Ruijie Networks – Innovation Beyond Networks

Ruijie SCN Solution FAQs V1.1

Copyright Statement

Exemption Statement

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

Revision History

Date	Change contents	Reviser
2016.09.01	Initial Release	Amy & Crystal
2017.02.01	Add Q33-Q36 on Publication V1.1	TAC Oversea

1 Abstract

This document details questions frequently asked during network deployment with reference to the use limit of the simplified network, to help after-sales personnel on deploying the simplified network solution and improve the deployment efficiency and quality.

Audience

- Network Engineers
- Network Administrator

Obtain Technical Assistance

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

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

Related Documents

- Ruijie SCN Solution FAQs V1.1

2 Index Description

This document describes questions that frequently occur on the simplified network. The questions are categorized based on the question description. Certain type of questions are centralized answered. A specific index is not available. However, you can search the keywords using the shortcut keys Ctrl+F.

3 Terms

Acronyms and Abbreviations	Full name in English	Description
FAQ	Frequently Asked Questions	Frequently asked questions
Super VLAN	Super VLAN	The super VLAN is also known as the VLAN aggregation. A super VLAN includes multiple sub VLANs. Each sub VLAN is a broadcast domain. Different sub VLANs are mutually isolated on layer 2.
BRAS	Broadband Remote Access Server	The broadband remote access server (BRAS) is a new access gateway, located at the edge layer of the backbone network. It is used to access the data of the IP or ATM network.
Newton	RG-Newton	The Newton switch is a core component of the simplified campus network.
SAM	security account manager	The security accounting managerment (SAM) is a Radius server providing authentication and accounting.
Tolly	Tolly	An international authoritative evaluation organization
VSU	Virtual Switching Unit	Based on the network system virtualization technology, two switches are combined as a single virtual switch, to simplify the network topology, reduce network complexity, shorten application recovery duration and service interruption duration, and improve network resource usage.
SNC	Smart Network Controller	A NMS product of Ruijie, performing monitoring and management on the entire network.
NAS	Network Access Server	Remote access device.
Radius	Remote Authentication Dial In User Service	The dial-in authentication system is defined by RFC2865 and RFC2866, which are the most widely used AAA protocols.
Su	Su	Ruijie 802.802.1x-authenticated client
CLI	command-line interface	An interface where a user can enter prompts to run a command.

4 Contents

5 SCN Solution FAQ

Q1: Why can't the web authentication page pop up?

A: You can perform the following steps to identify the issue:

Step 1: Check whether the terminal PC successfully obtains an IP address.

1. On the terminal, run ipconfig/all to check the IP address.
2. On the N18K, run show ip dhcp binding | include xxxx.xxxx.xxxx (user MAC address).

Step 2: Check the terminal PC connectivity.

1. Run arp –a to check whether the terminal has successfully learnt the ARP information of the gateway.
2. On the terminal, ping a common website to check whether the DNS is normal. By default, the DNS protocol is bypassed for web authentication.
3. On the terminal, ping the IP address of the Portal server. If the ping fails, check whether N18K bypasses the Portal IP address, for example, http redirect direct-site 172.18.18.35.

Step 3: On the N18K, run show arp | include IP to check whether the terminal has correctly learnt the ARP entry of the corresponding PC.

1. If the ARP entry is dynamically learned and the MAC address is not the actual terminal MAC address, you can run clear arp IP address to clear the address to perform fast recovery.
2. If the ARP entry is learnt in static mode, and the MAC address is not the actual terminal MAC address, you need to check the online entry of the web.
3. If the queried information of the online user is inconsistent with that on the terminal, information residual of the online user may occur. This issue can be rapidly recovered by running the commands clear web-auth user ip x.x.x.x and clear ip dhcp binding x.x.x.x.

Q2: Why does the device fail the 802.1x authentication although the basic configuration of the 802.1x is correct?

1. On access layer switch, 802.1x configuration and AAA configuration should be removed to ensure that they can transparently transmit the 802.1x packets to Core switch.
2. A key configuration of the simplified campus network solution is to prune the VLAN on Trunk port. Therefore, when deploying a scn network, check whether the VLAN where the user exists is pruned. If yes, the packets cannot be transparently transmitted.

Q3: Why does the system prompt user authentication expiration?

A: The possible reasons are as follows:

Generally, the NAS IP may not be added to the SAM or incorrectly added to the SAM. You can check the authentication logs on the SAM and check whether the log prompts incorrect NAS IP.

The Su client does not select a proper network interface card when multiple network NIC exist, resulting in the authentication expiration.

The SAM is inaccessible. You can ping the IP address of the SAM on the N18K.

The VLAN ID of the access device is missing on the distributed device. The EAP packet cannot be transparently transmitted to the N18K, resulting in the authentication failure.

The 802.1x configuration must be removed on the access device. Otherwise, the 802.1x packets cannot be transparently transmitted to Core switch.

Q4: What are differences between the latest authentication collection solution on the simplified campus network and the previous controlled access authentication solution?

A: The previous controlled access authentication solution uses access devices as the NASs. Network administrator has to configure authentication on all layer and all access device. The configuration, management, and maintenance workload is huge. In the simplified campus network solution, the NAS authentication devices are centralized performed on the core switch. The management and maintenance are only performed on the core layer, to achieve controlled authentication. Therefore, the subsequent management and maintenance work is relative simple.

Q5: Can I configure it to push different Web Portal to different authentication interface?

A. Yes, Newton series switches supports configure multiple authentication templates and different authentication templates can be customized for different Web Portal. Therefore, you can apply different web authentication templates to different authentication interfaces.

Q6: Is the performance increased after the VSU is deployed? For example, is the online user capacity doubled in VSU solution? Do different products in the same series support built up VSU?

A. The performance capacity does not increase and still remains the capacity of the standalone device. The VSU technology can be deployed on different products in the same series， like N18010 is able to built VSU with N18007. The VSU technology ensures device reliability. When a device fails, the services are switches to the standby device without user awareness. Therefore, it ensures continuous service running and no data forwarding interruption within 50 ms.

Q7: Why is the console hanged after a stand-alone system is configured in the VSU mode?

A. According to normal operation habits, generally, the network administrator adjusts the baud rate to 115200 baud and saves the configurations. After a stand-alone device is changed to the VSU mode, the device loads the VSU configuration template instead of that of the stand-alone device. If the VSU mode is initially configured, the baud rate is 9600 by default. After the device is switched over and restarted, you cannot access the system and the CLI is hanged, caused by different baud rates. In such a situation, you need to adjust the baud rate to 9600.

Q8: How does the system implement user isolation and locating after user authentication?

A: Currently, the simplified campus network supports two deployment modes: access isolation and QinQ.

User isolation: Each access device is in a VLAN. Protected interfaces are enabled between ports to achieve isolation. For the QinQ mode, the ports of the access device belongs to different VLANs to achieve isolation.

locating: Currently, the locating tool is used for information locating. After a user accesses to the access device, the access device transmits the MAC address, port number, VLAN information, and device information of the user to the locating tool through the SNMP. After the user is authenticated, the SAM server synchronizes the user information to the locating tool. According to the information, the locating tool can locate the user. In addition, the locating tool can save the history login records of the user to rapidly identify any account hacking.

Q9: In the configuration template, the default-router command is not configured for the DHCP pool. Does this affect the client to obtain the IP address of the gateway?

A: In network planning, if the default-router command is not configured, the device sends the interface address, as the gateway address, to the client by default. For example, if the network segment configured for the DHCP is 10.0.0.0/24 and the IP address of the VLAN100 interface is 10.0.0.1/24, if the default-router command is not configured, the device sends the IP address of the SVI100, as the gateway address, to the client. It is recommended to configure ”default router” during network deployment because it makes the configuration command planning clear and easy to check.

Q10: As a core-layer device, the Newton device provides gateway services and DHCP server functions. Why is the DHCP snooping still required?

A: The DHCP snooping is a standard configuration on the simplified campus network, which is mandatory, because:

The IP authorization modes in the 802.1x authentication include Su authorization, Radius authorization, DHCP authorization, and Mixed authorization. The DHCP authorization requires the information in the entries of the DHCP snooping to authorize rights to users.

In the MAB authentication, the users' IP address cannot be delivered. Therefore, the entries of the DHCP snooping are required to deliver the IP address of the to-be-authenticated client to the Radius server, to generate the corresponding online authentication entries.

Q11: How can I inherit the planned network addresses during the network reconstruction for the simplified campus network?

A: The DHCP scheme has the following changes:

CLI changes: Besides the original DHCP pool configurations, the following configuration commands are added:

```
address-manage
match ip default 1.1.0.0 255.255.254.0----------------------------------------Global configuration
match ip 1.1.1.1 255.255.255.255 Gi0/1 vlan 1,11-20----------------------Interface+VLAN configuration
match ip 1.1.1.2 255.255.255.255 Gi0/1-------------------------------------Router interface
configuration (temporarily not supported)
```

Changes in implementation:

1) In versions earlier than 11.x, the addresses in the subvlan-address-range range are allocated as follows. The association with the DHCP is canceled. You do not need to focus on these messages. The address allocation is not subject to the configurations. The original configuration commands are as follows:

```
vlan 2
supervlan
subvlan 21-29
vlan 24
subvlan-address-range 20.1.1.1 20.1.1.100
```

2) If the **address-manage** command is not configured, the DHCP allocation scheme adopts the original DHCP pool process.

3) If only the default rule in the **address-manage** command is configured, all interfaces are allocated based on the default rule. When this command is configured, the existing address is not deleted. When this command is deleted, the existing address is not deleted and the address allocation is based on the rule upon the next user request.

4) If only the interface+VLAN in the **address-manage** command is configured, addresses are allocated to users accessed through the interfaces in the specific VLANs. Addresses are not allocated to users accessed through the interfaces in other VLANs. When this command is configured, the existing address is not deleted. When this

command is deleted, the existing address is not deleted and the address allocation is based on the rule upon the next user request.

5) If the default rule and interface+VLAN in the **address-manage** command are configured, for the interfaces that match the interface+VLAN rule, the addresses are allocated according to the rules. For interfaces in other VLANs, the addresses are not allocated. When this command is configured, the existing address is not deleted. When this command is deleted, the existing address is not deleted and the address allocation is based on the rule upon the next user request.

Software limitation:

```
Assume that the configurations exist:
match ip 1.1.1.0 255.255.255.0  Gi0/1 vlan 2-10
match ip 2.1.1.0 255.255.255.0  Gi0/1 vlan 11-20
```

Assume that PC1 belongs to VLAN11. If the static IP address is 1.1.1.0/24, the PC cannot normally communicate with the network. If the **address-manage** command is configured, it is equivalent to enable the filter entry, and the interface filters packets according to the rules. Therefore, during the deployment, this limitation shall be noticed.

Q12: How can I rapidly locate the faulty position when a terminal is abnormal?

A: The logs of the SAM server record the NASIP, Port, and VLAN ID information of the user. With reference to the VLAN planning list, you can check the IP address and port number of the corresponding access device.

Q13: How can I upgrade the software version of the device? Is there any change in the upgrade mode?

The software version upgrade remains unchanged, using the USB flash drive or the TFTP. The upgrade commands have certain differences.

1) Version upgrade using the USB flash drive

Copy the software version file to the USB flash drive. Insert the USB flash drive to the USB interface of the device management board.

Configure the following commands to upgrade the version:

```
Upgrade usb0:/xxxxx (file name of the line board)
Show upgrade status (view the software version upgrade status)
Upgrade usb0:/xxxxx (file name of the management board)
Show upgrade status
```

After the software version is successfully upgraded, save the configurations and restart the device.

1) Version upgrade using the TFTP

Configure the IP address of the MGMT interface to access the network. Ensure that the TFTP Server and the MGMT interface can successfully interwork with each other.

Access the Shell mode of the system and the temporary directory.

```
N18K#run-system-shell
#cd /tmp/vsd/0*** (This directory corresponds to the tmp directory of the system, queried using the
N18K#dir tmp command)
Tftp -g 200.1.1.1 -m -r lc.bin (the file name cannot include brackets)
Exit the Shell mode and run the following configuration commands:
Ruijie#upgrade flash:lc.bin force (upgrade the version of the line board)
Ruijie#upgrade flash:cm.bin force (upgrade the version of the management board)
```

After the software version is successfully upgraded, save the configurations and restart the device.

Remarks: The versions are saved on the device for archive after the upgrade.

Q14: Is there a simple method to allocate VLANs because the workload is heavy for access VLAN allocation?

A: When the original campus network is upgraded to the simplified network, the VLANs should be re-allocated to the access devices. The simplified campus network deployment tool can be used to reduce the workload of the network center.

Usage of the auto VLAN configuration tool

1) Batch configuration delivery: The VLAN configuration is imported using the pre-configured VLAN template. The configuration commands are automatically delivered in batch.
2) Backup configuration: This tool supports data backup. It can automatically back up the device configuration in a file named config.bak+current date, by means of the Telnet.
3) Display of the command execution result: The tool can display the command execution structure and number of successful and unsuccessful execution records. The unsuccessful execution records can be exported in Excel format for error correction.

Features and advantages of the flattened solution:

1) Previously, the device configurations are manually implemented, which is time consuming. The simplified network deployment tool can greatly reduce the workload (with the configuration backup and restoration functions).
2) After the original network is upgraded to the simplified network, the network management personnel can import the original configuration commands to the access switch.

3) The solution is flexible applicable to the VLAN allocation of the campus network.

4) If error occurs, the version can be rolled back according to the system prompts.

Q15: How to handle the issue that the upgraded version is abnormal?

A: The version rollback function is provided. Note that the patch is a part of the system version. After the system version is rolled back, the patch file is also rolled back. The configuration command is as follows:

Upgrade rollback slot all

Q16: How to install a patch on the device?

A: Using the OSPF hot patch as an example, the operation is as follows:

```
Ruijie#copy usb0:xxx tmp:----------------------------Copy the files in the USB flash drive in the tmp directory.
•Ruijie#run-system-shell--------------------------------Enter the Shell configuration mode.
•~ # cd /sbin-------------------------------------------------Access the sbin file.
•/sbin # ls -la | grep ospf.elf------------------------------Check the current OSPF process.
•/sbin # mv /sbin/ospf.elf /sbin/ospf.elf.bak-----------Back up the OSPF process.
•/sbin # mv ospf.elf /tmp/vsd/0/ospf.elf.new----------Replace the OSPF file with the new OSPF file.
•/sbin # chmod 777 ospf.elf-----------------------------Authorization
•/sbin # sync-------------------------------------------------Synchronization
•/sbin # ls -la | grep ospf.elf------------------------------Check the current OSPF process.
•sbin # pgrep ospf.elf-----------------------------Check the current OSPF process.
•/sbin # pkill -9 ospf.elf-----------------------------------Restart the OSPF process.
•After the OSPF process is restarted, the system outputs the following information:
•/sbin # *Mar  5 18:42:39: %HA-5-HA_SCRIPT_RESTART: Process: /sbin/ospf.elf  Pid: 3743 receives error_signal[9] and quits, Process: /sbin/ospf.elf  is restarting ...
•*Mar  5 18:42:39: %HA-5-HA_SCRIPT_RESTART: Process: /sbin/ospf.elf  restarts 2 times newpid is 3864 and restarts successfully
```

Q17: How do different Sub VLANs in the same Super VLAN communication with each other?

It is also known as VLAN aggregation and is a specialized IP address optimization technology. According to this technology, IP addresses in a network segment are allocated to different sub VLANs, which belong to the same super VLAN. Each sub

VLAN is an independent broadcast domain. Different sub VLANs are isolated on layer 2. When users in the sub VLANs require L3 communication, the IP address of virtual interface of the super VLAN is used as the gateway address. In this manner, multiple VLANs share the same IP address, thereby saving IP resources. In addition, the ARP proxy is used to enable the interworking between sub VLANs on L3 and the interworking between the sub VLAN and other networks. The ARP proxy can forward and process ARP requests and responses, thereby enabling the interworking between ports, isolated on L2, on the L3. In default state, the ARP proxy is enabled for the super VLAN and sub VLAN.

Q18: Why does a user who passes the 802.1x authentication fail to connect to the network after manually modifying the IP address?

A: After the user passes the 802.1x authentication, the device generates the static ARP entry, for example, 1.1.1.10 +mac1. If the user manually modify the IP address, for example, 1.1.1.11, the IP address corresponding to the static ARP entry is inconsistent with the IP address set by the user. The packets cannot be successfully forwarded. At this time, the user does not trigger the device to authentication again. As a result, the user cannot access the network.

Q19: Can the existing route configuration information of the old network be inherited during network reconstruction?

A: The configuration of the OSPF routing information of the old network should be revised. Generally, the OSPF routing protocol uses commands network x.x.x.x area x to broadcast OSPF hello packet to all devices. If the old OSPF configuration is directly inherited, because the IP addresses of the super VLAN on the N18K are gateway IP addresses in each network segment, the OSPF hello packet is broadcast to all sub VLANs. Therefore, if the OSPF route is dynamically advertised using the network manner, the OSPF-based passive interfaces should be enabled on the N18K, that is, passive-interface xxx. All SVI interfaces (gateways) of the super VLAN should be set to OSPF-based passive interfaces. In this manner, when the device advertises the network segment addresses, the L2 network does not have a large number of OSPF hello packets, thereby reducing the network pressure. In another deployment mode, the network dynamic route advertisement is not implemented. The advertisement is implemented by means of route re-distribution. In OSPF routing mode, the redistribute connected subnets are configured, so that the device does not send the OSPF hello packet to all sub VLANs. The route is only advertised to the directly-connected L3 physical ports.

Q20: Why does the SA prompt "You are not in the permitted range. Please confirm your rights" during 802.1x authentication?

A. If this information is prompted, you can choose Start > Run. Enter cmd > ipconfig /release > ipconfig /renew. The client obtains an IP address again. Then, you can perform the 802.1x authentication. The reason is: After the network reconstruction,

an IP address in a new network segment is assigned. However, the client does not learn the address change and still uses the old IP address dynamically acquired to perform 802.1x authentication. As a result, the system fails the 802.1x authentication. To address this issue, you can manually enable the client to acquire an IP address in the new network segment.

Q21: Does the active/standby switchover of hot backup management boards affect the authenticated services? Can the non-authenticated user successfully pass the authentication and get online?

A: Currently, the VSU hot backup switchover has the following limitations:

1) In dual-management board deployment mode, if the active and standby management boards are switched over (3-4 minutes are cost from switchover start to the display of the CLI of the new management board), you cannot perform 802.802.1x authentication within one minute before the hot backup switchover, which ensure non-interrupted data flow of online users. During the switchover, because the 802.1x-dependent modules need to be initialized, other parts of the system, for example, underlying and related channels cannot get ready soon. Therefore, within one minute before the hot backup switchover, the 802.1x authentication cannot be implemented. This issue will be addressed in later solutions.

2) In dual-management board deployment mode, if the active and standby management boards are switched over (3-4 minutes are cost from switchover start to the display of the CLI of the new management board), you cannot connect to the network within two minutes after the hot backup switchover, although the 802.1x authentication is passed. This is because of a restraint of the SS framework. Within a short period after the active/standby switchover, the interaction of the PI and SS on the control plane is shielded (tens of seconds to two minutes, which is subject to the configuration). The newly-authenticated online user cannot access the network within two minutes after the active/standby switchover. However, the services are not affected. This issue will be addressed in later solutions.

Q22: How does the system perform user migration?

The station move is disabled:

- The re-authentication process is applicable to the 802.1x authentication.
- The re-authentication process is applicable to the web authentication.

The station move is enabled:

- 802.1x authentication
  - When the IP addresses before and after migration are the same, the network access is available without re-authentication. When the IP addresses before and after migration are different, the authentication is performed again.
- Web authentication
  - The authentication page pops up again, and re-authentication is required.

› the command **web-auth station-move auto** is enabled. When the IP addresses before and after migration are the same (the IP addresses are in the same super VLAN), the network access is available without re-authentication. When the IP addresses before and after migration are different, the authentication is performed again.

Application scenario:

- The user migration is mainly applicable to the wireless terminals. The user migration does not require repeated authentication, which improves customer experience.

Precautions:

- Before and after migration, the IP addresses should be in the same super VLAN.
- Before and after migration, the IP allocation policy based on the AM rules should remain unchanged. That is, the IP addresses before and after migration should remain unchanged. Otherwise, the migration fails.

Q23: How to avoid ARP spoofing on the simplified campus network?

The users are isolated on Layer 2 to avoid ARP and DHCP snooping.

- Access isolation: The **protected interfaces** of all access devices are enabled to avoid L2 interworking.
- QinQ isolation: The inner VID and outer VID are used to isolate the broadcast domain of the users to avoid L2 interworking.

Automatically binding a static ARP entry to an authenticated user on the N18K

- The authenticated user is automatically binding a static ARP entry on the N18K. If the user IP address is changed after authentication, the communication fails.

Q24: How to handle the issue that the addresses in the DHCP pool are exhausted?

DHCP DOS Attack

- The terminal sends a large number of DHCP requests to attack the N18000 (including the terminal loop), which exhausts the IP addresses in the DHCP pool on the DHCP server.
- Currently, the usage of the DHCP pool can be monitored by reading the MIB information using the network management software.
- In later versions that support the NFPP function, the attackers can be isolated based on the VIDs, to avoid the DOS attack.

Q25: How to configure the straight-through VLAN?

In order to bypass the straight-through VLAN, which vlan should be configured to bypass , super VLAN or sub VLAN?

- The pass-through VLAN ID of the straight-through VLAN is configured based on the sub VLAN.

What is a typical application scenario of the straight-through VLAN

- Capwap tunnel VLAN, wireless 802.1x VLAN, management VLAN, or special service VLAN, for example, video surveillance or all-in-one card.

What are precautions for straight-through VLAN configurations?

- In **access isolation**, the number of straight-through VLANs cannot exceed 200.
- In **QinQ isolation**, the number of straight-through VLANs used for non-user services cannot exceed 200. The PE-VLAN of the user services should not be configured as a straight-through VLAN.

Q26: Is the VLAN of the CE-VLAN in QinQ isolation mode mandatory?

Principles of QinQ dual-layer tag termination performed by the N18K are as follows:

- The class-id is used to identify the CE-VLAN, and the traditional VLAN is used to identify the PE-VLAN.
- When a packet sent by the terminal arrives the N18K device, it carries a two-layer tag. In the host routing information internally delivered by the N18K device, the tag contains two layers, in which the outer-layer tag indicates the VLAN tag (PE-VLAN) corresponding to the L3 interface, and the inner-layer tag indicates the private VLAN tag (CE-VLAN).

Is the VLAN ID of the CE-VLAN mandatory?

- For the CE-VLAN, only the CE-VLAN ID terminated by the QinQ needs to be configured. By default, the system considers that the CE-VLAN mapping is completed for the class-id.

Q27: What is the function of the radius-server attribute nas-port-id format qinq command?

The radius-server attribute nas-port-id format qinq command has the following functions:

- After this command is configured, the authentication and accounting packets sent by the N18K device and the SAM server carry two-layer VIDs.
- Upon searching the two-layer VID, the SAM server displays the star topology and locates the user port.

This command should be disabled in the following situations:

- The SAM version is earlier than V3.98, that is, the QinQ is not supported. This command cannot be enabled on the N18K device because the authentication packets that contain two-layer tags may not be identified by the SAM server, resulting in an authentication failure. The following command should be used:

Q28: Why does the MTU need to be modified in QinQ isolation scenario?

The reason is as follows:

- In the QinQ scenario, the distribution device adds a two-layer tag to a packet. Compared with the default MTU 1518 on the Ethernet, a four-byte tag is added. To facilitate operation and ensure redundancy, the MTU is uniformly changed to 1530.

Which devices and interfaces need to modify the MTU?

- The MTUs of the core interfaces of the upstream aggregation devices and core aggregation interfaces should be set to 1530.

Q29: DHCP Address Management (AM) rules

Functions of the AM rules:

- The AM rules are used to allocate network segments based on VLANs and ports.
- One DHCP pool can be configured with only one network range, which cannot satisfy the refined address management, especially in the super VLAN deployment scenario on the simplified network.
- Compared with the DHCP pool, the configurations of the AM rules are simple and achieve better effects with less command lines.

Is the AM rule mandatory for the DHCP pool?

- No. It is suggested to configure the AM rule for the DHCP pool.

Can part of the DHCP pools use the AM rule while the other part uses the traditional mode?

- Not available in the earlier versions. Once the AM rule is configured for a DHCP pool, all DHCP pools on the network should be configured with the AM rule. Otherwise, addresses cannot be applied. This is a defect of the solution.
- This issue is addresses in the version 11.0(1)B2 Build(10) released in early October. In this way, both AM rules and traditional rules can co-exist. Therefore, the AM rule configuration for the DHCP pool is not limited.

How to configure the VLAN that adopts the AM rule in DHCP relay scenario or no switchport scenario?

- The VLAN of the AM rule is set to the service sub VLAN of the user.
- In no switchport scenario, the VLAN matching is unavailable. Only port matching is available.

Q30: What is the mechanism for avoiding IP and IPv6 conflict in the isolation scenario?

- To detect the IPv4 and IPv6 address conflict, the address conflict detection of the IPv4-based host relies on the free ARP broadcast, and the address conflict detection of the IPv6-based host relies on the DAD broadcast mechanism.
- The N18000 adopts the ARP and ND proxy mechanism to address the address conflict issue. When the address in the ARP request sent by a terminal conflicts with the static ARP address or ND address generated in the authentication on the N18000, the N18000 sends gratuitous ARP and ND packets on behalf of the conflicted terminal.
- In gateway mode, the mechanism is enabled by default without using other commands.

Q31: How to prevent a successfully authenticated user from modifying the IP address?

When the IP address is modified by a successfully authenticated user:

- In 802.1x authentication mode, the client automatically triggers the re-authentication.
- In web authentication mode, the user cannot obtain the ARP information from the gateway.so user is disconnected. Administrator has to configure static ARP entry on gateway to match the user 's new IP address and MAC address

Q32: What is the ARP proxy mechanism after the authentication is enabled on the N18K device?

In the web authentication scenario on the N18K, the ARP proxy mechanism is as follows:

- The N18K sends the ARP requests to users only in the authentication-exempt VLANs.
- After a user is successfully authenticated, a static ARP entry is generated.
- In the VLAN that requires authentication, only when the authentication-exempt user actively initiates an ARP request, the N18K device generates an ARP entry for the authentication-exempt user.

Precautions for ARP proxy mechanism planning:

- This type of terminals should be uniformly planned in the authentication-exempt VLAN.

Q33: Both http redirect direct-site 1.1.1.1 and web-auth direct-host 1.1.1.1 Are Configured for Authentication-free Access to IP Addresses. What Are Their Differences?

A: The direct-site command is used to let packets destined for a specified destination IP address to pass. For example, if the command is executed to configure authentication-free access to a SAM server, users can access the IP address of the SAM server without authentication.

The direct-host command is used to let packets from a specified source IP address to pass. For example, if this command is executed to configure authentication-free access to a printer, the printer can be accessed without authentication. Nevertheless, users need to be authenticated but authentication is not required for the printer. If a user needs to be accessed without authentication, the direct-site command needs to be configured for the IP address of the user.

Q34: How Can I Import an Electronic Certificate to the N18000K?

Steps given by R&D to import certificate to N18K.

Plan to replace the expired certificate on N18K to test whether the HTTPS redirection can be improved or ignored.

The generated cert (SCN-N18K.crt & SCN-N18K.key) copied to USB key and plug into N18K CM. The certificate must be in ASCII (Base64) format, usually the file can be opened with noted pad and prefixed with a "—— BEGIN …" line.

```
#run-system-shell
#cd /tmp/vsd/0/security/webauth/
#cp /mnt/sub/0/SCN-N18K.crt httprdsrv.pem
#chmod 777 httprdsrv.pem
#cp /mnt/usb/0/SCN-N18K.key httprdkey.pem
#chmod 777 httprdkey.pem
#sync
#pkill -9 wbamain
```

Q35: How Can I Complete Escape Settings on Simplified RADIUS?

In order for Radius authentication bypass when the SAM(Radius) service down or not available, below are the command to configure in order the bypass authentication, based on the test in XLAB UM.

```
aaa authentication dot1x default group radius none
aaa authentication web-auth default group radius none

radius-server timeout 1
radius-server deadtime 1
radius-server retransmit 1
```

In the even radius escape, all user will be able to access to internet without proper authentication been done, which mean in the web-authen, any user id (known/unknown) will be authenticated successfully. If dot1x authentication enabled on the interface, new online user will be authenticated via the dot1x.

In order to view the full list of connected user when the radius(SAM) not available, should check with the 2 commands below.

```
show web-auth user all --> web-authen user
show dot1x summary  --> dot1x authen user
```

Q36: What Are Precautions for Configuring the Simplified Solution — N18000K?

The CPP rate limit needs to be configured after HTTPS is enabled.

1. On the N18000K of the latest version, HTTPS performance is optimized, the CPU resource utilization of HTTPS and HTTP is separated in an optimized manner so that HTTPS and HTTP do not affect each other. You can enable HTTPS redirection as required. The CPP rate limit must be configured for HTTPS.

```
Ruijie(config)#http redirect port 443
Ruijie(config)#cpu-protect type web-auths bandwidth 2000
```

2. After DHCP snooping is enabled, **check-giaddr** needs to be configured to solve the problem that a device fails to obtain an IP address when both DHCP snooping and DHCP relay are configured on the device.

```
ip dhcp snooping
ip dhcp snooping check-giaddr
```

3. After RADIUS escape is configured, the default parameter values need to be adjusted, to prevent misjudgment and jitter caused by the high detection sensitivity.

```
radius-server host (radius ip) test username (user-name) idle-time 2 key (radius key)
radius-server dead-criteria time 120 tries 12
```

4. After RADIUS escape is configured, relevant configuration needs to be applied to ports. Check whether the configuration is complete.

```
dot1x critical
dot1x critical recovery action reinitialize
```

5. Certified migration is configured differently now: ARP detection needs to be enabled on the N18000K and ARP proxy needs to be disabled on the AC.

```
N18K(config)#web-auth station-move arp-detect
N18K(config)#dot1x station-move arp-detect
AC(config)#no proxy_arp enable
```