Contents

1 Configuring Web Authentication

1.1 Introduction

1.1.1 Overview

Web authentication is an identity authentication method for controlling users' network access permissions. When an unauthenticated user attempts to access the Internet through a browser, the network access server (NAS) forcibly redirects the browser to a specified site (portal server). The user can access services of the portal server without authentication. If the user wants to access network resources beyond the portal server, the user must pass through authentication.

Web authentication has the following advantages:

- Convenient to use: Users do not need to install dedicated client software and can complete authentication through a browser.
- Personalized services and service extension: Through interaction between the browser and the portal server, users can customize services, such as advertisements, notifications, and business links on the portal server page.

1.1.2 Principles

1. Basic Concepts

- Authentication client

  Generally, an authentication client refers to a browser running Hypertext Transfer Protocol (HTTP). When a user accesses the Internet via a browser, the browser will send HTTP requests.

- NAS

  Generally, the NAS refers to an access-layer device in a network. It is directly connected to user hosts and needs to be enabled with web authentication.

- Portal server

  The portal server provides the web authentication page to interact with user hosts.

- RADIUS server

  The RADIUS server provides RADIUS-based remote user authentication.

- HTTP interception

  HTTP interception means that the NAS intercepts to-be-forwarded HTTP packets.

  These HTTP packets are sent by the browsers of the user hosts connected to the NAS but they are not destined for the NAS. For example, a user accesses www.google.com via the Internet Explorer (IE). The NAS is supposed to forward the HTTP request packets from the user to the gateway. If HTTP interception is enabled, these packets will not be forwarded.

  HTTP interception is the foundation of web authentication. Web authentication is triggered automatically once HTTP interception succeeds.

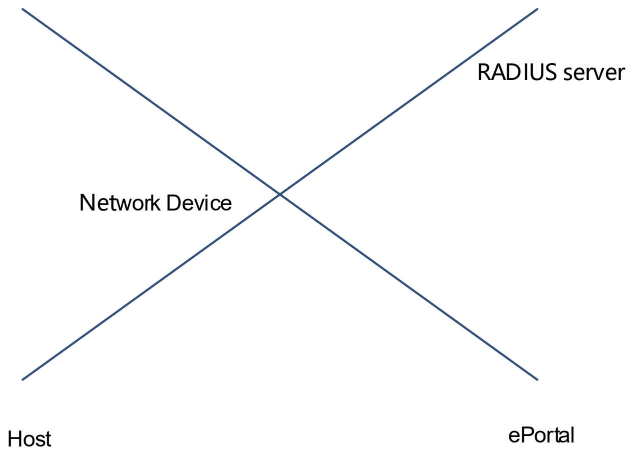
- HTTP redirection

  In normal cases, after a user host sends an HTTP GET or HEAD request through a browser, the receiver responds with a 200 response if it can provide resources and a 302 response if it cannot provide resources. The 302 response provides a new site path. After receiving the response, the user host can send an HTTP GET or HEAD packet to the new site to request resources. This is called redirection.

2. Web Authentication Solutions

Orion web authentication has multiple versions that use different web authentication processes. Currently, Orion first-generation and second-generation web authentications are supported. You can select a version based on your actual requirements.

Figure 1-1Typical Networking for Web Authentication



- Orion first-generation web authentication

  Orion first-generation web authentication requires cooperation of the Orion dedicated ePortal server. The ePortal server provides the authentication and accounting functions, which relieves the NAS from service burden.

  The authentication process is as follows:
  A user submits authentication information through the authentication page provided by the ePortal server.
  The ePortal server initiates an authentication request to the RADIUS server.
  After authentication succeeds, the ePortal server sends the user information to the NAS through Simple Network Management Protocol (SNMP).
  The NAS controls user access permissions.

- Orion second-generation web authentication

  Orion second-generation web authentication. The portal server is responsible for interaction on the user page only and is easily compatible with products of different vendors. However, the main authentication process is performed on the NAS, and therefore higher requirements are raised for the NAS.

  The authentication process is as follows:
  A user submits authentication information through the authentication page provided by the portal server.
  The portal server informs user identity information to the NAS through the portal protocol. The NAS initiates

an authentication request to the RADIUS server using the identity information, assigns access permissions to authenticated users, and returns authentication results to the portal server.

- Web authentication solutions

Table 1-1Web Authentication Solutions

		Orion First-Generation Web Authentication	**Orion Second-Generation Web Authentication**
Authentication roles	Client	In these two authentication solutions, clients have the same functions.	
	NAS	The NAS redirects users and exchanges user online/offline notifications with the portal server.	The NAS redirects and authenticates users, and notifies the portal server of the authentication results.
	Portal server	The portal server interacts with clients through the authentication page, authenticates users, and notifies the NAS of the authentication results.	The portal server interacts with clients through the authentication page, notifies the NAS of users' authentication information, and receives the authentication results from the NAS.
	RADIUS server	In these two authentication solutions, the RADIUS servers have the same functions.	
Authentication process	Authentication and accounting	The portal server initiates authentication and accounting to the RADIUS server.	The NAS initiates authentication and accounting to the RADIUS server.
Offline process	Offline action	An offline action may be triggered by a notification from the portal server and traffic detection or port status detection performed by the NAS.	An offline action may be triggered by a notification from the portal server, a kickout notification from the RADIUS server, and traffic detection or port status detection performed by the NAS.
	Accounting completion packet	Accounting completion packets are initiated by the portal server.	Accounting completion packets are initiated by the NAS.

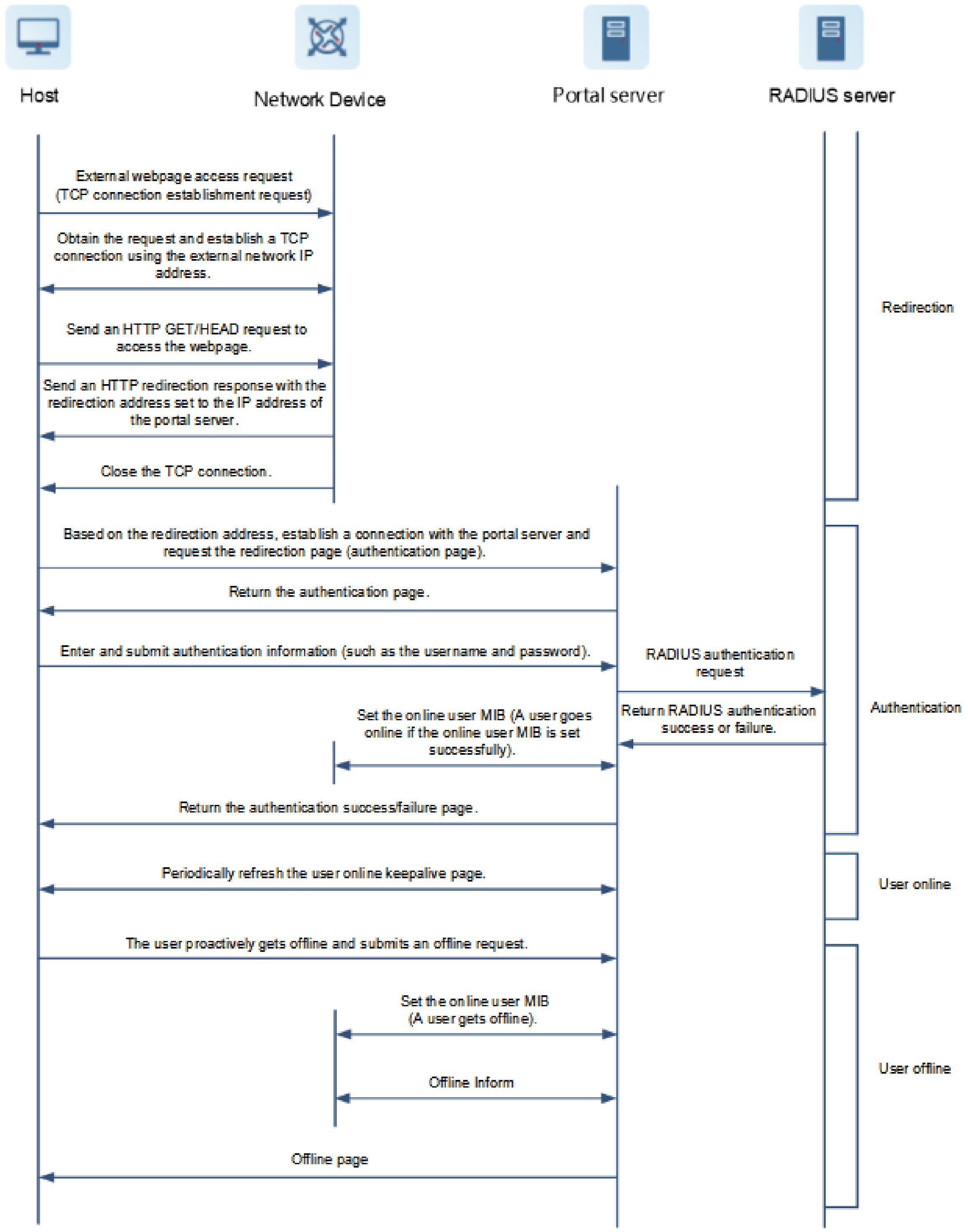
Instruction

- The web authentication solution is selected based on the type of the portal server in use.

- Some parameters can be shared by different web authentication solutions but some are not. Distinguish these parameters carefully to avoid abnormal web authentication due to parameter misconfiguration.

3. Orion First-Generation Web Authentication

Figure 1-1Flowchart of Orion First-Generation Web Authentication


Host
Network Device
Portal server
RADIUS server
External webpage access request (TCP connection establishment request)
Obtain the request and establish a TCP connection using the external network IP address.
Send an HTTP GET/HEAD request to access the webpage.
Send an HTTP redirection response with the redirection address set to the IP address of the portal server.
Close the TCP connection.
Redirection
Based on the redirection address, establish a connection with the portal server and request the redirection page (authentication page).
Return the authentication page.
Enter and submit authentication information (such as the username and password).
RADIUS authentication request
Return RADIUS authentication success or failure.
Set the online user MIB (A user goes online if the online user MIB is set successfully).
Authentication
Return the authentication success/failure page.
Periodically refresh the user online keepalive page.
User online
The user proactively gets offline and submits an offline request.
Set the online user MIB (A user gets offline).
Offline Inform
Offline page
User offline

As shown in Figure 1-1, the Orion first-generation web authentication process includes four phases: redirection, authentication, user online, and user offline.

(1) Redirection

Before authentication, the NAS intercepts all HTTP requests from unauthenticated users and redirects these requests to the portal server. An authentication page is displayed on the browser of a user.

(2)Authentication

During authentication, the user enters information, for example, the username, password, and verification code on the web authentication page to interact with the portal server and complete authentication.

(3)User online

After the user succeeds in the authentication, the portal server notifies the NAS that the user has been authenticated. The NAS allows the user to access Internet resources.

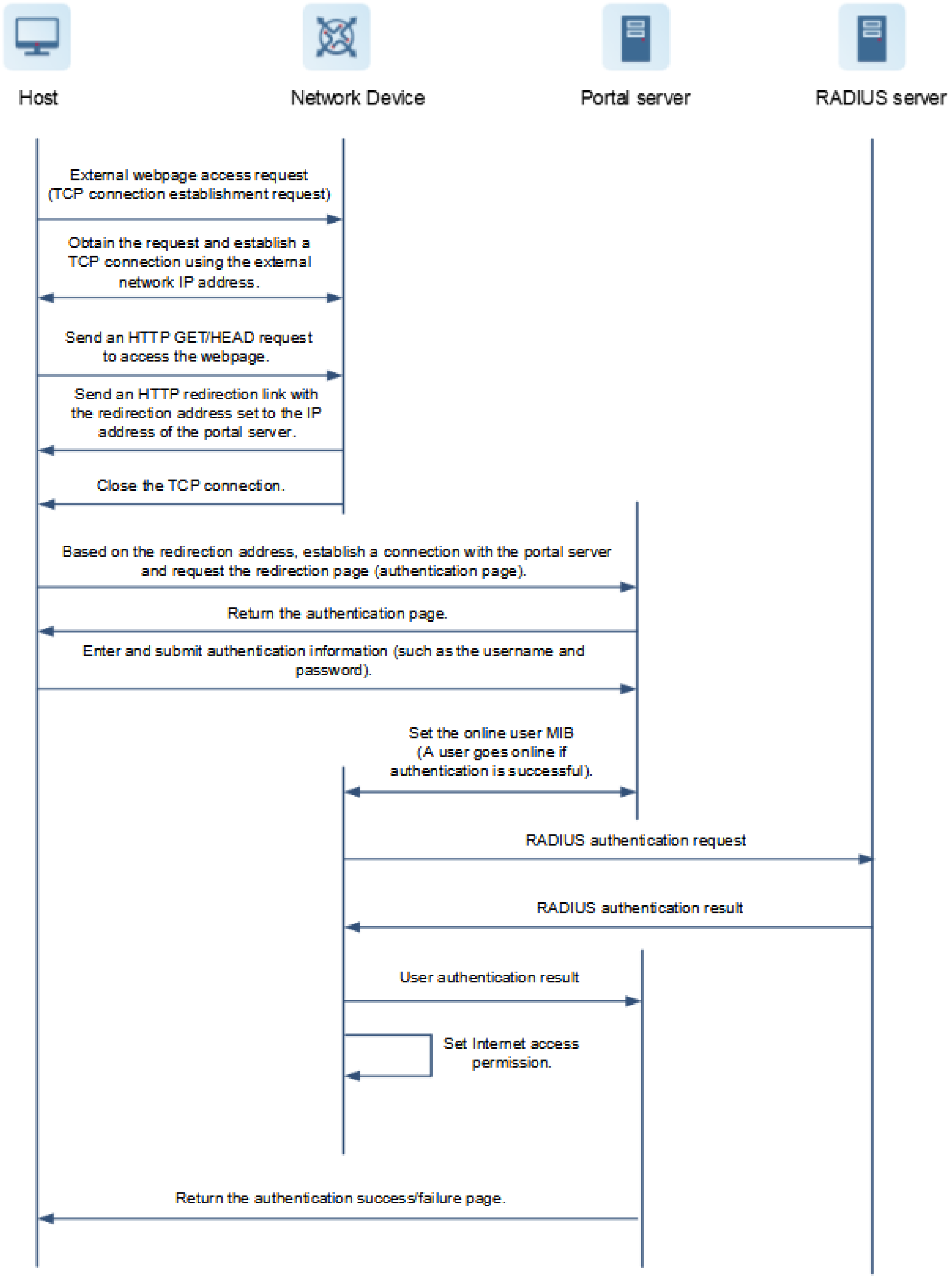
(4)User offline

After the user gets offline, the portal server sends an accounting completion request to the RADIUS server and notifies the RADIUS server that the user has gotten offline. There are two user offline detection types:

- The NAS detects offline of a user when the user's time is due, the data quota is reached, or the link is disconnected. The NAS will notify the portal server of a user offline message. After receiving the message, the portal server requires the NAS to delete user information through SNMP and returns the offline page to the user host.
- The portal server detects getting offline of a user when the user triggers an offline request through the offline page or the keepalive page becomes invalid. The portal server notifies the NAS of a user offline message and returns the offline page to the user host.

4. Orion Second-Generation Web Authentication

Figure 1-1Flowchart of Orion Second-Generation Web Authentication


Host
Network Device
Portal server
RADIUS server
External webpage access request (TCP connection establishment request)
Obtain the request and establish a TCP connection using the external network IP address.
Send an HTTP GET/HEAD request to access the webpage.
Send an HTTP redirection link with the redirection address set to the IP address of the portal server.
Close the TCP connection.
Based on the redirection address, establish a connection with the portal server and request the redirection page (authentication page).
Return the authentication page.
Enter and submit authentication information (such as the username and password).
Set the online user MIB (A user goes online if authentication is successful).
RADIUS authentication request
RADIUS authentication result
User authentication result
Set Internet access permission.
Return the authentication success/failure page.

- Authentication process

aBefore authentication, the NAS intercepts all HTTP requests from unauthenticated users and redirects these requests to the portal server. An authentication page is displayed on the browser of a user.

bThe user enters authentication information, such as the username, password, and verification code on the authentication page to interact with the portal server.

cThe portal server sends the user authentication information to the NAS.

dThe NAS initiates authentication to the RADIUS server and returns the authentication result to the portal server.

eThe portal server displays the authentication result (success or failure) to the user on a page.

- User offline

  There are two user offline detection types: (1) The NAS detects offline of a user when the user's time is due, the data quota is reached, or the link is disconnected. (2) The portal server detects offline of a user when the user triggers an offline request through the offline page.

  Common offline scenarios are as follows:

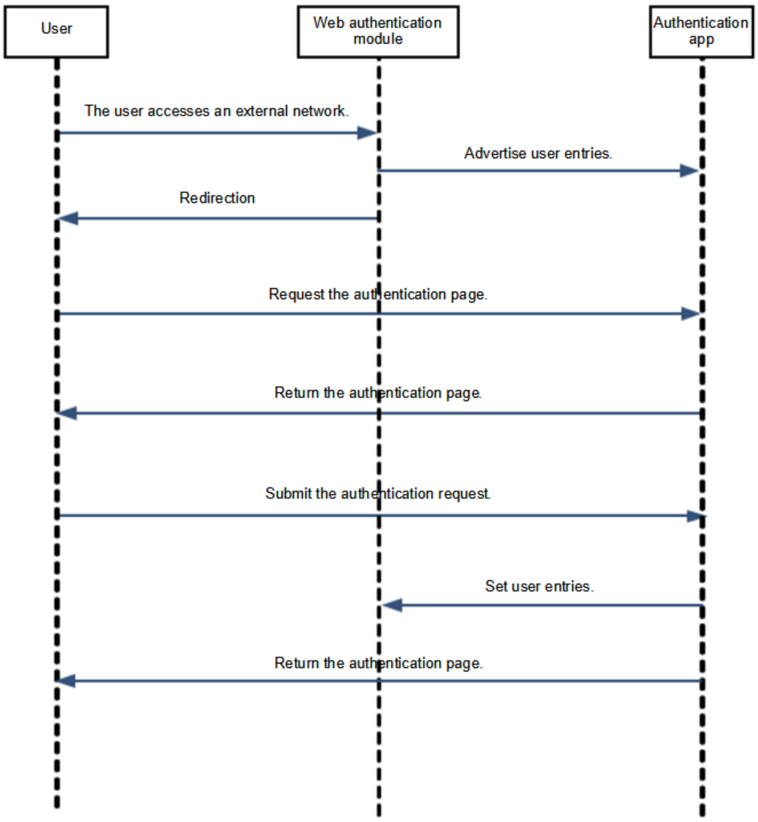
  - When a user clicks the Logout button on the page, the portal server instructs the NAS to get the user offline.
  - The NAS forces a user offline when detecting that the traffic of the user is lower than the threshold, depending on the configured traffic threshold detection parameter.
  - When the RADIUS server plans to force a user offline based on a certain policy, the NAS instructs the portal server to push an offline page to the user host.

5. App-based Authentication

App-based authentication is actually performed by a third-party app. The web authentication module is not responsible for authentication. It serves as an agent to connect the user host and authentication app.

- Main roles
  - User host: user host to be authenticated when accessing network resources.
  - Webauth: web authentication component that is responsible only for redirection and user entry settings and not for interaction with the server.
  - Authentication app: performs authentication.
- Authentication process

Figure 1-1Flowchart of App-based Web Authentication


User
Web authentication module
Authentication app
The user accesses an external network.
Advertise user entries.
Redirection
Request the authentication page.
Return the authentication page.
Submit the authentication request.
Set user entries.
Return the authentication page.

As shown in Figure 1-1, the authentication app interacts with the server, and the web authentication component does not need to care about the internal authentication process of the authentication app. In the preceding figure, the portal server role is not provided. The app-based authentication process is as follows:

aA user host accesses an external network and triggers HTTP redirection. Webauth creates a user and advertises it to the authentication app.

bThe user host accesses the redirection page.

cThe user submits an authentication request on the login page.

dThe authentication app authenticates the user. After authentication succeeds, the authentication app sends a message to Webauth to allow packets from the user to pass through.

eThe authentication app returns the authentication result to the user host.

1.1.3 Protocols and Standards

- RFC1945: Hypertext Transfer Protocol -- HTTP/1.0
- RFC2068: Hypertext Transfer Protocol -- HTTP/1.1
- RFC2818: HTTP Over TLS
- RFC1157: Simple Network Management Protocol (SNMP)
- RFC2865: Remote Authentication Dial In User Service (RADIUS)
- RFC2866: RADIUS Accounting
- RFC3576: Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)

1.2 Restrictions and Guidelines

- Different web authentication versions are highly divergent in the authentication processes and configurations. Read the relevant chapters carefully before configuring functions related to web authentication to prevent misconfiguration.
- Orion second-generation web authentication supports local account authentication on the NAS. Because RADIUS authentication is more commonly used in networks, it is generally used in application examples.
- Web authentication supports the authentication of domain names. That is, accounts can be authenticated in the format of user name@domain name. This requires enabling the domain-name-based authentication, authorization and accounting (AAA) service. For details, see "Configuring AAA" in the *Security Configuration Guide*.

1.3 Configuration Task Summary

Web authentication configuration includes the following tasks:

(1)Configure basic web authentication functions. Select any of the following configuration tasks to configure.

- Configuring Orion First-Generation Web Authentication
- Configuring Orion Second-Generation Web Authentication
- Configuring App-based Authentication

(2)(Optional) Configure web authentication template attributes. Perform the following optional configuration tasks as required.

- Configuring an Authentication Method List
- Configuring an Accounting Method List
- Configuring the Portal Communication Destination Port
- Configuring the Binding Mode

(3)(Optional) Configure parameters for communicating with the portal server. Perform the following optional configuration tasks as required.

- Configuring the Redirection HTTP Port
- Configuring the Redirection Connection Timeout Time
- Configuring Portal Detection
- Configuring Portal Escape
- Configuring the Portal Communication Source Port
- Disabling Portal Specification Extension

(4)(Optional) Configure authentication-free resources. Perform the following optional configuration tasks as required.

- Configuring the Authentication-Free Network Resource Range
- Configuring a Straight-through ARP Resource Range
- Configuring an Authentication-Exempted User Range

(5)(Optional) Configure user management functions. Perform the following optional configuration tasks as required.

- Configuring Logging of the Web Authentication Module
- Configuring the Maximum Number of HTTP Sessions for Unauthenticated Users

- Configuring the Interval for Updating Online User Information
- Enabling DHCP Address Check
- Configuring an Address Whitelist
- Configuring VLAN-based Authentication on a Port
- Configuring the Authenticated User Logout Delay on a Port
- Enabling RADIUS Server Escape
- Configuring DHCP Server Detection
- Configuring Uniqueness Check of Portal Authentication Accounts
- Enabling Automatic Adding of Domain Information After Usernames

(6)(Optional) Configure other functions. Perform the following optional configuration tasks as required.

- Configuring Transparent Transmission of RADIUS Private Attributes
- Configuring HTTPS Certificate Import
- Enabling Adding the Authentication Page to Favorite
- Configuring a Template Mapping Method

1.4 Configuring Orion First-Generation Web Authentication

1.4.1 Overview

After Orion first-generation web authentication is enabled, unauthenticated users will be redirected to the authentication page for authentication.

When an unauthenticated user attempts to access network resources, the NAS redirects the user to the authentication page, where the user can initiate authentication to the portal server.

1.4.2 Restrictions and Guidelines

- To apply web authentication successfully, you need to configure and apply a portal server.
- To apply web authentication successfully, you need to configure the key used for the communication between the access or convergence device and the portal server.
- To apply web authentication successfully, you need to configure the SNMP parameters used for the communication between the NAS and portal server. For more information about SNMP, see "Configuring SNMP" in the *Network Management and Monitoring Configuration Guide*.
- When the access or convergence device finds an unauthenticated user attempting to access network resources through HTTP, it redirects the access request to the specified portal authentication page, where the user can initiate authentication to the portal server. Unauthenticated users can directly visit the IP address of the portal server only if the IP address is configured as an authentication-free network resource.
- When web authentication is enabled in interface configuration mode, it is disabled by default. Web authentication is not performed on user hosts connected to the port.

1.4.3 Prerequisites

Valid to-be-authenticated user information is configured on the RADIUS server. For details about configuration of to-be-authenticated user information, see the user manual of the RADIUS server.

1.4.4 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

(4)Create a first-generation web authentication template and enter the template configuration mode.

web-auth template eportalv1

(5)Configure parameters for interaction between the NAS and portal server.

aConfigure the IP address and virtual routing and forwarding (VRF) instance of the portal server.

ip [*ip-address* | **oob** | **vrf** *vrf-name*]

No portal server IP address or VRF instance is configured by default.

After this command is configured, the NAS allows server access requests and can set a rate limit for requests sent to the server.

bConfigure the authentication page address of the portal server.

url *url-string*

No authentication page address of the portal server is configured by default.

The URL to which a user is redirected is usually the authentication page address of the portal server.

cConfigure the URL format of redirection packets.

fmt { **ace** | **default** }

The Orion URL format is used for redirection packets by default.

Access control entry (ACE) association is supported when **fmt** is set to **ace**.

dConfigure the binding mode used by a template.

bindmode { **ip-mac-mode** | **ip-only-mode** }

The default binding mode used by a template is IP address+MAC address.

eConfigure the encapsulation format of redirection packets.

redirect { **http** | **js** }

Redirection packets of the Orion URL format use the JavaScript (JS) encapsulation format, and redirection packets of CMCC-related URL formats use the HTTP encapsulation format by default.

Some apps cannot execute JS actions, and packets need to be encapsulated in HTTP format to trigger redirection.

(6)Return to the global configuration mode.

exit

(7)Configure the communication key between the NAS and the portal server.

web-auth portal key *key*

No communication key between the NAS and the portal server is configured by default.

During authentication, the communication key is used to encrypt some data exchanged between the NAS and portal server to improve security.

(8)Configure SNMP parameters.

The NAS and portal server use SNMP to manage users to be authenticated. SNMPv2 and SNMPv3 are available.

SNMPv2 is used as an example here. If high security requirements are raised, you are advised to use SNMPv3.

aConfigure the SNMP community string on the NAS for the portal server to manage online users on the NAS.

snmp-server community { *community-string* } **rw**

The portal server uses the SNMP community string to read/write user information from/to the NAS.

bConfigure the SNMP server.

snmp-server host { *ip-address* } **inform version 2c** { *community-string* } **web-auth**

The NAS sends Inform/Trap packets to notify the portal server of user offline.

cEnable the Webauth Trap/Inform function.

snmp-server enable traps web-auth

The Webauth Trap/Inform function is configured to enable the NAS to inform the portal server of user offline.

(9)Enter the interface configuration mode.

interface *interface-type interface-number*

(10)Enable first-generation web authentication on a port.

web-auth enable

The web authentication function is disabled on a port by default.

1.5 Configuring Orion Second-Generation Web Authentication

1.5.1 Overview

After Orion second-generation web authentication is enabled, unauthenticated users will be redirected to the authentication page for authentication.

When an unauthenticated user attempts to access network resources, the NAS redirects the user to the authentication page, where the user can initiate authentication to the portal server.

1.5.2 Restrictions and Guidelines

Orion second-generation web authentication complies with the *CMCC WLAN Service Portal Specification*. Furthermore, it is extended to support the Orion ePortal server. In actual deployment, compatible configuration is required based on the server performance.

1.5.3 Prerequisites

Authenticated user information is configured on the RADIUS server. For details about user information configuration on the RADIUS server, see the configuration guide of the RADIUS server.

1.5.4 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable AAA security services.

aaa new-model

The AAA security services are disabled by default.

In Orion second-generation web authentication, the NAS initiates authentication to the portal server through the AAA module.

(4)Configure the address, port number, and key of the RADIUS server.

radius-server host { *ipv4-address* | *ipv6-address* } [**auth-port** *auth-port-number*] [**acct-port** *acct-port-number*] [**key** [**0** | **7**] *text-string*]

No RADIUS server IP address, port number, or key is configured by default. The default authentication port is **1812** and the default accounting port is **1813**.

Users' account information is stored on the RADIUS server. The NAS needs to connect to the RADIUS server to validate a user.

(5)Configure a second-generation web authentication method list.

aaa authentication web-auth { **default** | *list-name* } { [**group** *group-name*]&<1-4> | **group radius** | **local** | **none** } *

No second-generation web authentication method list is configured by default.

A web authentication method list associates web authentication requests with the RADIUS server. The NAS selects an authentication method and a server based on the web authentication method list.

(6)Configure a network accounting method list.

aaa accounting network { **default** | *list-name* } **start-stop** { [**group** *group-name*]&<1-4> | **group radius** | **group tacacs+** | **none** } *

The web accounting function is disabled by default.

An accounting method list associates an accounting method and server. In web authentication, accounting is implemented to record user information or fees.

(7)Create a second-generation web authentication template and enter the template configuration mode.

web-auth template eportalv2

(8)Configure web authentication template parameters.

aConfigure an authentication method list for the template.

authentication *method-list*

The default authentication method list is used by a template by default.

bConfigure the accounting method list used by a template.

accounting *method-list*

The default accounting method list is used by a template by default.

cConfigure the IP address and VRF instance of the portal server.

ip [*ip-address* | **oob** | **vrf** *vrf-name*]

No portal server IP address or VRF instance is configured by default.

dConfigure the authentication page address of the portal server.

url *url-string*

The authentication page address of the portal server is configured by default.

When you configure the URL of the second-generation portal server, if the URL contains an IPv6 address, enclose it with a pair of square brackets. For example, when the IPv6 address is 2001::1, the actual configured URL is http://[2001::1]/index.jsp. The IPv6 template does not support **fmt** configuration.

eConfigure the URL format of redirection packets.

fmt { **cmcc-ext1** | **cmcc-ext2** | **cmcc-ext3** | **cmcc-mtx** | **cmcc-normal** | **ct-jc** | **cucc** | **default** }

The Orion URL format is used for redirection packets by default.

When **fmt** is set to **cmcc-normal** or **cmcc-ext1**, only the IPv4 format is supported.

fConfigure the binding mode used by a template.

bindmode { **ip**-**mac**-**mode** | **ip**-**only**-**mode** }

The default binding mode used by a template is IP address+MAC address.

gConfigure the encapsulation format of redirection packets.

redirect { **http** | **js** }

Redirection packets of the Orion URL format use the JS encapsulation format, and redirection packets of the CMCC-related URL formats use the HTTP encapsulation format by default.

(9)Return to the global configuration mode.

exit

(10)Configure the communication key between the NAS and the portal server.

web-auth portal key *key*

No communication key between the NAS and the portal server is configured by default.

(11)Enter the interface configuration mode.

interface *interface-type interface-number*

(12)Enable second-generation web authentication on a port.

web-auth enable eportalv2

1.6 Configuring App-based Authentication

1.6.1 Overview

The authentication app can interwork with the web authentication component to redirect unauthenticated users to the authentication page for authentication.

1.6.2 Restrictions and Guidelines

In template configuration mode, the authentication app name must be correctly configured.

1.6.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Create an app-based authentication template and enter the template configuration mode.

web-auth template appauth

(4)Configure the authentication app name in the template.

app-name { **APP_AUTH** | *app-name* }

(5)Configure attribute parameters of the app-based authentication template.

aConfigure the IP address and VRF instance of the portal server.

ip [*ip-address* | **oob** | **vrf** *vrf-name*]

No portal server IP address or VRF instance is configured by default.

bConfigure the communication port of the portal server.

port *port-number*

The default communication port of the portal server is **80**.

cConfigure the authentication page address of the portal server.

url *url-string*

The authentication page address of the portal server is configured by default, and must be started with http:// or https://.

dConfigure the binding mode used by a template.

bindmode { **ip-mac-mode** | **ip-only-mode** }

The default binding mode used by a template is IP address+MAC address.

eConfigure the encapsulation format of redirection packets.

redirect { **http** | **js** }

Redirection packets of the Orion URL format use the JS encapsulation format, and redirection packets of the CMCC-related URL formats use the HTTP encapsulation format by default.

When some apps cannot execute JS actions, packets need to be encapsulated in HTTP format to trigger redirection.

fConfigure the IP address of the NAS.

nas-ip { *ipv4-address* }

No NAS IP address is configured by default.

During app-based authentication, **nas-ip** is used only to specify the redirection URL transmitted to the portal server. If **nas-ip** is not configured, the local device address is automatically obtained based on the server IP address as **nas-ip**.

(6)Return to the global configuration mode.

exit

(7)Enter the interface configuration mode.

interface *interface-type interface-number*

(8)Enable app-based authentication on a port.

web-auth enable appauth

1.7 Configuring an Authentication Method List

1.7.1 Overview

After an authentication method list is configured, the NAS selects a server for authentication based on the specified authentication method list.

When a user submits authentication information, the portal server sends an authentication request to the NAS. The NAS resolves the authentication server and other information based on the configured authentication method list name before initiating authentication.

1.7.2 Restrictions and Guidelines

- Before you configure an authentication method list, ensure that the authentication methods in the list have been configured on the AAA module.
- The same authentication method needs to be used for IPv4 and IPv6 packets.

1.7.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the web authentication template configuration mode.

web-auth template { **eportalv2** | *template-name* **v2** }

(4)Configure an authentication method list for the template.

authentication *method-list*

The default authentication method list is used by a template by default.

1.8 Configuring an Accounting Method List

1.8.1 Overview

After an accounting method list is configured, the NAS selects a server for accounting based on the specified accounting method list.

After a user passes authentication, the NAS sends an accounting request. The recipient of the request depends on the configuration of the accounting method list and is usually the portal server.

1.8.2 Restrictions and Guidelines

- Before you configure an accounting method list, ensure that the accounting methods in the list have been configured on the AAA module.

- The same accounting method needs to be used for IPv4 and IPv6 packets.

1.8.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the web authentication template configuration mode.

web-auth template { **eportalv2** | *template-name* **v2** }

(4)Configure the accounting method used by a template.

accounting *method-list*

The default accounting method list is used by a template by default.

1.9 Configuring the Portal Communication Destination Port

1.9.1 Overview

After the portal communication destination port is configured, the NAS regards the port as the communication port of the portal server, monitors packets from the portal server over this port, and specifies this port in packets sent to the portal server.

The NAS interacts with the portal server through the portal protocol, which specifies the port number used to listen to and send/receive packets. When the NAS detects that a user gets offline, it notifies the portal server. When the portal server listening port is changed, the NAS needs to re-configure the portal server communication port.

1.9.2 Restrictions and Guidelines

- Only second-generation web authentication and app-based authentication are supported.
- The configured port number must be consistent with the port actually used by the portal server.

1.9.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the web authentication template configuration mode.

web-auth template { **eportalv2** | *template-name* **v2** | **appauth** }

(4)Configure the communication port of the portal server.

port *port-number*

The default portal server communication port is **50100** for second-generation web authentication and **80** for app-based authentication.

1.10 Configuring the Binding Mode

1.10.1 Overview

The binding mode defines the binding relationship between users and packets and is classified into the IP address binding mode and IP address+MAC address binding mode.

- In IP address binding mode, it is regarded that a packet belongs to a user if the IP address in the packet is the same as that of the user.
- In IP address+MAC address binding mode, it is regarded that a packet belongs to a user only if the IP address and MAC address in the packet are the same as those of the user.

1.10.2 Restrictions and Guidelines

The binding mode is selected based on the user information that the NAS can obtain. If the NAS can obtain a user's IP address and MAC address, the IP address+MAC address binding mode is preferred (such as L2 network deployment). Otherwise, the IP address binding mode is preferred (such as L3 network deployment, in which the NAS cannot obtain users' MAC addresses and can obtain only the gateway's MAC address).

1.10.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the web authentication template configuration mode.

web-auth template { **appauth** | **eportalv1** | **eportalv2** | *template-name* { **app** | **v1** | **v2** } }

(4)Configure the binding mode used by a template.

bindmode { **ip-mac-mode** | **ip-only-mode** }

The default binding mode used by a template is IP address+MAC address.

1.11 Configuring the Redirection HTTP Port

1.11.1 Overview

The NAS needs to intercept HTTP packets with specified ports from users and redirect these HTTP packets to the authentication page to complete authentication. The NAS intercepts HTTP packets with destination ports 80 and 443 by default. By configuring the redirection HTTP port, the NAS can intercept HTTP packets with custom ports.

1.11.2 Restrictions and Guidelines

- The commonly used management ports on the access or convergence device, such as ports 22, 23, and 53, and ports reserved by the system are not allowed to be configured as the redirection port.
- HTTP seldom uses ports with numbers smaller than 1000 except port 80. To avoid a conflict with well-known Transmission Control Protocol (TCP) ports, do not configure a port with a small number as the redirection port.

1.11.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the redirection HTTP port.

http redirect port *port-num*

The NAS intercepts HTTP packets with port numbers 80 and 443 from users and redirects them to the authentication page by default.

A maximum of 10 different destination port numbers can be configured, excluding the default ports 80 and 443.

1.12 Configuring the Redirection Connection Timeout Time

1.12.1 Overview

HTTP redirection is implemented by establishing a TCP connection between the NAS and a user host and adding the redirection page URL to the 302 packet replied by the NAS. After a TCP connection is established between the NAS and a user host, the TCP connection is closed after the NAS receives an HTTP GET/HEAD packet from the user host and responds with an HTTP redirection packet.

The redirection connection timeout time prevents a TCP connection being occupied for a long time because the user host does not send a GET/HEAD packet. After the timeout time expires, the NAS will forcibly disconnect the TCP connection.

1.12.2 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the redirection connection timeout time.

http redirect timeout *timeout*

The default redirection connection timeout time is **3** seconds.

1.13 Configuring Portal Detection

1.13.1 Overview

The portal detection function periodically detects whether the active portal server is available. When the active portal server is unavailable, the standby server automatically takes over the services.

The portal detection methods vary depending on the web authentication solution. The simple principles are as follows:

- First-generation web authentication: The NAS attempts to establish a connection with the portal server. If the connection can be established, the NAS determines that the portal server is available.

- Second-generation web authentication: The NAS constructs and sends portal packets to the portal server. If the portal server returns response packets, the NAS determines that the portal server is available.

1.13.2 Restrictions and Guidelines

- This function is used when multiple portal servers are deployed. In this case, when the active portal server is unavailable, services are automatically switched to a standby portal server.
- This function can be configured in first-generation and second-generation web authentication. However, the detection method varies depending on the web authentication solution.

1.13.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure portal detection.

web-auth portal-check [**interval** *interval*] [**timeout** *timeout*] [**retransmit** *retransmit-times*]

Portal detection is disabled by default.

1.14 Configuring Portal Escape

1.14.1 Overview

After portal escape is configured, new users are allowed to access network resources without authentication when no portal server is available.

Configure this function if some key services in the network need to be maintained when the portal server is faulty.

1.14.2 Restrictions and Guidelines

- To use this function, you must configure portal detection.
- If multiple portal servers are configured, the escape function takes effect only when all the portal servers are unavailable.
- This function is intended only for the portal server and does not take effect to the RADIUS server.

1.14.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure portal escape.

web-auth portal-escape [**nokick**]

Portal escape is disabled by default.

If the nokick attribute is configured, the system does not force users offline when the escape function takes effect. If the nokick attribute is not configured, the system forces users offline when the escape function takes effect.

1.15 Configuring the Portal Communication Source Port

1.15.1 Overview

After the portal communication source port is configured, the NAS uses the source port to communicate with the portal server, and the used source IP address is the IP address configured on the source port.

1.15.2 Restrictions and Guidelines

Only one portal communication source port can be configured.

1.15.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the portal communication source port.

ip portal source-interface *interface-type interface-num*

No portal communication source port is configured by default.

1.16 Disabling Portal Specification Extension

1.16.1 Overview

Disabling portal specification extension is configured to support different portal servers.

Orion second-generation web authentication extends the CMCC WLAN Service Portal Specification. You need to determine whether to use the extension mode based on the server performance. If the portal server is a Orion product, enable portal specification extension. If the portal server complies with the CMCC WLAN Service Portal Specification, disable portal specification extension.

1.16.2 Restrictions and Guidelines

- Only second-generation web authentication is supported. When the NAS interworks with a portal server that complies with the CMCC WLAN Service Portal Specification, you can select multiple redirection URL formats to achieve compatibility with different servers.

1.16.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Disable portal specification extension.

no web-auth portal extension

Portal specification extension is enabled by default.

1.17 Configuring Transparent Transmission of RADIUS Private Attributes

1.17.1 Overview

After transparent transmission of RADIUS private attributes is enabled, the web authentication module uploads the private attributes delivered by the portal server to the RADIUS server and transparently transmits Orion private attributes in RADIUS authentication results to the portal server.

1.17.2 Restrictions and Guidelines

This function is used only on Orion Serverless Application Model (SAM) servers and portal servers. If the NAS interworks with a portal server provided by other vendors, you are not advised to enable this function. If this function is enabled, the portal server may not respond to packets.

1.17.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure transparent transmission of RADIUS private attributes.

web-auth portal-import attr-26

Transparent transmission of RADIUS private attributes is disabled by default.

1.18 Configuring the Authentication-Free Network Resource Range

1.18.1 Overview

Authentication-free network resources allow user access without authentication.

After web authentication or 802.1X authentication is enabled on a port, the user hosts connecting to the port need to pass authentication before accessing network resources. After the authentication-free network resource range is configured, unauthenticated users can access resources within the range without authentication.

1.18.2 Restrictions and Guidelines

The number of authentication-free network resources and the number of authentication-exempted users cannot exceed 1000. The actual number of available resources may be reduced because of other security modules. Therefore, it is recommended that network segments be configured if many addresses need to be configured.

1.18.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the authentication-free network resource range.

http redirect direct-site *ipv4-address* [*mask*] [**arp** | *port-number*&<1-8>]

No authentication-free network resource range is configured by default.

1.19 Configuring a Straight-through ARP Resource Range

1.19.1 Overview

You can configure a straight-through Address Resolution Protocol (ARP) resource range to permit the ARP packets from the specified address to pass.

When ARP check or a similar function is enabled, users cannot learn the ARP entries of the gateway or other devices, which affects user experience. You can configure this function to ensure normal ARP learning.

1.19.2 Restrictions and Guidelines

- When ARP check is enabled, you need to configure the gateway of the PCs connecting to the L2 access device as a straight-through ARP resource. If both straight-through websites and ARP resources are configured for the same address/network segment, the commands will be combined automatically. If no ARP option is specified in the straight-through website configuration, the option will be added automatically after combination.
- When ARP check is enabled, if the outbound interface address of the PC connecting to the L2 access device is not the gateway address, you need to configure the outbound interface address as a straight-through ARP resource. If multiple outbound addresses exist, configure these addresses as straight-through ARP resources.
- If ARP check is enabled, you must configure the authentication-free network resources and gateway address as straight-through ARP resources.

1.19.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure a straight-through ARP resource range.

http redirect direct-arp { *ipv4-address* [*mask*] }

No straight-through ARP resource range is configured by default.

1.20 Configuring an Authentication-Exempted User Range

1.20.1 Overview

After an authentication-exempted user range is configured, users within the range can access all reachable network resources without authentication. The authentication-exempted user range can be defined by IP address and MAC address.

The authentication-exempted user range can be used to allow special user groups that do not need permission control to access network resources.

1.20.2 Restrictions and Guidelines

The number of authentication-exempted users and the number of authentication-free network resources cannot exceed 1000. The actual number of available resources may be reduced because of other security modules. Therefore, it is recommended that network segments be configured if many addresses need to be configured.

1.20.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure an authentication-exempted user range. Configure at least one of the tasks.

- Configure the IP address range of users who do not require authentication.

  web-auth direct-host { *ipv4-address* [*ipv4-mask* | **arp**] }

- Configure the MAC address range of users who do not require authentication.

  web-auth direct-host *mac-address*

  No IP/MAC address range of authentication-exempted users is configured by default. All users can access restricted network resources only after they pass web authentication.

1.21 Configuring Logging of the Web Authentication Module

1.21.1 Overview

The logging function of the web authentication module can send log messages to the administrator to display the information and relevant events of users who get online/offline and allow users to configure a log printing rate limit.

1.21.2 Restrictions and Guidelines

When the online/offline rate is high, you can configure a rate limit for log printing. This prevents frequent log output from affecting the device performance and resulting in spamming.

1.21.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure web authentication logging.

web-auth logging enable *log-rate*

The web authentication logging function is disabled by default.

1.22 Configuring the Maximum Number of HTTP Sessions for Unauthenticated Users

1.22.1 Overview

When an unauthenticated user accesses network resources, the user's PC sends requests for HTTP session connection. The access or convergence device intercepts the HTTP packets and redirects the user to a web authentication page. To prevent an unauthenticated user from initiating too many HTTP connection requests and save resources on the NAS, you need to limit the maximum number of HTTP sessions that the unauthenticated users can initiate on the NAS.

1.22.2 Restrictions and Guidelines

- User authentication occupies one HTTP session, and other applications of a user may also need HTTP sessions. Therefore, you are not advised to set the maximum number of HTTP sessions to 1 for unauthenticated users.
- If the authentication page fails to be displayed during web authentication, the maximum number of HTTP sessions may be reached. When this happens, the user can close the application programs that occupy HTTP sessions and perform web authentication again.

1.22.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the maximum number of HTTP sessions allowed for an unauthenticated user.

http redirect session-limit *session-number*

The maximum number of HTTP sessions allowed for an unauthenticated user is **255** by default.

1.23 Configuring the Interval for Updating Online User Information

1.23.1 Overview

The NAS needs to periodically update maintained online user information, for example, the online time. The interval for updating online user information can be manually configured based on different monitoring requirements for online user information in different scenarios.

1.23.2 Restrictions and Guidelines

The interval for updating online user information must be a multiple of 60. If the configured value is not a multiple of 60, the actual effective value is rounded up to the multiple of 60.

1.23.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the interval for updating online user information.

web-auth update-interval *update-interval*

The default interval for updating online user information is **180** seconds.

1.24 Enabling DHCP Address Check

1.24.1 Overview

After Dynamic Host Configuration Protocol (DHCP) address check is configured, authentication is performed only for addresses assigned through DHCP. This function can be configured in global and interface configuration modes based on actual requirements.

1.24.2 Restrictions and Guidelines

- To use this function, you must configure DHCP Snooping.
- Only second-generation web authentication is supported for users with IPv4 addresses.
- This function applies only to network environments with IP addresses assigned through DHCP. If users with statically configured IP addresses exist, network access of these users will be limited.
- If only a few users need to use static IP addresses, configure these IP addresses as straight-through addresses. In this case, these users are exempted from authentication.
- To apply this function to an interface, disable global DHCP address check first.

1.24.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure DHCP address check. Configure at least one of the tasks.

- Enable DHCP address check globally.

  web-auth dhcp-check

  DHCP address check is disabled globally by default.

- Enable DHCP address check on an interface. Run the following commands in sequence:

interface *interface-type interface-number*

web-auth dhcp-check vlan vlan-list

DHCP address check is disabled on an interface by default.

(4)(Optional) Disable DHCP address check on a VLAN.

web-auth dhcp-check vlan disable

DHCP address check is enabled on a VLAN by default.

1.25 Configuring an Address Whitelist

1.25.1 Overview

After an address whitelist is configured, users can access some network resources before authentication.

1.25.2 Restrictions and Guidelines

- A whitelist can contain a maximum of 1000 addresses.
- When whitelisted addresses are configured in domain name format, you need to configure the domain name server (DNS) function for the NAS to enable the NAS to correctly parse domain names.
- Some domain names correspond to multiple IP addresses. A domain name can map to eight IP addresses at most.

1.25.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure an address whitelist.

web-auth acl [**oob** | **vrf** *vrf-name*] **white-url** *white-url-name*

No whitelist is configured by default.

1.26 Configuring VLAN-based Authentication on a Port

1.26.1 Overview

After VLAN-based authentication is configured on a port, only the user hosts in the configured VLAN can initiate web authentication.

1.26.2 Restrictions and Guidelines

When this function is configured, multiple VLANs can be specified.

1.26.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the interface configuration mode.

interface *interface-type interface-number*

(4)Configure VLAN-based authentication on a port.

web-auth vlan-control *vlan-list*

VLAN-based authentication is not configured on a port by default. Port-based authentication is used by default.

1.27 Configuring the Authenticated User Logout Delay on a Port

1.27.1 Overview

After the authenticated user logout delay is configured on a port, the user hosts connected to the port go offline after the delay when the port is down.

1.27.2 Restrictions and Guidelines

You are advised to configure this function to prevent repeated user authentication in scenarios when a port goes down and then up quickly.

1.27.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure the authenticated user logout delay after a port is down.

web-auth linkdown-timeout *linkdown-timeout*

The default authenticated user logout delay after a port is down is **60** seconds.

1.28 Enabling RADIUS Server Escape

1.28.1 Overview

After the RADIUS server escape function is configured, users can still perform authentication to access the Internet when the RADIUS server fails.

1.28.2 Restrictions and Guidelines

This function must be used together with RADIUS server detection function. For details about the RADIUS server detection command, see "Configuring RADIUS" in the *Security Configuration Guide*.

1.28.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable RADIUS server escape.

web-auth radius-escape

The RADIUS server escape function is disabled by default.

1.29 Configuring DHCP Server Detection

1.29.1 Overview

DHCP server detection can find offline web authentication users in a DHCP environment in time, ensuring accurate accounting.

In a network environment where IP addresses are dynamically assigned through DHCP, a DHCP client can send a DHCP RELEASE packet to proactively release the IP address assigned by the DHCP server. The DHCP client without an IP address cannot access the network. If the DHCP server detection function is enabled, the NAS with DHCP Server and web authentication enabled will force the corresponding authenticated user offline when receiving a DHCP RELEASE packet from the DHCP client. If the DHCP server detection function is disabled, the NAS will not force the corresponding authenticated user offline in the preceding scenario.

1.29.2 Restrictions and Guidelines

- The DHCP server detection function is enabled by default.
- This function applies only to network environments with DHCP deployed and takes effect only when both DHCP server and web authentication are enabled on the device.

1.29.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Disable DHCP server detection.

no web-auth dhcp-server check

The DHCP server detection function is enabled by default.

1.30 Configuring Uniqueness Check of Portal Authentication Accounts

1.30.1 Overview

After uniqueness check of portal authentication accounts is enabled, the NAS returns an ACK_AUTH message carrying Errcode 2 to the portal server if account information of a new authenticated user is being used by an online user. Upon receiving such a reply message, some portal servers will send the "Terminal Preemption" prompt to users.

1.30.2 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable uniqueness check of portal authentication accounts.

web-auth portal-valid unique-name

Uniqueness check of portal authentication accounts is disabled by default.

1.31 Enabling Automatic Adding of Domain Information After Usernames

1.31.1 Overview

After automatic adding of domain information after usernames is enabled, the web authentication module will automatically add configured domain information after the original usernames and use the new usernames for authentication.

1.31.2 Restrictions and Guidelines

- The domain information can be 63 bytes at most.
- The new username is obtained by adding configured domain information after the username sent by the portal server. If the new username exceeds 253 bytes, the excess of domain information will be intercepted.

1.31.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enter the web authentication template configuration mode.

web-auth template { **appauth** | **eportalv1** | **eportalv2** | *template-name* **app** | *template-name* **v1** | *template-name* **v2** }

(4)Enable automatic adding of domain information after usernames.

domain *domain-info*

No domain information is added after usernames by default.

1.32 Configuring HTTPS Certificate Import

1.32.1 Overview

HTTPS is an encrypted data transmission protocol and relies on a certificate to ensure transmission security. Before enabling the HTTPS server function, you need to import an available certificate.

To configure HTTPS certificate import, first upload available HTTPS certificate and key files to the NAS and then apply the HTTPS certificate and key files.

1.32.2 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Upload the HTTPS certificate and key files.

web-auth import-ssl { **cert ftp:***path* | **cert tftp:***path* | **cert oob_ftp:***path* | **cert oob_tftp:***path* } { **key ftp:***path* | **key tftp:***path* | **key oob_ftp:***path* | **key oob_tftp:***path* } [**vrf** *vrf-name*]

(3)Apply the HTTPS certificate and key files.

web-auth ssl-policy https-redirect

No HTTPS certificate or key file is applied by default.

1.33 Enabling Adding the Authentication Page to Favorite

1.33.1 Overview

After the function of adding the authentication page to Favorite is enabled, a user can add the authentication page to Favorite and open the Favorite page for web authentication without needing redirection.

1.33.2 Restrictions and Guidelines

- This function must be used together with DHCP Snooping.
- This function cannot be configured with 802.1x authentication simultaneously. Otherwise, a user may be online for web authentication and 802.1x authentication at the same time.

1.33.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Enable the function of adding the authentication page to Favorite.

web-auth portal direct-auth

The function of adding the authentication page to Favorite is disabled by default.

1.34 Configuring a Template Mapping Method

1.34.1 Overview

The template mapping method is configured when multiple authentication scenarios exist on one port.

When web authentication is enabled on a port, and the method of template A is used, but some users do not apply to template A and want to use template B for authentication, you can configure a template mapping method for these users to enable these users to use the authentication method of template B.

1.34.2 Restrictions and Guidelines

By setting the VLAN or IP address range, you can select users for whom a template mapping method needs to be configured.

1.34.3 Procedure

(1)Enter the privileged EXEC mode.

enable

(2)Enter the global configuration mode.

configure terminal

(3)Configure a template mapping method, and determine the user range and the corresponding authentication template method.

web-auth mapping *mapping-method* { **vlan** *vlan-list* | **ip-mapping** *ipv4-address ipv4-mask* } **template** *tmpltate-name*

No template mapping method is configured by default.

(4)Enter the interface configuration mode.

interface *interface-type interface-number*

(5)Apply the template mapping method.

web-auth apply-mapping *mapping-method*

No template mapping method is applied on an interface by default.

1.35 Monitoring

Run the **show** commands to check the running status of a configured function to verify the configuration effect.

Run the **clear** commands to clear information.

⚠ **Notice**

Running the **clear** commands may lose vital information and thus interrupt services.

Table 1-1Monitoring

Command	Purpose
show web-auth acl [**white-url** | **white-port**]	Displays whitelist configurations.
show web-auth authmng [**statistic** | **abnormal**]	Displays the web authentication data.
show web-auth parameter	Displays basic parameter configurations for web authentication.
show web-auth control	Displays authentication control configuration.
show web-auth direct-arp	Displays the straight-through ARP resource range.
show web-auth direct-host	Displays the authentication-exempted user range.

Command	Purpose
show web-auth direct-site	Displays the straight-through website range.
show web-auth ip-mapping	Displays the configured mapping between servers and users.
show web-auth portal-check	Displays portal-check parameters.
show web-auth rdport	Displays the TCP interception port.
show web-auth syslog ip *ip-address*	Displays user online and offline records.
show web-auth template	Displays portal server configurations.
show web-auth user { **all** | **ip** *ipv4-address* | **mac** *mac-address* | **name** *name* }	Displays user online information.
clear web-auth acl white-url	Clears web authentication whitelist configurations.
clear web-auth direct-arp	Clears all ARP resources.
clear web-auth direct-host	Clears all authentication-exempted users.
clear web-auth direct-site	Clears all authentication-free network resources.
clear web-auth user { **all** | **id** *num* | **ip** *ipv4-address* | **mac** *mac-address* | **name** *name* }	Forces users offline.
debug web-auth all	Debugs web authentication.

1.36 Configuration Examples

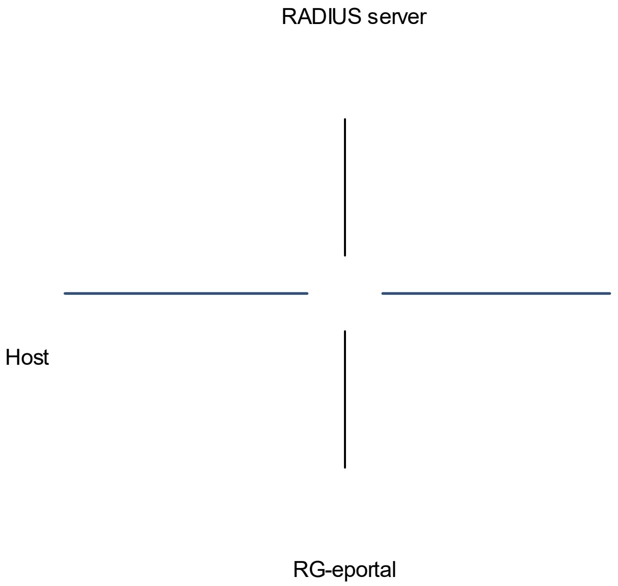
1.36.1 Configuring First-Generation Web Authentication

1. Requirements

The NAS serves as the network access server (NAS) and enables first-generation web authentication for user hosts connecting to a specified port. These user hosts can access the network only after authentication by using valid accounts and passwords.

2. Topology

Figure 1-1Configuring First-Generation Web Authentication



3. Notes

- Configure the portal server to support first-generation web authentication.
- Configure the RADIUS server to support first-generation web authentication.
- Configure the first-generation web authentication template and specify the portal server IP address, redirection page, and other parameters.
- Configure the communication key between the NAS and the portal server.
- Configure SNMP parameters between the NAS and the portal server.
- Enable first-generation web authentication on a port of the NAS.

4. Procedure

(1)Configure the portal server and RADIUS server to support first-generation web authentication. For details about the configuration procedure, see the corresponding configuration guide.

(2)Configure the first-generation web authentication template and set the portal server IP address to 192.168.1.3 and redirection page URL to http://192.168.1.3/eportal/index.jsp.

```
Device> enable
Device# configure terminal
Device(config)# web-auth template eportalv1
Device(config.tmplt.eportalv1)# ip 192.168.1.3
Device(config.tmplt.eportalv1)# url http://192.168.1.3/eportal/index.jsp
Device(config.tmplt.eportalv1)# exit
```

(3)Set the communication key between the NAS and the portal server to key_1 (which must be the same as that configured on the portal server).

```
Device(config)# web-auth portal key key_1
```

(4)Enable the SNMPv2 function.

```
Device(config)# enable service snmp-agent
Device(config)# snmp-server enable version v2c
```

(5)Configure SNMP community string community_1 and enable the SNMP trap/inform function. The SNMP server address is the portal server address.

```
Device(config)# snmp-server community community_1 rw
Device(config)# snmp-server host 192.168.1.3 inform version 2c community_1
web-auth
Device(config)# snmp-server enable traps web-auth
```

(6)Enable first-generation web authentication on GigabitEthernet 0/2 and GigabitEthernet 0/3.

```
Device(config)#int range gigabitEthernet 0/2-3
Device(config-if-range)#web-auth enable eportalv1
```

5. Verification

Check that first-generation web authentication takes effect on GigabitEthernet 0/2 and GigabitEthernet 0/3.

```
Device# show web-auth control
 Port                      Control  Server Name    Online User Count Arp-detect
Vlan Control List
 ------------------------- --------- --------------------------------
----------------- ----------
 GigabitEthernet 0/2       On       eportalv1       0                 Off
 GigabitEthernet 0/3       On       eportalv1       0                 Off
```

Check that parameters of the web authentication template are correctly configured.

```
Device# show web-auth template
Webauth Template Settings:
------------------------------------------------------------
  Name:                 eportalv1
  BindMode:             ip-only-mode
  Type:                 v1
  Ip:                   192.168.1.3
  Url:                  http://192.168.1.3/eportal/index.jsp
```

When user hosts connecting to GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS access a webpage, the hosts will be redirected to http://192.168.1.3/eportal/index.jsp for authentication. The hosts can access the network after they pass authentication.

6. Configuration Files

```
!
web-auth template eportalv1
 ip 192.168.1.3
 url 192.168.1.3/eportal/index.jsp
!
web-auth portal key key_1
!
enable service snmp-agent
!
```

```
snmp-server host 192.168.1.3 informs version 2c 7 $10$255$lxTDxZBSy7ToI2s=$ web-
auth
snmp-server enable traps web-auth
snmp-server enable version v2c
snmp-server community 7 $10$255$lxTDxZBSy7ToI2s=$ rw
!
interface GigabitEthernet 0/2
 web-auth enable eportalv1
!
interface GigabitEthernet 0/3
 web-auth enable eportalv1
!
```

7. Common Errors

- The SNMP parameters used for the communication between the portal server and the NAS are configured incorrectly, causing authentication failures.
- When web authentication is deployed on L3 networks, **ip-only-mode** is not selected as the binding mode in the template.
- When web authentication is used together with Virtual Router Redundancy Protocol (VRRP), the **snmp-server trap-source ip** command is not configured to specify the VRRP address. As a result, the portal server cannot process Trap packets correctly.

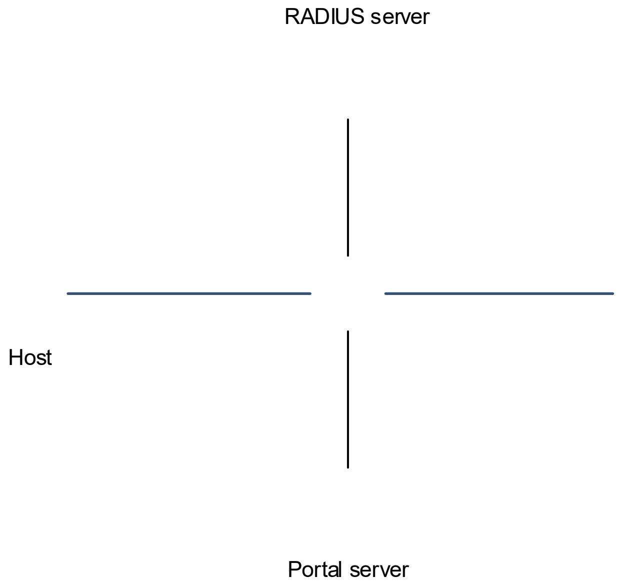
1.36.2 Configuring Second-Generation Web Authentication

1. Requirements

The NAS serves as the NAS and enables second-generation web authentication for user hosts connecting to a specified port. These user hosts can access the network only after authentication by using valid accounts and passwords.

2. Topology

Figure 1-1Configuring Second-Generation Web Authentication



3. Notes

- Configure the portal server to support second-generation web authentication.
- Configure the RADIUS server to support second-generation web authentication.
- Enable AAA security services on the device.
- Configure the IP address and communication key of the RADIUS server.
- Configure the default web authentication and accounting method lists for the AAA module.
- Configure the key used to communicate with the portal server.
- Configure the second-generation web authentication template.
- Enable second-generation web authentication on a port of the NAS.

4. Procedure

(1)Configure the portal server and RADIUS server to support second-generation web authentication. For details about the configuration procedure, see the corresponding configuration guide.

(2)Configure the second-generation web authentication template and set the portal server IP address to 192.168.1.3 and redirection page URL to http://192.168.1.3/eportal/index.jsp.

```
Device> enable
Device# configure terminal
Device(config)# web-auth template eportalv2
Device(config.tmplt.eportalv2)# ip 192.168.1.3
Device(config.tmplt.eportalv2)# url http://192.168.1.3/eportal/index.jsp
Device(config.tmplt.eportalv2)# exit
```

(3)Set the communication key between the NAS and the portal server to key_1 (which must be the same as that configured on the portal server).

```
Device(config)# web-auth portal key key_1
```

(4)Configure the IP address and communication key of the RADIUS server.

```
Device(config)# radius-server host 192.168.1.4 key radiuskey
```

(5)Enable AAA security services.

```
Device(config)# aaa new-model
```

(6)Configure the default web authentication and accounting method lists for the AAA module.

```
Device(config)# aaa authentication web-auth default group radius
Device(config)# aaa accounting network default start-stop group radius
```

(7)Enable second-generation web authentication on GigabitEthernet 0/2 and GigabitEthernet 0/3.

```
Device(config)#int range gigabitEthernet 0/2-3
Device(config-if-range)#web-auth enable eportalv2
```

5. Verification

Check that second-generation web authentication takes effect on GigabitEthernet 0/2 and GigabitEthernet 0/3.

```
Device# show web-auth control
 Port                      Control  Server Name     Online User Count Arp-detect
Vlan Control List
 ------------------------- -------- --------------------------------
----------------- ----------
 GigabitEthernet 0/2       On       eportalv2        0                 Off
 GigabitEthernet 0/3       On       eportalv2        0                 Off
```

Check that parameters of the second-generation authentication template are correctly configured.

```
Orion#show web-auth template
Webauth Template Settings:
------------------------------------------------------------
  Name:                eportalv2
  BindMode:            ip-mac-mode
  Type:                v2
  Port:                50100
  vrf:
  Ip:                  192.168.1.3
  Url:                 http://192.168.1.3/eportal/index.jsp
  Authentication:
  Accounting:
  Portal-State:        Enable
  Radius-State:        Enable
```

When user hosts connecting to GigabitEthernet 0/2 and GigabitEthernet 0/3 on the NAS access a webpage, the hosts will be redirected to http://192.168.1.3/eportal/index.jsp for authentication. The hosts can access the network after they pass authentication.

6. Configuration Files

```
!
web-auth template eportalv2
 ip 192.168.1.3
 url 192.168.1.3/eportal/index.jsp
!
web-auth portal key key_1
!
aaa new-model
!
aaa accounting network default start-stop group radius
aaa authentication web-auth default group radius
!
radius-server host 172.26.147.194 key 7 $10$3ed$f/3upXnVEhd9$
!
interface GigabitEthernet 0/2
 web-auth enable eportalv2
!
interface GigabitEthernet 0/3
 web-auth enable eportalv2
!
```

7. Common Errors

- The communication key between the portal server and NAS is configured incorrectly, or is configured only on the portal server or NAS, causing authentication errors.
- The communication parameters between the RADIUS server and the NAS are set incorrectly, causing authentication errors.
- The portal server does not support the CMCC WLAN Service Portal Specification, causing a compatibility failure.