

Ruijie Networks - Innovation Beyond Networks

SCN Solution Cookbook (V1.0)

Copyright Statement

Ruijie Networks©2013

Ruijie Networks reserves all copyrights of this document. Any reproduction, excerption, backup, modification, transmission, translation or commercial use of this document or any portion of this document, in any form or by any means, without the prior written consent of Ruijie Networks is prohibited.



Exemption Statement

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

Preface

Audience

- Network Engineers
- Network Administrator

Obtain Technical Assistance

- Ruijie Networks Websites: <u>http://www.ruijienetworks.com</u>
- Ruijie Service Portal: <u>http://caseportal.ruijienetworks.com</u>

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

Revision History

| Date | Change contents | Reviser |
|--------|---|-------------|
| 2018.7 | Initial publication V1.0 | Ruijie GTAC |
| 2018.7 | Adjust the overall structure of the cookbook | Ruijie GTAC |
| | Delete some content that doesn't fit with the | |
| | overseas scenerio | |

Content

| Pre | eface | | 2-2 |
|-----|-------------|--|-------|
| 1 | Solution Im | nplementation Process | 2-7 |
| | 1.1 P | reparation Before Implementation | 2-7 |
| | 1.1.1 | Customer Information Collection | 2-7 |
| | 1.2 D | eployment Model Selection | 2-10 |
| | 1.2.1 | Layer 2 Access Isolation | 2-10 |
| | 1.3 C | heck After Implementation | 2-12 |
| | 1.3.1 | Software Information Check on the RG-N18000 | 2-12 |
| | 1.3.2 | Software Information Check on the SAM+ Server | 2-13 |
| | 1.3.3 | Overall Network Running Check | 2-16 |
| | 1.3.4 | Check Points for Important Time Guarantee | 2-17 |
| | 1.3.5 | Network Authentication Health Check After Project Cutover | 2-30 |
| 2 | Solution Co | omponents and Parameters | 2-38 |
| | 2.1 P | arameters of Switch Products | 2-38 |
| | 2.1.1 | Specifications of Core Devices | 2-38 |
| | 2.1.2 | Specifications of Aggregation Devices | 2-39 |
| | 2.1.3 | Capacity Specifications | 2-40 |
| 3 | Typical Sc | enarios | 3-44 |
| | 3.1 A | ccess Isolation Scenario | 3-44 |
| | 3.1.1 | Overall Solution | 3-44 |
| | 3.1.2 | VLAN/IP Planning | 3-46 |
| | 3.2 W | /ireless Isolation Scenario | 3-48 |
| | 3.2.1 | Overall Solution | 3-48 |
| | 3.2.2 | VLAN/IP Planning | 3-51 |
| 4 | Configurati | ion of Important Functions | 4-53 |
| | 4.1 R | G-N18000 Configuration | 4-53 |
| | 4.1.1 | Common Scenario — Gateway | 4-53 |
| | 4.1.2 | Common Scenario — Address Management | 4-58 |
| | 4.1.3 | Common Scenario — Authentication-free Access | 4-73 |
| | 4.1.4 | Common Scenario — Authentication | 4-78 |
| | 4.1.5 | Common Scenario — Authentication Optimization Configuration | 4-94 |
| | 4.1.6 | QinQ Isolation Scenarios | 4-99 |
| | 4.1.7 | Anti-Loop Configuration for Simplistic Networks | 4-101 |
| | 4.1.8 | RG-N18000 Optimization Functions | 4-102 |
| | 4.2 S | AM+ and ePortal Configuration | 4-110 |
| | 4.2.1 | [Optional] Wired RG-N18000—802.1X Authentication | 4-110 |
| | 4.2.2 | [Optional] Wireless AC — 802.1x Authentication | 4-129 |
| | 4.2.3 | [Optional] RG-N18000 — Web Authentication (Wired & Wireless) | 4-146 |
| | 4.2.4 | [Optional] MAB Authentication | 4-166 |

| | 4.2. | [Optional] SSID-based Authentication Page Pushing | 4-172 |
|---|-----------|--|------------|
| 5 | Simplisti | Network Configuration Examples (Important) | 5-173 |
| | 5.1 | Configuration Examples of Access Isolation Solution + Wireless Isolation Solution | 5-173 |
| | 5.1. | Customer Requirements | 5-173 |
| | 5.1. | Topology | 5-175 |
| | 5.1. | Configuration Precautions | 5-175 |
| | 5.1. | VLAN/IP Planning on the Live Network | 5-176 |
| | 5.1. | Configuration Reference Commands on the Core RG-N18000 | 5-177 |
| | 5.1. | Aggregation Configuration Reference Commands for the Dormitory Area | 5-184 |
| | 5.1. | Access Configuration Reference Commands for the Dormitory Area | 5-184 |
| | 5.1. | SAM + and ePortal Related Configurations | 5-185 |
| 6 | Optimiza | on and Precautions for Simplistic Network Configuration | 6-193 |
| | 6.1 | Dptimization and Precautions for the RG-N18000 Configuration | 6-193 |
| | 6.1. | Disabling authentication accounting update | 6-193 |
| | 6.1. | Optimizing HTTPS redirection on the RG-N18000 | 6-193 |
| | 6.1. | Enabling interface index uniqueness | 6-193 |
| | 6.1. | Enabling migration of authenticated users on the RG-N18000 as user re-authe | ntication |
| | is re | uired after AC hot backup switchover | 6-194 |
| | 6.1. | Preventing users with all-zero IP addresses on SAM+ | 6-194 |
| | 6.1. | Ensuring accuracy of online user information on SAM+ and the RG-N18000 | 6-194 |
| | 6.1. | Restricting the number of authentication-free VLANs | 6-195 |
| | 6.1. | Pruning VLANs configured on downlink interfaces of the RG-N18000 | 6-195 |
| | 6.1. | Configuring the downlink interfaces of the RG-N18000 as routing protocol | passive |
| | inte | aces to prevent resource waste | 6-195 |
| | 6.1. | Enabling the RG-N18000 to process DHCP relay packets in a case with DHCP s | nooping |
| | ena | led 6-195 | |
| | 6.1. | 1 Reducing the number of CE-VLANs created during deployment | 6-195 |
| | 6.1. | 2 Disabling the DHCP guard function via NFPP | 6-196 |
| | 6.1. | 3 Configuring alarms for easily-missed or error-prone configurations | 6-196 |
| | 6.2 | Configuration Optimization and Precautions for Aggregation Devices and Access Devices and | vices6-196 |
| | 6.2. | Configuration Optimization of Aggregation Devices and Access Devices | 6-196 |
| | 6.2. | Precautions for Wireless Device Configuration | 6-198 |
| | 6.3 | Scenario Restrictions and Suggestions | 6-199 |
| | 6.3. | Scenario Restrictions | 6-199 |
| 7 | Commor | Troubleshooting for Simplistic Networks | 7-202 |
| | 7.1 | Authentication Page Display Failure During Web Authentication | 7-202 |
| | 7.1. | Symptom | 7-202 |
| | 7.1. | Possible Causes | 7-202 |
| | 7.1. | Handling Steps | 7-203 |
| | 7.1. | Fault Information Collection | 7-205 |
| | 7.1. | Fault Summary and Notes | 7-206 |

| 7.2 | W | eb Authentication Failure | 7-206 |
|-----|-------|---|-------|
| | 7.2.1 | Symptom | 7-206 |
| | 7.2.2 | Possible Causes | 7-206 |
| | 7.2.3 | Handling Steps | 7-207 |
| | 7.2.4 | Fault Information Collection | 7-210 |
| | 7.2.5 | Fault Summary and Notes | 7-210 |
| 7.3 | Ne | etwork Dropout During Web Authentication | 7-210 |
| | 7.3.1 | Symptom | 7-210 |
| | 7.3.2 | Possible Causes | 7-210 |
| | 7.3.3 | Handling Steps | 7-211 |
| | 7.3.4 | Fault Information Collection | 7-215 |
| | 7.3.5 | Fault Summary and Notes | 7-216 |
| 7.4 | 80 | 2.1x Authentication Failure | 7-216 |
| | 7.4.1 | Symptom | 7-216 |
| | 7.4.2 | Possible Causes | 7-216 |
| | 7.4.3 | Handling Steps | 7-216 |
| | 7.4.4 | Fault Information Collection | 7-218 |
| | 7.4.5 | Fault Summary and Notes | 7-219 |
| 7.5 | Ne | etwork Dropout During 802.1x Authentication | 7-219 |
| | 7.5.1 | Symptom | 7-219 |
| | 7.5.2 | Possible Causes | 7-219 |
| | 7.5.3 | Handling Steps | 7-219 |
| | 7.5.4 | Fault Information Collection | 7-221 |
| | 7.5.5 | Fault Summary and Notes | 7-222 |
| 7.6 | M | AB Authentication Failure | 7-222 |
| | 7.6.1 | Symptom | 7-222 |
| | 7.6.2 | Possible Causes | 7-222 |
| | 7.6.3 | Handling Steps | 7-222 |
| | 7.6.4 | Fault Information Collection | 7-225 |
| | 7.6.5 | Fault Summary and Notes | 7-226 |
| 7.7 | E> | ception/Failure in Dynamic Acquisition of IP Addresses | 7-226 |
| | 7.7.1 | Symptom | 7-226 |
| | 7.7.2 | Possible Causes | 7-226 |
| | 7.7.3 | Handling Steps | 7-227 |
| | 7.7.4 | Fault Information Collection | 7-232 |
| | 7.7.5 | Fault Summary and Notes | 7-232 |
| 7.8 | Fa | ilure to Access the Internet or Internet Access Stalling After Authentication | 7-232 |
| | 7.8.1 | Symptom | 7-232 |
| | 7.8.2 | Possible Causes | 7-232 |
| | 7.8.3 | Handling Steps | 7-233 |
| | 7.8.4 | Fault Information Collection | 7-235 |

| | 7.8.5 | Fault Summary and Notes | |
|------|--------|--|--------------------|
| 7.9 | ACL | Statistics Scripts of the Troubleshooting Tool | |
| 7.10 |) Lay | er-2 Loop Problem Locating in Simplistic Networks | |
| | 7.10.1 | Check RLDP logs | |
| | 7.10.2 | Find out the ports and VLANs that encounter the loop | |
| | 7.10.3 | Take measures based on the following cases: | 7-241 |
| 7.1 | I Fail | ure to Query Real-time Traffic of the User Gateway on SAM+ in MSC Ca | ard Scenarios7-245 |
| | 7.11.1 | Symptom | 7-245 |
| | 7.11.2 | Possible Causes | 7-245 |
| | 7.11.3 | Handling Steps | |
| 7.12 | 2 Net | work Access Exception After Traffic Goes Through the MSC Card | |
| | 7.12.1 | Symptom | |
| | 7.12.2 | Possible Causes | |
| | 7.12.3 | Handling Steps | |

1 Solution Implementation Procedure

1.1 Preparation Before Implementation

1.1.1 Customer Information Collection

1.1.1.1 Confirmation of Project Progress

- 1. **Project handover:** Obtain the pre-sales solution information of the project from the pre-sales personnel, to understand the main planning of the customer network. Consider the available project implementation solution based on the equipment list and equipment delivery status.
- Confirmation of implementation environment: Ensure that preparation of the peripheral environment for project implementation is completed, including equipment room construction, power supply (UPS or mains), and cabling of optical fibers/network cables, to guarantee the implementation progress.

1.1.1.2 Survey and Collection of Customer Requirement Information

Before the implementation, it is necessary to fully understand the customer's onsite service application requirements and network construction/reconstruction requirements. Collect information based on the customer's routine service usage and fully understand the customer's basic and special service requirements, to identify risks and make plans in advance based on the demarcation and limitation of the solution. A full understanding of information can provide necessary basis for the development of the implementation solution.

The information to be collected falls into the following categories:

- 1. Network status:
- Network topology information: includes the actual topology of the live network, locations of network equipment and servers, configurations of live network equipment (for in-depth analysis of the live network), and IP address and route planning information of live network equipment (route planning and routing table details).
- 2. Service application status:
- The following table describes the current service application, user scale, and network system operation & maintenance (O&M).

| Level-1 Directory | Level-2 Directory | Refined Service | Information to Be Collected |
|----------------------------------|---------------------|---------------------------------|--|
| Service application status | Office service | OA, mail, FTP, DNS, and DHCP | Information about whether the OA, mail, and FTP applications have extranet access requirements, have traffic guarantee, and allow access to the intranet or VPN environment |
| | Scientific research | Scientific research | Routing mode of scientific research websites or resource |

| | & teaching | websites | queries | |
|------------|------------------|--|---|--|
| | | Multimedia teaching and office | Information about whether the conventional client or virtual space system based on the cloud host is used in the multimedia classroom | |
| | | Online education | Information about whether the campus network provides online education resources, whether the traffic is transmitted over the CERNET or the networks of the three major operators, and whether the bandwidth is largely consumed | |
| | Entertainment | Browser-based entertainment, WeChat, QQ, Taobao, games, and videos | Major online behavior of students, whether rate limiting is performed on students, and whether content-accelerated devices are deployed for high-bandwidth applications | |
| | Campus multicast | 720p/1080p | Number of video program sources in campus network multicast applications, whether the definition standard is HD or ultra HD, and whether video freezing exists at peak hours | |
| | IPv6 | Resource requirements for accessing CERNETII | Information about whether the campus network provides IPv6 resource services, whether an egress exists on CERNET II, which IPv6 resource services are available, and whether a network node exists for IPv6-based independent interworking with other campus networks. | |
| | User type | Leader, teaching staff and relative, student, and visitor | Information about whether the campus network user types are missing, how to assign IP addresses for these users, access mode, and accounting mode | |
| | User count | Scale | Number of users in the campus network and number of online users on the authentication server at peak hours | |
| User scale | | Smart clients, such as the computer, mobile phone, and tablet | With more access clients and more diversified client types, the number of online users at peak hours poses higher pressure on the core and egress devices. Customers are concerned about security control, authorization, authentication, IP address assignment, behavior auditing, and location of clients. | |
| | Client type | All-in-one cards and dumb clients, such as the printer, water meter, and environment monitoring instrument | | |

| | | Video monitoring and multimedia experiment equipment | |
|---------------------------------|--------------------------------------|--|--|
| | Information center | Information system and network sources | Information about whether the school has an independent information center, how responsibilities are divided between the information center and network center, and major concerns of the information center and network center |
| Network system O&M status | Network center | O&M system integration | Information about whether a unified network management platform is configured for routine O&M and device management, and whether there are secondary development requirements for working with other application systems in the school |
| | Establishment and maintenance status | Self-establishment & self-maintenance, external establishment & external maintenance, and co-establishment & co-maintenance | Campus network types and information about how to maintain campus networks |

- 3. **Basic configuration of the server:** includes the server's CPU, memory, disks, network (check the provided server hardware based on the SAM+ system environment preparations to determine whether the SAM+ and ePortal requirements are met), operating system and database versions (check the operating system and database versions based on the SAM+ system environment preparations to check whether the operating system and database meet the installation requirements), and SAM+ software version purchased by the customer (check whether the software version matches with the dongle and meets the project application requirements).
- 4. **Earlier requirements from the customer:** Find out the requirements (check the function support status in the scenario based on the higher education industry solution), evaluate whether the requirements can be met ahead of time, and check whether the requirements are within the scope of the solution.
- 5. **Requirements for interconnecting with live network equipment:** Consider compatibility for interconnecting with the equipment of other vendors, such as the STP, AP aggregation, and SAM+ system.
- 6. User scale in the campus network: includes the number of areas, teaching buildings, dormitory buildings, Web authenticated users, 802.1x authenticated users, and MAB authenticated users.
- 7. **User groups of the customer:** includes the access authentication and accounting requirements for different types of user groups (mainly access control and accounting policies, preparing for the subsequent access control and associated accounting policies of user groups).
- 8. **Operation mode of the customer:** includes the user registration/deregistration process, payment mode, and reconciliation mode, which affect the whole network operation.

9. Special service application

- Confirm the processing requirements for the all-in-one card clients, monitoring clients, and dumb clients with the customer by checking:
- Whether the all-in-one cards are deployed in a private network, which requirements are imposed on solution deployment, whether IP addresses are fixed or automatically obtained, and whether IP address segments or VLANs are consistent or randomly set.
- Whether the door status control system is deployed in a private network and which deployment requirements are posed in the solution scenario.
- Whether the printer application is shared at layer 2 or layer 3.
- Whether a MAC forgery scenario occurs.

1.2 Deployment Model Selection

1.2.1 Layer 2 Access Isolation

1.2.1.1 Scenario Description

| Area | Deployment and Feature Description |
|------------------|---|
| Core area | Two RG-N18000 switches form a VSU, both connecting to the egress area in the upstream direction. One MSC-ED card is inserted into each RG-N18000 to implement user traffic accounting and control. As the user gateway and authentication NAS device on the whole network, the RG-N18000 simultaneously supports Web authentication, wired 802.1x authentication, and MAB authentication. |
| Server area | A SAM+ server and an ePortal server are configured. The SAM+ server collects statistics on the user traffic from the MSC based on the accounting policy. |
| Aggregation area | A layer-2 transparent transmission device is connected to the upstream core devices in master/slave VSU mode via dual links. A trunk interface is configured in the aggregation area, but it is only used for layer-2 transparent transmission. |
| Access area | A protection port is configured to implement layer-2 isolation. VLAN segments need to be independently planned for special services (such as door status control, all-in-on card, and video monitoring) to distinguish from user service VLANs. |

1.2.1.2 Scenario Topology



1.3 Check After Implementation

1.3.1 Software Information Check on the RG-N18000

1.3.1.1 Checking the CPU Usage

1. Method

2. Criteria

- In the healthy state, the value of CPU utilization in five minutes should be less than 30%. Pay attention to risks if the CPU usage exceeds 60%.
- (2) If a great number of configurations are made, a great deal of information is displayed, or the debugging command is configured on the device, the CPU usage may soar instantaneously (normal symptom). Stop the related operation or run the **undebug all** command.

1.3.1.2 Checking the Memory Usage

1. Method

HXJF-N18K#show memory

2. Criteria

```
p.pl {margin: 0.0px 0.0px 0.0px; text-align: justify; font: 10.5px Helvetica} span.sl
{font-kerning: none}
```

The memory usage should be less than 60%. Bearing more services may increase the memory usage. Pay attention to risks if the memory usage exceeds 80% and tends to continuously rise.

1.3.1.3 Checking Logs

1. Method

HXJF-N18K#show log

2. Criteria

```
p.p1 {margin: 0.0px 0.0px 0.0px 0.0px; text-align: justify; font: 10.5px Helvetica} span.s1
{font-kerning: none}
```

Check whether exceptions exist in logs, such as frequent up/down state switches of the interface, down state of the dynamic protocol, and alarms of higher severity.

1.3.1.4 Checking Configuration Information

1. Method

Run the **show run** command in privilege EXEC mode to check the switch configurations:

HXJF-N18K#show run

Pay attention to the following mandatory commands:

```
auth-mode gateway //Enable the gateway mode.
ip radius source-interface (radius interface) //Configure an interconnection interface for
communication between the RG-N18000 and server.
ip portal source-interface (portal interface)
offline-detect interval 15 threshold 0 //Configure no-traffic go-offline.
aaa authorization ip-auth-mode mixed //Configure IP-based AAA authorization.
radius-server attribute nas-port-id format qinq //Mandatory for the QinQ scenario
qinq termination pe-vlan 100-101 // Configure QinQ VLAN tag termination.
ginq termination ce-vlan 200 to 300
```

2. Criteria

Check whether the deployed functions are consistent with the implementation solution, and whether the functions can be optimized.

1.3.2 Software Information Check on the SAM+ Server

1.3.2.1 Monitoring the Management Status

1. Method

Enable the service manager on the SAM+ server to check the running status:



2. Criteria

For a standalone server, no error is prompted in the service manager. As shown in the preceding figure, normal prompt information includes: the system is started successfully, the SAM+ softdog type and validity period are checked, journals are recorded successfully, and a total of xxx users are processed.



1.3.2.2 Checking the CPU and Memory Usage



In the healthy state, the CPU usage should be less than 30%, and the memory usage less than 60%.

1.3.2.3 Checking O&M Logs

1. Method

(1) Enter the SAM+ management page and choose **Operation** > Log to check O&M logs.

| SAM ⁺ se | CURITY ACCOUNTING MAR | NAGEMENT SYSTEM | | | | | | | | | | | Å adr | nin 🕑 Abo | ut I C |
|--|--|---|-----------------------------------|-----------------------------|---------------------|------------------|------------------|---------|-----------|--------|----------|------------|------------------------------|-------------------------|--------------------|
| ihortcut Channel | ø | Homepage | System | Security | User | Access Cont | rol Billing | Account | Operation | | | | | | |
| Location: Operat | ion > Log Management | | | | | | | | | | | | | | |
| Log Type | Authentication Log: • | | Operator | | 1 | | | 🗭 Gene | al Search | Search | | | | | |
| Log Time (Start) | 2018-05-07 00:00:00 | | Log Time | e (End) | 2018-05- | 07 23:59:59 | | | | | | | | | |
| Log Content | | (Always fuzzy que | ry) | | | | | | | | | | | | |
| There were no re | sults found. | | | | | | erete the serect | | | | | C | urrently 1/1Pag | e 🏘 Very Pa | ige 10 |
| There were no re | <mark>sults found.</mark> g Type Lo | g Content | | | | | elete the select | | | | Log Time | (2) | urrently 1 /1Pag Operator | e 🗣 🕼 Very Pa Check | ge 10 Sub-log |
| There were no re | sults found. g Type Lo pt for fuzzy query no matt | g Content er the function is s | elected or not | in log cont | ent | | | | | ţ | Log Time | 🜒 c | urrently 1 /1Pag Operator | e 🕸 Very Pa Check | ge 10 sub-log |
| There were no re Lo The system will o Do you want to so | sults found. g Type Lo pt for fuzzy query no matt et fuzzy query for others b | g Content er the function is s resides log content | elected or not ? Tick to enabl | in log cont le fuzzy que | ent ery and lear | ve blank to enai | ole accurate qui | ny | | | Log Time | S c | urrently 1 /1Pag Operator | e 🕸 Very Pa Check | ge 10 • Sub-log |
| There were no re | sults found. g Type Lo pt for fuzzy query no matt et fuzzy query for others b | g Content ter the function is s sesides log content | elected or not ? Tick to enabl | in log cont le fuzzy que | ent rry and lear | ve blank to enat | ole accurate qui | ny | | | Log Time | 8 c | urrently 1 /1Pag Operator | e 🗐 Very Pa Check | ge 10 . Sub-log |
| There were no re | sults found. g Type Lo pt for fuzzy query no matt et fuzzy query for others b | g Content ter the function is s besides log content | elected or not ? Tick to enabl | in log cont le fuzzy que | ent rry and lear | ve blank to enat | ole accurate qui | ny | | 1 | Log Time | 8 c | urrently 1 /1Pac Operator | e 🗣 Ge Very Pa Check | ge 10 , Sub-log |
| There were no re Lo The system will o Do you want to se | sults found. g Type Lo pt for fuzzy query no matt et fuzzy query for others b | g Content ter the function is s resides log content | elected or not ? Tick to enabl | in log cont le fuzzy que | ent rry and lear | ve blank to enab | ole accurate qui | ny | | | Log Time | 2 c | urrently 1 /1Pac Operator | e 🕸 Ge Very Pa Check | ge 10 • Sub-log |
| There were no re | sults found. g Type Lo pt for fuzzy query no matt et fuzzy query for others b | g Content ter the function is s eesides log content | elected or not ? Tick to enabl | in log cont le fuzzy que | ent rry and lear | ve blank to enat | ole accurate qui | ny | | | Log Time | 8 c | urrently 1 /1Pag Operator | e 🕸 Ge Very Pa Check | ige 10 Sub-log |

(2) Enter the database backup directory to check sizes of backup files and disk space.

| 🌆 l 💽 🗿 = l | 2015-12-11 | | | L |
|-------------|-----------------------------------|--------------|------|----------|
| | | | | |
| ⊕ ⊚ - ↑ 퉬 🕨 | ► SAMDBBAK ► 2015-12-11 ► | • | v ¢ | 5-12-11" |
| | ^ | | | |
| | SAMDB1201_20151211020032_auto.bak | 2015/12/11 2 | :00: | 4,28 |

2. Criteria

- (1) Ensure that the database shrinks properly.
- (2) Ensure that database index fragments are organized properly.
- (3) Ensure that the database is integral.
- (4) Ensure that database parameters are normal.
- (5) Ensure that the automatic database backup is normal.
- (6) Ensure that database files are properly backed up. Ensure sufficient backup disk space to avoid backup failures.

1.3.2.4 Checking Solution Functions

Check whether the deployed functions are consistent with the implementation solution, and whether the functions can be implemented and optimized. For example:

- 1. Check whether the number of online authenticated users meets the expectation.
- 2. Check whether accuracy of traffic control meets the expectation.
- 3. Check whether the accounting policies are correct for different user types (such as the school director, teaching staff and their relatives, and student).
- 4. Check whether an account can log in on multiple clients.

- 5. Check whether different access modes match with different accounting policies.
- 6. Check whether the DHCP check in Web authentication succeeds.
- 7. Check whether users can log in via MAB authentication after the first Web authentication login.

1.3.3 Overall Network Running Check

1.3.3.1 Checking the Network Running Status

Perform a thorough check on the network running status, including the equipment check performed in the normal network running state and the function verification after network implementation:

- 1. Run the **show** command to check the running status of core device functions. For the regular operation commands, refer to the basic information check and spot check of access devices.
- 2. Run the **traceroute** command to check the network connectivity and whether data forwarding paths are correct. This check aims to test the consistency between the forward and return paths in the route design.

According to the configured function verification solution, perform link connection/disconnection and switch restart to test the application services, such as the connectivity test and download speed test, so as to verify the network reliability design.

- 3. Run the **ping** command to test the network delay and processing of large packets.
- 4. Check functions one by one according to the solution scenarios.
- 5. Check the actual service running status of users at peak hours.

1.3.3.2 Checking the Device and System Running Statuses at Peak Hours

1. Check the running status of the RG-N18000 at peak hours.

```
Ruijie#show cpu
                    //The average CPU usage of the switch should be less than 30% in normal
cases.
Ruijie#show cpu-protect mboard
Ruijie#show cpu-protect //Check whether the protocol rate exceeds the expectation and
protocol packets are dropped, to assist in locating the cause for high CPU usage.
Ruijie#show memory
                              //The memory usage of the switch should be less than 60% in
normal cases.
Ruijie#show arp counter //Check the ARP aging time and whether the number of ARP entries
is normal.
Ruijie#show mac-address-table count //Check the number of MAC address tables on the network.
Ruijie#show ip route
                                //Check the routing table scale on the live network.
Ruijie#show web-auth user all
                               //Display Web authenticated users.
Ruijie#show dot1x sum
                               //Display 802.1x authenticated users.
```

2. Check the running status of the SAM+ server at peak hours.

Check the number of authenticated users on the SAM+ server, and whether the CPU usage and memory usage are normal.

| SAM ⁺ security accounting man | AGEMENT SYSTEM | | 🛆 admin 丨 😰 About |
|---|--|---|--|
| Shortcut Channel 🔅 | Homepage System Security User Access | ontrol Billing Account Operation | |
| Health Score Disk Space Check The State S | Total Online Users Account Number License Number Unline | 0 Average Authentication Performance (1 Current Performance (User/s) Buffer 0.00% (0 / 1.00) | 0 Average Accounting Performance Current Performance (User/s) Buffer |
| Internet Traffic Receive Channel Internal Storage Check | SAM Sever Montrong CPU 1% Memory 2408MB / 4095MB (59%) | 17229.22 | Disk Input 0 B/s Disk Output 0 B/s Disk I/O 0 B/s |
| | Packet Handling Report (24Hrs) | | Authentication Packets Accox |

1.3.4 Check Points for Important Time Guarantee

Guide for Checking Important Functional Indicators of the RG-N18000 on Simplistic Network for the Back-to-School Season

1.3.4.1 Regular Information Check

1.3.4.1.1 CPU

1.3.4.1.1.1 Command

show cpu

show cpu | inc postgres

1.3.4.1.1.2 Check Point

Check the CPU usage of the management module and line card, which should not be greater than 50%.

Check whether the CPU usage of an independent process approaches 12.5%. If yes, risks may exist and independent analysis and evaluation are required.

N18014#show cpu

[Slot 1/1: M18000-24GT20SFP4XS-ED, Cpu 0] CPU Using Rate Information CPU utilization in five seconds:45.8% CPU utilization in one minute:41.7% CPU utilization in five minutes:47.8%

| NO | | 5Sec | 1Min | 5Min | Process |
|----|---|-------|-------|-------|-------------|
| | 1 | 0.00% | 0.00% | 0.00% | init |
| | 2 | 0.00% | 0.00% | 0.00% | kthreadd |
| | 3 | 0.00% | 0.00% | 0.00% | migration/0 |
| | 4 | 0.00% | 0.00% | 0.00% | ksoftirqd/0 |

4

÷

Check the CPU usage of the postgres process, which should not stay high.

| N18014#5 | sho | | | |
|----------|----------|-------|----------|----------|
| N18014#5 | show cpu | inc | postgres | 5 |
| 5920 | 0.00% | 0.00% | 0.00% | postgres |
| 5945 | 0.00% | 0.00% | 0.00% | postgres |
| 5947 | 0.00% | 0.00% | 0.00% | postgres |
| 5948 | 0.00% | 0.00% | 0.00% | postgres |
| 5949 | 0.00% | 0.00% | 0.00% | postgres |
| 5953 | 0.00% | 0.00% | 0.00% | postgres |
| 5954 | 0.00% | 0.00% | 0.00% | postgres |
| 5955 | 0.00% | 0.00% | 0.00% | postgres |
| 8101 | 0.00% | 0.00% | 0.00% | postgres |
| 8103 | 0.00% | 0.00% | 0.00% | postgres |
| N18014# | | | | |

1.3.4.1.2 Memory

1.3.4.1.2.1 Command

show memory

1.3.4.1.2.2 Check Point

Check the memory usage, which should not be greater than 50%.

N18014#show mem N18014#show memory System Memory: 1577216KB total, 6370892KB used, 10406324KB free, 37.9% used rate Used detail: 1849716KB active, 326060KB inactive, 146552KB mapped, 3885088KB slab, 390980KB core, 244292KB others PID Vsd Text Rss Data Stack Total Process 27065 0 928 584 656 84 4508 sleep 25727 0 104 1976 17866 84 25726 rl=cnr/0

1.3.4.1.3 Interface Traffic

1.3.4.1.3.1 Command

show int counters rate up

show int usage up

1.3.4.1.3.2 Check Point

Check the port utilization, which should not be greater than 80%.

| N18014#show int usage up Interface | Bandwi | dth | Average Usage | Output Usage | Input Usage | |
|---------------------------------------|--------|------|---------------|---------------|---------------|---|
| | | | | | | |
| GigabitEthernet 1/1/1 | 100 | MDIT | 0.00028200% | 0.00035400% | 0.00021000% | |
| GigabitEthernet 1/1/2 | 1000 | Mbit | 0.139269600% | 0.114220000% | 0.164319200% | |
| GigabitEthernet 1/1/12 | 1000 | Mbit | 0.209825700% | 0.192302800% | 0.227348600% | |
| GigabitEthernet 1/1/13 | 1000 | Mbit | 0.430890150% | 0.861780300% | 0.00000000% | |
| GigabitEthernet 1/1/15 | 1000 | Mbit | 0.529817550% | 0.044433600% | 1.015201500% | |
| GigabitEthernet 1/1/16 | 1000 | Mbit | 0.017101449% | 0.034164400% | 0.000038500% | |
| GigabitEthernet 1/1/17 | 1000 | Mbit | 0.017012000% | 0.034024000% | 0.00000000% | |
| GigabitEthernet 1/1/22 | 1000 | Mbit | 0.000031099% | 0.000031099% | 0.000031099% | |
| TenGigabitEthernet 1/1/47 | 10000 | Mbit | 0.0184451450% | 0.0301233200% | 0.0067669700% | |
| TenGigabitEthernet 1/1/48 | 10000 | Mbit | 0.0000515800% | 0.0000661100% | 0.0000370500% | |
| TenGigabitEthernet 1/7/3 | 10000 | Mbit | 0.0000086200% | 0.0000156200% | 0.0000016200% | |
| TenGigabitEthernet 1/7/4 | 10000 | Mbit | 0.0000086200% | 0.0000156200% | 0.0000016200% | |
| TenGigabitEthernet 1/7/5 | 10000 | Mbit | 0.0000088150% | 0.0000160100% | 0.0000016200% | 4 |

1.3.4.1.4 Error Frame

1.3.4.1.4.1 Command

show interface counters errors

1.3.4.1.4.2 Check Point

Check for the types of error frames.

| N18014#show | interface counters er | rors ex 0 | Collisions | 0 |
|-------------|-----------------------|---------------|------------|-----------|
| Interface | UnderSize | OverSize | | Fragments |
| Gi1/1/12 | 0 | 3518181 | 0 | 0 |
| Interface | Jabbers | CRC-Align-Err | Align-Err | FCS-Err |
| Gi1/1/1_ | 0 | 1 | 0 | 1 , |

1.3.4.1.5 Port Up/Down

1.3.4.1.5.1 Command

show interface link-state-change statistics

1.3.4.1.5.2 Check Point

Check whether a port becomes up and down repeatedly for more than 100 times.

| N18014#show Interface | interface l Link state | ink-state-change statistics Link state change times | Last change time |
|--------------------------|---------------------------|--|---------------------|
| | | | |
| Gi1/1/1 | up | 1 | 2017-08-08 12:31:26 |
| Gi1/1/2 | up | 1 | 2017-08-08 12:31:27 |
| Gi1/1/3 | down | 2 | 2017-08-10 17:44:05 |
| Gi1/1/4 | down | 2 | 2017-08-10 17:44:05 |
| Gi1/1/5 | down | 2 | 2017-08-10 17:44:05 |
| Gi1/1/6 | down | 2 | 2017-08-10 17:44:05 |

1.3.4.1.6 Loop

1.3.4.1.6.1 Command

show rldp loop-detect-log

1.3.4.1.6.2 Check Point

Check for loop logs.

N18014#show rldp loop-detect-log rldp vlan loop log Tue Aug 8 12:47:02 2017 VLAN 2222 is detected loop on interface GigabitEthernet 1/1/24. Tue Aug 8 12:49:03 2017 VLAN 2222 is detected loop on interface GigabitEthernet 1/1/23. Tue Aug 8 12:50:59 2017 VLAN 2222 is detected loop on interface GigabitEthernet 1/1/24.

1.3.4.1.7 Line Card

1.3.4.1.7.1 Command

show version slots

1.3.4.1.7.2 Check Point

Check whether the line card is normal.

| Dev | Slot | Port | Configured Module | Online Module | Software Status |
|-----|------|------|------------------------|------------------------|-----------------|
| 1 | 1 | 48 | M18000-24GT205FP4X5-ED | M18000-24GT205FP4X5-ED | ok |
| 1 | 2 | 0 | none | none | none |
| 1 | 3 | 0 | none | none | none |
| 1 | 4 | 0 | none | none | none |
| 1 | 5 | 0 | none | none | none |
| 1 | 6 | 0 | none | none | none |
| 1 | 7 | 7 | M18000-MSC-ED | M18000-MSC-ED | ok |
| 1 | 8 | 0 | none | none | none |

1.3.4.1.8 Temperature

1.3.4.1.8.1 Command

show temperature

INTOATHARSHOW CEN

1.3.4.1.8.2 Check Point

Check whether the temperature is normal.

| N18014# Switch Switch slot | show temperature 1: RG-N18014 2: RG-N18014 card_type | warning(C) | shutdown(C) | current(C) | |
|--|--|---|---|---|--|
| 1/1 1/2 1/3 1/4 1/5 1/6 1/7 1/8 | M18000-24GT20SFP4X5-ED N/A N/A N/A N/A M18000-MSC-ED N/A | 56 N/A N/A N/A N/A 56 N/A | 80 100 100 N/A N/A N/A N/A 80 100 100 N/A | 39 44 45 44 (68) (55) N/A N/A N/A N/A N/A 45 40 38 47 (-64) (55) N/A | |

1.3.4.1.9 Fan

1.3.4.1.9.1 Command

show fan

1.3.4.1.9.2 Check Point

| fan-id | status | mode | speed-level |
|--------|--------|--------|-------------|
| | | | |
| 1/1 | fail | normal | N/A |
| 1/2 | ok | normal | N/A |
| 1/3 | fail | normal | N/A |
| 1/4 | ok | normal | N/A |
| 1/5 | ok | normal | N/A |
| 2/1 | ok | normal | N/A |
| 2/2 | ok | normal | N/A |
| 2/3 | ok | normal | N/A |
| 2/4 | ok | normal | N/A |
| 2/5 | ok | normal | N/A |

1.3.4.1.10 VSU

1.3.4.1.10.1 Command

show switch virtual topology

show switch virtual link port

1.3.4.1.10.2 Check Point

Check whether the VSU topology and port traffic are normal.

```
N18014#show switch virtual topology
Introduction: '[num]' means switch num, '(num/num)' means vsl-aggregateport num.
Chain topology:
[1](1/1)---(2/1)[2]
Switch[1]: master, MAC: 1414.babe.f012, Description:
Switch[2]: standby, MAC: 00d0.f810.1010, Description:
N18014#
N18014#show switch virtual link port
switch 1:
Port
ime
                            AP State Peer-port
                                                                      RX
                                                                                            TX
                                                                                                                 Upt
         _____
TenGigabitEthernet 1/1/47 1 OK
                                         TenGigabitEthernet 2/4/3
                                                                       53889149
                                                                                            2029005154531
                                                                                                                  3d,
TenGigabitEthernet 1/1/48
2h,8m
                            1 OK
                                        TenGigabitEthernet 2/4/4
                                                                      533083
                                                                                            849009
                                                                                                                  3d.
switch 2:
Port
ime
                             AP State Peer-port
                                                                      RX
                                                                                            TX
                                                                                                                 Upt
TenGigabitEthernet 2/4/3
                                                                      2029005154743
                                                                                            53889239
                          1 OK TenGigabitEthernet 1/1/47
                                                                                                                 3d,
TenGigabitEthernet 2/4/4
2h.8m
                            1 OK TenGigabitEthernet 1/1/48
                                                                                                                 3d,
                                                                     849009
                                                                                            $33083
```

1.3.4.1.11 Packets Destined for the CPU

1.3.4.1.11.1 Command

show cpu-protect

1.3.4.1.11.2 Check Point

Check whether the number of packets destined for the CPU is normal, whether the rate of important packets is normal, and whether packet loss occurs.

Pay attention to the following packet types: arp, dhcp, dot1x, web-auth, web-auths, and rldp.

| %cpu port band Traffic-class | Bandwidth: 200000(pps) Bandwidth(pps) Ra | te(pps) Drop(pp | os) | | | |
|---------------------------------|---|-----------------|-----------|-----------|---------|------------|
| 0 | 40000 10 | 0 | | | | |
| 1 | 40000 2 | 0 | | | | |
| 2 | 150000 0 | 0 | | | | |
| 3 | 40000 | 1 0 | | | | |
| 4 | 40000 0 | 0 | | | | |
| 2 | 40000 0 | 0 | | | | |
| 0 | 40000 0 | 0 | | | | |
| Packet Type | Traffic-class | Bandwidth(pps) | Rate(pps) | Drop(pps) | Total | Total Drop |
| bpdu | 6 | 256 | 0 | 0 | 0 | 0 |
| arp | 1 | 36000 | 2 | 0 | 2265576 | 0 |
| tpp | 6 | 256 | 0 | 0 | 0 | 0 |
| dot1x | 2 | 0 | 0 | 0 | 0 | 0 |
| gvrp | 5 | 256 | 0 | 0 | 0 | 0 |
| rldp | 5 | 2560 | 0 | 0 | 145192 | 0 |
| lacp | 5 | 512 | 0 | 0 | 0 | 0 |
| rerp | 5 | 256 | 0 | 0 | 0 | 0 |
| reup | 5 | 256 | 0 | 0 | 0 | 0 |
| 11dp | 5 | 1536 | 0 | 0 | 36062 | 0 |
| cdp | 5 | 1536 | 0 | 0 | 0 | 0 |
| dhcps | 2 | 20000 | 0 | 0 | 9746962 | 0 |
| dhcps6 | 2 | 20000 | 0 | 0 | 0 | 0 |
| dhcp6-client | 2 | 20000 | 0 | 0 | 0 | 0 |
| dhcp6-server | 2 | 20000 | 0 | 0 | 3345 | 0 |
| dhcp-relay-c | 2 | 20000 | 0 | 0 | 0 | 0 |

1.3.4.1.12 Log

1.3.4.1.12.1 Command

show logging

1.3.4.1.12.2 Check Point

Check whether logs are abnormal.

1.3.4.2 Information Check Specific to Simplistic Network

1.3.4.2.1 DHCP Allocation and Conflict-incurred Failure

1.3.4.2.1.1 Command

show ip dhcp binding

show ip dhcp pool

show ip dhcp conflict

1.3.4.2.1.2 Check Point

Check the total number of IP addresses allocated via DHCP and the number allocated IP addresses in each address pool.

| N18014#show ip dhcp binding | | | | |
|---|------------------|---------------|-----------------------|------|
| Total number of clients : (Expired clients : (Running clients : (|)) | | | |
| IP address Hardware ad N18014# | idress Lea | ase expiratio | on | туре |
| N18014#show ip dhcp pool Pool name Total | Distributed 0 | Remained 0 | Percentage 0.00000 | |
| N18014# | | | | |

Check the status of conflict-incurred failures.

1 · · · P . . N18014#show ip dhcp conflict IP address Detection Method N18014# N18014#

1.3.4.2.2 Number of ARP/MAC Addresses

1.3.4.2.2.1 Command

show arp count

debug bridge mac

show mac count

undebug all

1.3.4.2.2.2 Check Point

Check the number of static ARP/MAC addresses, which should be equal to the total number of authenticated users.

Check the number of ARP addresses, which should be equal to that of IP addresses allocated via DHCP (in the case without static IP addresses).

÷

```
N18014#show arp counter
                                               170000
ARP Limit:
                                               30001
Count of static entries:
Count of dynamic entries:
                                                          (complete: 21007 incomplete: 1)
                                               21008
                                               51009
Total:
MI OOI 44ch mar cou
N18014#debug bridge mac
                                                                                    Quantity of static MAC addresses
N18014#show mag count
051038: *Aug 11 14:54:27: N18014 MMAC-7-SERVER_DEBUG: Remain(97989): Total(128000), SS-origin-count(10), BRI-origin-count (30001)
051039: *Aug 11 14:54:27: N16014 %MAC-7-SERVER_DEBUG: Local Address Count : 64
Dynamic Address Count : 10
Static Address Count : 0
Filtering Address Count: 0
Total Mac Addresses : 10
                    : 10
Total Mac Address Space Available: 97989
N18014#und all
All possible debugging has been turned off
```

1.3.4.2.3 ND Entry

1.3.4.2.3.1 Command

show ipv6 neighbors statistics

1.3.4.2.3.2 Check Point

Check the number of ND entries:

Entries: not greater than three times the number of ARP entries.

Probe: not greater than 1000.

Incomplete: not greater than 1000.

N18014#show ipv6 neighbors statistics

Memory: 11648 bytes
Entries: 16
Static: 0,Dynamic: 6,Local: 10
Incomplete:0, Reachable:11, Stale:5, Delay:0, Probe:0
N18014#
N18014#

1.3.4.2.4 Status of RADIUS Server and Portal Server

1.3.4.2.4.1 Command

show web-auth portal

show radius server

1.3.4.2.4.2 Check Point

Check whether the status of the portal server is **Enable**.



Check whether the status of the RADIUS server is Active.

If the timeouts values of Authen/Author are high, the authentication may take a long time or the authentication fails.

If the timeouts value of Account is high, check whether abnormal logs exist on the SAM+ server.

```
NLOVIATSION I AUTUS SEI
N18014#show radius server
Server IP:
             192.168.1.13
Accounting Port: 1813
                  1812
Authen Port:
Test Username: <Not Configured>
                  60 Minutes
Test Idle Time:
                 Authen and Accounting
Test Ports:
Server State:
                Active
    Current duration 4650s, previous duration Os
    Dead: total time Os, count 0
    Statistics:
       Authen: request 11, timeouts 0
       Author: request 11, timeouts 0
        ACCOUNT: request 114, timeouts 100
```

1.3.4.2.5 Number of 802.1x Authenticated Users and Failure Events

1.3.4.2.5.1 Command

show dot1x

show dot1x authmng abnormal

1.3.4.2.5.2 Check Point

Check the number of 802.1x users.

| N18014#show dot1x | |
|--|---|
| 802.1X Status: Authentication Mode: Total User Number: Authed User Number: Dynamic User Number: Pending User Number: Re-authen Enabled: Re-authen Period: Quiet Timer Period: Tx Timer Period: Supplicant Timeout: Server Timeout: Re-authen Max: Maximum Request: Private supplicant only: Client Online Probe: Eapol Tag Enable: Authorization Mode: Hello Interval: Hello Alive: | enabled eap 3(exclude dynamic user) 3(exclude dynamic user) 0 0 disabled 3600 sec 10 sec 3 sec 10 sec 5 sec 3 times 3 times disabled disabled disabled mixed 20 Seconds (default 20s) 250 Seconds (default 250s) |
| £ | |

Check for abnormal events in 802.1x authentication.

| v18014#show Fime User | dot1x authmng ab Mac | AuthTime | AaaTout | ReqIdTout | ReqTout | RsnaNtfy | StrNtfy | туре | Reason | Rs |
|-----------------------------|-------------------------|----------|---------|-----------|---------|----------|---------|-------------|--------------|----|
| | | | | | | | | | | |
| 3.11 15:20 | :59 0040.6400.004 | 4 24 | 0 | 0 | 0 | 0 | 0 | D1X_AUTH | aaa reject | 0 |
| 3.11 15:20 | :59 1414.4b3c.770 | 2 0 | 0 | 0 | 0 | 0 | 0 | D1X_AUTH | valid ip mab | 0 |
| 3.11 15:23 | :56 0040.6400.004 | 4 60 | 0 | 0 | 0 | 0 | 0 | D1X_AUTH | aaa reject | 0 |
| 3.11 15:26 3m 00406400 | :45 0040.6400.000 | 4 0 | 0 | 0 | 0 | 0 | 0 | D1X_OFFLINE | no flow | 0 |
| 3 .11 15:38 3m 002064020 | :16 0020.6402.000 | 1 0 | 0 | 0 | 0 | 0 | 0 | D1X_OFFLINE | no flow | 0 |
| 3 .11 15:38 3m 002064020 | :16 0020.6402.000 | 2 0 | 0 | 0 | 0 | 0 | 0 | D1X_OFFLINE | no flow | 0 |
| 3.11 15:38 | :16 0020.6402.000 | 0 0 | 0 | 0 | 0 | 0 | 0 | D1X_OFFLINE | no flow | 0 |

1.3.4.2.6 Number of Web Authenticated Users and Failure Events

1.3.4.2.6.1 Command

show web-auth user all

show web-auth authmng abnormal

1.3.4.2.6.2 Check Point

Check the number of Web authenticated users.

N18014#show web-auth user all Current user num: 1, Online 1 Address Online Time Limit Time Used Status Name Terminal-type 100.0.46.166 On 240d 00:01:37 Od 00:17:26 Active ceshi3 PC windows 7

Check for abnormal events in Web authentication.

N18014#show web-auth authmng abnormal record num:0, value:3000, max-num:1000, clock:1 N18014#

1.3.4.2.7 No-traffic Go-offline

1.3.4.2.7.1 Command

show run | in off

1.3.4.2.7.2 Check Point

Check whether only the VLAN-based no-traffic go-offline period is configured.

```
N18014#show run | in off
offline-detect interval 6 threshold 0
offline-detect interval 6 threshold 0 vlan 2001
N18014#
```

1.3.4.2.8 Number of Authentication-free VLANs

1.3.4.2.8.1 Command

show direct-vlan

1.3.4.2.8.2 Check Point

Check whether the number of authentication-free VLANs exceeds 50.

N18014#show direct-vlan direct-vlan 192,1600-1601,2006-2007,2101-2102 Port direct-vlan Ag57 direct-vlan 333

1.3.4.2.9 One-to-Many Mirroring

1.3.4.2.9.1 Command show run | inc remote-span show run | inc mac-loopback show monitor show switch virtual link port show int usage up

1.3.4.2.9.2 Check Point

Check whether one-to-many mirroring is configured and whether a VSL has approximately full bandwidth.

If yes, it is necessary to take countermeasures, for example, change the mirroring mode (one-to-one mirroring to the layer-2 switch and flooding to multiple egresses), and change the VSL to 40 Gbps.

If no countermeasure is available, contact the TAC and R&D engineers.

1.3.4.2.10 AP Across Line Cards and Chassis

1.3.4.2.10.1 Command

show version slot

show agg sum

1.3.4.2.10.2 Check Point

Check whether an AP across line cards and chassis exists, and whether a VAC solution is used. If a VAC solution is used and the CPU usage of a line card exceeds 70%, contact the TAC and R&D engineers.

1.3.5 Network Authentication Health Check After Project Cutover

1.3.5.1 802.1x Authentication

DLUT-CORE-N18014#show dot1x authmng statistic

show 802.1x authentication information:

802.1x authentication statistics:

| authentication number: | |
|--------------------------------------|--|
| authentication success: | 0. |
| authentication success rate: | |
| aaa reject | : 49 |
| user logoff | : 0 |
| conflict account | : 0 |
| valid ip mab | : 0 |
| adjust authentication success rate: | |
| request id timeout | : 2258> |
| request timeout | : 14> |
| aaa timeout | : 1> |
| other timeout | : 0> The network or server is unstable |
| according to the preceding four time | eout items. |
| ipam not allowed | : 0> AM rules are not met. |
| ip band width fall | : 0> IP/bandwidth authorization fails. |
| set scc fall | : 0> SCC setting fails due to bottom |
| layer errors. | |
| author vlan fail | : 0 |
| vid modify | : 0 |
| prot user limit | : 0> The number of users is limited |
| due to configuration errors. | |
| total user limit | : 0> The total number of users is |
| limited due to configuration errors | |
| acct cache deny | : 0> Accounting results are cached |
| slowly due to the unstable server of | r network. |
| other security type | : 0> Other security functions are |
| configured generally. | |
| close auth switch | : 0> 802.1x authentication is |
| disabled globally. | |
| deny non-rg client | : 0> Non-Ruijie clients are |
| filtered out. | |

| mab vlan deny | : 0> | The VLAN does not comply with |
|---------------------------------------|-------|-------------------------------|
| MAB VLAN configurations. | | |
| valid ip | : 0> | No IP address is obtained. |
| set acl fail | : 0 | |
| port down | : 0 | |
| not allow user | : 0 | |
| authentication success rssi avgvalue: | 0dBm. | |
| authentication fail rssi avgvalue: | 0dBm. | |

802.1x offline statistics:

| offline_total: | | |
|----------------------------------|------------|------------------------------------|
| user logoff | : 0 | |
| server kickout user | : 0 | |
| no flow | : 0 | > The user goes offline due to |
| no traffic. | | |
| noip | : 0 | > The user is forced to go offline |
| because it fails to obtain an II | P address. | |
| session timeout | : 0 | > The available online period |
| times out. | | |
| flux out | : 0 | > The traffic is used up. |
| svr kickout user | : 0 | |
| hello timeout | : 0 | > The client detection times |
| out. | | |
| scc rollback | : 0 | > SCC setting fails due to bottom |
| layer errors. | | |
| mac rollback | : 0 | > MAC setting fails due to bottom |
| layer errors. | | |
| ip bandwith fail | : 0 | > Authorization fails. Check |
| whether any configuration error | exists. | |
| mng no port control | : 0 | > |
| mng author change | : 0 | |
| mng allow user change | : 0 | |
| mng direct vlan change | : 0 | |
| mng clear cli | : 0 | |
| mng ipam change | : 0 | |
| mng staitc mac | : 0 | |
| mng filter mac | : 0 | |
| mng set mumab | : 0 | |
| mng mab vlan change | : 0 | |
| mng ip acct change | : 0 | |
| mng ctrl mode | : 0 | |

| mng vlan change | : 0> The preceding items indicate |
|--|---|
| that configurations are changed. | |
| port move | : 295 |
| vlan move | : 0 |
| port-vlan move | : 0> The preceding items indicate |
| that migration occurs. | |
| invalid ip | : 0 |
| port down | : 0 |
| gsn fail | : 0 |
| mab to 1x | : 0> MAB authentication is replaced |
| by 802.1x authentication. Check whethe | r 802.1x authentication is used by the user. |
| mab to guest vlan | : 0 |
| dhcp author fail | : 0 |
| db recover fail | : 0 |
| adb author fail | : 0> The preceding VLAN |
| authorization items are generally not | configured in the simplistic network environment. |
| recover to scc fail | : 0> SCC setting fails possibly |
| due to bottom layer errors. | |
| ha recover fail | : 0> Hot backup recovery fails |
| possibly due to processing logic error | s in 802.1x authentication. |
| ip mab unset ip | : 0 |
| s mab change | : 0 |
| offline_by_auth: | 0. |
| request id timeout | : 0 |
| request timeout | : 0 |
| aaa timeout | : 0 |
| other timeout | : 0 |
| aaa reject | : 0 |
| ipam not allowed | : 0 |
| ip band width fall | : 0 |
| set scc fall | : 0 |
| user logoff | : 0 |
| author vlan fail | : 0 |
| vid modify | : 0 |
| prot user limit | : 0 |
| total user limit | : 0 |
| acct cache deny | : 0 |
| other security type | : 0 |
| close auth switch | : 0 |
| deny non-rg client | : 0 |
| mab vlan deny | : 0 |

| valid ip | : 0 |
|---|-----------------------------------|
| set acl fail | : 0 |
| port down | : 0 |
| not allow user | : 0 |
| conflict account | : 0 |
| valid ip mab | : 0> The preceding items indicate |
| failure statistics collected during the | authentication. |

1.3.5.2 MAB Authentication (Same as 802.1x Authentication)

1.3.5.3 Web Authentication

DLUT-CORE-N18014#show web-auth authmng statistics

Show web authentication information:

Web authentication redirect statistics:

HTTP packet processing:

| number of users:1297 | 73993 Number of users |
|--|------------------------|
| whose HTTP packets are processed | |
| number of HTTP packets received:1543 | 3216156 Number of HTTP |
| packets received | |
| redirection time consumption for successful users: | Time consumption for |
| redirection | |
| average time consumption:58ms | 5. |
| aggregate time consumption: | 35499875ms. |
| number of less than half one second:6638 | 309946(98.738%). |
| number of between half and one second:2082 | 2988(0.310%). |
| number of more than one second:6402 | 2954. |
| Web authentication statistic: | Statistics related to |
| Web authentication | |
| authentication processing: | |
| number of authentication requests received:7841 | |
| number of reauthentication requests received:2255 | 537. |
| number of error password: | 339. |
| number of authentication failures: | 32(6.202%). |

| AAA timeout: | AAA |
|---|--------------------|
| authentication times out due to the unstable network or server. | |
| authentication status timeout:1(0.002%). | Authentication |
| device timeout | |
| fail to set SCC:0(0.000%). | SCC setting |
| fails due to bottom layer errors. | |
| accounting reject:0(0.000%). | Rejection from |
| the accounting server | |
| accounting dev timeout:0(0.000%). | Accounting |
| device timeout | |
| user unexist:1154(2.373%). | The user does |
| not exist. | |
| portal timeout:0(0.000%). | Portal server |
| timeout | |
| DHCPrelease pkt:0(0.000%). | No statistics |
| are collected for the following four items. Neglect them. | |
| sta move:0(0.000%). | |
| clear user:0(0.000%). | |
| config change:0(0.000%). | |
| other: | |

Authentication time consumption for successful users:

| average time consumption: | .94ms. | | Time | consumptior | for |
|---|------------|---------|-------|--------------|-------|
| authentication | | | | | |
| aggregate time consumption: | .32609811 | ms. | | | |
| number of less than one second: | .341995(9 | 9.372% |). | | |
| number of between one and three second: | .667(0.19 | 4%). | | | |
| number of more than three second: | .1494(0.4 | 34%). | | | |
| number of less than one second(exclude server): | .344121(9 | 9.990% |). | | |
| number of between one and three second(exclude server) | :6(0.002% |). | | | |
| number of more than three second(exclude server): | .29(0.008 | %). | | | |
| | | | | | |
| Web authentication offline information: | | Sta | tisti | cs related t | o Web |
| user go-offline | | | | | |
| number of offline count: | 341069. | | | | |
| <pre>number of abnormal offline(rate):</pre> | .408(0.11 | 9%). | | | |
| number of portal timeout: | 408(100.0 | 00%). | 7 | The user go | es |
| offline because the portal server does not respond, which | is possibl | ly resu | lted | from an unst | able |
| network or server. | | | | | |
| number of set fail: | 0.000%) | | s(| CC setting f | ails |
| due to bottom layer errors. | | | | | |

| number of link change:0. | No statistics are |
|--|--------------------|
| collected. | |
| no flow: | The user goes |
| offline due to no traffic. | |
| kick off:23745. | The user is forced |
| to go offline by the server. | |
| dhcp release: | The user goes |
| offline due to DHCP release. | |
| STA delete:0. | The user is forced |
| to go offline. | |
| STA move:0. | The user goes |
| offline due to client migration. | |
| active offline:15817. | The user goes |
| offline actively. | |
| session timeout: | The user goes |
| offline because the available online period times out. | |
| cli clear:0. | The user goes |
| offline because the CLI command is cleared. | |
| no control:0. | The user goes |
| offline because control is disabled. | |
| interface default:0. | The interface is |
| the default one. | |
| interface destroy:0. | The interface is |
| destroyed. | |
| interface add ap:0. | The interface is |
| added to an AP. | |
| del ap:0. | The interface is |
| deleted from an AP. | |
| dhcp ip check:0. | The user goes |
| offline due to DHCP IP check. | |
| vlan change:0. | The user goes |
| offline due to VLAN changes. | |
| intfvlan change:0. | The user goes |
| offline due to layer-3 VLAN configuration changes. | |
| other: | |
| aggregate online time:444256014min | |
| average online time of user: | Average online |
| duration of the user | |
| Station-move: | |
| move count. 060627 | Number of |
| migrations | Maniper OI |
| mitgractons | |
--- Number of migration failures Other important process statistics: --- Time consumption statistics of all modules are listed below. ∆uth• --- Time consumption for Web authentication average time consumption:.....71ms. AAA authentication: --- Time consumption for AAA authentication average time consumption:.....2ms. aggregate time consumption:.....1013078ms. number of more than one second:.....2. Radius authentication: --- Time consumption for RADIUS authentication number of more than one second:.....0. Radius server authentication: --- Time consumption for RADIUS server authentication average time consumption:.....55ms. aggregate time consumption:.....19158014ms. SCC: --- Time consumption for SCC setting average time consumption:.....Oms. number of more than one second:.....0.

Accounting: --- Time consumption for accounting average time consumption:.....23ms. AAA accounting: --- Time consumption for AAA accounting aggregate time consumption:.....1081861ms. number of more than one second:.....2. Radius accounting: --- Time consumption for RADIUS accounting average time consumption:.....1ms. Radius server accounting: --- Time consumption for RADIUS server accounting average time consumption:.....2ms. Portal: --- Time consumption of the portal server average time consumption:.....0ms. aggregate time consumption:.....Oms. number of more than one second:.....0.

2 Solution Components and Parameters

2.1 Parameters of Switch Products

2.1.1 Specifications of Core Devices

| Device Type | Product Type | Product Model | Quantity of Clients Supported in Authentication |
|------------------|-------------------|---------------|--|
| RG-N18000 | Supervisor module | СМ | 600 for Web authentication; 3000 for 802.1x authentication |
| RG-N18000 | Supervisor module | CMII | 60000 |
| N18007 | Supervisor module | СМ | 600 for Web authentication; 3000 for 802.1x authentication |
| N18007 | Supervisor module | CMII | 60000 |
| N18007 | Supervisor module | CM II-LITE | 15000 |
| Device Type | Product Type | Product Model | Quantity of Supported Online Dual-stack Clients (ARP) |
| RG-N18000/N18007 | Line card | ED card | 60000 |
| RG-N18000/N18007 | Line card | DB card | 30000 |
| Device Type | Product Type | Product Model | Quantity of Inner VLANs Supported in QinQ Scenarios |
| RG-N18000/N18007 | Line card | ED card | 511 |
| RG-N18000/N18007 | Line card | DB card | 61 |
| Device Type | Product Type | Product Model | Quantity of Supported MAC Tables |
| RG-N18000/N18007 | Line card | ED card | 128000 |
| RG-N18000/N18007 | Line card | DB card | 96000 |
| Device Type | Product Type | Product Model | Supported DHCPv4 Capacity |
| RG-N18000 | Supervisor module | СМ | 8000 |
| RG-N18000 | Supervisor module | CMII | 90000 |
| N18007 | Supervisor module | СМ | 8000 |
| N18007 | Supervisor module | CMII | 90000 |
| N18007 | Supervisor module | CM II-LITE | 90000 |

| Device Type | Product Type | Product Model | Supported DHCP Snooping Capacity |
|---|--|---|---|
| RG-N18000 | Supervisor module | СМ | 8000 |
| RG-N18000 | Supervisor module | CM II | 90000 |
| N18007 | Supervisor module | СМ | 8000 |
| N18007 | Supervisor module | CM II | 90000 |
| N18007 | Supervisor module | CM II-LITE | 90000 |
| | | | |
| Device Type | Product Type | Product Model | Supported DHCPv6 Capacity |
| Device Type RG-N18000 | Product Type Supervisor module | Product Model | Supported DHCPv6 Capacity 8000 |
| Device Type RG-N18000 RG-N18000 | Product Type Supervisor module Supervisor module | Product Model CM CM II | Supported DHCPv6 Capacity 8000 90000 |
| Device Type RG-N18000 RG-N18000 N18007 | Product Type Supervisor module Supervisor module Supervisor module | Product Model CM CM II CM | Supported DHCPv6 Capacity 8000 90000 8000 |
| Device Type RG-N18000 RG-N18000 N18007 N18007 | Product TypeSupervisor moduleSupervisor moduleSupervisor moduleSupervisor module | Product Model CM CM II CM CM II | Supported DHCPv6 Capacity 8000 90000 8000 90000 |

2.1.2 Specifications of Aggregation Devices

| Device Type | Product Model | Whether Flexible QinQ Supported | Recommended Version | Description |
|-------------|---------------------------------|------------------------------------|------------------------------|--|
| Aggregation | S5750 series (hardware V1.0) | Yes | 10.4(3)p4 release(161753) | Only 768 outer VIDs are supported for inner/outer VID mapping. |
| Aggregation | S5750 series (hardware V2.0) | Yes | 10.4(3)p4 release(161753) | N/A |
| Aggregation | S5750E series | Yes | 10.4(3b18)p2,Release(207466) | N/A |
| Aggregation | S29E | Yes | 10.4(2b12)p2 release(180357) | N/A |
| Aggregation | S2910XS-E series | Yes | S2910_RGOS 11.4(1)B1 | N/A |
| Aggregation | S6200 | Yes | 10.4(5b1) release(150539) | N/A |
| Aggregation | S5760 series | No | N/A | The device needs to be replaced. |
| Aggregation | S26 series | No | N/A | The device needs to be |

| | | | | replaced. |
|-------------|-----------|----|-----|----------------------------------|
| Aggregation | S7610 | No | N/A | The device needs to be replaced. |
| Aggregation | S7604 | No | N/A | The device needs to be replaced. |
| Aggregation | S35 | No | N/A | The device needs to be replaced. |
| Aggregation | NBS5526XG | No | N/A | The device needs to be replaced. |

2.1.3 Capacity Specifications

| Level-1 Specifications | Level-2 Specifications | Level-3 Specifications | RG-N18000 (ED) | RG-N18000 (DB) |
|------------------------------------|---------------------------|---|-----------------------|-----------------------|
| | Web authentication | Web user capacity | 60,000 for dual-stack | 30,000 for dual-stack |
| Authentication | 802.1x authentication | 802.1x user capacity | 60,000 for dual-stack | 30,000 for dual-stack |
| capacity | Web MAB authentication | Web MAB authentication capacity | 60,000 for dual-stack | 30,000 for dual-stack |
| IPv4 application protocol features | DHCP server | Quantity of users supported by the DHCP server | 256K | 256K |
| | DHCP relay | Quantity of supported servers | N/A | N/A |
| | DHCP snooping | Capacity of software-bound database | 256K | 256K |
| Layer-2 features | MAC address | Quantity of global MAC addresses (the maximum quantity of MAC addresses supported by the MAC address table need to be learned in full mesh mode) | | |
| | | Quantity of static MAC addresses | 10000 | 10000 |
| | | Quantity of filtered MAC | 10000 | 10000 |

| | | addresses | | |
|------------------|---------------------|--|---|--|
| | | MAC address learning rate | 2000/S | 2000/S |
| | Quantity of clients | Quantity of clients (for IPv4/IPv6 dual-stack, each client is assigned with an IPv6 address and an IPv4 address) | CM: 5000 for the case with only 802.1x authentication 1000 for the case with only Web authentication CM II: 60,000 (recommended) in default mode | CM: 5000 for the case with only 802.1x authentication 1000 for the case with only Web authentication CM II: 45,000 (recommended) in default mode. |
| | ARP | ARP entry capacity (the maximum quantity of ARP entries supported by the ARP table need to be learned in full mesh mode) | Default mode: 170,000 (sharing resources with ND) | Default mode: 85000 (sharing resources with ND) |
| | | ARP learning rate | CM I: 3000/s; CM II: 10,000/s | CM I: 3000/s; CM II: 10,000/s |
| | ND | ND entry capacity (the maximum quantity of ND entries supported by the ND table need to be learned in full mesh mode) | CM: 5000 CM II: 75,000 in default mode (sharing resources with ARP). | CM: 5000 CM II: 60000 in default mode (sharing resources with ARP). |
| Layer 3 Features | | ND learning rate | CM I: 1500/s; CM II: 5000/s | CM I: 1500/s; CM II: 5000/s |
| | | Quantity of IP addresses set on each layer-3 interface | 4000 | 4000 |
| | IPv4 | Capacity of IPv4 hardware routing table (the maximum quantity of routing entries supported by the routing table need to be learned in full mesh mode) | Default mode: 12,000 | Default mode: 384000 |
| | | Capacity of static routing table | The default value is 1024. A command can be used to configure a maximum of 10,000 | The default value is 1024. A command can be used to configure a maximum of 10,000 |

| | | | routes. | routes. |
|--|-------|---|---|---|
| | | Quantity of equal-cost routes supported by each route | 32 | 32 |
| | | Quantity of routes supporting equal-cost routing | 64 | 64 |
| | | Quantity of weighted next-hop routes supported by each route | 8 (Weight = 4) 4 (Weight = 8) Weight x Route count ≤ 32 | 8 (Weight = 4) 4 (Weight = 8) Weight x Route count ≤ 32 |
| | | Multicast routing table | 16000 | 16000 |
| | IPv6 | Quantity of IPv6 addresses set on each layer-3 interface | 1000 at most | 1000 at most |
| | | Capacity of IPV6 hardware routing table (network routes) (the maximum quantity of routing entries supported by the routing table need to be learned in full mesh mode) | Default mode: 6000 | Default mode: 1000 |
| | | Capacity of routing table supporting the subnet mask length of 65–128 (If no description is made, the capacity is not limited by the subnet mask length and the hardware routing table capacity prevails.) | Default mode: 1000 | Default mode: 4000 |
| | | Capacity of static IPv6 routing table | 1000 | 1000 |
| | | Quantity of IPv6 tunnel interfaces | 127 | 127 |
| | | Multicast routing table | 8000 | 8000 |
| | PBRv4 | Quantity of supported policy-based routes | 1500–7000 | 1500–7000 |

| | | Quantity of equal-cost routes supported by each policy-based route | 32 | 32 |
|-----|--------------|--|--|-----------|
| | | Quantity of supported policy-based routes | 1500–3000 | 1500–3000 |
| | PBR v6 | Quantity of equal-cost routes supported by each policy-based route | es ased 32 32 32 32 32 32 32 32 32 33 32 33 32 33 32 33 32 33 32 33 33 | 32 |
| | ACE capacity | Maximum number of inbound ACE entries associated with the SVI | 7000 | 7000 |
| | | Maximum number of inbound ACE entries associated with the physical port/AP | 7000 | 7000 |
| | | Maximum number of outbound ACE entries associated with the SVI (simulated based on inbound ACE entries, limited, and with inbound entries occupied) | N/A | N/A |
| ACL | | Maximum number of outbound ACE entries associated with the SVI (actual outbound ACE entries) | 1000 | 1000 |
| | | Maximum number of outbound ACE entries associated with the physical port/AP (simulated based on inbound ACE entries) | N/A | N/A |
| | | Maximum number of outbound ACE entries associated with the physical port/AP (actual outbound ACE entries) | 1000 | 1000 |

3 Typical Scenarios

3.1 Access Isolation Scenario

3.1.1 Overall Solution

3.1.1.1 Solution Description

The simplistic network access isolation solution employs one VLAN for each access switch, and allows locating the specific access switch according to the VLAN ID. In addition, this solution provides layer-2 isolation for all users, effectively preventing layer-2 broadcast packet attacks and ARP and DHCP spoofing attacks.

- 1. The core RG-N18000 serves as the gateway and authentication NAS device on the whole network:
- A maximum of 60,000 online dual-stack clients are supported in coordination with ED cards, and a maximum of 30,000 online clients are supported in coordination with DB cards or both of ED and DB cards.
- Web authentication, wired 802.1x authentication, and MAB authentication are simultaneously supported. Wireless 802.1x authentication is not supported currently, because it needs to be deployed on the AC.
- Wireless 802.1x VLANs, AP management VLANs, and other special service VLANs requiring no authentication (such as door status control, all-in-one card, and video monitoring) are configured as authentication-free VLANs.
- As the core layer-2 gateway, the RG-N18000 can support the super VLAN function to perform aggregation gateway configurations for sub VLANs. One super VLAN can be deployed for each area, for example, one super VLAN for the office area of the xx campus and one super VLAN for the student dormitory area of the xx campus.
- The ARP proxy function is enabled on the super VLAN gateway of the core device by default, to guarantee layer-3 communication between sub VLANs and decrease ARP flooding traffic.
- The port protection function needs to be configured on the downlink interface of the core device (by running the switchport protected command), to prevent layer-2 broadcast between the same VLANs in different areas. In addition, unused VLANs need to be pruned to minimize the broadcast domain.
- The SVI of the super VLAN gateway needs to be set to OSPF passive if OSPF is configured.
- 2. The aggregation device serves as layer-2 transparent transmission device:
- The VLAN and trunk interfaces are configured for layer-2 transparent transmission only.
- The SVI of the user gateway needs to be set to OSPF passive if the conventional 3-layer network is deployed and OSPF is configured on the aggregation device.
- The port protection function needs to be configured on the downlink interface of the aggregation device (by running the switchport protected command), to prevent layer-2 broadcast between the same VLANs in different areas. In addition, unused VLANs need to be pruned to minimize the broadcast domain.
- The storm suppression function is configured to suppress broadcast packets at 1000 pps and multicast packets at 1000 pps. In addition, this function needs to be adjusted according to the live network applications. For example, if multicast

services exist on the live network, do not configure multicast packet suppression and suppress broadcast packets at 1000 pps.

- 3. The access device provides user-based layer-2 isolation:
- The same VLAN is configured on all interfaces of each access switch, and different VLANs are configured for different access switches.
- The port protection function needs to be configured on the interfaces of each switch (by running the **switchport protected** command), to implement layer-2 VLAN isolation.
- Different VLANs need to be configured for different access switches, with incremental VLAN IDs.
- VLAN segments need to be independently planned for special services (such as door status control, all-in-on card, and video monitoring) to distinguish from user service VLANs, to facilitate authentication-free VLAN configuration on the core device for special services.
- RDLP is enabled on the interface of the access device connected to the clients, and an anti-loop policy is configured to shut down a port upon a loop.
- The storm suppression function is enabled on the interfaces of the access device connected to the clients, to suppress broadcast packets at 300 pps and multicast packets at 300 pps. In addition, this function needs to be adjusted according to the live network applications. For example, if multicast services exist on the live network, do not configure multicast packet suppression and suppress broadcast packets at 1000 pps.

3.1.1.2 Solution Topology



3.1.1.3 Recommended Scenario

1. In the case of network construction, an access cascading scenario exists in the live network and flexible QinQ is not supported on the aggregation device.

Suggestion for the wired network scenario: It is recommended to deploy access isolation, configure one VLAN for each switch, and configure one super VLAN for each area (such as the office area of the xx campus, library of the xx campus, and student dormitory area of the xx campus).

2. In the case of network reconstruction, it is unclear whether devices are interconnected and whether flexible QinQ is supported.

Suggestion for the wired network scenario: It is recommended to deploy access isolation, configure one VLAN for each switch, and configure one super VLAN for each area (such as the office area of the xx campus, library of the xx campus, and student dormitory area of the xx campus).

3.1.2 VLAN/IP Planning

3.1.2.1 Planning Idea

Configure one VLAN (sub VLAN) for the access switch of each floor, and one super VLAN for each area (such as the student dormitory area of the xx campus).

Reserve VLANs (30% or more) for each area for further network change or expansion.

Reference templates:

Wired network VLAN/IP planning for the student dormitory area:

| Device Model | Device Type | Location | Management Address | Sub VLAN | Super VLAN | Network Segment (planned according to rules, with the actual subnet mask length being /16) | Gateway | Network Management VLAN | Video Monitoring VLAN | All-in-one Card VLAN | Door Status Control VLAN |
|-----------------|---------------------------|---|-----------------------|-------------|---------------|---|------------------|-------------------------------|-----------------------------|----------------------------|-----------------------------------|
| S2928G | Floor access switch | 1/F, building 1, student dormitory area | 192.168.132.1 | 1001 | 4000 | 172.16.0.0/24 | 172.16.15.254/16 | 100 | 101 | 102 | 103 |
| S2928G | Floor access switch | 2/F, building 1, student dormitory area | 192.168.132.2 | 1002 | | | | | | | |
| S2928G | Floor access | 1/F, building 2, student | 192.168.132.3 | 1003 | | 172.16.1.0/24 | 172.16.15.254/16 | | | | |

| S2928G | switch Floor access switch | dormitory area 2/F, building 2, student dormitory area | 192.168.132.4 | 1004 | | | | |
|--------|-------------------------------------|---|----------------|------|---------------|------------------|--|--|
| S2928G | Floor access switch | 1/F, building 3, student dormitory area | 192.168.132.5 | 1005 | 172.16.2.0/24 | 172.16.15.254/16 | | |
| S2928G | Floor access switch | 2/F, building 3, student dormitory area | 192.168.132.6 | 1006 | | | | |
| S2928G | Floor access switch | 1/F, building 4, student dormitory area | 192.168.132.7 | 1007 | 172.16.3.0/24 | 172.16.15.254/16 | | |
| S2928G | Floor access switch | 2/F, building 4, student dormitory area | 192.168.132.8 | 1008 | | | | |
| S2928G | Floor access switch | 1/F, building 5, student dormitory area | 192.168.132.9 | 1009 | 172.16.4.0/24 | 172.16.15.254/16 | | |
| S2928G | Floor access switch | 2/F, building 5, student dormitory area | 192.168.132.10 | 1010 | | | | |
| S2928G | Floor access switch | 1/F, building 6, student dormitory area | 192.168.132.11 | 1011 | 172.16.5.0/24 | 172.16.15.254/16 | | |
| S2928G | Floor access switch | 2/F, building 6, student dormitory area | 192.168.132.12 | 1012 | | | | |
| S2928G | Floor access switch | 1/F, building 7, student dormitory area | 192.168.132.13 | 1013 | 172.16.6.0/24 | 172.16.15.254/16 | | |
| S2928G | Floor access switch | 2/F, building 7, student dormitory area | 192.168.132.14 | 1014 | | | | |

| S2928G | Floor access switch | 1/F, building 8, student dormitory area | 192.168.132.15 | 1015 | 172.16.7.0/24 | 172.16.15.254/16 | | |
|--------|---------------------------|--|----------------|------|----------------|------------------|--|--|
| S2928G | Floor access switch | 2/F, building 8, student dormitory area | 192.168.132.16 | 1016 | | | | |
| S2928G | Floor access switch | 1/F, building 9, student dormitory area | 192.168.132.17 | 1017 | 172.16.8.0/24 | 172.16.15.254/16 | | |
| S2928G | Floor access switch | 2/F, building 9, student dormitory area | 192.168.132.18 | 1018 | | | | |
| S2928G | Floor access switch | 1/F, building 10, student dormitory area | 192.168.132.19 | 1019 | 172.16.9.0/24 | 172.16.15.254/16 | | |
| S2928G | Floor access switch | 2/F, building 10, student dormitory area | 192.168.132.20 | 1020 | | | | |
| S2928G | Floor access switch | 1/F, building 11, student dormitory area | 192.168.132.21 | 1021 | 172.16.10.0/24 | 172.16.15.254/16 | | |
| S2928G | Floor access switch | 2/F, building 11, student dormitory area | 192.168.132.22 | 1022 | | | | |

3.2 Wireless Isolation Scenario

3.2.1 Overall Solution

3.2.1.1 Solution Description

1. The simplistic network wireless isolation solution employs one super VLAN for each area (for example, a super VLAN for the office area of the xx campus), and two sub VLANs for each building in the area (one for wireless Web authentication and the other for wireless 802.1x authentication). This solution helps you locate wireless users to a specific building based on the VLAN, and enables wireless user isolation to prevent layer-2 broadcast packet attacks and ARP and DHCP spoofing attacks.

- 2. This solution also supports super VLANs based on the SSID, for example, one super VLAN separately for 802.1x authenticated student users, 802.1x authenticated teacher users, Web authenticated student users, and Web authenticated teacher users. This solution employs sub VLANs based on the area, building, and floor to control the scope of the broadcast domain.
- 1. The core RG-N18000 serves as the gateway and authentication NAS device on the whole network:
- A maximum of 60,000 online dual-stack clients (a maximum of 90,000 online clients in theory) are supported in coordination with ED cards, and a maximum of 30,000 online clients are supported in coordination with DB cards or both of ED and DB cards.
- Web authentication, wired 802.1x authentication, and MAB authentication are simultaneously supported. Wireless 802.1x authentication is not supported currently, because it needs to be deployed on the AC.
- Wireless 802.1x VLANs and AP management VLANs are configured as authentication-free VLANs.
- As the core layer-2 gateway, the RG-N18000 can support the super VLAN function to perform aggregation gateway configurations for sub VLANs. One super VLAN can be deployed for each area, for example, one super VLAN for the office area of the xx campus and one super VLAN for the student dormitory area of the xx campus.
- The ARP proxy function is enabled on the super VLAN gateway of the core device by default, to guarantee layer-3 communication between sub VLANs and decrease ARP flooding traffic.
- The port isolation function needs to be configured on the downlink interface of the core device, to prevent layer-2 broadcast between the same VLANs in different areas. In addition, unused VLANs need to be pruned to minimize the broadcast domain.
- 2. The AC serves as wireless controller in fit mode to perform the basic wireless configurations and simplistic network planning configurations:
- The basic wireless configuration mode is set to support centralized forwarding or local forwarding.
- Wireless user isolation is configured to prevent an overlarge wireless user broadcast domain in a VLAN.
- The ARP proxy function is disabled on the AC, so that the RG-N18000 serves as the ARP proxy, to prevent failures in migration of wireless authenticated users.
- One super VLAN is configured for each area, for example, one super VLAN for the office area of the xx campus.
- Two sub VLANs are configured for the AP of each building, one for wireless Web authentication and the other for wireless 802.1x authentication.
- SSIDs are set based on the operator and authentication mode, for example, SSID 1 for operator A Web authentication, SSID 2 for operator A - 802.1x authentication, SSID 3 for operator B - Web authentication, and SSID 4 for operator B -802.1x authentication.

3.2.1.2 Solution Topology



Supervlan 4092

 Sub VLAN of building yy in area A for 802.1x authentication

Sub VLAN of building 1 in area B for Web authentication

- Sub VLAN of building 1 in area B for 802.1x authentication
- Sub VLAN of building 2 in area B for Web authentication
- Sub VLAN of building 2 in area B for 802.1x authentication

3.2.1.3 Recommended Scenario

Wireless

campus network

The wireless simplistic network uses the wireless isolation solution.

Wireless

network of area B

3.2.2 VLAN/IP Planning

3.2.2.1 Planning Idea

- Configure one super VLAN for each area, for example, one super VLAN for the office area of the xx campus.
- Configure two sub VLANs for the AP of each building, one for wireless Web authentication and the other for wireless 802.1x authentication.
- Set SSIDs based on the operator and authentication mode, for example, SSID 1 for operator A Web authentication, SSID 2 for operator A - 802.1x authentication, SSID 3 for operator B - Web authentication, and SSID 4 for operator B -802.1x authentication.
- Reserve VLANs (30% or more) for each area for further network change or expansion.

Reference templates:

Wired network VLAN/IP planning for the student dormitory area:

| Location | AP Management | AP | Gateway | Web | 802.1x | Super | Network | Gateway | Web | 802.1x |
|---|------------------|-----------------|----------------|----------|----------|--------|----------------|------------------|----------|-------------|
| | VLAN | Segment | | Sub VLAN | Sub VALN | V LAIN | Segment | | SSID | SSID |
| Building 1, student dormitory area | 900 | 192.168.16.0/20 | 192.168.31.254 | 3001 | 3501 | 4201 | 172.16.64.0/20 | 172.16.79.254/20 | web-auth | 802.1x-auth |
| Building 2, student dormitory area | 900 | 192.168.16.0/20 | 192.168.31.254 | 3002 | 3502 | 4201 | 172.16.64.0/20 | 172.16.79.254/20 | web-auth | 802.1x-auth |
| Building 3, student dormitory area | 900 | 192.168.16.0/20 | 192.168.31.254 | 3003 | 3503 | 4201 | 172.16.64.0/20 | 172.16.79.254/20 | web-auth | 802.1x-auth |
| Building 4, student dormitory area | 900 | 192.168.16.0/20 | 192.168.31.254 | 3004 | 3504 | 4201 | 172.16.64.0/20 | 172.16.79.254/20 | web-auth | 802.1x-auth |
| Building 5, student dormitory | 900 | 192.168.16.0/20 | 192.168.31.254 | 3005 | 3505 | 4201 | 172.16.64.0/20 | 172.16.79.254/20 | web-auth | 802.1x-auth |

| area | | | | | | | | | | |
|---|-----|-----------------|----------------|------|------|------|----------------|------------------|----------|-------------|
| Building 6, student dormitory area | 900 | 192.168.16.0/20 | 192.168.31.254 | 3006 | 3506 | 4201 | 172.16.64.0/20 | 172.16.79.254/20 | web-auth | 802.1x-auth |
| Building 7, student dormitory area | 900 | 192.168.16.0/20 | 192.168.31.254 | 3007 | 3507 | 4201 | 172.16.64.0/20 | 172.16.79.254/20 | web-auth | 802.1x-auth |
| Building 8, student dormitory area | 900 | 192.168.16.0/20 | 192.168.31.254 | 3008 | 3508 | 4201 | 172.16.64.0/20 | 172.16.79.254/20 | web-auth | 802.1x-auth |
| Building 9, student dormitory area | 900 | 192.168.16.0/20 | 192.168.31.254 | 3009 | 3509 | 4201 | 172.16.64.0/20 | 172.16.79.254/20 | web-auth | 802.1x-auth |
| Building 10, student dormitory area | 900 | 192.168.16.0/20 | 192.168.31.254 | 3010 | 3510 | 4201 | 172.16.64.0/20 | 172.16.79.254/20 | web-auth | 802.1x-auth |
| Building 10, student dormitory area | 900 | 192.168.16.0/20 | 192.168.31.254 | 3011 | 3511 | 4201 | 172.16.64.0/20 | 172.16.79.254/20 | web-auth | 802.1x-auth |

4 Configuration of Important Functions

4.1 RG-N18000 Configuration

4.1.1 Common Scenario — Gateway

4.1.1.1 [Mandatory] Gateway Mode

Principles:

In the simplistic network solution, the core device acts as the gateway of the entire network, and controls access authentication. Users can be normally authenticated and go online only after the authentication mode is set to gateway authentication mode and dot1x or Web authentication is enabled.

Otherwise, when the number of 802.1x/Web authenticated users reach about 2000, the system prompts that the TCAM table is full and 802.1x/Web authentication is abnormal.

In comparison to the conventional network, the simplistic network in gateway mode has the following features:

- 1. An authenticated client is automatically bound with a static ARP address on the RG-N18000.
- 2. The RG-N18000 automatically enables the ARP proxy function on the SVI interface of a super VLAN. The ARP proxy can be disabled on a sub VLAN. (Valid to authenticated users)
- The RG-N18000 does not actively send ARP requests to a sub VLAN of a super VLAN configured on an interface with authentication under control. Instead, the RG-N18000 actively sends ARP requests to authentication-free VLANs and common VLANs.
- 4. In gateway mode of the simplistic network, the **ip source-guard** command does not take effect.

Configuration commands:

auth-mode gateway //Configured in global configuration mode.

Precautions:

This command takes effect only after it is configured and saved and the device is restarted. After the device is restarted, run the **show run** command to check whether the configuration takes effect.

Configuration example



| Configuration | Set the authentication mode to the gateway authentication mode on the core gateway Switch A. | | | | | | | | | |
|---------------|--|--|--|--|--|--|--|--|--|--|
| Steps | | | | | | | | | | |
| Switch A | SwitchA(config)#auth-mode gateway | | | | | | | | | |
| | Please save config and reload system. | | | | | | | | | |
| | SwitchA(config) #exit | | | | | | | | | |
| | *Nov 7 10:13:27: %SYS-5-CONFIG_I: Configured from console by console | | | | | | | | | |
| | SwitchA#reload | | | | | | | | | |
| | Reload system?(Y/N)y | | | | | | | | | |
| | SwitchA# | | | | | | | | | |
| Verification | Run the show running command to check whether the configuration takes effect. | | | | | | | | | |
| Switch A | SwitchA(config)#show running-config include auth-mode | | | | | | | | | |
| | auth-mode gateway | | | | | | | | | |
| | SwitchA#debug scc st | | | | | | | | | |
| | ====================================== | | | | | | | | | |
| | rdnd role : 2/2. | | | | | | | | | |
| | ready notify : CLI LSM BRIDGE SS ACLK BRIDGE-READY TCPIP VFW | | | | | | | | | |
| | aclk-socket info: async - 8, sync - 9, alive - 7. snd_cnt:692. rcv_cnt:692 | | | | | | | | | |

```
data sync info : depend/ready(0x201e/0x201e) aclk(reg:0) ss(reg:0) mac(reg:0)
current scc mode: GATE MODE, new mode(GATE MODE).
ability: 0x3f.
offline-status : open, interval:6 min, threshold:0 bytes.
station move
               : close.
dot1x cpp
               : set. author mode:D1xAuthorMixed.
proc status
               : svrid:75 todo-cnt:0 ret-cnt:0.
max wait
               : client:9, cost:16(ms)
max proc
               : client:11, svrid:72, tlvtype:105, ss-cnt:0, aclk-cnt:0 rv:0.
cost:748(ms).
cnt-stat
               : web-guery-add-arp:[0], web-guery-del-arp:[0].
: add-arp:[2], del-arp:[1].
: add-mac:[2], del-mac:[1].
```

4.1.1.2 [Mandatory] super VLAN

Principles:

The super VLAN technology is used to implement flat layer 2 networks for gateways. Super VLAN is also called VLAN aggregation. The aggregated VLAN range is called sub VLAN of the super VLAN. A super VLAN has the following features:

Each sub VLAN has the same functions as common VLANs. Different sub VLANs belong to different broadcast domains, and cannot access each other due to layer-2 isolation.

The SVI address of a super VLAN serves as the gateway address of the sub VLAN of the super VLAN.

When a sub VLAN requires layer-3 communication, the IP address of the virtual interface of the super VLAN is used as the gateway address for addressing and forwarding.

When sub VLANs need to access each other, the ARP proxy and ND proxy of the super VLAN need to be configured.

Note: When super VLANs and sub VLANs are configured in the simplistic network solution, super VLAN IDs are used only on SVIs, while sub VLAN IDs are used for AM rules, QinQ VLAN tag termination, and direct VLANs that need the VLAN ID range.

Configuration commands:

```
vlan (supervlan) //Create a VLAN.
supervlan //Define the VLAN as a super VLAN.
subvlan (subvlan-list) //Define the sub VLAN range for the super VLAN.
name (supervlan-name) //Name the super VLAN.
int vlan (supervlan) //Create the gateway SVI for the super VLAN.
ip address (ip/netmask) //Define the gateway address and mask.
```

Precautions:

An SVI and an IP gateway need to be configured for a super VLAN. Otherwise, communication is not supported between sub VLANs or between sub VLANs and other VLANs.

The ARP proxy is enabled by default. If the ARP proxy is disabled on a super VLAN or sub VLAN, users of sub VLANs cannot perform inter-VLAN communication.

Configuration example



192.168.1.10~192.168.1.50 192.168.1.60~192.168.1.100 192.168.1.110~192.168.1.150

| Configuration | ifiguration Configure a super VLAN on the core switch. (Omitted) | | | | | | | | | |
|---------------|---|--|--|--|--|--|--|--|--|--|
| Steps | On the access switch, configure common VLANs corresponding to sub VLANs of the core switch. | | | | | | | | | |
| Α | SwitchA#configure terminal | | | | | | | | | |
| | Enter configuration commands, one per line. End with CNTL/Z. | | | | | | | | | |
| | SwitchA(config)#vlan 2 | | | | | | | | | |
| | SwitchA(config-vlan)#exit | | | | | | | | | |
| | SwitchA(config)#vlan 10 | | | | | | | | | |
| | SwitchA(config-vlan)#exit | | | | | | | | | |
| | SwitchA(config)#vlan 20 | | | | | | | | | |
| | SwitchA(config-vlan)#exit | | | | | | | | | |
| | SwitchA(config)#vlan 30 | | | | | | | | | |
| | | | | | | | | | | |

| | SwitchA(confi | g-vlan)#exit | | | | | | | | | |
|--------------|--------------------|--|------------------|------------------|------------|----------------------|--|--|--|--|--|
| | SwitchA(confi |)#vlan 2 | | | | | | | | | |
| | SwitchA(confi | (-vlan) #supervlan | | | | | | | | | |
| | SwitchA(confi | -vlan)#subvlan 10,20,30 | | | | | | | | | |
| | SwitchA(confi | g-vlan)#exit | | | | | | | | | |
| | SwitchA(confi | ig)#interface vlan 2 | | | | | | | | | |
| | SwitchA(confi | A(config-if-VLAN 2)#ip address 192.168.1.1 255.255.255.0 | | | | | | | | | |
| | SwitchA(confi | cchA(config)#interface range gigabitEthernet 0/1,0/5,0/9 | | | | | | | | | |
| | SwitchA(confi | g-if-range)#switchport mode trunk | | | | | | | | | |
| | | | | | | | | | | | |
| | | | | | | | | | | | |
| Verification | Check whether th | ne source device (192.168. | 1.10) and the de | estination devic | e (192.168 | .1.60) can ping each | | | | | |
| | other successfully | ully. | | | | | | | | | |
| Α | SwitchA(confi | g-if-range)# show su | pervlan | | | | | | | | |
| | supervlan id | supervlan arp-proxy | subvlan id | subvlan ar | p-proxy | subvlan ip range | | | | | |
| | | | | | | | | | | | |
| | 2 | ON | 10 | ON | 192. | 168.1.10 - | | | | | |
| | 192.168.1.50 | | | | | | | | | | |
| | | | 20 | ON | 192 | .168.1.60 - | | | | | |
| | 192.168.1.100 | | | | | | | | | | |
| | | | 30 | ON | 192 | .168.1.110 - | | | | | |
| | 192.168.1.150 | | | | | | | | | | |
| | | | | | | | | | | | |

4.1.1.3 [Mandatory] Protected Port Isolation

Principles:

The simplistic network solution implements layer-2 user isolation by using protected ports. A protected port can prevent layer-2 forwarding within one VLAN of the same switch. When ports are configured as protected ports, protected ports of the same VLAN cannot communicate with each other but a protected port can normally communicate with a non-protected port.

Configuration

commands:

switchport protected //Configured in interface configuration mode.

Precautions:

N/A

Configuration example

Ruijie(config)#interface GigabitEthernet 0/1 Ruijie(config-if-GigabitEthernet 0/1)# switchport protected

4.1.1.4 [Mandatory] Interface Index Uniqueness

Principles:

The interface index of each port is unique. You can run the **show interface** command to display the **Index** field. After the device restarts, the interface index of the device may change. As a result, the area division function of SAM+ will fail. It is recommended to enable the interface index uniqueness function. After this function is configured, interface indexes are permanently recorded by the device. They do not change even if the device is restarted or a line card is removed and then inserted.

Configuration commands:

Ruijie(config)#snmp-server if-index persist

//Enable interface index uniqueness.

Precautions:

N/A

Configuration example

N/A

4.1.1.5 [Mandatory] Regular User Synchronization

Principles:

Some users on SAM+ may fail to go offline normally due to exceptions. For this, SAM+ automatically checks online users with the NAS at 02:00 A.M. every day, to delete information about fake online users.

Configuration commands:

| snmp-server host | (radius ip) | informs version 2c | (key) | //Configure SNMP f | or communicating |
|------------------|-------------|--------------------|-------|--------------------|------------------|
| with SAM+. | | | | | |

Precautions:

Configure related information on SAM+.

Configuration example

N/A

4.1.2 Common Scenario — Address Management

4.1.2.1 [Mandatory] DHCP Snooping

Principles:

The DHCP snooping feature provides the following functions in simplistic networks:

- A simplistic network adopts the flat layer-2 gateway architecture. DHCP snooping can prevent DHCP spoofing within the same VLAN of the DHCP downlink interface. (In theory, DHCP spoofing does not exist in the simplistic network solution and DHCP snooping mainly provides layer-2 protection. In simplistic networks, port protection needs to be enabled on interfaces of the same VLAN on core devices and access devices, to isolate layer-2 broadcast domains and prevent DHCP spoofing.)
- 2. DHCP snooping provides IP address authorization for 802.1x authentication or MAC Address Bypass (MAB) Authentication by using a DHCP snooping table, provided that the AAA IP authorization function is enabled, the dot1x valid-ip-acct enable and dot1x mac-auth-bypass valid-ip-auth commands are executed, and DHCP is configured to dynamically assign IP addresses to authenticated users.

Configuration commands:

ip dhcp snooping //Mandatory. The command is used for DHCP snooping and IP authorization for 802.1x authentication. ip dhcp snooping check-giaddr //Mandatory. It is configured to prevent the RG-N18000 with DHCP snooping enabled from discarding DHCP relay packets from aggregation devices. ip dhcp snooping arp-detect //Optional. Enable fast ARP address reclaiming of DHCP snooping. The ARP address reclaiming is performed once per second during ARP aging and can be performed five times at most.

interface gi2/3/8 //Optional. It is configured in scenarios in which the DHCP server is not deployed on the RG-N18000 and the DHCP server communicates with the RG-N18000 at layer 2. description link-to-dhcpserver

ip dhcp snooping trust //Configure a DHCP trusted port on the layer-2 port of the interconnected DHCP server.

Precautions:

When the IP DHCP snooping feature is configured, the **ip dhcp snooping check-giaddr** command must be executed, so that the RG-N18000 with DHCP snooping enabled can process DHCP relay packets from aggregation devices. The **ip dhcp snooping check-giaddr** command has no drawbacks. Therefore, it is recommended to enable the command by default.

Configuration example

N/A

4.1.2.2 [Mandatory] Fast Address Reclaiming of DHCP Snooping

Principles:

Fast address reclaiming reclaims addresses of DHCP snooping entries rapidly, to prevent an overlarge DHCP snooping binding table caused by generation of multiple address entries by the same client during wireless user migration.

This function can be associated with the ARP module. When an ARP entry corresponding to an IP address in the DHCP snooping table is about to age, ARP detection is started. If no response is received within the detection count, the DHCP snooping entry of the IP address is deleted.

Configuration

commands:

ip dhcp snooing arp-detect //Optional. Enable fast ARP address reclaiming of DHCP snooping. The ARP address reclaiming is performed once per second during ARP aging and can be performed five times at most.

Precautions:

N/A

Configuration example

N/A

4.1.2.3 [Optional] DHCP Server

Principles:

Principles of a DHCP server in a simplistic network scenario are similar to those in a universal scenario. Identical parts of the principles are not described here.

Differences are as follows:

- 1. The recommended DHCP lease time is 2 hours. The purpose is to rapidly reclaim DHCP address resources that are not in use, to prevent IP address resources of the gateway from being fully occupied in areas with heavy traffic.
- 2. When the DHCP lease period of the client expires or the RG-N18000 receives a DHCP release packet, the RG-N18000 kicks the client offline during authentication.

This prevents a problem that, when the DHCP server assigns the IP address originally obtained by the client to a new client, the IP address is still corresponding to the original client in the authentication entry and stays in the online state, and the new client cannot be authenticated.

Configuration commands:

| DSW-18KX_LX(config)#ip dhcp pool 4000 | //Set the DHCP address pool for the wired | | | | | | | |
|---|---|--|--|--|--|--|--|--|
| network in the dormitory area. | | | | | | | | |
| DSW-18KX_LX(dhcp-config)#lease 0 2 0 | //Mandatory. Set the lease time to 2 hours. | | | | | | | |
| DSW-18KX_LX(dhcp-config)#network 172.16.0.0 255.255.240.0 | | | | | | | | |
| DSW-18KX LX(dhcp-config)#dns-server 202.115.32.39 202.115.32.36 | | | | | | | | |

DSW-18KX_LX(dhcp-config)#default-router 172.16.15.254

Precautions:

It is recommended to set the DHCP server lease period to 2 hours.

When the DHCP lease period of the client expires or the RG-N18000 receives a DHCP release packet, the RG-N18000 kicks the client offline during authentication.

It is recommended to set the period for no-traffic go-offline detection to be shorter than the lease period of DHCP server.

Configuration example

N/A

4.1.2.4 [Optional] Fast Address Reclaiming of DHCP Server

Principles:

Fast address reclaiming is configured to enable the DHCP server to detect whether a user is offline. If a user goes offline and does not go online again within a period of time, the DHCP server reclaims the IP address assigned to the user.

The principles are described as follows: The DHCP server, based on IP addresses in the DHCP server table, conducts keepalive detection via the ARP module. If identifying that a user goes offline and does not go online again within a period of time (5 minutes by default), the DHCP server reclaims the IP address assigned to the user.

If the DHCP server function is configured on the RG-N18000, the fast address reclaiming function is mandatory.

Configuration commands:

ip dhcp server arp-detect //Enable fast address reclaiming of the DHCP server. If identifying that a user goes offline and does not go online again within a period of time (5 minutes by default), the DHCP server reclaims the IP address assigned to the user.

Precautions:

N/A

Configuration example

N/A

4.1.2.5 [Optional] AM Rules

Principles:

AM rules can be used to divide the DHCP address segment based on the VLAN+port of the RG-N18000, but the DHCP address segment must exist in the DHCP address pool. The address segment assigned by using AM rules must be smaller than or equal to the DHCP address pool. Example:

DHCP address pool: network 192.168.0.0 255.255.0.0

AM rule: match ip 192.168.1.0 255.255.255.0 Gi5/3 vlan 1005

In the simplistic network environment, the gateway is deployed via super VLAN. Generally, the gateway is deployed in the following manners:

Scenario 1 (AM rules not required): Sub VLAN of each dormitory building or sub VLANs of some dormitory buildings form one super VLAN. The network segment corresponding to the gateway of the super VLAN is small (for example, several type C addresses). Each super VLAN is corresponding to one DHCP address pool. The network segments corresponding to the IP addresses obtained by students are refined and easily managed.

Scenario 2 (AM rules not required): Sub VLANs of the entire campus network form one super VLAN. The network segment corresponding to the gateway of the super VLAN is relatively large (for example, several type B addresses). Each super VLAN is corresponding to one DHCP address pool. The network segments corresponding to the IP addresses obtained by students are scattered and disordered and hard to manage. The school does not raise a requirement on provision of different policies on SAM+ or egress based on source IP addresses, for example, Internet access area control and PBR.

Scenario 3 (AM rules required): Sub VLANs of the entire campus network form one super VLAN. The network segment corresponding to the gateway of the super VLAN is relatively large (for example, several type B addresses). Each super VLAN is corresponding to one DHCP address pool. The network segments corresponding to the IP addresses obtained by students are scattered and disordered and hard to manage. The school requires refined management, and requires precise identification on user areas based on IP addresses, to implement requirements, for example, Internet access area control and PBR.

Scenario 4 (AM rules required): sub VLANs of the entire campus network form one super VLAN, and multiple secondary addresses are configured for the gateway of the super VLAN. In this scenario, AM rules must be configured. Otherwise, DHCP addresses cannot be assigned according to secondary addresses. (By default, the DHCP software assigns only the network segment to which the main gateway address belongs.)

Note 1: AM rules support the DHCP server and DHCP relay modes. In DHCP relay mode, the AM rules can be used only in scenario 4. The gateway has multiple secondary addresses. The AM rules are used to notify the DHCP server of the address segment to be used. In this scenario, the DHCP server must configure an address pool for each secondary address of the RG-N18000. Otherwise, the AM rules do not take effect. Example:

```
Configuration of the RG-N18000: ip helper-address 1.1.1.1 (Configure the DHCP relay on the RG-N18000.)
int vlan 4000
ip add 192.168.1.1 255.255.255.0
```

ip add 192.168.2.1 255.255.255.0 secondary

ip add 192.168.3.1 255.255.255.0 secondary

AM rules: address-manage

match ip 192.168.1.0 255.255.255.0 Gi5/3 vlan 1005
match ip 192.168.2.0 255.255.255.0 Gi5/3 vlan 1006
match ip 192.168.3.0 255.255.255.0 Gi5/3 vlan 1007

DHCP server: network 192.168.1.0 255.255.255.0 //Multiple small address pools are configured. The network segment of each address pool is corresponding to the gateway address of one super VLAN. network 192.168.2.0 255.255.255.0 network 192.168.3.0 255.255.255.0

Note 2:

1. AM rules are in strict mode by default when enabled. AM rules are described as follows:

After an AM rule is created, when a client requests an IP address via the RG-N18000, the client whose DHCP packets do not match the AM rule will not be assigned an IP address. Pay attention to this case during network reconstruction.

When Internet access packets from a client having a static IP address pass through the RG-N18000, if the static IP address does not match the created AM rule, the packets are allowed to pass. When the static IP address matches the AM rule but does not match the specified network segment, the client will fail the authentication and the Internet access will be rejected.

If a network segment is divided into excessively small network segments according to the created AM rule in wireless scenarios, IP addresses may not match the AM rule after wireless migration, and packets are discarded, causing migration failures. For example, the IP address segment for wireless super VLAN 3000 is 172.18.0.0/16. Two AM rules are configured: 172.18.1.0/24 for sub VLAN 2001, and 172.18.2.0/24 for sub VLAN 2002. When a client obtains an IP address in sub VLAN 2001 and then is migrated to sub VLAN 2002, because the original IP address does not match the AM rule of sub VLAN 2002, the client needs to obtain a new IP address and be authenticated before it can access the network.

2. (Optional) AM rules can be configured in loose mode, and are described as follows (recommended):

For DHCP packets matching an AM rule, IP addresses in an address segment configured in the AM rule are assigned to clients. DHCP packets that match no AM rule can apply for addresses according to the conventional logic of the DHCP address pool. The DHCP packets are not discarded.

Packets from static IP addresses are not discarded.

Packets from user IP addresses that do not match the AM rules are not discarded during wireless migration.

Note 3: The AM rule matching sequence is as follows:

More detailed AM rules are preferential for matching. In code implementation, AM rules containing the port parameters are matched with a higher priority. For example:

address-manage match ip 192.168.1.0 255.255.255.0 vlan 400 match ip 192.168.2.0 255.255.255.0 Gi1/3 vlan 400(preferential for matching)

Configuration

commands:

AM rules support VLAN-based and VLAN+port-based IP address assignment.

address-manage//Enable the address management function.

match ip 10.1.5.0 255.255.255.0 gi5/3 vlan 1005//Configure VLAN+port-based IP address assignment. match ip 10.1.6.0 255.255.255.0 vlan 1006//Configure VLAN-based IP address assignment. match ip default 172.16.128.0 255.255.128.0//Assign IP addresses from the default address segment to clients that do not match the AM rule. match ip loose//Configure the loose mode for the AM rule (recommended). For details, see the above-mentioned Note 2 .

address-manage //Enable address management. clear match ip//Access the address management configuration mode to disable AM rules globally.

Precautions:

When both the DHCP relay and AM rules are enabled, multiple small address pools must be configured on the DHCP server.

The strict mode is adopted by default after AM rules are enabled on the RG-N18000. In this mode, no IP address is assigned to areas that do not match AM rules in the live network. Pay attention to this case during network reconstruction. It is recommended to configure the loose mode for AM rules.

VLANs configured in AM rules map to outer sub VLANs in QinQ solutions and map to sub VLANs in access isolation solutions.

Configuration example

N/A

4.1.2.6 [Optional] Stateless IPv6 Address Acquisition

Scenario

The stateless IPv6 address acquisition is mainly applied on the layer-3 switch serving as the LAN user gateway. It is used when the IPv4/IPv6 dual-stack service needs to be enabled and users of downlink hosts need to access IPv6 resources. An IPv6 address contains up to 128 bits, and therefore the configuration is complex, and errors are prone to occur. It is expected that hosts can obtain IPv6 prefixes and gateway information without configuration, and IPv6 plug-and-play can be implemented. In this case, the stateless IPv6 address assignment function can be enabled on the user gateway, to assign IPv6 address prefixes and gateway information to downlink hosts.

In another case, a DHCPv6 server is deployed in a network, and IPv6 addresses and parameter information are assigned to downlink hosts in stateful mode. However, DHCPv6 is incapable of assigning gateway address information, lifetime, and other parameters. Therefore, the stateless IPv6 address assignment function needs to be enabled on the switch.

Currently, IPv6 addresses are mainly applied to campus networks on a large scale, and are seldom used in other sectors.

Description

An IPv6 address consists of a prefix and a 64-bit interface ID that is automatically generated from a 48-bit MAC address and is usually called EUI-64 address.

The prefix of an IPv6 address identifies the network between a host and a router. The prefix required by a host is actually the gateway prefix. A protocol can be run between the gateway switch and a host to automatically obtain the prefix. The Router

Solicitation and Router Advertisement (RA) of the Neighbor Discovery Protocol (NDP) can be used, where the former is used to discover a gateway and urge the gateway to send the RA containing the prefix to the host.

The RA contains the prefix, lifetime, default gateway, and other information. It cannot deliver the IPv6 address of the DNS server.

The RA function is disabled by default. You can run the **no ipv6 nd suppress-ra** command in interface configuration mode to enable it.

Network requirements

A customer requests that IPv6 prefixes be obtained in stateless mode and interface addresses be obtained according to the EUI-64, to form IPv6 addresses.

Obtaining IPv6 addresses in stateless mode can be easily configured.

The IPv6 protocol stack is enabled on Windows 7 clients by default. For Windows XP clients, run the **IPv6 install** command in the **Run** window to enable the IPv6 protocol and restart the clients.

Network topology



U Configuration key points

- 1. Configure an IPv6 address on the core switch.
- 2. Enable the RA and O-bit flag on the user gateway.
- 3. Configure a DHCPv6 server and call it in interface configuration mode.

U Configuration steps

1. Configure an IPv6 address for an interface and enable IPv6 on the interface.

```
Ruijie#conf t
Ruijie(config)#interface gigabitEthernet 1/1
Ruijie(config-if-GigabitEthernet 1/1)#no switchport
Ruijie(config-if-GigabitEthernet 1/1)#ipv6 enable
Ruijie(config-if-GigabitEthernet 1/1)#ipv6 address
2001:250:2003:2000::1/64 ----->Configure an IPv6 address for the interface.
```

2. Enable the RA function on the interface, set the O-bit flag to enable the host to obtain DNS, domain name, and other information, and call the address pool.

Ruijie(config-if-GigabitEthernet 1/1) #no ipv6 nd suppress-ra ----->Enable the RA function.

Ruijie(config-if-GigabitEthernet 1/1)#ipv6 nd other-config-flag ----->Set the O-bit flag to enable the host to obtain other information. Ruijie(config-if-GigabitEthernet 1/1)# ipv6 dhcp pool ruijie ---->Call the address pool in interface configuration mode.

3. Configure an IPv6 server, including the domain name, prefix, and DNS server.

```
Ruijie(config)#ipv6 dhcp pool ruijie ---->Create an IPv6 address pool.
Ruijie(dhcp-config)#domain-name www.example.com.cn ---->Configure the domain name to be
assigned to the client.
Ruijie(dhcp-config)#dns-server 2003::1 ---->Configure the DNS server to be
assigned to the client.
Ruijie(dhcp-config)#exit
```

Verification

Check the IPv6 address obtained by a client.

| ļ | 以太网适配器 local | - | | | | | | | | | |
|---|---------------|--------------|---|---|---|---|---|---|---|---|--|
| | 连接特定的 DNS / | 后缀 | | | | | | | | : | |
| | IPv6 地址 | | | | | | | | | Ξ | 2001:250:2003:2000:54b3:e737:71fc:4da3 |
| | 临时 IPv6 地址. | . | | | | | | | | = | 2001:250:2003:2000:6593:b6f4:9367:d1be |
| | ─ 本地链接 IPv6 地 | 1.11- | - | - | - | - | - | - | - | = | fe80::54b3:e737:71fc:4da3%12 |
| | IPv4 地址 | | | | | | | | | : | 192.167.70.92 |
| | - 子网掩码 | | - | - | - | - | - | - | - | = | 255.255.128.0 |
| ł | 默认网关 | | | | | | | | | = | fe80::5a69:6cff:fea2:9eca%12 |
| | | | | | | | | | | | 192.167.127.254 |
| | | | | | | | | | | | |

Note: In the figure above, another IPv6 address is a temporary address automatically generated by the system. The interface address of the temporary address is randomly generated.

The probability of reconnecting to the local address by using the randomly derivative interface ID is very low. Therefore, clients running Windows Vista or Windows Server 2008 can send router requests by using the derivative local address, without waiting for completion of the Duplicate Address Detection (DAD). This is called optimistic DAD. The router discovery and DAD are performed simultaneously, which reduces time required for the interface initialization process. In the generation of this temporary address, however, data packets are sent to the network, which occupies network resources, affects the network health, and hinders IPv6 user uniqueness control. Therefore, it is recommended to disable this function. To do so, click **Start > Run**. In the **Run** window, enter **netsh**, **int ipv6** and **set privacy state=disable** in sequence, as shown in the figure below.



For more information about temporary addresses, see http://technet.microsoft.com/zh-cn/magazine/2007.08.cableguy.aspx.

4.1.2.7 [Optional] Stateful IPv6 Address Automatic Acquisition

Network requirements

A switch is used as a DHCPv6 client, to obtain an IPv6 address from the DHCPv6 server, as well as the DNS server address, domain name, and other network parameters.

Note: If a PC expects to obtain a dynamic IPv6 address, the host must has a DHCPv6 client.

Windows 7, Windows Vista, and Windows Server 2008 each have a built-in DHCPv6 client.

Windows XP and Windows Server 2003 have no built-in DHCPv6 client. Users need to install the DHCPv6 client or enable the IPv6 protocol stack.

Network topology



Configuration key points

- 1. Configure the RG-N18000 switch as the DHCPv6 server and set its address to 2001::1/64.
- 2. Enable the DHCPv6 server to assign 2001::X/64 to the DHCPv6 client.
- 3. Set the address of the DNS server to 2003::1/64.
- 4. The domain name of the DHCPv6 client is <u>www.example.com.cn</u>.

Configuration steps

DHCPv6 server configuration:

1. Enable the IPv6 routing function.

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#ipv6 unicast-routing---->Enable the IPv6 routing function.
Ruijie(config)#end
```

2. Configure an IPv6 address for an interface and enable the IPv6 function on the interface.

```
Ruijie#conf t
Ruijie(config)#
Ruijie(config)#interface gigabitEthernet 1/24
Ruijie(config-if-GigabitEthernet 1/24)#no switchport
Ruijie(config-if-GigabitEthernet 1/24)#ipv6 address 2001::1/64 ----->Configure an IPv6
address for the interface.
Ruijie(config-if-GigabitEthernet 1/24)#ipv6 enable ----->Enable the IPv6 function
on the interface.
Ruijie(config-if-GigabitEthernet 1/24)#end
```

3. Enable the RA function and set the M-bit flag and O-bit flag.

- a. The DHCPv6 server does not assign a gateway address to the client. The RA function needs to be enabled on the device.
- b. Set the **managed address configuration** flag bit in the RA packet to 1. This flag bit determines whether the host receiving the RA packet uses the stateful automatic configuration to obtain an IP address. By default, the flag bit is not set to 1 in the RA packet.
- c. Set the **other stateful configuration** flag bit in the RA packet. This flag bit determines whether the host receiving the RA packet uses the stateful automatic configuration to obtain information other than addresses. By default, the flag bit is not set to 1 in the RA packet.

Ruijie>enable

Ruijie#configure terminal

Ruijie(config)#interface gigabitEthernet 1/24

Ruijie(config-if-GigabitEthernet 1/24) #no ipv6 nd suppress-ra ---->Enable the RA function. Ruijie(config-if-GigabitEthernet 1/24) #ipv6 nd managed-config-flag---->Set the M-bit flag of the RA.

Ruijie(config-if-GigabitEthernet 1/24)#ipv6 nd other-config-flag---->Set the O-bit flag of the RA.

Ruijie(config-if-GigabitEthernet 1/24)#ipv6 nd prefix 2001::/64 no-autoconfig ---->Specify that the RA prefix cannot be used for stateless automatic configuration. Ruijie(config-if-GigabitEthernet 1/24)#end

4. Configure an IPv6 server, including the domain name, prefix, and DNS server.

```
Ruijie(config)#ipv6 dhcp pool ruijie ----->Create an IPv6 address pool.
Ruijie(dhcp-config)#domain-namewww.example.com.cn ---->Configure the domain name to be
assigned to the client.
Ruijie(dhcp-config)#dns-server 2003::1 ---->Configure the DNS server to be
assigned to the client.
Ruijie(dhcp-config)#iana-address prefix 2001::/64 ---->Apply the IPv6 prefix pool.
Ruijie(dhcp-config)#exit
```

5. Enable the DHCPv6 server function on the interface.

Ruijie(config)#interface gigabitEthernet 1/24 Ruijie(config-if-GigabitEthernet 1/24)#ipv6 dhcp server ruijie ---->Enable the IPv6 function on the interface. Ruijie(config-if-GigabitEthernet 1/24)#end

Verification

1. Check information about the address pool of the DHCPv6 server.

```
Ruijie #show ipv6 dhcp pool
DHCPv6 pool: ruijie
IANA address range: 2001::1/64 -> 2001::FFFF:FFFF:FFFF:FFFF/64
preferred lifetime 3600, valid lifetime 3600
DNS server: 2003::1
Domain name: www.example.com.cn
```

Information about the address pool of the DHCPv6 server shows the name of the DHCPv6 address pool, name of the prefix pool, DNS, and domain name.

2. Check the binding table on the DHCPv6 server.

```
Ruijie #sho ipv6 dhcp binding
Client DUID: 00:03:00:01:00:1a:a9:15:46:e2
IANA: iaid 100001, T1 1800, T2 2880
Address: 2001::2
preferred lifetime 3600, valid lifetime 3600
expires at Aug 25 2014 16:35 (3571 seconds)
The binding table shows the client DUID and prefix.
```

The sinding caste showe one errone sets and profi

3. Check information obtained from the DHCPv6 server.

```
Ruijie #show ipv6 dhcp interface gigabitEthernet 5/1
GigabitEthernet 5/1 is in client mode
State is IDLE
next packet will be send in : 1744 seconds
List of known servers:
DUID: 00:03:00:01:14:14:4b:1b:54:6c
Reachable via address: FE80::1614:4BFF:FE1B:546D
```

```
Preference: 0

Configuration parameters:

IA NA: IA ID 0x186a1, T1 1800, T2 2880

Address: 2001::2

preferred lifetime 3600, valid lifetime 3600

expires at Jan 1 1970 7:38 (3544 seconds)

DNS server: 2003::1

Domain name: <u>www.example.com.cn</u>

Rapid-Commit: disable
```

4. Check the status of the IP address obtained by the interface.

```
Ruijie #show ipv6 int g5/1
interface GigabitEthernet 5/1 is Up, ifindex: 1
  address(es):
   Mac Address: 00:1a:a9:15:46:e3
    INET6: FE80::21A:A9FF:FE15:46E3, subnet is FE80::/64
    INET6: 2001::2 [ DEPRECATED ], subnet is 2001::/64
     valid lifetime 3526 sec
 Joined group address(es):
   FF01::1
   FF02::1
   FF02::2
   FF02::1:FF00:2
   FF02::1:FF15:46E3
 MTU is 1500 bytes
 ICMP error messages limited to one every 100 milliseconds
 ICMP redirects are enabled
 ND DAD is enabled, number of DAD attempts: 1
 ND reachable time is 30000 milliseconds
 ND advertised reachable time is 0 milliseconds
 ND retransmit interval is 1000 milliseconds
 ND advertised retransmit interval is 0 milliseconds
 ND router advertisements are sent every 200 seconds<160--240>
 ND router advertisements live for 1800 seconds
```

4.1.2.8 [Optional] DHCPv6 Relay

Scenario

A dedicated DHCPv6 server running Windows 2003 or 2008 is deployed in the network center to assign IPv6 address prefixes and network parameters to hosts in the campus network, to implement centralized management and maintenance. The DHCP relay function needs to be enabled on all IPv4/v6 dual-stack layer-3 switches, to forward packets between

DHCPv6 clients and the DHCPv6 server. In this way, DHCPv6 clients can obtain IPv6 addresses and configuration parameters even if the DHCPv6 clients and the DHCPv6 server are not connected through local links.

In another case, a DHCPv6 server is deployed in the network, and IPv6 addresses and parameter information are assigned to clients in stateful mode. However, DHCPv6 is incapable of assigning gateway information, lifetime, and other parameters. Therefore, the stateless IPv6 address assignment function needs to be enabled on the switch, so that hosts can obtain gateway information.

Description

The DHCPv6 application model consists of the server, client, and relay. The client and server obtain configuration parameters in request-response mode. The relay can transparently bridge clients and the server that are not connected through local links. The packet interaction and parameter maintenance of DHCPv6 are basically the same as those of DHCPv4, but DHCPv6 adjusts the packet structure and processing based on new networks.

Network requirements

User PCs are used as DHCPv6 clients to obtain IPv6 addresses from the DHCPv6 server running Windows 2008. After IPv6 addresses are obtained, the PCs can ping the DHCPv6 server successfully. The RG-N18000 serves as the DHCPv6 relay.



Network topology

U Configuration key points

Complete the following configuration on the DHCPv6 server:

- 1. Configure an IPv6 address and gateway for the DHCPv6 server.
- 2. Configure scope information.
- 3. Configure log information.
- 4. Enable the IPv6 routing function on the DHCPv6 relay, create an IPv6 address, and configure the DHCPv6 relay.

****Configuration steps

DHCP agent configuration:
1. Enable the IPv6 routing function.

```
Ruijie>enable
Ruijie#configure terminal
Ruijie(config)#ipv6 unicast-routing ---->Enable the IPv6 routing function.
Ruijie(config)#end
```

2. Configure an IPv6 address for an interface of the DHCPv6 server and enable the IPv6 function on the interface.

```
Ruijie(config)#int g0/13
Ruijie(config-if-GigabitEthernet 0/13)#no switchport
Ruijie(config-if-GigabitEthernet 0/13)#ipv6 enable ----->Enable the IPv6 function
on the interface.
Ruijie(config-if-GigabitEthernet 0/13)#ipv6 address 2001::2/64 ----->Configure an IPv6
address for the interface.
Ruijie(config-if-GigabitEthernet 0/13)#end
```

3. Create a VLAN for the DHCPv6 client and configure the VLAN on an interface.

```
Ruijie(config)#vlan 2
Ruijie(config-vlan)#exit
Ruijie(config)#int g0/14
Ruijie(config-if-GigabitEthernet 0/14)#switchport mode access
Ruijie(config-if-GigabitEthernet 0/14)#switchport access vlan 2
Ruijie(config-if-GigabitEthernet 0/14)#end
Ruijie#
```

4. Configure the gateway IPv6 address for the DHCPv6 client and enable the DHCPv6 relay function.

```
Ruijie#conf t
Ruijie(config)#interface vlan 2
Ruijie(config-if-VLAN 2)# ipv6 address 2001:1::1/64
Ruijie(config-if-VLAN 2)# ipv6 enable
Ruijie(config-if-VLAN 2)#ipv6 nd prefix 2001:1::/64 no-autoconfig ----->Specify that the RA
prefix cannot be used for stateless automatic configuration.
```

Ruijie(config-if-VLAN 2)# ipv6 dhcp relay destination 2001::1 ---->Configure the DHCPv6 relay and set its next hop to the interface of the server that is connected to the RG-N18000. Ruijie(config-if-VLAN 2)# no ipv6 nd suppress-ra ---->Enable the RA function. Ruijie(config-if-VLAN 2)# ipv6 nd managed-config-flag ---->Set the M-bit flag of the RA. Ruijie(config-if-VLAN 2)# ipv6 nd other-config-flag ---->Set the O-bit flag of the RA. Ruijie(config-if-VLAN 2)# end

Enabling the RA function and setting the M-bit flag and O-bit flag:

a. The DHCPv6 server does not assign a gateway address to the client. The RA function needs to be enabled on the device.

- b. Set the **managed address configuration** flag bit in the RA packet to 1. This flag bit determines whether the host receiving the RA packet uses the stateful automatic configuration to obtain an IP address. By default, the flag bit is not set to 1 in the RA packet.
- c. Set the **other stateful configuration** flag bit in the RA packet. This flag bit determines whether the host receiving the RA packet uses the stateful automatic configuration to obtain information other than addresses. By default, the flag bit is not set to 1 in the RA packet.

4.1.3 Common Scenario — Authentication-free Access

4.1.3.1 [Optional] Authentication-free VLAN

Principles:

Authentication-free VLANs enable users in the specified VLANs to access the Internet without authentication.

The number of authentication-free VLANs is limited. Pay attention to the limit.

The number of authentication-free VLANs cannot exceed 100 in consideration that performance resources are greatly exhausted due to broadcast packet duplication in sub VLANs or in PE-CE VLANs. Countermeasures need to be taken to prevent the RG-N18000 from sending excessive ARP requests, which affects the CPU usage of the device and causes protocol flapping (such as OSPF flapping), packet loss, and network interruption at a high probability. When the number of authentication-free VLANs cannot meet service requirements, security channels are recommended. In a simplistic network, the ARP proxy function is enabled on the RG-N18000 serving as the network-wide gateway by default. Once ARP request scanning attacks occur, the RG-N18000 acts a proxy to flood ARP packets to authentication-free VLANs, resulting in great overhead in the CPU of the RG-N18000.

In a simplistic network, the following VLANs are usually configured as authentication-free VLANs (for reference only):

- 1. Special service VLANs (such as VLANs for all-in-one cards, video monitoring, and door status control systems, server VLANs, and other non-user VLANs)
- 2. NMS VLANs (switch NMS VLANs and wireless NMS VLANs)
- 3. VLANs corresponding to AC 802.1x authentication. Wireless 802.1x authentication must be carried out on the AC, and authentication exemption is required to avoid re-authentication.
- 4. Privilege user VLANs (such as VLANs for school principals and other directors).

If dumb clients (which do not actively send ARP packets) exist on the network, such as printers of some types and door status control systems, only authentication-free VLANs can be used to exempt authentication. This is because the RG-N18000 does not actively send ARP request packets to sub VLANs and therefore cannot learn the ARP information of the dumb clients.

Configuration

commands:

direct-vlan 400, 600, 800-820 //Configure VLANs 400, 600, and 800-820 as authentication-free VLANs. Users in these VLANs can access the network without authentication.

Note: The VLAN IDs used in the direct-vlan command are IDs of sub VLANs.

Precautions:

Authentication-free VLANs are exempted only from checks related to access authentication, but still need to undergo checks specified in security ACLs. If a specific user or VLAN is disallowed in a security ACL, the specific user or users in the specific VLAN cannot access the network. For users in authentication-free VLANs to access the network without authentication, ensure that the VLANs or users in the VLANs are not blocked by ACLs.

The number of authentication-free VLANs cannot exceed 100. Otherwise, the ARP proxy function may enable the RG-N18000 to send excessive ARP packets, resulting in CPU overload of the RG-N18000.

Configuration example

N/A

4.1.3.2 [Optional] Authentication-free sites

Principles:

Before users are authenticated, provide some site resources for users to log in or download data. This is called destination IP-based authentication exemption. In the simplistic network solution, this feature can be usually applied to:

1. Download the SU client and exempt the download server from authentication.

2. Provide public authentication-free resources in a campus network.

3. Allow unauthenticated users to access the portal server and enable the portal server to direct to the authentication page. (In the current version, users can directly access the portal server without authentication after the Web authentication template is configured.)

Configuration commands:

http redirect direct-site x.x.x.x [Mask is optionally configured.] //Configured in global configuration mode. The server with the address x.x.x.x. is configured as an authentication-free site.

Precautions:

A maximum of 50 authentication-free site entries can be configured.

Configuration example

N/A

4.1.3.3 [Optional] Source IP-based authentication exemption

Principles:

Authentication-free source IP addresses can be configured, so that users with the specified source IP addresses can access the Internet without authentication.

The application scenario is similar to that of authentication-free VLANs. The difference lies in that authentication is exempted based on different dimensions, and can be performed as required.

Configuration

commands:

web-auth direct-host x.x.x.x [The mask is optional.] //Configured in global configuration mode. The source IP address of x.x.x.x. is used as an authentication-free site.

Precautions:

A maximum of 1000 authentication-free entries can be configured (the total maximum number of entries that can be configured for both authentication-free source addresses and security channels is 1000).

Configuration example

N/A

4.1.3.4 [Optional] Security channels

Principles:

- 1. The security channel can invoke ACLs and is configured globally or based on ports, enabling ACL-based authentication exemption. ACLs support flexible ACEs. Therefore, the security channel can be used to accurately control authentication-free user groups by allowing packets with the specified source/destination MAC address, source/destination IP address, or the protocol ID above layer 4 without authentication. The security channel further avoids excessive CPU usage caused by ARP packets as in the authentication-free VLAN feature, and therefore is recommended.
- 2. The security channel must be configured on an interface or globally. If it is configured on both the interface and globally, the priority sequence is as follows: interface > global.
- 3. An excluded interface of the security channel is optional. After an excluded interface is configured, the global security channel is invalid to this excluded interface.
- 5. The maximum number of entries that can be configured is 1000 for ED and EF cards and 100 for DB cards (the total maximum number of entries that can be configured for both authentication-free source addresses and security channels is 1000). If the ED and DB cards are both used, the entry capacity may be reduced to 100.

Configuration commands:

ACL-related configuration is omitted here.

| security global access-group | {acl-id | acl-name } | //Apply a security channel in global |
|------------------------------|---------|------------|--------------------------------------|
| configuration mode. | | | |

```
security access-group {acl-id | acl-name } //Apply a security channel in
interface configuration mode.
security uplink enable//Configure a security channel excluded port in interface configuration
mode. The global security channel does not take effect on this interface.
```

Precautions:

An ACL uses the permit statement to set the authentication-free entry, and uses the deny statement to block an entry.

If the security channel is configured on both an interface and globally, the priority sequence is as follows: interface > global.

In an environment with only 802.1x authentication, this command is required to allow critical protocol packets such as ARP and DHCP packets.

Ruijie(config)# expert access-list extended 2700 Ruijie(config-exp-nacl)#10 permit arp any any any any any Ruijie(config-exp-nacl)#20 permit udp any any any any eq bootpc Ruijie(config-exp-nacl)#30 permit udp any any any any eq bootps Ruijie(config)# security global access-group 2700

Configuration example

Scenario



Gateway: 11.1.1.1/24

Configuration Steps:

Configure an Expert extended ACL named exp_ext_esc.

Add an ACE to the ACL to allow the destination host 10.1.1.2.

Add an ACE to the ACL to allow DHCP packets.

Add an ACE to the ACL to allow ARP packets.

On the interface of the 802.1x authentication controlled area, configure the ACL exp_ext_esc as a security channel.

Run the following commands on SW1:

```
swl(config)#expert access-list extended exp_ext_esc
swl(config-exp-nacl)# permit ip any any host 10.1.1.2 any
swl(config-exp-nacl)# permit 0x0806 any any any any any
swl(config-exp-nacl)# permit udp any any any any eq 67
swl(config-exp-nacl)# permit udp any any any any eq 68
swl(config)#int gigabitEthernet 0/1
swl(config-if-GigabitEthernet 0/1)# security access-group exp ext esc
```

Verification:

On a client of the Sales Department, ping the server of the Sales Department and check whether the ping operation is successful.

On clients of R&D Department 1 and R&D Department 2, ping the server of the Sales Department and check whether the ping operations are successful.

```
swl#show access-lists
expert access-list extended exp_ext_esc
10 permit ip any any host 10.1.1.2 any
20 permit arp any any any any any any
30 permit tcp any any any any eq 67
40 permit tcp any any any any eq 68.....
swl#show running-config interface gigabitEthernet 0/1
Building configuration...
Current configuration : 59 bytes
interface GigabitEthernet 0/1
security access-group exp_ext_esc
```

4.1.3.5 [Optional] Free-DNS (Fee Evasion Prevention)

Principles:

After control of Web authentication and 802.1x authentication is enabled on interfaces of the RG-N18000, all DNS packets are allowed to pass before user authentication by default (Web authentication allows DNS packets as specified in the protocol while 802.1x authentication allows DNS packets by using secure channels). Based on the vulnerability of allowing DNS packets prior to authentication, the fee evasion software in the market encapsulates all packets into DNS packets, to

implement Internet access without paying fees. The free-DNS mode can be configured to select DNS packets that are allowed to pass prior to authentication, so as to prevent user fee evasion.

Configuration commands:

1. Configure the free-DNS mode.

free-dns ip-address ip-mask

- 2. Delete the free-DNS mode.
- no free-dns ip-address ip-mask

3. Precautions:

Free-DNS is valid only before user authentication. All DNS packets are allowed to pass after user authentication.

4. Configuration example

N/A

4.1.4 Common Scenario — Authentication

4.1.4.1 [Optional] 802.1x Authentication

Principles:

Authentication roles are described as follows:

Client: Ruijie SU client or an open-source client.

NAS: controls the network connection status of a client based on its current authentication status. The device serves as an agent between clients and the sever. It request usernames from clients, checks the authentication information from the server, and forwards the information to the clients.

RADIUS server: corresponding to Ruijie SAM+ system, which provides the authentication service for users.

The figure below shows the authentication flow.



Configuration commands:

aaa new-model//Enable the AAA function.

aaa accounting network (list name) start-stop group(group name) //AAA reference configuration. The actual service deployment prevails.

aaa authentication dot1x (list name) group (group name)//802.1x template reference configuration for AAA. The actual service deployment prevails.

aaa authentication login default local //Use the local username/password to log in to the AAA device.

aaa group server radius (group name) //Configure an AAA server group, which is applicable to multi-RADIUS scenarios.

server (radius ip)//Configure an AAA server group, which is applicable to multi-RADIUS scenarios.

radius-server host (radius ip) key 7 (radius key) //Configure the IP address and key for the AAA server, which are applicable to single-RADIUS scenarios.

aaa accounting update periodic 30 //Set the interval for AAA accounting update to 30s. aaa accounting update //Configure AAA accounting update.

aaa authorization ip-auth-mode mixed //Set the IP address authorization mode of 802.1x clients to the mixed mode. The IP addresses can be obtained via polling in multiple ways (DHCP/RADIUS). no aaa log enable //Disable the AAA log function.

dot1x valid-ip-acct enable//Mandatory. The accounting update packets are used to upload the user IP address to SAM+. If the 802.1x authentication module does not have IP entries of the user, the user is forced to go offline 5 minutes later, to prevent users at the IP address 0.0.0.0

```
snmp-server community xx(community name) rw
```

Precautions:

The list name configured in **aaa authentication dot1x** (*list name*) **group** (group name) should be consistent with that in **dot1x authentication** (*list name*).

When only 802.1x authentication is enabled on an interface, security channels must be configured to allow DHCP packets to pass. Otherwise, users cannot obtain IP addresses. For specific configuration, see the security channel configuration.

Configuration example

| Scenario | Radius Server |
|---------------|--|
| | Switch A F 0/1 F 0/24 192.168.217.82 F 0/24 NSA 192.168.217.81 Internet |
| | |
| | |
| Configuration | Register the IP address of the device with the RADIUS server and configure the key for the device to |
| Steps | communicate with the server. |
| | Create an account on the RADIUS server. |
| | Enable AAA on the device. |
| | Configure RADIUS parameters on the device. |
| | Enable 802.1x authentication on interfaces of the device. |
| | The following shows relevant configurations on the device. For the configurations of the server, see the |
| | server configuration guide. |
| | ruijie# configure terminal |
| | ruijie (config)# aaa new-model |

| | ruijie (config)# aaa accounting network radius start-stop group default | | | | |
|--------------|---|--|--|--|--|
| | ruijie (config)# aaa authentication dot1x radius group default | | | | |
| | ruijie (config)# aaa authentication login default local | | | | |
| | ruijie (config)# aaa accounting update periodic 30 | | | | |
| | ruijie (config)# aaa accounting update | | | | |
| | ruijie (config)# aaa authorization ip-auth-mode mixed | | | | |
| | ruijie (config)# no aaa log enable | | | | |
| | ruijie (config)# radius-server host 192.168.32.120 key 7 ruijie | | | | |
| | <pre>ruijie (config)# interface FastEthernet 0/1</pre> | | | | |
| | ruijie (config-if)# dot1x port-control auto | | | | |
| | | | | | |
| Verification | Test whether authentication can be performed normally and whether network access behavior changes after | | | | |
| | authentication. | | | | |
| | Create an account on the server, for example, username:test,password:test. | | | | |
| | An unauthenticated client fails to ping 192.168.32.120. | | | | |
| | Start Supplicant on the client and enter the username for authentication. After the client is authenticated, it | | | | |
| | can ping 192.168.32.120 successfully. | | | | |

4.1.4.2 [Mandatory] Web Authentication

Principles:

A user opens the Internet Explorer (IE) and accesses a website to initiate an HTTP request.

The NAS intercepts the HTTP request from the client, and forcibly forwards the HTTP request to the portal server. It also adds some relevant parameters to the portal URL. For the parameters, see CHAP authentication.

The portal server pushes the Web authentication page to the client.

The user enters the username and password on the authentication page and submits them to the portal server.

The portal server sends the username and password to the NAS to initiate authentication.

The NAS sends the username and password to the RADIUS server, which checks whether the user is valid and returns the Radius access-accept/reject message to the NAS.

The NAS returns the authentication result to the portal server.

The portal server pushes the authentication result page to the user based on the authentication result.

The portal server notifies the NAS that the authentication result packet has been received.

The NAS sends the accounting start packet.

Note: Web authentication acceleration supports direct access to the portal page for authentication, without redirection.

Difference from the 1st-generation portal: The authentication is completed by the NAS and RADIUS server, which greatly reduces the load of the portal server.

In simplistic network environments, static ARP addresses are automatically bound after Web authentication succeeds, which is different from that in conventional solutions.



Configuration commands:

aaa new-model //Enable the AAA function. aaa accounting network (list name) start-stop group(group name) //AAA reference configuration. The actual service deployment prevails. aaa authentication web-auth (list name) group(group name) //Web authentication template reference configuration for AAA. The actual service deployment prevails. aaa authentication login default local //Use the local username/password to log in to the AAA device. aaa group server radius (group name) //Configure an AAA server group, which is applicable to multi-RADIUS scenarios. server (radius ip) //Configure an AAA server group, which is applicable to multi-RADIUS scenarios. radius-server host (radius ip) key 7 (radius key) //Configure the IP address and key for the AAA server, which are applicable to single-RADIUS scenarios. aaa accounting update periodic 30 //Set the interval for AAA accounting update to 30s. aaa accounting update //Configure AAA accounting update. aaa authorization ip-auth-mode mixed //Set the IP address authorization mode of 802.1x clients to the mixed mode. The IP addresses can be obtained via polling in multiple ways (DHCP/RADIUS). no aaa log enable //Disable the AAA log function.

web-auth template eportalv2 //Create a Web authentication template. ip 202.204.193.32 //Set the IP address of the portal server. url http://202.204.193.32/eportal/index.jsp //Set the URL of the portal server. authentication (list name) //Optional. This command is required when the authentication list name for AAA is not set to **default**. accounting (list name) //Optional. This command is required when the accounting list name for AAA is not set to **default**. web-auth portal key university //Optional. Configure the key. interface range GigabitEthernet 0/2-3 //Configure the interface for enabling Web authentication. web-auth enable eportalv2 //Enable Web authentication on the interface. web-auth vlan-control 2000-3000 //Enable VLAN-based Web authentication control. This command is used in a scenario in which both 802.1x authentication and Web authentication are enabled on the same port of the RG-N18000, and some VLANs need to support only 802.1x authentication control. Such VLANs can be excluded from the Web authentication VLAN range. snmp-server host x.x.x.x(server IP address) informs version 2c xx(community name) snmp-server community xx(community name) rw

Precautions:

The AAA method list must be consistent with the Web authentication method list.

Configuration example



| | server configuration guide. | | | | | |
|--------------|---|--|--|--|--|--|
| | ruijie# configure terminal | | | | | |
| | ruijie (config)# aaa new-model | | | | | |
| | ruijie (config)# aaa accounting network radius start-stop group default | | | | | |
| | ruijie (config)# aaa authentication web-auth radius group default | | | | | |
| | ruijie (config)# aaa authentication login default local | | | | | |
| | ruijie (config)# aaa accounting update periodic 30 | | | | | |
| | ruijie (config)# aaa accounting update | | | | | |
| | ruijie (config)# no aaa log enable | | | | | |
| | ruijie (config)# radius-server host 192.168.32.120 key 7 ruijie | | | | | |
| | <pre>ruijie (config)# web-auth template eportalv2</pre> | | | | | |
| | ruijie (config)# ip 202.204.193.32 | | | | | |
| | <pre>ruijie (config)# urlhttp://202.204.193.32/eportal/index.jsp</pre> | | | | | |
| | <pre>ruijie (config)# interface FastEthernet 0/1</pre> | | | | | |
| | <pre>ruijie (config-if)# web-auth enable eportalv2</pre> | | | | | |
| | <pre>snmp-server host 192.168.21.120 informs version 2c xx (community name)</pre> | | | | | |
| | <pre>snmp-server community XX(community name) rw</pre> | | | | | |
| | | | | | | |
| | | | | | | |
| Verification | Test whether authentication can be performed normally and whether network access behavior changes after | | | | | |
| | authentication. | | | | | |
| | Create an account on the server, for example, username:test,password:test. | | | | | |
| | An unauthenticated client fails to ping 192.168.32.120. | | | | | |
| | The client browser automatically redirects to the Web authentication page. Enter the username for | | | | | |
| | authentication. After the client is authenticated, it can ping 192.168.32.120successfully. | | | | | |

4.1.4.3 [Mandatory] AAA IP Authorization

Principles:

802.1x authentication and MAB authentication do not support IP address identification. Ruijie extends the authentication application, which supports MAC+IP binding. This function is called IP authorization. There are four IP authorization modes:

SU authorization: IP addresses are provided by the Supplicant. This mode needs to be used in combination with Ruijie Supplicant.

RADIUS authorization: IP addresses are delivered to the device by the RADIUS server after clients are authenticated.

DHCP-server authorization: An authenticated client initiates a DHCP request to obtain an IP address. After an IP address is obtained, the system binds the IP address with the MAC address of the client. This mode is applicable to dynamic IP environments.

Mixed authorization: The system performs MAC+IP binding for authenticated clients in the sequence of Supplicant authorization, RADIUS authorization, and DHCP-server authorization. If the Supplicant provides an IP address, the authenticated client uses it preferentially; if the Supplicant does not provide an IP address, the IP address provided by the

RADIUS server is used; if the RADIUS server does not provide an IP address, the IP address provided by the DHCP server is used.

Note: Mixed authorization is recommended to all scenarios.

Configuration

commands:

aaa authorization ip-auth-mode mixed//Configured in global configuration mode.

Precautions:

The configuration of this command is irrelevant to whether IP addresses can be uploaded to SAM+. The functions of this command are as follows: If no IP address is authorized to a user, there is no entry of the IP address and the user cannot be charged or brought offline upon no traffic. This command can be used in combination with **valid ip acct** to bring users who do not meet authorization configuration requirements offline.

Configuration example

N/A

4.1.4.4 [Optional] MAB Authentication

Principles:

MAB authentication, one of the main authentication modes in the simplistic network solution, is applicable to wireless users in office areas of campus networks. With the MAB authentication model and high-performance authentication processing capacity of the RG-N18000, MAB authentication enables the RG-N18000 to learn the MAC address of a client when the client accesses the network, so that teachers do not need to repeatedly entering their usernames and passwords when using wireless clients for Web authentication, to prevent deteriorating user experience. The RG-N18000 uses the MAC address of the client as the username and password to send an authentication request to SAM+ to complete the authentication as a proxy. The user cannot perceive the authentication in this process.

The following is the MAB authentication process:

Enable the client MAB authentication on SAM+ by accessing the access control directory.

After Web authentication succeeds for the first time, a user can select MAB authentication on the authentication success page.

When the user chooses to enable MAB authentication, the MAC address of the user client is registered with SAM+.

After the client connects to the network, the RG-N18000 serving as a NAS, identifies the MAC address of the client, and uses the MAC address as the username and password to initiate authentication to SAM+.

SAM+ determines validity of the MAC address and returns the authentication success/failure message to the NAS.

If the authentication is successful, the NAS sends the accounting start packet.

Configuration

commands:

Note: MAB authentication takes effect only after each user is WEB authenticated for the first time. In addition, MAB authentication belongs to the 802.1x authentication system. Therefore, both Web authentication and 802.1x authentication need to be configured for MAB authentication.

Configuring global AAA parameters

aaa new-model //Enable the AAA function. aaa accounting network (list name) start-stop group(group name) //AAA reference configuration. The actual service deployment prevails. aaa authentication dot1x (list name) group (group name) //802.1x template reference configuration for AAA. The actual service deployment prevails. aaa authentication web-auth (list name) group(group name) //Web authentication template reference configuration for AAA. The actual service deployment prevails. aaa authentication login default local //Use the local username/password to log in to the AAA device. aaa group server radius (group name) //Configure an AAA server group, which is applicable to multi-RADIUS scenarios. server (radius ip) //Configure an AAA server group, which is applicable to multi-RADIUS scenarios. radius-server host (radius ip) key 7 (radius key) //Configure the IP address and key for the AAA server, which are applicable to single-RADIUS scenarios. aaa accounting update periodic 30 //Set the interval for AAA accounting update to 30s. aaa accounting update //Configure AAA accounting update. //Disable the AAA log function. no aaa log enable

Configuring 802.1x parameters and enabling 802.1x authentication on the interface

dot1x accounting (list name) //Optional. This command is required when the 802.1x accounting list name for AAA is not set to default. dot1x authentication (list name) //Optional. This command is required when the 802.1x authentication list name for AAA is not set to default. interface range GigabitEthernet 0/2-3 //Configure the interface for enabling 802.1x authentication.

dot1x port-control auto//Enable 802.1x authentication on the interface.

U Configuring Web authentication parameters and enabling Web authentication on the interface

```
web-auth template eportalv2
ip 202.204.193.32 //Set the IP address of the portal server.
url <u>http://202.204.193.32/eportal/index.jsp</u> //Set the URL of the portal server.
authentication (list name) //Optional. This command is required when the authentication
list name for AAA is not set to default.
accounting (list name) //Optional. This command is required when the accounting list name
for AAA is not set to default.
```

```
web-auth portal key university //Optional. Configure the key.
interface range GigabitEthernet 0/2-3 //Configure the interface for enabling Web
authentication.
```

web-auth enable eportalv2////Enable Web authentication on the interface.

Configuring MAB authentication parameters and enabling MAB authentication on the interface

aaa authorization ip-auth-mode mixed //Mandatory. Set the IP address authorization mode of 802.1x clients to the mixed mode. The IP addresses can be obtained via polling in multiple ways (DHCP/RADIUS).

ip dhcp snooping //Mandatory. An IP address needs to be obtained via the DHCP snooping module for MAB authentication. Otherwise, a user with the IP address of 0.0.0.0 appears on SAM.

dot1x mac-auth-bypass valid-ip-auth //Mandatory. The DHCP module instructs the MAB module to start authentication. Clients must obtain IP addresses before starting MAB authentication. Otherwise, the MAB authentication is blocked to prevent clients with the IP address of 0.0.0.0 on SAM+. The configuration of this command will drop users out of the network. It is not recommended to run this command in service peak hours.

dot1x valid-ip-acct enable //Mandatory. The accounting update packets are used to upload the user IP address to SAM+. If the 802.1x authentication module does not have an IP entry of the user, the user is kicked offline 5 minutes later, to prevent users at the IP address 0.0.0.0 on SAM+. The configuration of this command will drop users out of the network. It is not recommended to run this command in service peak hours.

dot1x mac-auth-bypass multi-user //Mandatory. Enable MAB authentication on the interface.

dot1x mac-auth-bypass vlan (vlan-list) //Optional. Configure this command in interface configuration mode to enable VLAN-based MAB authentication.

dot1x multi-mab quiet-period 0 //Optional. Configure the quiet period for MAB authentication. In this period, after a client fails the authentication, MAB authentication cannot be restarted before the MAC entry of the client ages on the RG-N18000. In this way, SAM+ does not generate logs of users who are not registered with SAM+. However, after failing the MAB authentication at the first time, the client needs to wait for its MAC entry on the RG-N18000 to age before it can trigger MAB authentication again. Configure this function as required.

Precautions:

MAB authentication takes effect only after relevant configurations are completed on SAM+. For details, see MAB authentication configuration in "SAM+ Configuration".

MAB authentication takes effect only after it is selected on the authentication page.

MAB authentication takes effect after a client is MAB authenticated for the first time.

MAB authentication supports only dynamic DHCP users. It does not support static IP users. The RG-N18000 transfers IP addresses from the DHCP snooping module to SAM+, and therefore information about static IP users does not exist in the DHCP snooping module.

802.1x authentication has a higher priority than MAB authentication. Therefore, if a client is MAB authenticated and then uses the client software to perform 802.1x authentication, the MAB authentication entry will be deleted.

After MAB authentication is enabled, avoid configuring **User Preemption** or setting **Concurrent Logins Limit** to **1**. Otherwise, two clients using the same username will preempt a MAB authentication resource and be dropped out of the network.

Configuration example

See description about the configuration commands.

4.1.4.5 [Optional] MAB Authentication

Principles:

MAB authentication, one of the main authentication modes in the simplistic network solution, is applicable to wireless users in office areas of campus networks. With the MAB authentication model and high-performance authentication processing capacity of the RG-N18000, MAB authentication enables the RG-N18000 to learn the MAC address of a client when the client accesses the network, so that teachers do not need to repeatedly entering their usernames and passwords when using wireless clients for Web authentication, to prevent deteriorating user experience. The RG-N18000 uses the MAC address of the client as the username and password to send an authentication request to SAM+ to complete the authentication as a proxy. The user cannot perceive the authentication in this process.

The following is the MAB authentication process:

Enable the client MAB authentication on SAM+ by accessing the access control directory.

After Web authentication succeeds for the first time, a user can select MAB authentication on the authentication success page.

When the user chooses to enable MAB authentication, the MAC address of the user client is registered with SAM+.

After the client connects to the network, the RG-N18000 serving as a NAS, identifies the MAC address of the client, and uses the MAC address as the username and password to initiate authentication to SAM+.

SAM+ determines validity of the MAC address and returns the authentication success/failure message to the NAS.

If the authentication is successful, the NAS sends the accounting start packet.

Configuration commands:

Note: MAB authentication takes effect only after each user is WEB authenticated for the first time. In addition, MAB authentication belongs to the 802.1x authentication system. Therefore, both Web authentication and 802.1x authentication need to be configured for MAB authentication.

U Configuring global AAA parameters

aaa new-model //Enable the AAA function. aaa accounting network (list name) start-stop group(group name) //AAA reference configuration. The actual service deployment prevails. aaa authentication dot1x (list name) group (group name) //802.1x template reference configuration for AAA. The actual service deployment prevails. aaa authentication web-auth (list name) group(group name) //Web authentication template reference configuration for AAA. The actual service deployment prevails. aaa authentication login default local //Use the local username/password to log in to the AAA device. aaa group server radius (group name) //Configure an AAA server group, which is applicable to multi-RADIUS scenarios. server (radius ip) //Configure an AAA server group, which is applicable to multi-RADIUS scenarios. radius-server host (radius ip) key 7 (radius key) //Configure the IP address and key for the AAA server, which are applicable to single-RADIUS scenarios. aaa accounting update periodic 30 //Set the interval for AAA accounting update to 30s. aaa accounting update //Configure AAA accounting update. no aaa log enable //Disable the AAA log function.

2 Configuring 802.1x parameters and enabling 802.1x authentication on the interface

dot1x accounting (list name) //Optional. This command is required when the 802.1x accounting list name for AAA is not set to default. dot1x authentication (list name) //Optional. This command is required when the 802.1x authentication list name for AAA is not set to default. interface range GigabitEthernet 0/2-3 //Configure the interface for enabling 802.1x authentication.

dot1x port-control auto//Enable 802.1x authentication on the interface.

Configuring Web authentication parameters and enabling Web authentication on the interface

web-auth template eportalv2 ip 202.204.193.32 //Set the IP address of the portal server. url <u>http://202.204.193.32/eportal/index.jsp</u> //Set the URL of the portal server. authentication (list name) //Optional. This command is required when the authentication list name for AAA is not set to **default**. accounting (list name) //Optional. This command is required when the accounting list name for AAA is not set to **default**. web-auth portal key university //Optional. Configure the key. interface range GigabitEthernet 0/2-3 //Configure the interface for enabling Web authentication. web-auth enable eportalv2////Enable Web authentication on the interface.

Configuring MAB authentication parameters and enabling MAB authentication on the interface

aaa authorization ip-auth-mode mixed //Mandatory. Set the IP address authorization mode of 802.1x clients to the mixed mode. The IP addresses can be obtained via polling in multiple ways (DHCP/RADIUS).

ip dhcp snooping //Mandatory. An IP address needs to be obtained via the DHCP snooping module for MAB authentication. Otherwise, a user with the IP address of 0.0.0.0 appears on SAM.

dot1x mac-auth-bypass valid-ip-auth //Mandatory. The DHCP module instructs the MAB module to start authentication. Clients must obtain IP addresses before starting MAB authentication. Otherwise, the MAB authentication is blocked to prevent clients with the IP address of 0.0.0.0 on SAM+. The configuration of this command will drop users out of the network. It is not recommended to run this command in service peak hours.

dot1x valid-ip-acct enable //Mandatory. The accounting update packets are used to upload the user IP address to SAM+. If the 802.1x authentication module does not have an IP entry of the user, the user is kicked offline 5 minutes later, to prevent users at the IP address 0.0.0.0 on SAM+. The configuration of this command will drop users out of the network. It is not recommended to run this command in service peak hours.

dot1x mac-auth-bypass multi-user //Mandatory. Enable MAB authentication on the interface.

dotlx mac-auth-bypass vlan (vlan-list) //Optional. Configure this command in interface configuration mode to enable VLAN-based MAB authentication.

dot1x multi-mab quiet-period 0 //Optional. Configure the quiet period for MAB authentication. In this period, after a client fails the authentication, MAB authentication cannot be restarted before the MAC entry of the client ages on the RG-N18000. In this way, SAM+ does not generate logs of users who are not registered with SAM+. However, after failing the MAB authentication at the first time, the client needs to wait for its MAC entry on the RG-N18000 to age before it can trigger MAB authentication again. Configure this function as required.

Precautions:

MAB authentication takes effect only after relevant configurations are completed on SAM+. For details, see MAB authentication configuration in "SAM+ Configuration".

MAB authentication takes effect only after it is selected on the authentication page.

MAB authentication takes effect after a client is MAB authenticated for the first time.

MAB authentication supports only dynamic DHCP users. It does not support static IP users. The RG-N18000 transfers IP addresses from the DHCP snooping module to SAM+, and therefore information about static IP users does not exist in the DHCP snooping module.

802.1x authentication has a higher priority than MAB authentication. Therefore, if a client is MAB authenticated and then uses the client software to perform 802.1x authentication, the MAB authentication entry will be deleted.

After MAB authentication is enabled, avoid configuring **User Preemption** or setting **Concurrent Logins Limit** to **1**. Otherwise, two clients using the same username will preempt a MAB authentication resource and be dropped out of the network.

Configuration example

See description about the configuration commands.

4.1.4.6 [Mandatory] No-traffic Go-offline

Principles:

When detecting that a client generates no traffic in a period of time, the core device RG-N18000 used in simplistic networks actively forces the client to go offline, thereby preventing invalid charging.

No-traffic go-offline can be enabled based on VLANs. In simplistic networks, VLANs represent different planned areas, and areas can be selected to enable/disable this function.

The family area of a campus network uses a router as a proxy to complete authentication for Internet access. After the traffic keepalive function is globally enabled on the RG-N18000, if a client in the family area does not access the Internet within a period of time, the client is forced to go offline and needs to be re-authenticated. Therefore, the traffic keepalive function is not recommended for this area. The

VLAN-based no-traffic go-offline can be configured for control.

Implementation principles:

To implement no-traffic go-offline, the system traverses the MAC address table of the device and compares the MAC address table with MAC addresses in the entries of authenticated users. If the MAC address of an authenticated user in the MAC address table has aged, the system determines that the user has no traffic and kicks the user offline. Note: The time consumed for traversing the MAC address table causes an error of 3–5 minutes to the original period for no-traffic go-offline detection is set to 15 minutes, it actually takes 18 to 20 minutes to kick clients offline.

Configuration commands:

offline-detect interval 15 threshold 0 //If no traffic from a user is detected within 15 minutes, the user is kicked offline. The RG-N18000 checks whether there is user traffic matching the MAC address table for judgment.

offline-detect interval infinity threshold 0 vlan 300 //Set the no-traffic go-offline detection period to an infinite large value for VLAN 300. If the no-traffic go-offline function is globally enabled, run this command to disable this function for some VLANs.

VLAN-based no-traffic go-offline is applicable only to router dialup scenarios, in which routers are online for long. It cannot be applied to common client scenarios. Otherwise, the online duration on SAM+ will be inaccurate and affects the charging results.

Precautions:

Only no-traffic go-offline is supported currently, and low-traffic go-offline is not supported.

When the DHCP lease period of the client expires or the RG-N18000 receives a DHCP release packet, the RG-N18000 kicks the client offline during authentication.

It is recommended to set the period for no-traffic go-offline detection to be shorter than the lease period of DHCP server.

The function involves the traversal of the MAC address table, which increases the detection period by 3–5 minutes based on original parameter configuration. If the original period for no-traffic go-offline detection is set to 15 minutes, it actually takes 18 to 20 minutes to kick clients offline.

Configuration example

N/A

4.1.4.7 [Mandatory] IPv6 Authentication Mode

Principles:

Note that independent IPv6 authentication is not supported in simplistic networks. The IPv6 authentication mode is determined according to the IPv4 authentication result. Three modes are available:

Compatible: If IPv4 authentication fails, IPv6 packets cannot be forwarded; if IPv4 authentication succeeds, IPv6 packets can be forwarded.

Strict: IPv6 packets cannot be forwarded regardless of whether IPv4 authentication succeeds.

Loose: IPv6 packets can be forwarded regardless of whether IPv4 authentication succeeds.

Note: In simplistic networks, the RG-N18000 uses the strict mode by default, which will result in the failure to forward IPv6 packets. Change the mode to the compatible mode.

Configuration

commands:

Ruijie(config)#address-bind ipv6-mode compatible//Compatible modeRuijie(config)#address-bind ipv6-mode strict//Strict modeRuijie(config)#address-bind ipv6-mode loose//Loose mode

Precautions:

Note: In simplistic networks, the RG-N18000 uses the strict mode by default, which will result in the failure to forward IPv6 packets. Change the mode to the compatible mode.

Configuration example

N/A

4.1.4.8 [Mandatory] Source Port for Communicating with the RADIUS/Portal Server

Principles:

After configuration, the source port of the device for communicating with the RADIUS server is any specified port. After configuration, the source port of the device for communicating with the portal server is any specified port.

Configuration

commands:

ip portal source-interface loopback 0
ip radius source-interface lookback 0

Precautions:

Only one source port of the RADIUS server can be configured.

Only one source port of the portal server can be configured.

Configuration example

N/A

4.1.4.9 [Mandatory] Migration of Authenticated Users

Principles:

Scenario 1: When an online authenticated client migrates across super VLANs, migration of authenticated users must be enabled. Otherwise, the original authentication entry still exists and the client cannot be authenticated after moving to another VLAN/port.

Scenario 2: An online client migrates across different sub VLANs of the same super VLAN and the IP address keeps unchanged before and after migration. After migration of authenticated users is configured, the user is exempted from authentication before and after migration (the portal page does not pop up). It prevents user experience deterioration caused by frequent re-authentication.

Scenario 3: An online client migrates across super VLANs, and even if migration of authenticated users is configured, the client needs to be re-authenticated before accessing the network (the portal page pops up).

Scenario 4 (spoofing scenario): User A is authenticated in VLAN A. User B uses the same MAC address as User A and logs in by using the same username/password or MAC address to simulate migration. In such spoofing scenarios, the RG-N18000 sends an ARP detection packet to User A in VLAN A. If the RG-N18000 receives an ARP response from User A, it determines that spoofing occurs and rejects migration.

Note: VLANs here refer to sub VLANs.

Configuration commands:

station-move permit//Mandatory. The overall switch for migration of authenticated users must be enabled, so that migration of Web and 802.1x authenticated users becomes available. When an authenticated user triggers migration, the pre-migration authentication entry is automatically deleted and the post-migration authentication entry is automatically added.

web-auth station-move auto//Mandatory. After migration of Web authenticated users is enabled, when an authenticated user triggers migration, the Web authentication module automatically deletes the pre-migration authentication entry and automatically adds the post-migration authentication entry.

web-auth station-move info-update //Mandatory. When migration of Web authenticated users is enabled, the accounting update packet is used to notify the RADIUS server of the latest value of the user VID/port.

Precautions:

VLAN changes after user migration refer to sub VLAN changes.

If a user migrates across super VLANs, that is, the IP address changes after migration, the migration cannot be completed.

Configuration example

N/A

4.1.5 Common Scenario — Authentication Optimization Configuration

4.1.5.1 [Optional] Portal Escape

Principles:

The portal escape mechanism exempts new users from authentication when the portal server on the live network becomes unavailable.

Configuration

commands:

web-auth portal-check interval 3 timeout 3 retransmit 10 //Set the detection interval to 3s, timeout duration to 3s, and retransmission count to 10. web-auth portal-escape [nokick] //When portal escape takes effect and the nokick attribute is set, an online user will not be kicked offline. If the nokick attribute is deleted, an online user will be kicked offline.

Precautions:

The portal detection needs to be configured.

If multiple Portal servers are configured, the escape function takes effect only when all the Portal servers are unavailable.

This function is valid only to Portal servers.

Configuration example

N/A

4.1.5.2 [Optional] RADIUS Escape

Principles:

After the RADIUS escape function is configured, users can still be authenticated and access the Internet even if the RADIUS server malfunctions.

Configuration commands:

radius-server host (radius ip) test username ruijieidle-time 2 key (radius key) //Mandatory. Use this command to keep the detection between the device and the RADIUS server alive. The RG-N18000 sends a detection packet with the username/password being ruijie/ruijie (the username can be user-defined, but the password is always ruijie) to the RADIUS server for authentication. If the authentication succeeds, it indicates that the RADIUS is still alive. **radius key** here is not the user password. Instead, it is the key set by SAM+ server for interaction with the RG-N18000.

radius-server dead-criteria time 120 tries 12//Mandatory. The timeout duration is 120s. If the RG-N18000 does not receive a response after an authentication request is retransmitted for 12 times, the RG-N18000 determines to escape. This function prevents authentication jitter caused by oversensitivity of escape detection.

The account (user name: ruijie; password: ruijie) needs to be configured and activated on SAM+. This is mandatory.

web-auth radius-escape//Globally configured to enable RADIUS escape for Web authentication. dot1x critical//Configured on the interface to enable RADIUS escape for dot1x authentication. dot1x critical recovery action reinitialize //Configured on the interface, so that after the RADIUS server is recovered, the user that uses dot1x escape is kicked offline for re-authentication.

Precautions:

The account needs to be configured and activated on the SAM server. For example, the username and password are both ruijie. Otherwise, a great number of spam logs from inexistent accounts are generated.

To cancel the escape detection command **no radius-server host** (*radius ip*) **test username ruijie idle-time 2 key** (*radius key*), delete it, and then configure the **radius-server host** (*radius ip*) **key 7** (*radius key*) command. Otherwise, the RADIUS server is unreachable.

Configuration example

N/A

4.1.5.3 [Optional] Web Authentication — IP/VLAN-based SSID Mapping

Principles:

In conventional network solutions, an AC serving as the NAS for wireless user authentication obtains SSIDs of wireless users via the association module between the AC and APs and uploads the SSIDs to SAM+ server. In addition, policies are configured on SAM+ server/portal server to implement the mapping between SSIDs and authentication pages pushed by the portal server, so that different authentication pages are displayed for different ISPs or users.

In simplistic networks, the core device RG-N18000 cannot associate with APs to obtain SSIDs of wireless users. To address this defect, you can manually configure the VLAN-based SSID mapping function on the RG-N18000, so that SSIDs are uploaded to SAM+ server via authentication packets, thereby meeting the requirements of different ISPs or user groups for different authentication pages.

Configuration commands:

Ruijie(config)#web-auth mapping map-ssid vlan100 ssid ChinaNet //Define the mapping template name, mapped VLAN ID, and mapped SSID name. Ruijie(config-if-GigabitEthernet 0/1)# web-auth apply-mapping map-ssid //Apply the mapping template to the interface.

Precautions:

Multiple mappings can be configured. If a user is out of the mapping range, the portal server is used for authentication by default.

VLANs cannot overlap with each other.

Configuration example

See description about the configuration commands.

4.1.5.4 [Optional]Static IP Address MAB Authentication

Note: This function is supported only in N18000_RGOS 11.0(1)B3P3 and later versions.

Principles:

Static IP address MAB authentication is MAB authentication triggered by using ARP packets. It needs to be used in combination with the quiet function as well as fast MAC binding entries of SAM+ server.

- 1. The fast MAC binding information of users need to be added to SAM+ server.
- 2. This function needs to be used in combination with the quiet function.

Configuration

commands:

dot1x mac-auth-bypass static-ip-segment 1.1.1.0 255.255.255.0 unforced //Send ARP packets from the static IP address segment to trigger MAB authentication. MAB authentication can be initiated based on only IP address segments.

dot1x multi-mab quiet-period 300 //Enable 802.1x quiet function and set the quiet period to 300s. In this period, MAB authentication cannot be performed, but Web authentication and 802.1x authentication are available.

dot1x pending-user authen-num 24 //Optional. Set the default rate of MAB authentication triggered by ARP packets to 24 users/second. It is not recommended to change the default value.

Precautions:

 The static IP address MAP authentication needs to be used together with the quiet function. Otherwise, users who fail the authentication performs authentication repeatedly, imposing great pressure on SAM+ and incurring exceptions. The recommended quiet period is 5 minutes. 2. Static IP address MAB authentication takes effect only when fast MAC binding entries are configured on SAM+. If no fast MAC binding entry is available on SAM+, manually bind MAC addresses. MAC addresses cannot be configured in Web authentication mode (if a static IP address is within the IP address segment range configured by using the dot1x mac-auth-bypass static-ip-segment command, the Web authentication page does not pop up and redirection cannot be performed).

Configuration example

interface GigabitEthernet 1/1 //Enable MAB authentication on the interface.

switchport protected switchport mode trunk switchport trunk allowed vlan only 2-50,3000-3001 dot1x port-control auto dot1x mac-auth-bypass multi-user web-auth enable eportalv2 dot1x mac-auth-bypass static-ip-segment 10.20.50.0 255.255.255.0 //Configured globally send ARP packets from the static IP address segment to trigger MAB authentication.

dot1x multi-mab quiet-period 300 //Enable the 802.1x quiet function and set the quiet period to 300s.

After a user is authenticated, SAM+ automatically binds the MAC address of the user and enables static IP address MAB authentication upon next user login.

| SAM ⁺ security accounting mar | IAGEMENT SYSTEM | | | | | | | | |
|--|-----------------|-------------------------|-----------------|--------------|------------------|-----------|------------|-----------------|------------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | |
| Location: Operation > Online User | | | | | | | | | |
| Username | Full Name | | | | 🖉 General Sea | rch Searc | h Advar | nced Search | |
| User IP(v4) | te | ^a Please Sel | ect 🔻 | | | | | | |
| | | | Force the | Users Offlir | ne Delete the | Selected | Delete All | Show the | Backgrou |
| | (| Add the us | sers to the bla | cklist when | forced offline 5 | | mins eff | fective; blackl | ist messag |
| There were no results found. Column Con | fig | | | | | | | | |
| Username User I | P(v4) U | ser MAC | NAS | IP(v4) | NAS Port | Service | ÷ | Acce | ss Contro |
| Invalid wireless user internet traffic blockag | e | | | | | | | | |

4.1.5.5 [Optional] 802.1x Authentication Quiet Function

Note: This function is supported only in N18000_RGOS 11.0(1)B3P3 and later versions.

Principles:

After the quiet function is configured, users who fail the authentication are added to the quiet queue and do not initiate authentication. They can initiate authentication after the quiet period expires.

Configuration

commands:

dot1x multi-mab quiet-period 300 //Enable the 802.1x quiet function and set the quiet period to 300s.

Precautions:

The quiet function does not need to be configured if static IP address MAB authentication is not required. Otherwise, the function may affect authentication performance and cause high CPU usage of line cards.

Configuration example

N/A

4.1.5.6 [Mandatory] Preventing 802.1x Authentication from Preempting MAB Authentication Resources

Note: This function is supported only in N18000_RGOS 11.0(1)B3P3 and later versions.

Principles:

By default, 802.1x authentication has a higher priority than MAB authentication, and 802.1x authentication preempts resources of MAB authentication. If it is required that 802.1x authentication not preempt resources of MAB authentication and they have the same priority, configure this command on an interface. After configuration, 802.1x authentication does not preempt resources of MAB authentication and 802.1x authentication will fail if a MAB authenticated user is online.

Configuration commands:

DLUT-CORE-N18014(config-if-GigabitEthernet 1/3/34)#dot1x mac-auth-bypass precedence ? <cr>

Ψ

Precautions:

Before the function is configured, do not enable Windows-embedded 802.1x authentication when MAB authentication is used. By default, 802.1x authentication preempts MAB authentication resources. As a result, a MAB authenticated user is kicked offline.

Configuration example

N/A

4.1.6 QinQ Isolation Scenarios

4.1.6.1 [Mandatory] QinQ VLAN Tag Termination

Principles:

The QinQ VLAN tag termination enables the routing forwarding module to receive and send packets with dual VLAN tags.

CE-vlan//QinQ inner VLAN tag. VLANs must be consecutive, for example, 101–150.

PE-vlan//QinQ outer VLAN tag (sub VLAN).

Note: The modified CE-VLAN configuration will overwrite original configuration. Improper configuration will cause network interruption.

Example: Original configuration: qinq termination ce-vlan 200 to 300

New configuration: qinq termination ce-vlan 301 to 310

The original configuration will be overwritten as follows: qinq termination ce-vlan 301 to 310

Configuration commands:

Configuring CE-VLANs Command ging termination ce-vlan start-vid to end-vid Parameter Description start-vid indicates the minimum CE-VLAN ID. end-vid indicates the maximum CE-VLAN ID. Defaults By default, user VLANs have no QinQ VLAN tag termination. Command Mode Global configuration mode Usage Guide There is no CE-VLAN by default. Configuring PE-VLANs Command qinq termination pe-vlan [add | remove] vlan-list Parameter Description vlan-list: Indicates the VLAN list in the range of 1 to 4094.

Defaults

By default, ISP VLANs have no QinQ VLAN tag termination.

Command Mode

Global configuration mode

Usage Guide

ISP VLANs with QinQ VLAN tag termination can be configured in incremental mode.

Precautions:

QinQ VLAN tag termination is performed only in the case of routing and forwarding, and layer-2 forwarding enables only transparent transmission through tunnels.

If users of different CE-VLANs need to communicate with each other, the local ARP proxy (enabled by default) needs to be enabled on the SVI corresponding to the PE-VLAN.

ED cards support 511 CE-VLANs by default.

DB cards support 61 CE-VLANs by default.

It is recommended to reduce the number of CE-VLANs to be created during deployment, for example, if only 50 CE-VLANs are used on the live network, run the **qinq termination ce-vlan 101 to 151** command to create required VLANs. Avoid creating 511 CE-VLANs at a time. More CE-VLANs will result in high CPU usage of the RG-N18000.

Determine whether a client with a single VLAN tag exists on the RG-N18000. If yes, the VLAN ID of the client cannot be the same as that of the PE-VLAN (outer VLAN) configured in QinQ VLAN tag termination command.

Case:

The following command is executed to configure the outer VLAN range for QinQ VLAN tag termination on the RG-N18000: qinq termination pe-vlan 100-101.

After packets from a client with a single VLAN tag reach the RG-N18000, the RG-N18000 performs the following processing:

- 1. Determine whether the VLAN ID is 100, and if yes, enter the QinQ processing logic.
- 2. Check whether there is no inner VLAN ID from parsed packets, and if yes, discard the packets.

As a result, packets from the client with a single VLAN tag (VLAN ID = 100) cannot be forwarded. After the VLAN ID is changed to a value other than 100 and 101, packets from the client can be forwarded normally.

Configuration example

Configuration Steps

Enable QinQ VLAN tag termination on the core switch and configure the PE-VLAN/CE-VLAN.

```
SwitchA#configure terminal
Enter one configuration command in each line, ended with CNTL/Z.
Ruijie(config)#qinq termination pe-vlan 100-101
Ruijie(config)#qinq termination ce-vlan 200 to 300
```

Verification

Ruijie(config)#show qinq termination CE-VLAN: 200-300 PE-VLAN: 100 and 101

4.1.6.2 [Mandatory] Transparent Transmission of RADIUS Packets in QinQ Format

Principles:

The configuration of NAS-port-ID encapsulation format for RADIUS packets is mandatory in QinQ isolation scenarios in simplistic networks. RADIUS packets are encapsulated in a format that combines the interface name of the client and the inner and outer VIDs in a specified manner. SAM+ reads dual VLAN IDs based on the **nas-port-id** field.

Configuration

commands:

radius-server attribute nas-port-id format qinq //Configured in global configuration mode.

Precautions:

This function is mandatory in QinQ isolation scenarios.

Configuration example

Ruijie(config) # radius-server attribute nas-port-id format qinq

4.1.7 Anti-Loop Configuration for Simplistic Networks

4.1.7.1 [Mandatory] Anti-Loop Configuration on the Core Device

- 1. By default, the Rapid Link Detection Protocol (RLDP) is enabled on the core device RG-N18000 of N18000_RGOS 11.0(1)B3P1 and later versions, to generate alarms for VLAN loops and make records. Therefore, do not disable RLDP.
- 2. Pay attention to RLDP loop logs.
- 3. Run the show rldp log command to display relevant logs.

4.1.7.2 [Mandatory] Anti-loop Configuration on Access Devices

1. Configure the Spanning Tree Protocol (STP) on the access device to assist RLDP loop prevention. Enable the Rapid Spanning Tree Protocol (RSTP) globally, and enable BPDU filter on the uplink interface of the access device, and BPDU guard on the downlink interface. Example:

| S2928-student(config)#spanning-tree | //Enable STP. |
|---|---|
| S2928-student(config)#spanning-tree mode rstp | //Enable RSTP, to prevent low convergence |
| speed of interfaces. | |

S2928-student(config)#spanning-tree portfast bpduguard default //BPDU guard is enabled on PortFast interfaces by default. S2928-student(config)#int ran gi 0/1-23

S2928-student(config-if-range)#spanning-tree portfast //PortFast is enabled on the downlink interface and BPDU guard takes effect on the downlink interface. Once BPDU packets are received, the system considers that a loop occurs. Therefore, disable the downlink interface. S2928-student(config-if-range)#interface gi0/24

S2928-student(config-if- GigabitEthernet 0/24)#spanning-tree bpdufilter enable //Enabl e BPDU filter on the uplink interface, which does not send BPDU packets to external devices, so that no topology is established and no root bridge is elected, and loops are prevented on a single device.

S2928-student(config-if-AggregatePort 1))#exit

4.1.8 RG-N18000 Optimization Functions

4.1.8.1 [Optional] Fast Packet Capture

Note: This function is supported only in N18000_RGOS 11.0(1)B3P3.

Principles:

If the packet sending/receiving fails or an exception occurs during routine maintenance, you can specify the packet capture point, direction, as well as packet characteristics. Then, start packet capture and check whether packets are transmitted to/from the device to pinpoint the cause for the failure.

Configuration commands:

1. Create a packet capture rule.

```
packet capture rule rule-name [src-macsmac] [dst-mac dmac] [etype type | ip |arp ]
[src-ip sip sip-mask] [dst-ip dip dip-mask] [src-ipv6 sipv6 sipv6-prefix] [dst-ipv6 dipv6
dipv6-prefix][protocol protocol |tcp | udp] [src-port sport ] [dst-port dport]
```

2. Specify the packet capture point.

```
packet capture point capture-point-namerule rule-name location {interfaceinterface-name
| vlan vlan-id | control-plane} {in | out | both}
```

3. Enable/Disable the packet capture rule.

packet capture {start | stop}

Precautions:

- 1. This function is not risky theoretically. Nevertheless, it is not recommended to use it in service peak hours and non-fault cases. If the packet capture period is set to XX minutes in the software, the software stops packet capture after the period expires.
- 2. If the packet capture rate is higher than the data write speed of the device, packets cannot be completely written into the device. It is recommended to configure more accurate packet capture matching rules. The system CPU supports a packet capture rate up to 1000 pps in idle hours and 600 pps when the CPU usage is 65%. If the system CPU usage exceeds 70% (including 70%), packet capture is not started even if it is configured.

Configuration example

1. The following example captures the RADIUS authentication packets exchanged between a client (100.0.30.77) and SAM+ and those exchanged between the RG-N18000 (192.168.3.1) and SAM+.

Captured RADIUS packets need to be saved in the **tmp** directory (or the **usb0** directory in actual application). This directory does not need to be copied.

```
packet capture rule testdown filter ipv4 sip 100.0.30.77 0.0.0.0
packet capture rule testup filter ipv4 sip 192.168.3.1 0.0.0.0 v4 protocol udp ipv4 dport eq
1812
packet capture point testup rule testup location interface gigabitEthernet 1/1/2 both
packet capture point testdown rule testdown location interface gigabitEthernet 1/1/15 both
packet capture file tmp://test.pcap
packet capture file usb0://test.pacp ?
buffer-size Buffer size of packet info //Define the size of the file for storing captured
packets. The default size is 2 MB.
packet-num Number of packets
                                  //Define the number of packets to be captured. The default
value is 1024.
timeout
           Timeout of minutes //Define the packet capture duration. The default value
is 10 min.
packet capture start
show packet capture status
packet capture stop
```

| N18014#show packet capture status |
|---|
| Capture rules: Capture rules testdown: Etype: 0x0800 Source IP: 100.0.30.77 Capture rules testup: Etype: 0x0800 Protocol: 0x11 Source IP: 192.168.3.1 Destination port: 1812 |
| Capture points: Capture point testdown: Capture rules: testdown Location: Gi1/1/15 Direction: all Packets captured(all): 28 Capture point testup: Capture rules: testup Location: Gi1/1/2 Direction: all Packets captured(all): 2 |
| Capture file: Filename: /tmp///test.pcap Buffer size: 2(MB) |
| Capture Statistic: Status: running Start time: 2017-6-28 7:4:14 Timeout: 10(minutes) Packets limit: 1024 Write file packet count: 30 |

2. The screenshot below shows the ping packets sent by the client (100.0.30.77) and RADIUS packets sent by the device.

| 192.168.3.1 | 192.168.1.13 | RADIUS | 5 26/ ACCESS-REQUEST(1) (10=1, 1=225) |
|-------------|--------------|--------|--|
| 100.0.30.77 | 100.0.0.1 | ICMP | 74 Echo (ping) request id=0x0001, seq=245/62720, ttl=6 |
| 192.168.3.1 | 192.168.1.13 | RADIUS | <pre>S 267 Access-Request(1) (id=1, 1=225)</pre> |
| 100.0.30.77 | 100.0.0.1 | ICMP | 74 Echo (ping) request id=0x0001, seq=246/62976, ttl=0 |
| 100.0.0.1 | 100.0.30.77 | ICMP | 74 Echo (ping) reply id=0x0001, seq=246/62976, ttl=6 |
| 100.0.30.77 | 100.0.0.1 | ICMP | 74 Echo (ping) request id=0x0001, seq=247/63232, ttl=0 |
| 100.0.0.1 | 100.0.30.77 | ICMP | 74 Echo (ping) reply id=0x0001, seq=247/63232, ttl=0 |
| 100 0 20 22 | 100 0 0 1 | TOMO | 74 Echo (pipa) provinct id 000001 cpg 340/63400 ++1 6 |

3. If the captured packets are stored in the **TMP** directory, you can run the following commands to copy them to another directory:

```
Ruijie#run-system-shell
```

```
cd /tmp
```

/tmp # mv xxx.pacp /tmp/vsd/0/ xxx.pacp

Start the TFTP software on the client and run the commands to copy information about captured packets to the client.

copy tmp:/xxx.pacp tftp://xxx.xxx.xxx.xxx/xxx.pacp //Select oob tftp for the MGMT port.

4.1.8.2 Analysis of VSL Traffic Faults in the Case of One-to-Many Mirroring

Basic information

Y Fault symptom

On-site topology:



A customer mirrors the egress traffic to multiple servers in one-to-many mode. Two 10 Gbps VSLs are configured but the interface traffic of one VSL is about to reach the limit.

Y Fault analysis

1. Possible causes

With one-to-many mirroring, the traffic of the MAC self-loop port is flooded to a VSL via remote VLAN. There is no measure for balancing the layer-2 traffic flooded to the VSLs.

2. Cause locating

The traffic of one VSL is about to reach the limit, that is, 10 Gbps. Data is transmitted from RG-N18000 2 to RG-N18000 1.

It is found that the traffic in the inbound direction of RG-N18000 2 is not heavy but the traffic of the mirroring self-loop port is about 10 Gbps.

The self-loop port belongs to VLAN 1581.

3. Detailed analysis

a. Related configuration

```
vlan 1581
name_VLAN student egress remote mirroring
remote-span
!
interface TenGigabitEthernet 2/7/3
```

description to- mirroring port

switchport access vlan 1581 spanning-tree bpdufilter enable ip dhcp snooping trust nfpp arp-guard enable nfpp icmp-guard enable I interface TenGigabitEthernet 2/7/4 description to- destination mirroring port- source ten2/7/7&2/7/1 no mac-address-learning switchport access vlan 1581 ip dhcp snooping trust mac-loopback

```
!
```

!

interface TenGigabitEthernet 2/7/8 description link_to_ASME1000_moniter no mac-address-learning switchport mode trunk switchport trunk native vlan 1581 switchport trunk allowed vlan only 1581

monitor session 4 remote-source monitor session 4 destination remote vlan 1581 interface TenGigabitEthernet 2/7/4 switch monitor session 4 source interface TenGigabitEthernet 2/7/7 both

b. Principle analysis

One-to-many mirroring is configured on the RG-N18000, to mirror the traffic of the outbound port Te2/7/7 to port Te2/7/3 and port Te2/7/8.

- λ Create remote VLAN 1581 on the device.
- λ Specify the device as the RSPAN source device, configure the outbound port Te2/7/7 as the mirroring source port. Select a down port (port Te2/7/4) as the mirroring output port, add the port to the remote VLAN, and configure MAC self-loop by running the mac-loopback command in interface configuration mode.
- λ Add port Te2/7/3 and port Te2/7/8 to the remote VLAN.

In this scenario, the traffic of the VLAN is flooded to all chips. The traffic of the MAC self-loop port is flooded to the VSL port regardless of whether RG-N18000 1 has a port included in VLAN 1581.

Solution

1. Optimization solution

a. Increase the VSL bandwidth.

Change the VSL port to 40G port. Line cards with 40G ports include 16XS2QXS-BD.



For one-to-many mirroring requirement, a layer-2 switch can be added to mirror the traffic of the mirroring source port to the layer-2 switch in one-to-one mode, and then the layer-2 switch floods the traffic to multiple destination ports over the same VLAN on the layer-2 switch.


Note: In the topology above, the source ports are Ten 2/7/7 and Ten 1/7/1, and the destination port is AP 1.

Configuration steps:

- = Add port Ten 1/7/1 and port Ten 2/7/1 of RG-N18000 1 to AP 1.
- Configure local mirroring on the RG-N18000, and specify port Ten 2/7/7 and AP1 as the source port and destination port of mirroring respectively.
- = Add port Ten 0/1 and port Ten 0/2 of the S6220 to AP 1.

Add AP1, port Ten0/3, and port Ten0/4 of the S6220 to VLAN 100.

RG-N18000:

```
Ruijie# configure
Ruijie(config)#interface aggregatePort 1
Ruijie(config-if-AggregatePort 1)#exit
Ruijie(config)#interface tenGigabitEthernet 1/7/1
Ruijie(config-if-TenGigabitEthernet 1/7/1)#port-group 1
Ruijie(config)#interface tenGigabitEthernet 2/7/1
Ruijie(config-if-TenGigabitEthernet 2/7/1)#port-group 1
Ruijie(config)# monitor session 1 source interface tenGigabitEthernet 2/7/7
Ruijie(config)# monitor session 1 destination interface aggregatePort 1
S6220:
Ruijie(config)#interface aggregatePort 1
Ruijie(config)#interface aggregatePort 1
Ruijie(config-if-AggregatePort 1)#switchport access vlan 100
Ruijie(config-if-AggregatePort 1)#exit
```

Ruijie(config)#interface tenGigabitEthernet 0/1
Ruijie(config-if-TenGigabitEthernet0/1)#port-group 1
Ruijie(config)#interface tenGigabitEthernet 0/2
Ruijie(config)#interface tenGigabitEthernet 0/3
Ruijie(config)#interface tenGigabitEthernet 0/3)# switchport access vlan 100
Ruijie(config)#interface tenGigabitEthernet 0/4
Ruijie(config-if-TenGigabitEthernet 0/4)# switchport access vlan 100

Thorough solution

N/A

4.2 SAM+ and ePortal Configuration

4.2.1 [Optional] Wired RG-N18000—802.1X Authentication

4.2.1.1 Adding the RG-N18000 on SAM

4.2.1.1.1 Function requirements

Add the NAS (RG-N18000) on SAM+.

4.2.1.1.2 Configuration key points

The NAS-relevant parameters added on SAM+ must be consistent with the actual settings of the NAS. Otherwise, an authentication exception occurs.

- The address for the RG-N18000 to interwork with SAM+ must be correct on SAM+. For example, if the source port for communicating with SAM+ is configured on the RG-N18000 by running the **ip radius source-interface loopback 0** command, the IP address of the loopback0 interface of the RG-N18000 needs to be entered in the **Device IP Address** column of SAM+.
- The key for interworking with the RG-N18000 needs to be consistent.
- The SNMP community for interworking with the RG-N18000 needs to be consistent.

4.2.1.1.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose System > Device Management.

| | MANAGEMENT SYSTEN Homepage | 1 System | Security | User | Access Control | Billing | Account | Operation | |
|--|-------------------------------|---|--|--------|----------------|-------------|------------|---------------|--------|
| Location: Operation > Online User Username User IP(v4) | Full Name User Temp te | System Se Authentic Billing Set LDAP Con | ettings ation Settings tings figuration | | € General S | earch Sea | rch Adv | vanced Search | |
| | C | Self-confi Custom Fi Device Ma IP Manage | guration ield anagement ement | ers Of | fline Delete t | he Selected | Delete All | Show the B | s t |
| There were no results found. Column (| Config | Blacklist N | /lanagement | | | | | | |
| Username Us | er IP(v4) | Region M | anagement | v4) | NAS Por | t Servi | ce | Access | 5 |
| Invalid wireless user internet traffic block | kage | Certificate Guest Mo | e Management de | | | | | | |
| | | | | | | | | | |

3. Click **Add** to add a device.

| SAM ⁺ security accounting man | AGEMENT SYSTE | м | | | | | |
|--|---------------|-------------|-----------|-------------|----------------------|----------|-------------------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account |
| Location: System > Device Management | | | | | | | |
| Device IP Address | | Device Type | Please Se | lect | T | 🕑 Gene | ral Search |
| There were no results found. Column Conf | Add | Batch | Add Ser | nd Notifica | tion to the Selected | Send | Notification to A |
| Device IP Address | D | evice Type | | Ma | del | Device G | roup |
| | | | | | | | |

4. Set NAS-relevant parameters and ensure that the key parameters are consistent with the actual settings of the NAS. Then, click **Save**.

| SAM ⁺ security accounting | G MANAGEMENT SYSTEM | ٨ | | | | | |
|--------------------------------------|-----------------------|--------------|----------------|-------------|-----------------------|---------|------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | , |
| Location: System > Device Managen | nent > Add | | | | | | |
| Device | | | | | | | |
| Device IP Address* | 192.168.54.98 | | | | | | IP T |
| Device Type* | Ruijie Switch | T | | | | | Мо |
| PPPoE Authentication Domain | | Please us | e comma or sp | pace to se | oarate multiple dom | ains | IPO |
| Device Key* | key | | | | | | Cor |
| MAC Addresst | | For truste | d ARP binding | g applicati | on, MAC address mu | ist be | CNU |
| MAC Address* | filled | | | | | | SINI |
| DHCP Login Username | | | | | | | DH |
| Telnet Login Username | | | | | | | Telı |
| Telnet Privileged Password | | | | | | | Dev |
| Device Name | | | | | | | Dev |
| Device Timeout (secs)* | 3 | | | | | | Dev |
| Device Feature | Re-authentication | Account | Update 🔲 C | lient Dete | ction | | Are |
| Web Authentication Option | Select this to enable | le the web a | uthentication | for the sw | itch | | RG |
| Integration Port(1~65535) | | | | | | | Des |
| SU Version Check | 🕑 Enable (Applicable | to authentio | ation client + | access sw | itch authentication r | node) | N18 |

• If "Other Non-Ruijie Authentication Device" is selected as the "Device Type", only the username and password will be verified without full support of SAM but meet the RADIUS standard.

• If the RGAC + Passthrough solution is implemented and the switch model is not higher than S21XX or S26XX, please make sure t

4.2.1.1.4 Verification

1. Check whether the SAM+ server can ping the device successfully. If yes, it indicates that their communication is normal (ensure that ping packets are not intercepted by the firewall).

4.2.1.2 Access Control Configuration

4.2.1.2.1 Function requirements

Configure access control to restrict Internet access behavior of users.

4.2.1.2.2 Configuration key points

The Internet access behavior of access users needs to be confirmed with customers and access control needs to be configured based on actual conditions.

4.2.1.2.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose Access Control > Access Control.



3. Click Add to add access control.

| SAM ⁺ security accounting man | AGEMENT SYSTEM | A | | | | | | | |
|---|----------------|------------|-----------|--------|-------------------|---------|-----------------|-----------|-------------------------------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | l. |
| Location: Access Control > Access Control | | | | | | | | | |
| Access Control Name |] | 🕑 Genera | al Search | Search | | | | | |
| | | | | | Add | Del | ete the Selecte | d | |
| | | | | | | | | | |
| Total of 1 records, the currently displayed 1 t | to 1 records | | | | | | | | |
| Access Control Name | | Public Ser | vice | | Access Control | Туре | | | Description |
| default | | No | | | default access co | ontrol | | | System Default Access Control |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

4. On the **Access Control Information** tab page, enter the access control name, for example, "dot1x", and set other parameters based on actual conditions.

| SAM ⁺ security accounting | 5 MANAGEMENT SYSTE | м | | | | | |
|--|-------------------------|----------------|---------------|---------------|---------------------|---------------|---------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Ac |
| Location: Access Control > Access C | ontrol > Add | | | | | | |
| Access Control Information Use | er Information Check | Network Us | age Control | Public Se | rvice User Behav | ior Control | VPM |
| Access Control Name * | dot1x | | | | | | |
| Concurrent Logins Limit(0 to 99) 0 means no limit * | 1 | | | | | | Syr |
| According to the Terminal Type | Concurrent Logins (1 to | o 99 times) | | | | | |
| | 🗹 Display accountin | g policy info | mation when | user onlin | e | | Au |
| | Show users on-lin | e access con | trol time | | | | Acc |
| Gateway Access Restriction | It does not allow | traffic throug | h the gatewa | y server (ga | ateway device needs | to be deplo | oyed li |
| Export linkage strategy | | * non | NPE / EG gat | eway billin | g model deploymer | nt, no need t | to cont |
| Firewall Policy | | * not | deploy firewa | ills linkage, | the need to configu | ure | |
| Description | | | | | | | |

* Please refer to respective label content for access details

5. On the **User Information Check** tab page, select **Wired 1X Access** and configure whether to bind accounts with IP/MAC addresses based on actual conditions. Then, click **Save**.

| S | | G MANAGEMENT SYSTEM | | | | | 음 adm |
|----|------------------------------------|----------------------------|----------------------|-------------------------|-------------------------|---|---------|
| Sł | nortcut Channel 🔅 | Homepage Syst | em Security U | ser Access Control | Billing Account | Operation | |
| L | ocation: Access Control > Access C | ontrol > Add | | | | | |
| | Access Control Information | er Information Check Netwo | rk Usage Control Pub | olic Service User Behav | vior Control VPN Contro | Client Version Management Wireless Access Pro | perties |
| | Allowed Access | Access Mode Verifi | cation Information | | | | |
| | FIAGrad 1V Access | User IP(v4) | User IP(v6) | User MAC | NAS IP(v4) | NAS IP(v6) NAS Port | |
| | Wiled TA Access | VLAN | Internal VLAN | External VLAN | Access IP Type Static | Ŧ | |
| 1 | Wired Web Portal Access | User IP(v4) | User MAC | Web Authenticatio | on Device IP(v4) | Web Authentication Device Port | |
| | Winders 1V Access | User IP(v4) | User MAC | NAS IP(v4) | AP MAC | SSID | |
| | Willeless IX Access | Access IP Type | itatic 💌 | | | | |
| | CWireless Web Portal Access | User MAC | NAS IP(v4) | AP MAC | SSID | | |
| | Smart Device 1X Access | User MAC | NAS IP(v4) | AP MAC | SSID | | |
| | INAC East Assess | User MAC | NAS IP(v4) | AP MAC | SSID | NAS Port | |
| | MAC Fast Access | VLAN | Internal VLAN | External VLAN | | | |
| | (B)AGrad Ctransford Destal Assess | User IP(v4) | User MAC | INAS IP(v4) | NAS Port | VLAN | |
| | writeu Stanuard Portal Access | Internal VLAN | External VLAN | | | | |
| | Wirelace Standard Portal Access | User IP(v4) | User MAC | NAS IP(v4) | AP MAC | SSID | |

4.2.1.2.4 Verification

Verify that access control is added successfully.

| SAM ⁺ security accounting management s | YSTEM | | 🐣 admin 丨 😰 About |
|--|-------------------------|--|----------------------------------|
| Shortcut Channel 🌵 Homepa | ge System Security User | Access Control Billing Account Operation | |
| Location: Access Control > Access Control | | | |
| Access Control Name | General Search Search | | |
| | | Add Delete the Selected | |
| Total of 1 records, the currently displayed 1 to 1 records | | | Currently 1 /1Page 👾 🐨 Very Page |
| Access Control Name | Public Service | Access Control Type Description | Modify Check |
| 🗐 default | No | default access control System Defa | ult Access Control |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |
| | | | |

4.2.1.3 Billing Policy Configuration

4.2.1.3.1 Function requirements

Configure billing policies based on billing requirements of access users, to pay for Internet access.

4.2.1.3.2 Configuration key points

Billing requirements of access users need to be confirmed with customers and billing policies need to be configured based on actual conditions.

4.2.1.3.3 Configuration steps (monthly milling)

- 1. Log in to the SAM+ management page.
- 2. Choose **Billing** > **Billing** Policy.

| SAM ⁺ security accounting man | AGEMENT SYSTEM | | \Lambda admin 🗗 |
|---|--|--|--|
| Shortcut Channel | Homepage System Security User Access Cont | ol Billing Account Operation | |
| 900 Health Score Oisk Space Check 3rd Party Development Interface Local License Monitoring Internet Traffic Receive Channel Internal Storage Check | Total Online Users O Account Number 1 License Number Unlimited SAM Server Monitoring CPU T% Memory 2587/MB / 4095/MB (63%) | Average Authentication Performance 0 Current Performance (User/s) 0 Buffer 0.00% (0 / 1.000) | Average Accounting Performance Current Performance (User/s) Buffer Disk Input 0 B/s Disk Output 0 B/s Disk V/O 0 B/s |
| | Packet Handling Report (24Hrs) | | Authentication Packets |

3. Select Monthly Billing Policy and click Add.

| SAM ⁺ security accounting many | AGEMENT SYSTEM | | | | | | | | | |
|---|----------------|----------|---------------|---------------|---------------------|-----------|-----------------|-----------|---------------------|-----|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | | |
| Location: Billing > Billing Policy | | | | | | | | | | |
| Billing Policy Name | | 🗹 Gener | al Search | Search | | | | | | |
| | | Pleas | se select the | billing polic | y which you want to | o add Mor | thly Billing Po | oli ▼ Add | Delete the Selected | |
| There were no results found. | | | | | | | | | | (a |
| Billing Policy Name | | Descript | tion | | | | | | | Moo |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

4. Enter the billing policy name, for example, "dot1x", set **Period Type** to **30 Days** or **Month**, and set **Rate (MYR)**, for example, 30 Yuan/month. Then, click **Save**.

| SAM ⁺ security accounting | G MANAGEMENT SYSTEM | | | | | | | | | |
|--|---|------------------------|---------------|--------------|----------------------|----------------|-----------------|--------------------------|-----------------------|---------------------------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | | |
| Location: Billing > Billing Policy > / | Add > Add Monthly | | | | | | | | | |
| Monthly Billing Policy | | | | | | | | | | |
| Billing Policy Name* | |] | | | | | Description | | | |
| Period Type* | 30 Days Month | | | | | | Ending Date | | Enable | (1-31) |
| Compensation | The remaining days | during accou | nt suspensio | in can be i | used after recovery | | Rate (MYR)* | | | |
| Authentication Related Options | Allow login when th internet traffic billing p | ere is no rem Han.) | aining intern | et traffic o | or the account has u | npaid charg | es. (Must use | the NTD penetration me | ode with access co | ntrol or ACE device. Must |
| Advances Options | Monthly Payment for | or Limited Du | ration/ Mont | hly Payme | nt for Limited Inter | net Traffic/ M | Monthly Paym | ent for Limited Authent | ication Device Traf | fic Configuration |
| • Monthly | / charge: charges extend t | o the next me | onth. For exa | mple, if th | e user creates the a | ccount and | paid for the se | rvices on the 6th this m | nonth, the fee will b | e charged again on the 6 |
| | | | | | | Save | Return | | | |
| | | | | | | | | | | |

4.2.1.3.4 Verification

Verify that the billing policy is added successfully.

| SAM ⁺ security accounting main | NAGEMENT SYSTEM | M | | | | | | |
|---|-----------------|---------|---------------|---------------|---------------------|---------|------------------|-----------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation |
| Location: Billing > Billing Policy | | | | | | | | |
| Billing Policy Name | | 🕑 Gener | ral Search | Search | | | | |
| | | Plea | se select the | billing polic | y which you want to | add Mor | nthly Billing Po | oli ▼ Add |
| There were no results found. | | | | | | | | |
| Billing Policy Name | | Descrip | tion | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

4.2.1.4 User Template Configuration

4.2.1.4.1 Function requirements

Configure user templates based on user attributes for later account creation.

4.2.1.4.2 Configuration key points

It is recommended to classify user templates with the same attribute into a group and give concise and intuitive names to the templates, for example, student monthly billing template or teacher monthly billing template.

4.2.1.4.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose User > User Template.

| SA | M ⁺ security accounting ma | NAGEMENT SYSTE | м | | | | | |
|-------|---------------------------------------|----------------|--------|----------|------|----------------|---------|---------|
| Short | cut Channel 🌼 | Homepage | System | Security | User | Access Control | Billing | Ac |
| Locat | tion: User > User Template | | | | | | | |
| | | | | | | | | |
| | | | | | | Add | De | lete th |
| | Template Name | | | | | | | |
| | default | | | | | | | |
| | Classroom Default Template (Do No | t Delete) | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

3. Click Add.



4. In the **Add User Template** dialog box, enter the template name, for example, "dot1x", and click **Save**.

| 0 | Add User Template |
|---|------------------------------|
| User Templates Template Name* Custom Options Monthly Modification Limit (1~10 times) Description | Allow self-change plan 10 |
| | Save |

4.2.1.4.4 Verification

Verify that the user template is added successfully.

| SAN | Λ^+ security accounting mana | GEMENT SYSTE | ٨ | | | | | | | |
|--------------------------|---|------------------|-------------|----------------|---------------|-----------------------|---------------|--|--|--|
| Shortcut | Channel 🔯 | Homepage | System | Security | User | Access Control | Billing | | | |
| Location | Location: User > User Template > User Templates | | | | | | | | | |
| Temp Self-M Descri | late Name: dot1x Modification Option : Not allowed | to change the p | lan | | | Us | er Template: | | | |
| | Plan | | _ | | _ | | _ | | | |
| | | A | cess Area | De | efault Rule | Service | | | | |
| 1 | The number of repeated logins of the p | olan is user's n | naximum nur | nber of online | e STAs. | | | | | |
| U | Users can use different services for Inte | ernet access and | the number | of online use | rs of the san | ne service is restric | ted by the nu | | | |

4.2.1.5 User Plan Configuration

4.2.1.5.1 Function requirements

Configure a user plan to cover access limits of authenticated users, including the area, time range, access control, and billing policy. A user plan is akin to a phone service package.

4.2.1.5.2 Configuration key points

A plan covers all control options and fees for access users. Be sure to clearly confirm plans with customers before configuration.

4.2.1.5.3 Configuration steps

1. In the configured user template "dot1x", click Add Plan.

| SAM ⁺ security accounting man | AGEMENT SYSTEM | м | | | |
|---|---|---|-----------------------------------|--|---------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Acces |
| Location: User > User Template | lates I to change the p | lan | | | |
| Add Plan Add Plan Users can use different services for Intervices | Ad plan is user's n ternet access and | ccess Area naximum nur I the number | Dunber of online of online use | efault Rule e STAs. rs of the sa | me serv |

2. Enter the plan name, for example, "dot1x", select a configured billing policy or **Not Charging** based on actual requirements, and then click **Save**.

| an | |
|---------------------------------|-----------------------------------|
| Plan * | |
| Concurrent Logins Limit | 🗹 Enable 1 (1 ~ 99 times) |
| Billing Policy | Not Charging |
| Cycle expired and suspend user. | Activate |
| MAC Binding Validity | 0 (0-365 days, 0 for not limited) |
| Description | |
| | |
| | |
| Cava | Cancal |
| Save | Cancer |

Click Modify Plan and modify the access area, access time range, access control, and billing mode. 3.

| Shortcu | t Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account |
|------------------------------------|---|--|-------------|----------------|------------------------|----------------------|----------------|--------------|
| Locatio Temp Self-I Desci | n: User > User Template > User Tem plate Name: dot1x Modification Option : Not allow ription: | uplates ed to change the | plan | | | U | ser Templates | : dot1x 🗖 |
| | Plan | | Acces | s Area | Default I | Rule S | ervice | Allo |
| | Name:dot1x Concurrent Logins Limit :1 Billing Policy:Not Charging Cycle Expired to Suspend User.:N Modify Plan Delete Plan | ot Enabled | Unlimited | | o | default | | Unlimited |
| | The number of repeated logins of the Users can use different services for | ne plan is user's Internet access a | maximum nur | mber of online | STAs. rs of the sar | me service is restri | cted by the nu | mber of repe |

4. Modify the rule based on actual conditions. The figure below shows that the access area of authenticated users is unlimited, access control is set to "dot1x", the access time range is unlimited, and billing is performed based on the plan "dot1x".

O Modify Plan

| an | |
|---------------------------------|-----------------------------------|
| 'lan * | dot1x |
| Concurrent Logins Limit | 🖉 Enable 1 (1 ~ 99 times) |
| Billing Policy | Not Charging 🔻 |
| Cycle expired and suspend user. | Activate |
| WAC Binding Validity | 0 (0-365 days, 0 for not limited) |
| Description | |
| | |
| | |
| Save | Cancel |

4.2.1.5.4 Verification

Verify that the plan meets customer requirements.

| Sh | ortcut | t Channel 🛛 🏟 | ł | | Homepage | System | Security | User | |
|----|-------------------------|--|---|---|------------------------|--------------------|--------------------------|-----------------------|------|
| Lo | ocatio | n: User > User | Template | • > User Templat | es | | | | |
| | Temp Self-N Descr | olate Name: Modification C ription: | Option : | dot1x Not allowed to | o change the | plan | | | |
| | | | | Diam | | | _ | _ | |
| | | | | Plan | | | | | _ |
| | | | | | | Acces | s Area | Default | t R |
| | | Name:dot1x Concurrent L Billing Policy Cycle Expired Suspension I MAC Binding Description: | ogins Lin V:Not Char d to Suspe End Time: g Expiry:0 | n it : 1 ·ging end User.: Not Ei Day | nabled | Acces Unlimited | s Area | Default o | |
| | | Name:dot1x Concurrent L Billing Policy Cycle Expired Suspension I MAC Binding Description: The number o | Logins Lin y:Not Char d to Suspe End Time: g Expiry:0 f repeated | n it : 1 rging end User.: Not Er Day I logins of the pl | nabled an is user's | Acces Unlimited | s Area nber of online | Default © STAs. | t Ri |

4.2.1.6 User Group Configuration

4.2.1.6.1 Function requirements

Add authenticated users with the same attribute to the same group, and define a response user template and plan for the user group to prepare for later account creation.

4.2.1.6.2 Configuration key points

It is recommended to group access users by attribute, for example, group users on campus networks into "student user group" or "teacher user group".

4.2.1.6.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose User > User Group.

| SAI | M^+ security accounting management syst | тем | | | | | |
|---------|---|-----------|----------|---------|-----------------------|---------------|-------------|
| Shortcu | t Channel 🌵 Homepage | System | Security | User | Access Control | Billing | Account Ope |
| Locatio | n: User > User Template > User Templates | | | User M | anagement | | |
| | | | | | Pre-cancelled Account | | |
| | | | | User G | roup | er Templates: | dot1x 😺 |
| Tem | plate Name: dot1x | | | User Te | emplate | | |
| Desc | ription: | e plan | | Traffic | Control Policy | | |
| | Dian | | _ | Guaran | tor and Guest | | |
| | Fiaii | Access | s Area | Dealar | ne Deller | rvice | Allow Acce |
| | Name:dot1x | | | Real-na | ame Policy | | |
| | Concurrent Logins Limit :1 | | | Real-na | ame System | | |
| | Billing Policy:Not Charging Cycle Expired to Suspend User.:Not Enabled | Unlimited | | MAC A | uthentication | | Unlimited |
| | Suspension End Time: | | | Auto P | re-cancellation | | |

3. Click Add.

| SAM ⁺ security accounting m | ANAGEMENT SYSTE | м | | | | | |
|--|-----------------|--------------------------------|---------------|--------|----------------------|-----------------|----------------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account |
| Location: User > User Group | | | | | | | |
| Expand All Collapse All | | Change User | Group | | | | |
| M User Group | | User Group * | | root | | | |
| | | Default User 1 Uplink Speed | 「emplate* | defaul | t 🔻 | | |
| | | (8~261120KB | ps) | 0 | | | |
| | | User group au | uthentication | | | | |
| | | Description | iopinks. | Root | Jser Group | | |
| | | | | 🖉 Sync | hronize the update d | lefault user te | emplate or pla |
| | | | | Please | perform system oper | ration when i | dle.) |
| | | | | | | | |
| | | | | | | | |

4. Enter the user group name, for example, "dot1x", and select the default user template and default plan. Then, click **Save**.

| User Group * | dot1x | Parent Group Na |
|---------------------------|---------|-----------------|
| Default User Template* | dot1x 🔻 | Default Plan* |
| Uplink Speed | | Downlink Speed |
| (8~261120KBps) | 0 | (8~261120KBps) |
| User group authentication | | Downlink Speed |
| is successful hoplinks. | | (8~261120KBps) |
| Description | | Creator |

4.2.1.6.4 Verification

Verify that the user group is added successfully.

| SAIN' SECURITY ACCOUNTING MAN/ | AGEMENT SYST Homepage | EM System | Security | User | Access Control | Billing | Account | Operat |
|--------------------------------|--------------------------|---|--|------|---------------------------------------|---------|---------|--------|
| Location: User > User Group | | | | | | | | |
| User Group | | Add User Group * Default User ⁻ Uplink Speed (8~261120KB User group at is successful H Description | Template* ps) uthentication noplinks. | 0 | · · · · · · · · · · · · · · · · · · · | | Sa | ve |

4.2.1.7 Account Creation

4.2.1.7.1 Function requirements

Create accounts in the SAM+ system.

4.2.1.7.2 Configuration key points

- 1. The account creation process generally requires users to go to business halls and apply for accounts by using their ID cards.
- 2. Accounts with the names same as those on their ID cards are registered during account creation.
- 3. A user group and a user template need to be selected during account creation as planned.

4.2.1.7.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose User > User Management.

| SAM ⁺ security accounting main | NAGEMENT SYSTEM | | | | | | | |
|---|-----------------|-------------|--------|----------------------|------------|---------|-----------|----------------|
| Shortcut Channel 🌼 | Homepage Sy | ystem Secur | ity Us | er Access Contr | ol Billing | Account | Operation | |
| Location: User > User Management | | | Us | er Management | | | | |
| User Search | User Search 🍄 | | Pr | e-cancelled Account | | | | |
| langest Course | | | Us | er Group | | | | |
| Import search | Username | | Us | er Template | | 0 | | Multiple Userr |
| | Account | | Tr | affic Control Policy | | | | |
| Create Account | | | Gu | arantor and Guest | | | | |
| Batch Account Activation | Balance | | Re | al-name Policy | | | | |

3. Click Create Account in the left pane.

| SAM ⁺ security accounting man | IAGEMENT SYSTEM | |
|--|----------------------------------|--|
| Shortcut Channel 🔅 | Homepage System Securit | ty User Access Control Billing Account O |
| Location: User > User Management | | |
| User Search | User Search 🄯 | |
| Import Search | Username | |
| Create Account | Account | |
| Batch Account Activation | Balance User Templates | Please Select |
| Import Accounts | Plan | Please Select |
| Import Changes | Billing Policy | Please Select |
| Import Payments | User Group | 🙀 📩 Contains The Child User Gr |
| Import Change User Templates and | Account Creation Source | Please Select |
| Plans | Recent Offline Duration | Recently I Week Inactive Network Users Within This |
| import change over broup | | 📄 from 🔄 🥅 🥅 Inactive Network Users From |
| | Pause Duration | |
| | Last Self-service Pause Duration | n 🔄 📅 🗖 - |

4. Enter the username and password, select a user group, user template, and plan. Then, click **Save**.

| Username* | dot1x | Full Name |
|----------------------------------|--|------------------------------------|
| Password* | **** | Confirm Password* |
| User Group* | dot1x | Account |
| User Templates | Use Default Template of User Group Plan: d | lot1x Billing Policy: Not Charging |
| Self-service Permission | All Self-service Privileges | Authentication-free |
| Auto Pre-Cancellation | | BACL |
| User Status | Normal | Pause Duration |
| Last Self-service Pause Duration | | Next Available Self-service Paus |
| Guarantor Ranking | | |
| Advanced Options | Show Advanced User Settings options | |
| Sex | | Email Address |
| ID Type | | ID No. |
| Education Level | | Online Information |
| Telephone No. | | Mobile Phone |
| Address | | Postal Code |
| Create Time | 2018-05-08 14:06:02 | Last Update |
| Creator | admin | |

4.2.1.7.4 Verification

1. In the left pane of the **User Management** page, click **User Search**. In the displayed right pane, click **Search**. The added user is displayed.

| SAM ⁺ security accounting main | NAGEMENT SYSTEM | | | | | | |
|---|------------------------|-------------|-----------------|-----------------|--------------|----------------|-----------|
| Shortcut Channel 🛛 🔅 | Homepage System | Security | User | Access Control | Billing | Account | Opera |
| Location: User > User Management User Search | User Search 🌣 | | | | | | |
| Import Search | Username | | | | | ! | |
| Create Account | Account | | | | | | |
| Batch Account Activation | Liser Templates | | Diease Sele | | | | |
| Import Accounts | Plan | | Please Sele | ect | | V | |
| Import Changes | Billing Policy | I | Please Sele | ct | | • | |
| Import Payments | User Group | | | - | Contains | The Child Use | r Groups |
| Import Change User Templates and | Account Creation So | urce | Please Select 🔹 | | | | |
| Plans | Recent Offline Durat | ion 🗌 | Recently | 1 Week 🔻 Inacti | ve Network l | Jsers Within T | his Perio |
| Import Change User Group | | | from | | lnactive N | etwork Users | From |
| | Pause Duration | | | . - | Ī | | |
| | Last Self-service Paus | se Duration | | | | | |
| | | | | | | | |

4.2.1.8 Payment

4.2.1.8.1 Function requirements

Collect fees from newly created users, so that they can be authenticated, be charged, and access the Internet.

4.2.1.8.2 Configuration key points

The payment operation involves fees. Ensure that paid fees are consistent with the fees recorded in the system.

4.2.1.8.3 Configuration steps

1. Log in to the SAM+ management page.

2. Choose Billing > Fees Management.

| SAM ⁺ security accounting m | IANAGEMENT SYSTEM | | | | |
|---|-------------------|------------------------|-------------------|---|----------------------------|
| Shortcut Channel 🔅 | Homepage System | n Security Us | er Access Control | Billing Account | t Operation |
| Location: Billing > Fees Management | Status | Please Select | • | Account Management Fees Management Billing Compensation | Advanced Search |
| m (MYR) | To | e select the operation | type Payment | Billing Policy Customize Policy | raid (MVR) |
| | , icas | Pay A | II Account Enquir | ry Upon Service Expiry | Show the Background Tasks |
| Total of 2 records, the currently displayed | 1 to 2 records | | | | |
| Account ID Full 1 | Name Baland | ce (MYR) Is Ov | erdraft Allowed | Credit Limit (MYR) | Available Credit (MYR) Sta |

3. The newly created user has insufficient balance. Click the icon in the **Payment** column.

| Locati | on: Billing > Fees Manager | nent | | | | | | | | |
|-----------------|---------------------------------|-----------------------|----------|-------------------|-------------------|-------------------------------------|--------------------------|---------|-----------|---|
| Accou | nt ID | | Status | Please Select | • | General Search | Search Advanced Se | arch | | |
| Balanc m (MY | re Fro (R) | | То | | | | | | | |
| | | | Please s | elect the operati | on type Payment | Balance to be I | Paid (MYR) | Payment | | |
| | | | | Pa | y All Account Enq | uiry Upon Service Expiry | Show the Background Task | s | | |
| Total o | of 2 records, the currently dis | played 1 to 2 records | | | | | | | Currently | 1 |
| | Account ID | Full Name | Balance | (MYR) is | Overdraft Allowed | Credit Limit (MYR) | Available Credit (MYR) | Status | Payment | R |
| | dot1x | | 0.00 | N |)) | | | Normal | E C | |
| | 123 | 123 | 0.00 | N | b | | | Normal | 1 | |
| | | | | | Tota | Balance: 0.00 Total Over | draft:0.00 | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

4. Collect the fees, record the fees actually paid by the user in the system, and click **Payment**.

| Location: Billing > Fees Management | > Payment | | |
|-------------------------------------|---|--------------------------------|---------------------------|
| Account | | | |
| Account ID | dot1x | Email | |
| Overdraft Options | The account can be overdrawn. | | |
| Balance (MYR) | 0.00 | | |
| Status | Normal | Description | |
| Account Associated With The User | Q , | Account Activation Fee | Unpaid |
| | | | |
| | | | |
| Balance to be Paid (MYR) | | Receivables (MYR) | |
| Account Activation Fee (MYR) | | Receivables (MYR) | |
| | | | |
| | Payment Reset Return to Expense Managemen | t Return to Account Management | Return to User Management |

4.2.1.8.4 Verification

1. Verify that the fees are paid successfully.



Account (dot1x) Successfully paid (MYR) 123.00 for account activation!;Account (dot1x) payment for (MYR) 123.00 is successful!

 Verify that the fees are corrected and the account is in the normal state. As shown in the figure below, 123 Yuan is deducted from the user account "dot1x" for the current month, and the account has 246 Yuan balance, and is in the normal state.

| | | | Please select the op | eration type Payment | Balance to be Pa | id (MYR) | Payment | | |
|--------|-------------------------------|------------------------|----------------------|----------------------|--------------------------------------|--------------------------|---------|-----------|----------|
| | | | | Pay All Account Enqu | uiry Upon Service Expiry | Show the Background Task | s | | |
| otal d | f 2 records, the currently di | splayed 1 to 2 records | | | | | | Currently | 1 /1Pa |
| | Account ID | Full Name | Balance (MYR) | Is Overdraft Allowed | Credit Limit (MYR) | Available Credit (MYR) | Status | Payment | Refund |
| | dot1x | | 246.00 | No | | | Normal | 1 | iiî) |
| | 123 | 123 | 0.00 | No | | | Normal | 1 | 1 |
| | | | | Total | Balance: 246.00 Total Over | draft:0.00 | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |
| | | | | | | | | | |

4.2.2 [Optional] Wireless AC — 802.1x Authentication

4.2.2.1 Adding an AC on SAM+

4.2.2.1.1 Function requirements

Add ACs on SAM+.

4.2.2.1.2 Configuration key points

The AC parameters added on SAM+ must be consistent with the actual settings of the AC. Otherwise, an authentication exception will occur.

4.2.2.1.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose System > Device Management.

| GEMENT SYSTE | N | | | | |
|--------------|----------------------------------|--|---|--|--|
| Homepage | System | Security | User | Access Control | Billing |
| | | | | | |
| | Device Type | Please Se | lect | • | 🕑 Gene |
| Add | Batch A | Add Ser | d Notifica | tion to the Selected | Send |
| 9 | | | | | |
| D | evice Type | | Mo | del | Device G |
| | | | | | |
| | GEMENT SYSTEM Homepage Add | GEMENT SYSTEM Homepage System Device Type Add Batch A | GEMENT SYSTEM Homepage System Security Device Type Please Se Add Batch Add Sen | GEMENT SYSTEM Homepage System Security User Device Type Please Select Add Batch Add Send Notifica Device Type Mc | GEMENT SYSTEM Homepage System Security User Access Control Device Type Please Select • Add Batch Add Send Notification to the Selected Device Type Model |

3. Click **Add** to add a device.

| SAM ⁺ security accounting mana | GEMENT SYSTEM | и | | | |
|---|---------------|-------------|-----------|-------------|-------------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access |
| Location: System > Device Management | | | | | |
| Device IP Address | | Device Type | Please Se | elect | • |
| | Add | Batch / | Add Se | nd Notifica | tion to the |
| There were no results found. Column Confi | g | | | | |
| Device IP Address | D | evice Type | | Mo | del |
| | | | | | |

4. Set AC parameters and ensure that the key parameters are consistent with the actual settings of the AC. Then, click **Save**.

| Device | | | | |
|-----------------------------|-----------------------|--|--------------------------------|--------------|
| Device IP Address* | 192.168.54.226 | | IP Туре* | IPv4 |
| Device Type* | Wireless Switch 🔹 |] | Model* | RG-WS5708 |
| PPPoE Authentication Domain | | Please use comma or space to separate multiple domains | IPOE+Web Authentication Domain | |
| Device Key* | kevy | | Community* | key |
| | | For trusted ARP binding application, MAC address must be | | |
| VIAC Address* | filled | | SNMP Proxy Port | |
| OHCP Login Username | | | DHCP Login Password | |
| Felnet Login Username | | | Telnet Login Password | |
| Felnet 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 Selec |
| Web Authentication Option | Select this to enable | the web authentication for the switch | RG-ePortal Management Port | |
| ntegration Port(1~65535) | | | Description | |
| SU Version Check | Enable (Applicable t) | o authentication client + access switch authentication mode) | | |

4.2.2.1.4 Verification

1. Check whether the SAM+ server can ping the device successfully. If yes, it indicates that their communication is normal (ensure that ping packets are not intercepted by the firewall).

4.2.2.2 Access Control Configuration

4.2.2.2.1 Function requirements

Configure access control to restrict Internet access behavior of users.

4.2.2.2.2 Configuration key points

The Internet access behavior of access users needs to be confirmed with customers and access control needs to be configured based on actual conditions.

4.2.2.2.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose Access Control > Access Control.

| SAM ⁺ security accounting man | AGEMENT SYSTE | м | | | | | |
|---|---------------|------------|----------|------|----------------|-----------|-------------------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account C |
| 90 Health Score | Total Online | e Users | | | 0 | Average | Authentication F |
| 🙁 Disk Space Check 🔹 | Account Nu | mber | | | 0 | Current P | Performance (User |
| 3rd Party Development Interface | License Nun | nber | | | 0 | Buffer | |
| Cocal License Monitoring | SAM Server | Monitoring | | | | | |
| Internet Traffic Receive Channel | 1 | CPU | J | | | | |
| Oatabase Integrity Check | | 0% | ,) | | | | |
| Oatabase Parameter Check | | Me | mory | | | | |
| Database Document Compression Check | | 0/0 | J(U76) | | | | |
| Oatabase Index Fragment Check | | | | | | | 172.29.2.2 |

3. Click **Add** to add access control.

| SAM^+ security accounting m | IANAGEMENT SYSTE | м | | | | |
|---|------------------|------------|-----------|--------|-------------------|---------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing |
| Location: Access Control > Access Cont | rol | | | | | |
| Access Control Name | | 🕑 Genera | al Search | Search | | |
| | | | | | Add | D |
| Total of 1 records, the currently displayed | 1 to 1 records | | | | | |
| Access Control Name | | Public Ser | vice | | Access Control | Туре |
| default | | No | | | default access co | ontrol |
| | | | | | | |
| | | | | | | |
| | | | | | | |

4. On the **Access Control Information** tab page, enter the access control name, for example, "wireless1x", and set other parameters based on actual conditions.

| Sho | ortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing |
|-----|--|--------------------------|----------------|---------------|---------------|---------------------|------------------|
| Lo | cation: Access Control > Access C | Control > Add | | | | | |
| | Access Control Information | ser Information Check | Network Us | age Control | Public Se | ervice User Behavi | or Control V |
| | Access Control Name * | wireless1x | | | | | |
| | Concurrent Logins Limit(0 to 99) 0 means no limit * |) | | | | | |
| | According to the Terminal Type | e Concurrent Logins (1 t | o 99 times) | | | | |
| | | 🕑 Display accountir | ng policy info | rmation when | user onlin | e | |
| | | Show users on-lin | ne access con | trol time | | | I 1 |
| | Gateway Access Restriction | It does not allow | traffic throug | h the gatewa | y server (ga | ateway device needs | to be deployec |
| | Export linkage strategy | | * non | NPE / EG gat | eway billin | g model deploymen | t, no need to cc |
| | Firewall Policy | | * not | deploy firewa | ills linkage, | the need to configu | re |
| | Description | | | | | | |
| | * Please refer to respective label co | ntent for access details | | | | | |
| | · | | | | | | Save |

5. On the **User Information Check** tab page, select **Wireless 1X Access** and configure whether to bind accounts with IP/MAC addresses based on actual conditions. Then, click **Save**.

| S | AM^+ security account | ITING MANAGEMENT SYST | EM | | | | | | | | | |
|----|-------------------------------|------------------------|----------------|---------------|-----------|----------|--------------|-------------|---------------|-------------|---------------------|-------------|
| Sh | ortcut Channel 🌼 | Homepage | System | Security | User | Access | Control | Billing | Account | Operation | | |
| Lo | cation: Access Control > Acce | ss Control > Add | | | | | | | | | | |
| | Access Control Information | User Information Check | Network U | sage Control | Public Se | ervice L | Jser Behavio | or Control | VPN Control | Client Vers | ion Management | Wireless Ac |
| | Allowed Access | Access Mo | de Verificatio | n Information | | | | | | | | |
| | Wired 1X Access | User IP(\ | (4) | User IP(v6) | 6 | User MA | с | NAS IP(| /4) | NAS IP(v6) | NAS Po | rt |
| | Wild Wrecess | VLAN | | Internal VLA | N | External | VLAN | Access I | P Type Static | | v | |
| | ✓ Wired Web Portal Access | User IP(\ | (4) | User MAC | | Web Aut | hentication | Device IP(v | l) | Web Authen | tication Device Por | t |
| | Wireless 1X Access | User IP(\ | (4) | User MAC | (| NAS IP(v | 4) | AP MAC | | SSID | | |
| | Willies IX Access | Access I | • Type Static | : | ▼ | | | | | | | |
| | ✓ Wireless Web Portal Access | User MA | С | NAS IP(v4) | 0 | AP MAC | | SSID | | | | |
| | Smart Device 1X Access | User MA | С | NAS IP(v4) | | AP MAC | | SSID | | | | |
| | MAC East Accord | User MA | С | NAS IP(v4) | | AP MAC | | SSID | | NAS Port | | |
| | MAC Past Access | VLAN | | Internal VLA | N | External | VLAN | | | | | |
| | Wired Standard Dortal Acces | User IP(\ | (4) | User MAC | (| NAS IP(v | 4) | NAS Por | t 🗉 | VLAN | | |
| | wireu stanuard Portal Acces | Internal | VLAN | External VLA | N | | | | | | | |
| | | User IP(\ | (4) | User MAC | 0 | NAS IP(v | 4) | | | SSID | | |

4.2.2.2.4 Verification

Verify that access control is added successfully.

| Shortcut Cl | nannel 🌼 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | |
|-----------------------------|---|-------------|---------------------------|----------|--------|---|-----------------|------------------|-----------|--------------------------------------|
| Location: | Access Control > Access Control | | | | | | | | | |
| Access Cor | ntrol Name | | 🕑 Genera | l Search | Search | | | | | |
| | | | | | | Add | Del | ete the Selected | | |
| | | | | | | | | | | |
| Total of 2 i | ecords, the currently displayed 1 to | o 2 records | | | | | | | | |
| Total of 2 i | ecords, the currently displayed 1 to ess Control Name | o 2 records | Public Servic | e | | Access Control Type | 2 | | | Description |
| Total of 2 r Acc | ecords, the currently displayed 1 to ess Control Name ault | o 2 records | Public Servic No | e | | Access Control Type default access contro | e Dl | | | Description System Default Access |
| Total of 2 r | ecords, the currently displayed 1 to ess Control Name ault vless1x | 0 2 records | Public Servic No No | e | | Access Control Type default access contro Common access con | e bl trol | | | Description System Default Access |
| Total of 2 r Acc defi | ecords, the currently displayed 1 to ess Control Name ault eless1x | o 2 records | Public Servic No No | e | | Access Control Type default access contro Common access con | e bl trol | | | Description System Default Access |
| Total of 2 r | ecords, the currently displayed 1 to ess Control Name ault eless1x | o 2 records | Public Servic No No | e | | Access Control Type default access contro Common access con | e bl trol | | | Description System Default Access |
| Total of 2 r | ecords, the currently displayed 1 to ess Control Name ault eless1x | o 2 records | Public Servic No No | e | | Access Control Type default access contro Common access con | e bl trol | | | Description System Default Access |

4.2.2.3 Billing Policy Configuration

4.2.2.3.1 Function requirements

Configure billing policies based on billing requirements of access users, to pay for Internet access.

4.2.2.3.2 Configuration key points

Billing requirements of access users need to be confirmed with customers and billing policies need to be configured based on actual conditions.

4.2.2.3.3 Configuration steps (monthly milling)

- 1. Log in to the SAM+ management page.
- 2. Choose Billing > Billing Policy.



3. Select Monthly Billing Policy and click Add.

| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation |
|------------------------------------|----------|----------|-----------------|---------------|----------------------|---------|------------------|-----------|
| Location: Billing > Billing Policy | | | | | | | | |
| Billing Policy Name | | 🕑 Gener | al Search | Search | | | | |
| | | Pleas | se select the l | oilling polic | cy which you want to | add Mor | nthly Billing Po | li 🔻 Add |
| There were no results found. | | | | | | | | |
| Billing Policy Name | | Descript | tion | | | | | |
| | | | | | | | | |
| | | | | | | | | |

4. Enter the billing policy name, for example, "wireless_month", set **Period Type** to **30 Days** or **Month**, and set **Rate** (**MYR**), for example, 30 Yuan/month. Then, click **Save**.

| Billing Policy Name* | wireless_month | Description | |
|---------------------------------|--|----------------------------------|-----------------------|
| Period Type* | 30 Days Month | Ending Date | 🗌 Enable |
| Compensation | The remaining days during account suspension can be used after recovery | Rate (MYR)* | |
| Authoritication Balatad Ontions | Allow login when there is no remaining internet traffic or the account has unpaid | charges. (Must use the NTD pene | tration mode with acc |
| dunentication Related Options | internet traffic billing plan.) | | |
| Advances Options | Monthly Payment for Limited Duration/ Monthly Payment for Limited Internet Trades 1 (2019) | ffic/ Monthly Payment for Limite | d Authentication Devi |
| • Month | ly charge: charges extend to the next month. For example, if the user creates the account | and paid for the services on the | 6th this month, the f |

4.2.2.3.4 Verification

| Shortcut Channel 💠 | Homepage | System | Security | User | Access Control | Billing | Account | Ор |
|---|--------------|----------|---------------|---------------|---------------------|---------|-----------------|-------|
| Location: Billing > Billing Policy | | - | - | | | | | |
| Billing Policy Name | | 🗹 Gener | al Search | Search | | | | |
| | | Pleas | se select the | billing polic | y which you want to | add Mor | nthly Billing P | oli 🔻 |
| Total of 1 records, the currently displayed 1 | to 1 records | | | | | | | |
| Billing Policy Name | | Descript | ion | | | | | |
| wireless_month | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |

Verify that the billing policy is added successfully.

4.2.2.4 User Template Configuration

4.2.2.4.1 Function requirements

Configure user templates based on user attributes for later account creation.

4.2.2.4.2 Configuration key points

It is recommended to classify user templates with the same attribute into a group and give concise and intuitive names to the templates, for example, student monthly billing template or teacher monthly billing template.

4.2.2.4.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose **User > User Template**.

| SA | M^+ security accounting m | | ٨ | | | | | | |
|------|----------------------------------|-------------|--------|----------|------|----------------|-----------|------------|---------------|
| Shor | tcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing A | ccount | Operation |
| Loca | stion: User > User Template | | | | | Add | Delete t | he Selecte | d |
| | Template Name | | | | | | | Descr | iption |
| | default | | | | | | | Defau | lt Template |
| | Classroom Default Template (Do N | Not Delete) | | | | | | Classr | oom Default T |
| | dot1x | | | | | | | | |
| | | | | | | | | | |
| 3. | Click Add. | | | | | | | | |
| Loca | ation: User > User Template | | | | | | | | |

4. Enter the template name, for example, "wireles_month", and click **Save**.

Delete the Selected

| | Kule | |
|----|--|-----|
| I | O Add User Template | |
| ne | User Templates | con |
| | Template Name* wireless_month Custom Options Allow self-change plan | |
| | Monthly Modification Limit (1~10 times) Description | |
| | Save Cancel | |

4.2.2.4.4 Verification

Verify that the user template is added successfully.

| Shortcut Chan | el 🗇 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | |
|---|--|---|-----------------------------|---------------------------------|--------------------------|------------------------|--------------|----------------|------------------|------------------|
| Location: User Template N. Self-Modific Description: | > User Template > User Te me: ation Option | mplates month wed to change the p | əlan | | | User Te | mplates: w | vireless_montl | h 🔽 | |
| 177 | Plan | _ | _ | | _ | | | _ | Rule | _ |
| | | A | ccess Area | De | efault Rule | Service | | Allow Acce | ess Time | Access Cor |
| The nu Users c | mber of repeated logins of an use different services fo | the plan is user's i Internet access and | naximum nui d the number | mber of online of online use | e STAs. ers of the sa | ame service is restric | ted by the n | umber of repe | ated logins of t | he corresponding |

4.2.2.5 User Plan Configuration

4.2.2.5.1 Function requirements

Configure a user plan to cover access limits of authenticated users, including the area, time range, access control, and billing policy. A user plan is akin to a phone service package.

4.2.2.5.2 Configuration key points

A plan covers all control options and fees for access users. Be sure to clearly confirm plans with customers before configuration.

4.2.2.5.3 Configuration steps

1. In the configured user template "wireless_month", click Add Plan.

| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control |
|---|--|-----------------------------|---------------------------------|--------------------------|--------------------------|
| Location: User > User Template > User Temp | olates | | | | |
| Template Name: wireless_model Self-Modification Option : Not allowed Description: Not allowed | onth d to change the p | blan | | | User Tem |
| Pian | | | | (D | |
| Add Plan | A | ccess Area | De | efault Rule | Service |
| Users can use different services for In | e plan is user's i iternet access and | naximum nur d the number | mber of online of online use | e STAs. ers of the sa | nme service is restricte |
| | | | | | |

2. Enter the plan name, for example, "wireless_month", select a configured billing policy or **Not Charging** based on actual requirements, and then click **Save**.

| Add Plan | |
|---------------------------------|-----------------------------------|
| | |
| Plan | |
| Plan * | wireless_month |
| Concurrent Logins Limit 🛛 🖣 | Endble 1 (1 ~ 00 times) |
| Billing Policy | Not Charging |
| Cycle expired and suspend user. | Activate |
| MAC Binding Validity | 0 (0-365 days, 0 for not limited) |
| Description | |
| | |
| | |
| Save | Cancel |
| | |

3. Click Modify Plan and modify the access area, access time range, access control, and billing mode.

| Plan Access Area Default Rule Service Name:wireless_month Concurrent Logins Limit :1 Billing Policy:Not Charging Cycle Expired to Suspend User.:Not Enabled Suspension End Time: MAC Binding Expiry:0Day Unlimited Image: Construction of the service of the ser | Femp Self-N Descr | late Name: /Iodification Option : iption: | wireless_month Not allowed to change the | e plan | | oser remplates. | wireless_i |
|---|-------------------------|---|--|-----------|--------------|-----------------|------------|
| Name:wireless_month Concurrent Logins Limit :1 Billing Policy:Not Charging Cycle Expired to Suspend User.:Not Enabled Suspension End Time: MAC Binding Expiry:0Day Unlimited O default | | | Plan | | Default Pule | Convice | |
| Description: | | Name:wireless_month Concurrent Logins Lir Billing Policy:Not Cha Cycle Expired to Susp Suspension End Time MAC Binding Expiry: Description: | nit :1 rging end User.:Not Enabled : Day | Unlimited | o | default | Unli |

4. Modify the rule based on actual conditions. The figure below shows that the access area of authenticated users is unlimited, access control is set to "wireless1x", the access time range is unlimited, and billing is performed based on the plan "wireless_month".

| Shortcu | ıt Channel | 🕸 Homepage | s System Se | curity User A | ccess Control | Billing | Account | Operation | | | | | | |
|---------------------------------|--|--|---|--|---|--------------------|---|----------------------------|---|-------|-----------|--------------|--------------|-----|
| Locatio Tem Self- Desc | plate Name Modificatio ription: | Iser Template > User Templates wireless_month on Option : Not allowed to change th | e plan | | User Tem; | plates: wi | ireless_month [| 2 | | | | Return to th | e User Templ | ite |
| | | | Access Are | a Default Rul | 0.00 | | _ | Rule | _ | Billi | na Policy | Rule | _ | |
| æ | Name:wir Concurre Billing Po Cycle Exp Suspensio MAC Bind Descriptio | eless_month nt Logins Limit :1 licy:Not Charging ired to Suspend User.:Not Enabled on End Time: ding Expiry:0Day on: | Unlimited | • | Rule Plan | | vireless_a ontr | | | Not C | harging | | R |] |
| | The numbe Users can u | r of repeated logins of the plan is user' ise different services for Internet access | s maximum number and the number of o | of online STAs. aline users of the same | Access Area Service* Access Contro Allov Access Billing Polid | ol [Time cy | default wireless1x Without limiti Press Plan b | v ng the į v lling v |] | rol. | | | | |
| | | | | | | | Save | Cancel | | | | | | |

4.2.2.5.4 Verification

Verify that the plan meets customer requirements.

| Temp Self-I Desci | plate Name: Modification Option: ription: | wireless_month Not allowed to change the | e plan | | User Templates: wi |
|-------------------------|---|---|-----------|---|--|
| | Plan | | | | o de la companya de la |
| | Name:wireless_month Concurrent Logins Limit :1 Billing Policy:Not Charging Cycle Expired to Suspend User.:Not Enabled Suspension End Time: MAC Binding Expiry:0Day Description: | | Unlimited | ° | default |

4.2.2.6 User Group Configuration

4.2.2.6.1 Function requirements

Add authenticated users with the same attribute to the same group, and define a response user template and plan for the user group to prepare for later account creation.

4.2.2.6.2 Configuration key points

It is recommended to group access users by attribute, for example, group users on campus networks into "student user group" or "teacher user group".

4.2.2.6.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose User > User Group.

| SAM ⁺ security accounting manage | GEMENT SYSTE | м | | | | | | | |
|--|----------------|---------------|---------------|--------------------|--------------------------|----------------|------------------------|------------------|--|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account C | Operation | |
| Location: User > User Template > User Template | tes | | | User M | lanagement | | | | |
| | | | | Pre-car | ncelled Account | | | | |
| | | | | User G | roup | mplates: w | vireless month 🗔 | 2 | |
| Template Name: wireless_mon | th . | | | | User Template | | • | | |
| Self-Modification Option : Not allowed t Description: | o change the j | olan | | Traffic | Control Policy | | | | |
| Plan | | | | Guaran | itor and Guest | | | Rule | |
| | | Acce | ss Area | Real-na | ame Policy | rvice | Allow A | ccess Time | |
| Name:wireless_month Concurrent Logins Limit :1 | | | | Real-na | ame System | | | | |
| Billing Policy:Not Charging | | | | MAC Authentication | | | 11 11 15 11 | | |
| Cycle Expired to Suspend User.:Not E Suspension End Time: | nabled l | Jnlimited | | IVIAC A | utilentication | | Unlimited | | |
| 3. Click Add. | | | | | | | | | |
| Shortcut Channel 🍄 Homepag | je System | Security | User Acce | ss Control | Billing Account | Operation | 1 | | |
| Location: User > User Group | | | | | | | | | |
| Expand All Collapse All | Change User | Group | | | | | | | |
| C User Group | User Group * | | root | | | | Parent Group Na | me * | |
| dot1x | Default User | Template* | default | • | | | Default Plan* | | |
| | Uplink Speed | | | | | | Downlink Speed | | |
| | (8~261120KE | (sos) | 0 | | | | (8~261120KBps) | | |
| | User group a | uthentication | | | | | Downlink Speed | | |
| | is successful | hoplinks. | | | | | (8~261120KBps) | | |
| | Description | | Root User Gro | up | | | Creator | a | |
| | · · | | Synchronize | the undate o | default user template or | nlan user used | in this user group (If | there are a larr | |

| Synchronize the update default user template or plan user used in this user group (If there are a larg |
|--|
| Please perform system operation when idle.) |
| Synchronous modification of the user templates and plans of all sub-user groups in the current user |
| system idle.) |
| Save |
| |

4. Enter the user group name, for example, "wireless_month", and select the default user template and default plan. Then, click **Save**.

| Add User Group | | | | | |
|---------------------------|------------------|---------------------|------------------|--|--|
| User Group * | wireless_month | Parent Group Name * | root 🌄 | | |
| Default User Template* | wireless_month • | Default Plan* | wireless_month 🔻 | | |
| Uplink Speed | 0 | Downlink Speed | | | |
| (8~261120KBps) | U | (8~261120KBps) | U | | |
| User group authentication | | Downlink Speed | | | |
| is successful hoplinks. | | (8~261120KBps) | | | |
| Description | | Creator | admin | | |

4.2.2.6.4 Verification

Verify that the user group is added successfully.

| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account |
|---|----------|--|--|-----------------------|----------------------------|----------------|----------------|
| Location: User > User Group | | | | | | | |
| Expand All Collapse All | | Change User | Group | | | | |
| User Group o toot o dot1x o wireless_month | | User Group * Default User ⁻ Uplink Speed (8~261120KB User group a is successful I Description | Template* ps) uthentication roplinks. | wirele wirele ¢ | ss_month ss_month ss_month | lefault user t | emplate or pli |

4.2.2.7 Account Creation

4.2.2.7.1 Function requirements

Create accounts for users in the SAM+ system.

4.2.2.7.2 Configuration key points

- 1. The account creation process generally requires users to go to business halls and apply for accounts by using their ID cards.
- 2. Accounts with the names same as those on their ID cards are registered during account creation.
- 3. A user group and a user template need to be selected during account creation as planned.

4.2.2.7.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose User > User Management.

| SAM ⁺ security accounting mana | AGEMENT SYSTEM | | | | | | | | |
|---|----------------|--------|----------|-----------|----------------|---------|---------|-----------|----|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | |
| Location: User > User Management | | | | User Ma | anagement | | | | |
| User Search | User Search 🌼 | | | Pre-can | celled Account | | | | |
| | | | | User Gr | oup | | | | |
| Import Search | Username | | | User Te | mplate | | (!) | | Mu |
| | Account | | | Traffic (| Control Policy | | | | |
| Create Account | | | | Guaran | tor and Guest | | | | |
| Batch Account Activation | Balance | | | Real-na | me Policy | | | | |

3. Click **Create Account** in the left pane.

| SAM ⁺ security accounting ma | ANAGEMENT SYSTEM | | | | | | |
|---|-------------------------|--|--|--|--|--|--|
| Shortcut Channel 🛛 🍄 | Homepage System Secu | | | | | | |
| Location: User > User Management | | | | | | | |
| User Search | Basic Information | | | | | | |
| Import Search | Username* | | | | | | |
| | Password* | | | | | | |
| Create Account | User Group* | | | | | | |
| Batch Account Activation | User Templates | | | | | | |
| Import Accounts | Self-service Permission | | | | | | |
| | Auto Pre-Cancellation | | | | | | |
| Import Changes | Guarantor Ranking | | | | | | |
| Import Payments | Advanced Options | | | | | | |
| | Sev | | | | | | |

4. Enter the username and password, select a user group, user template, and plan. Then, click **Save**.
| Username* | wireless1x | Full Name | |
|-------------------------|---|---------------------|--------------------------|
| Password* | ••• | Confirm Password* | |
| User Group* | wireless_month | Account | Same As username 📑 |
| User Templates | ◉ Use Default Template of User Group [©] Customize | | |
| Self-service Permission | All Self-service Privileges | Authentication-free | Verification is required |
| Auto Pre-Cancellation | | BACL | Please Select 🔻 🟹 |
| Guarantor Ranking | Please Select | | |
| Advanced Options | Show Advanced User Settings options | | |
| Sex | Please Select | Email Address | |
| ID Type | Please Select 🔻 | ID No. | |
| Education Level | Please Select | Online Information | |
| Telephone No. | | Mobile Phone | |
| Address | | Postal Code | |
| | | | |

4.2.2.7.4 Verification

1. In the left pane of the **User Management** page, click **User Search**. In the displayed right pane, click **Search**. The added user is displayed.

| 5 | Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | | | | | |
|---|---|--------------|-------------------|----------------|-----------|---------------------|-----------|-----------|-------------|-------------|----------------|--------|--------------------|----------|
| [| Location: User > User Management User Search | | | | | | | | 🔹 To Search | | | | | |
| | Import Search | Update | | Delete | | Pre-delete | | Pay and R | efund | Suspend | i | Resume | | Notifica |
| | Create Account | Total of 1 r | ecords, the curre | ntly displayed | 1 to 1 re | cords Select All Re | cords | Colu | umn Config | | | 8 | Currently 1 | /1Page |
| | Batch Account Activation | • | Username | 1 | | ull Name | | | | unt Balance | User Templates | | Binding Info on | |
| | Import Accounts | | wireless1x | | | | wireless1 | x | 0.00 | | wireless_month | | | |
| | Import Changes Import Payments | L | | 1 | | | | | | | | | | |
| | | | | | | | | | | | | | | |

4.2.2.8 Payment

4.2.2.8.1 Function requirements

Collect fees from newly created users, so that they can be authenticated, be charged, and access the Internet.

4.2.2.8.2 Configuration key points

The payment operation involves fees. Ensure that paid fees are consistent with the fees recorded in the system.

4.2.2.8.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose Billing > Fees Management.

| SAI | M ⁺ security accoun | ITING MANAGEMENT SYSTEM | | | | | | | |
|--------------------------------------|--|-------------------------|-------------------------------------|-------------------------|-------------------------|--|---|------------------------|--------------|
| Shortcu | ıt Channel 🔅 | Homepage | System Security | User | Access Contr | ol Billing | Account | Operation | |
| Locatic Accour Balanc m (MY | n: Billing > Fees Manage nt ID [e Fro R) | ment Sta | Please Select Please select the ope | eration type Pay All | Payment Account Enqu | Account I Fees Man Billing Co Billing Po Customiz V Balar | Management agement mpensation licy e Policy cce to be Paid cce to be Paid | (MYR) | arch Payment |
| Total o | f 3 records, the currently di | splayed 1 to 3 records | | | | | | | |
| | Account ID | Full Name | Balance (MYR) | Is Overdra | ft Allowed | Credit Limit (N | AYR) A | Available Credit (MYR) | Status |
| | wireless1x | | 0.00 | No | | | | | Normal |
| | dot1x | | 246.00 | No | | | | | Normal |
| | 123 | 123 | 0.00 | No | | | | | Normal |
| | | | | | Total | Balance: 246.00 | Total Overdra | ft:0.00 | |

3. The newly created user has insufficient balance. Click the icon in the **Payment** column.

| nortcu | ut Channel 👷 | nome | page System Secu | rity User Access Con | trol Billing Accou | int Operation | | | |
|----------------|---|--|--|--|--|---|---|----------------------|-----------------|
| ocatio | on: Billing > Fees Ma | inagement | | | | | | | |
| ccou | nt ID | | Status Please S | elect 🔹 | 🕑 General Search | Search Advanced Se | arch | | |
| alanc n (MY | e Fro (R) | | То | | | | | | |
| | | | | | | | | | |
| | | | Diama and a state | | - Polyanta ha | n-14 a avm | | | |
| | | | Please select the | operation type Payment | Balance to be | Paid (MYR) | Payment | | |
| | | | Please select the | Pay All Account En | Balance to be quiry Upon Service Expiry | Paid (MYR) Show the Background Tas | Payment | | |
| otal c | of 3 records, the curren | tly displayed 1 to 3 recorc | Please select the | Payment Payment Pay All Account En | Balance to be quiry Upon Service Expiry | Paid (MYR) Show the Background Tas | Payment | Currently | 1 /1P |
| otal c | of 3 records, the curren | tly displayed 1 to 3 recorc Full Name | Please select the ds Balance (MYR) | e operation type Payment Pay All Account En Is Overdraft Allowed | Balance to be quiry Upon Service Expiry Credit Limit (MYR) | Paid (MYR) Show the Background Tas Available Credit (MYR) | Payment ks Status | Currently Payment | 1 /1P Refund |
| otal c | of 3 records, the curren Account ID wireless1x | tly displayed 1 to 3 record Full Name | Please select the ds Balance (MYR) 0.00 | Payment Payment Payment Pay All Account En | Balance to be quiny Upon Service Expiry Credit Limit (MYR) | Paid (MVR) Show the Background Tasl Available Credit (MVR) | Payment ks Status Normal | Currently Payment | 1 /1P Refund |
| otal c | of 3 records, the curren Account ID wireless1x dot1x | tly displayed 1 to 3 record Full Name | Please select the ds Balance (MYR) 0.00 246.00 | Payment Payment Payment Payment Pay All Account En | Balance to be quiry Upon Service Expiry Credit Limit (MYR) | Paid (MYR) Show the Background Tasl Available Credit (MYR) | Payment ks Status Normal Normal | Currently Payment | 1 /1P Refund |

4. Collect the fees, record the fees actually paid by the user in the system, and click **Payment**.

| Account | | | |
|----------------------------------|--|------------------------------|---------------------------|
| Account ID | wireless1x | Email | |
| Overdraft Options | The account can be overdrawn. | | |
| Balance (MYR) | 0.00 | | |
| Status | Normal | Description | |
| Account Associated With The User | | Account Activation Fee | Unpaid |
| | | | |
| | | | |
| | | | |
| Balance to be Paid (MYR) | 123 | Receivables (MYR) | 123 |
| Account Activation Fee (MYR) | | Receivables (MYR) | |
| | | | |
| | Payment Reset Return to Expense Management | Return to Account Management | Return to User Management |
| | | | |
| | | | |

4.2.2.8.4 Verification

1. Verify that the fees are paid successfully.

Account (wireless1x) payment for (MYR) 123.00 is successful!

2. Verify that the fees are corrected and the account is in the normal state. As shown in the figure below, 123 Yuan is deducted from the user account "wireless1x" for the current month, and the account has 123 Yuan balance, and is in the normal state.

| Shortci | ut Channel 🔅 | Homepage | System Secu | irity User Access Co | ntrol Billing Accour | nt Operation | | |
|--------------------------|--|--|--|--------------------------|--|---|----------------------------------|---|
| Locatio | on: Billing > Fees Managem | ent | | | | | | |
| Accou Balanc m (MY | nt ID re Fro (R) |] s | Status Please S | elect • | | Search Advanced Se | earch | |
| | | | Please select the | e operation type Payment | ▼ Balance to be | Paid (MYR) | Payment | |
| | | | | | | | | |
| | | | | Pay All Account E | nguiry Upon Service Expiry | Show the Background Tasl | ks | |
| | | | | Pay All Account E | nquiry Upon Service Expiry | Show the Background Tasl | ks | _ |
| Total o | of 3 records, the currently disp | layed 1 to 3 records | | Pay All Account E | nquiry Upon Service Expiry | Show the Background Task | ks | 📓 Current |
| Total c | of 3 records, the currently disp Account ID | layed 1 to 3 records Full Name | Balance (MYR) | Pay All Account E | nquiry Upon Service Expiry Credit Limit (MYR) | Show the Background Task Available Credit (MYR) | ks Status | Current Payment |
| Total o | of 3 records, the currently disp Account ID wireless1x | layed 1 to 3 records Full Name | Balance (MYR) 123.00 | Pay All Account E | nquiry Upon Service Expiry Credit Limit (MYR) | Show the Background Task Available Credit (MYR) | ks Status Normal | Current Payment I |
| Total o | of 3 records, the currently disp Account ID wireless1x dot1x | layed 1 to 3 records Full Name | Balance (MYR) 123.00 246.00 | Pay All Account E | nquiry Upon Service Expiry Credit Limit (MYR) | Show the Background Tasl Available Credit (MYR) | ks Status Normal Normal | Payment |
| Total c | of 3 records, the currently disp Account ID wireless1x dot1x 123 | layed 1 to 3 records Full Name 123 | Balance (MYR) 123.00 246.00 0.00 | Pay All Account E | nquiry Upon Service Expiry Credit Limit (MYR) | Show the Background Tasl | ks Status Normal Normal Normal | Current Payment Current Cu |

4.2.3 [Optional] RG-N18000 — Web Authentication (Wired & Wireless)

4.2.3.1 Adding the RG-N18000 on SAM+ (2)

4.2.3.1.1 Function requirements

Add the NAS (RG-N18000) on SAM+.

4.2.3.1.2 Configuration key points

The NAS-relevant parameters added on SAM+ must be consistent with the actual settings of the NAS. Otherwise, an authentication exception occurs.

- The address for the RG-N18000 to interwork with SAM+ must be correct on SAM+. For example, if the source port for communicating with SAM+ is configured on the RG-N18000 by running the **ip radius source-interface loopback 0** command, the IP address of the loopback0 interface of the RG-N18000 needs to be entered in the **Device IP Address** column of SAM+.
- The key for interworking with the RG-N18000 needs to be consistent.
- The SNMP community for interworking with the RG-N18000 needs to be consistent.

4.2.3.1.3 Configuration steps

1. Log in to the SAM+ management page.

2. Choose System > Device Management.

| SAI | M ⁺ security acc | OUNTING MANAGEMENT SYSTE | м | | | | | | |
|--|--|------------------------------|---|--|--------------|-----------------|-----------------|----------|-------|
| Shortcu | t Channel 🛛 🔅 | Homepage | System | Security | User | Access Control | Billing | Accoun | nt O |
| Locatic Accour Balance m (MY) | n: Billing > Fees Ma nt ID [e Fro R) | nagement S | System Se Authentic Billing Set LDAP Cor Self-confi | ettings ation Setting tings ofiguration guration ield | s V | Payment | General | Search | Searc |
| | | [| Device Ma IP Manag | anagement ement | All | Account Enquiry | Upon Servic | e Expiry | Show |
| Total o | f 3 records, the current | tly displayed 1 to 3 records | Blacklist | //anagement | | | | | |
| | Account ID wireless1x dot1x | Full Name | Region M Certificate Guest Mo | anagement e Managemer de | verdra nt | aft Allowed (| Credit Limit (I | MYR) | Avai |
| | 123 | 123 | 0.00 | | No | | | | |

Total Balance: 492.00 Total Overdraft:0.

3. Click **Add** to add a device.

| SAM ⁺ security accounting mana | AGEMENT SYSTE | м | | | | | |
|---|---------------|-------------|-----------|-------------|----------------------|---------|--------|
| Shortcut Channel 🌼 | Homepage | System | Security | User | Access Control | Billing | 1 |
| Location: System > Device Management | | | | | | | |
| Device IP Address | | Device Type | Please Se | lect | ¥ | 🕑 Gen | eral s |
| There were no results found. Column Confi | Add | Batch / | Add Ser | nd Notifica | tion to the Selected | Send | l Not |
| Device IP Address | | Device Type | | Mo | odel | Device | Grou |
| | | | | | | | |

4. Set NAS-relevant parameters and ensure that the key parameters are consistent with the actual settings of the NAS. Then, click **Save**.

| Location: Custom & Davies Manage | mont N Add | | |
|----------------------------------|---|--------------------------------|---------------------------------------|
| Location. System > Device Manage | ment > Add | | |
| Device | | | |
| Device IP Address* | 192.168.33.111 | IP Type* | IPv4 • |
| Device Type* | Ruijie Switch 🔻 | Model* | N18K • |
| PPPoE Authentication Domain | Please use comma or space to separate multiple domains | IPOE+Web Authentication Domain | Please use comm |
| Device Key* | key | Community* | key |
| MAC Address | For trusted ARP binding application, MAC address must be | SNMD Drovy Port | If you do not fill is |
| MAC Address | filled | SNWP PTOXY POIL | II you do not ill li |
| 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 | $\ensuremath{\mathscr{C}}$ Enable (Applicable to authentication client + access switch authentication mode) | N18K Feature | Layer Gateway Certification 🗌 Use Por |

4.2.3.1.4 Verification

1. Check whether the SAM+ server can ping the device successfully. If yes, it indicates that their communication is normal (ensure that ping packets are not intercepted by the firewall).

4.2.3.2 Adding the ePortal Server on SAM+

4.2.3.2.1 Function requirements

Add information about the ePortal Server on SAM+.

4.2.3.2.2 Configuration key points

The ePortal parameters added on SAM+ must be consistent with the actual settings of the ePortal server. Otherwise, an authentication exception occurs.

4.2.3.2.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose System > Device Management.

| SA | | | NT SYSTEM | | | | |
|---------|-------------------------|---------------|-------------|-----------|--------------|-------------------|--------------|
| Shortc | ut Channel 🔅 | Hom | epage Sy | stem S | ecurity | User Ac | cess Control |
| Locati | on: System > Device N | lanagement | | | | | |
| Device | e IP Address | | Devi | ce Type | Please Sel | ect 🔻 | |
| | | | Add | Batch Add | Send | d Notification t | o the Select |
| There | were no results found. | Column Config | | | | | |
| | Device IP Address | | Device | Туре | | Model | |
| | | | | | | | |
| 3. Cli | ck Add to add a devic | e. | | | | | |
| Shortcu | t Channel 🔅 | Homepage | System | Security | User | Access Contro | l Billing |
| Locatio | n: System > Device Mana | agement | | | | | |
| Device | IP Address | | Device Type | Please Se | elect | ¥ | 🗹 Gen |
| | | Ado | l Batch A | Add Se | nd Notificat | ion to the Select | ed Senc |

There were no results found. Column Config

4. Add the ePortal server and ensure that the key parameters are consistent with the actual settings of the ePortal server. Then, click **Save**.

Model

| Shortcut Channel 🛛 🏟 | Homepage | System | Security | User | Access Control | Billing | Account | Oper |
|-----------------------------------|-----------------------|--------------|---------------|-------------|---------------------|---------|-----------------|-----------|
| Location: System > Device Manager | ment > Add | | | | | | | |
| Device | | | | | | | | |
| Device IP Address* | 192.168.54.231 | | | | | | IP Type* | |
| Device Type* | RG-ePortal | • | | | | | Model* | |
| PPPoE Authentication Domain | | Please us | e comma or s | bace to se | parate multiple dom | ains | IPOE+Web Au | uthentica |
| Device Key* | key | | | | | | Community* | |
| | | For truste | d ARP binding | g applicati | on, MAC address mu | ist be | | |
| MAC Address* | filled | | | | | | SNMP Proxy F | Port |
| DHCP Login Username | | | | | | | DHCP Login P | assworc |
| Telnet Login Username | | | | | | | Telnet Login F | asswore |
| Telnet Privileged Password | | | | | | | Device Group | * |
| Device Name | | | | | | | Device Location | on |
| Device Timeout (secs)* | 3 | | | | | | Device Idle Ti | me (secs |
| Device Feature | Re-authentication | Account | Update 🔲 | lient Dete | ction | | Area | |
| Web Authentication Option | Select this to enable | le the web a | uthentication | for the sw | itch | | RG-ePortal M | anagem |
| Integration Port(1~65535) | | | | | | | Description | |

4.2.3.2.4 Verification

- 1. Check whether the SAM+ server can ping ePortal successfully. If yes, it indicates that their communication is normal (ensure that ping packets are not intercepted by the firewall).
- 2. On the SAM+ server, log in to the ePortal system in HTTP mode and check whether you can log in successfully. If yes, it indicates that their communication is normal.

4.2.3.3 Adding SAM+ on the ePortal Server

4.2.3.3.1 Function requirements

Set parameters of the ePortal server so that it can communicate with the SAM+ and NAS normally.

4.2.3.3.2 Configuration key points

The parameters on the ePortal server must be consistent with those on the SAM+ and NAS.

4.2.3.3.3 Configuration steps

1. Log in to the ePortal management page, click **System Settings**, and enter the SAM+ address, RADIUS key, and authentication and accounting ports in the **RADIUS Server** area. Ensure that the parameters are consistent with those on the SAM+ server.

| RG-ePortal F | Portal Components | Network | Acce | ess Portal Syste | 900 |
|--|---------------------------------|-------------------------------|---------|-------------------------|---------------------------------|
| Network Access Portal S System Settings | Location: Network Access Portal | . System > System Set | tings | | |
| Device Management | | | | | RADIUS Server |
| Administrator Access | Radius Server Address | 192.168.33.214 | | Restart Effective | Authentication Port |
| Log Management | Authentication Retry Interval | 0 | secs | (Default 0 sec) | RADIUS Key |
| System Maintenance | Authentication Overtime | 3 | Secs | (Default 3 secs) | Authentication Retry Count |
| Authentication Reque | Accounting | Activated | | | Accounting Port |
| | Accounting Packet Overtime | 3 | secs | (Default 3 secs) | Accounting Packet Retry Count |
| | Accounting Thread Count | 5 | uni ts | (Default 5 units) | Accounting Buffer Zone Settings |
| | | | | | DeviceCommunication Settings |
| | ePortal Listening Informs Port | 162 | (Defaul | t 162)Restart Effective | Informs Community |
| | Communication Overtime | 3 | secs | (Default 3 secs) | Communication Retransmission |
| • | Online Scanning Cycle | 30 | mins | (Default 30 mins) | |
| | | | | | SNMP Settings |
| | SNMP Port | 161 | (Defaul | t 161)Restart Effective | SNMP Community |
| | | | | | Browser Client Related |
| | Keep Alive Cycle | 15 | mins | (Default 15 mins) | Keep Alive Overtime Count |
| | | | | | System Settings |
| | Record Entry on Each Page | 20 | (Defa | ult 20) | |

2. Set SNMP parameters in **Device Communication Settings**.

Informs Community: SNMP community name used for receiving traps from the device. It must be consistent with the community name configured on the device.

SNMP Community: community name of the virtual SNMP agent maintained on the ePortal system. It is used to process SNMP packets between the ePortal system and the RADIUS server.

| ePortal Listening Informs Port | 162 | (Default 162) Restart Effective | Informs Community | ruijie | (Default public) |
|--------------------------------|-----|---------------------------------|------------------------------|--------|-------------------------|
| Communication Overtime | 3 | secs (Default 3 secs) | Communication Retransmission | 3 | times (Default 3 times) |
| Online Scanning Cycle | 30 | mins (Default 30 mins) | | | |
| | | | SNMP Settings | | |
| SNMP Port | 161 | (Default 161) Restart Effective | SMMP Community | ruijie | (Default public) |
| | | | Browser Client Related | | |
| Keep Alive Cycle | 15 | mins (Default 15 mins) | Keep Alive Overtime Count | 5 | times (Default 5 times) |
| | | | System Settings | | |
| Record Entry on Each Page | 20 | (Default 20) | | | |

4.2.3.3.4 Verification

Check parameters and verify that relevant parameters are consistent with those on SAM+ and the NAS.

4.2.3.4 Adding the RG-N18000 on the ePortal Server

4.2.3.4.1 Function requirements

Add the NAS on the ePortal server.

4.2.3.4.2 Configuration key points

The NAS parameters added on the ePortal server must be consistent with those on the NAS.

4.2.3.4.3 Configuration steps

 Log in to the ePortal management page, click Device Management, select 2nd-Generation Web Authentication Access Device from the Device Type drop-down list, and enter the IP address and relevant parameters of the Web authentication access device. Keep these parameters consistent with those on the NAS. Then, click Save.

| Device | Details |
|-------------------------------------|---|
| | 192.168.33.39 |
| * Device IP | |
| | Support adding multiple devices and please separate each device using comma (,). Support max 500 devices. For H3C, only support adding single device. |
| * Read/Write Community | |
| * SNMP Version | SNMPv2c v |
| * Device Type | 2nd-Generation Web Auth |
| * NAT Proxy Mode | Close |
| * web-auth portal key | abcd |
| IPv6 Authentication Portal Protocol | - Select Portal Protocol - V |

4.2.3.4.4 Verification

1. Check whether the ePortal server can ping the device successfully. If yes, their communication is normal (ensure that ping packets are not intercepted by the firewall).

4.2.3.5 Access Control Configuration

4.2.3.5.1 Function requirements

Configure access control to restrict Internet access behavior of users.

4.2.3.5.2 Configuration key points

The Internet access behavior of access users needs to be confirmed with customers and access control needs to be configured based on actual conditions.

4.2.3.5.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose Access Control > Access Control.

| Shortcut Channel Homepage System Security User Access Control Billing Account 90 Health Score Image: System Total Online Users 0 Average Authentical © Disk Space Check Image: System Total Online Users 0 Average Authentical © Jisk Space Check Image: System Sam Server 0 Average Authentical © Local License Monitoring Internet Traffic Receive Channel Unlimited Buffer Buffer O Database Integrity Check SAM Server Monitoring Image: CPU 4% Image: CPU Image: CPU 3. Click Add to add access control. Security User Access Control Billing Account Operation Incation: Access Control > Access Control Security User Access Control Billing Account Operation Access Control Name @ General Search Search Search Med Delete the Selected | + SECURITY ACCOUNTING MANAG | EMENT SYSTEM | | | | | |
|--|--|------------------------------------|------------------------|---|----------------------|--|--|
| 90 Health Score Disk Space Check 3 rd Party Development Interface Local License Monitoring Internet Traffic Receive Channel Database Integrity Check 3. Click Add to add access control. Shortcut Channel Homepage System Security User Access Control & Access Control Security User Access Control & Access Control Ceru and the selected Internet Traffic Receive Channel Ontabase Integrity Check Source Channel Berner System Security User Access Control Billing Account Operation Control Name Ceru and Ceru a | annel 🌣 | Homepage System Se | curity User Access (| Control Billing | Account O | | |
| Source Check Start Party Development Interface Local License Monitoring Internet Traffic Receive Channel Database Integrity Check Shortcut Channel Homepage System Security User Access Control Access Control > Access Control General Search General Search Access Control Name | Health Score | Total Online Users | | 0 Averag | e Authentication P | | |
| Local License Monitoring Internet Traffic Receive Channel Database Integrity Check 3. Click Add to add access control. Shortcut Channel Homepage System Security User Access Control Billing Account Operation Location: Access Control > Access Control Access Control Name General Search Add Delete the Selected | ace Check 🔹 | Account Number License Number | Unlir | 3 Current Performance Unlimited Buffer | | | |
| Shortcut Channel I Image Homepage System Security User Access Control Billing Account Operation Location: Access Control > Access Control > Access Control > Access Control > Image: Image | cense Monitoring t Traffic Receive Channel se Integrity Check Add to add access cont | SAM Server Monitoring CPU 4% | | • | | | |
| Location: Access Control > Access Control Access Control Name | nel 🍄 Homepag | e System Security User | Access Control Billing | Account Operatio | on | | |
| Access Control Name General Search | cess Control > Access Control | | | | | | |
| Add Delete the Selected | l Name | General Search Search | | | | | |
| Total of 2 records, the currently displayed 1 to 2 records | ords, the currently displayed 1 to 2 records | | Add Delet | te the Selected | | | |
| Access Control Name Public Service Access Control Type Description | Control Name | Public Service | Access Control Type | | Description | | |
| default No default access control System Default | | No | default access control | | System Default Acces | | |
| Vireless1x No Common access control | s1x | No | Common access control | | | | |

4. On the **Access Control Information** tab page, enter the access control name, for example, "wired_web", and set other parameters based on actual conditions.

| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | | | |
|--|------------------------|--------------|---------------|---------------|---------------------|--------------|---|--|--|--|--|
| Location: Access Control > Access Co | ntrol > Add | | | | | | | | | | |
| Access Control Information User | Information Check | Network Usa | age Control | Public Se | vice User Behav | ior Control | VPN Control | Client Version Management Wireless Acce | | | |
| Access Control Name * | wired_web | | | | | | | | | | |
| Concurrent Logins Limit(0 to 99) 0 means no limit * | 1 | | | | | | Synchroniza | tion Accounting Update Interval | | | |
| According to the Terminal Type C | oncurrent Logins (1 to | 99 times) | | | | | | | | | |
| | 🗷 Display accounting | policy infor | mation wher | n user onlin | e | | Automatic B | Binding MAC authentication information quickly | | | |
| | Show users on-line | access cont | rol time | | | | Account information is displayed on a subscriber line | | | | |
| Gateway Access Restriction | It does not allow tr | affic throug | h the gatewa | y server (ga | ateway device needs | to be deplo | eployed linkage in penetration mode) | | | | |
| Export linkage strategy | | * non | NPE / EG ga | teway billin | g model deploymen | t, no need t | o configure the | export collaboration policy | | | |
| Firewall Policy | | * not | deploy firewa | alls linkage, | the need to configu | ire | | | | | |
| Description | | | | | | | | | | | |
| * Please refer to respective label cont | ent for access details | | | | | | | | | | |
| | | | | | | Save | Back | | | | |

5. On the **User Information Check** tab page, select **Wired Web Portal Access** and configure whether to bind accounts with IP/MAC addresses based on actual conditions. Then, click **Save**.

| Shortcut Channel 🔅 | Homepage | System Security | User Access Control | Billing Account | Operation |
|----------------------------------|------------------------|--------------------------|----------------------------|-------------------------|--|
| Location: Access Control > Acces | s Control > Print | | | | |
| Access Control Information | User Information Check | Network Usage Control | Public Service User Behavi | ior Control VPN Control | Client Version Management Wireless Access Properties |
| Allowed Access | Access Mode | Verification Information | | | |
| ✓ Wired 1X Access | User IP(v4) | User IP(v6) | User MAC | Access IP Type | NAS IP(v6) NAS Port |
| Wired Web Portal Access | User IP(v4) | User MAC | Web Authentication | n Device IP(v4) | Web Authentication Device Port |
| G Minday 1V Arrest | User IP(v4) | User MAC | NAS IP(v4) | AP MAC | SSID |

4.2.3.5.4 Verification

Verify that access control is added successfully.

| Short | cut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation |
|-------|---|-----------|---------------|-----------|--------|--|---------|-----------------|-----------|
| Loca | tion: Access Control > Access Control | | | | | | | | |
| Acce | ss Control Name | | 🗹 Genera | al Search | Search | | | | |
| | | | | | | Add | Dele | ete the Selecte | d |
| Total | of 3 records the currently displayed 1 to | 3 records | | | | | | | |
| | Access Control Name | 51000103 | Public Servio | e | | Access Control Typ | e | | Ľ |
| | default | | No | | | default access contr | ol | | |
| | actual | | | | | | | | S |
| | wired_web | | No | | | Common access cor | ntrol | | S |
| | wired_web wireless1x | | No No | | | Common access cor Common access cor | ntrol | | S |
| | wirel_web wireless1x | | No No | | | Common access cor Common access cor | ntrol | | |

4.2.3.6 Billing Policy Configuration

4.2.3.6.1 Function requirements

Configure billing policies based on billing requirements of access users, to pay for Internet access.

4.2.3.6.2 Configuration key points

Billing requirements of access users need to be confirmed with customers and billing policies need to be configured based on actual conditions.

4.2.3.6.3 Configuration steps (monthly milling)

- 1. Log in to the SAM+ management page.
- 2. Choose **Billing** > **Billing Policy**.

| SAM ⁺ security accounting m | NAGEMENT SYSTEM | | | | | | | | | |
|---|---|--|-----------------|------------------------|----------|---------|--------------|--|--|--|
| Shortcut Channel 🔅 | Homepage | System Se | ecurity Us | er Access Co | ntrol | Billing | Account | Operation | | |
| 90 Health Score | Total Online (| Jsers | | (| 0 | Average | Authenticati | on Performanc | | |
| Disk Space Check 3rd Party Development Interface | Account Num License Numb | Account Number 3 License Number Unlimited | | | | | | Current Performance (User/s) Buffer | | |
| Local License Monitoring Internet Traffic Receive Channel Database Integrity Check | SAM Server M | CPU 6% | | | • | | | | | |
| 3. Select Monthly Billing | Policy and cli | ck Add . | | _ | | | | | | |
| Shortcut Channel 🍄 Homepag | e System Security | User Acces | s Control Billi | ng Account Op | peration | | | | | |
| | | | | | | | | | | |
| Location: Billing > Billing Policy Billing Policy Name | | Search | | | | | | | | |
| Location: Billing > Billing Policy Billing Policy Name | General Search Please select the | Search e billing policy which | you want to add | Monthly Billing Poli 🔻 | Add | Delete | the Selected | | | |
| Location: Billing > Billing Policy Billing Policy Name Total of 1 records, the currently displayed 1 to 1 records Billing Policy Name | General Search | Search | you want to add | Monthly Billing Poli 🔻 | Add | Delete | the Selected | Currently | | |

4. Enter the billing policy name, for example, "wired_month", set **Period Type** to **30 Days** or **Month**, and set **Rate (MYR)**, for example, 30 Yuan/month. Then, click **Save**.

| Shortcut Channel 🔅 | Homepage System | n Security | User | Access Control | Billing | Account | Operation | | |
|--|-----------------------------------|-------------------|----------------|----------------------|--------------------|---------------------------|--------------------------|------------------------|-----------------------------|
| Location: Billing > Billing Policy > / | Add > Add Monthly | | | | | | | | |
| Monthly Billing Policy | | | | | | | | | |
| Billing Policy Name* | wired_month | | | | | Description | | | |
| Period Type* | 30 Days Month | | | | | Ending Date | | Enable | (1-31) |
| Compensation | The remaining days during | account suspens | ion can be u | ised after recovery | | Rate (MYR)* | | 30 | |
| Authentication Related Ontions | Allow login when there is a | io remaining inte | rnet traffic o | r the account has u | inpaid charg | es. (Must use 1 | he NTD penetration m | ode with access cont | rol or ACE device. Must use |
| Autoentication Related Options | internet traffic billing plan.) | | | | | | | | |
| Advances Options | Monthly Payment for Limit | ed Duration/ Mo | nthly Paymer | nt for Limited Inter | net Traffic/ I | Monthly Payme | ent for Limited Authent | ication Device Traffic | Configuration |
| • Monthly | r charge: charges extend to the r | ext month. For e | xample, if the | e user creates the a | ccount and Save | paid for the se Return | rvices on the 6th this m | oonth, the fee will be | charged again on the 6th o |

4.2.3.6.4 Verification

Verify that the billing policy is added successfully.

| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | | | |
|--|-------------|----------|---------------|---------------|---------------------|---------|------------------|-----------|---------------------|----------|-----------|
| Location: Billing > Billing Policy | | | | | | | | | | | |
| Billing Policy Name | | 🕑 Gener | al Search | Search | | | | | | | |
| | | Plea | se select the | billing polic | y which you want to | add Mor | nthly Billing Po | li 🔻 Add | Delete the Selected | | |
| Total of 2 records, the currently displayed 1 to | o 2 records | | | | | | | | | 8 | Currently |
| Billing Policy Name | | Descript | | | | | | | | Modif | |
| wired_month | | | | | | | | | | 5 | |
| wireless_month | | | | | | | | | | 1 | |
| | | | | | | | | | | | |

4.2.3.7 User Template Configuration

4.2.3.7.1 Function requirements

Configure user templates based on user attributes for later account creation.

4.2.3.7.2 Configuration key points

It is recommended to classify user templates with the same attribute into a group and give concise and intuitive names to the templates, for example, student monthly billing template or teacher monthly billing template.

4.2.3.7.3 Configuration steps

1. Log in to the SAM+ management page.

2. Choose User > User Template.

| SA | M^+ security accounting ma | NAGEMENT SYSTE | M | | | 122 | | | | |
|--------------|--|----------------|---------|------------|--|---|---------|--------------------|-----------|---------------|
| Sho | rtcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | |
| Loc Billi | ation: Billing > Billing Policy | | ✓ Gene | ral Search | User M Pre-car User G User Te | anagement ncelled Account roup emplate | | akh, Dilling Dal | | Delete the C |
| Tot | al of 2 records, the currently displayed 1 | to 2 records | rica | | Traffic Guarar | Control Policy itor and Guest | | intrity bining For | Au | Delete the st |
| | Billing Policy Name wired_month | | Descrip | tion | Real-na | ame Policy ame System | | | | |
| | wireless_month | | | | MAC A Auto P | uthentication re-cancellation | | | | |
| | | | | | Packag | e Modify History | | | | |
| 3. | Click Add. | | | | | | | | | |

| Location: User > User Template | |
|--------------------------------|-------------------------|
| | |
| | Add Delete the Selected |
| Template Name | Description |

4. Enter the template name, for example, "wired_month", and click **Save**.

| 0 | | Add User Template | 2 |
|---|--|------------------------|-------|
| U | ser Templates | | contr |
| | Template Name* | wired_month | |
| | Custom Options | Allow self-change plan | |
| | Monthly Modificatio Limit (1~10 times) Description | n 10 | l |
| | | Save Cancel | |
| | | Save Cancel | |

4.2.3.7.4 Verification

Verify that the user template is added successfully.

| Shortcut Chai | nnel 🍄 | ŀ | lomepage | System | Security | User | Access Control | Billing | Account | Operation | |
|---|--|---|----------------------------------|---------------------------|------------------------------------|-----------------------|-----------------------|--------------|----------------|----------------|--------------|
| Location: Use | er > User Template | > User Template | es - | | | | | | | | |
| Template I Self-Modif Description | wired_month Not allowed to | change the p | lan | | | User 1 | emplates: | wired_month | | | |
| | Plan | | | _ | _ | _ | | _ | _ | Rule | _ |
| | - Hall | | Access Area | | De | fault Rule | Service | ; | Allow Acce | ss Time | Acce |
| The n Users | umber of repeated can use different s | l logins of the pla ervices for Interr | an is user's n net access anc | naximum nu I the numbe | imber of online r of online use | sTAs. rs of the sa | me service is restric | ted by the I | number of repe | ated logins of | the correspo |
| | | | | | | | | | | | |

4.2.3.8 User Plan Configuration

4.2.3.8.1 Function requirements

Configure a user plan to cover access limits of authenticated users, including the area, time range, access control, and billing policy. A user plan is akin to a phone service package.

4.2.3.8.2 Configuration key points

A plan covers all control options and fees for access users. Be sure to clearly confirm plans with customers before configuration.

4.2.3.8.3 Configuration steps

1. In the configured user template "wired_month", click Add Plan.



2. Enter the plan name, for example, "wired_month", select a configured billing policy or **Not Charging** based on actual requirements, and then click **Save**.

| O Add Plan | |
|---|---|
| Plan | |
| Plan * Concurrent Logins Limit Billing Policy Cycle expired and suspend use MAC Binding Validity Description | wired_month Enable 1 (1 ~ 99 times) wired_month A. Activate 0 (0-365 days, 0 for not limited) |
| Sa | ave Cancel |

3. Click **Modify Plan** and modify the access area, access time range, access control, and billing mode.

| Template Name: wired_month User Templates: wired_month Wir | | | | | | | | | | |
|--|--|--|---------------------------|--------------------------------|-------------------------------|-------------------------------|-----------------|------------------|--------------------------|--|
| | Plan | | Dafash Dala | fur la | Rule | Auron Control | Differe Dellars | 8-4- | | |
| | Nameswired_month Concurrent Logins Limit :1 Billing Policywired_month Cycle Expired to Suspend User.JNot Enabled Suspension End Time: MAC Binding Expirys0Day Description: | Unlimited | • | default | Unlimited | default | Not Charging | Add Ru Modify | le Rule the Policy | |
| | The number of repeated logins of the plan is user' Users can use different services for Internet access a | s maximum number of online nd the number of online user | STAs. s of the same se | rvice is restricted by the num | ber of repeated logins of the | corresponding access control. | | | | |

4. Modify the rule based on actual conditions. The figure below shows that the access area of authenticated users is unlimited, access control is set to "wired_web", the access time range is unlimited, and billing is performed based on the plan"wired_month".

| O Modify Rule | |
|---|---|
| Rule | |
| Plan Access Area | wired_month Unlimited |
| Service* Access Control Allow Access Time Billing Policy | Wired_web ▼ Without limiting the I ▼ |
| | Save Cancel |
| | |

4.2.3.8.4 Verification

Verify that the plan meets customer requirements.

| Locatio Temp Self-I Descr | n: User > User Template > User | lates | plan | | User Templates | : wired_month | | | | Return to |
|------------------------------------|--|------------------------------------|-------------------------|--|-----------------------------|---------------|---------------------|------------------------------|----------------|-----------|
| | Plan | | Access Area | Default Rule | Service | الم | Rule | Access Control | Billing Policy | Rule |
| | Name:wired_month Concurrent Logins Limit :1 Billing Policy:wired_month Cycle Expined to Suspend User.:Not Suspension End Time: MAC Binding Expiry:0Day Description: | t Enabled | Unlimited | • | default | Unlimite | d | wired_web | Not Charging | |
| | The number of repeated logins of the Users can use different services for Int | plan is user's ternet access ar | maximum number of onlin | online STAs. e users of the same se | ervice is restricted by the | number of rep | eated logins of the | corresponding access control | | |

4.2.3.9 User Group Configuration

4.2.3.9.1 Function requirements

Add authenticated users with the same attribute to the same group, and define a response user template and plan for the user group to prepare for later account creation.

4.2.3.9.2 Configuration key points

It is recommended to group access users by attribute, for example, group users on campus networks into "student user group" or "teacher user group".

4.2.3.9.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose User > User Group.



4. Enter the user group name, for example, "wireless_month", and select the default user template and default plan. Then, click **Save**.

| iser Group * | wireless_month | Parent Group Name * | root |
|---------------------------|------------------|---------------------|------------------|
| Default User Template* | wireless_month • | Default Plan* | wireless_month • |
| Jplink Speed | 0 | Downlink Speed | 0 |
| 8~261120KBps) | 0 | (8~261120KBps) | 0 |
| Jser group authentication | | Downlink Speed | |
| s successful hoplinks. | | (8~261120KBps) | |
| Description | | Creator | admin |

4.2.3.9.4 Verification

Verify that the user group is added successfully.

| Location: User > User Group | Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account |
|---|-----------------------------|----------|---|---|--|-------------------------------|-----------------|----------------|
| Expand All/Collapse All Change User Group User Group User Group * wireless_month • dot1x • wireless_month • Default User Template* wireless_month • Uplink Speed (8~261120KBps) • User group authentication is successful hoplinks. • Description • • | Location: User > User Group | | | | | | | |
| Please perform system operation when idle.) | Expand All/Collapse All | | Change User User Group * Default User 1 Uplink Speed (8~261120KB User group au is successful H Description | Group Femplate* ps) uthentication toplinks. | wirele wirele ¢ Synce Please | ss_month ss_month involution | lefault user to | emplate or pli |

4.2.3.10 Account Creation

4.2.3.10.1 Function requirements

Create accounts for users in the SAM+ system.

4.2.3.10.2 Configuration key points

- 1. The account creation process generally requires users to go to business halls and apply for accounts by using their ID cards.
- 2. Accounts with the names same as those on their ID cards are registered during account creation.

3. A user group and a user template need to be selected during account creation as planned.

4.2.3.10.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose User > User Management.

| SAM ⁺ security accounting management system | | | | | | | | | | | | |
|--|----------|--------|----------|---------------|-----------------|---------|---------|-----------|---|--|--|--|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | | | | |
| Location: User > User Management | | | | User M | anagement | | | | | | | |
| User Search User Search | | | | Pre-car | ncelled Account | | | | | | | |
| | | | | User Gi | roup | | ~ | | | | | |
| Import Search | Username | | | User Template | | | (!) | | M | | | |
| | Account | | | Traffic | Control Policy | | | | | | | |
| Create Account | Delener | | | Guaran | tor and Guest | | | | | | | |
| Batch Account Activation | Balance | | | Real-na | ame Policy | | | | | | | |
| | U | | | | | | - | | | | | |

3. Click **Create Account** in the left pane.

| SAM ⁺ security accounting management system | | | | | | | | | | | |
|--|-------------------------|--|--|--|--|--|--|--|--|--|--|
| Shortcut Channel 🛛 🌼 | Homepage System Secu | | | | | | | | | | |
| Location: User > User Management | | | | | | | | | | | |
| User Search | Basic Information | | | | | | | | | | |
| Import Search | Username* | | | | | | | | | | |
| | Password* | | | | | | | | | | |
| Create Account | User Group* | | | | | | | | | | |
| Batch Account Activation | User Templates | | | | | | | | | | |
| Import Accounts | Self-service Permission | | | | | | | | | | |
| | Auto Pre-Cancellation | | | | | | | | | | |
| Import Changes | Guarantor Ranking | | | | | | | | | | |
| Import Payments | Advanced Options | | | | | | | | | | |

4. Enter the username and password, select a user group, user template, and plan. Then, click **Save**.

| Username* | wireless1x | Full Name | |
|-------------------------|---|---------------------|--------------------------|
| Password* | ••• | Confirm Password* | ••• |
| User Group* | wireless_month | Account | Same As username |
| User Templates | ● Use Default Template of User Group ^O Customize | | |
| Self-service Permission | All Self-service Privileges 🔹 | Authentication-free | Verification is required |
| Auto Pre-Cancellation | | BACL | Please Select 🔻 🏹 |
| Guarantor Ranking | Please Select 🔻 | | |
| Advanced Options | Show Advanced User Settings options | | |
| Sex | Please Select 🔻 | Email Address | |
| ID Type | Please Select 🔻 | ID No. | |
| Education Level | Please Select 🔻 | Online Information | |
| Telephone No. | | Mobile Phone | |
| | | Postal Code | |

4.2.3.10.4 Verification

1. In the left pane of the **User Management** page, click **User Search**. In the displayed right pane, click **Search**. The added user is displayed.

| Shortcut Channel 🔅 | Homepage | e System | Security | User | Access Control | Billing | Account | Operation | | | | | |
|---|------------|--------------------|-----------------|------------|--------------------|-----------|------------|-------------|------------|----------------|--------|-------------------|----------|
| Location: User > User Management User Search | | | | | | | | ✤ To Search | | | | | |
| Import Search | Update | | Delete | | Pre-delete | | Pay and Re | fund | Suspend | | Resume | | Notifica |
| Create Account | Total of 1 | records, the curre | ently displayed | 1 to 1 rec | ords Select All Re | cords | Colu | mn Config | | | 6 | Currently 1 | /1Page |
| Batch Account Activation | ۰. | Username | - | | uli Name | | | | nt Balance | User Templates | | Binding Inf on | |
| Import Accounts | | wireless1x | | | | wireless1 | x | 0.00 | | wireless_month | | | |
| Import Changes Import Payments | L | |] | | | | | | | | | | |
| Import Channe Licer Templates and | | | | | | | | | | | | | |

4.2.3.11 Payment

4.2.3.11.1 Function requirements

Collect fees from newly created users, so that they can be authenticated, be charged, and access the Internet.

4.2.3.11.2 Configuration key points

The payment operation involves fees. Ensure that paid fees are consistent with the fees recorded in the system.

4.2.3.11.3 Configuration steps

- 1. Log in to the SAM+ management page.
- 2. Choose Billing > Fees Management.

| SAM+ | | | | | | | |
|--|-----------------|------------------------|----------|-------------------|-------------|-------------------|--------------------------|
| | EMENT SYSTEM | | | | _ | | |
| Shortcut Channel 💠 | Homepage System | n Security | User | Access Control | Billing | Account | Operation |
| Location: Billing > Fees Management | | | | | Account | Management | |
| | | | | Г | Fees Mar | nagement | |
| Account ID | Status | Please Select | • | | Billing Co | ompensation | Advanced Search |
| Balance Fro m (MYR) | То | | | | Billing Po | olicy | |
| | | | | | Customi | ze Policy | |
| | Pleas | e select the operation | ion type | Payment | ▼ Bala | nce to be Paid (N | IYR) |
| | | De | | A | un conto | - Funda - Cha | with a Database of Table |
| | | Paj | iy All | Account Enquiry (| upon Servic | e expiry Sho | w the Background Tasks |
| Total of 3 records, the currently displayed 1 to 3 | records | | | | | | |

3. The newly created user has insufficient balance. Click the icon in the **Payment** column.

| Shortc | ut Channel 🔅 | Homepage | System Se | curity User | Access Control | Billing | Account | Operation | | | |
|--------------------------|---|---|--|--------------------|-----------------|---|----------------|-------------------------|--------------------------------------|---------------------|--------|
| Locati | on: Billing > Fees Manageme | ent | | | | | | | | | |
| Accou Balanc m (MY | int ID ce Fro (R) | | Status Please | e Select 🔹 | | General General | Search | Search Advanced Se | earch | | |
| | | | Please select | the operation type | Payment | ▼ Balar | ice to be Paic | i (MYR) | Payment | | |
| | | | | Pay All | Account Enquiry | Upon Service | Expiry | Show the Background Tas | ks | | |
| | | | | | | | | | | | |
| Total | of 3 records, the currently disp | ayed 1 to 3 records | | | | | | | | 😰 Currei | ntly 1 |
| Total (| of 3 records, the currently disp Account ID | ayed 1 to 3 records Full Name | Balance (MYR) |) is Overdra | ft Allowed C | redit Limit (N | AYR) | Available Credit (MYR) | Status | Payment | ntly 1 |
| Total (| of 3 records, the currently disp Account ID wireless1x | ayed 1 to 3 records Full Name | Balance (MYR) 123.00 | Is Overdra | ift Allowed C | redit Limit (N | IYR) | Available Credit (MYR) | Status Normal | B Curren Payment | ntly 1 |
| Total o | of 3 records, the currently displet Account ID wireless1x dot1x | ayed 1 to 3 records Full Name | Balance (MYR) 123.00 246.00 | Is Overdra | ift Allowed C | redit Limit (N | IYR) | Available Credit (MYR) | Status Normal Normal | Curren Payment | ntly 1 |
| | of 3 records, the currently displ Account ID wireless1x dot1x 123 | ayed 1 to 3 records Full Name 123 | Balance (MYR) 123.00 246.00 0.00 | No No No | ft Allowed C | redit Limit (N | AYR) | Available Credit (MYR) | Status Normal Normal Normal | Current Payment | ntly 1 |

4. Collect the fees, record the fees actually paid by the user in the system, and click **Payment**.

| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | | |
|-------------------------------------|-------------------|-------------|----------|--------|---------------------|---------|----------------|-----------------|---------------|------|
| Location: Billing > Fees Management | t > Payment | | | | | | | | | |
| Account | | | | | | | | | | |
| Account ID | wireless1x | | | | | | Email | | | |
| Overdraft Options | The account can b | e overdrawr | ı. | | | | | | | |
| Balance (MYR) | 123.00 | | | | | | | | | |
| Status | Normal | | | | | | Description | | | |
| Account Associated With The User | Q | | | | | | Account Act | ivation Fee | Unpaid | |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | _ | | | | | | | | |
| Balance to be Paid (MYR) | 123 | | | | | | Receivables | (MYR) | 123 | |
| Account Activation Fee (MYR) | | | | | | | Receivables | (MYR) | | |
| <u></u> | | | | | | | | | | |
| | | Payment | Reset | Returr | n to Expense Manage | ement | Return to Acco | ount Management | Return to Use | er M |
| | | | | | | | | | | |
| | | | | | | | | | | |
| | | | | | | | | | | |

4.2.3.11.4 Verification

1. Verify that the fees are paid successfully.

Account (wireless1x) payment for (MYR) 123.00 is successful!

 Verify that the fees are corrected and the account is in the normal state. As shown in the figure below, 123 Yuan is deducted from the user account "wireless1x" for the current month, and the account has 246 Yuan balance, and is in the normal state.

| Shortc | ut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation |
|--------------------------|--------------------------------|------------------------|-------------|-----------------|------------|----------------|----------------|---------------|----------------|
| Locati | on: Billing > Fees Manage | ment | | | | | | | |
| Accou Balanc m (MY | nt ID e Fro R) | 2 S | itatus o | Please Select | V | | | Search | Search Ac |
| | | | Please | select the oper | ation type | Payment | ▼ Bala | nce to be Pai | d (MYR) |
| | | | | | Pay All | Account Enquir | ry Upon Servic | e Expiry | Show the Backg |
| Total o | of 3 records, the currently di | splayed 1 to 3 records | | | | | | | |
| | Account ID | Full Name | Balance | (WITH) | Is Overdra | ft Allowed | Credit Limit (| MYR) | Available Cred |
| | wireless1x | | 246.00 | | No | | | | |
| | dot1x | | 246.00 | | No | | | | |
| | 123 | 123 | 0.00 | | No | | | | |
| | | | | | | Total Ba | alance: 492.00 | Total Overd | raft:0.00 |

4.2.4 [Optional] MAB Authentication

4.2.4.1 [Optional] MAB Authentication in Automatic Mode

4.2.4.1.1 Function requirements

Enable MAB authentication in automatic mode on SAM+.

The process of MAC binding in automatic mode is as follows (Web authentication is required for initial access):



In automatic mode, users do not need to select **Smart Login** on the authentication page, which is different from the operation in manual mode.

4.2.4.1.2 Configuration key points

Basic settings of Web authentication need to be completed to implement MAB authentication, and details are not described here.

For basic settings of Web authentication on SAM+, see "RG-N18000 — Web Authentication (Wired & Wireless)" in "Common Scenario — Authentication" in "SAM+ and ePortal Configuration."

4.2.4.1.3 Configuration steps

1. Choose Access Control > Access Control > Modify > User Information Check, and select MAC Fast Access.

| Sh | ortcut Channel 🔅 | Homepage System | n Security Use | r Access Control | Billing Account | Operation |
|----|---|-------------------------|----------------------|-----------------------|---------------------|--|
| Lo | cation: Access Control > Access Control > | Modify | | | | |
| | Access Control Information User Inform | ation Check Network | Usage Control Public | c Service User Behavi | or Control VPN Cont | Client Version Management Wireless Access Properties |
| | Allowed Access | Access Mode Verifica | tion Information | | | |
| | Wired 1X Access | User IP(v4) | User IP(v6) | User MAC | NAS IP(v4) | NAS IP(v6) NAS Port |
| | | VLAN | Internal VLAN | External VLAN | Access IP Type Sta | tic 🔻 |
| | Wired Web Portal Access | User IP(v4) | User MAC | Web Authentication | Device IP(v4) | Web Authentication Device Port |
| | Wireless 1X Access | User IP(v4) | User MAC | NAS IP(v4) | AP MAC | SSID |
| | | Access IP Type Static * | | | | |
| | Wireless Web Portal Access | User MAC | NAS IP(v4) | AP MAC | SSID | |
| | Smart Device 1X Access | User MAC | NAS IP(v4) | AP MAC | SSID | |
| Г | MAC Fast Access | User MAC | NAS IP(v4) | AP MAC | SSID | NAS Port |
| L | | VLAN | Internal VLAN | External VLAN | | |
| | Wired Standard Portal Access | User IP(v4) | User MAC | NAS IP(v4) | NAS Port | VLAN |
| | | Internal VLAN | External VLAN | | | |
| | Wireless Standard Portal Access | User IP(v4) | User MAC | NAS IP(v4) | AP MAC | SSID |
| | in the second second | NAS Port | VLAN | Internal VLAN | External VLAN | |
| | ✓VPN Dial-up access | User IP(v4) | NAS IP(v4) | | | |
| | TRANSFE During Lawrence Access | | | | | |

2. Choose Access Control > Access Control > Modify > Access Control Information, and select Automatic Binding MAC authentication information quickly.

| ortcut Channel 🔅 | Homepage | System Security | User Ac | cess Control | Billing | Account | Operation |
|--|--------------------------|-------------------------|---------------------|-------------------|--------------|---|--|
| ocation: Access Control > Access Cor | ntrol > Modify | | | | | | |
| Access Control Information User | Information Check N | etwork Usage Control | Public Service | User Behavio | or Control | VPN Control | Client Version Management Wireless Access Properties |
| Access Control Name * | wired_web | | | | | | |
| Concurrent Logins Limit(0 to 99) 0 means no limit * | 1 | | | | | Synchronizat | tion Accounting Update Interval |
| According to the Terminal Type C | oncurrent Logins (1 to 9 | 9 times) | | | _ | | |
| | Display accounting p | olicy information whe | n user online | | Automatic Bi | inding MAC authentication information quickly | |
| | Show users on-line a | ccess control time | | | | | ormation is displayed on a subscriber line |
| Gateway Access Restriction | It does not allow traf | ffic through the gatewa | ay server (gatewa | ay device needs t | to be depl | oyed linkage in p | penetration mode) |
| Export linkage strategy | | * non NPE / EG ga | teway billing mo | del deployment | no need | to configure the | export collaboration policy |
| Firewall Policy | | * not deploy firew | alls linkage, the r | need to configur | e | | |
| Description | | | | | | | |
| * Please refer to respective label conte | ent for access details | | | | | | |
| | | | | | Save | Back | |

4.2.4.1.4 Verification

- 1. When a user uses a mobile phone to connect to an SSID with MAC authentication enabled, Web authentication needs to be completed for initial access.
- On SAM+, choose User > MAC Authentication and check whether information about the MAB authenticated user has been learned.

| Shortcut Channel 🔅 | Homepage System | Security User | Access Control E | lling Account | Operation | | |
|-------------------------------------|-----------------|-------------------------|------------------|----------------|------------------|--------|------------------------|
| Location: User > MAC Authentication | | | | | | | |
| Username | | User MAC | | | 🗹 General Search | Search | |
| Registraion Time F | | Registraion Time T o | m | 3 | | | |
| Expired From | | Expired To | | 3 | | | |
| | | | Add Dele | e the Selected | Delete All | | |
| There were no results found. | | | | | | | 😰 Currently 1 /1Page 🖣 |
| Register User | Register MA | | MAC Bindi | g Expiry | Register | | Registrar |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

3. After the user goes offline, enable the user to connect to the SSID with MAC authentication enabled, and check online user records on SAM+.

| SAM ⁺ security accounting mana | GEMENT SYSTEM | | | | | | | | |
|---|------------------------------|----------------------|---------------------|------------------|---------------|---------------------------------|---------------------|----------|-----------|
| Shortcut Channel 🔅 | Homepage | System Security | User Acc | ess Control Bil | lling Account | Operation | | | |
| Location: Operation > Online User | | | | | | | | | |
| Username User IP(v4) | Full Name User Temp te | la Please Select | | 6 General Search | Search A | dvanced Search | | | |
| | | Force t | he Users Offline | Delete the Sele | cted Delete A | II Show the Background | l Tasks | | |
| | | Add the users to the | blacklist when forc | ed offline 5 | mir | is effective; blacklist message | User is in the blac | cklist! | |
| There were no results found. Column Confi | 9 | | | | | | R | efresh 📓 | Currently |
| Username User IP | v4) L | Jser MAC N | AS IP(v4) | NAS Port | Service | Access Control | Login Time | | On |
| Invalid wireless user internet traffic blockage | | | | | | | | | |

4.2.4.2 [Optional] MAB Authentication in Manual Mode

4.2.4.2.1 Function requirements

Enable MAB authentication in manual mode on SAM+.

The process of MAC binding in manual mode is as follows (Web authentication is required for initial access):



In manual mode, users need to select **Smart Login** on the authentication page, which is different from the operation in automatic mode.

4.2.4.2.2 Configuration key points

Basic settings of Web authentication need to be completed to implement MAB authentication, and details are not described here.

For basic settings of Web authentication on SAM+, see "RG-N18000 — Web Authentication (Wired & Wireless)" in "Common Scenario — Authentication" in "SAM+ and ePortal Configuration."

4.2.4.2.3 Configuration steps

1. Choose Access Control > Access Control > Modify > User Information Check, and select MAC Fast Access.

| Shortcut Channel 🔅 | Homepage Syste | m Security Us | er Access Control | Billing Account | Operation |
|---|---------------------|---------------------|-------------------------|----------------------|---------------------------------|
| Location: Access Control > Access Control > | Modify | | | | |
| Access Control Information User Inform | nation Check Networ | k Usage Control Pub | lic Service User Behavi | ior Control VPN Cont | rol Client Version Management W |
| Allowed Access | Access Mode Verific | ation Information | | | |
| Wind 1X Access | User IP(v4) | User IP(v6) | User MAC | NAS IP(v4) | NAS IP(v6) NAS Port |
| Wiled IX Access | VLAN | Internal VLAN | External VLAN | Access IP Type Sta | tic 🔻 |
| Wired Web Portal Access | User IP(v4) | User MAC | Web Authentication | Device IP(v4) | Web Authentication Device Port |
| Wireless 1X Access | User IP(v4) | User MAC | NAS IP(v4) | AP MAC | SSID |
| | Access IP Type St | atic 🔻 | | | |
| Wireless Web Portal Access | User MAC | NAS IP(v4) | AP MAC | SSID | |
| Smart Device 1X Access | User MAC | NAS IP(v4) | AP MAC | SSID | |
| MAC Fast Access | User MAC | NAS IP(v4) | AP MAC | SSID | NAS Port |
| | VLAN | Internal VLAN | External VLAN | | |
| | Ellear ID4+4 | | INAC ID640 | INAC Dort | |

2. Choose Access Control > Access Control > Modify > Access Control Information, ensure that Automatic Binding MAC authentication information quickly is deselected.

| Access Control Information Use | r Information Check | Network Usage Control | Public Service | User Behavior Control | VPN Control | Client Version Management | Wireless Access Properties |
|--|------------------------|----------------------------|---------------------|-------------------------|--------------------|---------------------------------|----------------------------|
| Access Control Name * | wired_web | | | | | | |
| Concurrent Logins Limit(0 to 99) 0 means no limit * | 1 | | | | Synchronizatio | on Accounting Update Interval | |
| According to the Terminal Type | Concurrent Logins (1 t | o 99 times) | | _ | | | |
| | 🗷 Display accounti | ng policy information when | user online | | Automatic Bin | ding MAC authentication infor | mation quickly |
| | Show users on-li | ne access control time | | | Account inform | mation is displayed on a subscr | iber line |
| Gateway Access Restriction | It does not allow | traffic through the gatewa | y server (gateway | device needs to be depl | oyed linkage in pe | enetration mode) | |
| Export linkage strategy | | * non NPE / EG gat | eway billing mod | el deployment, no need | to configure the e | xport collaboration policy | |
| Firewall Policy | | * not deploy firewa | lls linkage, the ne | eed to configure | | | |
| Description | | | | | | | |
| | | | | | | | |

4.2.4.2.4 4. Verification

- 1. When a user uses a mobile phone to connect to a SSID with MAC authentication enabled, Web authentication needs to be completed for initial access, and **Enable MAB Authentication** needs to be checked.
- 2. On SAM+, choose **User** > **MAC Authentication** and check whether information about the MAB authenticated user has been learned.

| SAM ⁺ security accounting M | IANAGEMENT SYSTEM | | | | |
|--|-------------------|-------------------------|------------------------|-------------------|----------|
| Shortcut Channel 🔅 | Homepage System | n Security User | Access Control Billing | Account Operation | |
| Location: User > MAC Authentication | | | | | |
| Username | | User MAC | | 🕑 General Search | Search |
| Registraion Time F rom | | Registraion Time T o | | | |
| Expired From | | Expired To | | | |
| | | | Add Delete the Se | lected Delete All | |
| There were no results found. | | | | | B |
| Register User | Register MA | \C | MAC Binding Expiry | / Register | |
| | | | | | |
| | | | | | |
| | | | | | |

3. After the user goes offline, enable the user to connect to the SSID with MAC authentication enabled, and check online user records on SAM+.

| GEMENT SYSTEM | | | | ی adm | in 🕼 About 🖒 Logout |
|-------------------|---|--|--|---|--|
| Homepage System S | iecurity User Access Contro | ol Billing Account | Operation | | |
| | | | | | |
| Full Name | 🖌 General | Search Search Adva | inced Search | | |
| User Templa te | t v | | | | |
| | Force the Licen Offline Delete | a the Salacted Delete All | Show the Packground Tarke | | |
| - Add the use | s to the blacklist when forced offline | | Heating blacklist message Liese is in | the blackford | |
| E Add the user | s to the blacklist when forced online | initis e | nective, blacklist message oser is in | ule blackisc | |
| 1 | | | | Refresh 😰 Currently 1/1Page | 9 Go Very Page 10 • Entry |
| vaj Oser MAC | NAS IP(V4) NAS P | ort Service | Access Control Login I | ime Online Duration | Internet Trainc Check |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |
| | GEMENT SYSTEM Homepage System S Full Name User Templa Please Selec te Add the user User MAC | GEMENT SYSTEM Homepage System Security User Access Contre Full Name & General User Templa Please Select • Force the Users Offline Deleter Add the users to the blacklist when forced offline Add the users to the blacklist when forced offline User MAC NAS IP(v4) NAS P | CEMENT SYSTEM Homapage System Security User Access Control Billing Account Full Name User Templa Please Select • te Force the Users Offline Delete the Selected Delete All Add the users to the blacklist when forced offline 5 mins e with User MAC NAS IP(v4) NAS Port Service | CEMENT System Homepage System Security User Access Centrol Billing Account Operation Full Name Image: Select image Image: Select image Image: Select image Image: Select image: Selec | CEMENT SYSTEM CONTROL OF Access Control Billing Account Operation Full Name General Search Search Advanced Search User Templa Fiesse Select Force the Users Offline Delete the Selected Delete All Show the Background Takks Add the users to the blacklist when forced offline Delete All Show the Background Takks Add the users to the blacklist when forced offline Refresh @ Currently 1_//Page wdy User MAC NAS IP(v4) NAS Port Service Access Control Login Time Online Duration |

4.2.4.3 [Optional] Binding Validity Setting of MAB Authentication

4.2.4.3.1 Function requirements

The MAC binding validity period (0–365 days) can be configured for a plan. After the validity period expires, MAC addresses are automatically unbound and the MAB authentication permission for the user is canceled.

4.2.4.3.2 Configuration key points

N/A

4.2.4.3.3 Configuration steps

| | ption: | e plan | | | | |
|-------|---|---|-----------------|--|----------|-------------|
| | | Access Area | Defau | Q Modify Plan | rol | Billing Pol |
| III 1 | Conclusion Cognized and Conclusion of State Conclusion Conclusico Conclusion Conclusion Conclusico Conclusico Conclusico | Unlimited s maximum number of online s and the number of online users | STAs. of the | Plan Plan * Concurrent Logins Liait Billing Policy Cycle expired and supend user. MaC Binding Validity Description Save Cancel | s contro | Not Chargin |

4.2.4.3.4 Verification

N/A

4.2.5 [Optional] SSID-based Authentication Page Pushing

4.2.5.1 Function requirements

In some projects involving the networks of multiple ISPs, schools may request different Web authentication pages be pushed based on the SSIDs of the ISP networks.

The ePortal system allows displaying different authentication pages based on SSIDs or user groups.

4.2.5.2 Configuration key points

In the simplistic network solution, the core device RG-N18000 cannot associate with APs to obtain SSIDs of users who adopt wireless authentication and the VLAN-based SSID mapping function is required.

For the configuration of the VLAN-based SSID mapping on the RG-N18000, see "Web Authentication — IP/VLAN-based SSID Mapping" in "Common Scenario — Authentication" in "RG-N18000 Configuration."

4.2.5.3 Configuration steps

1. In **Page Management**, customize authentication pages for user PCs and mobile phones based on customer requirements (one authentication page for the SSID of each ISP).



2. Complete the mapping between different SSIDs and customization pages.

位置:网络访问门户系统>页面定制>添加页面定制

| | 页面定制 |
|-----------|----------|
| * 模式 | SSID模式 ~ |
| ★ SSID或组名 | |
| PC页面管理 | 请选择 |
| 手机页面管理 | 请选择 |
| | 保存電子 |

4.2.5.4 Verification

Verify that the different customized authentication pages are displayed when users connect to different SSIDs.

5 Simplistic Network Configuration Examples (Important)

5.1 Configuration Examples of Access Isolation Solution + Wireless Isolation Solution

5.1.1 Customer Requirements

- 1. Layer-2 network requirements
- Deploy the access isolation solution to implement layer-2 isolation of users on the whole network.
- Deploy centralized forwarding on the wireless network.
- Enable IPv6 on the whole network, so that IPv6 users can access the network only after IPv4 authentication succeeds.
- Use the core device as the wired/wireless gateway and authentication NAS on the whole network, to provide unified management, and support a maximum of 20,000 online clients.
- 2. Requirements related to authentication types
- In the office area, deploy wired and wireless Web authentication and MAB authentication.
- In the student dormitory area, deploy wired 802.1x authentication, wireless 802.1x authentication, and wireless Web authentication.
- In the visitor area, deploy QR code authentication.
- In the headmaster office and other school director offices, deploy authentication exemption.
- Exempt re-authentication for users who move in the same area.

- In the dormitory area and office area, deploy no-traffic go-offline so that clients automatically go offline when the clients generate no traffic in 15 minutes.
- 3. Requirements related to authentication access control (Note: Access time control is only used for testing, and the actual deployment is subject to the onsite situation.)
- In the student dormitory area, network access is allowed only at 10:30–10:32.
- In the teaching area, network access is prohibited for student users at 9:00–12:00 and 14:00–16:00.
- In the office area, student users cannot be authenticated.
- 4. Address management requirements (Note: Address segment assignment is only used for case demonstration, and the actual deployment is subject to the onsite situation.)
- For the wired network, configure a private address with a 20-bit subnet mask for each area, and a private address with a 24-bit subnet mask for each building:

Office area: 10.1.16.0/20 (building 1: 10.1.16.0/24, building 2: 10.1.17.0/24 ... building 5: 10.1.20.0/24)

Student dormitory area: 10.1.32.0/20 (building 1: 10.1.32.0/20, building 2: 10.1.33.0/20 ... building 5: 10.1.36.0/20)

• For the wireless network:

Office area: 10.1.16.0/20 (building 1 for 802.1x authentication: 10.1.21.0/24, building 1 for Web authentication: 10.1.22.0/24, building 2 for 802.1x authentication: 10.1.23.0/24, and building 2 for Web authentication: 10.1.24.0/24)

Student dormitory area: 10.1.32.0/20 (building 1 for 802.1x authentication: 10.1.37.0/24, building 1 for Web authentication: 10.1.38.0/24, building 2 for 802.1x authentication: 10.1.39.0/24, and building 2 for Web authentication: 10.1.40.0/24)

(Note: One super VLAN is set in each area for both wired and wireless networks. You can also set one super VLAN in each area for the wireless network according to actual situations.)

• Special services need independent network segments:

Door status control service: 10.0.10.0/24

All-in-one card service: 10.0.11.0/24

Video monitoring service: 10.0.12.0/24

Wired device NMS: 10.0.1.0/24

AP management address: 10.0.2.0/24

- 5. Other requirements
- Only the network in the new campus is reconstructed. In the network in the old campus, layer-3 protocols are still used to connect to the RG-N18000, and the aggregation device serves as the user gateway and DHCP relay, and is interconnected with the RG-N18000 via OSPF.
- Configure the escape function on the RADIUS server and ePortal server, to avoid affecting the users' online services if either server is down.
- Configure VLAN pruning to avoid broadcast floods.
- Configure passive ports for routing optimization to avoid unnecessary protocol overheads of the CPU.

5.1.2 Topology



5.1.3 Configuration Precautions

- 1. The RG-N18000 does not support 802.1x authentication. Therefore, configure the wireless 802.1x NAS function on the AC.
- 2. IPv6 does not support direct authentication. Therefore, configure IPv6 authentication to compatible mode, so that IPv6 users can access the network after successful IPv4 authentication.
- 3. To avoid re-authentication for users who move in the same area, configure the migration function for authenticated users on the RG-N18000.
- 4. Enable AM rules to plan IP addresses for buildings in each area.
- 5. DHCP relay is enabled on the aggregation device of the original network. To prevent DHCP packets from being dropped by the DHCP snooping module on the RG-N18000, run the **ip dhcp snooping check-giaddr** command on the RG-N18000.

- 6. Configure the escape function on the RG-N18000 for the RADIUS server and portal server.
- 7. Configure VLAN pruning for the downlink trunk port of the RG-N18000.

5.1.4 VLAN/IP Planning on the Live Network

The following tables list VLAN/IP plans for the wired and wireless networks in the student dormitory area (plans for other areas are the same).

Wired network VLAN/IP planning for the student dormitory area:

| Device Model | Device type | Position | Management Address | Sub VLAN | Super VLAN | IP Address Segment | Gateway | Network Management VLAN | Door Status Control VLAN | All-in-One Card VLAN | Video Monitoring VLAN |
|-----------------|---------------------------|--|-----------------------|-------------|---------------|--------------------------|-------------|-------------------------------|-----------------------------------|----------------------------|-----------------------------|
| S2928G | Floor access switch | 1F, building 1, student dormitory area | 10.0.1.10 | 200 | 2001 | 10.1.32.0 | 10.1.32.254 | 3000 | 3010 | 3011 | 3012 |
| S2928G | Floor access switch | 2F, building 1, student dormitory area | 10.0.1.11 | 201 | 2001 | 10.1.33.0 | 10.1.32.254 | 3000 | 3010 | 3011 | 3012 |
| S2928G | Floor access switch | 1F, building 2, student dormitory area | 10.0.1.12 | 202 | 2001 | 10.1.34.0 | 10.1.32.254 | 3000 | 3010 | 3011 | 3012 |
| S2928G | Floor access switch | 2F, building 2, student dormitory area | 10.0.1.13 | 203 | 2001 | 10.1.35.0 | 10.1.32.254 | 3000 | 3010 | 3011 | 3012 |
| S2928G | Floor access switch | 1F, building 3, student dormitory area | 10.0.1.14 | 204 | 2001 | 10.1.36.0 | 10.1.32.254 | 3000 | 3010 | 3011 | 3012 |

Wireless network VLAN/IP planning for the student dormitory area:

| Location | AP Management VLAN | AP Management Network Segment | Gateway | Sub VLAN of Web Authentication | IP Address Segment of Web Authentication | Sub VLAN of 802.1x Authentication | IP Address Segment of 802.1x Authentication | Super VLAN | Gateway | SSID of Web Authentication | SSID of 802.1x Authentication |
|--|--------------------------|--|------------|--------------------------------------|---|---|--|---------------|-------------|-------------------------------|----------------------------------|
| Building 1, student dormitory area | 3001 | 10.0.2.0/24 | 10.0.2.254 | 301 | 10.1.37.0/24 | 351 | 10.1.38.0/24 | 2001 | 10.1.32.254 | su-web | su-1x |
| Building 2, student dormitory area | 3001 | 10.0.2.0/24 | 10.0.2.254 | 302 | 10.1.39.0/24 | 352 | 10.1.40.0/24 | 2001 | 10.1.32.254 | su-web | su-1x |
| Building 3, student | 3001 | 10.0.2.0/24 | 10.0.2.254 | 303 | 10.1.41.0/24 | 353 | 10.1.42.0/24 | 2001 | 10.1.32.254 | su-web | su-1x |

| dormitory area | | | | | | | | | | | |
|----------------|------|-------------|------------|-----|--------------|-----|--------------|------|-------------|--------|-------|
| Building 4, | | | | | | | | | | | |
| student | 3001 | 10.0.2.0/24 | 10.0.2.254 | 304 | 10.1.43.0/24 | 355 | 10.1.44.0/24 | 2001 | 10.1.32.254 | su-web | su-1x |
| dormitory area | | | | | | | | | | | |
| Building 5, | | | | | | | | | | | |
| student | 3001 | 10.0.2.0/24 | 10.0.2.254 | 305 | 10.1.45.0/24 | 356 | 10.1.46.0/24 | 2001 | 10.1.32.254 | su-web | su-1x |
| dormitory area | | | | | | | | | | | |

Overall VLAN/IP planning

| Area | Service | Common VLAN | Super VLAN | Sub VLAN | IP | Gateway | |
|---------------------|--|-------------|------------|-----------------|---------------|------------------|--|
| Egress | Device interconnection | N/A | | | 10.0.0/24 | 10.0.0.1 | |
| Server area | VM | N/A | | | 172.29.2.0/24 | 172.29.2.253 | |
| Wired NMS | Device NMS | 3000 | | | 10.0.1.0/24 | 10.0.1.254 | |
| Wireless AP | AP management | 3001 | | | 10.0.2.0/24 | 10.0.2.254 | |
| Authentication-free | Door Status Control VLAN | 3010 | | | 10.0.10.0/24 | 10.0.10.254 | |
| area | All-in-one card | 3011 | | | 10.0.11.0 | 10.0.11.254 | |
| | Monitoring | 3012 | | | 10.0.12.0/24 | 10.0.12.254 | |
| Office area | Wired 802.1x authentication and Web authentication Wireless 802.1x authentication | | 2000 | 1–99 100–149 | 10.1.16.0/24 | - 10.1.16.254/20 | |
| | Wireless Web authentication | | | 150–199 | 10.1.19.0/24 | | |
| Dormitory area | Wired 802.1x authentication and Web authentication | | 0004 | 200–299 | 10.1.32.0/24 | - 10.1.32.254/20 | |
| | Wireless 802.1x authentication | | 2001 | 300–349 | 10.1.34.0/24 | | |
| | Wireless Web authentication | | | 350–399 | 10.1.35.0/24 | | |

5.1.5 Configuration Reference Commands on the Core RG-N18000

1. Configuring network communication in the egress area

Configure an uplink port on the RG-N18000, perform layer-3 configuration for the uplink port, configure routes, and check whether the external network communication is normal on the RG-N18000. The configuration commands are omitted.

2. Completing basic settings on the RG-N18000

DSW-18KX LX(config) #auth-mode gateway//Configure the gateway mode and restart the device. DSW-18KX LX(config)#snmp-server host 172.29.2.9 informs version 2c ruijie //Configure SNMP interaction between the RG-N18000 and SAM+. DSW-18KX LX(config) #snmp-server if-index persist//Set the port index to be permanently unique. DSW-18KX LX(config) #service dhcp//Enable the DHCP service on the core device. DSW-18KX LX(config) #ip dhcp snooping//Mandatory. This command is required for IP authorization for 802.1X authentication and MAB authentication. DSW-18KX LX(config) #ip dhcp snooping check-giaddr//Configure a compatible command for DHCP snooping and relay, to prevent DHCP packets from being dropped by the DHCP snooping module on the RG-N18000. DSW-18KX LX(config) #aaa group server radius SAM DSW-18KX LX(config-gs-radius) # server 172.29.2.9 DSW-18KX LX(config) #aaa new-model DSW-18KX LX(config) #aaa accounting update periodic 30 DSW-18KX LX(config) #aaa accounting update DSW-18KX LX(config) #aaa accounting network default start-stop group SAM DSW-18KX LX(config) #aaa authentication login default none DSW-18KX LX(config)#aaa authentication dot1x default group SAM DSW-18KX LX(config) #aaa authentication web-auth default group SAM DSW-18KX LX(config) #aaa authorization ip-auth-mode mixed //Configure IP authorization to the mixed mode. DSW-18KX LX(config)#dot1x accounting default//Enable the 802.1x accounting list. DSW-18KX LX(config)#dot1x authentication default //Enable the 802.1x authentication list DSW-18KX LX(config) #ip radius source-interface GigabitEthernet 1/24 //Configure the source interface for the device to communicate with the RADIUS server. The device address added to SAM+ should be the address of this interface. DSW-18KX LX(config) #ip portal source-interface GigabitEthernet 1/24 //Configure the source interface for the device to communicate with the ePortal server. The device address added to the ePortal server should be the address of this interface. DSW-18KX LX(config) #ip dhcp snooping arp-detect //Enable fast ARP address reclaiming of DHCP snooping. The ARP address reclaiming is performed once per second during ARP aging and can be performed five times at most. DSW-18KX LX(config) #ip dhcp server arp-detect//Enable fast address reclaiming of the DHCP server. If identifying that a user goes offline and does not go online again within a period of time (5 minutes by default), the DHCP server reclaims the IP address assigned to the user. DSW-18KX LX(config) #no aaa log enable DSW-18KX LX(config) #web-auth template eportalv2 DSW-18KX LX(config.tmplt.eportalv2) #ip 172.29.2.8 DSW-18KX LX(config.tmplt.eportalv2)#url http://172.29.2.8/eportal/index.jsp

DSW-18KX LX(config.tmplt.eportalv2)# exit

DSW-18KX LX(config) #web-auth portal key su

DSW-18KX_LX(config)#http redirect direct-site 192.168.9.12 //Configure the address of the RG-SU server as an authentication-free address.

DSW-18KX_LX(config) #web-auth direct-host 10.1.16.200 //Configure the client of a school director as an authentication-free client.

DSW-18KX_LX(config)#dot1x mac-auth-bypass valid-ip-auth //Mandatory. The DHCP module instructs the MAB module to start authentication. Clients must obtain IP addresses before starting MAB authentication.

DSW-18KX_LX(config)#dot1x valid-ip-acct enable //Mandatory. The accounting update packets are used to upload the user IP address to SAM+. If the 802.1x authentication module does not have an IP entry of the user, the user is kicked offline 5 minutes later.

DSW-18KX_LX(config)#direct-vlan 100-149,300-349,3000-3001,3010-3012 //Configure VLANs for wireless 802.1x authentication, monitoring, device management, and wireless AP management as authentication-free VLANs.

DSW-18KX_LX(config)#web-auth portal-check interval 3 timeout 3 retransmit 10 //Configure portal escape.

DSW-18KX LX(config) #web-auth portal-escape nokick

DSW-18KX_LX(config)#radius-server host 172.29.2.9 test username ruijie idle-time 2 key ruijie DSW-18KX_LX(config)#radius-server dead-criteria time 120 tries 12 //Configure an IP address for the RADIUS server and enable the RADIUS escape test function.

DSW-18KX_LX(config)#web-auth radius-escape //Globally enable RADIUS escape in Web authentication mode.

DSW-18KX_LX(config)#address-bind ipv6-mode compatible//Set IPv6 authentication to the compatible mode.

DSW-18KX_LX(config)#station-move permit //Enable migration of 802.1x authenticated clients. DSW-18KX_LX(config)#web-auth station-move auto //Enable migration of Web authenticated clients.

DSW-18KX LX(config) #web-auth station-move info-update

DSW-18KX_LX(config)#no dot1x station-move arp-detect //It is recommended to disable ARP detection after migration of 802.1x authenticated clients, because the ARP detection will cause broadcast packet floods.

DSW-18KX_LX(config) #http redirect port 443 //Because this configuration consumes device resources, it is recommended to discuss with the customer about whether to enable the configuration if a great number of users need authentication.

DSW-18KX_LX(config)#cpu-protect type web-auths bandwidth 2000 //Configure the HTTPS optimization command. HTTPS involves socket encryption and decryption, consuming a great deal of processing resources. 11.0(1)B2T11 and later versions separate HTTPS from HTTP for the use of CPU resources. If HTTPS redirection is enabled, configure CPP rate limiting for HTTPS.

DSW-18KX_LX(config)#offline-detect interval 15 threshold 0 //Set the no-traffic go-offline detection period to 15 minutes.
DSW-18KX_LX(config)#snmp-server host 172.29.2.9 informs version 2c ruijie //Configure SNMP. DSW-18KX_LX(config)#snmp-server host 172.29.2.9 traps su DSW-18KX LX(config)#snmp-server community su rw

3. Configuring VLANs on the RG-N18000

DSW-18KX LX(config) #vlan range 1-399 DSW-18KX LX(config-vlan-range)#exit DSW-18KX LX(config) #vlan 2000 DSW-18KX LX(config-vlan-range)#supervlan//Configure a super VLAN in the office area. DSW-18KX LX(config-vlan-range)#subvlan 1-199 //Associate sub VLANs with the super VLAN. DSW-18KX LX(config-vlan-range)#exit DSW-18KX LX(config) #vlan 2001 DSW-18KX LX(config-vlan-range)#supervlan//Configure a super VLAN in the dormitory area. DSW-18KX LX(config-vlan-range)#subvlan 200-399 //Associate sub VLANs with the super VLAN. DSW-18KX LX(config-vlan-range) #exit DSW-18KX LX(config) #vlan 3000 DSW-18KX LX(config-vlan) # name DeManagement DSW-18KX_LX(config)#vlan 3001 DSW-18KX LX(config-vlan)#name APManagement DSW-18KX LX(config) #vlan 3010 DSW-18KX LX(config-vlan) # name MenJin DSW-18KX LX(config) #vlan 3011 DSW-18KX LX(config-vlan) #name YiKaTong DSW-18KX LX(config) #vlan 3012 DSW-18KX LX(config-vlan) #name JianKong

4. Configuring the IPv4/IPv6 gateway and DHCPv4/DHCPv6

DSW-18KX_LX(config)#ipv6 dhcp pool DHCPv6 //Create a DHCPv6 address pool for the DNS server. DSW-18KX_LX(dhcp-config)# domain-name scu6.edu.cn DSW-18KX_LX(dhcp-config)# dns-server 2001:250:2003::8 DSW-18KX_LX(dhcp-config)# dns-server 2001:250:2003::9 DSW-18KX_LX(config)#ip dhcp pool sushe-pool//Configure a DHCP address pool in the dormitory area. DSW-18KX_LX(dhcp-config)#lease 0 2 0//Mandatory. Set the lease period to 2 hours. DSW-18KX_LX(dhcp-config)#network 10.1.32.0 255.255.240.0 DSW-18KX_LX(dhcp-config)#dns-server 202.115.32.39 202.115.32.36 DSW-18KX_LX(dhcp-config)#default-router 10.1.32.254 DSW-18KX_LX(dhcp-config)#ip dhcp pool bangong-pool//Configure a DHCP address pool in the office area. DSW-18KX_LX(dhcp-config)#lease 0 2 0//Mandatory. Set the lease period to 2 hours. DSW-18KX_LX(dhcp-config)#lease 0 2 0//Mandatory. Set the lease period to 2 hours. DSW-18KX_LX(dhcp-config)#lease 0 2 0//Mandatory. Set the lease period to 2 hours. DSW-18KX_LX(dhcp-config)#lease 0 2 0//Mandatory. Set the lease period to 2 hours. DSW-18KX_LX(dhcp-config)#lease 0 2 0//Mandatory. Set the lease period to 2 hours. DSW-18KX_LX(dhcp-config)#lease 0 2 0//Mandatory. Set the lease period to 2 hours. DSW-18KX_LX(dhcp-config)#lease 0 2 0//Mandatory. Set the lease period to 2 hours. DSW-18KX_LX(dhcp-config)#lease 0 2 0//Mandatory. Set the lease period to 2 hours. DSW-18KX_LX(dhcp-config)#dns-server 10.1.16.0 255.255.240.0 DSW-18KX_LX(dhcp-config)#default-router 10.1.16.254 DSW-18KX LX(config) #ip dhcp pool ap-pool//Configure a DHCP address pool for wireless AP management. DSW-18KX LX(dhcp-config)#option 138 ip 10.10.1.1 DSW-18KX LX(dhcp-config) #network 10.0.2.0 255.255.255.0 DSW-18KX LX(dhcp-config)#default-router 10.0.2.254 DSW-18KX LX(config) #int vlan 2000//Configure the gateway address for the super VLAN in the office area. DSW-18KX LX(config-if-VLAN 2000) #ip address 10.1.16.254/20 DSW-18KX LX(config-if-VLAN 2000) #ipv6 enable DSW-18KX LX(config-if-VLAN 2000)#ipv6 address 2001:250:2003:2000::1/64 DSW-18KX LX(config-if-VLAN 2000) #no ipv6 nd suppress-ra DSW-18KX LX(config-if-VLAN 2000) #ipv6 nd other-config-flag DSW-18KX LX(config-if-VLAN 2000) #ipv6 dhcp server DHCPv6 DSW-18KX LX(config)#int vlan 2001//Configure the gateway address for the super VLAN in the dormitory area. DSW-18KX LX(config-if-VLAN 2001) #ip address 172.16.32.254/20 DSW-18KX LX(config-if-VLAN 2001) #ipv6 enable DSW-18KX LX(config-if-VLAN 2001)#ipv6 address 2001:250:2003:2001::1/64 DSW-18KX LX(config-if-VLAN 2001) #no ipv6 nd suppress-ra DSW-18KX LX(config-if-VLAN 2001) #ipv6 nd other-config-flag DSW-18KX LX(config-if-VLAN 2001) #ipv6 dhcp server DHCPv6 DSW-18KX LX(config)#interface GigabitEthernet 1/1//Configure the port of the core RG-N18000 for connecting to the egress device. DSW-18KX LX(config-if-GigabitEthernet 1/1) # no switchport DSW-18KX LX(config-if-GigabitEthernet 1/1) #ip address 10.0.0.2 255.255.255.0 DSW-18KX LX(config)#int vlan 3000//Configure the gateway address for device management. DSW-18KX LX(config-if-VLAN 3000) #ip address 10.0.1.254/24 DSW-18KX LX(config) #int vlan 3001//Configure the gateway address for the wireless AP device. DSW-18KX LX(config-if-VLAN 3001) #ip address 10.0.2.254/24 DSW-18KX LX(config) #int vlan 3010//Configure the gateway address for door status control. DSW-18KX LX(config-if-VLAN 3010) #ip address 11.0.10.254/24 DSW-18KX LX(config) #int vlan 3011//Configure the gateway address for the all-in-one card service. DSW-18KX LX(config-if-VLAN 3011) #ip address 10.0.11.254/24 DSW-18KX LX(config)#int vlan 3012//Configure the gateway address for the monitoring service. DSW-18KX LX(config-if-VLAN 3012)#ip address 10.0.12.254/24 DSW-18KX LX(config)#address-manage //Enable AM rules to perform refined matching of address segments. DSW-18KX LX(config-address-manage) #match ip 10.1.16.0 255.255.255.0 Gi1/2 vlan 2 DSW-18KX LX(config-address-manage) #match ip 10.1.17.0 255.255.255.0 Gi1/2 vlan 3 DSW-18KX LX(config-address-manage) #match ip 10.1.32.0 255.255.255.0 Gi1/3 vlan 200 DSW-18KX LX(config-address-manage) #match ip 10.1.33.0 255.255.255.0 Gi1/3 vlan 201

DSW-18KX_LX(config-address-manage) #match ip 10.0.2.0 255.255.255.0 vlan 3001 DSW-18KX_LX(config-address-manage) #match ip 10.1.18.0 255.255.255.0 Gi1/4 vlan 100 DSW-18KX_LX(config-address-manage) #match ip 10.1.19.0 255.255.255.0 Gi1/4 vlan 150 DSW-18KX_LX(config-address-manage) #match ip 10.1.34.0 255.255.255.0 Gi1/4 vlan 300 DSW-18KX_LX(config-address-manage) #match ip 10.1.35.0 255.255.255.0 Gi1/4 vlan 350 DSW-18KX_LX(config-address-manage) #match ip loose //It is recommended to configure the loose mode.

... AM rules can be created one by one based on the preceding VLAN/IP planning tables. Note: Once AM rules are enabled, port/VLAN mapping needs to be performed for the network segments to be assigned on the whole network, including the network in the old campus that is not reconstructed (the corresponding port is the port of the RG-N18000 for connecting to the aggregation device of the old campus network; the corresponding VLAN is the VLAN of the SVI on the RG-N18000 for connecting to the aggregation device of the old campus network).

5. Enabling authentication on the port of the RG-N18000

DSW-18KX LX(config) #int GigabitEthernet 1/2//Configure the interface for connecting to the aggregation device in the office area. DSW-18KX LX(config-if-GigabitEthernet 1/2)#switchport mode trunk DSW-18KX LX(config-if-GigabitEthernet 1/2)#dot1x port-control auto //Enable 802.1x authentication control on an interface. DSW-18KX LX(config-if-GigabitEthernet 1/2) #web-auth enable eportalv2//Enable Web authentication on an interface. DSW-18KX LX(config-if-GigabitEthernet 1/2)#dot1x mac-auth-bypass multi-user //Enable multi-user MAB authentication on an interface. DSW-18KX LX(config-if-GigabitEthernet 1/2) #dot1x mac-auth-bypass vlan 1-99 //Enable MAB authentication for VLANs 1-99. DSW-18KX LX(config-if-GigabitEthernet 1/2) #switchport trunk allowed vlan only 1-199,3000-3001,3010-3012 DSW-18KX LX(config-if-GigabitEthernet 1/2) #dot1x critical//Configure RADIUS escape in 802.1x authentication mode on an interface. DSW-18KX LX(config-if-GigabitEthernet 1/2)#dot1x critical recovery action //Enable an escaped user to perform re-authentication after RADIUS escape is reinitialize recovered. DSW-18KX LX(config-if-GigabitEthernet 1/2) #switchport protected //Configure port protection on an interface. DSW-18KX LX(config)#int GigabitEthernet 1/3//Configure the interface for connecting to the aggregation device in the dormitory area. DSW-18KX LX(config-if-GigabitEthernet 1/3)#switchport mode trunk DSW-18KX LX(config-if-GigabitEthernet 1/3)#dot1x port-control auto //Enable 802.1x authentication control on an interface. DSW-18KX LX(config-if-GigabitEthernet 1/3) #web-auth enable eportalv2//Enable Web authentication on an interface.

DSW-18KX LX(config-if-GigabitEthernet 1/3) #switchport trunk allowed vlan only 200-399,3000-3001,3010-3012 DSW-18KX LX(config-if-GigabitEthernet 1/3)#dot1x critical//Configure RADIUS escape in 802.1x authentication mode on an interface. DSW-18KX LX(config-if-GigabitEthernet 1/3)#dot1x critical recovery action reinitialize //Enable an escaped user to perform re-authentication after RADIUS escape is recovered. DSW-18KX LX(config-if-GigabitEthernet 1/3) #switchport protected //Configure port protection on an interface. DSW-18KX LX(config) #int GigabitEthernet 1/4//Configure the interface for connecting to the wireless controller. DSW-18KX LX(config-if-GigabitEthernet 1/4) #switchport mode trunk DSW-18KX LX(config-if-GigabitEthernet 1/4)#dot1x port-control auto //Enable 802.1x authentication control on an interface. DSW-18KX LX(config-if-GigabitEthernet 1/4)#dot1x mac-auth-bypass multi-user //Enable multi-user MAB authentication on an interface. DSW-18KX LX(config-if-GigabitEthernet 1/4) #dot1x mac-auth-bypass vlan 150-199//Enable MAB authentication for VLANs 150-199 (wireless Web authentication in the office area). DSW-18KX LX(config-if-GigabitEthernet 1/4) #web-auth enable eportalv2//Enable Web authentication on an interface. DSW-18KX LX(config-if-GigabitEthernet 1/4) #switchport trunk allowed vlan only 100-199,300-399,3000 DSW-18KX LX(config) #int GigabitEthernet 1/44//Configure the port for connecting to the server area. DSW-18KX LX(config-if-GigabitEthernet 1/44) #no switchport DSW-18KX LX(config-if-GigabitEthernet 1/44)#description linkto-SAM&eportalSERVER DSW-18KX LX(config-if-GigabitEthernet 1/44) #ip address 172.29.2.253 255.255.25.0

6. Optimizing VLAN pruning on the downlink port of the RG-N18000

7. Performing routing related configurations

| DSW-18KX_LX(config)#router ospf 1 | | |
|---|-----------|--|
| DSW-18KX_LX(config-router) #redistribute conn | ected | |
| DSW-18KX_LX(config-router) #passive-interfac | vlan 2000 | //Mandatory. Configure a passive port |
| to to reduce CPU overheads. | | |
| DSW-18KX_LX(config-router) #passive-interfac | vlan 2001 | //Mandatory. Configure a passive port |
| to to reduce CPU overheads. | | |
| DSW-18KX_LX(config-router) #passive-interfac | vlan 3000 | <pre>//Mandatory. Configure a passive port</pre> |
| to to reduce CPU overheads. | | |
| DSW-18KX_LX(config-router) #passive-interfac | vlan 3001 | //Mandatory. Configure a passive port |
| to to reduce CPU overheads. | | |

```
DSW-18KX_LX(config-router) #passive-interfac vlan 3010 //Mandatory. Configure a passive port
to to reduce CPU overheads.
DSW-18KX_LX(config-router) #passive-interfac vlan 3011 //Mandatory. Configure a passive port
to to reduce CPU overheads.
DSW-18KX_LX(config-router) #passive-interfac vlan 3012 //Mandatory. Configure a passive port
to to reduce CPU overheads.
```

5.1.6 Aggregation Configuration Reference Commands for the Dormitory Area

```
S5750-student(config)#vlan range 200-399,3000-3001,3010-3012 //Configure the VLAN range
for the access device in the student dormitory area, as well as the monitoring and management
VLANs.
S5750-student(config)#int GigabitEthernet 0/24 //Configure the uplink port of the aggregation
device as a trunk port for transparent transmission.
S5750-student(config-if-GigabitEthernet 0/24)#switchport mode trunk
S5750-student(config-if-GigabitEthernet 0/24)#switchport trunk allowed vlan remove
1-199,400-2999,3002-3009,3013-4094
S5750-student(config)#int GigabitEthernet 0/23//Configure the downlink port of the aggregation
device as a trunk port for transparent transmission.
S5750-student(config-if-GigabitEthernet 0/23)#switchport mode trunk
S5750-student(config-if-GigabitEthernet 0/23)#switchport mode trunk
S5750-student(config-if-GigabitEthernet 0/23)#switchport trunk allowed vlan remove
1-199,400-2999,3002-3009,3013-4094
```

5.1.7 Access Configuration Reference Commands for the Dormitory Area

```
S2928G-student1-1(config)#vlan range 200-399,3000-3001,3010-3012
                                                                     //Configure the VLAN
range for the access device in the student dormitory area, as well as the monitoring and management
VLANS.
S2928G-student1-1(config)#spanning-tree//Enable STP.
S2928G-student1-1(config)#spanning-tree mode rstp //Enable RSTP to avoid overlow port
convergence speed.
S2928G-student1-1 (config) #spanning-tree portfast bpduguard default //Enable BPDU guard for
all PortFast ports by default.
S2928G-student1-1(config)#errdisable recovery interval 300//Configure the recovery interval
after a port is disabled by RLDP.
S2928G-student1-1(config)#int range gi0/1-22
S2928G-student1-1(config-if-range)#switchport access vlan 200 //Create an access port and
assign it to the corresponding VLAN.
S2928G-student1-1(config-if-range)#switchport protected//Mandatory. Configure port
protection.
```

S2928G-student1-1(config-if-range)#spanning-tree portfast //Enable PortFast on all downlink interfaces, which validates BPDU guard at the same time. Once a BPDU packet is received, the access switch regards that a loop occurs and shuts down the interfaces. S2928G-student1-1(config-if-range)#rldp port loop-detect shutdown-port //Mandatory. Configure RLDP to prevent loops. S2928G-student1-1(config) #int gi0/23//Configure the port for connecting to the AP. S2928G-student1-1(config-if-GigabitEthernet 0/23)# switchport access vlan 3001 S2928G-student1-1(config-if-GigabitEthernet 0/23) #rldp port loop-detect shutdown-port S2928G-student1-1 (config) #int gi0/24//Configure the uplink port of the access device as a trunk port for transparent transmission. S2928G-student1-1 (config-if-GigabitEthernet 0/24) #switchport mode trunk S2928G-student1-1(config-if-GigabitEthernet 0/24)#spanning-tree bpdufilter enable//Enable a BPDU filter for the uplink port, so that loop protection is provided only on single devices, and BDPU packets are not transmitted externally, no topology is created, and no root bridge is elected.

S2928G-student1-1(config-if-GigabitEthernet 0/24)# switchport trunk allowed vlan only 200-399,3000-3001,3010-3012

5.1.8 SAM + and ePortal Related Configurations

1. Adding an RG-N18000 on SAM+

| s | hortcut Channel 🛛 🗇 | Homepage | System Security | User / | Access Control | Billing | Account | Operation | | | | |
|---|-----------------------------------|-------------------|----------------------|------------------|-------------------|---------|-----------------|---------------------|---------------|-------------------------------|--------------------------|---------|
| 1 | Location: System > Device Manager | ment > Add | | | | | | | | | | |
| | | | | | | | | | | | | |
| | Device | | | | | | | | | | | |
| | Device IP Address* | 172.29.2.253 | | | | | IP Type* | | IPv4 | • | | |
| | Device Type* | Ruijie Switch | • | | | | Model* | | N18K | • | | |
| | PPPoE Authentication Domain | | Please use comma or | space to separa | ate multiple doma | ins | IPOE+Web Au | thentication Domain | | Please us | e comma or space to | separat |
| | Device Key* | su | | | | | Community* | Γ | su | | | |
| | | | For trusted ARP bind | ing application, | MAC address mus | st be | | | | _ | | |
| | MAC Address* | filled | | | | | SNMP Proxy P | ort | | If you do | not fill in, the default | port 16 |
| | DHCP Login Username | | | | | | DHCP Login Pa | assword | | | | |
| | Telnet Login Username | | | | | | Telnet Login P | assword | | | | |
| | Telnet Privileged Password | | | | | | Device Group* | | default | • | | |
| | Device Name | | | | | | Device Locatio | n | | | | |
| | Device Timeout (secs)* | 3 | | | | | Device Idle Tin | ne (secs) | | | | |
| | Device Feature | Re-authentication | Account Update | Client Detectio | n | | Area | | Please Select | (Device I | P(v4)) | |

2. Adding an AC on SAM+

| SAM ⁺ security accounting | MANAGEMENT SYSTEM | | 홉 admin 😰 Al |
|--------------------------------------|---|--------------------------------|--|
| Shortcut Channel 🔅 | Homepage System Security User Access Control Bi | ling Account Operation | |
| Location: System > Device Managem | nent > Add | | |
| Device | | | |
| Device IP Address* | 10.10.1.1 | IP Туре* | IPv4 • |
| Device Type* | Wireless Switch | Model* | Other Model |
| PPPoE Authentication Domain | Please use comma or space to separate multiple domains | IPOE+Web Authentication Domain | Please use comma or space to separate multipl |
| Device Key* | su | Community* | su |
| MAC Address | For trusted ARP binding application, MAC address must be | SNIMD Brown Bort | If you do not fill in the default port 161 will be |
| MAC Address | filled | Shame Floxy Fort | il you do not ill in, the default port for will be |
| 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 | |

3. Adding ePortal on SAM+

| sł | hortcut Channel 🔅 | Homepage | System Security | User | Access Control | Billing | Account Operation | | | | | | | | |
|----|--|------------|----------------------|--------------|---------------------|---------|-----------------------------|------|-----------------|--|--|--|--|--|--|
| L | Location: System > Device Management > Add | | | | | | | | | | | | | | |
| | Device | | | | | | | | | | | | | | |
| | Device IP Address* | 172.29.2.8 | | | | | IP Type* | | IPv4 | | | | | | |
| | Device Type* | RG-ePortal | • | | | | Model* | | Please Select • | | | | | | |
| | PPPoE Authentication Domain | | Please use comma or | space to se | parate multiple dom | nains | IPOE+Web Authentication Dor | main | | Please use comma or space to separate multiple domains | | | | | |
| | Device Key* | su | | | | | Community* | | su | | | | | | |
| | MAC Address | | For trusted ARP bind | ng applicati | ion, MAC address mu | ust be | SNIMD Droves Doct | | | If you do not fill in the default part 161 will be adopted | | | | | |
| | MAC Address | filled | | | | | SNMF Floxy Fort | | | If you do not fin in, the default port for will be 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) | | | | | | | | |

4. Adding SAM+ on ePortal

| Location: Network Access Porta | l System > System Se | ttings | | | | | | | |
|--------------------------------|------------------------|--------------------------------|-------------------------------------|--------------------------|--------------------------------------|--|--|--|--|
| r | | | RADIUS Server | | _ | | | | |
| Radius Server Address | 172.29.2.9 | Restart Effective | Authentication Port | 1812 | (Delault 1812)Restart Effective | | | | |
| Authentication Retry Interval | 0 | secs (Default 0 sec) | RADIUS Key | key | | | | | |
| Authentication Overtime | 3 | secs (Default 3 secs) | Authentication Retry Count | 1 | times (Default 1 time) | | | | |
| Accounting | Activated | | Accounting Port | 1813 | (Default 1813)Restart Effective | | | | |
| Accounting Packet Overtime | 3 | secs (Default 3 secs) | Accounting Packet Retry Count | 1 | times (Default 1 time) | | | | |
| Accounting Thread Count | 5 | units (Default 5 units) | Accounting Buffer Zone Settings | 1000 | (Lefault 1000) | | | | |
| | | 1 | DeviceCommunication Settings | | | | | | |
| ePortal Listening Informs Port | 162 | (Default 162)Restart Effective | Informs Community | su | (Default public) | | | | |
| Communication Overtime | 3 | secs (Default 3 secs) | Communication Retransmission | 3 | times (Default 3 times) | | | | |
| Online Scanning Cycle | 30 | nins (Default 30 mins) | | | | | | | |
| | | | SIMP Settings | | | | | | |
| SNMP Port | 161 | (Default 161)Restart Effective | SNMP Community | au | (Default public) | | | | |
| | Browsor Client Related | | | | | | | | |
| Keep Alive Cycle | 15 | nins (Default 15 mins) | Keep Alive Overtime Count | 5 | times (Default 5 times) | | | | |
| | | | System Settings | | | | | | |
| Record Entry on Each Page | 20 | (Default 20) | | | | | | | |
| Authentication Server Address | 172.29.2.3 | | | | | | | | |
| Wanagement Port Access Address | 172 29 2 3 | ▼ Use http:/ | /172.29.2.3:80/enortal/ to visit th | e management system so : | as to separate from redirected IPv4. | | | | |

5. Adding an RG-N18000 on ePortal

RG-ePortal Portal Components Network Access Portal System



6. Configuring access control

(1) It is not necessary to enable MAB authentication for access control in the dormitory area.

| SAM ⁺ security accounting | MANAGEMENT SYSTE | м | | | | | | |
|--|-------------------------|----------------|--------------|--------------|---------------------|------------|------------------|----------------|
| nortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation |
| ocation: Access Control > Access Co | ontrol > Modify | | | | | | | |
| Access Control Information Use | r Information Check | Network Us | age Control | Public Se | ervice User Behav | or Control | VPN Control | Client Ver |
| Access Control Name * | wired_web | | | | | | | |
| Concurrent Logins Limit(0 to 99) 0 means no limit * | 10 | | | | | | Synchroniza | tion Account |
| According to the Terminal Type | Concurrent Logins (1 t | o 99 times) | | | | | | |
| | 🗷 Display accountir | ig policy info | rmation when | n user onlin | e | | Automatic B | inding MAC a |
| | Show users on-lir | ne access con | trol time | | | | Account info | ormation is di |
| Gateway Access Restriction | It does not allow | traffic throug | h the gatewa | y server (g | ateway device needs | to be depl | oyed linkage in | penetration r |
| Export linkage strategy | | * non | NPE / EG ga | teway billin | g model deploymen | t, no need | to configure the | export colla |
| Firewall Policy | | * not | deploy firew | alls linkage | the need to configu | re | | |
| Description | | | | | | | | |
| + Diana anti-ata ana ati in labal ana | | | | | | | | |
| - Please reler to respective laber con | tent for access details | | | | | Save | Back | |
| | | | | | | | | |

(2) It is necessary to enable MAB authentication for access control in the office area.

| hortcut Channel 🔅 | Homepage | System Security | User | Access Control | Billing | Account | Operation |
|--|----------------------------|------------------------|---------------|---------------------|------------|-------------------|--|
| Location: Access Control > Access Con | ntrol > Modify | | | | | | |
| Access Control Information User | Information Check N | letwork Usage Control | Public Se | ervice User Behavi | or Control | VPN Control | Client Version Management Wireless Access Properties |
| Access Control Name * | wired_web | | | | | | |
| Concurrent Logins Limit(0 to 99) 0 means no limit * | 10 | | | | | Synchronizat | tion Accounting Update Interval |
| According to the Terminal Type C | oncurrent Logins (1 to 9 | 9 times) | | | _ | | |
| | Display accounting p | policy information whe | n user onlin | e | | Automatic B | inding MAC authentication information quickly |
| | Show users on-line a | access control time | | | | Account info | rmation is displayed on a subscriber line |
| Gateway Access Restriction | It does not allow training | ffic through the gatew | ay server (ga | ateway device needs | to be depl | oyed linkage in p | penetration mode) |
| Export linkage strategy | | * non NPE / EG g | ateway billin | g model deploymen | t, no need | o configure the | export collaboration policy |
| Firewall Policy | | * not deploy fire | alls linkage, | the need to configu | re | | |
| Description | | | | | | | |
| * Diesse refer to respective label cont | ant for access details | | | | | | |
| riease relet to respective laber contr | ent for access details | | | | | | |
| | | | | | Save | Back | |
| | | | | | | | |
| | | | | | | | |
| | | | | | | | |

(3) The office area allows MAC fast access. To allow login using the native 802.1x authenticated client, select Smart Device

1X Access.

| hortcut Channel 🛛 🌼 | Homepage Syste | em Security Us | er Access Control | Billing Account | nt Operation |
|---|----------------------|----------------------|------------------------|----------------------|--|
| ocation: Access Control > Access Contro | ol > Modify | | | | |
| Access Control Information User Info | ormation Check Netwo | rk Usage Control Pub | lic Service User Behav | vior Control VPN Cor | ntrol Client Version Management Wireless Access Properties |
| Allowed Access | Access Mode Verific | ation Information | | | |
| Wired 1X Access | User IP(v4) | User IP(v6) | User MAC | NAS IP(v4) | NAS IP(v6) NAS Port |
| Wiled TX Access | VLAN | Internal VLAN | External VLAN | Access IP Type St | tatic 🔻 |
| Wired Web Portal Access | User IP(v4) | User MAC | Web Authenticatio | n Device IP(v4) | Web Authentication Device Port |
| @Window 1V Assess | User IP(v4) | User MAC | NAS IP(v4) | AP MAC | SSID |
| Willeless TA Access | Access IP Type St | tatic 🔻 | | | |
| ✓ Wireless Web Portal Access | User MAC | NAS IP(v4) | AP MAC | SSID | |
| Smart Device 1X Access | User MAC | NAS IP(v4) | AP MAC | SSID | |
| This fact the | User MAC | NAS IP(v4) | AP MAC | SSID | NAS Port |
| MAC Fast Access | VLAN | Internal VLAN | External VLAN | | |
| Wind Chandrad Dartal Assess | User IP(v4) | User MAC | NAS IP(v4) | NAS Port | VLAN |
| Willed Standard Portal Access | Internal VLAN | External VLAN | | | |
| Wireloss Standard Portal Assess | User IP(v4) | User MAC | NAS IP(v4) | AP MAC | SSID |
| writeless standard Portal Access | NAS Port | VLAN | Internal VLAN | External VLAN | |
| ✓ VPN Dial-up access | User IP(v4) | NAS IP(v4) | | | |
| CONCLUSION AND AND AND AND AND AND AND AND AND AN | | | | | |

7. Configuring accounting policies

(1) Monthly accounting policy in the dormitory area

| | G MANAGEMENT SYSTEM | | | | | | | | | |
|--|---|---|--------------------------------|--------------------------|--|-------------------------------------|---|--|--|--|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | | |
| Location: Billing > Billing Policy > I | Modify > Modify Month | nly | | | | | | | | |
| Monthly Billing Policy | | | | | | | | | | |
| Billing Policy Name* | wired_month | | | | | | Description | | | |
| Period Type* | 🔍 30 Days 🖲 Month | | | | | | Ending Date | | Enable | (1-31) |
| Compensation | 🔲 The remaining day | s during acc | ount suspens | sion can be | e used after recovery | | Rate (MYR)* | | 30.00 | |
| Authentication Related Ontions | Allow login when t | here is no re | emaining inte | rnet traffic | or the account has u | inpaid charg | es. (Must use | the NTD penetrati | ion mode with access cor | ntrol or ACE device. M |
| Automation related options | internet traffic billing | plan.) | | | | | | | | |
| Advances Options | Monthly Payment | for Limited E | Ouration/ Mo | nthly Payr | nent for Limited Inter | net Traffic/ I | Monthly Paym | ent for Limited Au | thentication Device Traff | ic Configuration |
| Not rec Month Month | ommended to change bi / billing policy. If the mor / charge: charges extend | lling policy. nthly billing to the next | rate or cycle month. For e: | type has b xample, if | een revised, the mon the user creates the a | thly charges account and Save | based no the paid for the se Return | new billing rate w rrvices on the 6th t | vill effective in the next p this month, the fee will b | ayment month. e charged again on th |

(2) Monthly accounting policy in the office area

| SAM ⁺ security accountin | IG MANAGEMENT SYSTEM | | 名 admin ㅣ @ |
|--------------------------------------|--|---|---|
| Shortcut Channel | Homepage System Security User Access Control B | illing Account Operation | |
| Location: Billing > Billing Policy > | Modify > Modify Monthly | | |
| Monthly Billing Policy | | | |
| Billing Policy Name* | wired_month | Description | |
| Period Type* | 30 Days Month | Ending Date | Enable (1-31) |
| Compensation | The remaining days during account suspension can be used after recovery | Rate (MYR)* | 0 |
| Authoritization Related Options | Allow login when there is no remaining internet traffic or the account has unpa | id charges. (Must use the NTD penetratio | n mode with access control or ACE device. Must use the monthly interne |
| Authentication Related Options | internet traffic billing plan.) | | |
| Advances Options | Monthly Payment for Limited Duration/ Monthly Payment for Limited Internet | Traffic/ Monthly Payment for Limited Aut | hentication Device Traffic Configuration |
| Not rec Monthl Monthl | ommended to change billing policy. y billing policy. If the monthly billing rate or cycle type has been revised, the monthly y charge: charges extend to the next month. For example, if the user creates the accor Sat | charges based no the new billing rate wi nnt and paid for the services on the 6th t re Return | ll effective in the next payment month. his month, the fee will be charged again on the 6th of next month. |

8. Configuring user templates

(1) User template in the dormitory area

| rtcut (| Channel 🕸 Homepa | ige System Security | User Acc | ess Control Billing | Account Operation | | |
|---------------------------|---|---------------------|--------------|---------------------|-------------------|----------------|----------------|
| ation | User > User Template > User Templates | | | | | | |
| empla elf-M Descrip | te Name: student odification Option : Not allowed to change otion: | the plan | | User Template | s: student 🔀 | | |
| - 1 | Plan | | | | Rule | | |
| - | | Access Area | Default Rule | Service | Allow Access Time | Access Control | Billing Policy |
| | Name:student Concurrent Logins Limit : 1 Billing Policy:Not Charging Cycle Expired to Suspend User.:Not Enabled Suspension End Time: MAC Binding Expiry:0Day | Unlimited | ٠ | default | Unlimited | default | Not Charging |

(2) User template in the office area

| SAI | M^+ security accounting management sys | ТЕМ | | | | | | | | |
|----------------------------------|--|-----------|-------------|------|--------|------------|---------------|---------------------------|-----------|-------------|
| Shortcu | t Channel 🔅 Homepage | System | Security | User | Acce | ss Control | Billing | Account | Operation | |
| Locatio Temp Self- Desc | n: User > User Template > User Templates plate Name: teacher Modification Option : Not allowed to change th ription: | e plan | | | | Use | er Templates: | teacher 📝 | | |
| | Plan | Acces | Access Area | | t Rule | S | ervice | Rule Allow Access Time | | Access Cont |
| | Name:teacher Concurrent Logins Limit :1 Billing Policy:Not Charging Cycle Expired to Suspend User.:Not Enabled Suspension End Time: MAC Binding Expiry:0Day Description: | Unlimited | | | | default | | Unlimited | 1 | default |
| | • | | | | | | | | | |

- 9. Configuring user plans
- (1) User plan in the dormitory area

| Locatio | on: User > User Template > User Templates | | | | | | | |
|----------------------|---|---|---------------------------|--------------------------------|---------------------------------|-------------------------------|----------------|--|
| Tem Self- Desc | plate Name: dormitory Modification Option : Not allowed to change the ription: | e plan | | User Templates: do | ormitory 🔯 | | | |
| | Plan | | | | Rule | | | |
| | Fiait | Access Area | Default Rule | Service | Allow Access Time | Access Control | Billing Policy | |
| | Namedormitory Concurrent Logins Limit : 1 Billing PolicyNot Charging Cycle Expired to Suspend User::Not Enabled Suspension End Time: MAC Binding Expiry:0Day Description: | Unlimited | • | default | Unlimited | default | Not Charging | |
| | The number of repeated logins of the plan is user' : Users can use different services for Internet access a | s maximum number of online nd the number of online user: | STAs. s of the same se | rvice is restricted by the num | ber of repeated logins of the o | corresponding access control. | | |

(2) User plan in the office area

| Shortcu | it Channel | \$ | Homepage | System | Security | User | Access Control | Billing | Account | Operation | | | | |
|----------------------|--|---|--|--|----------------------------------|-----------------------|---|---------------------------------|--|---|--------------------------|------------|----------------|--|
| Tem Self- Desc | plate Nam Modificati | User Template > User Ten e: teacher ion Option : Not allow | nplates red to change the | plan | | | Use | r Templates | : teacher ӣ | | | | | |
| | | | | Acce | ss Area | Defai | | _ | _ | Rule | | rol | Billing Policy | |
| | Name:te Concurr Billing P Cycle Ex Suspens MAC Bir Descript The numb Users can | acher ent Logins Limit : 1 olicyhot Charojng pired to Suspend User.it ion End Time: wing Expiryr0Day ion: er of repeated logins of t use different services for | Not Enabled I he plan is user's Internet access an | Unlimited maximum nu d the numbe | mber of onlin r of online use | e STAs. ers of the | Plan * Plan * Concurrent Login Billing Policy Cycle expired an Mac Binding Vali Description | s Limit d suspend us dity | teacher Enabl Not Cha er. Activ 0 (0-1 | e 1 (1 ~ 99 t arging ate 305 days, 0 for r | ines) 7 wt linited | s control. | Not Charging | |
| | | | | | | | | s | ave | Cancel | | | | |

10. Configuring user groups

| Shortcut Channel | Homepage | System | Security | User | Access Control | Billing | Account | Operation | | | | |
|-----------------------------|----------|-----------------|---------------|--------|--------------------|----------------|----------------|-----------------|---------------------------------|-------------------|------------------|------------------------------|
| Location: User > User Group | | | | | | | | | | | | |
| Expand All Collapse All | | Change User | Group | | | | | | | | | |
| M User Group | | User Group * | | stude | nt | | | | Parent Group Name * | root | | |
| -0 dot1x | | Default User 1 | Template* | studer | nt 🔻 | | | | Default Plan* | student | • | |
| o wireless_month | | Uplink Speed | 1 | | | | | | Downlink Speed | | | |
| | | (8~261120KB | lps) | 0 | | | | | (8~261120KBps) | 0 | | |
| | | User group as | uthentication | | | | | | Downlink Speed | | | |
| | | is successful h | hoplinks. | | | | | | (8~261120KBps) | | | |
| | | Description | | | | | | | Creator | admin | | |
| | | | | Sync | hronize the update | e default user | template or pl | an user used in | this user group (If there are a | large number of u | sers in the user | group, the system will be ve |
| | | | | Please | perform system op | eration when | idle.) | | | | | |
| | l | | | | | | | | | | | |
| | | | | | | | Sa | ve Ad | d Delete | | | |

| Shortcut Channel 🔅 | Homepage System Security | User Access Control Billing | Account Operation | | |
|---------------------------------|--------------------------------|-------------------------------------|---------------------------------|-----------------------------------|--------------------------------|
| Location: User > User Group | | | | | |
| Expand All Collapse All | Change User Group | | | | |
| | User Group * | teacher | | Parent Group Name * | root |
| o dot1x o student | Default User Template* | teacher 🔻 | | Default Plan* | teacher 🔻 |
| -0 teacher -0 wireless_month | Uplink Speed (8~261120KBps) | 0 | | Downlink Speed (8~261120KBps) | 0 |
| | User group authentication | | | Downlink Speed | |
| | is successful hoplinks. | | | (8~261120KBps) | |
| | Description | | | Creator | admin |
| | | Synchronize the update default use | er template or plan user used i | n this user group (If there are a | large number of users in the u |
| | | Please perform system operation whe | en idle.) | | |
| | | | | | |
| | | | Save A | dd Delete | |

11. Registering users

| Shortcut Channel 🔅 | Homepage System Security | User Access Control Billing Account O | Operation |
|---|----------------------------------|--|--|
| Location: User > User Management | | | |
| User Search | Basic Information | | |
| Import Search | Username* | test1 | Full Name |
| | Password* | ***** | Confirm Password* ****** |
| Create Account | User Group* | student | Account test1 🔍 |
| Batch Account Activation | User Templates | Use Default Template of User Group Plan: Default Bil | ling Policy: Not Charging |
| Import Accounts | Self-service Permission | All Self-service Privileges | Authentication-free Verification is required |
| Import recourts | Auto Pre-Cancellation | | BACL |
| Import Changes | User Status | Normal | Pause Duration |
| Import Payments | Last Self-service Pause Duration | | Next Available Self-service Pause Duration Unlimited |
| | Guarantor Ranking | | |
| Import Change User Templates and Plans | Advanced Options | Show Advanced User Settings options | |
| Import Change User Group | Sex | | Email Address |
| | ID Type | | ID No. |
| | Education Level | | Online Information |
| | Telephone No. | | Mobile Phone |
| | Address | | Postal Code |
| | Create Time | 2018-05-09 14:14:42 | Last Update 2018-05-09 14:14:42 |
| | Creator | admin | |

Copy Account Payment Print

| ortcut Channel 🔅 | Homepage System S | Security User Access Control | Billing Account Ope | eration | |
|---|-------------------------|------------------------------------|---------------------|---------------------|--------------------------|
| ocation: User > User Management | | | | | |
| User Search | Basic Information | | | | |
| Import Search | Username* | test2 | | Full Name | |
| | Password* | ••• | | Confirm Password* | ••• |
| Create Account | User Group* | teacher | | Account | Same As username |
| Batch Account Activation | User Templates | Use Default Template of User Group | p 🔍 Customize | | |
| mont Accounts | Self-service Permission | All Self-service Privileges | • | Authentication-free | Verification is required |
| inport Accounts | Auto Pre-Cancellation | | | BACL | Please Select |
| mport Changes | Guarantor Ranking | Please Select | • | | |
| moort Payments | Advanced Options | Show Advanced User Settings optic | ons | | |
| nport Payments | Sex | Please Select | * | Email Address | |
| nport Change User Templates and lans | ID Type | Please Select | ۲ | ID No. | |
| and Channel Have Course | Education Level | Please Select | • | Online Information | |
| nport change üser Group | Telephone No. | | | Mobile Phone | |
| | Address | | | Postal Code | |

12. Payment

| SAM ⁺ security accounting | MANAGEMENT SYSTE | м | | | | | | | |
|--------------------------------------|------------------|--------------|----------|--------|---------------------|---------|---------------|-----------------|---------------------------|
| Shortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | |
| Location: Billing > Fees Management | t > Payment | | | | | | | | |
| Account | | | | | | | | | |
| Account ID | test1 | | | | | | Email | | |
| Overdraft Options | The account can | be overdrawn | | | | | | | |
| Balance (MYR) | 0.00 | | | | | | | | |
| Status | Normal | | | | | | Description | | |
| Account Associated With The User | Q | | | | | | Account Ac | tivation Fee | Unpaid |
| | | | | | | | | | |
| | | | | | | | | | |
| Balance to be Paid (MYR) | 100 | | | | | | Receivables | (MYR) | 100 |
| Account Activation Fee (MYR) | | | | | | | Receivables | (MYR) | |
| | | | | | | | | | |
| | | Payment | Reset | Return | n to Expense Manage | ment | Return to Aco | ount Management | Return to User Management |
| | | | | | | | | | |

13. Controlling the access period

| AIVI SECURITY ACCOL | | | | | | | 🛆 admin 😰 A | |
|---|---|---|--|---|--|---|--|------------------------|
| rtcut Channel 🔅 | Homepage | System Security | User Acces | s Control Billing | Account Opera | ion | | |
| ation: Access Control > Ac | cess Time 🗲 Add | | Acces | Control | | | | |
| | | | Acces | s Time | | | | |
| ccess time | | | Simpli | fied Network RPID | | | | |
| Access Time Name* | 10.30-10.32 | | Acces | s Location | | | | |
| Secolation | daily | | | | | | | |
| escription | | | | | | | | |
| | Access time slot re | fers to the dial-up period | d available for users. | In other words, it is the p | period of time open fo | network access. | | |
| | | | | | | | | |
| | If there is a defined | d access time slot in a cer | tain day, the rest of | the day will not allow ne | twork access except th | e defined time slot. | | |
| Help | If there is a defined Three access times | d access time slot in a cer slot tuper public bolidau | tain day, the rest of | the day will not allow ne | twork access except th | e defined time slot. | | |
| Help | If there is a defined Three access time | d access time slot in a ce slot types: public holiday | rtain day, the rest of , weekend and week | the day will not allow ne day (in decreasing priori | twork access except th ty). | e defined time slot. | | |
| Help | If there is a define. Three access time An access time slot | d access time slot in a ce slot types: public holiday t record includes one or | rtain day, the rest of , weekend and week more of these three | the day will not allow ne day (in decreasing priori entries. Repeated access | twork access except th ty). time slots are not allo | e defined time slot. ved. | | |
| Help .ccess Time Entry | If there is a define Three access time An access time slot | d access time slot in a cer slot types: public holiday t record includes one or i | rtain day, the rest of , weekend and week more of these three | the day will not allow ne day (in decreasing priori entries. Repeated access | twork access except th ty). time slots are not allo | e defined time slot. ved. | | |
| ccess Time Entry Access Time Entry Name | If there is a define: Three access time An access time slov Access Time Type | d access time slot in a cer slot types: public holiday t record includes one or i | rtain day, the rest of , weekend and week more of these three | the day will not allow ne day (in decreasing priorit entries. Repeated access Time Config | twork access except tl ty), time slots are not allo guration | e defined time slot. ved. | Terminal Type Configuration | Apply |
| Help ccess Time Entry Access Time Entry Name | If there is a define. Three access time An access time slo Access Time Type | d access time slot in a cer slot types: public holiday t record includes one or | rtain day, the rest of , weekend and week more of these three | the day will not allow ne day (in decreasing priori entries. Repeated access Time Config | twork access except th ty). time slots are not allo guration | e defined time slot. ved. | Terminal Type Configuration | Apply |
| Help ccess Time Entry Access Time Entry Name | If there is a define Three access time An access time slo Access Time Type Daily | d access time slot in a cer slot types: public holiday t record includes one or r Every Day 10 | tain day, the rest of , weekend and week more of these three • Hrs 30 | the day will not allow ne day (in decreasing priori entries. Repeated access Time Config • minutes 00 second | twork access except th ty). time slots are not allo guration ds to 10 •)He | e defined time slot. ved. 32 • minutes 59 seconds | Terminal Type Configuration Wireles Mobile Device % PC | Apply |
| telp ccess Time Entry Access Time Entry Name | If there is a define Three access time An access time sto Access Time Type Daily | d access time slot in a cer slot types: public holiday t record includes one or r Every Day 10 | rtain day, the rest of , weekend and week more of these three more of these three + Hrs 30 | the day will not allow ne day (in decreasing priori entries. Repeated access Time Config • minutes 00 second | twork access except th ty). time slots are not allo guration ds to 10 • Hn | e defined time slot. wed. 32 • minutes 59 seconds | Terminal Type Configuration # Wireless Mobile Device # PC # Others | Apply Add |
| Help access Time Entry Access Time Entry Name | If there is a define Three access time An access time slo Access Time Type Daily | d access time slot in a cei slot types: public holiday t record includes one or r Every Day 10 | tain day, the rest of , weekend and week more of these three more of these three | the day will not allow ne day (in decreasing priori entries. Repeated access Time Config • minutes 00 second | twork access except th ty), time slots are not allo guration ds to 10 • Hr | e defined time slot. ved. 32 •)minutes 59 seconds | Terminal Type Configuration & Wireless Mobile Device & PC & Others | Apply Add |
| Help Access Time Entry Access Time Entry Name | If there is a define Three access time An access time slo Access Time Type Daily | d access time slot in a ces slot types: public holiday t record includes one or r Every Day 10 | tain day, the rest of , weekend and week more of these three • Hrs 30 | the day will not allow ne day (in decreasing priori) entries. Repeated access Time Config • minutes 00 second | twork access except th ty). time slots are not allo guration ds to 10 • Hn | e defined time slot. ved. 32 • minutes 59 seconds | Terminal Type Configuration #Wireless Mobile Device #DC #Others Wireless Mobile Device | Apply Add |
| ccess Time Entry Access Time Entry Name 10.30-10.32 | If there is a define Three access time An access time slo Access Time Type Daily Weekday | d access time slot in a cee slot types: public holiday trecord includes one or Every Day 10 | tain day, the rest of , weekend and week more of these three •)+trs 30 Eve | the day will not allow ne day (in decreasing priori) entries. Repeated access Time Config • minutes 00 second ry Day10Hrs30:00 To10H | twork access except th typ). time slots are not allo guration ds to 10 • Hn Irs32minutes 59 secon | e defined time slot. ved. 32 • minutes 59 seconds 55 | Terminal Type Configuration ⊮Wireless Mobile Device ⊮PC ⊮Others Wireless Mobile Device Computer | Apply Add Delete |

14. Associating the access period with the user template

| ocatio | SECURITY ACCOUNTING MAI | NAGEMENT SYSTEI Homepage plates | M System | Security | User A | ccess Control | Billing | Account | Operation | | | 各 admin | About |
|-------------------------|--|--|-----------------------------|---------------------------------|----------------------------|-------------------|---------------|---------------|--------------------|-----------------------------|----------------|-----------|-----------------|
| Temp Self-I Desci | blate Name: student Modification Option : Not allow ription: | d to change the p | olan | | | Us | er Templates | : student 🐼 | | | | Return to | the User Templa |
| | Plan | | Access | Area | Dofault Rul | | onico | Allow | Rule | Access Control | Rilling Doligy | Rulo | |
| Ħ | Name:student Concurrent Logins Limit :1 Billing Policy:Not Charging Cycle Expired to Suspend User.:N Suspension End Time: MAC Binding Expiry:0Day Description: | ot Enabled C | Classroom | | ۰ | default | | Unlimited | | default | Not Charging | | 1 |
| | The number of repeated logins of th Users can use different services for I | e plan is user's r nternet access and | maximum num d the number | nber of online of online use | e STAs. rrs of the same | service is restri | cted by the n | mber of repea | ated logins of the | corresponding access contro | ol. | | |

15. Verifying login failure of student users beyond the access period (10:34)

6 Optimization and Precautions for Simplistic Network Configuration

6.1 Optimization and Precautions for the RG-N18000 Configuration

6.1.1 Disabling authentication accounting update

The 2nd-generation portal accounting update needs accounting update responses. If no response is received within a period of time, the RG-N18000 deems that the server is unreachable, resulting in intermittent network connection during authentication.

Configuration command: Ruijie(config)# no radius-server account update retransmit

Note: The RG-N18000 has resolved this issue in 11.0(1)B2 Build(10) released in October 2015. This command does not need to be configured on the RG-N18000 of 11.0(1)B2 Build(10) and later versions.

6.1.2 Optimizing HTTPS redirection on the RG-N18000

1. It is recommended to disable HTTPS redirection for 11.0(1)B2 build(10), 11.0(1)B2 build(11), and earlier versions.

HTTPS redirection involves socket encryption and decryption, which consume considerable resources, greatly lower the performance, and affect HTTP redirection. Therefore, the HTTPS redirection port needs to be disabled.

Configuration command: Ruijie(config)#no http redirect port 443

For example, some famous Websites such as Baidu use HTTPS and the configuration of this command will incur a redirection failure. In this case, enter a non-HTTPS URL to trigger redirection, for example, <u>http://www.baidu.com</u>.

2. For 11.0(1)B2T11 and later versions, enable HTTPS redirection as required and configure the CPP rate limit.

The HTTPS performance is optimized in the latest version, and CPU resources used by HTTPS and HTTP are separated and optimized to avoid mutual impact. HTTPS redirection can be enabled as needed. The HTTPS CPP rate limit must be configured (2 kbps for 11.0(1)B2T11 and 5 kbps for 11.0(1)B3P1).

Ruijie(config)#http redirect port 443

6.1.3 Enabling interface index uniqueness

The interface index of each physical port is unique on the RG-N18000. You can run the **show interface** command to display the **Index** field. When there are multiple line cards and an Aggregate Port (AP) is configured (one line card is inserted, the AP is configured, and then another line card is inserted), after the device is restarted, the interface indexes of the device may change. As a result, the area division function of SAM+ will fail. The interface index uniqueness function must be enabled.

Configuration command: Ruijie(config)#snmp-server if-index persist

6.1.4 Enabling migration of authenticated users on the RG-N18000 as user re-authentication is required after AC hot backup switchover

After wireless Web authentication is enabled on the RG-N18000, when hot backup switchover is performed on master and slave ACs, the port+VID information of Web authenticated clients changes on the RG-N18000 and such clients need to be re-authenticated, which is against the purpose of wireless AC hot backup. Migration of Web authenticated clients can be enabled on the RG-N18000 to resolve this issue. After the migration is enabled, if the user port or VLAN changes in the same super VLAN, the RG-N18000 processes authentication information internally and user re-authentication is not required.

```
Ruijie (config)# station-move permit
Ruijie (config)# web-auth station-move auto
Ruijie (config)# web-auth station-move info-update
```

6.1.5 Preventing users with all-zero IP addresses on SAM+

IP addresses of users to be authenticated need to be obtained through the SU client or the DHCP snooping table of the RG-N18000 for both 802.1x authentication and MAB authentication. When the following configurations are lost, the RG-N18000 fails to obtain IP addresses of to-be-authenticated users and sends all-zero IP addresses to the SAM+ server. If the preemption policy for users with the same IP addresses is configured on the SAM+ server, users are forced to go offline. To resolve this problem, configure the following commands:

```
Ruijie (config) # ip dhcp snooping //Enable IP DHCP snooping.
Ruijie (config) # aaa authorization ip-auth-mode mixed //Set the IP authorization mode of
to-be-authenticated users to the mixed mode.
Ruijie (config) # dot1x mac-auth-bypass valid-ip-auth //Apply MAB authentication only after
IP addresses are obtained. The configuration of this command will force online users to go offline.
It is not recommended to run this command in service peak hours.
Ruijie (config) # dot1x valid-ip-acct enable //802.1x authenticated users
and MAB authenticated users are forced to go offline 5 minutes later if they fail to obtain IP
addresses. The configuration of this command will force online users to go offline. It is not
recommended to run this command in service peak hours.
```

6.1.6 Ensuring accuracy of online user information on SAM+ and the RG-N18000

To prevent exceptions caused by online user information inconsistency between SAM+ and the RG-N18000, SAM+ is configured to automatically check online user information with the RG-N18000 at 02:00 A.M. every day and delete information about fake online users.

```
Run the snmp-server command on the RG-N18000 to synchronize information with SAM+:
snmp-server host 172.18.18.18 informs version 2c ruijie //The IP address of SAM+ is used in
the command.
```

```
snmp-server community ruijie rw
```

6.1.7 Restricting the number of authentication-free VLANs

When excessive authentication-free VLANs (more than 50) are configured, the duplication of broadcast or multicast packets will cause high CPU usage of line cards and incur failures. It is recommended that no more than 50 authentication-free VLANs be configured. If more than 50 authentication-free VLANs are required, use security channels or authentication-free sites instead.

Configuration command in global/interface configuration mode: direct-vlan xxx,xxx-xxx (run the **show direct-vlan** command for judgment)

6.1.8 Pruning VLANs configured on downlink interfaces of the RG-N18000

There is a risk on the RG-N18000 on a large Layer-2 network that protocol packets sent from a sub VLAN of the RG-N18000 are flooded to all sub VLANs. Especially in QinQ scenarios, a large number (PE-VLAN quantity x CE-VLAN quantity) of protocol packets will be flooded, which greatly increases the CPU usage of the RG-N18000 and consumes the link bandwidth of the downlink aggregation and access devices. Therefore, it is required to prune unnecessary VLANs on the downlink interfaces of the RG-N18000, to prevent unnecessary resource consumption.

DSW-18KX_LX(config-if-AggregatePort 103)#switchport trunk allowed vlan only 100-103,900,3501-3550,4201-4204

6.1.9 Configuring the downlink interfaces of the RG-N18000 as routing protocol passive interfaces to prevent resource waste

As described above, it is recommended to reduce CPU resources and link bandwidth of the RG-N18000 consumed by unnecessary protocol packets.

DSW-18KX_LX(config-router) #passive-interfac aggregatePort 100

6.1.10 Enabling the RG-N18000 to process DHCP relay packets in a case with DHCP snooping enabled

If DHCP snooping is enabled, the RG-N18000 discards DHCP relay packets for address application from the aggregation device. Run the following command to ensure protocol compatibility:

DSW-18KX_LX(config)#ip dhcp snooping check-giaddr //DHCP snooping and DHCP relay compatibility command. It is used to prevent the DHCP snooping module of the RG-N18000 from discarding DHCP relay packets.

6.1.11 Reducing the number of CE-VLANs created during deployment

If only 50 CE-VLANs are required on the live network, run the **qinq termination ce-vlan 101 to 151** command to create required VLANs. Avoid creating 511 CE-VLANs at a time. More CE-VLANs will result in high CPU usage of the RG-N18000.

6.1.12 Disabling the DHCP guard function via NFPP

Disable the DHCP guard function of NFPP when the device serves as a DHCP relay. Otherwise, some users may fail to obtain IP addresses. NFPP has restrictions on the number of packets transmitted from MAC addresses.

Ruijie (config) #nfpp Ruijie (config-nfpp) # no dhcp-guard enable //The DHCP guard function can be enabled in interface configuration mode, to control the DHCP relay function on some interfaces.

6.1.13 Configuring alarms for easily-missed or error-prone configurations

1. If a message indicating that the entry quantity reaches the limit is displayed when there are only thousands of 802.1x authenticated users and Web authenticated users, check whether the gateway mode is configured (save the configuration and restart the device for the configuration to take effect).

Configuration command: auth-mode gateway Check command: show run | include gateway

6.2 Configuration Optimization and Precautions for Aggregation Devices

and Access Devices

6.2.1 Configuration Optimization of Aggregation Devices and Access Devices

6.2.1.1 Disabling security functions on the access and aggregation devices in simplistic network scenarios

NAS authentication-related functions (including AAA, Web authentication, and 802.1x authentication) as well as interface security and anti-spoofing security functions (DHCP snooping, ARP check, IP source guard) need to be disabled on the access and aggregation devices in simplistic networks. If such functions are not disabled, they may conflict with the simplistic network solution or unknown bugs may arise, affecting services on the live network.

For example, if 802.1x authentication is enabled on the RG-S21 series devices, 802.1x packets cannot be transparently transmitted to the RG-N18000.

6.2.1.2 Enabling functions on access devices

1. Enable the RLDP function:

Ruijie(config-if- FasterEthernet 0/1) #rldp port loop-detect shutdown-port

2. Enable the port protection function if there are interfaces belonging to the same VLAN:

Ruijie(config-if-FasterEthernet 0/1)# switchport protected

3. Enable the storm suppression function. It is recommended that the rate of multicast and broadcast access packets be limited to 30 PPS, which can be adjusted based on actual conditions.

```
Ruijie(config-if-FasterEthernet 0/1)# storm-control multicast pps 30
Ruijie(config-if-FasterEthernet 0/1)# storm-control broadcast pps 30
```

6.2.1.3 Enabling functions on the aggregation device

- 1. Enable VLAN pruning.
- 2. Enable the port protection function if there are interfaces belonging to the same VLAN:
- 3. Enable the storm suppression function. It is recommended that the rate of multicast and broadcast access packets be limited to 1000 PPS, which can be adjusted based on actual conditions.

Note: The aggregation device serves users in a building. Only VLAN pruning and port protection are required if the aggregation device serves users in an area.

6.2.1.4 Enabling port protection on access devices in the access isolation solution, to prevent DHCP spoofing

In the access isolation solution, all interfaces on the access device share the same VLAN and port protection must be enabled. Otherwise, when a private downlink router connected to the access device serves as a DHCP server, DHCP packets are flooded in the above-mentioned VLAN, resulting in DHCP spoofing. It is recommended to replace an access switch that does not support port protection in a project if any.

6.2.1.5 Enabling RLDP on access devices

Loops may occur due to private hub connections. RLDP must be enabled at the access device to. Otherwise, Web authentication or 802.1x authentication packets may be flooded after loops occur, and the CPP of the RG-N18000 reaches the limit. As a result, users throughout the network cannot perform 802.1x authentication or Web authentication. It is recommended to replace an access switch that does not support RLDP in a project if any.

6.2.1.6 Configuring STP and RLDP on access devices to prevent loops in QinQ isolation scenarios

Globally enable STP on each access device, enable BPDU filter on the uplink interface as well as BPDU guard and RLDP on downlink interfaces. The BPDU filter configured on the uplink interface of an access device ensures that STP takes effect only on a single device and topology learning and root bridge election are not performed. When receiving of BPDU packets, the BPDU guard configured on a downlink interface shuts down the downlink interface to prevent loops.

Note: STP does not need to be enabled in the access isolation solution whereas it is mandatory in the QinQ isolation solution, because RLDP may fail to detect loops when one VLAN is configured on each port of the access device in the QinQ scenario.

6.2.2 Precautions for Wireless Device Configuration

6.2.2.1 Disabling the ARP proxy function of the AC globally

The ARP proxy function of the AC is not globally disabled. As a result, the ARP keepalive packets sent by the RG-N18000 are responded to by the AC during migration of authenticated users. The ARP proxy function is enabled by default and needs to be disabled on the AC, so that the gateway ARP proxy function is carried out by the RG-N18000.

AC(config) #no proxy_arp enable

6.2.2.2 Enabling the layer-2 isolation function for wireless users on the AC to prevent an overlarge broadcast domain

AC(config-wids) #user-isolation ac enable

6.2.2.3 Creating NFPP trust lists on the AC and adding the gateway MAC address of the RG-N18000 to the trust lists of ARP-guard and DHCP-guard

The user gateway is deployed on the RG-N18000 on simplistic networks. The AC interacts with the RG-N18000 very frequently. As a result, the gateway MAC address of the RG-N18000 is added to the isolation lists by ARP-guard and DHCP-guard of NFPP. Create NFPP trust lists on the AC and add the gateway MAC address of the RG-N18000 to the trust lists of ARP-guard and DHCP-guard.

```
nfpp
arp-guard trusted-host 10.51.0.1 5869.6ca2.9ec
dhcp-guard trusted-host 10.51.0.1 5869.6ca2.9ec
```

6.2.2.4 Ensuring NAS consistency for Web authenticated wireless users

If the NAS of some wireless users is the RG-N18000 while the NAS of other wireless users is the AC, MAB authentication will fail during inter-area roaming and users need to be re-authenticated. In severe cases, information about the same user exists on two NASs, resulting in a charging error.

6.2.2.5 Configuring DHCP snooping + IP source guard + ARP check to prevent ARP spoofing and private IP address configuration of wireless users

802.1x authentication is configured on the AC and the following functions need to be enabled on the AC: DHCP snooping + IP verify source port-security + ARP-check.

Web authentication is configured on the RG-N18000, and static ARP addresses are bound after successful authentication by default, to prevent ARP spoofing. To prevent private IP address configuration, enable the **web-auth dhcp-check** command on the device.

6.3 Scenario Restrictions and Suggestions

6.3.1 Scenario Restrictions

6.3.1.1 MAB authentication does not support static IP addresses by default, but supports manually-added IP addresses.

IP addresses need to be authorized for MAB authenticated users by using the DHCP snooping table, source binding table, or 802.1x binding table of the RG-N18000. Static IP addresses are not contained in the DHCP snooping entries of the RG-N18000 because users of static IP addresses do not exchange DHCP packets. Therefore, no IP addresses can be authorized for MAB authenticated users. As a result, entries with all-zero addresses exist on SAM+. If the **dot1x mac-auth-bypass valid-ip-auth** command is configured, MAB authentication is not initiated.

MAB authentication is normal for manually added static IP addresses, and information about users who use MAC fast authentication needs to be manually added on SAM+. The configuration is as follows:

dot1x address-binding mac 9048.9a8e.a033 ip 10.0.100.188

ip source binding 5656.5656.6654 vlan 10 192.168.1.1 interface gi1/3

6.3.1.2 The aggregation device needs to support selective QinQ in the QinQ isolation solution. Otherwise, the QinQ isolation solution cannot be deployed.

In the QinQ isolation solution, the aggregation device needs to add an outer VLAN to packets with an inner VLAN from access devices. This requires the selective QinQ function. It is necessary to replace aggregation devices that do not support selective QinQ in a project if any.

6.3.1.3 After the AM rule function is enabled, AM rules need to be configured for assigned DHCP network segments throughout the network. Otherwise, the DHCP server cannot assign addresses.

The AM rule function is configured globally. After it is enabled, all DHCP packets sent to the RG-N18000 must match AM rules configured on the RG-N18000. DHCP packets that do not match the AM rules will be discarded.

This problem does not exist if the AM loose mode is enabled using the match ip loose command.

6.3.1.4 After the AM rule function is enabled, if the same network segment is configured in two AM rules, address preemption occurs and users who match the AM rule of a smaller address pool may fail to obtain IP addresses.

AM rule 1: match ip 192.168.0.0 255.255.0.0 Gi5/3 vlan 1005 AM rule 2: match ip 192.168.6.0 255.255.255.0 Gi5/4 vlan 1006

The same IP address segment is configured in AM rule 1 and AM rule 2 and users who match AM rule 1 may preempt IP addresses in the address pool of AM rule 2. As a result, users who match AM rule 2 fail to obtain IP addresses.

It is recommended to avoid overlapped IP address segments in entries of AM rules.

6.3.1.5 If the loose mode of the AM rule function is not configured, some users who do not match AM rules in strict mode cannot be pinged or fail to obtain IP addresses.

Ruijie(config)#address-manage Ruijie(config-address-manage)#match ip loose

6.3.1.6 When the AM rule function is enabled on the RG-N18000 serving as a DHCP relay, multiple secondary addresses must be configured for the RG-N18000 and multiple small DHCP address pools must be configured for the DHCP server.

A non-Ruijie device may be used as the DHCP server. The processing logic of the DHCP server is implemented according to RFC standards, and the DHCP server cannot perform refined address assignment according to Ruijie AM rules after only one large address pool is configured. Therefore, multiple small DHCP address pools must be created for the DHCP server based on the gateway address of the RG-N18000, so that the DHCP server is compatible with the AM rules configured on the RG-N18000 serving as a DHCP relay.

For example, if the DHCP relay is enabled on the RG-N18000 and the AM rules need to be used to achieve refined assignment of the DHCP address pool, multiple secondary addresses must be configured for the gateway of the super VLAN on the RG-N18000. If the AM rules are disabled, users can only request IP addresses in the network segment of the primary IP address of the gateway.

interface VLAN 4000
ip address 10.168.1.1 255.255.255.0
ip address 172.168.1.1 255.255.255.0 secondary //If no AM rule is configured, client in the
VLANs corresponding to the network segments of secondary addresses cannot obtain IP addresses.

Two address pools need to be created on the DHCP server: 10.168.1.0 255.255.255.0; 172.168.1.0 255.255.255.0.

6.3.1.7 DB cards support 51 CE-VLANs at most, and do not support excessive cascaded access devices in QinQ isolation scenarios.

Incremental IDs need to be assigned to CE-VLANs when access devices are cascaded in QinQ isolation scenarios. DB cards cannot support a number of cascaded switch interfaces greater than 51.

It is recommended to modify the cascading topology, and replace DB cards with ED cards when modifying the cascading topology cannot resolve the problem.

6.3.1.8 The FP entry capacity is limited.

ED cards support up to 7,000 ACLs while DB cards support a maximum of 2,000 ACLs only. All security functions share a fixed total quantity of FP table entries. Therefore, when ACL/PBR-related ACEs are configured, applications of the same category needs to be configured in the same super VLAN rather than on different SVIs. Otherwise, the FP entry capacity may be insufficient. The algorithm is described as follows:

For limitations and calculation methods of the FP entry capacity, see the *TCAM Hardware Resource Calculation Method of Security Functions*. Function groups occupy entries differently. It is required to calculate whether the number of entries reach the limit and how many entries are available in strict accordance with the preceding attachment. Both the configuration and card type affect the calculations. The following uses the FE entry capacity of the devices used by Xuzhou Medical College as an example to describe the TCAM occupancy.

1. Slice occupancy: Normally, the following five function groups occupy seven slices.

Function Group 3 (802.1x authentication, Web authentication, authentication-free VLANs, extended ACL-based security channels, and authentication-free sites): Occupies two slices and supports a maximum of 256 entries. Available space of this function group = 256 – Occupied space. The available space indicates how many entries can be configured in this function group and only applications in the same category as the function group can be configured.

Function Group 4 (authentication-free sites with ARP): Occupies one slice, and supports a total of 256 entries for DB cards and 512 entries for ED cards.

Function Group 5 (PBR and default route): Occupies two slices, and supports a total of 256 entries for DB cards and 512 entries for ED cards.

Function Group 7 (QinQ VLAN tag termination): Occupies one slice, and supports a total of 256 entries for DB cards and 512 entries for ED cards.

Function Group 8 (QinQ migration): Occupies one slice, and supports a total of 256 entries for DB cards and 512 entries for ED cards.

2. If the DB card is used, only eight slices are available, with each supporting 256 entries. After the five function groups above are configured, there is only one slice available, with the available space of 256 entries.

When there are more than 256 authentication-free VLANs in Function Group 3, this group occupies another two slices.

When the number of authenticated-free VLANs is smaller than 256, they occupy two slices; when the number is greater than 256, they occupy four slices.

For example, if 370 authentication-free VLANs are configured, they occupy four slices. Though five function groups are configured, nine slices are actually required. Therefore, the capacity is insufficient. If entries need to be configured for other function groups in single mode, the available slice can be used for entry delivery.

3. If the ED card is used, 14 slices are available, with each supporting 512 entries. After the five function groups above are configured, there are seven slices available, with each supporting 512 entries. There are two types of available space: one is the available space of the seven occupied slices and such available space supports the configuration delivery of the same function group; the other is the idle seven slices, which can be requested by other function groups.

6.3.1.9 Inter-VSL mirroring in VSU scenarios is limited.

- 1. The traffic mirrored across chassis cannot be balanced among VSL ports. As a result, all bandwidth of one VSL may be occupied and packets of other service may be discarded.
- 2. One-to-many mirroring floods the traffic to the mirrored VLAN through the loopback interface. Even if the peer chassis has no member port of the VLAN, mirrored traffic is also flooded to the peer chassis and the traffic cannot be balanced among VSLs. Consequently, all bandwidth of one VSL may be occupied and packets of other services are discarded.

Mitigation measures:

1. Limit the rate of inter-chassis traffic floods, to avoid affecting packets of other services.

- 2. As far as mirroring is concerned, it is recommended that the mirroring destination port be configured as the inter-chassis AP, which can balance traffic among ports. By default, local forwarding is preferred and traffic is not transmitted through VSLs.
- 6.3.1.10 In global ACLs, the permit entry does not take effect but the deny entry does.
- 6.3.1.11 In security channels, the permit entry takes effect but the deny entry does not.
- 6.3.1.12 The number of management VLANs in an AP cannot be too large in wireless scenarios. It is not recommended that the quantity exceed 512.
- 6.3.1.13 Wireless 802.1x authentication can be enabled only on the AC and the RG-N18000 does not support wireless 802.1x authentication.
- 6.3.1.14 It is not recommended to configure the IP source guard and ARP check functions in simplistic network scenarios.

By default, static ARP addresses are bound with authenticated users in simplistic networks, to prevent ARP spoofing. In addition, the IP source guard function occupies FP entries, resulting in entry insufficiency.

6.3.1.15 Restrictions on dumb clients that do not initiate network access actively

In the simplistic network solution, authentication-free VLANs, authentication-free sources, and security channels are configured on the RG-N18000, only clients in authentication-free VLANs can actively access dumb clients that do not actively send packets.

6.3.1.16 Restrictions on adding authentication-free devices to authentication-free VLANs

When excessive authentication-free VLANs (more than 50) are configured, the duplication of broadcast and multicast packets will cause high CPU usage of line cards and incur failures.

7 Common Troubleshooting for Simplistic Networks

7.1 Authentication Page Display Failure During Web Authentication

7.1.1 Symptom

A blank page is displayed, or a prompt indicating that no device is registered is displayed during Web authentication.

7.1.2 Possible Causes

1. The client cannot obtain an IP address, and fails to send HTTP packets.

- 2. The client obtains an unavailable DNS server, and the domain name fails to be parsed.
- 3. The redirection parameter, portal key, and source interface configured on the RG-N18000 are inconsistent with those on ePortal.
- 4. The DHCP check in Web authentication is enabled on an interface and a static IP address is used, resulting in redirection failures.
- 5. HTTP packets are lost and cannot reach the RG-N18000, and the RG-N18000 fails to perform redirection.
- 6. Packets cannot reach the Web process, and the RG-N18000 fails to perform redirection.
- 7. The client cannot communicate with the portal server via packets because of channel exceptions, such as unreachable routes and security device filtering.
- 8. The ePortal server works abnormally, sending no response packets.
- 9. If a non-SAM+ server is adopted, the possible cause is that the URL does not meet server requirements and therefore, the Web authentication page does not pop up.
- 10. The user uses a static IP address, but has the DHCP check in Web authentication configured: **web-auth dhcp-check** or **web-auth dhcp-check vlan xxx**.
- 11. In version 11.0(1)B3P3, the Web authentication page cannot be displayed and redirection cannot be performed if a static IP address is within the MAB authentication address range.

7.1.3 Handling Steps

- 1. Check whether the client obtains a correct IP address.
- 2. Open the browser, enter http://www.ruijie.com.cn and http://183.1.1.1 (the IP address must not exist in the intranet) separately, and observe whether the browser redirects to the URL.

If the browser fails to redirect to the entered website but redirects to the entered IP address, check whether the DNS resolution is normal.

If the redirection fails after the website and IP address are entered or no page pops up after redirection, proceed to the following step.

3. Check whether the configurations on the RG-N18000 and ePortal are correct.

Check whether the redirection configuration is correct on the RG-N18000, and whether the **web-auth portal key** and **IP portal source interface** commands on the RG-N18000 are consistent with those on the ePortal.

```
web-auth template eportalv2 //Create a Web authentication template.
ip 202.204.193.32 //IP address of the ePortal server
url http://202.204.193.32/eportal/index.jsp //URL of the ePortal server.
web-auth portal key ruijie //Encrypt the URL. There must be no space at the end of the command.
ip portal source-interface GigabitEthernet 1/24 //The IP address of the interface is 35.0.0.1
configured on the ePortal. Ensure that the route is reachable.
```

Check whether Web authentication is correctly configured on the interface. Ensure that both 802.1x authentication and Web authentication are enabled on a VLAN.

```
interface range GigabitEthernet 0/1 //Configure the interface for enabling Web
authentication.
web-auth enable eportalv2 //Enable Web authentication on the interface.
web-auth vlan-control 2000-3000 //Enable VLAN-based Web authentication.
```

Check whether the configuration on ePortal is consistent with that on the RG-N18000. See the figure below.

| RG-ePortal | Portal Components Ne | twork Access Portal System | | | | |
|--|---|--|--------|---|---|----|
| | | | | | | Ch |
| Network Access Portal S | Location: Network Access Portal System >1 | Device Management > Add Device | | | | |
| System Settings Device Management Administrator Access Page Management | | | | | | |
| Log Management | | п | Device | . Details | | |
| System Maintenance Authentication Reques | | | | 172.29.2.253 | | |
| | | * Device IP | | A superior adding sultiple devices a | d plassa comprete auch danica | |
| | | | | using comma (,). Support max 500 adding single device. | levices. For H3C, only support | |
| | | Read/Write Community | | au | | |
| | | SNMP Version | | SNMPv2c • | | |
| | | * Device Type | | 2nd-Generation Web Auth: * | | |
| | | * NAT Proxy Mode | | Close • | | |
| | | veb-auth portal key | | au | | |
| | | IPv6 Authentication Portal Protocol | | Ruijie Portal Protocol 🔹 | | |
| | | | | | | |
| | | Warran TD Comput | | | | |
| | | namage IP Segnerit | | A | | |
| | | | | Only H3C device is required to ad segment. Please use comma (,) to | d corresponding management IP separate multiple IP segments. | |
| | | Gateway IP | | | | |
| | | Gateway MAC | | | | |
| | | Device Location | | | | |

4. Check whether DHCP check in Web authentication is enabled on the interface, whether IP DHCP snooping is enabled, and whether the IP address is obtained dynamically. The DHCP check in Web authentication needs to be associated with DHCP snooping entries. If no DHCP snooping binding table is available, the Web authentication redirection will fail.

Command for DHCP check in Web authentication: web-auth dhcp-check or web-auth dhcp-check vlan xxx

- 5. Run the show version command to check whether the RG-N18000 is of version 11.0(1)B3P3. If yes, check whether static IP address MAB authentication is enabled. If a static IP address is within the IP segment range configured by using the dot1x mac-auth-bypass static-ip-segment command, the Web authentication page does not pop up and redirection cannot be performed.
- If the system still fails to redirect to the URL after the steps above are performed, check whether the RG-N18000 receives the packets.

```
show mac-address-table | include ***(MAC address of the user)
show arp | include ****(MAC address of the user)
If no output of the preceding commands is displayed, it indicates that the RG-N18000 does not
receive the packets. If relevant entries are displayed, perform ACL counting or packet capture
for confirmation.
ip access-list extended YYY
10 permit ip host 192.168.1.1 any //192.168.1.1 is the user IP address.
20 permit ip any any
interface gigabitEthernet 1/1
ip access-group YYY in //Apply the ACL to the faulty port.
ip access-list counter YYY //Display the packet count.
```

Example:

```
core (config) #expert access-list extended exp1
core(config-exp-nacl)#20 permit ip host 1.1.1.1 any any any
core(config-exp-nacl)#100 permit ip any any any any
core(config-exp-nacl)#100 permit ip any any any any
core(config-exp-nacl)#exit
core(config)#int te1/1
core (config-if-TenGigabitEthernet 1/1) #expert access-group exp1 in
core(config-if-TenGigabitEthernet 1/1)#exit
core(config) #expert access-list counter exp1
core(config) #show access-lists
expert access-list extended expl
                                                  Packet count
20 permit ip host 1.1.1.1 any any any
                                        (20)
100 permit ip any any any any (1000)
core(config)#
```

- 7. Normally, if the system still fails to redirect to the URL after the steps above are performed, collect debugging information on the RG-N18000 based on fault information, and contact the TAC for handling.
- 8. If the system successfully redirects to the URL but the authentication page does not pop up, check the connectivity between the client and ePortal.

For example, to run the ping command, disable the firewall on the ePortal server and ensure that the firewall on the intermediate link allows access.

 If the connectivity between the client and ePortal is normal, enable packet capture on both the client and ePortal, record the URL to which the client redirects as well as the logs on the ePortal server, and contact the ePortal R&D engineers for handling.

7.1.4 Fault Information Collection

Run the following commands to collect information on the RG-N18000:

```
terminal length 0
show ver detail
show run
show mac-address-table | include ***(MAC address of the user)
show arp | include ****(MAC address of the user)
show ip dhcp snooping
show ip dhcp snooping binding | in H.H.H
debug web-auth cli
show web-auth user name ***
debug web show
```

```
debug web stat
debug scc stat
undebug all
show log
terminal no length
```

The figure below shows the information collected on the ePortal server.

| 🕌 log | | | |
|------------------------|--------------------|-----------------|----------|
| € 0- ⊮ < | ▼ RG-ePortal ▼ log | - 🛃 | |
| 组织 ▼ 包含到库中 ▼ | 共享 🔻 新建文件夹 | | i 🕶 🗖 🔞 |
| | | | |
| | 10g_2014-05-15.4 | 2014/5/15 10:38 | 1,144 KB |
| | log_2014-05-15.3 | 2014/5/15 8:52 | 2,083 KB |
| | log_2014-05-15.2 | 2014/5/15 5:55 | 2,083 KB |
| | 10g_2014-05-15.1 | 2014/5/15 2:57 | 2,083 KB |
| | log_2014-05-14.8 | 2014/5/15 0:00 | 1,151 KB |
| | 10g_2014-05-14.7 | 2014/5/14 22:21 | 2,083 KB |

7.1.5 Fault Summary and Notes

The Web authentication page can be popped up in the following steps:

Step 1: The client exchanges HTTP packets with the RG-N18000, which pushes the redirection URL to the client. The client browser redirects to the redirection URL.

Step 2: The client accesses the redirection URL and exchanges packets with the ePortal server.

Therefore, if the client fails to redirect to the URL, the failure occurs between the client and the RG-N18000; if the client redirects to the URL but no page pops up, the failure occurs between the client and the ePortal.

7.2 Web Authentication Failure

7.2.1 Symptom

A Web authentication prompt shows that the authentication fails or the connection to the authentication server times out.

7.2.2 Possible Causes

- 1. The verification conditions of SAM+ are not met.
- 2. The interconnection configurations between the RG-N18000, ePortal, and SAM+ are inconsistent.
- 3. The connectivity between the RG-N18000 and ePortal or between the RG-N18000 and SAM+ is abnormal. As a result, packets cannot be exchanged normally.
- 4. Portal or RADIUS packets cannot be properly processed due to internal errors of the RG-N18000.
- 5. The ePortal server or SAM+ server malfunctions, causing failures in processing or responding to packets.

6. The RADIUS server is faulty, and both the escape function and the none mode of AAA are configured on the RG-N18000.

7.2.3 Handling Steps

1. Pay attention to the authentication failure prompt on the client page and that on the SAM+ server. Perform basic fault locating based on the prompts and check whether the verification conditions of SAM+ are met.

For example, if prompts on the client and SAM+ clearly show that the Web authentication service is not allowed in this area or information verification fails, check the area, service, and access control and make adjustments accordingly on SAM+.

| Shortcut Channel | Φ. | Homepage | System | Security | User | Access Contr | ol Billing | Account | Operatio | on | | | |
|---|---|----------------------------|----------------------|--------------|-----------|--------------|-----------------|---|------------|--------|----------|-------------|--------------------|
| Location: Operati | on > Log Management | | | | | | | | | | | | |
| Log Type Log Time (Start) Log Content | Authentication Log: 2018-05-09 00:00:00 (A | 💷 🗖 Always fuzzy query) | Operator Log Time | r e (End) | 2018-05-0 | 09 23:59:59 | | Gene Gen Gene Gene | ral Search | Search | | | |
| | | | | | | De | elete the Selec | ed Delete | All | | | | |
| | | | | | | | | | | | | | |
| There were no res | ults found. | | | | | | | | | | | Currently 1 | /1Page ♥₲ Very F |
| There were no res | ults found. J Type Log (| Content | | | | | | | | | Log Time | Currently 1 | /1Page 🕸 Go Very F |

2. Check the device configurations, mainly the RADIUS server configuration, RADIUS key, configurations on SAM+ and ePortal, and IP RADIUS source interface.

```
aaa new-model
                  //Enable the AAA function.
aaa authentication login default local //Use the local username/password for login to the
AAA device.
radius-server host 172.18.157.32 key ruijie
                                                 //Configure the IP address and key for the
AAA server, which are applicable to the scenarios with a single RADIUS server.
aaa accounting network default start-stop group radius //AAA reference configuration. The
actual service deployment prevails.
aaa authentication web-auth default group radius
                                                      //Reference configuration for AAA Web
template. The actual service deployment prevails.
aaa accounting update
                                   //Configure AAA accounting update.
aaa accounting update periodic 15
                                       //Set the interval for AAA accounting update to 15 min.
aaa authorization ip-auth-mode mixed //Set the IP address authorization mode of 802.1x clients
to the mixed mode. The IP addresses can be obtained via polling in multiple ways (DHCP/RADIUS).
no aaa log enable //Disable the AAA log function.
web-auth template eportalv2 //Create a Web authentication template.
  ip 172.18.157.33
                               //IP address of the ePortal server.
  url http://172.18.157.33/eportal/index.jsp //URL of the ePortal server.
  authentication default
                             //Optional. This command is required when the authentication list
name for AAA is not set to default.
  accounting default //Optional. This command is required when the accounting list name
for AAA is not set to default.
```

```
web-auth portal key ruijie //Mandatory. Configure the Web portal key.
ip radius source-interface GigabitEthernet 1/24 //Configure the source interface for the device
to communicate with the RADIUS server. The device address added to SAM+ should be the address
of this interface.
ip portal source-interface GigabitEthernet 1/24 //Configure the source interface for the device
to communicate with the ePortal server. The device address added to the ePortal server should
be the address of this interface.
interface range GigabitEthernet 0/2-3 //Configure the interface for enabling Web
authentication.
web-auth enable eportalv2 //Enable Web authentication on the interface.
web-auth vlan-control 2000-3000 //Enable VLAN-based Web authentication.
```

snmp-server host 172.18.157.32 informs version 2c ruijie

snmp-server community ruijie rw



| Location: System > Device Managem | ent > Add | | | | |
|-----------------------------------|-------------------|--|--------------------------------|---------------|--------------------------|
| Device | | | | | |
| Device IP Address* | 172.18.157.33 | | IP Type* | IPv4 | |
| Device Type* | RG-ePortal • | | Model* | Please Select | |
| PPPoE Authentication Domain | | Please use comma or space to separate multiple domains | IPOE+Web Authentication Domain | | Please use comma o |
| Device Key* | ruijie | | Community* | ruijie | |
| MACANNA | | For trusted ARP binding application, MAC address must be | CNIM D Desire Dest | 464 | Maria and Cill in a |
| MAC Address* | filled | | SNMP Proxy Port | 161 | If you do not fill in, t |
| 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 Undate Client Detection | Ares | Diasca Calart | (Device ID(v/I)) |

| Location: System > Device Manager | ent > Add | | | | |
|-----------------------------------|----------------------------------|---------------------------------------|--------------------------------|-----------------|------------------------------|
| Device | | | | | |
| Device IP Address* | 172.18.157.1 | | IP Type* | IPv4 • |] |
| Device Type* | Ruijie Switch | | Model* | N18K • | |
| PPPoE Authentication Domain | Please use comma o | or space to separate multiple domains | IPOE+Web Authentication Domain | | Please use comma or spa |
| Device Key* | ruijie | | Community* | ruijie | |
| MAC Address | For trusted ARP bind | ding application, MAC address must be | CNIMD Drown Dort | | If you do not fill in the du |
| MAC Address. | filled | | SNIMP Proxy Port | | I you do not nin in, the dr |
| 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)) |
| | | | | | |

- 3. Ping the server from the RG-N18000 (the ping operation is forbidden if the firewall is enabled on the server). The operation aims to check the connectivity between the IP address of the source interface and the server. If the connectivity test fails, check the network status.
- 4. If the RG-N18000 is unreachable to the server, check whether the network is normal and then check whether SAM+ is faulty. If SAM+ is faulty, check whether the escape function is configured on the RG-N18000.

Check whether the none mode of AAA is configured in the following case: The SAM+ server is faulty, and the escape function is configured, but the escape function does not take effect and a message is displayed during authentication, indicating that the authentication times out and the device does not respond.

```
SDYY-N18007-Center#sh run | inc radius
web-auth radius-escape
aaa accounting network default start-stop group radius none
aaa authentication dot1x default group radius none
aaa authentication web-auth default group radius none
ip radius source-interface Loopback 0
```

The none mode of AAA enables users to access the Internet without authentication when the RADIUS server is unreachable, provided that "radius-server timeout xxx" is displayed. RADIUS packets are sent at an interval of 5s by default and the default retransmission count is 3. The none mode of AAA is applied 20 seconds later. By default, the packet from ePortal times out when ePortal fails to receive a response within 9 seconds. As a result, the none mode of AAA is not applied when the packet from ePortal times out. The user escape function also fails.

Handling suggestions: 1. Delete the none mode of AAA.

2. Run the following command to set the RADIUS detection duration to a value smaller than the timeout duration (9s) of packets of ePortal: radius-server timeout 2

5. If the configuration is correct and the association is normal, run the following commands on the RG-N18000 to collect information:

```
debug scc stat
debug web-auth cli
sh web user ip ***(ip) -- Check whether a user using this IP address is online.
sh web syslog ip ***(ip) --Display the historical Internet access records of the IP address.
show web-auth authmng abnormal
show radius timeout record - Display RADIUS server timeout records.
```

show radius auth stat -- Display statistics relevant to RADIUS authentication. When a fault occurs, run this command several times to check statistical changes. show radius acct stat --- Display RADIUS accounting statistics. When a fault occurs, run this command several times to check statistical changes.

Capture user authentication packets on the client, ePortal, and SAM+, and submit them to the TAC for handling.

7.2.4 Fault Information Collection

```
terminal length 0
show ver detail
show run
debug scc stat
debug web cli
show mac-address-table | include *** (MAC address of the user)
show arp | include **** (MAC address of the user)
show ip dhcp snooping
show ip dhcp snooping binding | in **** (user MAC address)
sh web user ip ****** (user IP address)
sh web syslog ip ****** (user IP address)
show web-auth authmng abnormal
show radius timeout record
show radius auth stat
show radius acct stat
show log
terminal no length
```

7.2.5 Fault Summary and Notes

7.3 Network Dropout During Web Authentication

7.3.1 Symptom

Web authenticated users are dropped out of the network, cannot access the network, or are prompted for re-authentication.

7.3.2 Possible Causes

- 1. The SAM+ server forces users to go offline, or users go offline due to the change in RG-N18000 configurations.
- 2. Users go offline due to user preemption behavior.
- 3. Users go offline because the accounting updates on the RG-N18000 do not match configurations on the SAM+ server.
- 4. Users generate no traffic within a period of time (code 4, idle timeout).

5. Users go offline for data migration because the environment is abnormal (such as a loop).

7.3.3 Handling Steps

 Go to the SAM+ system and access Operation > Online User on the Web management page, locate the user, view the go-offline cause prompt, and find out the possible go-offline causes preliminarily.

| SAM ⁺ se | CURITY ACCOUNTING MAN | IAGEMENT SYSTEN | 4 | | |
|---------------------|------------------------------|----------------------|---------------------------|--|-------------------|
| Shortcut Channel | \$ | Homepage | System Security | User Access Control Billing | Account Operation |
| Location: Operat | ion > Log Management | | | | |
| Log Type | Authentication Log: • | | Operator | | General Search |
| Log Time (Start) | 2018-05-09 00:00:00 | | Log Time (End) | 2018-05-09 23:59:59 | |
| Log Content | | (Always fuzzy que | ry) | | |
| | | | | Delete the Selected | Delete All |
| There were no re | sults found. | | | | 8 |
| E Lo | g Type Log | y Content | | | Log Time |
| The system will o | pt for fuzzy query no matte | er the function is s | elected or not in log con | ntent | |
| Do you want to s | et fuzzy query for others be | esides log content | ? Tick to enable fuzzy qu | ery and leave blank to enable accurate query | |
| | | | | | |

Note: The user go-offline prompts provided on SAM+ are accurate, but there may be some errors due to complex network environments.

2. If **the** device prompts that the user go-offline is caused by no traffic detected, as shown in the figure below, it indicates that SAM+ receives the TCP2009 no traffic notification from the traffic audit device (such as the RSR77, ACE, or EG) and forces the RG-N18000 to bring the user offline.

| Address: 10.1.32.8 Core-index 1 Current index 65 Index: 57 Time: 2017-5-31 14:13:57 Behavior: ONLINE Mac: cof2.fb8c.ae8f Vid: 350 Port: Gi1/4 Timeused: Od 00:00:00 Flow_up: O Flow_down: O [usr_syslog_show_byip] Timestart: 1970-1-1 08:00:00 [usr_syslog_show_byip] Status: WBA_USTATE_WAIT_AFF_ACK [usr_syslog_show_byip] Event: WBA_USTATE_WAIT_AFF_ACK [usr_syslog_show_byip] Event: WBA_EVENT_AFF_ACK [usr_syslog_show_byip] Ipfix_Flow_up: O [usr_syslog_show_byip] Tffix_Flow_up: O [usr_syslog_show_byip] Tffix_Flow_down: O [usr_syslog_show_byip] Tffix_Flow_down: O Index: 62 Time: 2017-5-31 15:05:44 Behavior: OFFLINE Mac: cof2.fb8c.ae8f Vid: 350 Port: Gi1/4 Timeused: Od 00:51:48 Flow_up: O Flow_down: O [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | N18K#show web-auth sy | slog ip 10.1.32.8 | |
|--|-----------------------|---------------------|---|
| Index: 57 Time: 2017-5-31 14:13:57 Behavior: ONLINE Mac: c0f2.fb8c.ae8f Vid: 350 Port: Gi1/4 Timeused: 0d 00:00:00 Flow_up: 0 [usr_syslog_show_byip] Timestart: 1970-1-1 08:00:00 [usr_syslog_show_byip] Utype: 3 [usr_syslog_show_byip] Escape: 0 [usr_syslog_show_byip] Escape: 0 [usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Costime: 0 [usr_syslog_show_byip] Costime: 0 Index: 62 62 Time: 2017-5-31 15:05:44 8 Behavior: OFLINE 6 Mac: c0f2.fb8c.ae8f 7 vid: 350 7 7 Port: Gi1/4 7 | Address: 10.1.32.8 0 | ore-index 1 Current | index 65 |
| Time: 2017-5-31 14:13:57 Behavior: ONLINE Mac: COf2.fb8c.ae8f Vid: 350 Port: Gi1/4 Timeused: Od 00:00:00 Flow_up: O Flow_down: O [usr_syslog_show_byip] Timestart: 1970-1-1 08:00:00 [usr_syslog_show_byip] Utype: 3 [usr_syslog_show_byip] Status: WBA_USTATE_WAIT_AFF_ACK [usr_syslog_show_byip] Event: WBA_EVENT_AFF_ACK [usr_syslog_show_byip] Escape: O [usr_syslog_show_byip] Ipfix_Flow_up: O [usr_syslog_show_byip] Ipfix_Flow_down: O [usr_syslog_show_byip] Costime: O Index: 62 Time: 2017-5-31 15:05:44 Behavior: OFFLINE Mac: COf2.fb8c.ae8f Vid: 350 Port: Gi1/4 Timeused: Od 00:51:48 Flow_up: O Flow_down: O [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | Index: 57 | | |
| Behavior: ONLINE Mac: cof2.fb8c.ae8f Vid: 350 Port: Gi1/4 Timeused: Od 00:00:00 Flow_up: O [usr_syslog_show_byip] Timestart: 1970-1-1 08:00:00 [usr_syslog_show_byip] Utype: 3 [usr_syslog_show_byip] Status: WBA_USTATE_WAIT_AFF_ACK [usr_syslog_show_byip] Escape: O [usr_syslog_show_byip] Ipfix_Flow_up: O [usr_syslog_show_byip] Ipfix_Flow_up: O [usr_syslog_show_byip] Ipfix_Flow_down: O [usr_syslog_show_byip] Costime: O [usr_syslog_show_byip] O O [usr_syslog_show_byip] O O [usr_syslog_show_byip] O O Port: Gi1/4 Timestart: [usr_syslog_show_byip] | Time: 20 | 17-5-31 14:13:57 | |
| Mac: c0f2.fb8c.ae8f Vid: 350 Port: Gi1/4 Timeused: 0d 00:00:00 Flow_up: 0 [usr_syslog_show_byip] Timestart: 1970-1-1 08:00:00 [usr_syslog_show_byip] Utype: 3 [usr_syslog_show_byip] Status: WBA_USTATE_WAIT_AFF_ACK [usr_syslog_show_byip] Escape: 0 [usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Ipfix_Flow_down: 0 [usr_syslog_show_byip] Ipfix_Flow_down: 0 [usr_syslog_show_byip] Costime: 0 Index: 62 0 Time: 2017-5-31 15:05:44 0 Behavior: OFFLINE 0 Mac: cof2.fb8c.ae8f 0 Vid: 350 0 Port: Gi1/4 1 Timeused: 0 0 Flow_down: 0 0 [usr_syslog_show_byip] 0 0 Flow_down: </td <td>Behavior: ON</td> <td>LINE</td> <td></td> | Behavior: ON | LINE | |
| vid: 350 Port: Gi1/4 Timeused: 0d 00:00:00 Flow_up: 0 [usr_syslog_show_byip] Timestart: 1970-1-1 08:00:00 [usr_syslog_show_byip] Utype: 3 [usr_syslog_show_byip] Utype: 3 [usr_syslog_show_byip] Estatus: WBA_USTATE_WAIT_AFF_ACK [usr_syslog_show_byip] Escape: 0 [usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Ipfix_Flow_udown: 0 [usr_syslog_show_byip] Costime: 0 Index: 62 62 Time: 2017-5-31 15:05:44 8 Behavior: OFFLINE 0 Mac: cof2.fb8c.ae8f 7 vid: 350 7 7 Port: Gi1/4 7 7 Timeused: Od 00:51:48 6 7 Flow_up: 0 0 14:13:57 [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 <td>Mac: c0</td> <td>f2.fb8c.ae8f</td> <td></td> | Mac: c0 | f2.fb8c.ae8f | |
| Port: Gil/4 Timeused: Od 00:00:00 Flow_up: O Flow_down: O [usr_syslog_show_byip] Timestart: 1970-1-1 08:00:00 [usr_syslog_show_byip] Utype: 3 [usr_syslog_show_byip] Utype: 3 [usr_syslog_show_byip] Event: WBA_USTATE_WAIT_AFF_ACK [usr_syslog_show_byip] Event: WBA_EVENT_AFF_ACK [usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Ipfix_Flow_down: 0 [usr_syslog_show_byip] Costime: 0 Index: 62 62 Time: 2017-5-31 15:05:44 8 Behavior: OFFLINE 0 Mac: cof2.fb8c.ae8f 7 vid: 350 7 7 Port: Gil/4 7 7 Timeused: 0d 00:51:48 7 7 Flow_up: 0 0 7 7 [usr_syslog_show_byip] Timestart: 2017-5 | Vid: 35 | 0 | |
| Timeused: 0d 00:00:00 Flow_up: 0 Flow_down: 0 [usr_syslog_show_byip] Timestart: 1970-1-1 08:00:00 [usr_syslog_show_byip] Utype: 3 [usr_syslog_show_byip] Status: WBA_USTATE_WAIT_AFF_ACK [usr_syslog_show_byip] Event: WBA_EVENT_AFF_ACK [usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Ipfix_Flow_down: 0 [usr_syslog_show_byip] Costime: 0 Index: 62 Time: 2017-5-31 15:05:44 Behavior: OFFLINE Mac: cof2.fb8c.ae8f Vid: 350 Port: Gi1/4 Timeused: 0d 00:51:48 Flow_up: 0 Flow_down: 0 [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | Port: Gi | 1/4 | |
| Flow_up:0Flow_down:0[usr_syslog_show_byip]Timestart:1970-1-108:00:00[usr_syslog_show_byip]Utype:3[usr_syslog_show_byip]Status:WBA_USTATE_WAIT_AFF_ACK[usr_syslog_show_byip]Event:WBA_EVENT_AFF_ACK[usr_syslog_show_byip]Ipfix_flow_up:0[usr_syslog_show_byip]Ipfix_flow_up:0[usr_syslog_show_byip]Ipfix_flow_down:0[usr_syslog_show_byip]Costime:0Index:620Time:2017-5-3115:05:44Behavior:OFFLINEMac:cof2.fb8c.ae8fvid:350Port:Gi1/4Timeused:0Flow_up:0[usr_syslog_show_byip]Timestart:2017-5-3114:13:57[usr_syslog_show_byip]Utype:3 | Timeused: Oc | 00:00:00 | |
| Flow_down:0[usr_syslog_show_byip]Timestart:1970-1-1 08:00:00[usr_syslog_show_byip]Utype:3[usr_syslog_show_byip]Evant:WBA_USTATE_WAIT_AFF_ACK[usr_syslog_show_byip]Evant:WBA_EVENT_AFF_ACK[usr_syslog_show_byip]Escape:0[usr_syslog_show_byip]Ipfix_Flow_up:0[usr_syslog_show_byip]Ipfix_Flow_down:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0Index:6262Time:2017-5-31 15:05:44Behavior:OFFLINEMac:cof2.fb&c.ae&fvid:350Port:Gi1/4Timeused:0d 00:51:48Flow_up:0[usr_syslog_show_byip]Timestart:2017-5-31 14:13:57[usr_syslog_show_byip]Utype:3 | Flow_up: 0 | | |
| [usr_syslog_show_byip]Timestart:1970-1-1 08:00:00[usr_syslog_show_byip]Utype:3[usr_syslog_show_byip]Status:WBA_USTATE_WAIT_AFF_ACK[usr_syslog_show_byip]Event:WBA_EVENT_AFF_ACK[usr_syslog_show_byip]Escape:0[usr_syslog_show_byip]Ipfix_Flow_up:0[usr_syslog_show_byip]Ipfix_Flow_down:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]00[usr_syslog_show_byip]0[usr_syslog_show_byip]0[usr_syslog_show_byip]0[usr_syslog_show_byip]0[usr_syslog_show_byip]0[usr_syslog_show_byip]11mestart:[usr_syslog_show_byip]0[usr_syslog_show_byip]0[usr_syslog_show_byip]0[usr_syslog_show_byip]0[usr_syslog_show_byip]0[usr_syslog_show_byip]0[usr_syslog_show_byip]0[usr_syslog_show_byip]0[usr_syslog_show_byip]0[usr_sys | Flow_down: 0 | | |
| [usr_syslog_show_byip]Utype:3[usr_syslog_show_byip]Status:WBA_USTATE_WAIT_AFF_ACK[usr_syslog_show_byip]Event:WBA_EVENT_AFF_ACK[usr_syslog_show_byip]Escape:0[usr_syslog_show_byip]Ipfix_Flow_up:0[usr_syslog_show_byip]Ipfix_Flow_down:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Timestart:2017-5-31 14:13:57[usr_syslog_show_byip]Timestart:2017-5-31 14:13:57[usr_syslog_show_byip]Utype:3 | [usr_syslog_show_byip |] Timestart: | 1970-1-1 08:00:00 |
| [usr_syslog_show_byip]Status:WBA_USTATE_WAIT_AFF_ACK[usr_syslog_show_byip]Event:WBA_EVENT_AFF_ACK[usr_syslog_show_byip]Ipfix_Flow_up:0[usr_syslog_show_byip]Ipfix_Flow_down:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costine:0[usr_syslog_show_byip]0Costine:[usr_syslog_show_byip]Timestart:2017-5-31[usr_syslog_show_byip]Utype:3 | [usr_syslog_show_byip |] Utype: | 3 |
| [usr_syslog_show_byip]Event:WBA_EVENT_AFF_ACK[usr_syslog_show_byip]Escape:0[usr_syslog_show_byip]Ipfix_Flow_up:0[usr_syslog_show_byip]Costime:0[usr_syslog_show_byip]Costime:0Index:62Time:2017-5-31 15:05:44Behavior:OFFLINEMac:cof2.fb8c.ae8fvid:350Port:Gil/4Timeused:0d 00:51:48Flow_up:0Flow_up:0Flow_down:0[usr_syslog_show_byip]Timestart:2017-5-31 14:13:57[usr_syslog_show_byip]Utype:3 | [usr_syslog_show_byip |] Status: | WBA_USTATE_WAIT_AFF_ACK |
| <pre>[usr_syslog_show_byip] Escape: 0 [usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Ipfix_Flow_down: 0 [usr_syslog_show_byip] Costime: 0 Index: 62 Time: 2017-5-31 15:05:44 Behavior: 0FFLINE Mac: c0f2.fb8c.ae8f Vid: 350 Port: Gil/4 Timeused: 0d 00:51:48 Flow_up: 0 Flow_down: 0 [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3</pre> | [usr_syslog_show_byip |] Event: | WBA_EVENT_AFF_ACK |
| <pre>[usr_syslog_show_byip] Ipfix_Flow_up: 0 [usr_syslog_show_byip] Ipfix_Flow_down: 0 [usr_syslog_show_byip] Costime: 0 Index: 62 Time: 2017-5-31 15:05:44 Behavior: 0FFLINE Mac: c0f2.fb8c.ae8f Vid: 350 Port: Gil/4 Timeused: 0d 00:51:48 Flow_up: 0 Flow_down: 0 [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3</pre> | [usr_syslog_show_byip |] Escape: | 0 |
| <pre>[usr_syslog_show_byip] Ipfix_Flow_down: 0 [usr_syslog_show_byip] Costime: 0 Index: 62 Time: 2017-5-31 15:05:44 Behavior: 0FFLINE Mac: c0f2.fb8c.ae8f Vid: 350 Port: Gi1/4 Timeused: 0d 00:51:48 Flow_up: 0 Flow_down: 0 [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3</pre> | [usr_syslog_show_byip |] Ipfix_Flow_up: | 0 |
| <pre>[usr_syslog_show_byip] Costime: 0 Index: 62 Time: 2017-5-31 15:05:44 Behavior: OFFLINE Mac: c0f2.fb8c.ae8f Vid: 350 Port: Gi1/4 Timeused: 0d 00:51:48 Flow_up: 0 Flow_down: 0 [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3</pre> | [usr_syslog_show_byip |] Ipfix_Flow_down: | 0 |
| Index: 62 Time: 2017-5-31 15:05:44 Behavior: OFFLINE Mac: c0f2.fb8c.ae8f Vid: 350 Port: Gil/4 Timeused: Od 00:51:48 Flow_up: O Flow_down: O [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | [usr_syslog_show_byip |] Costime: | 0 |
| Time: 2017-5-31 15:05:44 Behavior: OFFLINE Mac: c0f2.fb8c.ae8f vid: 350 Port: Gi1/4 Timeused: 0d 00:51:48 Flow_up: 0 Flow_down: 0 [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | Todex: 67 | | |
| Behavior: OFFLINE Mac: c0f2.fb8c.ae8f vid: 350 Port: Gi1/4 Timeused: 0d 00:51:48 Flow_up: 0 Flow_down: 0 [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | Time: 20 | 17-5-31 15:05:44 | |
| Mac: c0f2.fb8c.ae8f vid: 350 Port: Gi1/4 Timeused: 0d 00:51:48 Flow_up: 0 Flow_down: 0 [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | Behavior: 00 | | |
| vid: 350 Port: Gil/4 Timeused: Od 00:51:48 Flow_up: O Flow_down: O [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | Mac: c(| f2_fb8c_ae8f | |
| Port: Gil/4 Timeused: Od 00:51:48 Flow_up: O Flow_down: O [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | vid: 39 | 0 | |
| Timeused: Od 00:51:48 Flow_up: O Flow_down: O [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | Port: Gi | 1/4 | |
| Flow_up: 0 Flow_down: 0 [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | Timeused: 00 | 00.51.48 | |
| Flow_down: 0 [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | Flow up: 0 | 00152140 | |
| [usr_syslog_show_byip] Timestart: 2017-5-31 14:13:57 [usr_syslog_show_byip] Utype: 3 | Flow down: 0 | | |
| [usr_syslog_show_byip] Utype: 3 | fusr syslog show byin |] Timestart: | 2017-5-31 14:13:57 |
| | [usr_syslog_show_byin | 1 Utype: | 3 |
| [usr_syslog_show_byip] Status: WBA_USTATE_ONLINE | [usr_syslog_show_bvin | j Status: | WBA_USTATE_ONLINE |
| [usr_sýslog_show_býip] event: WBA_EVENT_DHCP_UNBINDING_USER | [usr_syslog_show_byin | j Event: | WBA_EVENT_DHCP_UNBINDING_USER |
| lusr_sýslog_show_býtpl Escape: 0 | [usr_syslog_show_byin | Escape: | 0 |
| ľusr sýslog show býjpi ipfix Flow up: 0 | [usr_syslog_show_byin |] Ipfix_Flow_up: | 0 |
| [usr_sýslog_show_býip] Ipfix_Flow_down: 0 | [usr_sýslog_show_býin |] Ipfix_Flow_down: | 0 |
| [usr_sýslog_show_býip] Costime: 3108 | [usr_sýslog_show_býin |] Costime: | 3108 |
| [usr_sýslog_show_býip] acct_upd_cnt: 3 | [usr_sýslog_show_býin |] acct_upd_cnt: | 3 |
| [usr_sýslog_show_byip] time_last_upd: 2017-5-31 14:58:56 | [usr_syslog_show_byin |] time_last_upd: | 2017-5-31 14:58:56 |
| [usr_syslog_show_byip] | [usr_sýslog_show_býin |] time acct stop: | 1970-1-1 08:00:00 |
| [usr_sýslog_show_býip] cause: Administrator reset the port or session | [usr_sýslog_show_býip |] cause: | Administrator reset the port or session |

Note: As shown in the figure, the prompt displayed on the RG-N18000 shows that the user is forced to go offline.

If the device prompts that the go-offline cause is code4 (idle value timeout), as shown in the figure below, it indicates that the code value in the accounting stop packet of the RG-N18000 is 4, representing that the RG-N18000 forces the user to go offline because no user traffic is detected.

| Index: 2 | 0 | |
|----------------------|--------------------------------|----------------------------|
| Time: 2 | 017-5-9 19:42:02 | |
| Behavior: 0 | NLINE | |
| Mac: c | 0f2.fb8c.ae8f | |
| vid: 1 | 00 | |
| Port: G | i1/3 | |
| Timeused: 0 | d 00:00:00 | |
| Flow_up: 0 | | |
| Flow_down: 0 | | |
| [usr_syslog_show_byi | p] Timestart: | 1970-1-1 00:00:00 |
| [usr_sýslog_show_býi | p] Utype: | 3 |
| [usr_sýslog_show_býi | p] Status: | WBA_USTATE_WAIT_AFF_ACK |
| [usr_syslog_show_byi | p] Event: | WBA_EVENT_AFF_ACK |
| [usr_syslog_show_byi | p] Escape: | 0 |
| [usr_syslog_show_byi | p] Ipfix_Flow_up: | 0 |
| [usr_syslog_show_byi | <pre>p] Ipfix_Flow_down:</pre> | 0 |
| [usr_sýslog_show_býi | p] Costime: | 0 |
| | | |
| Index: 2 | 1 | |
| Time: 2 | 017-5-9 20:07:11 | |
| Behavior: 0 | FFLINE | |
| Mac: c | 0†2.†b8c.ae8† | |
| Vid: 1 | 00 | |
| Port: G | 11/3 | |
| Timeused: 0 | d 00:25:09 | |
| Flow_up: 0 | | |
| Flow_down: 0 | | |
| [usr_syslog_show_byi | p] Timestart: | 2017-5-9 19:42:02 |
| [usr_syslog_show_byi | pj Utype: | 3 |
| [usr_syslog_show_byi | p] Status: | WBA_USTATE_ONLINE |
| [usr_syslog_show_byi | pj Event: | WBA_EVENT_LOW_FLOW_OFFLINE |
| [usr_syslog_show_byi | p] Escape: | 0 |
| [usr_syslog_show_byi | p] Iprix_Flow_up: | 0 |
| [usr_syslog_show_byi | pj Iptix_Flow_down: | 0 |
| [usr_syslog_show_byi | pj Costime: | 1509 |
| [usr_syslog_show_byi | p] acct_upd_cnt: | 1 |
| [usr_syslog_show_byi | pj_time_last_upd: | 2017-5-9 19:57:02 |
| [usr_syslog_show_byi | pl time acct stop: | 2017-5-9 19:40:58 |
| [usr_syslog_show_by1 | pj cause: | Low Tlow detected |

Check the go-offline time and the RG-N18000 configuration based on relevant prompts.

offline-detect interval 15 threshold 0 //If no traffic from a user is detected within 15 minutes, the user is brought offline. The RG-N18000 performs judgment by checking whether there is user traffic matching entries in the MAC address table. offline-detect interval 15 threshold 0 vlan 1000-1500 //Optional. Enable the no-traffic go-offline function for VLANs 1000 to 1500.

If the user is brought offline before the go-offline detection interval set on the RG-N18000 expires, the no-traffic go-offline function is initiated by another device. In this case, check the traffic detection function on other associated devices.

For example, the configurations on the RSR77 are as follows:

| sam-acct user keepalive-detect enable | //Enable the keepalive detection function (enabled |
|--|---|
| by default). | |
| sam-acct user keepalive-detect 900 | //Force a user to go offline if no traffic from the |
| user is detected within 900 seconds (900 | seconds by default). |

3. If the server prompts that the user is brought offline due to preemption, check the system settings and attributes of accounts, whether the MAC address uniqueness limit is configured, and whether the number of clients is limited.

| Shortcut Channel | Homepage System Security User Access Control Billing Account Operation |
|------------------------------------|--|
| Location: System > System Settings | |
| Notification | Registered MAC |
| Subcription Reminder | Authentications (1~10) |
| Self-Service Plan Change | MAC Exclusive Safeguard Not Enable |
| External Link | IP(V4) Exclusive Safeguard Not Enable Preemption mode Exclusive Safeguard Not Enable Preemption mode |
| Conflict & Grab | Username Preemption Mode 🕢 When the user has reached the maximum user mit, the first online user will be forced offline so that the newly authenticated user can access the Internet |
| Email Server | Device Priority 🔲 Enable |
| Others | Preemption mode: For same IP, the online user will be forced offline so the user login later can access the Internet. It is usually used in DHCP environment |
| | Non-preemption mode: For same IP, the online user will be forced offline. It is usually used in a fixed IP distribution environment |
| | Save Reset |
| | |
| | |
| | |

4. Check whether the accounting update configuration on the RG-N18000 is consistent with that on SAM+.

| Shortcut Channel | mepage System Security User Access Control Billing |
|--------------------------------|--|
| ,, | |
| accounting default //Enable | the accounting update function. |
| authentication default | |
| url http://172.18.157.33/eport | l/index.jsp |
| ip 172.18.157.33 | |
| web-auth template eportalv2 | |
| actual service deployment prev | ils. |
| aaa accounting network default | start-stop group radius //AAA reference configuration. The |
| aaa accounting update periodic | 5 //Set the interval for AAA accounting update to 15 min. |
| aaa accounting update | //Configure AAA accounting update. |

| harging Configuration | | | | | |
|------------------------------------|-------------------|----------------|------------------|-----------------|------------------|
| Accounting Port* | 1813 | | | | |
| Accounting Update Options | 🕑 Enable Accounti | ng Update Pacl | ket Processing(C | vertime=Account | ting Update Inte |
| Accounting Update Interval (Mins)* | 15 | | | | |
| Maximum Waiting Times (1~9) * | 3 | | | | |

5. If the server prompts that the user is brought offline due to migration (VLAN migration, port migration, or VLAN & port migration), check the user go-offline cause on the device. If the device also prompts that the user is brought offline due to migration, as shown in the figure below, check the MAC address of the user.

```
YCXY-LC-N18010#show web syslog ip 10.102.92.163
Address: 10.102.92.163 Core-index 3 Current index 10592
Index:
                 11172
 Time:
                 2017-3-28 20:19:31
                ONLINE
Behavior:
Mac:
                 40c6.2a6f.288b
Vid:
                1204
                 Te2/4
Port:
                Od 00:00:00
Timeused:
 Flow up:
                 0
Flow down:
                 0
[usr_syslog_show_byip] Timestart: 1970-1-1 08:00:00
[usr syslog show byip] Utype:
                                       3
[usr syslog show byip] Status:
                                      WBA USTATE ESCAPE PENDING
[uar_syslog_show_byip] Event:
                                      WBA EVENT NEW SOCK
[usr syslog show byip] Escape:
                                       2
[usr_syslog_show_byip] Ipfix_Flow_up:
                                       0
[usr_syslog_show_byip] Ipfix_Flow_down: 0
                                       0
[usr_syslog show byip] Costime:
Index:
                 11271
                 2017-3-28 20:24:13
Time:
Behavior:
               STATION-MOVE
Mac:
                 40c6.2a6f.288b
Vid:
                 2400
Port:
                Ag20
                Od 00:00:00
Timeused:
Flow up:
                0
                 0
Flow down:
[uar syslog show byip] Timestart:
                                      2017-3-28 20:19:31
[usr_syslog_show_byip] Utype:
                                        3
[usr syslog show byip] Status:
                                       WEA USTATE ONLINE
[usr syslog show byip] Event:
                                     WBA EVENT STATION MOVE OFFLINE
[uar syslog show byip] Escape:
                                        2
[usr_syslog_show_byip] Ipfix Flow up:
                                       0
[usr syslog show byip] Ipfix Flow down: 0
[usr syslog show byip] Costime:
                                       282
```

Run the **show mac-address-table address** *** and **show arp** *** commands on the device to check whether the VID or port associated with the MAC address changes. If yes, proceed to the following step.

Based on the new VID or port, locate the earliest device that learns the MAC address and pinpoint the cause for MAC address drift.

A loop or IP address spoofing occurs on the downlink device.

7.3.4 Fault Information Collection

Run the following commands to collect information on the RG-N18000:

```
terminal length 0
show ver detail
show run
show mac-address-table | include ***(MAC address of the user)
```
```
show arp | include ****(MAC address of the user)
show ip dhcp snooping
show ip dhcp snooping binding | in ****(user MAC address)
debug scc stat
debug web cli
sh web user ip ***(ip)
sh web syslog ip ***(ip) ---
show web-auth authmng abnormal
debug scc pgsql st --- Display relevant statistics of the database.
undebug all
show log
terminal no length
```

7.3.5 Fault Summary and Notes

7.4 802.1x Authentication Failure

7.4.1 Symptom

802.1x authentication fails or 802.1x authenticated users are dropped out of the network.

7.4.2 Possible Causes

- 1. The configurations for interconnection between the RG-N18000 and SAM+ server are incorrect. As a result, the RG-N18000 fails to send packets to the SAM+ server, or the SAM+ server fails to process received packets.
- 2. The channel between the RG-N18000 and SAM+ server is abnormal, and RADIUS packets cannot be sent to the SAM+ server.
- 3. The channel between the client and the RG-N18000 is abnormal, and EAP packets cannot be sent to the RG-N18000.
- 4. The configurations are incorrect on the RG-N18000, and the RG-N18000 fails to process or respond to packets.
- 5. Users fail to obtain correct IP addresses.
- Software failures occur on the RG-N18000 or SAM+ server, and authentication packets cannot be properly sent or processed.
- 7. VLAN ports are migrated, and a prompt about active user go-offline is displayed even if the user does not go offline actively (11.0(1)B3P2 and earlier versions).

7.4.3 Handling Steps

1. On the client and SAM+, access **Operation** > **Log**, collect relevant authentication failure prompts, and make basic judgment based on the prompts.

2. If the system is stuck in the connection to the authentication server or a prompt about an authentication server connection failure is displayed during client authentication, check whether 802.1x authentication configurations on the RG-N18000 and SAM+ are correct. If a prompt is provided on SAM+, follow the prompt to complete the configuration. If no prompt is provided on SAM+, check whether the RADIUS server is configured correctly.

```
aaa new-model
radius-server host 192.168.32.120 key 7 ruijie
ip radius source-interface gigabitEthernet 1/24
aaa accounting network default start-stop group radius
aaa authentication dot1x default group radius
aaa accounting update periodic15
aaa accounting update
dot1x accounting default
dot1x authentication default
aaa authorization ip-auth-mode mixed
no aaa log enable
interface FastEthernet 0/1
  dot1x port-control auto
expert access-list extended 2700
 10 permit arp any any
 20 permit udp any any any any eq bootpc
 30 permit udp any any any any eq bootps
security global access-group 2700
```

| s | hortcut Channel 🔅 | Homepage | System | Security | User | Access Control | Billing | Account | Operation | | |
|---|--|---------------|------------|---------------|---------------|---------------------|---------|----------------|---------------------|-----------|--|
| | Location: System > Device Management > Add | | | | | | | | | | |
| | Device | | | | | | | | | | |
| | Device IP Address* | 172.18.157.1 | | | | | | IP Type* | | IPv4 • | |
| | Device Type* | Ruijie Switch | | | | | | Model* | | N18K • | |
| | PPPoE Authentication Domain | | Please use | comma or s | bace to sep | parate multiple dom | ains | IPOE+Web Au | thentication Domain | | Please use comma or space to separate multiple domains |
| | Device Key* | ruijie | | | | | | Community* | | ruijie |] |
| | MAC Aridrecc* | | For truste | d ARP binding | g application | on, MAC address mu | ist be | SNMP Provy P | lort | | If you do not fill in the default nort 161 will be adopted |
| | infection cos | filled | | | | | | Stan Proxy P | U.L. | | In you do not in my the demain port for this be deduced |
| | DHCP Login Username | | | | | | | DHCP Login P | assword | | |
| | Telnet Login Username | | | | | | | Telnet Login P | assword | | |
| | Telnet Privileged Password | | | | | | | Device Group | • | default 🔻 | |

3. Check whether the connectivity between the IP address of the source interface of the RG-N18000 and SAM+ is normal.

4. If the authentication is stuck in the phase of authentication server searching or a prompt is displayed, indicating that searching for an authentication server fails, check whether the link between the client and the RG-N18000 is normal and whether the 802.1x authentication function is configured on a downlink port connected to the RG-N18000.

Check whether EAP packets are filtered out because 802.1x authentication is enabled on the access-layer S21 series switch, or whether EAP packets are not forwarded because the switch connects to a TP-LINK device.

5. If the fault persists after the steps above are performed, run the following command to collect go-online/offline records, and capture packets on the client and the SAM+ server.

Show dot1x user diag mac xxx

```
VSU-N18K-CORE#show dot1x user diag mac 78e3.b5a5.9cc2
USER-RECORD: 78e3.b5a5.9cc2
Time
            ifx vid authstate
                                   backstate paestate authT
                                                                                       detail
                                                                 ipT
                                                                         event
04.26 08:40:43 133 1511 Disconnected Idle
                                             0x800000 0 ms 0
                                                                      ms create pae
                                                                                       none
04.26 08:40:44 133 1511 Authenticated Idle
                                             0x10a39020 643 ms 0
                                                                      ms pkt start
                                                                                       none
04.26 08:40:44 133 1511 Authenticated Idle
                                             0x10a39021 643 ms 0
                                                                      ms acct start
                                                                                       none
04.26 08:41:01 133 1511 Disconnected Idle
                                             0x13a39021 92 ms 0
                                                                      ms acct stop
                                                                                       none
VSU-N18K-CORE#
```

As shown in the figure above: create pae: Indicates that a user is created. pkt start: Indicates authentication initiated by the start packet from the client. acct start: Indicates that the authentication is successful and accounting starts. acct stop: Indicates that the user goes offline and the accounting stop packet is sent. Show dotlx authmng statistics Show dotlx authmng mab statistics sh ip dhcp snooping binding

6. Check whether an IP address can be obtained normally.

expert access-list extended 2700

```
10 permit arp any any
20 permit udp any any any any eq bootpc
30 permit udp any any any any eq bootps
security global access-group 2700
```

After verifying that the configuration above is normal, if an IP address still fails to be obtained, check possible causes and rectify the fault by following the handling procedure of a DHCP fault.

7. If the authentication still fails after the configuration above is adopted, collect information on the RG-N18000, enable packet capture on both the client and SAM+, and send the information and captured packets to the TAC for handling.

7.4.4 Fault Information Collection

```
Run the following commands to collect information on the RG-N18000:
terminal length 0
show ver detail
show run
show mac-address-table | include ***(MAC address of the user)
show arp | include ****(MAC address of the user)
show ip dhcp snooping
show ip dhcp snooping binding | in ****(user MAC address)
show dotlx user diag mac xxx
show dotlx authmng abnormal | in xxx
```

```
show dot1x authmng mab statistic
show dot1x user mac xxx
show dot1x
deb dot1x dump gl
show log
terminal no length
```

The directory for storing logs to be collected on SAM+ is as follows:

| 📙 log | | | |
|----------------|--------------------|-----------------|----------|
| € . . . | ▼ RG-ePortal ▼ log | ▼ ₩ | 2 |
| 组织 ▼ 包含到库中 ▼ | 共享 🔻 新建文件夹 | | i= 🕶 🔟 🔞 |
| | | | |
| | 10g_2014-05-15.4 | 2014/5/15 10:38 | 1,144 KB |
| | log_2014-05-15.3 | 2014/5/15 8:52 | 2,083 KB |
| | log_2014-05-15.2 | 2014/5/15 5:55 | 2,083 KB |
| | log_2014-05-15.1 | 2014/5/15 2:57 | 2,083 KB |
| | log_2014-05-14.8 | 2014/5/15 0:00 | 1,151 KB |
| | 10g_2014-05-14.7 | 2014/5/14 22:21 | 2,083 KB |

7.4.5 Fault Summary and Notes

7.5 Network Dropout During 802.1x Authentication

7.5.1 Symptom

Network Dropout During 802.1x Authentication

7.5.2 Possible Causes

- 1. Users generate no traffic within a period of time.
- 2. The client version is not compatible with the SAM+ server version.
- 3. VLAN ports are migrated, and a prompt about active user go-offline is displayed even if the user does not go offline actively (11.0(1)B3P2 and earlier versions).

7.5.3 Handling Steps

1. Go to the SAM+ system and access Operation > Online User on the Web management page, locate the user, view the go-offline cause prompt, and find out the possible go-offline causes preliminarily.

| Shortcut Channel | \$ | Homepage | System | Security | User | Access Contr | ol | Billing | Account | Operati | ion | | |
|--|-----------------------|---------------------|---------|----------|----------|--------------|---------|-------------|---------|------------|--------|----------|------------|
| Location: Operation | on > Log Management | | | | | | | | | | | | |
| Log Type | Authentication Log: • | | Operato | or | | | | | 🕑 Gene | ral Search | Search | | |
| Log Time (Start) | 2018-05-09 00:00:00 | | Log Tim | ne (End) | 2018-05- | 09 23:59:59 | 1 | | | | | | |
| Log Content | | (Always fuzzy query | 0 | | | | | | | | | | |
| | | | | | | De | lete th | ne Selected | Delete | e All | | | |
| There were no res | ults found. | | | | | | | | | | | | B (|
| 🔲 Log | J Type Log | g Content | | | | | | | | | | Log Time | |
| The system will opt for fuzzy query no matter the function is selected or not in log content Do you want to set fuzzy query for others besides log content? Tick to enable fuzzy query and leave blank to enable accurate query | | | | | | | | | | | | | |

Note: The user go-offline prompts provided on SAM+ are accurate, but there may be some errors due to complex network environments.

2. If the device prompts that the user go-offline is caused by no traffic detected, as shown in the figure below, it indicates that SAM+ receives the TCP2009 no traffic notification from the traffic audit device (such as the RSR77 or ACE).

If the device prompts that the go-offline cause is code4 (idle value timeout), as shown in the figure below, it indicates that the code value in the accounting stop packet of the RG-N18000 is 4, representing that the RG-N18000 forces the user to go offline because no user traffic is detected.

Check the go-offline time and the RG-N18000 configuration based on relevant prompts.

offline-detect interval 15 threshold 0 //If no traffic from a user is detected within 15 minutes, the user is brought offline. The RG-N18000 performs judgment by checking whether there is user traffic matching entries in the MAC address table. offline-detect interval 15 threshold 0 vlan 1000-1500 //Optional. Enable the no-traffic go-offline function for VLANs 1000 to 1500.

If the user is brought offline before the go-offline detection interval set on the RG-N18000 expires, the no-traffic go-offline function is initiated by another device. In this case, check the traffic detection function on other associated devices.

For example, the configurations on the RSR77 are as follows:

```
sam-acct user keepalive-detect enable //Enable the keepalive detection function (enabled
by default).
sam-acct user keepalive-detect 900 //Force a user to go offline if no traffic from the
user is detected within 900 seconds (900 seconds by default).
```

3. The RG-N18000 sends the EAP failure packet to the client during user VLAN or port migration. After receiving the packet, the client actively initiates a go-offline request.

Run the **show dot1x authmng abnormal** command to display the user go-offline cause. If it is determined that the fault is caused by port or VLAN migration, run the **show mac-address-table** and **show arp** commands to display the migration information and find out the cause for migration (loop or other causes) to rectify the fault.

| 118K#show dot1x authmng abnorm | al AuthTime | AaaTout | RegtdTout | RegTout | RsnaNtfv | StrNtfy | Type | Peason | Pssi | liser |
|--------------------------------|----------------|----------|-----------|---------|----------|----------|--------------|--------------------|-------|-----------|
| | Auchine | Additout | Requirouc | ReqTout | KSHarry | Scrivery | | Reason | K331 | 0361 |
| .10 17:29:36 9048.9a8e.a033 | 9317 | | 1 | | | | D1X_AUTH | user logoff | 0 dBm | ruijie001 |
| 5 .10 17:31:55 9048.9a8e.a033 | 6858 | | 1 | | | | D1X_AUTH | auth success | 0 dBm | ruijie001 |
| 5 .10 17:32:13 9048.9a8e.a033 | 2531 | | 1 | | | | D1X_AUTH | auth success | 0 dBm | ruijie001 |
| 5 .10 17:33:6 9048.9a8e.a033 | | | | | | | D1X_AUTH | request id timeout | 0 dBm | |
| 5 .10 17:39:7 9048.9a8e.a033 | | | | | | | D1X_AUTH | request id timeout | 0 dBm | |
| 5 .10 17:39:9 9048.9a8e.a033 | 1213 | | | | | | D1X_AUTH | auth success | 0 dBm | ruijie001 |
| 5 .10 17:39:12 9048.9a8e.a033 | 2870 | | 1 | | | | D1X_REAUTH | auth success | 0 dBm | ruijie001 |
| 5 .10 17:41:6 9048.9a8e.a033 | 2603 | | 1 | 1 | | | D1X_REAUTH | auth success | 0 dBm | ruijie001 |
| 5 .10 17:42:0 9048.9a8e.a033 | 2886 | | 1 | | | | D1X_AUTH | auth success | 0 dBm | ruijie001 |
| 5 .10 17:42:20 9048.9a8e.a033 | 2498 | | 1 | | | | D1X_AUTH | auth success | 0 dBm | ruijie001 |
| 5.10 17:42:32 9048.9a8e.a033 | 0 | 0 | 1 | 1 | 0 | 0 | D1X OFFLITNE | svr kickout user | 0 dBm | ruiiie001 |
| 5 .10 9 :58:45 9048.9a8e.a033 | 2837 | 0 | 1 | 1 | 0 | 0 | D1X_AUTH | auth success | 0 dBm | ruijie001 |
| 5.10 9 :58:51 9048.9a8e.a033 | 5677 | | | | | | D1X_REAUTH | auth success | 0 dBm | ruijie001 |
| 5.10 10:4 :55 9048.9a8e.a033 | 5752 | | | | | | D1X_AUTH | auth success | 0 dBm | ruijie001 |
| .10_10:6 :53 9048.9a8e.a033 | 0 | 0 | 2 | 1 | 0 | 0 | D1X_OFFLINE | svr kickout user | 0 dBm | ruijie001 |

Common causes:

"user logoff" : \--->>The client logs out. "server kickout user" : \--->>The server kicks the user off the network. "no flow" : \--->>No traffic is detected. "port move" : \--->>Port migration occurs. "vlan move" : \--->>VLAN migration occurs. "port-vlan move" : \--->>Both port migration and VLAN migration occur. "invalid ip" : \--->>No valid IP address is available.

7.5.4 Fault Information Collection

Run the following commands to collect information on the RG-N18000:

```
terminal length 0
show ver detail
show run
show mac-address-table | include *** (MAC address of the user)
show arp | include ****(MAC address of the user)
show ip dhcp snooping
show ip dhcp snooping binding | in ****(user MAC address)
show dot1x user diag mac xxx
show dot1x authmng abnormal | in xxx
show dot1x authmng statistic
show dot1x authmng mab statistic
show dot1x user mac xxx
show dot1x
deb dot1x dump gl
show log
terminal no length
```

The directory for storing logs to be collected on SAM+ is as follows:

| 📕 log | | | |
|--------------|--------------------|-----------------|----------|
| ○ ■ < | ▼ RG-ePortal ▼ log | ▼ 🙀 | |
| 组织 ▼ 包含到库中 ▼ | 共享 👻 新建文件夹 | | := 🕶 🚺 🔞 |
| | | | |
| | 1 vg_2014-05-15.4 | 2014/5/15 10:38 | 1,144 KB |
| | 📄 log_2014-05-15.3 | 2014/5/15 8:52 | 2,083 KB |
| | 📄 log_2014-05-15.2 | 2014/5/15 5:55 | 2,083 KB |
| | 📄 log_2014-05-15.1 | 2014/5/15 2:57 | 2,083 KB |
| | 10g_2014-05-14.8 | 2014/5/15 0:00 | 1,151 KB |
| | □ 1₀g_2014-05-14.7 | 2014/5/14 22:21 | 2,083 KB |

7.5.5 Fault Summary and Notes

7.6 MAB Authentication Failure

7.6.1 Symptom

MAB perception-free authentication fails.

7.6.2 Possible Causes

- 1. MAB perception-free authentication is not enabled on the SAM+ server, and the SAM+ server fails to learn MAC addresses of clients.
- 2. The RG-N18000 is incorrectly configured, and fails to initiate MAB perception-free authentication.
- 3. Users fail to obtain correct IP addresses, not meeting the mechanism of **dot1x mac-auth-bypass valid-ip-auth**.
- 4. The device fails to learn the corresponding MAC address, and does not initiate MAB authentication.
- 5. Software failures occur on the RG-N18000 or SAM+ server, and MAB perception-free authentication is not initiated or processed properly.

7.6.3 Handling Steps

 On the client and SAM+, access Operation > Log, collect relevant authentication failure prompts, and make basic judgment based on the prompts. As shown in the figure below, the RG-N18000 initiates MAB authentication but there is no MAB authentication entry on the SAM+ server. As a result, the MAB authentication fails.

| Shortcut Channel 🔯 | Homepage | System Security | User Access Control | Billing Account | Operation | |
|-------------------------------------|---------------------------|----------------------------|----------------------------------|-------------------------|--------------|--|
| Location: Operation > Log Mana | gement | | | | | |
| Log Type Authenticatio | n Log: 🔻 | Operator | | 🗹 General S | earch Search | |
| Log Time (Start) 2018-05-09 0 | 0:00:00 📰 🚍 | Log Time (End) | 2018-05-09 23:59:59 📷 🗖 | 3 | | |
| Log Content | (Always fuzzy que | ery) | | | | |
| | | | Daleta | the Selected Delete All | | |
| | | | Delete | | | |
| There were no results found. | | | | | | |
| Log Type | Log Content | | | | Log Time | |
| The system will opt for fuzzy query | no matter the function is | selected or not in log con | tent | | | |
| Do you want to set fuzzy query for | others besides log conten | t? Tick to enable fuzzy qu | ery and leave blank to enable ac | curate query | | |

As shown in the figure below, access **User** > **MAC** Authentication and check whether binding entries of the username corresponding to the MAC address exist.

| SAM ⁺ security accounting ma | ANAGEMENT SYSTEM | | | | |
|---|------------------|-------------------------|------------------------|-------------------|----------|
| Shortcut Channel 🔅 | Homepage System | Security User | Access Control Billing | Account Operation | |
| Location: User > MAC Authentication | | | | | |
| Username |] | User MAC | | 🗷 General Search | Search |
| Registraion Time F rom | | Registraion Time T o | m | | |
| Expired From | | Expired To | | | |
| | | | Add Delete the Selec | cted Delete All | |
| There were no results found. | | | | | 🗐 Curren |
| Register User | Register MA | c | MAC Binding Expiry | Register | F |
| | | | | | |
| | | | | | |
| | | | | | |
| | | | | | |

Check whether MAC fast authentication is checked for access control.

| Shortcut Channel 🔅 | Homepage System | n Security Use | Access Control | Billing Account | Operation |
|---|----------------------|---------------------|-----------------------|-----------------------|--|
| Location: Access Control > Access Control > | Modify | | | | |
| Access Control Information User Inform | ation Check Network | Usage Control Publi | c Service User Behavi | ior Control VPN Contr | ol Client Version Management Wireless Acce |
| Allowed Access | Access Mode Verifica | tion Information | | | |
| Wired 1X Access | User IP(v4) | User IP(v6) | User MAC | NAS IP(v4) | NAS IP(v6) NAS Port |
| | VLAN | Internal VLAN | External VLAN | Access IP Type Stat | ic 🔻 |
| Wired Web Portal Access | User IP(v4) | User MAC | Web Authentication | Device IP(v4) | Web Authentication Device Port |
| Miralass 1V Assess | User IP(v4) | User MAC | NAS IP(v4) | AP MAC | SSID |
| Wileless TA Access | Access IP Type Sta | ntic 🔻 | | | |
| ✓ Wireless Web Portal Access | User MAC | NAS IP(v4) | AP MAC | SSID | |
| Smart Device 1X Access | User MAC | NAS IP(v4) | AP MAC | SSID | |
| | User MAC | NAS IP(v4) | AP MAC | SSID | NAS Port |
| MIAC Fast Access | VLAN | Internal VLAN | External VLAN | | |
| Mired Standard Destal Access | User IP(v4) | User MAC | NAS IP(v4) | NAS Port | VLAN |
| Wired Standard Portal Access | Internal VLAN | External VLAN | | | |
| Wireless Standard Portal Access | User IP(v4) | User MAC | NAS IP(v4) | AP MAC | SSID |
| wireless standard Portal Access | NAS Port | VLAN | Internal VLAN | External VLAN | |
| ✓VPN Dial-up access | User IP(v4) | NAS IP(v4) | | | |
| Web Pure Internet Access | User IP(v4) | | | | |
| PPPoE Access | User MAC | NAS IP(v4) | Internal VLAN | External VLAN | Authentication Domain |

2. If SAM+ has no authentication failure entry of the MAC address, MAB authentication interaction exceptions may be caused by improper configuration on the RG-N18000.

aaa new-model //Enable the AAA function.

aaa accounting network default start-stop group radius //AAA reference configuration. The actual service deployment prevails. aaa authentication dot1x default group radius //Reference configuration for AAA 802.1x authentication template. The actual service deployment prevails. aaa authentication web-auth default group radius //Reference configuration for AAA Web authentication template. The actual service deployment prevails. aaa authentication login default local //Use the local username/password for login to the AAA device. radius-server host 172.18.157.32 key ruijie //Configure the IP address and key for the AAA server, which are applicable to the scenarios with a single RADIUS server. aaa accounting update periodic 15 //Set the internal for AAA accounting update to 15 min. //Configure AAA accounting update. aaa accounting update no aaa log enable //Disable the AAA log function. dot1x accounting default //Optional. This command is required when the accounting list name for AAA is not set to **default**. dot1x authentication default //Optional. This command is required when the 802.1x authentication list name for AAA is not set to default. web-auth template eportalv2 ip 172.18.157.33 //IP address of the ePortal server url http://172.18.157.33/eportal/index.jsp //URL of the ePortal server. authentication default //Optional. This command is required when the authentication list name for AAA is not set to **default**. accounting default //Optional. This command is required when the accounting list name for AAA is not set to **default**. web-auth portal key ruijie //Mandatory. Configure the key for encrypting the URL for interconnection with ePortal. aaa authorization ip-auth-mode mixed //Mandatory. Set the IP address authorization mode of 802.1x clients to the mixed mode. The IP addresses can be obtained via polling in multiple ways (DHCP/RADIUS). ip dhcp snooping //Mandatory. An IP address needs to be obtained via the DHCP snooping module for MAB authentication. Otherwise, a user with the IP address of 0.0.0.0 appears on SAM+. dot1x mac-auth-bypass valid-ip-auth //The DHCP module instructs the MAB module to start authentication. The configuration of this command will drop users out of the network. It is not recommended to run this command in service peak hours. //Mandatory. The accounting update packets are used to dot1x valid-ip-acct enable upload the user IP address to SAM+. If the 802.1x authentication module does not have an IP entry of the user, the user is kicked offline 5 minutes later. interface range GigabitEthernet 0/2-3 //Enable 802.1x authentication on the interface. web-auth enable eportalv2 //Enable Web authentication on the interface. dot1x port-control auto //Enable 802.1x authentication on the interface.

```
dot1x mac-auth-bypass multi-user //Mandatory. Enable MAB authentication
on the interface.
    dot1x mac-auth-bypass vlan (vlan-list) //Optional. Configure this command in
interface configuration mode to enable VLAN-based MAB authentication.
```

3. After the **dot1x mac-auth-bypass valid-ip-auth** command is configured, dynamic users must obtain IP addresses and relevant entries exist in the DHCP snooping binding table before MAB authentication can be initiated for them.

Run the **show ip dhcp snooping binding** or **show ip dhcp snooping binding | include 192.168.1.1** command to check whether relevant entries are displayed.

If no, check whether the IP address is proper and whether the DHCP process is normal.

If the user IP address is static and there is no DHCP interaction, statically bind entries on the RG-N18000 to trigger MAB authentication. See the following command.

dot1x address-binding mac 9048.9a8e.a033 ip 10.0.100.188

- 4. If the configuration is correct, run the show mac-address-table command to check whether the MAC address is learned successfully. If yes but MAB authentication is not initiated, contact the TAC for handling. If no, enable packet capture to check whether the RG-N18000 receives packets. If yes, contact the TAC for handling.
- 5. If the cause cannot be pinpointed after the operations above are performed, the software of the RG-N18000 may be faulty, which result in the failure to initiate MAB authentication, or the software of SAM+ may be faulty, which result in the failure in processing of MAB authentication. Collect information on the RG-N18000, enable packet capture on both the client and SAM+, and send the information and captured packets to the TAC for handling.

7.6.4 Fault Information Collection

Run the following commands to collect information on the RG-N18000:

```
terminal length 0
show ver detail
show run
show mac-address-table | include ***(MAC address of the user)
show arp | include ****(MAC address of the user)
show ip dhcp snooping
show ip dhcp snooping binding | in **** (MAC address of the user)
show dot1x user diag mac xxx
show dot1x authmng abnormal | in xxx
show dot1x authmng statistic
show dot1x authmng mab statistic
show dot1x user mac xxx
deb web-auth mab user-show
show dot1x
deb dot1x dump gl
show log
```

terminal no length

The directory for storing logs to be collected on SAM+ is as follows:

| 📙 log | | | |
|------------------------|--------------------|-----------------|----------|
| € 0- ⊮ € | + RG-ePortal + log | - 🔯 | |
| 组织 ▼ 包含到库中 ▼ | 共享 🔻 新建文件夹 | | i= 👻 🗍 🔞 |
| | | | _ |
| | 10g_2014-05-15.4 | 2014/5/15 10:38 | 1,144 KB |
| | 📄 log_2014-05-15.3 | 2014/5/15 8:52 | 2,083 KB |
| | 10g_2014-05-15.2 | 2014/5/15 5:55 | 2,083 KB |
| | 10g_2014-05-15.1 | 2014/5/15 2:57 | 2,083 KB |
| | 10g_2014-05-14.8 | 2014/5/15 0:00 | 1,151 KB |
| | 0s_2014-05-14.7 | 2014/5/14 22:21 | 2,083 KB |

7.6.5 Fault Summary and Notes

7.7 Exception/Failure in Dynamic Acquisition of IP Addresses

7.7.1 Symptom

The device fails to dynamically obtain IP addresses or the dynamically obtained IP addresses are abnormal.

7.7.2 Possible Causes

- 1. The DHCP address pool and sub VLANs are not associated with a super VLAN, and AM rules are incomplete, resulting in IP address allocation failures.
- 2. Addresses in the address pool are exhausted, and no IP address can be allocated.
- 3. Only 802.1x authentication is configured on interfaces and no security channel is configured.
- 4. The intermediate channel fails or ACL configurations are incorrect, and DHCP packets cannot reach the RG-N18000.
- 5. DHCP snooping is enabled on the downstream switch and the upstream port is not added to the list of trusted ports, and therefore DHCP response packets are dropped.
- 6. The client is faulty, and DHCP packets cannot be sent or received DHCP packets cannot be processed.
- 7. The DHCP relay is incorrectly configured on the RG-N18000, or the channel between the gateway and DHCP server is abnormal.
- 8. The RG-N18000 serves as a DHCP relay, packets between the RG-N18000 and the server are transmitted at layer 2, and the client is not in the same VLAN as the server. As a result, the RG-N18000 does not send packets to the client according to the DHCP snooping binding table.
 - 9. The DHCP server performance is abnormal, resulting in packet processing or response failures.
- 10. DHCP packets are dropped at the IP layer (founded by displaying the TCP/IP CPU usage).

7.7.3 Handling Steps

1. Check whether the DHCP, super VLAN, gateway interface, and AM rules are correctly configured.

The main DHCP configuration is as follows:

```
ip dhcp pool bangong
lease 0 2 0
network 10.1.32.0 255.255.240.0 //The mask here contains 20 bits.
dns-server 192.168.58.110
default-router 10.1.32.254
```

Note: If the subnet mask of an address in the DHCP address pool contains 20 bits but that of the IP address configured for the gateway interface does not, DHCP needs to be configured based on the network segment to which the subnet mask of the gateway IP address belongs.

The main super VLAN configuration is as follows:

```
vlan 2001
Super VLAN
subvlan 200-399 //Associate the sub VLANs with the super VLAN.
name susheZONE
```

Note: The VLAN of each interface on the client connected to the access switch is a sub VLAN, which needs to be associated with the super VLAN.

The main AM rule configuration is as follows:

| address-man | nage | //Enable the address |
|-------------|---|---|
| management | function. | |
| match | ip 10.1.5.0 255.255.255.0 gi5/3 vlan 1005 | //Configure VLAN+port-based |
| matching mo | ode. | |
| match | ip 192.168.2.0 255.255.255.0 Gi5/3 vlan 100 | 6 |
| match | ip 192.168.3.0 255.255.255.0 Gi5/3 vlan 100 | 7 |
| match | ip loose | //Set the AM rule to |
| loose mode. | . If the loose mode is not configured, client | s that do not match the AM rules cannot |
| obtain IP a | addresses. | |

Note: The matching of AM rules is matching the interface and VLAN configured in the AM rules, for example, the Gi5/3 interface and VLAN 1005 above. If it is confirmed that DHCP packets are from the Gi5/3 interface and VLAN 1005, the DHCP packets match the AM rules. In this case, the IP address obtained by the user must be in the range of 10.1.5.0 to 10.1.5.255 regardless of whether in loose or strict mode. If no AM rule is matched or IP addresses in the range of 10.1.5.0 to 10.1.5.255 are all assigned, no IP address can be obtained regardless of whether in loose mode or strict mode. If no AM rule is matched, it indicates that neither the interface (for example, Gi5/3) nor VLAN (for example, VLAN 1005) is matched. If no AM rule is matched in loose mode, an IP address outside the DHCP address pool is assigned.

2. Run the **show** command to check whether IP addresses in the DHCP address pool are used up.

Collect basic DHCP information and check whether IP addresses in the DHCP address pool are used up.

show ip dhcp pool

| 86-WS# 86-WS# 86-WS#show ip Pool name | dhcp pool Total | Number of assigned addresses Distributed | Number of available addresses Remained | Address pool usage |
|--|--------------------|--|--|--------------------|
| vlan-71 | 65533 | 175 | 65358 | 0.26704 |
| vlan-72 | 65533 | 0 | 65533 | 0.00000 |
| vlan-73 | 65533 | 0 | 65533 | 0.00000 |
| vlan-74 | 65533 | 0 | 65533 | 0.00000 |

Note: If the value in the **Percentage** column is greater than 80%, addresses in the DHCP address pool are to be used up.

show ip dhcp server statistics

| 86-WS#show ip dhcp server | statistics |
|---|--|
| Address pools | 7 |
| Lease counter | 2958 |
| Dynamic address pools | 7 |
| Active Lease Counter | 1625 |
| Expired Lease Counter | 1333 |
| Malformed messages | 0 |
| Dropped messages | 0 |
| Message BOOTREQUEST DHCPDISCOVER DHCPREQUEST DHCPDECLINE DHCPRELEASE DHCPINFORM | Received 385431 203124 182307 0 IP address 0 conflict exists. |
| Message | Sent |
| BOOTREPLY | 203124 |
| DHCPOFFER | 203124 |
| DHCPACK | 0 |
| DHCPNAK | 0 |

Note: Focus on the value of the **DHCPDELINE** field. A larger value indicates more IP address conflicts in the network. This field shows the total number of IP address conflicts since startup. It is recommended to refresh the field every 10 minutes to check whether the value increases greatly. If yes, an IP address conflict occurs.

show ip dhcp snooping binding | in H.H.H

86-W5#show ip dhcp snooping binding

| Total | number of binding | s: 1272 snooping b | binding entries | | | | |
|-------|--------------------|--------------------|---------------------|------------------|-----------|------------|--|
| NO. | MACADDRESS | IPADDRESS | LEASE (SEC) | TYPE | VLAN | INTERFACE | |
| 1 | 520c. 345c. 0529 | 90.70.3.197 | 787667 | DHCP-Snooping | 70 | wlan 1001 | |
| 2 | 520c.123a.0191 | 90.70.0.81 | 786627 | DHCP-Snooping | 70 | Wlan 1000 | |
| 3 | 520c.356a.03df | 90.70.4.225 | 787890 | DHCP-Snooping | 70 | Wlan 1001 | |
| 4 | 520c.123a.037b | 90.70.0.179 | 786628 | DHCP-Snooping | 70 | Wlan 1000 | |
| 5 | 520c.356a.023b | 90.70.4.141 | 787890 | DHCP-Snooping | 70 | Wlan 1001 | |
| 6 | 520c.345c.051f | 90.70.3.195 | 787667 | DHCP-Snooping | 70 | Wlan 1001 | |
| 7 | 520c.345c.06af | 90.70.4.19 | 787676 | DHCP-Snooping | 70 | Wlan 1001 | |
| 8 | 520c.345c.03b7 | 90.70.3.123 | 787668 | DHCP-Snooping | 70 | Wlan 1001 | |
| 9 | 520c.123a.053d | 90.70.1.13 | 786628 | DHCP-Snooping | 70 | Wlan 1000 | |
| 10 | 520c.123a.0385 | 90.70.0.181 | 786628 | DHCP-Snooping | 70 | Wlan 1000 | |
| 11 | 520c.345c.0100 | 90.70.2.240 | 787665 | DHCP-Snooping | 70 | Wlan 1001 | |
| 12 | 520c.134a.028b | 90.70.1.225 | 786893 | DHCP-Snooping | 70 | Wlan 1000 | |
| 13 | 520c.345c.03f8 | 90.70.3.136 | 787667 | DHCP-Snooping | 70 | Wlan 1001 | |
| 14 | 520c.123a.01b9 | 90.70.0.89 | 786626 | DHCP-Snooping | 70 | Wlan 1000 | |
| 15 | 520c.356a.03f8 | 90.70.4.230 | 787890 | DHCP-Snooping | 70 | Wlan 1001 | |
| 16 | 520c.345c.026d | 90.70.3.57 | 787666 | DHCP-Snooping | 70 | Wlan 1001 | |
| 17 | 520c.345c.0146 | 90.70.2.254 | 787665 | DHCP-Snooping | 70 | Wlan 1001 | |
| 18 | 520c.356a.0092 | 90.70.4.56 | 787888 | DHCP-Snooping | 70 | Wlan 1001 | |
| 19 | 520c.134a.00c4 | 90.70.1.134 | 786885 | DHCP-Snooping | 70 | Wlan 1000 | |
| 06 MG | "chow in dhen enoe | ning binding i | - | DHCP snoopin | ng bindir | ng entry | |
| 80-W5 | #show ip dhep shoo | ping binding [1 | 11 n 520c 245c 0 | of a specific l | MAC ad | dress | |
| 1 | 520c 345c 0529 | | 787654 | DHCP_Spooning | 70 | Wlan 1001 | |
| 86-WS | # | 50.70.5.157 | 10/034 | Brief Briddpring | / • | W1001 1001 | |

tal number of DHCP

Note: Pay attention to the value of DHCP snooping binding entries. If DHCP snooping is enabled and the number of entries exceeds the specified limit (256,000), no new DHCP snooping binding entry can be generated. If an entry is displayed, it indicates the MAC address is associated with an IP address.

3. Run the **show ip dhcp server agent mac** *xx.xx.xx* command to display the packet exchange for a client to acquire an IP address.

| HXJF-N18K#show Hardware addres Client status Discover receive Ack sent Decline receive Release receive | ip dhcp server agent m s : 0010.9400.0061 : running ved : 10 2d : 5 : 5 2d : 0 2d : 4 | ac 0010.9400.0061 | |
|--|--|-------------------|--------------------------|
| Offer sent | : 10 | | |
| Events status 0010.9400.0061 | : Discover, Offer syslog index 6: | , Request, Ack | ac. 1010 |
| IP | State | Event | Time |
| 10.20.1.55 | Idle>Checking | Recv_Discover | Mon Jul 10 15:52:19 2017 |
| 10.20.1.55 | Checking>Offer | PING_PASS | Mon Jul 10 15:52:20 2017 |
| 10.20.1.55 | Offer>Bind | Recv_Request | Mon Jul 10 15:53:19 2017 |
| 10.20.1.55 | Bind>Idle | Recv_Release | Mon Jul 10 15:58:09 2017 |
| 10.20.1.55 | Idle>Checking | Recv_Discover | Mon Jul 10 15:58:15 2017 |
| 10.20.1.55 | Checking>Offer | PING_PASS | Mon Jul 10 15:58:16 2017 |
| 10.20.1.55 | Offer>Bind | Recv_Request | Mon Jul 10 15:59:15 2017 |
| 10.20.1.55 | Bind>Bind | Recv_Request | Mon Jul 10 16:59:15 2017 |

4. Check whether only 802.1x authentication is configured on interfaces, and no security channel is configured.

Configure a security channel if none is configured.

expert access-list extended 2700

10 permit arp any any

20 permit udp any any any any eq bootpc

30 permit udp any any any any eq bootps

security global access-group 2700

5. Check whether DHCP packets sent by the client normally reach the RG-N18000.

Manually configure an IP address to ping the gateway to check the connectivity (the ping operation fails if authentication is enabled). Alternatively, run the **debug** command to check whether the RG-N18000 receives the packets, and if no, check the intermediate network.

debug ip dhcp filter mac H.H.H //Run this command so that only packets of a specific MAC address are displayed.

debug ip dhcp server all

Search logs by keywords:

%DHCPD-7-DEBUG: recv dhcp packet from 10.8.8.1 mac 0010.184a.ae10 ifx(4296), I2_port(50), vlan(200), vrf(3) inner_vid (0) vni(0), len=300

--->>This log shows that the DHCP request from the user is received.

%DHCPD-7-DEBUG: send dhcp packet to 10.8.8.1, len=324, ret =324, success!

%DHCPD-7-DEBUG: make ack success, send packet

--->>This log shows that the ACK packet is sent to the user.

6. Check whether the DHCP snooping trust port is correctly configured on the downlink switch.

| switch#show ip dhcp snooping | //Display the | e DHCP sn | ooping configuration. |
|--------------------------------|---------------|-----------|-----------------------|
| Switch DHCP snooping status | | : ENA | BLE |
| DHCP snooping Verification of | hwaddr status | : DI | SABLE |
| DHCP snooping database write- | delay time | : 0 | seconds |
| DHCP snooping option 82 status | 5 | : DIS | SABLE |
| DHCP snooping Support bootp b: | ind status | : DI | SABLE |
| Interface | Trusted | Rate lim | nit (pps) |
| | | | |
| GigabitEthernet 1/2 | YES | unlimit | ed |
| Default | No | u | nlimited |

Note: Check whether relevant uplink ports are configured as trusted ports and whether a rate limit is configured on downlink ports.

7. Enable the debug function on the RG-N18000, and check the packet interaction based on ACL counting (capture packets on the downlink port of the RG-N18000 if condition permit) and packet capture on the client.

expert access-list extended exp1

20 permit udp any host 1111.1111.1111 any any range bootps bootpc (Replace "1111.1111.1111" with the user MAC address.)

90 permit etype-any any any

100 permit ip any any any any

int te1/1 (faulty port)

expert access-group exp1 in

exit

expert access-list counter exp1

show access-list --(Check whether packet statistics are collected.)

The digit enclosed in the red rectangle indicates that 10 DHCP packets are received.

```
core(config) #expert access-list extended expl
core(config-exp-nacl) #$ost 1111.1111.1111 any any range bootps bootpc
core(config-exp-nacl)#90 permit etype-any any any
core(config-exp-nacl) #100 permit ip any any any any
core(config-exp-nacl)#exit
core(config) #int te1/2/1
core(config-if-TenGigabitEthernet 1/2/1) #expert access-group expl in
core(config-if-TenGigabitEthernet 1/2/1)#exit
core(config) #expert access-list counter expl
core(config) #show access-lists
mac access-list extended 700
10 permit any any etype-any
expert access-list extended expl
                                                                     (10)
20 permit udp any host 1111.1111.1111 any any range bootps bootpd
90 permit etype-any any any (3)
100 permit ip any any any any (40)
core(config)#
```

If the client sends out packets but the RG-N18000 does not receive the packets, check whether the intermediate network is reachable.

If the RG-N18000 receives the packets but no relevant log output or response log is generated for the **debug** command, contact the TAC for handling.

If the RG-N18000 returns a response but the client does not receive it, check whether the intermediate network is reachable (check whether ACL or DHCP snooping is configured).

8. If DHCP relay is configured on the RG-N18000, packet interaction between the gateway IP address of the access client and the DHCP server is abnormal due to unreachable route or firewall errors.

On the RG-N18000, ping the DHCP server from the source IP address, to check whether the DHCP server is reachable.

9. The RG-N18000 serves as a DHCP relay, packets between the RG-N18000 and the server are transmitted at layer 2, and the client is not in the same VLAN as the server. As a result, the RG-N18000 does not send packets to the client according to the DHCP snooping binding table.

The principles are described as follows:

- 1. The client is configured on VLAN 60 and the WDS server is configured on VLAN 2.
- The client with the IP address of 192.168.60.2 from VLAN 60 sends the DHCP-Request packet to the WDS server with the IP address of 192.168.0.65. When the packet passes through the DHCP snooping module of the core device, a temporary entry containing the MAC address + VLAN 60 is recorded.
- 3. When the WDS server from VLAN 2 responds to the client with the DHCP-ACK packet, the core device uses MAC address + VLAN 2 for matching in the DHCP snooping table but fails to find the temporary entry. As a result, the packet is directly sent to SVI2 and the client fails to receive the DHCP-ACK packet.

Solution: Run the **no ip dhcp snooping vlan 2** (server VLAN) command on the core device.

10. Capture packets for interaction between the client and the RG-N18000. Capture packets of the RG-N18000 and the DHCP server.

7.7.4 Fault Information Collection

Run the following commands to collect information on the RG-N18000:

```
debug ip dhcp filter mac H.H.H - //Run this command so that only packets of a specific MAC address
are displayed.
debug ip dhcp server all
terminal length 0
show ver detail
show run
show ip dhcp pool
show ip dhcp server statistics
show arp | include ***
sho mac-address-table | include ***
show ip dhcp snooping binding
show ip dhcp snooping binding | in H.H.H
show ip dhcp server agent mac xx.xx.xx (supported in version 11.0(1)B3P3)
show nfpp dhcp-guard host
show ip dhcp relay-statistics
show ip dhcp conflict
show log
show interface counters rate
show interface counters summary
terminal no length
```

7.7.5 Fault Summary and Notes

7.8 Failure to Access the Internet or Internet Access Stalling After Authentication

7.8.1 Symptom

A user fails to access the Internet or the Internet access is stalling after authentication.

7.8.2 Possible Causes

1. The authentication fails or the user goes offline immediately after successful authentication.

- 2. A loop in the downlink device causes random packet loss between the client and the gateway.
- 3. A static IP address is configured for the client and AM rules are configured. Packets are discarded when no AM rule is met.
- 4. Packets are discarded due to improper routing of the RG-N18000 or intermediate device.
- 5. Some packets are discarded due to very high CPU usage of the device, and incorrect VLAN tags are added to packets due to software bugs.

7.8.3 Handling Steps

 On the RG-N18000, run the show web-auth user name *** and show dot1x user name*** commands to check whether the user is online. In addition, access Operation > Online User on SAM+ to check whether there are online users.

If the user is offline, rectify the fault based on authentication symptoms by referring to authentication failure troubleshooting procedures. If the user is online, proceed to the following step.

2. Check the port rate or logs and check whether there are loops. If a loop exists, rectify the fault by referring to the loop locating manual.

See the Procedure for Layer-2 Loop Problem Locating in Simplistic Networks.

3. If the IP address is manually configured, check the AM configuration.

In loose mode, data forwarding is allowed for manually configured normal IP addresses regardless of whether the IP addresses are within the AM range.

In strict mode, data forwarding is allowed for manually configured IP addresses that are within the AM range.

- 4. Check relevant routing entries on the RG-N18000 to check whether more detailed routes are learned from other devices.
- 5. Locate the packet loss point based on ACL-based packet counting or packet capture.

Enable ACL-based packet counting on the RG-N18000 (enable packet capture for troubleshooting if conditions permits).

expert access-list extended exp1

20 permit arp host 1111.1111.1111 any //Check whether ARP packets are received. Replace "1111.1111.1111" with the user MAC address.

40 permit icmp host 1.1.1.1 any any any //Check whether the ICMP packets are received. Replace "1.1.1.1" with the user IP address.

90 permit etype-any any any

100 permit ip any any any any

int te1/2/1 //te1/2/1 is the ingress of the RG-N18000.

expert access-group exp1 in

expert access-list counter exp1 //Enable packet counting for an ACL named exp1.

```
core(config)#show access-lists
expert access-list extended exp1
20 permit arp host 1111.1111.1111 any (4)
40 permit icmp host 1.1.1.1 any any any (15)
90 permit etype-any any any (3)
100 permit ip any any any (40)
core(config)#
```

The ACL-based packet count above shows whether ARP packets or ICMP packets are lost.

If the RG-N18000 does not receive the ARP packets or ICMP packets, check whether the access and aggregation links of the downlink port are faulty.

If the RG-N18000 receives the ARP packets or ICMP packets, check whether ACLs or AM rules for filtering out ARP or ICMP packets are configured.

If no filtering is configured, run the **debug arp ip** + *user IP address* command to check whether ARP packets are sent to the IP layer. Run the **un al** command to disable the debug function, as shown in the figure below.

```
core#debug arp ip 1.1.1.1
*May 16 16:48:24: %SYS-5-CONFIG_I: Configured from console by console
core#*May 16 16:48:28: %P1143-7-DEBUG: ARP:recv request src 1.1.1.1 00d0.f822.33d3; dst 1.1.1.2
0000.0000.0000; TenGigabitEthernet 1/2/5, subvlan 0, inner_vid 0
*May 16 16:48:28: %P1143-7-DEBUG: ARP send reply src 1.1.1.2 00d0.f822.33bb; dst 1.1.1.1 00d0.f822.33d3;
TenGigabitEthernet 1/2/5, subvlan 0, inner_vid 0
*May 16 16:48:28: %P1143-7-DEBUG: ARP:send request src 1.1.1.2 00d0.f822.33bb; dst 1.1.1.1 00d0.f822.33d3;
TenGigabitEthernet 1/2/5, subvlan 0, inner_vid 0
*May 16 16:48:28: %P1143-7-DEBUG: ARP:recv reply src 1.1.1.1 00d0.f822.33d3; dst 1.1.1.2 00d0.f822.33d3;
TenGigabitEthernet 1/2/5, subvlan 0, inner_vid 0
*May 16 16:48:28: %P1143-7-DEBUG: ARP:recv reply src 1.1.1.1 00d0.f822.33d3; dst 1.1.1.2 00d0.f822.33bb;
TenGigabitEthernet 1/2/5, subvlan 0, inner_vid 0
*May 16 16:48:28: %P1143-7-DEBUG: ARP:recv reply src 1.1.1.1 00d0.f822.33d3; dst 1.1.1.2 00d0.f822.33bb;
TenGigabitEthernet 1/2/5, subvlan 0, inner_vid 0
*May 16 16:48:28: %P1143-7-DEBUG: ARP:recv reply src 1.1.1.1 00d0.f822.33d3; dst 1.1.1.2 00d0.f822.33bb;
TenGigabitEthernet 1/2/5, subvlan 0, inner_vid 0
*May 16 16:48:28: %P1143-7-DEBUG: ARP:recv reply src 1.1.1.1 00d0.f822.33d3; dst 1.1.1.2 00d0.f822.33bb;
TenGigabitEthernet 1/2/5, subvlan 0, inner_vid 0
*May 16 16:48:28: %P1143-7-DEBUG: ARP:recv reply src 1.1.1.1 00d0.f822.33d3; dst 1.1.1.2 00d0.f822.33bb;
TenGigabitEthernet 1/2/5, subvlan 0, inner_vid 0
*May 16 16:48:28: %P1143-7-DEBUG: ARP:recv reply src 1.1.1.1 00d0.f822.33d3; dst 1.1.1.2 00d0.f822.33bb;
TenGigabitEthernet 1/2/5, subvlan 0, inner_vid 0
*May 16 16:48:28: %P1143-7-DEBUG: ARP:recv reply src 1.1.1.1 00d0.f822.33d3; dst 1.1.1.2 00d0.f822.33bb;
TenGigabitEthernet 1/2/5, subvlan 0, inner_vid 0
*May 16 16:48:28: %P1143-7-DEBUG: ARP:recv reply src 1.1.1.1 00d0.f822.33d3; dst 1.1.1.2 00d0.f822.33bb;
TenGigabitEthernet 1/2/5, subvlan 0, inner_vid 0
*May 16 16:48:28: %P1143-7-DEBUG: %P1143-7-DEBUG: %P1143-7-DEBUG: %P1143-7-DEBUG: %P1143
```

If ARP packets are not sent to the IP layer or the RG-N18000 does not send out the response from the IP layer, contact the TAC to rectify the fault by using the frame path method.

6. If the ping result shows that no packet loss occurs but it is slow in opening websites and some websites even cannot be opened, check whether only some websites or all websites have the same problem. If only some websites encounter this problem, such websites may be faulty.

If most websites and even some famous websites have this problem, connect the client to the uplink device of the RG-N18000 for testing. If the fault persists, check the uplink device or enable packet capture on the border router to check whether packets are sent out and whether responses are received.

If the Internet access is normal, check whether the RG-N18000 receives and forwards packets normally based on the ACL-based packet counting or packet capture in the inbound direction of the uplink interface or outbound direction of the downlink interface of the RG-N18000.

```
expert access-list extended expl
20 permit ip host 1.1.1.1 any any any (Replace "1.1.1.1" with the actual website IP address.)
90 permit etype-any any any
100 permit ip any any any
```

```
int te1/2/1 //Uplink interface of the RG-N18000
expert access-group expl in
int te1/2/1 //Downlink interface of the RG-N18000
expert access-group expl out
expert access-list counter expl
show access-lists
```

Note: Compare the inbound packets and outbound packets counted based on ACLs to check whether the RG-N18000 forwards packets normally.

7. If packet exchange is normal and an MSC card is configured, check whether PBR is configured and whether the configured uplink and downlink paths are consistent. See the figure below.

```
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 next-hop 10.10.10.2
!
route-map pbr-download permit 10
match ip address download
set ip policy load-balance dst-ip
set ip policy no-ttl-decrease
set ip next-hop 10.10.20.2
```

For specific configuration, see the Typical Configuration Cases of MSC Cards in Simplistic Networks.

If the configured paths are inconsistent, the MSC card discards packets because the packets fail the TCP connection validity check.

If the configuration is free of errors, compare whether the number of packets received by the downlink interface of the RG-N8000 is consistent with that sent by the uplink interface of the RG-N18000 by using the ACL-based packet counting method.

7.8.4 Fault Information Collection

- 1. Record fault symptoms clearly, including the fault scope, packet loss frequency, fault pattern, and whether the network is changed before the fault.
- 2. Clarify the network topology so that the TAC learns about the environment, which is conducive to troubleshooting.

7.8.5 Fault Summary and Notes

- 1. Record fault symptoms clearly, including the fault scope, packet loss frequency, fault pattern, and whether the network is changed before the fault.
- 2. Clarify the network topology so that the TAC learns about the environment, which is conducive to troubleshooting.
- 3. Locate the packet loss point based on ACL-based packet counting or packet capture.
- 4. Check the configuration or work with the TAC to pinpoint the packet loss cause.

7.9 ACL Statistics Scripts of the Troubleshooting Tool

ACL statistics scripts for:

- 1. ARP-based packet statistics
- 2. ICMP-based packet statistics
- 3. IP-based packet statistics
- 4. TCP-based packet statistics
- 5. UDP-based packet statistics
- 6. MAC-based packet statistics

1. ARP-based packet statistics

expert access-list extended exp1

```
20 permit arp host 1111.1111.1111 any (Check whether ARP packets are received. Replace
"1111.1111.1111" with the actual user MAC address.)
90 permit etype-any any any
100 permit ip any any any any
exit
int tel/2/1 (tel/2/1 is the ingress of the RG-N18000.)
expert access-group expl in
exit
expert access-list counter exp1
show access-lists
```

```
expert access-list extended exp1
    20 permit arp host 1111.1111.1111 any
    90 permit etype-any any any
    100 permit ip any any any any
    exit
int te1/2/1
    expert access-group exp1 in
    exit
expert access-list counter exp1
show access-list counter exp1
show access-lists
expert access-list extended exp1
20 permit arp host 1111.1111.1111 any (4)
90 permit etype-any any any (3)
100 permit ip any any any any (40)
core(config)#
```

2. ICMP-based packet statistics

expert access-list extended exp1

```
40 permit icmp host 1.1.1.1 any any any (Check whether ICMP packets are received. Replace
"1.1.1.1" with the actual user IP address.)
  90 permit etype-any any any
  100 permit ip any any any any
  exit
int te1/2/1
                     (te1/2/1 is the ingress of the RG-N18000.)
  expert access-group expl in
  exit
expert access-list counter exp1
show access-lists
expert access-list extended exp1
     40 permit icmp host 1.1.1.1 any any any
     90 permit etype-any any any
     100 permit ip any any any any
     exit
 int te1/2/1
     expert access-group exp1 in
     exit
expert access-list counter exp1
 show access-lists
expert access-list extended exp1
 40 permit icmp host 1.1.1.1 any any any (4)
 90 permit etype-any any any (3)
 100 permit ip any any any any (40)
core(config)#
3. IP-based packet statistics
expert access-list extended exp1
     20 permit ip host 1.1.1.1 any any any (Replace "1.1.1.1" with the actual user IP address.)
     90 permit etype-any any any
100 permit ip any any any any
        exit
        int te1/2/1 (faulty port)
            expert access-group expl in
         exit
           expert access-list counter exp1
           show access-list -- (Check whether packet statistics are collected.)
```

```
core(config) #expert access-list extended exp1
core(config-exp-nacl) #20 permit ip host 1.1.1.1 any any any
core(config-exp-nacl) #100 permit ip any any any any
core(config-exp-nacl) #100 permit ip any any any any
core(config-exp-nacl) #exit
core(config) #int tel/1
core(config) #int tel/1
core(config-if-TenGigabitEthernet 1/1) #expert access-group exp1 in
core(config) #expert access-list counter exp1
core(config) #expert access-list counter exp1
core(config) #show access-lists
expert access-list extended exp1
20 permit ip host 1.1.1.1 any any any (20)
```

4. TCP-based packet statistics

```
expert access-list extended exp1
        20 permit tcp host 1.1.1.1 any any any (Replace "1.1.1.1" with the actual user IP
address.)
     90 permit etype-any any any
100 permit ip any any any any
        exit
        int te1/2/1 (faulty port)
            expert access-group expl in
         exit
           expert access-list counter expl
           show access-list -- (Check whether packet statistics are collected.)
expert access-list extended exp1
    20 permit tcp host 1.1.1.1 any any any
    90 permit etype-any any any
    100 permit ip any any any any
    exit
int te1/2/1
    expert access-group expl in
    exit
expert access-list counter exp1
show access-lists
expert access-list extended exp1
 20 permit tcp host 1.1.1.1 any any any (4)
 90 permit etype-any any any (3)
 100 permit ip any any any any (40)
core(config)#
```

5. UDP-based packet statistics

```
expert access-list extended expl
        20 permit udp host 1.1.1.1 any any any (Replace "1.1.1.1" with the actual user IP
address.)
     90 permit etype-any any any
100 permit ip any any any any
        exit
        int te1/2/1 (faulty port)
            expert access-group expl in
         exit
           expert access-list counter expl
           show access-list -- (Check whether packet statistics are collected.)
expert access-list extended exp1
    20 permit tcp host 1.1.1.1 any any any
    90 permit etype-any any any
    100 permit ip any any any any
    exit
int te1/2/1
    expert access-group expl in
    exit
expert access-list counter exp1
show access-lists
expert access-list extended exp1
 20 permit udp host 1.1.1.1 any any any (4)
 90 permit etype-any any any (3)
 100 permit ip any any any any (40)
core(config)#
6. MAC-based packet statistics
```

```
mac access-list extended macl
20 permit host 1111.1111 any
100 permit any any
exit
int te1/2/1
expert access-group macl in
exit
mac access-list counter macl
show access-lists show access-list --(Check whether packet statistics are
collected.)
```

```
expert access-list extended exp1
    20 permit host 1111.1111.1111 any
    100 permit any any
    exit
int te1/2/1
    expert access-group mac1 in
    exit
mac access-list counter mac1
show access-lists
mac access-list extended mac1
    30 permit host 1111.1111.1111 any etype-any (10)
    100 permit any any etype-any (50)
core(config)#
```

7.10 Layer-2 Loop Problem Locating in Simplistic Networks

7.10.1 Check RLDP logs.

Run the following command to check RLDP logs to preliminarily locate the ports and VLANs experiencing the loop: show rldp loop-detect-log,



7.10.2 Find out the ports and VLANs that encounter the loop.

Run the **rldp reset** and **show rldp** commands several times and check the **neighbor** field. Check whether the VLANs and ports change each time after the **rldp reset** command is executed, in an effort to determine the loop type (see the figure below).



7.10.3 Take measures based on the following cases:

7.10.3.1 Same VLAN and same port

The VLANs and ports causing the loop can be determined after the operations above are performed. If the VLANs and ports keep unchanged after the **rldp reset** command is executed several times, the possible topology is as follows:



Operation steps

- 1. Find out the aggregation switch experiencing the loop based on the ports and find out the access switch based on the VLANs.
- 2. Run the following command to check whether port traffic statistics is abnormal on the aggregation switch and access switch. If yes, rectify the fault step by step based on the abnormal traffic. show interface counters rate [up]

| Ruijie#show Interface ate C) | interfaces counter Sampling Time Output Rate (packets/sec) | s rate ex 0 Input Rate (bits/sec) | 0 Input Rate (packets/sec) | \$ Output R (bits/se |
|---------------------------------------|---|---|----------------------------------|----------------------------|
| Gi0/11 1 Gi0/23 | 5 seconds 940099 5 seconds | 849671428 0 | 940095 0 | 84967524 85704022 |
| 7 Gi0/29 6 | 894072 5 seconds 940096 | 849675580 | 940100 | 84967178 |

3. If the condition permits, enable the RLDP function on the aggregation switch and access switch (the enabling of RLDP will shut down the loop ports) to check whether a loop is detected.



4. Run the **show mac-address-table vlan** *xx* command multiple times to check whether MAC addresses in the MAC address table have drifted. If MAC addresses have drifted, a loop occurs on the drift source and destination ports. If no MAC address drift exists on the access switch, check whether it occurs on the aggregation switch.

7.10.3.2 Same VLAN but different ports

The VLANs and ports causing the loop can be determined after the operations above are performed. If the VLANs keep unchanged but the ports change after the **rldp reset** command is executed several times, the possible topology is as follows:



Operation steps

- 1. Run the **rldp reset** and **show rldp** commands several times and check the **neighbor** field to find out the ports and VLANs of all loops.
- 2. Run the **show mac | in vlan** command on the aggregation switches at both ends and check whether entries of the same MAC address exist.
- 3. If yes, the interface corresponding to the MAC address is a loop interface.

7.10.3.3 Different VLANs but same port

The VLANs and ports causing the loop can be determined after the operations above are performed. If VLANs are different but ports are the same after the **rldp reset** command is executed several times, the possible topology is as follows:

Operation steps

- 1. Find out the aggregation switch experiencing the loop based on the ports and find out the access switch based on the VLANs.
- 2. Run the **show mac | in vlan** command to display the MAC address tables of VLANs on the two access switches and check whether entries of the same MAC address exist.

7.10.3.4 Different VLANs and different ports

Possible topology:



Operation steps

1. Run the **rldp reset** and **show rldp** commands several times and check the **neighbor** field to find out all ports and VLANs experiencing the loop.

2. Run the **show rldp** command and check the **neighbor** field. Check whether the neighbor ports are on the same downlink port of the core switch. 3. Run the **show mac | in vlan** command on the aggregation switches at both ends and check whether entries of the same MAC address exist.

7.10.3.5 Trunk port loop

Possible topology:



Operation steps

- 1. Run the **show rldp** command and check the **neighbor** field. Check whether the neighbor ports are on the same downlink port of the core switch.
- 2. Check whether MAC address drift occurs on the aggregation switch or check the port traffic statistics.

7.10.3.6 Hub loop



Run the show interface counters summary up command to check traffic statistics of access ports.

7.11 Failure to Query Real-time Traffic of the User Gateway on SAM+ in MSC Card Scenarios

7.11.1 Symptom

No user traffic information is found when the real-time traffic of the gateway is queried on SAM+.

7.11.2 Possible Causes

- 1. Configurations for interconnecting with SAM+ are improper on the RG-N18000. As a result, IPFIX packets are exchanged abnormally.
- 2. The gateway policy name added to SAM+ is inconsistent with that added to the RG-N18000. As a result, the user group synchronization between the SAM+ and the RG0N18000 fails.
- 3. The PBR is configured incorrectly on the RG-N18000 and MSC, and therefore, traffic is not diverted to the MSC.

7.11.3 Handling Steps

1. Check whether the interconnection configurations of the RG-N18000 and SAM+ are correct.

RG-N18000 configuration: The authentication and accounting mode is set to IPFIX.

dot1x acct-method ipfix //Set the 802.1x authentication and accounting mode to IPFIX, to upload traffic information to the SAM+ server (192.168.1.6 indicates the source interface, which can be a layer-3 interface or VLAN, or configured as required.)

Check whether the SAM+ configuration is correct.

| Shortcut Channel 🔅 | Homepage System Security User Access Control Billin | g Account Operation | |
|-----------------------------------|---|--------------------------------|---|
| Location: System > Device Managem | ient > Add | | |
| Device | | | |
| Device IP Address* | 172.18.157.251 | IP Type* | IPv4 • |
| Device Type* | Ruijie Switch | Model* | N18K • |
| PPPoE Authentication Domain | Please use comma or space to separate multiple domains | IPOE+Web Authentication Domain | Please use comma or space to separate multiple |
| Device Key* | ruijie | Community* | ruijie |
| MAC Address | For trusted ARP binding application, MAC address must be | Child D Desire Desit | the set of |
| MAC Address | filled | SNMP Proxy Port | Il you do not fill in, the default port for will be a |
| 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 | \blacksquare Enable (Applicable to authentication client + access switch authentication mode) | N18K Feature | 🗷 Layer Gateway Certification 📄 Use Port 2009 |
| | | | |

| Shortcut Channel 🔅 | Homepage System | Security User | Access Control | Billing | Account | Operation |
|---------------------------------------|-------------------------------|-----------------------|--------------------|----------------|-------------|-------------|
| Location: System > Billing Settings | | | | | | |
| Charging Configuration | | | | | | |
| Accounting Port* | 1813 | | | | | |
| Accounting Update Options | Enable Accounting Update Pack | et Processing(Overtim | e=Accounting Updat | e Interval * N | Aaximum Wai | ting Times) |
| Internet Traffic Server Configuration | n | | | | | |
| Internet Traffic Server | 🕑 Open | | | | | |
| Internet Traffic Server Port* | 4739 | | | | | |
| Cost Negative Compensation | 🕑 Open | | | | | |
| Session Billing Configuration | | | | | | |
| Daily Accounting Processing | 🕑 Open | | | | | |
| Daily Account Billing Time* | 2 : 0 | | | | | |
| | | | | | | |
| | | | | Save | Reset | |

The gateway policy name is mandatory, so that the gateway policy can be delivered to the RG-N18000 and the RG-N18000 can synchronize user information to the MSC. Pay attention to the following items when configuring the gateway policy:

The gateway policy name should be consistent with that configured on the MSC card, for example, default.

| Shortcut Channel 🔅 | Homepage | System Security | User | Access Control | Billing | Account | Operation | | | |
|--|----------------------------|------------------------|---------------|---------------------|------------|--|--|--|--|--|
| ocation: Access Control > Access Control > Modify | | | | | | | | | | |
| Access Control Information User | Information Check N | etwork Usage Control | Public Se | rvice User Behavi | or Control | VPN Control | Client Version Management Wireless Access Proper | | | |
| Access Control Name * | solution | | | | | | | | | |
| Concurrent Logins Limit(0 to 99) 0 means no limit * | 1 | | | | | Synchroniza | tion Accounting Update Interval | | | |
| According to the Terminal Type Control | oncurrent Logins (1 to 9 | 9 times) | | | | | | | | |
| | 🕑 Display accounting p | oolicy information whe | n user onlin | e | | Automatic Binding MAC authentication information quickly | | | | |
| | Show users on-line a | access control time | | | | Account information is displayed on a subscriber line | | | | |
| Gateway Access Restriction | It does not allow training | ffic through the gatew | ay server (ga | ateway device needs | to be depl | ployed linkage in penetration mode) | | | | |
| Export linkage strategy | | * non NPE / EG ga | teway billin | g model deployment | , no need | to configure the | export collaboration policy | | | |
| Firewall Policy | | * not deploy firew | alls linkage, | the need to configu | re | | | | | |
| Description | | | | | | | | | | |
| * Please refer to respective label conte | ent for access details | | | | | | | | | |
| | | | | | Save | Back | | | | |

2. Check the PBR configuration.

Use the client to access an extranet and run the **show ip fpm flows** | **include (IP)** command on the MSC card to check the values of **SendBytes** and **RecvBytes** and whether traffic is increasing. If the values are **0** or the traffic is not increasing, check the PBR configuration.

| Pr | SrcAddr | 5 | DstAddr | | SrcPort | DstPort | Vrf | SendBytes | RecvBytes | St | srcif |
|----|----------------|----------|---------------|-----------|----------|----------|-----|-----------|-----------|----|-------|
| 6 | 10.0.3.2 (| 0.0.0.0) | 10.0.3.254 | (0.0.0.0) | 55332(0) | 3333 (0) | | 60 | 0 | 2 | fff |
| 6 | 10.0.5.2 | 0 | 10.0.5.1 | | 42091 | 3333 | | 204678876 | 204590106 | 1 | fff |
| 6 | 10.0.5.2 | | 10.0.5.1 | | 42092 | 3333 | | 204485958 | 204502204 | 1 | fff |
| 6 | 10.0.5.2 | | 0 10.0.5.1 | | 42093 | 3333 | | 204532961 | 204511386 | 1 | fff |
| 6 | 10.0.5.2 | | 0 10.0.5.1 | | 42094 | 3333 | | 204485916 | 204486051 | 1 | fff |
| 17 | 172.18.159.172 | 40000 | 239.192.152.1 | .43 | 6771 | 6771 | 511 | 984 | 0 | 1 | 2001 |
| 6 | 10.0.5.2 | 40000 | 10.0.5.1 | | 42097 | 3333 | | 204488420 | 204489255 | 1 | fff |
| 6 | 10.0.5.2 | | 0 10.0.5.1 | | 42098 | 3333 | | 204488334 | 204488445 | 1 | fff |
| 17 | 10.0.5.2 | | 172.18.157.32 | | 1230 | 123 | | 2302116 | 2676904 | | fff |
| 17 | 10.0.5.2 | 0 | 10.0.5.1 | | 1230 | 123 | 0 | 2302116 | 2302116 | 3 | fff |

RG-N18000 ip access-list extended pbr-download 10 permit ip any 10.20.0.0 0.0.255.255//The network segment is a network segment whose traffic needs to be diverted to the MSC. ip access-list extended pbr-upload 10 permit ip 10.20.0.0 0.0.255.255 any//The network segment is a network segment whose traffic needs to be diverted to the MSC.

route-map pbr-upload permit 10
match ip address pbr-upload
set ip policy load-balance src-ip
set ip policy no-ttl-decrease
set ip next-hop 10.0.3.2 //LAN address of the MSC card.
!
route-map pbr-download permit 10
match ip address pbr-download
set ip policy load-balance dst-ip
set ip policy no-ttl-decrease
set ip next-hop 10.0.4.2 //WAN address of the MSC card.

HXJH-18K(config)#int vlan 2001 //Invoke PBR-upload on the downlink interface. HXJH-18K(config-if-VLAN 2001)#ip policy route-map pbr-upload

HXJH-18K(config)#int gi1/23 //Invoke PBR-download on the uplink interface. HXJH-18K(config-if-GigabitEthernet 1/23)# ip policy route-map pbr-download

MSC configuration: ip access-list standard PBR-ACL //Matching needs to be performed on all user traffic. 10 permit any

route-map port2-WAN permit 10 match ip address user-data set ip next-hop 10.0.3.1 //Set the next hop of data flows of the WAN port to the IP address of the WAN port on the RG-N18000.

```
route-map port1-LAN permit 10
match ip address user-data
set ip next-hop 10.0.4.1 //Set the next hop of the data flows from the LAN port to the IP address
of the WAN port on the RG-N18000.
```

MSC(config)#int tenGigabitEthernet 0/1

MSC(config-if-TenGigabitEthernet 0/1)# ip policy route-map port1-LAN
MSC(config)#int tenGigabitEthernet 0/2
MSC(config-if-TenGigabitEthernet 0/2)# ip policy route-map port2-WAN

7.12 Network Access Exception After Traffic Goes Through the MSC Card

7.12.1 Symptom

A network access exception occurs after traffic goes through the MSC card.

7.12.2 Possible Causes

- 1. Check whether the PBR is configured correctly. Incorrect PBR configuration may result in incorrect traffic diversion.
- 2. The number of ACEs on the RG-N18000 exceeds the limit. As a result, a PBR diversion exception occurs.
- 3. The IP connection count exceeds the upper limit, causing failures in opening some websites.
- 4. Packets cannot be processed and are discarded due to poor MSC performance.

7.12.3 Handling Steps

1. Check whether the PBR is configured correctly. Incorrect PBR configuration may result in incorrect traffic diversion.

Use the client to access an extranet and run the **show ip fpm flows** | **include (IP)** command on the MSC card to check the values of **SendBytes** and **RecvBytes** and whether the traffic is increasing. If the values are **0** or the traffic is not increasing, check the PBR configuration.

| MSC#s | how ip fpm flows rcAddr | | DstAddr | | SrcPort | DstPort | vrf | SendBytes | RecvBytes | srcif |
|----------|----------------------------|---------------------|----------------|-----------|----------|----------|-----|-----------|------------|-------|
| † 6 1 | 0.0.3.2 (0.0 | trl_flag d .0.0) | 10.0.3.254 | (0.0.0.0) | 55332(0) | 3333 (0) | 0 | 60 | 0 | fff |
| 6 1 | .0.0.5.2 | 0000 | 10.0.5.1 | | 42091 | 3333 | 0 | 204678876 | 204590106 | fff |
| 6 1 | 0.0.5.2 | 1 | .0 10.0.5.1 | | 42092 | 3333 | 0 | 204485958 | 204 502204 | fff |
| 6 1 | 0.0.5.2 | 0 | 10.0.5.1 | | 42093 | 3333 | 0 | 204532961 | 204511386 | fff |
| 6 1 | 0.0.5.2 | 0 | 10.0.5.1 | | 42094 | 3333 | 0 | 204485916 | 204486051 | fff |
| 17 1 | 72.18.159.172 | 0 | 239.192.152.14 | | 6771 | 6771 | 511 | 984 | 0 | 2001 |
| 6 1 | 0.0.5.2 | 0000 | 10.0.5.1 | | 42097 | 3333 | 0 | 204488420 | 204489255 | fff |
| 6 1 | 0.0.5.2 | 0 | 10.0.5.1 | | 42098 | 3333 | 0 | 204488334 | 204488445 | fff |
| 17 1 | 0.0.5.2 | 0 | 172.18.157.32 | | 1230 | 123 | | 2302116 | 2676904 | fff |
| 17 1 | 0.0.5.2 | | 10.0.5.1 | | 1230 | 123 | | 2302116 | 2302116 | fff |

2. The number of ACEs exceeds the limit. As a result, a PBR diversion exception occurs.

Delete PBR configuration from the interface and reconfigure the PBR (exercise caution when performing this operation), or configure an ACL that can be invoked by any interface, and check whether the number of ACEs exceeds the limit. If relevant logs are produced, it indicates that the number of ACEs exceeds the limit.

QJNU-CORE(config)#web-auth direct-host 003681: sep 28 11:35:17 QJNU-CORE: %AAA-6-USER_AUTH_PASSED: User authenticated 003682: sep 28 11:35:18 QJNU-CORE: %AAA-6-USER_AUTH_PASSED: User authenticated. Username: 2016112150. 003683: sep 28 11:35:20 QJNU-CORE: %AAA-6-USER_AUTH_PASSED: User authenticated. Username: 2015113224. 2.2.2.2 003684: sep 28 11:35:24 QJNU-CORE: %CLI-5-EXEC_CMD: Configured from vty0(10.19.9.104) by rgs command: web-auth direct QJNU-CORE(config)#003685: sep 28 11:35:24 QJNU-CORE: %SS_FP_CORE-4-ACE_CAP_SHORTAGE: TCAM's hardware resources is sho 3. The IP connection count exceeds the upper limit, causing failures in opening some websites.

If several people in a dormitory share one IP address for Internet access, the IP quantity upper limit is small and some connections will be blocked. If a PC, mobile phone, or server has multiple external connections, the Internet access will be affected.

Locate the MSC card connected to the faulty client and run the **show flow-pre-mgr ip-info** *[ip-address]* command on the MSC card to check the IP connection quantity. In the figure below, the IP connection quantities of the first two IP addresses reach the upper limit and the corresponding clients may experience similar access exceptions. See the figure below.

| M18000-MSC-EDA#show IP-ADDRESS | flow-pre-mgr i flow-cnt | p-info flow-limit |
|-----------------------------------|----------------------------|----------------------|
| 172.24.29.14 | 2000 | 2000 |
| 172.24.8.87 | 2000 | 2000 |
| 172.24.38.234 | 1997 | 2000 |
| 172.24.21.24 | 1975 | 2000 |
| 172.24.21.119 | 1806 | 2000 |
| 59.73.166.65 | 1780 | 2000 |
| 172.26.129.59 | 1722 | 2000 |
| 172.24.19.137 | 1692 | 2000 |
| 172.24.10.54 | 1649 | 2000 |
| 172.24.22.172 | 1643 | 2000 |
| 172.24.4.194 | 1587 | 2000 |
| 172.24.12.205 | 1479 | 2000 |
| 172.26.138.86 | 1389 | 2000 |
| 172.26.35.33 | 1353 | 2000 |
| 172.26.11.88 | 1198 | 2000 |
| 172.26.4.236 | 1169 | 2000 |
| 172.24.34.147 | 1101 | 2000 |
| 172.26.130.12 | 1090 | 2000 |
| 172.24.4.199 | 1019 | 2000 |
| 59.73.160.143 | 959 | 2000 |
| 172.24.34.6 | 944 | 2000 |
| 59.73.145.76 | 937 | 2000 |

4. Packets cannot be processed and are discarded due to poor MSC performance.

Run the **show interface** command to check the value of **no buffer**. If the value increases rapidly, it indicates that the performance is poor. If the value is not zero but increases occasionally, the performance is acceptable.

