. Then it parses the DSCP field of the HTTP packet to obtain the template ID bound to the portal server, and forwards the packet to the specified portal server. The Web authentication module adds related parameters to the portal URL. For parameter details, see the description of CHAP authentication.
7. The portal server pushes the Web authentication page to the user.
8. The user fills in an account name, password, and other information on the authentication page, and then submits the information to the portal server.
9. The portal server submits the account name and password to the NAS in order to initiate authentication.
10. The NAS sends the account name and password to the RADIUS server bound with the template ID for authentication. The RADIUS server determines user validity according to the user information, and then returns the RADIUS access-accept/reject response to the NAS.
11. The NAS returns the authentication result to the portal server.
12. The portal server pushes a page containing the authentication result to the user.
13. The portal server returns a response to the NAS to indicate the reception of the authentication result.
14. The NAS sends a Start Accounting packet.

**Quick configuration case:**

一. Configure ip address of the radius server

```
aaa group server radius xjd1
server 192.168.1.13
aaa group server radius xjd3
server 192.168.1.25
```

二 Enable accounting and authentication function of 2 group

```
aaa accounting network default start-stop group xjd1
aaa authentication web-auth xjd1 group xjd1
aaa accounting network xjd1 start-stop group xjd3
aaa authentication web-auth xjd3 group xjd3
```

三 Create mapping template

```
web-auth template t1 v2
ip 172.18.105.11
url http://172.18.105.11:8080/eportal/index.jsp
authentication xjd1
accounting xjd1
```

```
web-auth template t2 v2
ip 10.10.10.11
url http://10.10.10.11:8080/eportal/index.jsp
authentication xjd3
accounting xjd3
```

四 Configure mapping relation of different segments.

```
web-auth mapping 1 ip-mapping 102.0.0.0 255.0.0.0 template t1
web-auth mapping 1 ip-mapping 104.0.0.0 255.0.0.0 template t2
```

五 Apply mapping on the interface.

```
interface GigabitEthernet 3/5
switchport access vlan 2
web-auth apply-mapping 1
```

**Configuration example:**

**Configure the RADIUS authentication and accounting server as follows:**

```
aaa group server radius xjd1
server 192.168.1.13
    aaa group server radius xjd3
        server 192.168.1.25
aaa accounting network default start-stop group xjd3
aaa authentication web-auth default group xjd3 >>> Configure the default RADIUS server named xjd.
aaa accounting network xjd1 start-stop group xjd1
aaa authentication web-auth xjd1 group xjd1>>> Configure the RADIUS server named xjd1.
```

**Configure multiple templates as follows:**

```
web-auth template eportalv2
```

```
ip 172.18.105.9
url http://172.18.105.9:8080/eportal/index.jsp
web-auth template t1 v2
ip 172.18.105.11
url http://172.18.105.11:8080/eportal/index.jsp
authentication xjd1
accounting xjd1
```

Bind the t1 template to the portal server 172.18.105.11 and to the RADIUS server 192.168.1.13 named **xjd1**.

```
web-auth template t2 v2
ip 172.18.105.12
url http://172.18.105.12:8080/eportal/index.jsp
```

Bind the t2 template to the portal server 172.18.105.12 and to the default RADIUS server 192.168.1.1.25 named **xjd3**.

**(Mandatory) Delete ports except HTTP Port 80 as follows** (the IP mapping feature only supports HTTP Port 80, but the RG-N18000 enables HTTP Port 80 and HTTP Port 443 by default):

```
no http redirect port 443
```

**Configure mapping rules as follows:**

```
web-auth mapping 1 ip-mapping 102.0.0.0 255.0.0.0 template t1
web-auth mapping 1 ip-mapping 104.0.0.0 255.0.0.0 template t2
```

**Apply the IP mapping feature and enable authentication on a port as follows:**

The HTTP request packets that match the IP mapping rules are forcibly forwarded to the portal server associated with the corresponding template. (Packets with SIP in the 102.0.0.0/8 network segment are forcibly forwarded to the portal server bound with the t1 template, and the xjd3 RADIUS server bound with the t1 template implements authentication and accounting. Packets with SIP in the 104.0.0.0/8 network segment are forcibly forwarded to the portal server bound with the t2 template, and the xjd1 RADIUS server bound with the t2 template implements authentication and accounting.) Packets with SIP in other network segments are forcibly forwarded to the portal server bound with the default eportalv2 template, and the default xjd3 RADIUS server implements authentication and accounting.

```
interface GigabitEthernet 3/5
switchport access vlan 2
web-auth apply-mapping 1 //Apply the mapping rules on the port.
web-auth enable eportalv2
```

---

**Note:**

The IP-portal mapping feature has the following restrictions in the scenario where users perform authentication by clicking the portal link in **Favorites**:

1. Only the default template-bound RADIUS server is supported in the scenario where users with static IP addresses perform authentication by clicking the portal link in **Favorites**.

**The reasons are as follows:**

- A user clicks the portal link in **Favorites** and submits the user's account name and password to the portal server. Because the packet does not enter the authentication port of the NAS, the SS module of the NAS does not change the DSCP value of the packet. The Web authentication module does not know the authentication port associated with the packet and therefore cannot obtain the template bound with the authentication port.
  - The portal server submits the account name and password to the NAS in order to initiate authentication.
  - The NAS sends the account name and password to the default RADIUS server because it cannot obtain the template.
  - In the case that the IP mapping rules are applied on the authentication port and the template is bound with a non-default RADIUS server, the default RADIUS server determines that the user is invalid because it does not store the user's account name and password, causing an authentication failure.
2. When users with dynamic IP addresses perform Layer 3 authentication in gateway mode, the DHCP-learned interface must be bound to the Web controlled port. In this way, when users click the portal link in **Favorites**, the users can obtain the Web controlled port according to the interface for DHCP address allocation and then obtain the correct template and the bound RADIUS server according to the Web controlled port.

The command is **web binding source interface xxx destination interface yyy**, in which *xxx* indicates the DHCP-learned interface and *yyy* indicates the Web controlled port.

## 4.3 MSC-ED Configuration

### 4.3.1 (Mandatory) Attack Prevention Configuration

The function of Web authentication attack prevention is used to discard packets that exceed the rate limit in the case of an authentication attack, in order to prevent other users from performing authentication for Internet access when the switch is attacked.

Configuration example: **Ruijie(config)#webauth-rate xx xx //rate limit per user**

---

#### Forwarding Attack Prevention

---

1. Connection limit

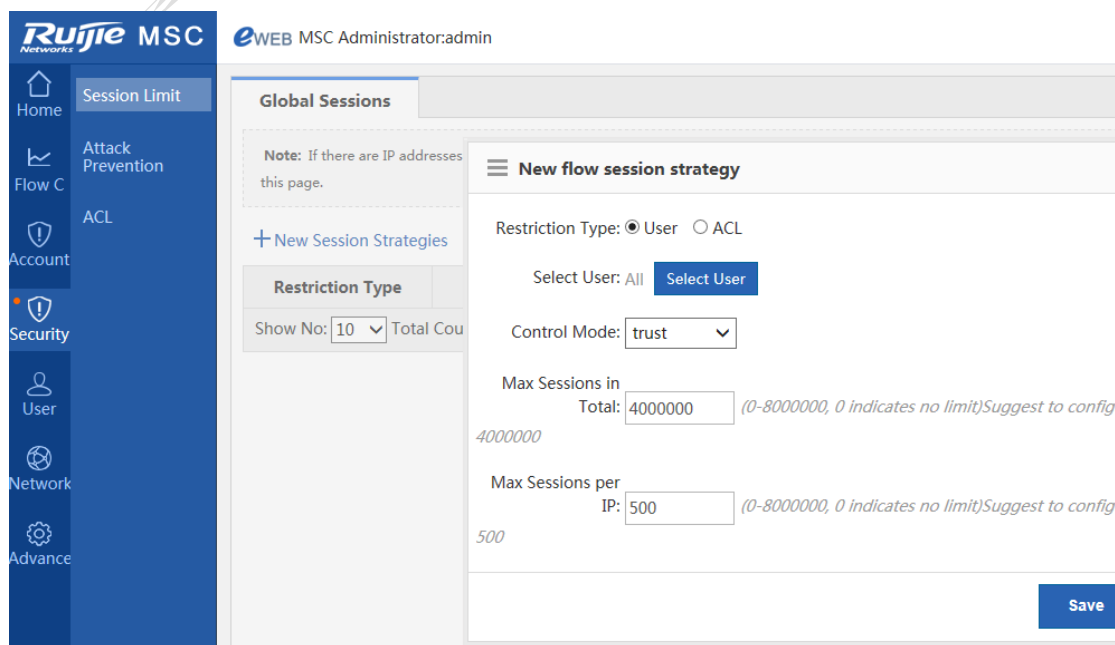
In the case of virus infection or an attack, an IP address may initiate many connections, causing resource depletion on the MSC-ED card (which supports up to 8,000,000 connections). Therefore, the number of connections must be limited in the

actual environment. It is recommended that the connection limit be set in the range 3,000 to 12,000 for PCs and smaller than 200,000 for servers. (The specific connection limit for a PC depends on whether the PC has tethering or other behaviors. After configuration, you can check the number of IP connections to determine whether to increase the connection limit.) Because the connection limit varies greatly between PCs and servers, two policies are configured (the latter policy takes effect first):

- (a) For all users (PCs), set the connection limit in the range 3,000 to 12,000 per IP address.
- (b) For the specified user group (all servers are added to the user group), set the connection limit in the range 200,000 to 500,000 per IP address.

**Note:**

- The connection limit per IP address is only supported on the user basis.
- The connection limit takes effect only for real IP addresses (which are used for TCP connection setup). To prevent attacks that use forged IP addresses to send non-TCP packets, configure a new flow session strategy, as shown in the following figure.



2. Global new connection limit

The preceding description introduces a type of attacks that deplete resources by setting up many connections from an IP address. Another type attacks targets at forwarding performance by setting up many connections within a short time. For a connection to set up, all enabled function modules need to match the full policy set, which greatly consumes forwarding performance. If many connections are set up within a short time, the performance of the MSC-ED card will become unstable, affecting Internet access experience. You can limit the number of new connections to prevent this type of attack.

**Steps for configuring a new connection limit:**

- 1) Default global configuration

For simplified configuration, the MSC-ED card delivers default parameters, as shown in the following figure.

Ruijie MSC eWEB MSC Administrator:admin

Session Limit

Attack Prevention

Session Policy: [Default Global Configuration] [Single IP Address Configuration] \ [Attack Suspect List]

DOS Attack Prevention:  Enable to prevent flow attacks

Attack Flow Logs: [Current Attack Logs] [Historical Attack Logs]

Save Restore default settings.

### Global Session Limit

Sessions per Virtual Host per Second in First 3 Min:  Range: 0-100000. Recommended: 5000-15000

Sessions per Virtual Host per Second Later:  Range: 0-100000. Recommended: 5000-15000

Default sessions per Real Host per Second:  Range: 0-100000. Recommended: 50-300

Save

#### Note:

- Virtual hosts refer to IP addresses without a TCP connection. Except DNSs, regular devices set up TCP connections. Therefore, related configurations have the effect of IP spoofing protection.
- It is recommended that the new connection limit for PCs be set in the range 50 and 300. The default value 2,000 is the new connection limit for servers of universities.

#### (1) Configuration per IP address

You can configure the new connection (session) limit for a single IP address to meet the new connection requirements of particular devices and forcibly specify the IP address as a real IP address (after which TCP connection setup is not required for the IP address). Then you can apply the new connection limit to the real IP address.

Ruijie MSC eWEB MSC Administrator:admin

Home Session Limit  
 Attack Prevention  
 Flow C  
 ACL  
 Account  
 Security  
 User  
 Network

**Attack Prevention**

Session Policy: [Default Global Configuration] [Single IP Address Configuration] [Attack Suspect List] ?

DOS Attack  
 Prevention:  Enable to prevent flow attacks

Attack Flow Logs: [Current Attack Logs] [Historical Attack Logs]

Save Restore default settings.

You can specify the session limit for a real host. 0 indicates no limit, which prevails over the default policy.  
 If an IP address is identified as a virtual IP address, you can configure it on this page as a real IP address.

### Session Limit per IP

IP :

Sessions per Second:  Range: 0-100000

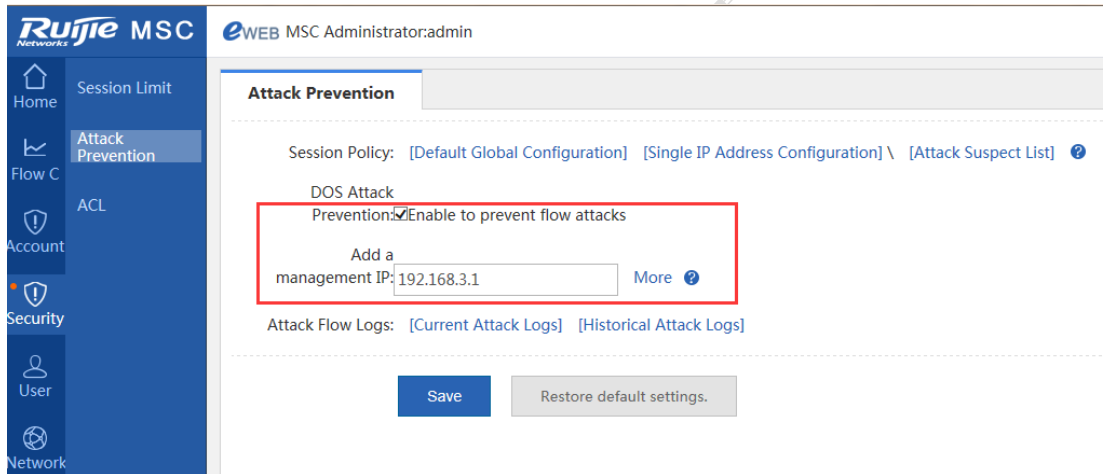
Save

IP	Sessions per Second	Action
Show No: 10 Total Count : 0	◀ First ◀ Previous 1 Next Last ▶	1 GO

### 3. Local attack prevention

To prevent attacks at the management layer (for example, heavy traffic is sent to the management IP address), you can enable local attack prevention for ensuring normal telnet and Web functions. You can configure rate limiting for the traffic sent to the management layer and set IP addresses exempt from rate limiting. The following figure shows the configuration interface. The IP address 1.1.1.1 is not rate-limited.





After flood attack prevention is enabled, an ACL is delivered, in which the **deny** section contains the protocols exempt from rate limiting, including routing protocols, UDP packets for DNS resolution and NTP, and TCP packets related to the telnet and Web functions.

```
ip access-list extended 2397
10 deny ospf any any
20 deny 112 any any
30 deny udp any eq domain any
40 deny udp any eq ntp any
50 deny tcp any any eq telnet
60 deny tcp any any eq www
1000 permit ip any any
list-remark //Local attack prevention
```

## 4.3.2 (Mandatory) Access Mode and Interface Configuration

### Access mode

#### 1) Overview

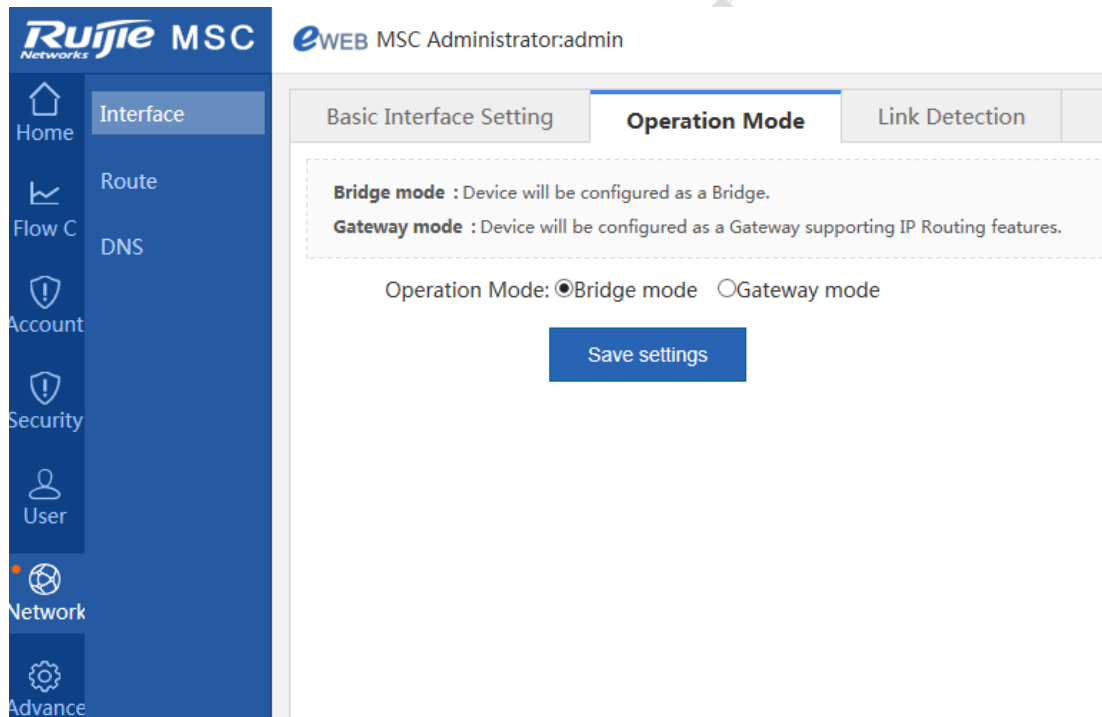
You can select the gateway mode or the bridge mode as the access mode based on your needs.

In gateway mode, all network interfaces are Layer 3 interfaces, and packets are forwarded based on a routing table.

In bridge mode, all network interfaces are Layer 2 interfaces, and packets are forwarded based on a bridge mapping table. Packets that are forwarded normally will not be modified.

#### (1) Access mode selection

Log in to the Web management interface of the MSC-ED card, and choose **Network > Interface > Operation Mode**.



## Interface Configuration

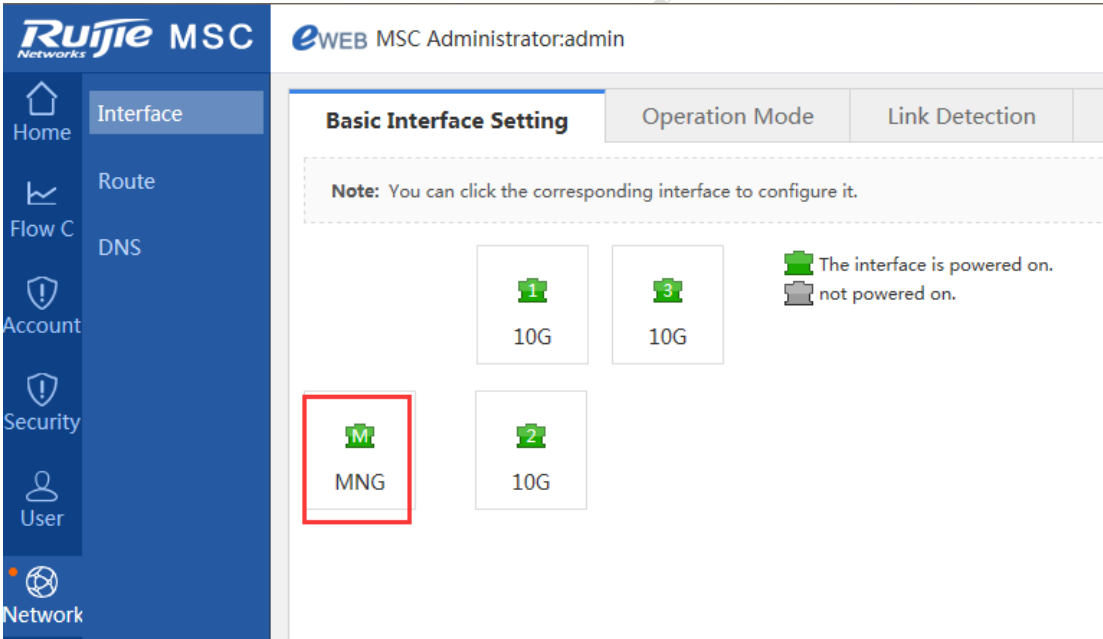
### (1) Configuration in gateway mode

The MSC-ED card in gateway mode has four Layer 3 interfaces, one of which is a management interface and the other three 10-GB interfaces.

#### (a) Management interface configuration

The management interface is used to manage the MSC-ED card. You only need to configure an IP address and a gateway address on the interface.

Log in to the Web management interface of the MSC-ED card, and choose **Network > Interface > Basic Interface Setting**.



(b) 10-GB interface configuration

The 10-GB interfaces are Layer 3 interfaces. You can configure IP addresses, NAT, PBR, and other routing functions on the interfaces.

Log in to the Web management interface of the MSC-ED card, and choose **Network > Interface > Basic Interface Setting**.

2) Configuration in bridge mode

The MSC-ED in bridge mode has a management interface and three 10-GB interfaces. The management interface is a Layer 3 interface used to manage the MSC-ED card, whereas the 10-GB interfaces are Layer 2 interfaces used to configure a bridge mapping table and implement bridge forwarding.

a) Management interface configuration

### MNG Intf Configuration

Management-IP Address:  \*

Subnet Mask:  \*

Gateway:  \*

b) Bridge mapping table configuration

The MSC-ED card has three 10-GB interfaces; therefore, up to two bridge mapping tables can be configured.

Log in to the Web management interface of the MSC-ED card, and choose **Network > Interface > Basic Interface Setting**. You can configure two bandwidth lines (that is, bridge mapping tables).

**Note:**

The first bandwidth line requires two 10-GB interfaces and supports two operation modes:

- In bridge forwarding mode, the MSC-ED card implements the following functions on incoming packets: traffic recognition, traffic blocking, flow control, and traffic audit.
- In software bypass mode, the MSC-ED card collects statistics on incoming and outgoing packets on interfaces, and then forwards the packets directly.

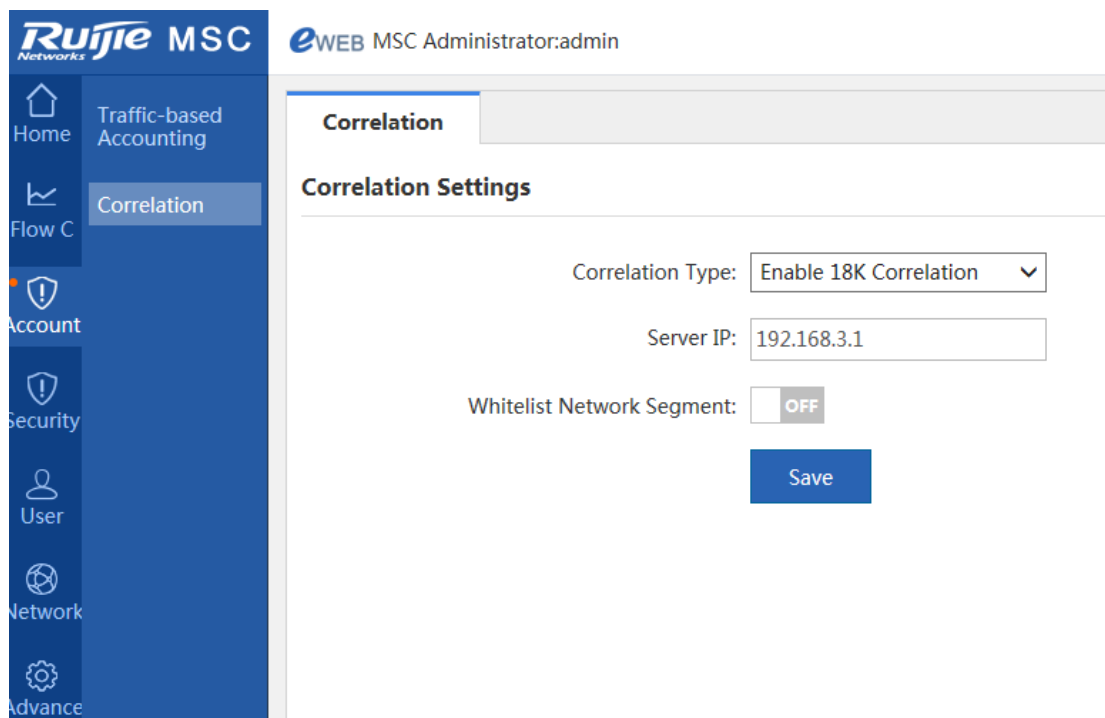
The second bandwidth line requires only one 10-GB interface and only supports the single-interface bridge mode.

In single-interface bridge mode, the interface does not forward packets, but is only used to exchange accounting data. It is different from the management interface.

Special attention: In both gateway mode and bridge mode, the TenG0/3 interface of the MSC-ED card is designed to exchange data with the RG-N18000. IPFIX support is enabled by default.

### 4.3.3 (Mandatory) RG-N18000 Correlation and IPFIX Configuration

Enabling correlation between the MSC-ED card and the RG-N18000 is a key configuration step.

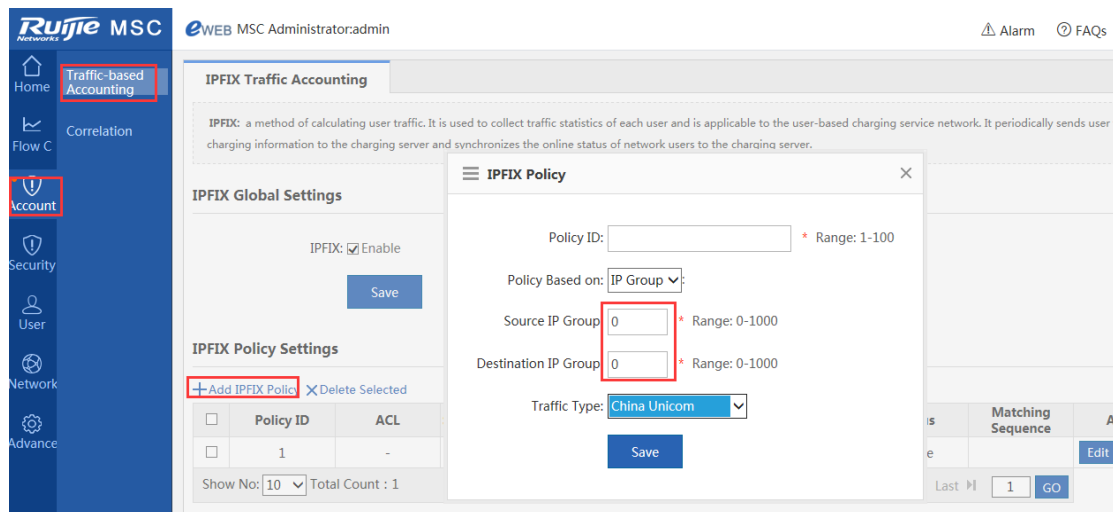
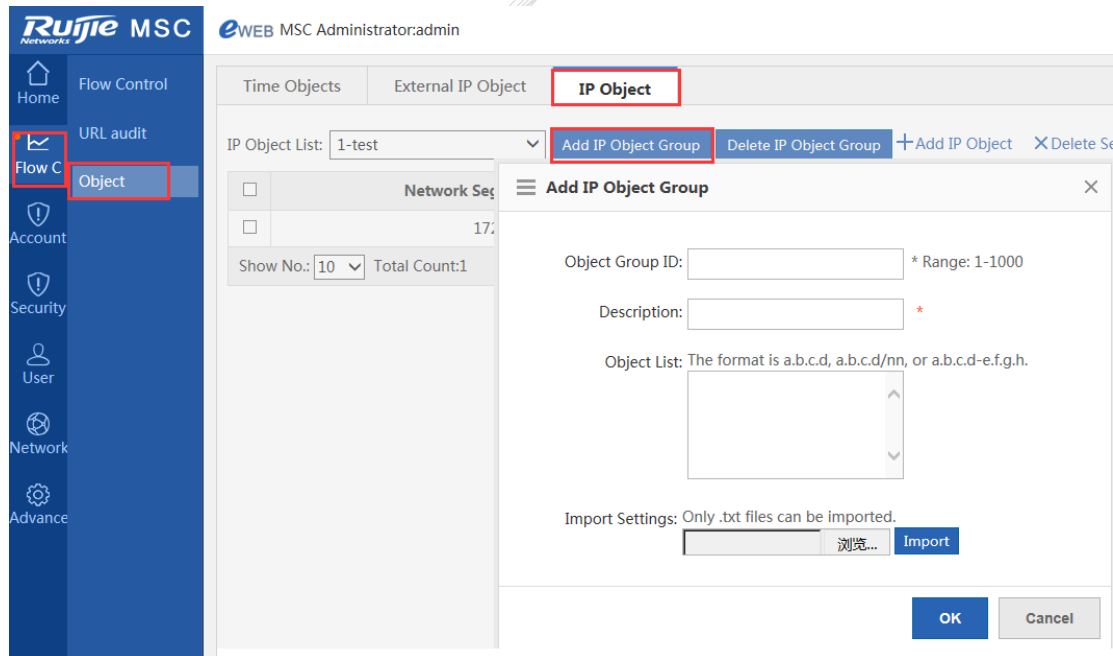


IPFIX configuration example:

1. Exempt the 10.0.0.0/8 network segment allocated to teachers from accounting.
2. Implement accounting for other network segments.

Step 1: Add teachers to an IP object group.

Step 2: Configure Policy 1 and set **Traffic Type** to **China Unicom**.



Step 3: Configure Policy 2, and set **Source IP Group** (network segment for teachers) to **1** and **Traffic Type** to **Accounting-exempt**.

The screenshot shows the 'IPFIX Traffic Accounting' configuration page. A modal window titled 'IPFIX Policy' is open, allowing the configuration of a specific policy. The fields in the modal are: Policy ID (empty, range 1-100), Policy Based on (IP Group), Source IP Group (1, range 0-1000), Destination IP Group (0, range 0-1000), and Traffic Type (Accounting-exempt). A 'Save' button is visible at the bottom of the modal.

Step 4: Check the configured policies. (The policy on top is matched preferentially.)

The screenshot shows the 'IPFIX Policy Settings' section of the configuration page. It displays a table of configured policies. The table has columns for Policy ID, ACL, Source IP Group, Destination IP Group, Traffic Type, Enable/Disable, Status, Matching Sequence, and Action.

Policy ID	ACL	Source IP Group	Destination IP Group	Traffic Type	Enable/Disable	Status	Matching Sequence	Action
1	-	0	0	Abroad	Enable	Active		Edit Delete

#### 4.3.4 (Mandatory) Clock Synchronization Configuration

Clock synchronization must be configured for the MSC-ED card to maintain clock consistency with the background and thus ensure proper accounting.

1. Configure the time zones of the RG-N18000 and the MSC-ED card to be consistent. (The time zone of the MSC-ED card is managed by the SNTP server.)

Configuration example: **clock timezone dongba +8 0**

Configure the NTP master on the RG-N18000.

Configuration example: **ntp master 8**

2. Configure the NTP function on the MSC-ED card (applicable to the CLI version).

```
sntp interval 60
sntp server xxx.xxx.xxx.xxx //The address is the address of the RG-N18000.
sntp enable
```

3. Configure the NTP function on the MSC-ED card (applicable to the Web version).

The following figure shows how to configure the data management interface of the MSC-ED card. The interface is used for accounting information transfer and clock synchronization.

The screenshot displays the Ruijie MSC eWEB MSC Administrator interface. The left sidebar contains navigation options: Home, Interface (highlighted with a red box), Route, Flow C, DNS, Account, Security, User, Network (highlighted with a red box), and Advance. The main content area is titled "Basic Interface Setting" and includes tabs for "Operation Mode" and "Link Detection". A note states: "Note: You can click the corresponding interface to configure it." Below this, there are four interface icons: "1G", "3" (highlighted with a red box), "10G", and "MNG". A legend indicates that a green icon means "The interface is powered on" and a grey icon means "not powered on". The "10G Intf Configuration" section contains the following fields: Te0/3-IP Address (192.168.3.2), Subnet Mask (255.255.255.0), Next-hop IP (empty), Description (empty), MAC Address (5869.6c60.aaf1), and Downlink Speed (10000). The MAC address format is noted as (Format: 00d0.f822.1234). The Downlink Speed field has a note: (Mbps(0.5-10000) The default value is 100 wh).

The following figure shows how to configure the SNTP Web function of the MSC-ED card.



Ruijie MSC eWEB MSC Administrator:admin

Change Password Restart Factory Default Configuration Backup **SysTime** Enhancements

**Note:** Changing the system time may cause incorrect audit time of historical traffic reports.  
**Tip:** If you select Automatically Synchronize with an Internet Time Server, make sure that DNS Server is correctly configured.

### System Time

Current Time: 2016-12-19-p.m.9:20:17

New Time:

Time Zone: UTC+8

Time Server: 192.168.3.1

It is recommended to set the IP address of the time server to the N18k IP address and enable the N18k with the NTP Server function.

Automatically Synchronize with an Internet Time Server

Save

## 4.3.5 URL Audit Configuration

### Overview

URL audit is intended to monitor and record the website access behaviors of intranet users.

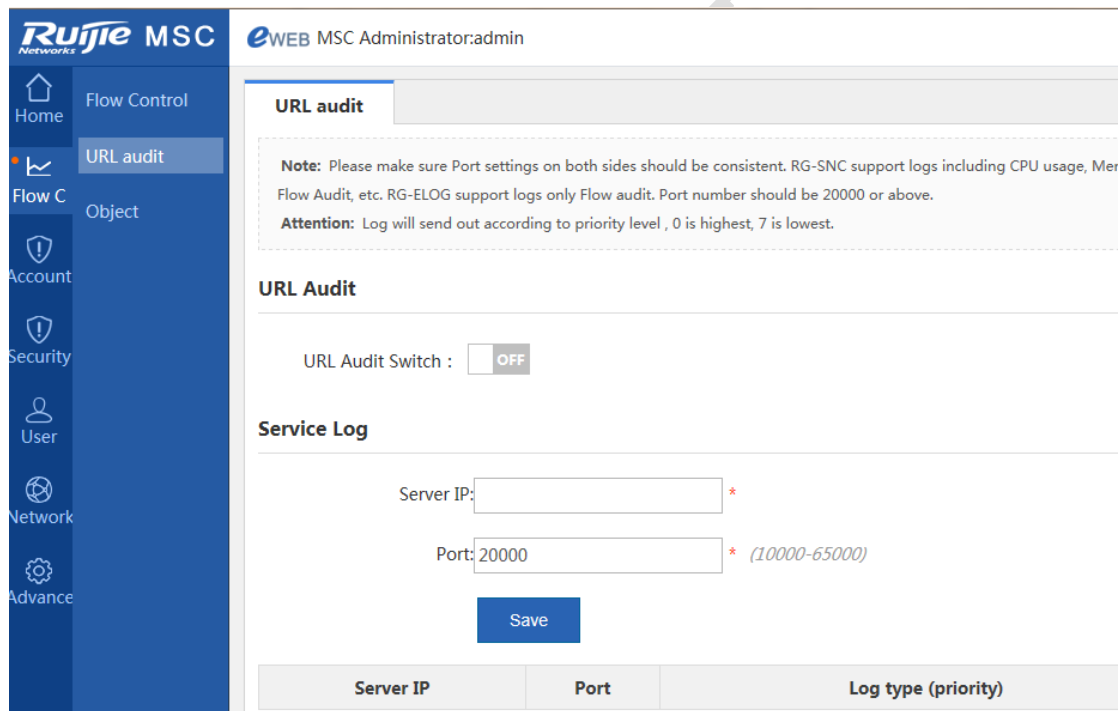
### Working Principle

URL, short for uniform resource locator, is also called the Web address.

The URL audit function can recognize the URL contained in the HTTP header in data streams. After you enable this function, you can extract user information and the URLs accessed by users in order to record the users' website access behaviors. If this function is not enabled, such information is not recorded.

### Configuration Steps

Log in to the Web management interface of the MSC-ED card and choose **Flow Control > URL audit**.



After you enable URL audit, the MSC-ED card performs auditing of intranet users' website access behaviors.

**Note:**

Because the MSC-ED card does not have a hard disk, URL audit logs cannot be stored locally but must be sent to a log server. You can connect the MSC-ED card to the eLog server, and you only need to set the server IP address and use the default Port 20000, as shown in the preceding figure.

### 4.3.6 Traffic Monitoring Configuration

#### I. Requirements

- Intranet users can access the Internet only after real-name authentication.
- Flow control must be implemented to limit the bandwidth of intranet users.
- Set the maximum upload bandwidth to 100 kbps and the maximum download bandwidth to 100 kbps for real-name users.

#### II. Configuration Tips

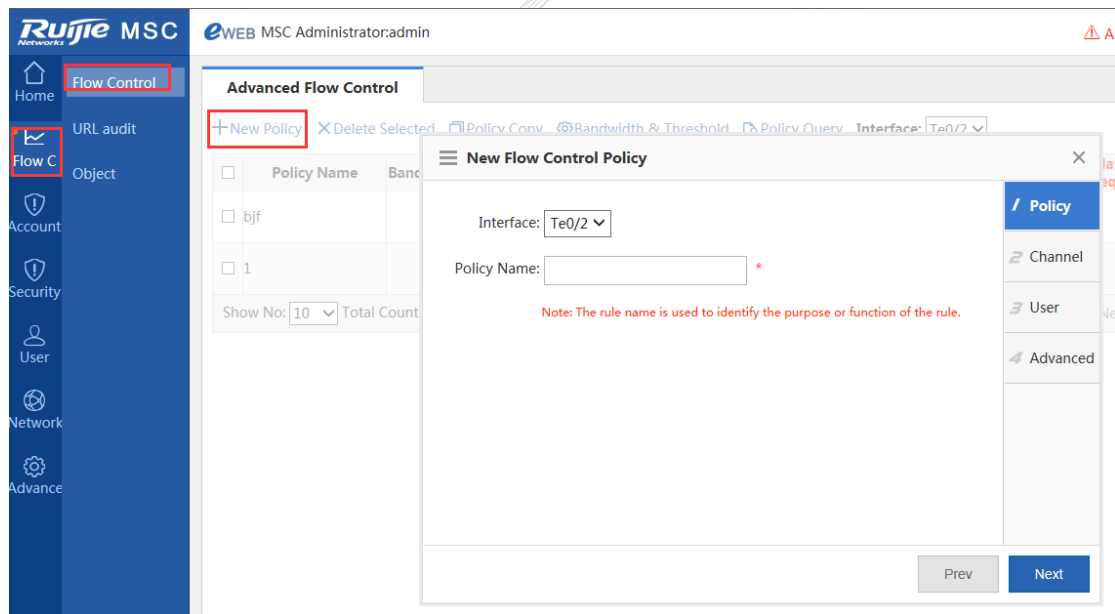
Real-name flow control is based on the usernames used for authentication, not based on IP addresses.

Because the flow control effect is related to the actual egress bandwidth, the actual egress bandwidth must be confirmed.

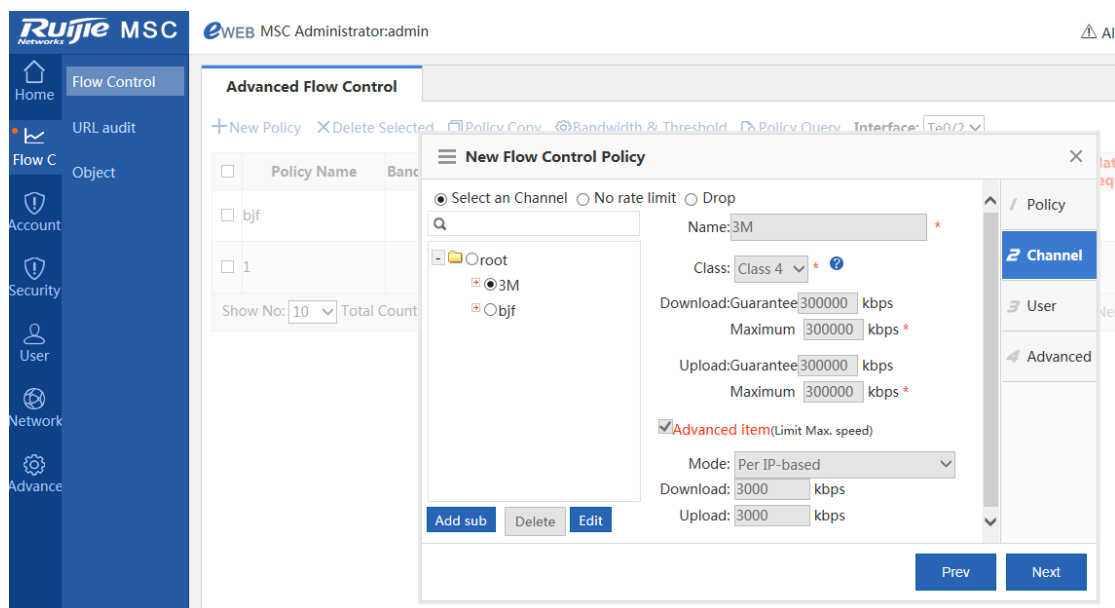
#### III. Configuration Steps

Choose **Flow Control** and click **New Policy** to configure a policy used to limit the download speed of real-name users. The steps are as follows:

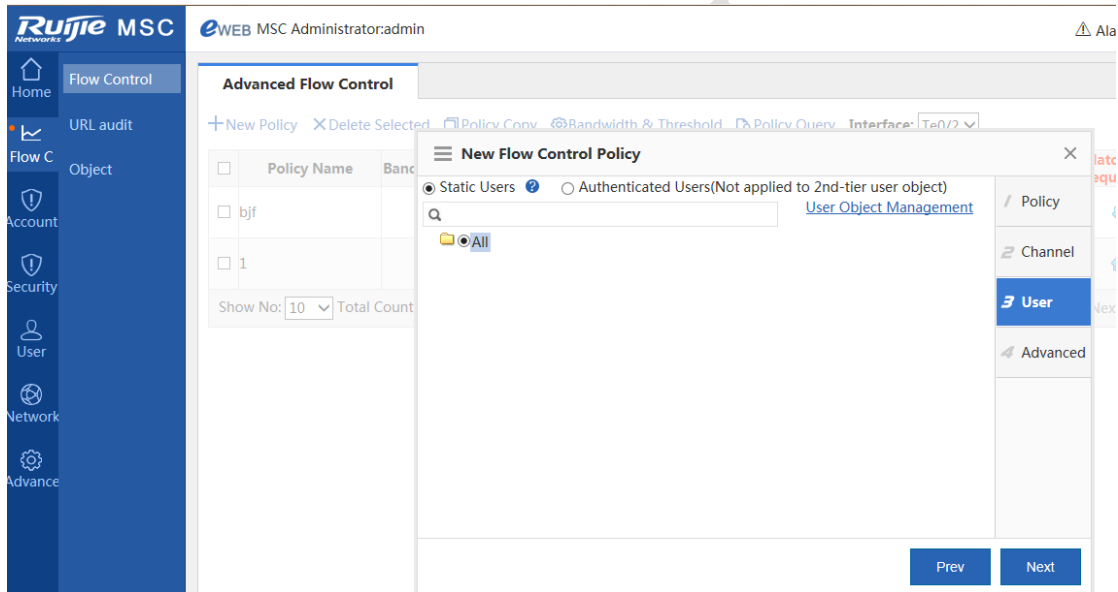
- (1) Select an interface and set a policy name.



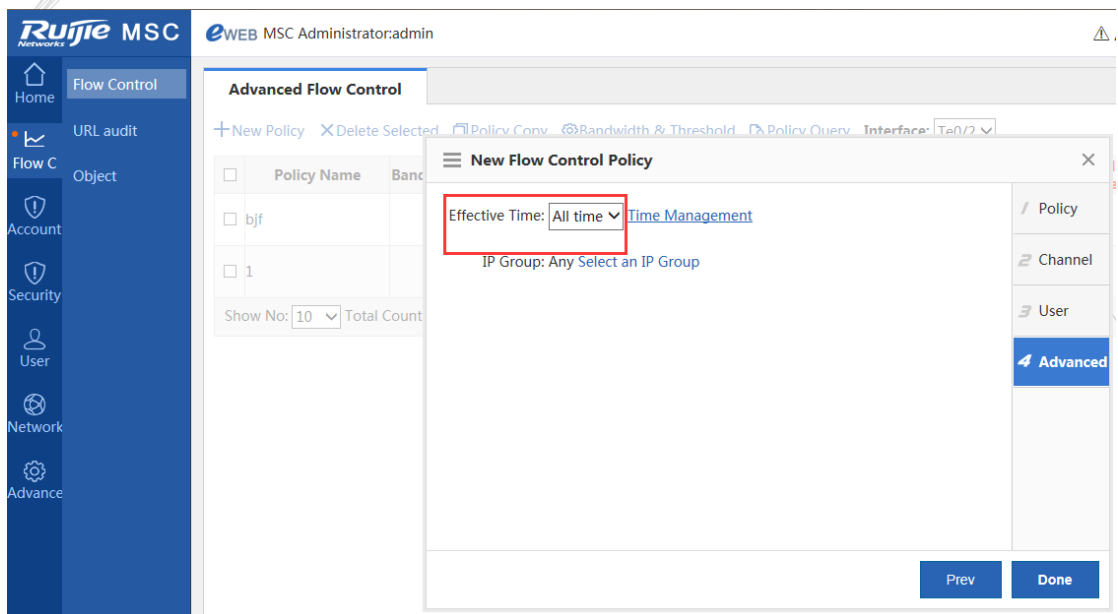
- (2) Select the traffic entrance channel, and set the guaranteed bandwidth (CIR), maximum bandwidth (PIR), and other information. You can also select No rate limit or Drop.



- (3) Select the type of real-name users for association.



(4) Set the effective time. You can leave this parameter as it is.



(5) Check the configured policy.

Ruijie MSC eWEB MSC Administrator:admin

Home | Flow Control | URL audit | Object | Account | Security | User

**Advanced Flow Control**

+ New Policy | X Delete Selected | Policy Copy | Bandwidth & Threshold | Policy Query | Interface: Te0

<input type="checkbox"/>	Policy Name	Bandwidth Channels	Selected Users	Effective Time	Advanced Options
<input type="checkbox"/>	bjf	bjf	100	All time	Extranet IP objects:Any
<input type="checkbox"/>	1	3M	1	All time	Extranet IP objects:Any

Show No: 10 Total Count : 2

The SAM+ server implements rate limiting based on user names. When the data of a user named Yang Lin enters the MSC-ED card, the policy automatically takes effect.

<input checked="" type="checkbox"/> On	Status	Matching Sequence	Operation
<input checked="" type="checkbox"/> On	Ineffective ?	↓	Edit Delete Move
<input checked="" type="checkbox"/> On	Ineffective ?	↑	Edit Delete Move

#### IV. Verification

The rate of users is limited to about 100 kbps.

## 4.4 SAM+ Support Configuration

### 4.4.1 (Mandatory) SAM+ Support Configuration

1. Log in to the SAM+ management page, choose System > Device to add the IP address of the RG-N18000. The gateway mode must be enabled.

**SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM** admin

Shortcut Channel **System** Security User Access Control Billing Account Operation

**Device**

Device IP Address\* 172.29.2.254 IP Type\* IPv4

Device Type\* Ruijie Switch Model\* N18K

PPPoE Authentication Domain domains IPOE+Web Authentication domains

Device Key\* ruijie Community\* ruijie

MAC Address\* be filled For trusted ARP binding application, MAC address must be filled SNMP Proxy Port adopted

DHCP Login Username DHCP Login Password

Telnet Login Username Telnet Login Password

Telnet Privileged Password Device Group\* default

Device Name Device Location

Device Timeout (secs)\* 3 Device Idle Time (secs)

Device Feature  Re-authentication  Account Update  Client Detection Area Please Select (Device IP(v4))

Web Authentication Option  Select this to enable the web authentication for the switch RG-ePortal Management Port

Integration Port(1~65535) Description

SU Version Check  Enable (Applicable to authentication client + access switch authentication) N18K Feature  Layer Gateway Certification  Use Port 2009

- Because the source MAC addresses for egress gateway authentication are the same, choose System > System Settings and select Not Enable for MAC Exclusive Safeguard.

**SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM**

Shortcut Channel **System** Security User Access Control Billing Account Operation

Location: System > System Settings

Notification

Subscription Reminder

Self-Service Plan Change

External Link

**Conflict & Grab**

Email Server

Others

Registered MAC Authentications 1 (Number of MAC which can be registered by a username) (1~10)

**MAC Exclusive Safeguard** Not Enable

IP(v4) Exclusive Safeguard Not Enable Preemption mode

Exclusive Safeguard Not Enable Preemption mode

Username Preemption Mode  When the user has reached the maximum user limit, the first online user will be forced offline so that other users can log in to the Internet

- Preemption mode: For same IP, the online user will be forced offline so the user can log in to the Internet environment
- Non-preemption mode: For same IP, the online user will be forced offline. It is usually used for Internet access.

Save Reset

- For other settings, see the simplified network configuration.

## 4.4.2 Billing Policy Configuration

Steps:

- Log in to the SAM+ management page.
- Choose Billing > Billing Policy, select Internet Traffic Billing, and click Add.

**SAM<sup>+</sup> SECURITY ACCOUNTING MANAGEMENT SYSTEM**

Shortcut Channel ⚙️    Homepage   System   Security   User   Access Control   **Billing**   Account   Operation

Location: Billing > Billing Policy

Billing Policy Name      General Search   [Search](#)

Please select the billing policy which you want to add Internet Traffic Billing   [Add](#)   [Delete](#)

**There were no results found.**

<input type="checkbox"/>	Billing Policy Name	Description
--------------------------	---------------------	-------------

3. Select Enable Cumulative Segment Charging.

**SAM<sup>+</sup> SECURITY ACCOUNTING MANAGEMENT SYSTEM**    admin | About | Logout

Shortcut Channel ⚙️    Homepage   System   Security   User   Access Control   **Billing**   Account   Operation

**International Downlink Traffic Billing Policy**

Policy Name\*     Rate\*  MYR  MB

Segment Charging Options    Enable Cumulative Segment Charging    Monthly Gift Options    Enable the Free Gift Each Month

Discount Options for Different Periods    Enable the Period Discount

Description

---

**Segment Setting**

Area Initial Point		Area End Point	Billing Rate	Partition Activation Fees	
<input type="text" value="0"/>	To	<input type="text" value="Infinity"/> ∞	<input type="text" value="0"/> MYR <input type="text" value="1"/> MB <input type="text"/>	<input type="text" value="0"/> MYR	<a href="#">Add</a>
0.00	To	1.00	0.00MYR1MB	0.00MYR	
1.00	To	10.00	10.00MYR1MB	0.00MYR	<a href="#">Delete</a>

4. Choose Billing > Billing Policy, select Custom, and click Add.

**SAM<sup>+</sup> SECURITY ACCOUNTING MANAGEMENT SYSTEM**    admin | About | Logout

Shortcut Channel ⚙️    Homepage   System   Security   User   Access Control   **Billing**   Account   Operation

Location: Billing > Billing Policy

Billing Policy Name      General Search   [Search](#)

Please select the billing policy which you want to add

- Monthly Billing Policy
- Daily Billing Policy
- Duration Billing Policy
- Internet Traffic Billing Policy
- Customize   [Add](#)   [Delete the Selected](#)

Total of 1 records, the currently displayed 1 to 1 records    📄 Currently 1 / 1 Page 🔍 Very Page 10 📄 Entry

5. Configure a segment billing policy.

SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM admin

Shortcut Channel Homepage System Security User Access Control Billing Account Operation

Location: Billing > Billing Policy > Modify > Modify Customized

Basic Information Billing Cycle Custom Billing Policy

Billing Policy Name\*  Description

Authentication Related Options  Allow login when there is no remaining internet traffic or the account has unpaid charges. (Must use the NTD penetration mode with access control or ACE device. Must use the monthly internet traffic plan or the internet traffic billing plan.)

- Not recommended to modify billing policy. The changes may affect the billing of online users when they get offline.
- The newly revised cycle billing rule rate will be effective after this cycle ends.

SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM admin

Shortcut Channel Homepage System Security User Access Control Billing Account Operation

Location: Billing > Billing Policy > Modify > Modify Customized

Basic Information Billing Cycle Custom Billing Policy

Billing Cycle  Set the Period Rate

Period Length\*   Day  Month Ending Date   Enable

Minimum Self-service Enablement\*  Period Billing Cycle   No charges if it has not been used in the period

Compensation  The remaining days during account suspension can be used after recovery Rate (MYR)\*

SAM+ SECURITY ACCOUNTING MANAGEMENT SYSTEM admin

Shortcut Channel Homepage System Security User Access Control Billing Account Operation

Location: Billing > Billing Policy > Modify > Modify Customized

Basic Information Billing Cycle Custom Billing Policy

Billing Options Supported  After enabled, the user plan supports payment deductions according to the rules and is able to select multiple segment billing policies.

Gift Options  Enable the Gift Policy (Monthly Gift)

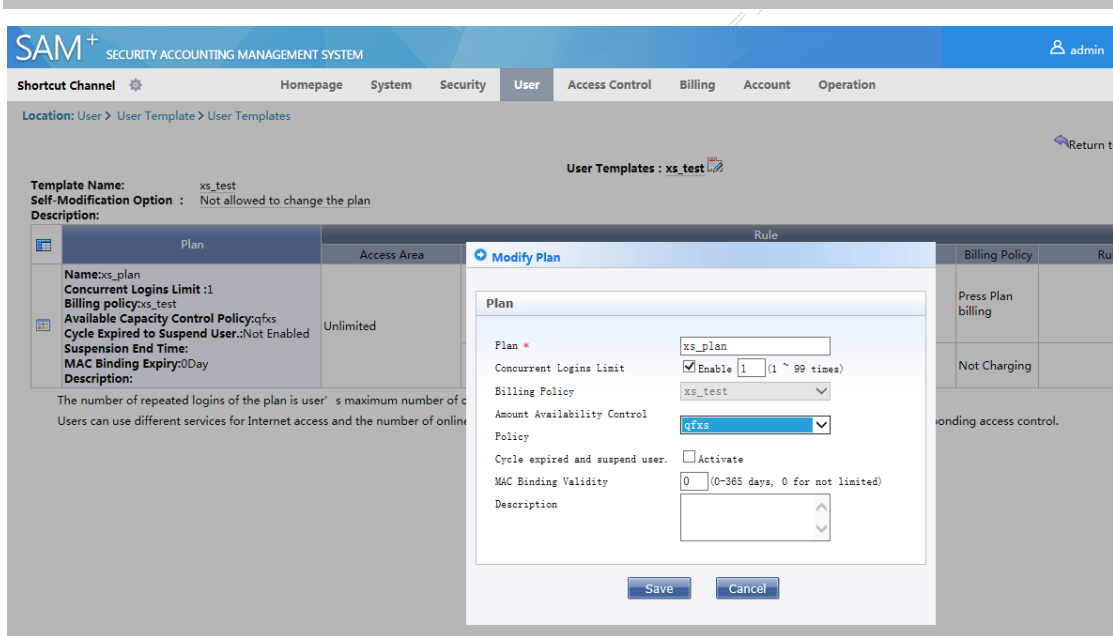
Segment Charging Options  Enable Segment Billing

Custom Rule	Description
<input type="checkbox"/>	speed-10M
<input type="checkbox"/>	speed-3M
<input type="checkbox"/>	international-up
<input checked="" type="checkbox"/>	xs_test

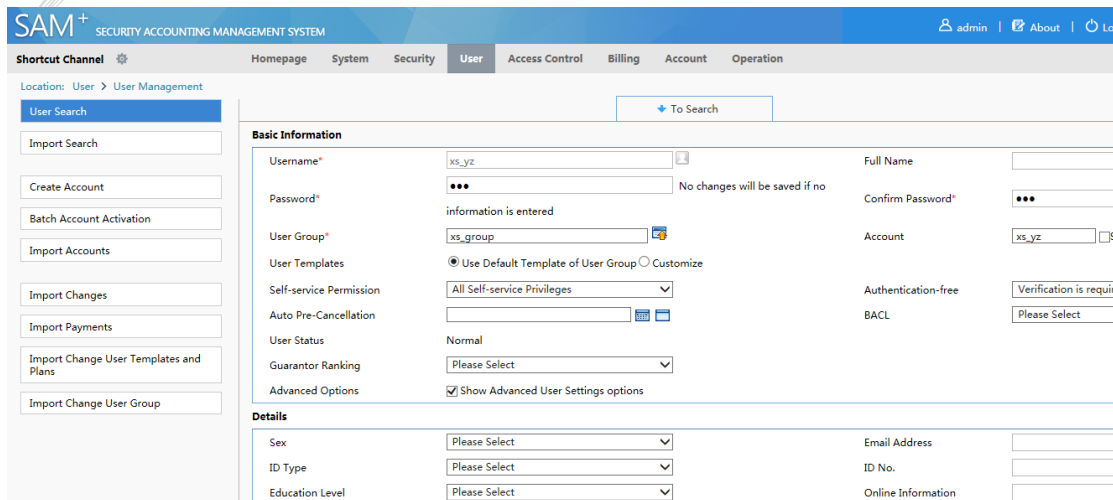
Segmental billing is divided based on accumulation. A cycle rule association is required to ensure cycle accumulation. Accumulation amount is the accumulated duration and data within a certain period of time. If you do not require regular cleaning up of accumulation amount, you can set the cycle length with a larger value.

6. Associate the billing policy with a package.





7. Add the users who subscribe to the package to the user template.



### 4.4.3 SMP Server Configuration

#### SMP server configuration differences

The SMP server also delivers authentication and accounting policies to users connected to the MSC-ED card. Different from the SAM+ server, the SMP server does not deliver the user group attribute field. After users pass authentication, the MSC-ED card cannot rate-limit user groups based on the negotiated field.

Solution: Configure the **filter id** field on the SMP server.

Step 1: Configure RADIUS attribute authorization.

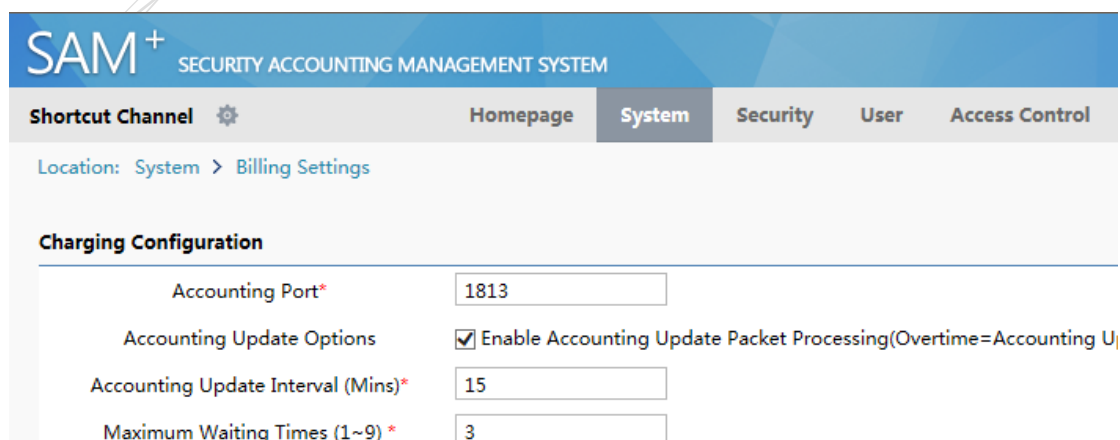
Step 2: Add the **filter id** field, define the attribute name, and set the attribute number to 11.

Step 3: Associate the user template with the **filter-id** attribute.

## 4.4.4 Accounting Update

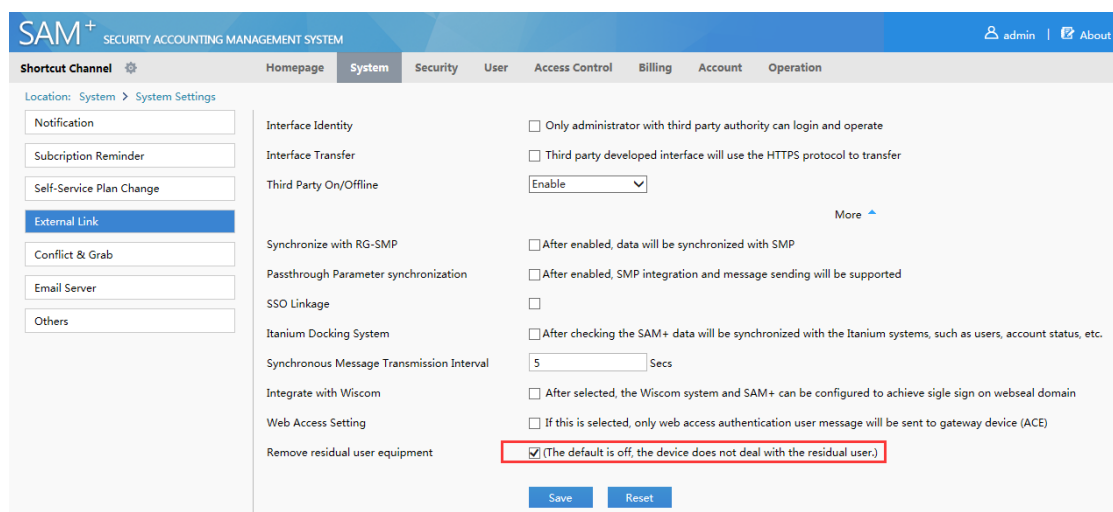
The accounting update function is used to synchronize online user information between the RG-N18000 and the SAM server. When online user information is available on the RG-N18000 but not available on the SAM server, the RG-N18000 sends an accounting update packet to the SAM server. When the SAM server checks that a user has no online information, it forces the user offline.

SAM server configuration:



The screenshot shows the SAM+ Security Accounting Management System interface. The top navigation bar includes 'Shortcut Channel', 'Homepage', 'System', 'Security', 'User', and 'Access Control'. The current location is 'System > Billing Settings'. The 'Charging Configuration' section contains the following settings:

Accounting Port*	1813
Accounting Update Options	<input checked="" type="checkbox"/> Enable Accounting Update Packet Processing(Overtime=Accounting U
Accounting Update Interval (Mins)*	15
Maximum Waiting Times (1~9) *	3



The screenshot shows the SAM+ Security Accounting Management System interface. The top navigation bar includes 'Shortcut Channel', 'Homepage', 'System', 'Security', 'User', 'Access Control', 'Billing', 'Account', and 'Operation'. The current location is 'System > System Settings'. The 'System Settings' page includes a left sidebar with categories like 'Notification', 'Subscription Reminder', 'Self-Service Plan Change', 'External Link', 'Conflict & Grab', 'Email Server', and 'Others'. The main content area lists various system settings:

Interface Identity	<input type="checkbox"/> Only administrator with third party authority can login and operate
Interface Transfer	<input type="checkbox"/> Third party developed interface will use the HTTPS protocol to transfer
Third Party On/Offline	Enable
Synchronize with RG-SMP	<input type="checkbox"/> After enabled, data will be synchronized with SMP
Passthrough Parameter synchronization	<input type="checkbox"/> After enabled, SMP integration and message sending will be supported
SSO Linkage	<input type="checkbox"/>
Itanium Docking System	<input type="checkbox"/> After checking the SAM+ data will be synchronized with the Itanium systems, such as users, account status, etc.
Synchronous Message Transmission Interval	5 Secs
Integrate with Wiscom	<input type="checkbox"/> After selected, the Wiscom system and SAM+ can be configured to achieve sigle sign on webseal domain
Web Access Setting	<input type="checkbox"/> If this is selected, only web access authentication user message will be sent to gateway device (ACE)
Remove residual user equipment	<input checked="" type="checkbox"/> (The default is off, the device does not deal with the residual user.)

Buttons: Save, Reset

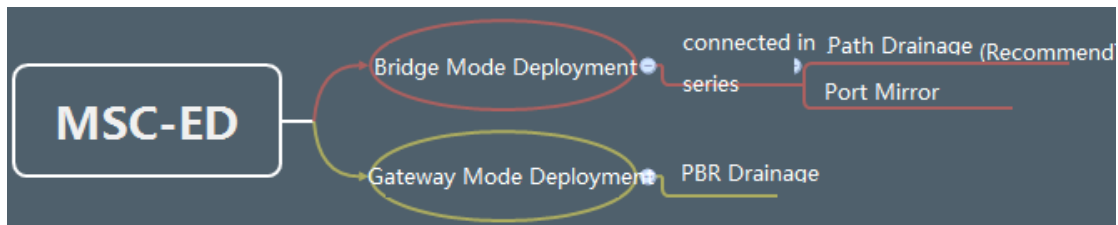
---

## 5 Typical Configuration

### 5.1 Overall Solution

#### 5.1.1 Networking Mode

To understand the onsite condition and develop deployment requirements, we need to understand the overall solution.

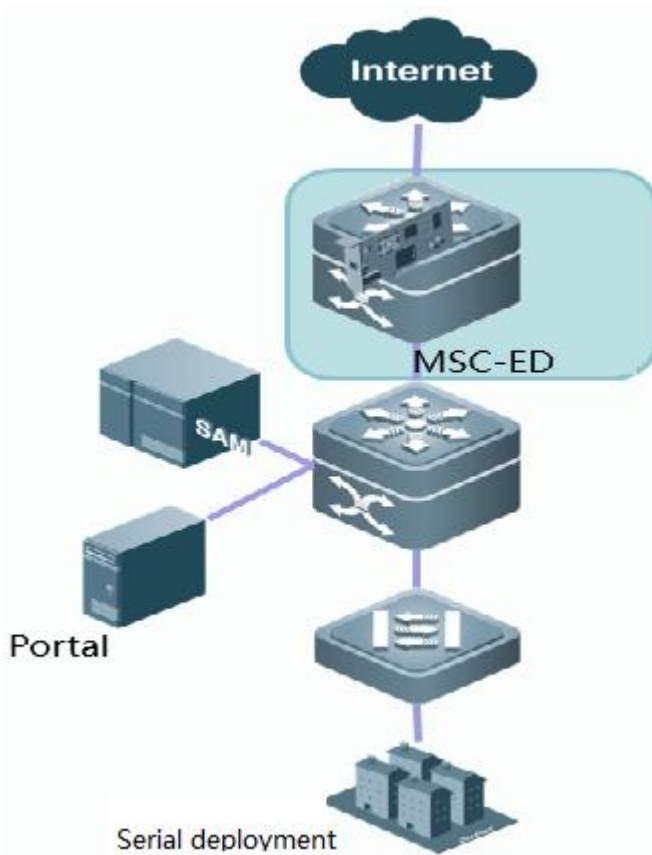


**Note 1:**

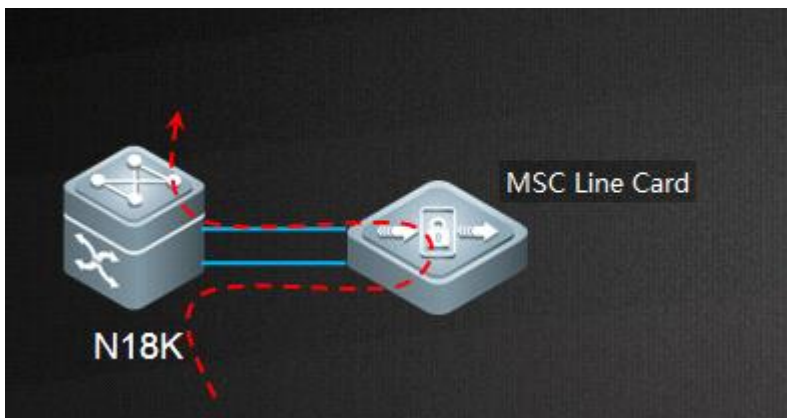
- In the Layer 2 solution, the MSC-ED card cannot be used in conjunction with the WS and FW cards.
- In the Layer 3 solution, the MSC-ED card can be used in conjunction with other service cards.

**Note 2:**

- The Layer 2 solution requires the MSC-ED card and the RG-N18000 to be serially connected as a whole to the network.



- In the Layer 3 solution, the MSC-ED card is deployed independently on a network device in PBR traffic diversion mode.

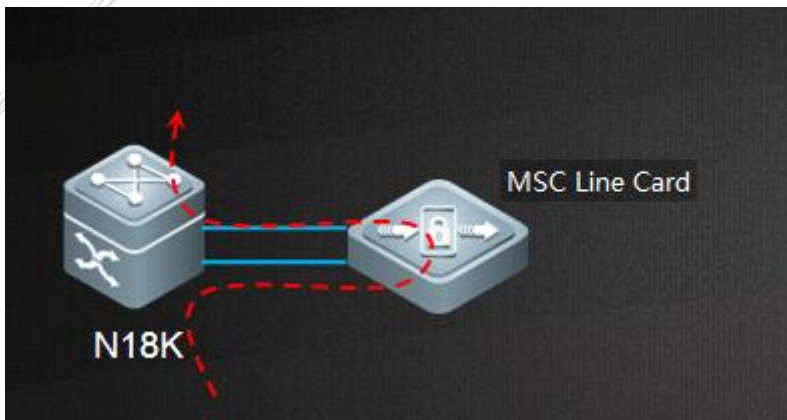


**Note 3:**

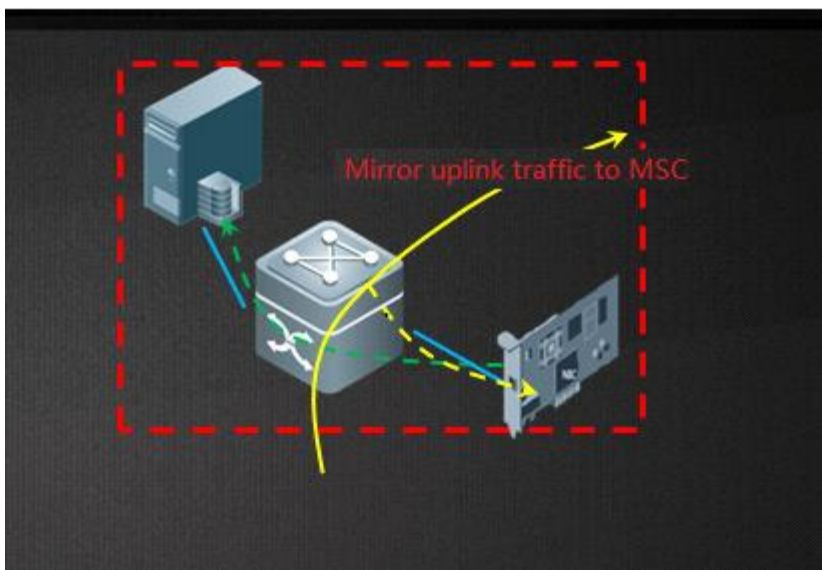
In the Layer 2 solution, the MSC-ED integrated device has two types of structural combination: Layer 2 policy-based traffic diversion and port mirroring. The following figure shows the MSC-ED integrated device.



The following figure shows the MSC-ED card deployed in bypass mode.



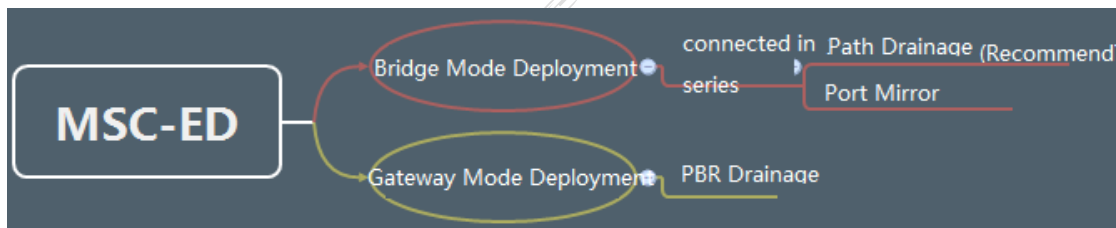
The following figure shows the MSC-ED card deployed in mirror mode.



---

## 5.1.2 Functional Differences between the Bridge Mode and Gateway Mode.

To understand the onsite condition and develop deployment requirements, we need to understand the overall solution.



### 1. Combination forms:

Traffic diversion in bridge mode (Layer 2): The RG-N18000 chassis and the MSC-ED card are bundled for sale, and the MSC-ED card cannot be used in conjunction with the WS and FW cards.

Traffic diversion in gateway mode (Layer 3): The MSC-ED card is deployed as an independent component and can be used with the RG-N18000 of the corresponding version.

### 2. Difference in terms of service flow:

Traffic diversion in bridge mode (Layer 2): The traffic that enters the MSC-ED card is Layer 2 traffic.

Traffic diversion in gateway mode (Layer 3): The traffic that enters the MSC-ED card is Layer 3 traffic.

### 3. Difference in terms of traffic diversion

Traffic diversion in bridge mode (Layer 2): The internal bypass mode is implemented through Layer 2 ACL-based redirection. Traffic diversion is completed using the **PATH** command.

Traffic diversion in gateway mode (Layer 3): The internal bypass mode is implemented through Layer 3 PBR.

### 4. Switchover when a port is down due to a hardware fault

Traffic diversion in bridge mode (Layer 2): The MSC-ED card is suspended when a port is down due to a hardware fault. Traffic is flooded out from the correct VLAN. Accounting fails. Then traffic is restored automatically.

Traffic diversion in gateway mode (Layer 3): The MSC-ED card is suspended when a port is down due to a hardware fault. PBR and accounting fail. Then traffic is restored automatically.

### 5. Switchover when a port is up following a hardware fault

Traffic diversion in bridge mode (Layer 2): The MSC-ED card is suspended when a port is up following a hardware fault. The OBS is configured with the automatic bypass function. Traffic is flooded out from the correct VLAN. Accounting fails. Then traffic is restored automatically.

Traffic diversion in gateway mode (Layer 3): The MSC-ED card is suspended when a port is up following a hardware fault. The DLDP detection function is configured. PBR and accounting fail. Then traffic is restored automatically.

### 6. Version capability

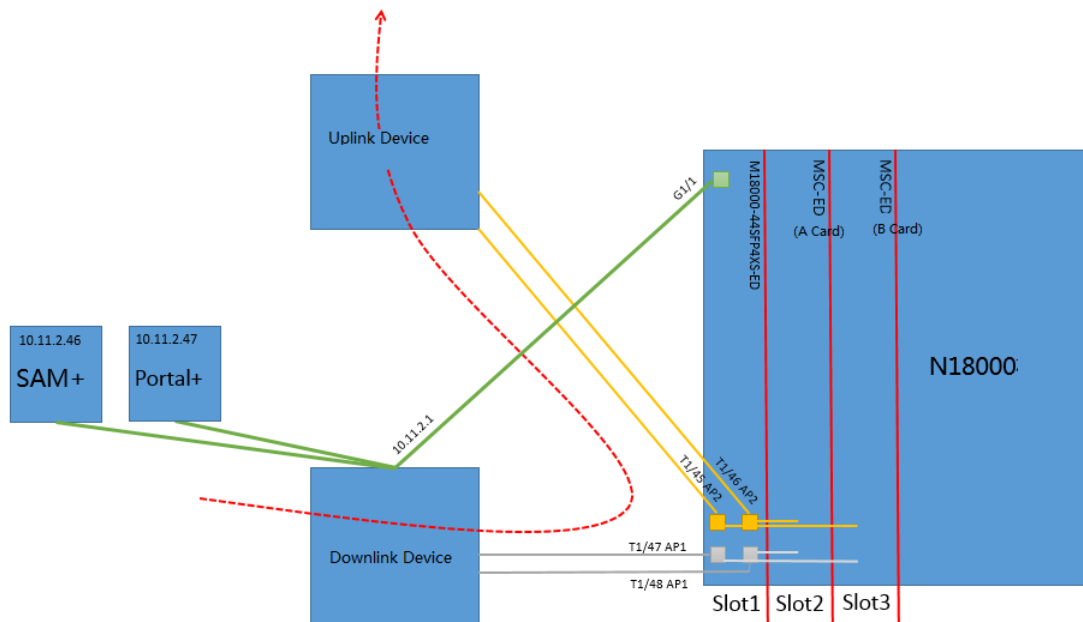
Phase 2 version (beta version): Only the bridge mode is supported, and the command for configuring the automatic bypass function is complex.

Phase 3 version (formal version): The bridge mode and gateway mode are supported. The command for configuring the Layer 2 automatic bypass function is simplified. Layer 3 Web authentication is supported.

## 5.2 Layer 2 Bridge Mode Configuration Case

### 5.2.1 General Configuration Template

To ensure successful initial configuration, the following configuration template is developed for your reference:



#### I. Network Topology

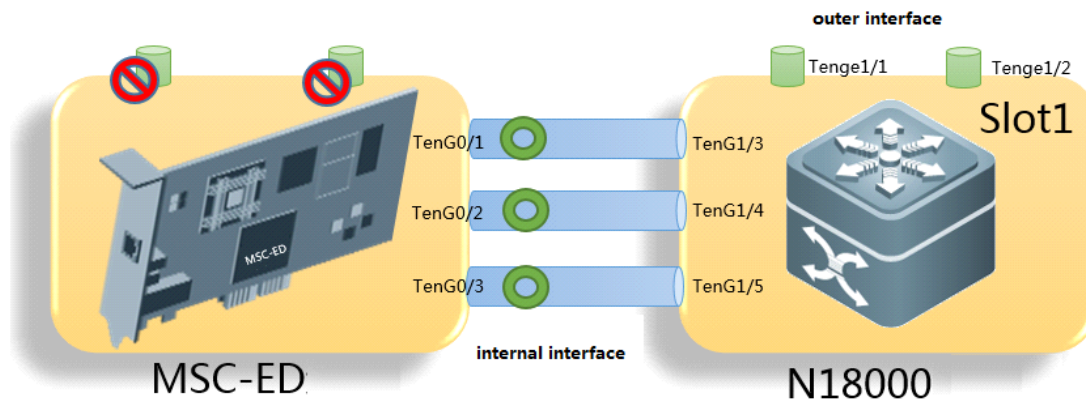
1. The configuration template is applicable to Layer 2 bridge mode deployment.
2. Slot 1 accommodates the relay card which is used to transfer users' service data and functions as the LAN and WAN egresses for the MSC-ED card.

G1/1 interface: The MSC-ED card stores accounting information in the local database of the RG-N18000 over IPFIX, and the RG-N18000 exchanges data with the SAM+ server and the portal+ server over the G1/1 interface.

T1/45 and T1/46: The MSC-ED card is connected to the RG-N18000 over internal interfaces. The WAN interface relay is AP2.

T1/47 and T1/48: The MSC-ED card is connected to the RG-N18000 over internal interfaces. The LAN interface relay is AP1.

3. Slot 2 and Slot 3 accommodate two MSC-ED cards, each of which provides 10 Gbps bandwidth in a single direction. Two cards provide 20 Gbps bandwidth. The following figure shows the connection of an MSC-ED card to the chassis.



#### 4. Data transfer direction

- (1) A user's access request is sent by the user's downlink device to the RG-N18000, and the user performs Layer 2 authentication on the RG-N18000.
- (2) The SAM+ server returns the authentication result to the RG-N18000, which then stores the result in the local database.
- (3) The traffic is diverted to the LAN interface of the MSC-ED card by the Layer 2 PATH (AP1) load balancing function of the RG-N18000.
- (4) The MSC-ED card retrieves authentication information from the database of the RG-N18000 in order to perform flow control on the user.
- (5) The traffic is forwarded by AP2 to the RG-N18000 over the WAN interface of the MSC-ED card, which then uses the IPFIX function to send accounting information over its TenG0/3 interface to the database of the RG-N18000.
- (6) The user is allowed to access partial network resources before authentication. The SAM+ server synchronizes the accounting database with the RG-N18000.

#### 5. Recommended implementation steps

##### Step 1: preparation

- (1) Obtain the correct versions of the MSC-ED card, RG-N18000, SAM+ server, and ePortal+ server.

##### Step 2: Implementation on the RG-N18000

- (1) Insert the MSC-ED card, line card, and management board. Upgrade to the corresponding versions.
- (2) On the RG-N18000, shut down the corresponding internal interface of the MSC-ED card used for handling users' service data.
- (3) Configure the NTP server.
- (4) Check that the time of the RG-N18000 is consistent with that of the SAM+ server and the ePortal+ server respectively.
- (5) Configure Web authentication parameters.



- 
- (6) Configure routing parameters.
  - (7) Configure traffic diversion.

Step 3: Implementation on the MSC-ED card

- (1) Configure a bridge and a management address.
- (2) Enable the service ports between the RG-N18000 and the MSC-ED card.
- (3) Configure time synchronization and ensure that the time of the MSC-ED card is consistent with that of the RG-N18000, SAM+ server, and ePortal+ server respectively.
- (4) Configure RG-N18000 correlation.
- (5) Configure other optional functions of the MSC-ED card.

Step 4: application software implementation

- (1) Add the ePortal+ server and RG-N18000 on the SAM+ server.
- (2) Add the RG-N18000 on the ePortal+ server.
- (3) Configure a traffic-based charging policy.

Step 5: implementation on other devices

- (1) Specify the original traffic diversion scheme and perform configuration based on PBR.
- (2) Check whether the return route for the uplink device is correct.
- (3) Test traffic diversion using an address segment. If no problem is found, divert all traffic.
- (4) Do not modify the uplink device and downlink device. When a problem occurs, shut down the uplink and downlink ports of the RG-N18000 to quickly restore the environment.
- (5) Enable the automatic switchover function.

## II. Configuration Steps

The configuration template is only applicable to the RG-N18000. For the configuration templates of other devices, see section 4 "Common Functions and Basic Configuration."

```
aaa new-model
aaa accounting update periodic 15
aaa accounting update
aaa accounting network default start-stop group radius
aaa authorization network default group radius
aaa authentication web-auth default group radius
no aaa log enable
no lldp enable

web-auth portal-escape nokick
web-auth acct-method ipfix
```

```
web-auth radius-escape
web-auth portal-check interval 3

ip dhcp pool ABC
  network 49.209.123.0 255.255.255.0
  dns-server 210.27.176.200 210.27.176.66
  default-router 49.209.123.1
ip auth-flow export destination 10.11.2.46 4739
nfpp
  no dhcp-guard enable

web-auth template eportalv2
  ip 10.11.2.47
  url http://10.11.2.47:8080/eportal/index.jsp

ip radius source-interface VLAN 11
radius-server host 10.11.2.46 key ruijie
radius-server dead-criteria time 61 tries 3

ntp master 8
!
ip route 0.0.0.0 0.0.0.0 10.11.2.1
!
offline-detect interval 15 threshold 0

snmp-server community ruijie rw
clock timezone beijing +8 0
!

interface ag1
  description TO_Up_Device
  switchport access vlan 2000
  web-auth enable eportalv2
!
interface ag2
  description TO_Down_Device
  switchport access vlan 2000
!
interface ag3
sw a vl 2000
```

```

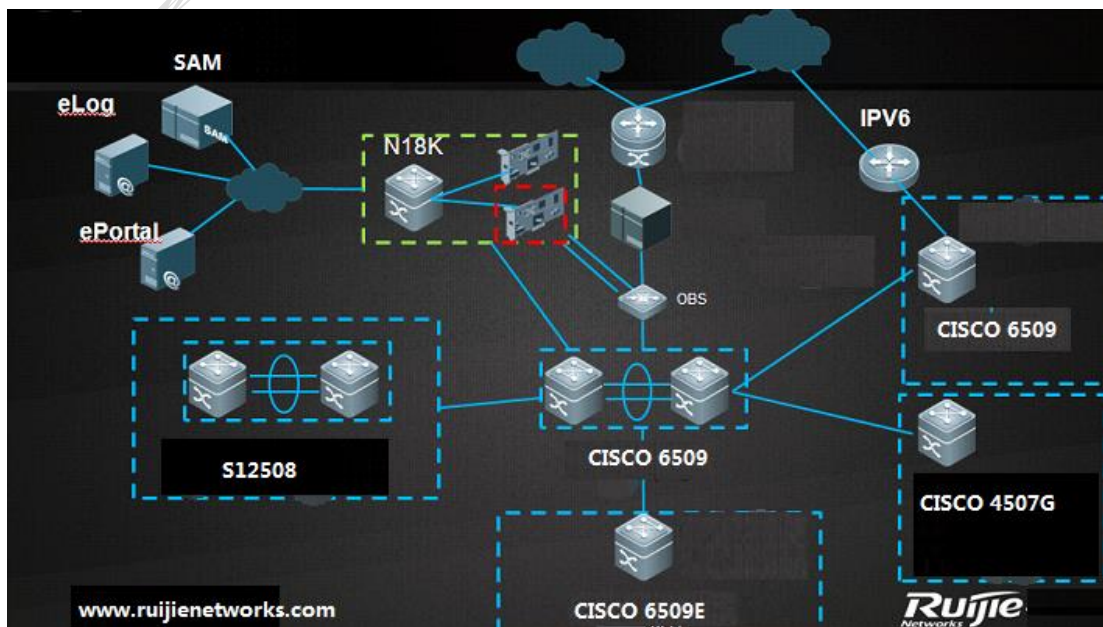
!
interface ag4
sw a vl 2000
!
msc path vlan 2000 dev-input ag1 dev-output ag2 msc-input ag3 msc-output ag4

```

## 5.2.2 Implementation Case of a Scientific Institute

### I. Implementation Preparations

#### 1. Pre-implementation topology



#### 2. Environment and implementation site

- a. The Cisco 6509 (IP address: \*.\*.16.112) is a core device providing services to the other four campuses (Campus 1, Campus 2, Campus 3, and Campus 4).
- b. The implementation site is located between the core device and the egress, that is, between the Cisco 6509 (IP address: \*.\*.16.112) and the Srun server in the topology.
- c. The access control mode is Web authentication.
- d. The servers are the SAM+ server, ePortal server, and eLog server.

#### 3. Preparation of modules and cables

- a. Check whether a single module or multiple modules are used between the core device and the egress device.

- 
- b. Prepare several optical cables.
  - c. Logical deployment process

**Step 1: implementation on the RG-N18000 (More details are provided in the following.)**

- (1) Insert the MSC-ED card, line card, and management board. Upgrade to the corresponding versions.
- (2) On the MSC-ED card, shut down Interface 6 and Interface 7 connected to the RG-N18000.
- (3) Configure traffic diversion.
- (4) Configure Web authentication parameters.
- (5) Configure the NTP server.
- (6) Check that the time of the RG-N18000 is consistent with that of the SAM+ server and the ePortal+ server respectively.
- (7) Configure routing parameters.

**Step 2: Implementation on the MSC-ED card (For details, see section 4 "Common Functions and Basic Configuration.")**

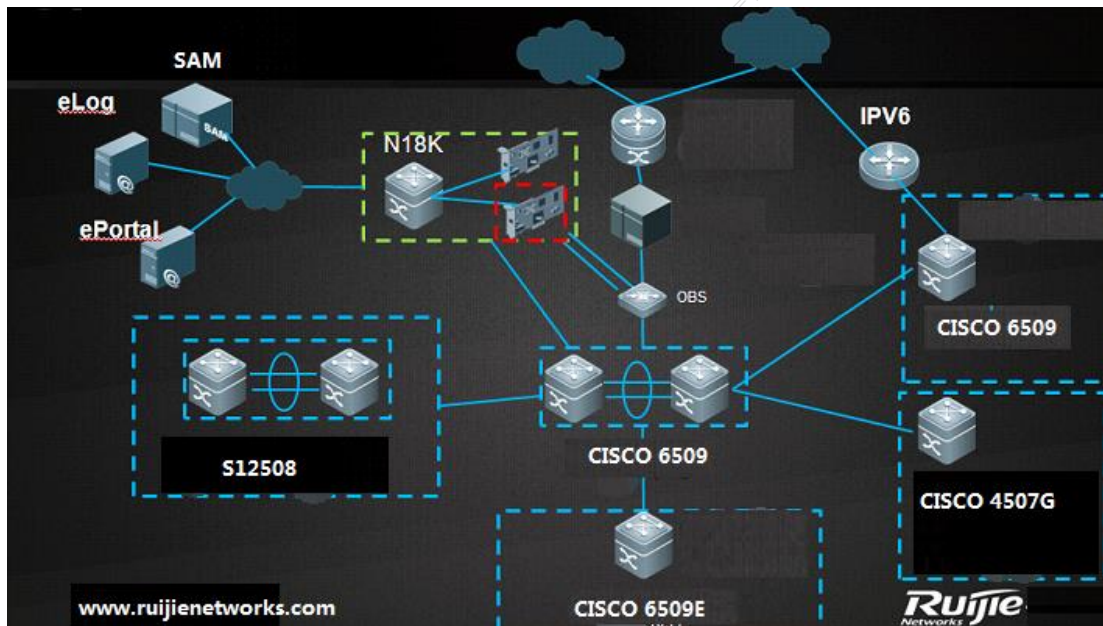
- (1) Configure a bridge and a management address.
- (2) Configure time synchronization and ensure that the time of the MSC-ED card is consistent with that of the RG-N18000, SAM+ server, and ePortal+ server respectively.
- (3) Configure RG-N18000 correlation.
- (4) Configure other optional functions of the MSC-ED card.

**Step 2: Application software implementation (For details, see section 4 "Common Functions and Basic Configuration.")**

- (1) Add the ePortal server and RG-N18000 on the SAM server.
- (2) Add the RG-N18000 on the ePortal server.
- (3) Configure a traffic-based charging policy.

## **II. Actual Deployment Process**

The following figure shows the topology after deployment is completed.



#### Topology description:

The RG-N18000 is added between the Cisco 6509 and the Srun server and is connected to the 10-GB optical port of the OBS. The Cisco 6509 is connected to the OBS then to the RG-N18000 over the OBS. The RG-N18000 is connected to the OBS then to the Srun server over the OBS. You can run the **show interface description** command on the RG-N18000 to display related information.

**OBS configuration is omitted in this document.**

#### Deployment requirements:

1. Transfer Web authentication to the RG-N18000.
2. IP address planning:
  - a. Retain the configurations of the original access, aggregation, and core devices, and use the IP addresses planned on the live network.
  - b. Configure the core devices in various campuses to work as DHCP servers for allocating IP addresses to all terminals.
3. Authentication-free host: allows unauthenticated users to access servers and allow particular users to access the network without authentication.
4. Ensure accurate traffic-based charging for Internet access.

#### Deployment description:

1. RG-N18000 deployment

## N18K Configuration description

Web Authentication	
aaa new-model	Start AAA service
aaa accounting network default start-stop group radius	Define AAA accounting update
aaa accounting update periodic 15	Define AAA accounting update period
aaa authentication web-auth default group radius	Define AAA authentication list
web-auth portal key ruijie	Define web-auth portal key
web-auth template eportalv2	Define web-auth template
ip *.*.16.21	Define ip address of portal
url http://*.*.16.21:80/eportal/index.jsp	Define redirect url
interface xxx	Enter interface mode
web-auth enable eportalv2	Enable web-auth
ip portal source-interface VLAN 1	Define Vlan
no aaa log enable	no aaa log enable
Without Authentication	
http redirect direct-site *.*.186.1	Define direct-site
http redirect direct-site direct-site *.*.14.0 255.255.255.0	Define direct-site segments.
web-auth direct-host *.*.19.253	Define direct-host
Web-auth radius-escape	
web-auth radius-escape	Define radius-escape
radius-server dead-criteria time 61 tries 3	Define radius-server dead-criterial time
radius-server host xxx.xxx.xxx.xxx test username ruijie key ruijie	Configure radius-server key
web-auth portal-escape [nokick]	Define portal-escape
web-auth portal-check interval 3 retransmit 3	Define portal-escape way
Path Drainage	
msc path vlan 2001 dev-input Ag3 dev-output Ag4 msc-input Ag1 msc-output Ag2	Define flow trend of vlan 2001
Free Charge	
int ag 3	
redirect destination interface AggregatePort 4 acl mianjifei-downlink in	Redirect
int ag 4	
redirect destination interface AggregatePort 3 acl mianjifei-downlink in	Redirect
Net-Flow Charging	
web-auth acct-method ipfix	Define web-auth acct-method ipfix
ip auth-flow export destination *.*.16.19 4739	Auth-flow export
SNMP Management	
snmp-server community ruijie rw	Define snmp-server community

Check the operating status as follows:

Check that the noises generated by the RG-N18000 connected to more than 20,000 users do not affect Web authentication performance.

```
N18K#show cpu-protect type web
Packet Type      Traffic-class  Bandwidth(pps)  Rate(pps)  Drop(pps)  Total      Total Drop
-----
web-auth         2              100000          22729      0           1722048     0
```

Check the CPU usage.

```

[Slot 5: M18000-MSC-ED, Cpu 0]
CPU Using Rate Information
CPU utilization in five seconds:17.5%
CPU utilization in one minute:17.5%
CPU utilization in five minutes:17.4%

[Slot 6: M18000-MSC-ED, Cpu 0]
CPU Using Rate Information
CPU utilization in five seconds:15.3%
CPU utilization in one minute:15.5%
CPU utilization in five minutes:15.7%

[Slot 7: M18000-24GT20SFP4XS-ED, Cpu 0]
CPU Using Rate Information
CPU utilization in five seconds:8.8%
CPU utilization in one minute:9.2%
CPU utilization in five minutes:9.3%

[Slot FE1: M18010-FE-D I, Cpu 0]
CPU Using Rate Information
CPU utilization in five seconds:1.9%
CPU utilization in one minute:1.8%
CPU utilization in five minutes:1.8%

```

```

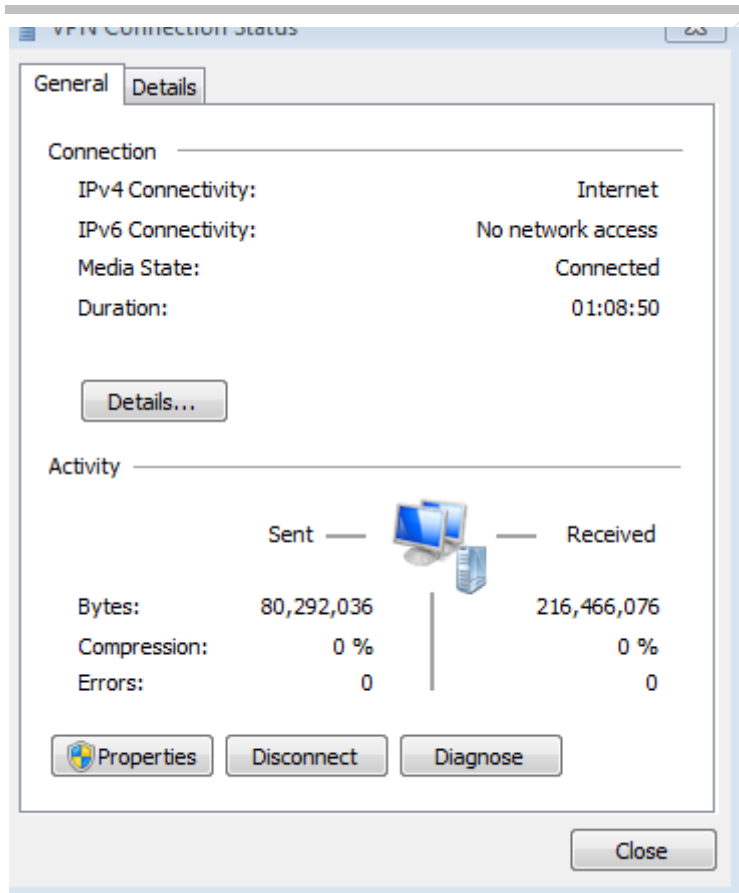
=====
[Slot M1: M18010-CMII]
CPU Using Rate Information
CPU utilization in five seconds: 3.20%
CPU utilization in one minute: 3.60%
CPU utilization in five minutes: 3.40%

```

Check the forwarding performance of the RG-N18000 during peak hours.

Interface	Sampling Time	exc 0 Input Rate (bits/sec)	0 Input Rate (packets/sec)	Output Rate (bits/sec)
Gi7/1	5 seconds	80692	19	311900
Gi7/24	5 seconds	71963	46	81855
Te5/3	5 seconds	467219902	61444	173009432
Te5/4	5 seconds	173027673	51164	467268085
Te5/5	5 seconds	218605	112	69836
Te6/3	5 seconds	378662904	44716	102478400
Te6/4	5 seconds	102466986	34020	378624892
Te6/5	5 seconds	157308	74	43824
Te7/47	5 seconds	655063472	79309	208430706
Te7/48	5 seconds	215205918	67074	656224994
Ag1	5 seconds	732719820	89633	221007024
Ag2	5 seconds	221009976	70136	732717688
Ag3	5 seconds	307411232	99229	987123741
Ag4	5 seconds	985414879	118757	299373253

Check accounting accuracy.

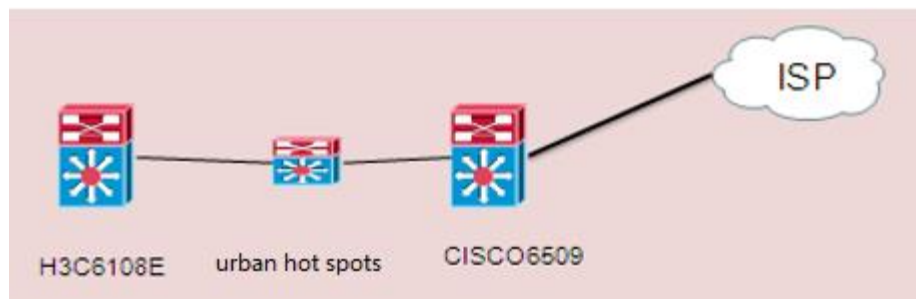


In the preceding figure, the traffic sent by the network adapter is almost the same as the traffic recorded in the accounting system. Note that the downlink traffic is  $216,466,046/1,024/1,024 = 206$  Mbps, and the uplink traffic is  $80,292,036/1,024/1,024 = 76$  Mbps.

Implementation case of a technology university

### I. Network reconstruction design

#### Original authentication network of the university

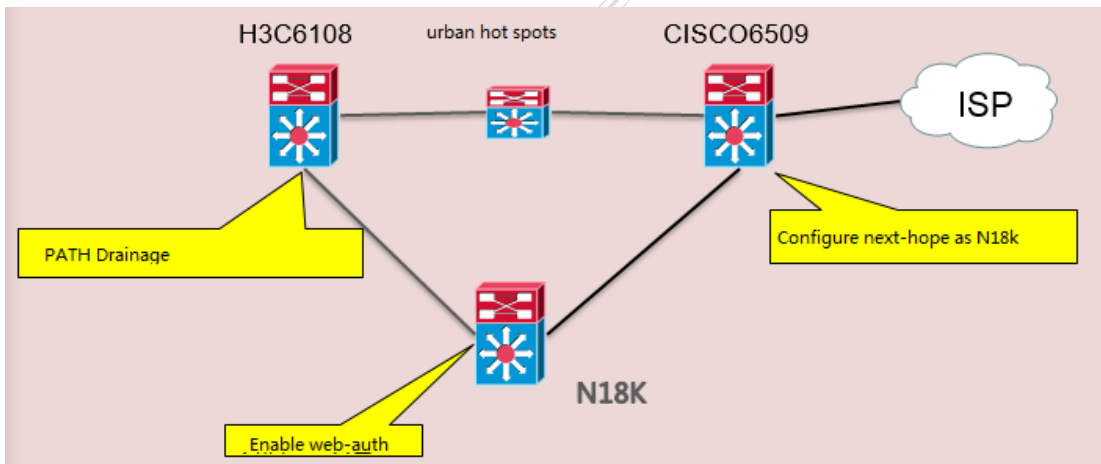


The preceding figure shows the simplified egress diagram.

1. Urban hot spots are used as the Web authentication server.
2. The H3C6108E works as a wireless gateway, and the DHCP server is located on the H3C6108E.



## Target network after reconstruction



Reconstruction objective: switch partial traffic to the RG-N18000 and enable Web authentication on the RG-N18000.

Reconstruction steps:

Step 1: Create an environment where the SAM server works properly with the RG-N18000 and the MSC-ED card. (This step is described in detail.)

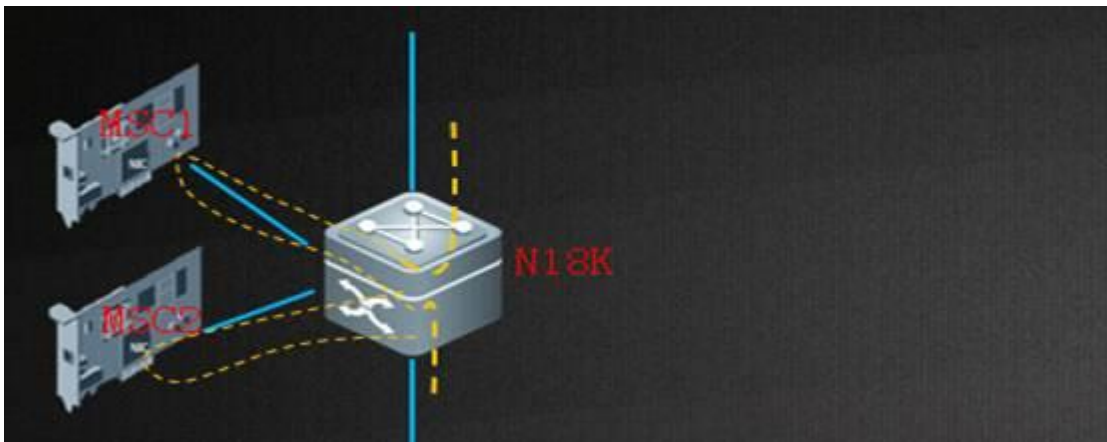
Step 2: Perform cutover of the wireless data stored in the computer center.

Step 3: Observe the authentication process when users go online.

## II. Implementation

(I) joint commissioning of the MSC-ED card and the RG-N18000

Networking principle:



Assume that MSC-ED Card 1 is located in Slot 2 and MSC-ED Card 2 in Slot 3 of the RG-N18000. That is, The TenG2/3 and TenG3/3 interfaces of the RG-N18000 correspond to the TenG0/1 interface of the MSC-ED card and the interfaces are

---

equivalent to LAN interfaces; the TenG2/4 and TenG3/4 interfaces of the RG-N18000 correspond to the TenG0/2 interface of the MSC-ED card and they are equivalent to WAN interfaces. The conditions in other slots are similar.

```
18K Slot2 2/3 -- MSC1 0/1 - LAN port
18K Slot3 3/3 -- MSC2 0/1 - LAN port
18K Slot2 2/4 -- MSC1 0/2 - WAN port
18K Slot3 3/4 -- MSC2 0/2 - WAN port
```

Step 1: Add TenG2/3 and TenG3/3 to AP1 (LAN).

Step 2: Add TenG2/4 and TenG3/4 to AP2 (WAN).

Step 3: Use the MSC path traffic diversion function to point the inbound interface and outbound interface of the RG-N18000 to the MSC-ED card.

Step 4: Apply the AP load balancing algorithm to the RG-N18000 to make the forward and return paths consistent.

Step 5: Complete the basic configurations of the MSC-ED card.

Step 6: Configure Web authentication on the RG-N18000.

Step 7: Divert user traffic to the RG-N18000.

Step 8: Enable Web authentication and observe the authentication process when users go online.

See the following deployment guide.

#### **Deployment guide:**

Step 1: Add TenG2/3 and TenG3/3 to AP1 (LAN).

Step 2: Add TenG2/4 and TenG3/4 to AP2 (WAN).

Step 3: Use the MSC path traffic diversion function to point the inbound interface and outbound interface of the RG-N18000 to the MSC-ED card.

Step 4: Apply the AP load balancing algorithm to the RG-N18000 to make the forward and return paths consistent.

#### **Configuration example:**

```
Ruijie(config)#int ag 1
Ruijie(config)#switchport access vlan 2000
Ruijie(config)# aggregateport load-balance src-ip (Implement load balancing based on the source IP address
in the uplink direction of the MSC-ED card.)
Ruijie(config)#int ag 2
Ruijie(config)#switchport access vlan 2000
Ruijie(config)# aggregateport load-balance dst-ip (Implement load balancing based on the destination IP
address in the downlink direction of the MSC-ED card.)
```

```
Ruijie(config)# msc path vlan 2000 dev-input gil/8 dev-output gil/9 msc-input Ag1 msc-output Ag2 (Set the direction of traffic diversion, so that user traffic enters from the GI1/8 interface and exits from the GI1/9 interface of the RG-N18000.)
```

**Step 5: Complete the basic configurations of the MSC-ED card.**

1. Log in to the MSC-ED card on the web page, use a network cable to connect the network adapter of the PC to the MGMT interface of the MSC-ED card, and set the IP address of the network adapter to any IP address in the 192.168.1.0 network segment (except 192.168.1.2 and 192.168.1.1). Enter <http://192.168.1.1> in the Internet Explorer to log in to the MSC-ED card, and enter the default username and password **admin**.
2. Perform configuration in interface configuration mode.

The screenshot displays the Ruijie MSC eWEB Administrator interface. The left sidebar contains navigation options: Home, Interface (selected), Route, Flow C, DNS, Account, Security, User, Network, and Advance. The main content area is titled 'Basic Interface Setting' and includes tabs for 'Operation Mode' and 'Link Detection'. A note states: 'Note: You can click the corresponding interface to configure it.' Below this, four interface cards are shown, each labeled '10G'. The 'MNG' interface card is highlighted with a blue border. A legend indicates that a green icon means 'The interface is powered on' and a grey icon means 'not powered on'. The 'MNG Intf Configuration' section contains three input fields: 'Management-IP Address' (192.168.200.2), 'Subnet Mask' (255.255.255.0), and 'Gateway' (192.168.200.1). 'Save' and 'Clear' buttons are located at the bottom.

3. Configure attack prevention.

The screenshot shows the Ruijie MSC eWEB interface. The left sidebar contains navigation options: Home, Flow C, Account, Security, User, and Network. The main content area is titled "Attack Prevention" and includes the following settings:

- Session Policy: [Default Global Configuration] [Single IP Address Configuration] \ [Attack Suspect List] ?
- DOS Attack Prevention:  Enable to prevent flow attacks
- Attack Flow Logs: [Current Attack Logs] [Historical Attack Logs]

At the bottom of the settings area, there are two buttons: "Save" and "Restore default settings."

4. Configure RG-N18000 correlation.

The screenshot shows the Ruijie MSC eWEB interface. The left sidebar contains navigation options: Home, Flow C, Account, Security, User, and Network. The main content area is titled "Correlation" and includes the following settings:

- Correlation Type: Enable 18K Correlation (dropdown menu)
- Server IP: 192.168.3.1
- Whitelist Network Segment:  OFF

At the bottom of the settings area, there is a "Save" button.

5. Configure a traffic-based charging policy.

Ruijie MSC eWEB MSC Administrator:admin

Home Traffic-based Accounting

Flow C Correlation

Account

Security

User

Network

Advance

### IPFIX Traffic Accounting

IPFIX: a method of calculating user traffic. It is used to collect traffic statistics of each user and is applicable to the user-based charging information to the charging server and synchronizes the online status of network users to the charging server.

#### IPFIX Global Settings

IPFIX:  Enable

Save

#### IPFIX Policy Settings

+ Add IPFIX Policy X Delete Selected

<input type="checkbox"/>	Policy ID	ACL	Source IP Group	Destination IP Group	Traffic Type	Enable/Disable
<input type="checkbox"/>	1	-	0	0	Abroad	<input checked="" type="checkbox"/> Enable

Show No: 10 Total Count : 1

First Previous 1

6. Upgrade the MSC-ED card version.

Ruijie MSC eWEB MSC Administrator:admin

Home System Settings

Flow C OS Upgrade

Authorization

Account One-Click Collection

Security Detection

User User Task

System Log

Network System Report

Advance Help

### System Upgrade

**Note:** During upgrade, you must not close or refresh this page until the successful upgrade is prompted, or else

**Attention:** 1. To upgrade the main program, you must name the file as **rgos.bin**. Please make sure the upgrade page may not respond temporarily due to flash processing. Do not switch off or restart the device at this moment

#### Local Upgrade

File name:  浏览... Upgrade Cancel

**Online** local [ˈləʊk(ə)l] 详细>  
n. [计] 局部; 当地居民; 本地新闻  
adj. 当地的; 局部的; 地方性的; 乡土的

Current Web Package Version:2016.8.18.16

No later Web package is available

#### Automatic Update Setting

Enable automatic update

3 hour 35 minute

Save

Step 6: Configure Web authentication on the RG-N18000.

```
aaa new-model
```

```
aaa accounting update periodic 15
aaa accounting update
aaa authentication web-auth default group radius
radius-server host 10.11.2.46 key ruijie
web-auth portal key ruijie
web-auth template eportalv2
ip 10.11.2.47
url http://10.11.2.47:8080/eportal/index.jsp
web-auth acct-method ipfix //The RG-N18000 sends traffic accounting information to the SAM server over
IPFIX.
ip auth-flow export destination 10.11.2.46 4739 //The IP address is the SAM server address.
```

### Step 7: Divert user traffic to the RG-N18000.

1. The H3C6108E diverts traffic to the RG-N18000 over PBR.

Configuration example:

- a. Configure an ACL.

```
acl number 3000
rule 0 permit ip source 49.209.88.0 0.0.0.255
```

- b. Configure PBR.

```
policy-based-route ruijie permit node 1
  if-match acl 3000
  apply ip-address next-hop 10.11.1.74
```

- c. Apply PBR in interface configuration mode.

```
interface Ethernet0/1/0
  port link-mode route
  ip address 10.11.1.73 255.255.255.252
  ip policy-based-route ruijie
```

2. The Cisco 6509 points the return path to the RG-N18000 over a static route.

Cisco 6509 configuration example:

```
ip route 49.209.88.0 255.255.255.0 10.11.1.73
```

### Step 8: Enable Web authentication and check whether users are authenticated properly when they go online.

Configuration example:

```
interface gil/8
web-auth enable eportalv2
```

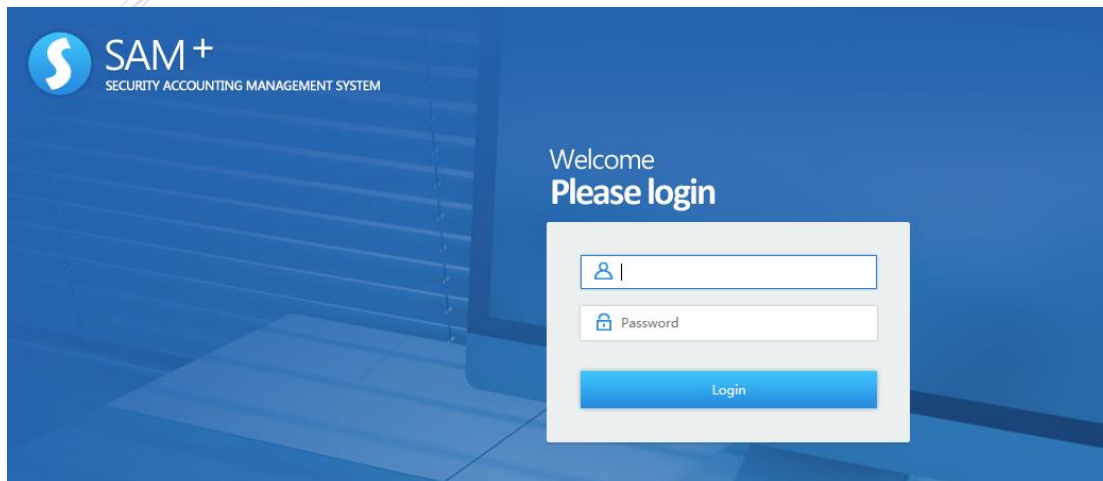
## I. Joint Commissioning of the SAM Server and the RG-N18000

Auxiliary configuration of the RG-N18000 (intended for communication between the RG-N18000 and the SAM server):

```
interface GigabitEthernet 1/13
description Link-To-SAM
switchport access vlan 11
ip radius source-interface vlan 11
```

### SAM server configuration

- i. Log in to the SAM server.



- b. Add the NAS.

**SAM+** SECURITY ACCOUNTING MANAGEMENT SYSTEM admin

Shortcut Channel Homepage **System** Security User Access Control Billing Account Operation

**Device**

Device IP Address*	<input type="text" value="172.29.2.254"/>	IP Type*	<input type="text" value="IPv4"/>
Device Type*	<input type="text" value="Ruijie Switch"/>	Model*	<input type="text" value="N18K"/>
PPPoE Authentication Domain	<input type="text" value="domains"/> <small>Please use comma or space to separate multiple</small>	IPOE+Web Authentication	<input type="text" value="domains"/> <small>Please use comma or space to separate multiple</small>
Device Key*	<input type="text" value="ruijie"/>	Community*	<input type="text" value="ruijie"/>
MAC Address*	<input type="text"/> <small>For trusted ARP binding application, MAC address must be filled</small>	SNMP Proxy Port	<input type="text" value="adopted"/> <small>If you do not fill in, the default is adopted</small>
DHCP Login Username	<input type="text"/>	DHCP Login Password	<input type="text"/>
Telnet Login Username	<input type="text"/>	Telnet Login Password	<input type="text"/>
Telnet Privileged Password	<input type="text"/>	Device Group*	<input type="text" value="default"/>
Device Name	<input type="text"/>	Device Location	<input type="text"/>
Device Timeout (secs)*	<input type="text" value="3"/>	Device Idle Time (secs)	<input type="text"/>
Device Feature	<input type="checkbox"/> Re-authentication <input type="checkbox"/> Account Update <input type="checkbox"/> Client Detection		
Web Authentication Option	<input type="checkbox"/> Select this to enable the web authentication for the switch		
Integration Port(1~65535)	<input type="text"/>	Area	<input type="text" value="Please Select"/> (Device IP(v4))
SU Version Check	<input checked="" type="checkbox"/> Enable (Applicable to authentication client + access switch authentication)	RG-ePortal Management Port	<input type="text"/>
		Description	<input type="text"/>
		N18K Feature	<input checked="" type="checkbox"/> Layer Gateway Certification <input checked="" type="checkbox"/> Use Port 2009

c. Add access control.

<http://172.29.2.2:8080/sam/> SAM+ Security Accountin... x

**SAM+** SECURITY ACCOUNTING MANAGEMENT SYSTEM admin

Shortcut Channel Homepage System Security **User** **Access Control** Billing Account Operation

Location: Access Control > Access Control > Add

**Access Control Information** User Information Check Network Usage Control Public Service User Behavior Control VPN Control Client Version Management Wireless Access Prop...

Access Control Name\*

Concurrent Logins Limit(0 to 99)  0 means no limit\*  Synchronization Accounting Update Interval

According to the Terminal Type Concurrent Logins (1 to 99 times)

Display accounting policy information when user online  Automatic Binding MAC authentication information quickly

Show users on-line access control time  Account information is displayed on a subscriber line

Gateway Access Restriction  It does not allow traffic through the gateway server (gateway device needs to be deployed linkage in penetration mode)

Export linkage strategy  \* non NPE / EG gateway billing model deployment, no need to configure the export collaboration policy

Firewall Policy  \* not deploy firewalls linkage, the need to configure

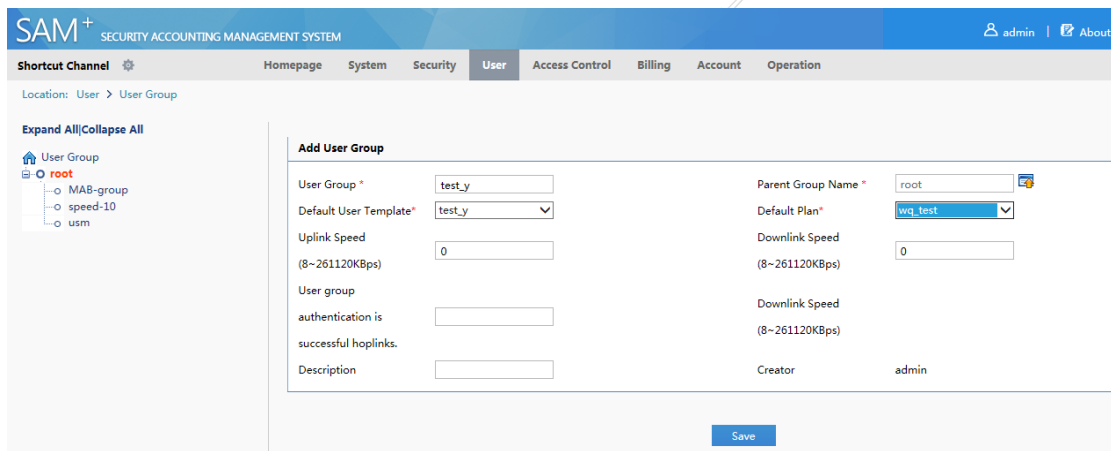
**Gateway Stratrgy**  \* non-ACE gateway billing model deployment, no need to configure the gateway policy names

Description

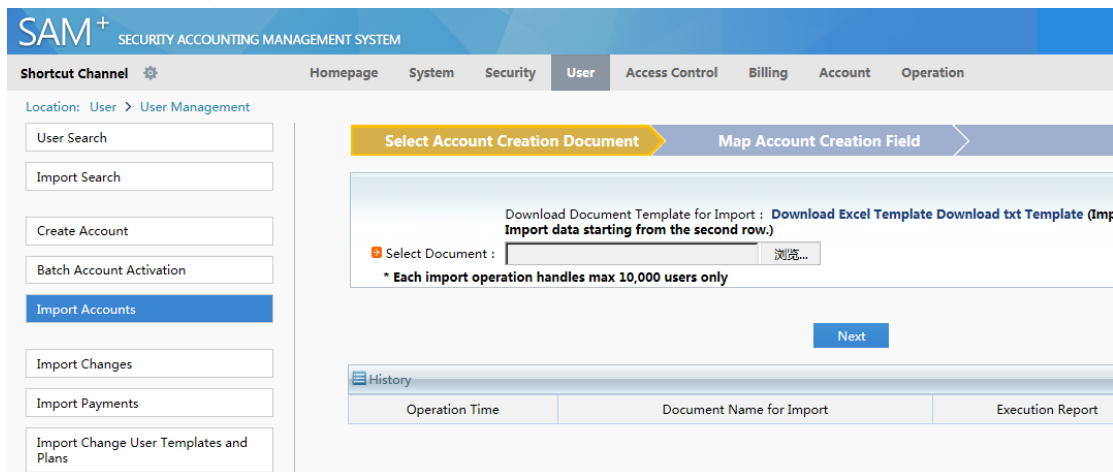
\* Please refer to respective label content for access details

d. Add a user group.





e. Activate accounts in batches.



3. Verify AP load balancing.

Run the **show ipfix on** command on the two MSC-ED cards and check that each card has traffic statistics.

4. Observe the authentication process when users go online.

Run the **show web-auth user all** command on the RG-N18000 to display online user information.

Display the go-online information of users on the SAM server.

## II. Configuration Tips

To avoid loops, run the traffic diversion command of the RG-N18000 and then configure the interface bridge mode of the MSC-ED card.

To avoid loops, when you need to cancel the traffic diversion command of the RG-N18000, exit the interface bridge mode of the MSC-ED card and then exit the bridge mode of the RG-N18000.

Do not run the port migration command when the Layer 2 egress solution is used; otherwise, authentication will be abnormal.

---

## 5.3 Layer 3 Authentication Configuration Case

### 5.3.1 Precautions

Perform the following operations in sequence. Do not skip any operation.

Modify the default passwords of the RG-N18000 and the MSC-ED card to prevent malicious operations and security vulnerabilities.

You can disable the Web management function of the MSC-ED card when necessary for enhanced security.

### 5.3.2 Layer 3 Authentication and Limitations

The switch-based Layer 3 authentication and accounting solution was launched at the beginning of 2016, following the launch of the simplified network solution.

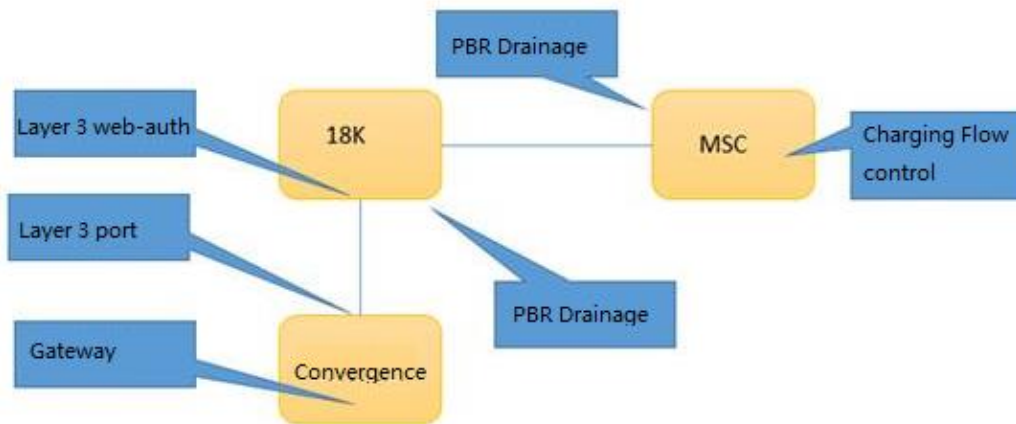
The solution is used in conjunction with the MSC-ED card to implement the Layer 3 Web authentication, accounting, and rate limiting functions.

Functional deployment and distribution:

Authentication: RG-N18000

Accounting: correlation between the MSC-ED card and the RG-N18000

Rate limiting: correlation between the MSC-ED card and the RG-N18000



#### Solution selection and limitations

**The MSC-ED Layer 3 authentication solution only supports Layer 3 Web authentication.**

The solution cannot be used in conjunction with Layer 2 authentication.

Authentication is enabled on the interface of the RG-N18000 connected to the access device. The user gateway cannot be deployed on the RG-N18000, but must be deployed in the downlink direction.

To enable perception-free authentication, deploy the DHCP server on the RG-N18000. The address pool can contain up to 90,000 addresses.

---

Up to four MSC-ED cards can be deployed in load balancing mode, providing a maximum rate of 10 Gbps x 4 in a single direction.

### 5.3.3 Version Selection and Upgrade

Version selection:

Version ID: 4070

MSC-ED authentication and accounting solution (phase 4)

[MSC\\_RGOS11.1\(8\)B1\\_MSC-ED\\_03201819\\_install.bin](#)

[N18000\\_RGOS11.5\(1\)B2\\_CMII\\_03212221\\_install.bin](#)

Note: This document was prepared on October 28, 2016. The version will be upgraded continually. The latest version must be reconfirmed by TAC before deployment.

Version upgrade:

Do not use this solution in conjunction with the simplified network solution in which the simplified gateway is deployed on the RG-N18000.

**MSC-ED card version:**

[MSC\\_RGOS11.1\(8\)B1\\_MSC-ED\\_03201819\\_install.bin](#)

The MSC-ED card must be upgraded independently. Log in to the Web management interface of the MSC-ED card and upgrade the card in one-click mode. Change the file name to **rgos.bin** during the upgrade process.

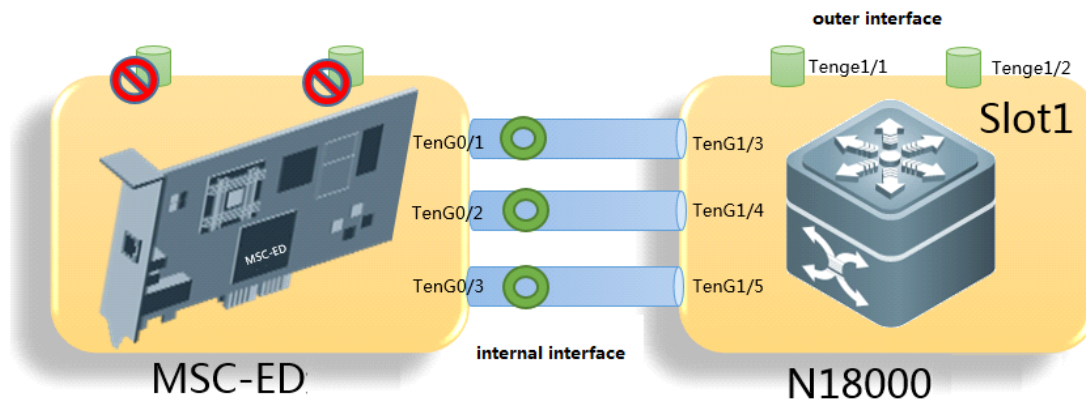
**RG-N18000 version:**

[N18000\\_RGOS11.5\(1\)B2\\_CMII\\_03212221\\_install.bin](#)

After the MSC-ED card is upgraded, upgrade the RG-N18000. Before upgrade, check the size of the flash memory. If it is smaller than 600 MB, clean up the memory.

### 5.3.4 Interconnection Address Design and Configuration

#### I. Mapping of the internal interfaces connected between the MSC-ED card and the RG-N18000



In the preceding figure, the MSC-ED card and the RG-N18000 exchange data over interconnected interfaces.

On the RG-N18000, only three of the seven ports in the corresponding slot can be used.

The usable ports are Port 3, Port 4, and Port 5.

The three ports correspond to Interface 1, Interface 2, and Interface 3 of the MSC-ED card.

Ports have strict service planning. Deploy services in correct ports.

18K	MSC PORT	Port Description
Slot*/3	T0/1	LAN
Slot*/4	T0/2	WAN
Slot*/5	T0/3	MGMT

#### Port description:

LAN interface: transmits uplink traffic from the user side to the Internet.

WAN interface: transmits the downlink traffic returned from the Internet to the user side.

MGMT interface: is used for database access and clock synchronization between the RG-N18000 and the MSC-ED card.

## II. Planning and configuration of internal interconnection addresses

The following describes how to design the internal interconnection addresses based on the model of VSU+dual MSC-ED cards. The address design is the same for a single MSC-ED card and four MSC-ED cards.

Switch the corresponding interfaces to routing mode.

Switch to routing mode on the MSC-ED card

Layer 3 authentication adopts PBR-based traffic diversion. You need to first switch the MSC-ED card to gateway mode. After switching, Layer 2 ports are changed to Layer 3 IP ports. The MSC-ED card restarts when it switches to gateway mode, but the switching does not cause the RG-N18000 to restart.

Log in to the Web management interface of the MSC-ED card, and choose **Network > Interface > Operation Mode**.

Select **Gateway mode**.

Ruijie MSC eWEB MSC Administrator:admin

Home Interface Route DNS Account Security User

Basic Interface Setting **Operation Mode** Link Detection

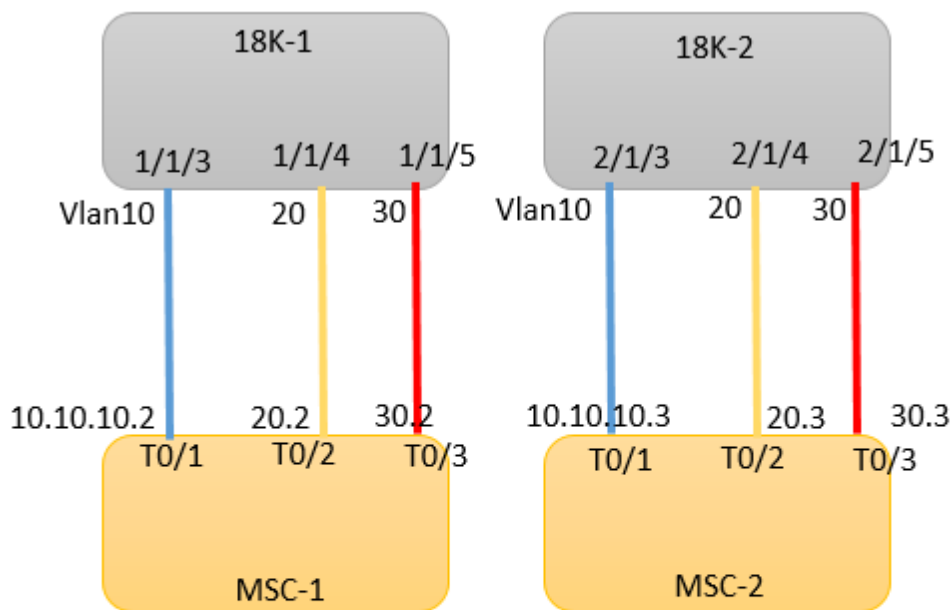
**Bridge mode** : Device will be configured as a Bridge.  
**Gateway mode** : Device will be configured as a Gateway supporting IP Routing features.

Operation Mode:  Bridge mode  Gateway mode

Save settings

Switch to interface routing mode on the RG-N18000

IP port configuration



- LAN** : 18K T1/1/3 ;SVI10 IP=10.10.10.1;→MSC1 T0/1 IP=10.10.10.2  
18K T2/1/3 ;SVI10 IP=10.10.10.1 →MSC2 T0/1 IP=10.10.10.3
- WAN** : 18K T1/1/4 ;SVI20 IP=10.10.20.1;→MSC1 T0/2 IP=10.10.20.2  
18K T2/1/4 ;SVI20 IP=10.10.20.1 →MSC2 T0/2 IP=10.10.20.3
- MGMT** : 18K T1/1/5 ;SVI30 IP=10.10.30.1;→MSC1 T0/3 IP=10.10.30.2  
18K T2/1/5 ;SVI30 IP=10.10.30.1 →MSC2 T0/3 IP=10.10.30.3

The preceding figure shows the IP address configuration of ports in the VSU+dual MSC-ED model. If you need to perform remote Web management of the MSC-ED cards, you are advised to configure a route destined for the management network segment. If remote Web management is not required, route advertisement is not required for the three interconnection address segments. The configuration process is simple and is omitted in this document.

**LAN: 10.10.10.0/24**

**WAN: 10.10.20.0/24**

**Management: 10.10.30.0/24**

	18K VLAN	18K VLAN IP	18K-1 VSU:Port	18K-2 VSU:Port	MSC Port	MSC1:Port Ip	MSC2:Port Ip
Lan	10	10.10.10.1	Slot1/1/3	Slot2/1/3	T0/1	10.10.10.2	10.10.10.3
Wan	20	10.10.20.1	Slot1/1/4	Slot2/1/4	T0/2	10.10.20.2	10.10.20.3
MGMT	30	10.10.30.1	Slot1/1/5	Slot2/1/5	T0/3	10.10.30.2	10.10.30.3

### 5.3.5 NTP Clock Synchronization Configuration

The MSC-ED card collects accounting information and therefore has high requirements for the clock source. It is recommended that the NTP clock source be set to the RG-N18000 for real-time clock synchronization. Before clock synchronization is

completed, the Web management interface and CLI of the MSC-ED card generate alarms indicating lack of clock information. (Accounting information will be inaccurate if clock synchronization is not performed.)

1. Configure the time zones of the RG-N18000 and the MSC-ED card to be consistent. (The time zone of the MSC-ED card is managed by the SNTP server.)

Configuration example:

```
clock timezone dongba +8 0
N18K is configured as NTP master
Configuration example
ntp master 8
```

2. Configure the NTP function on the MSC-ED card (applicable to the CLI version).

```
sntp interval 60
sntp server 10.10.30.1
sntp enable
```

### 5.3.6 MSC-ED Card and RG-N18000 Correlation Configuration

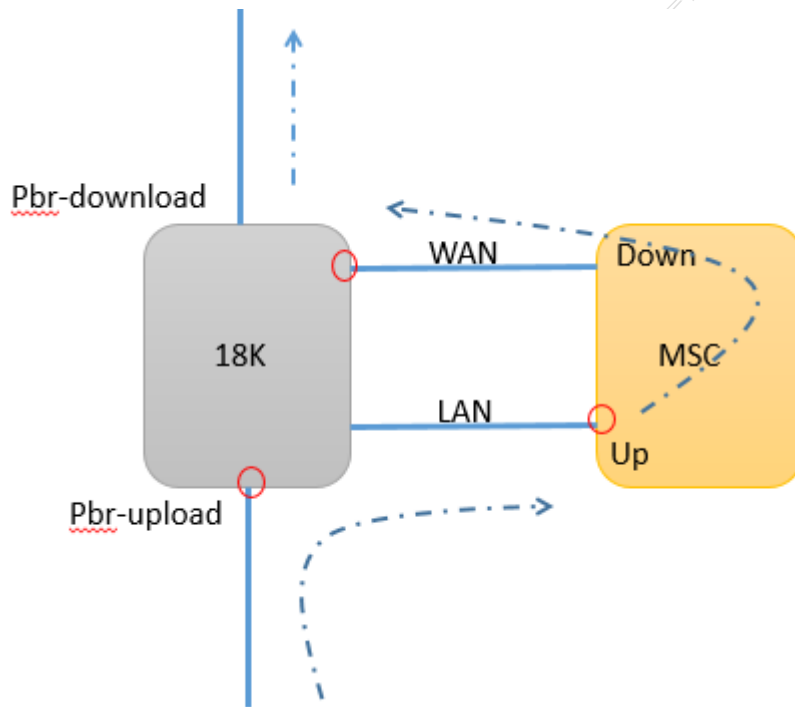
For the latest simplified and phase 4 versions, the correlation address is the interface address of the RG-N18000. You are advised to map the TenG0/3 interface of the MSC-ED card to Slot\*/5 of the RG-N18000 and set the correlation address to the IP address of Slot\*/5 (the IP address of the MGMT interface is 10.10.30.1).

Slot*/5	T0/3	mgmt
---------	------	------

The screenshot shows the Ruijie MSC eWEB MSC Administrator interface. The top navigation bar includes the Ruijie Networks logo, the user 'eWEB MSC Administrator:admin', and a menu with options: Home, Traffic-based Accounting, Correlation (selected), Flow C, Account, Security, and User. The main content area is titled 'Correlation' and 'Correlation Settings'. It features three configuration fields: 'Correlation Type' set to 'Enable 18K Correlation', 'Server IP' set to '192.168.3.1', and 'Whitelist Network Segment' set to 'OFF'. A 'Save' button is located at the bottom right of the settings area.

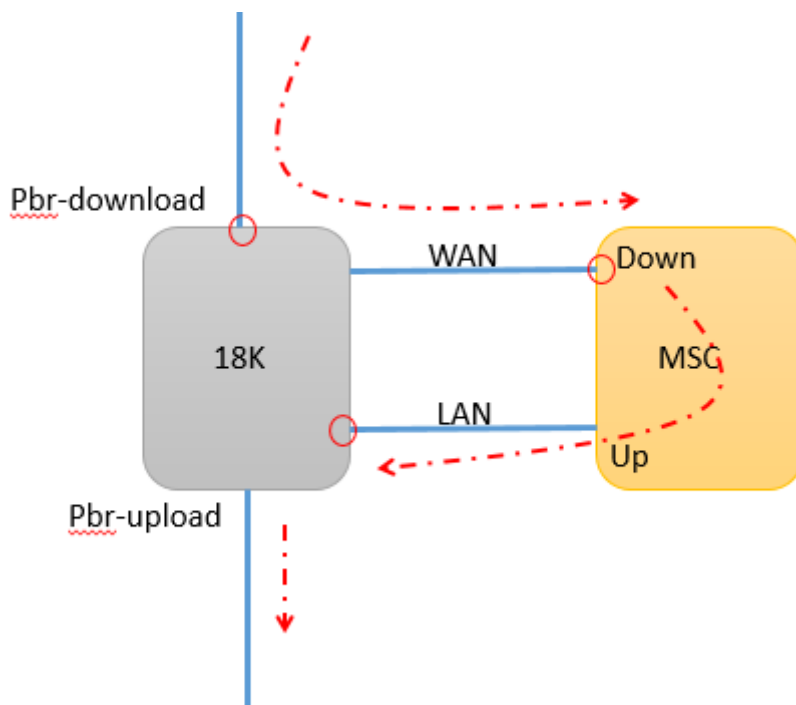
### 5.3.7 PBR-based Traffic Diversion Configuration

Uplink traffic diversion logic



1. When service traffic enters the inbound port of the RG-N18000, the PBR-based traffic diversion function configured on the port sets the next hop for the traffic to the LAN interface of the MSC-ED card.
2. When the traffic enters the LAN interface of the MSC-ED card, the PBR-based traffic diversion function sets the next hop for the traffic to the WAN interface of the RG-N18000.
3. The RG-N18000 forwards the traffic that enters its WAN interface normally.

Downlink traffic diversion logic

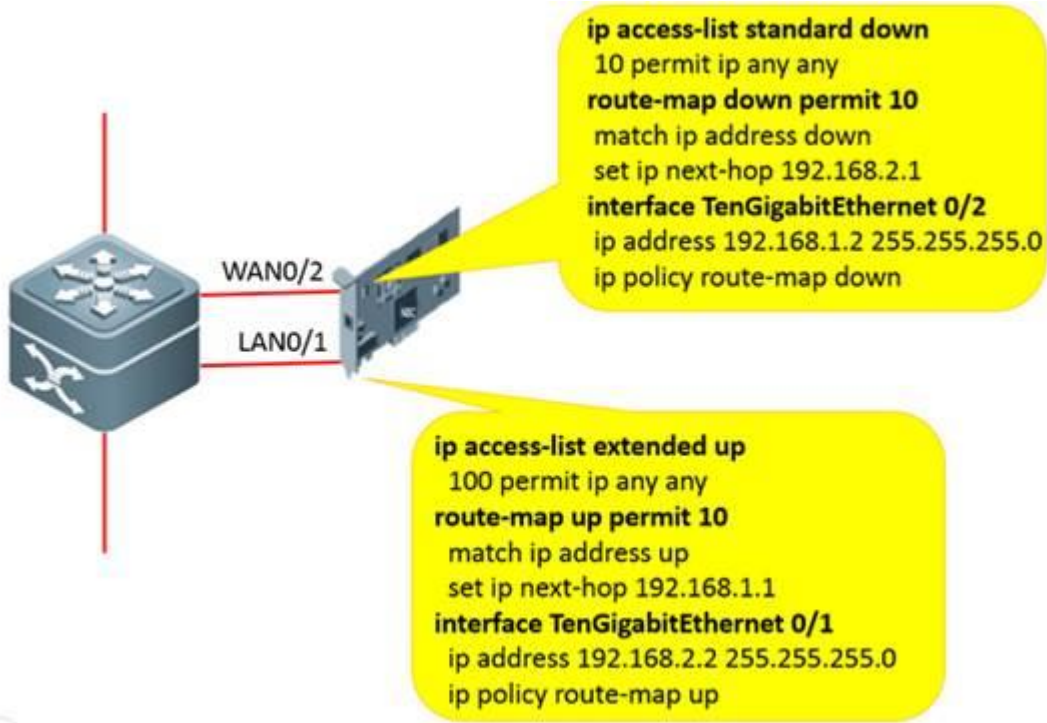




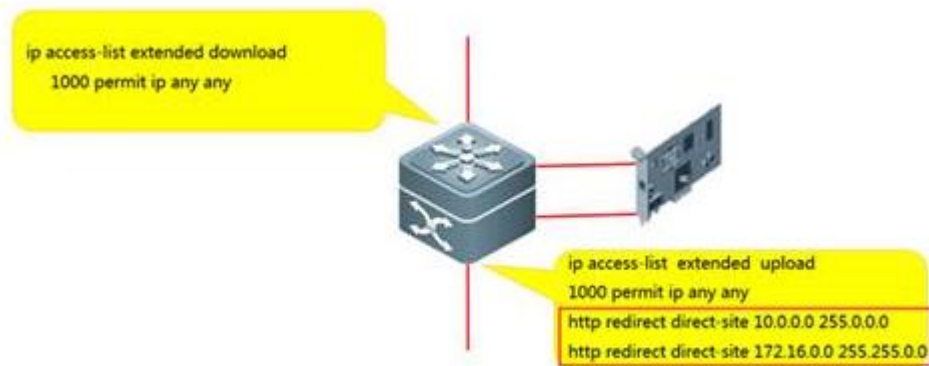
1. When the returned service traffic enters the inbound port of the RG-N18000, the PBR-based traffic diversion function configured on the port sets the next hop for the traffic to the WAN interface of the MSC-ED card.
2. When the traffic enters the WAN interface of the MSC-ED card, the PBR-based traffic diversion function sets the next hop for the traffic to the LAN interface of the RG-N18000.
3. The RG-N18000 forwards the traffic that enters its LAN interface normally.

Traffic diversion configuration

Step 1: Configure PBR-based traffic diversion on the MSC-ED card.



Step 2: Configure PBR-based traffic diversion on the RG-N18000.



```

route-map pbr-download permit 10
match ip address download
set ip policy load-balance dst-ip
set ip policy no-ttl-decrease

```



```

route-map pbr-upload permit 10
match ip address upload
set ip policy load-balance src-ip
set ip policy no-ttl-decrease
set ip policy l3-auth

```

**Note 1:**

- Authentication will fail if Layer 3 authentication is not configured or the upload PBR function does not take effect.
- The **load-balance** command is used to configure load balancing for multiple MSC-ED cards.

```

interface GigabitEthernet 9/1
no switchport
description link-to-server
ip address 192.168.1.144 255.255.255.0
ip policy route-map pbr-download

```



```

interface GigabitEthernet 9/5
no switchport
ip address 188.1.1.17 255.255.255.252
web-auth enable eportalv2
ip policy route-map pbr-upload

```

**Note 2:**

- Traffic diversion takes affect once PBR is invoked. If you have live network services, you are advised to use a test service to check whether traffic diversion is normal.
- If you do not configure track support for the RNS, add the next hop of PBR. (For details about track support for the RNS, visit <http://www.wiz.cn>.)

Add the next hop of PBR:

```

Route-map pbr-upload permit 10
Set ip next-hop 10.10.10.2
Set ip next-hop 10.10.10.3
Route-map pbr-download permit 10
Set ip next-hop 10.10.20.2

```

---

```
Set ip next-hop 10.10.20.3
```

### 5.3.8 Layer 3 Authentication Configuration

Enable Layer 3 authentication on the Layer 3 interconnected interface. If Web authentication is enabled on the Layer 2 interconnected interface, the command executed on the Layer 3 interface is automatically shielded.

```
aaa new-model
radius-server host 192.168.197.79 key ruijie
aaa authorization network default group radius
aaa authentication web-auth default group radius
aaa accounting update periodic 20
aaa accounting update
aaa accounting network default start-stop group radius
```