1 Web Authentication Commands

Command	Function
accounting	Configure the accounting method list used by a template.
app-name	Configure the app name used by a template.
authentication	Configure the authentication method list used by a template.
bindmode	Configure the binding mode used by a template.
clear web-auth acl	Clear all whitelist configurations for web authentication.
clear web-auth direct-arp	Clear all Address Resolution Protocol (ARP) resources.
clear web-auth direct-host	Clear all authentication-exempted users.
clear web-auth direct-site	Clear all authentication-free network resources.
clear web-auth user	Force a user offline.
domain	Enable automatic adding of domain information after usernames.
fmt	Configure the URL format of redirection packets.
http redirect direct-arp	Configure a straight-through ARP resource range.
http redirect direct-site	Configure an authentication-free network resource range.
http redirect port	Redirect HTTP requests with specified port numbers from users.
http redirect session-limit	Configure the global maximum number of HTTP sessions allowed for an unauthenticated user.
http redirect timeout	Configure the redirection connection timeout time.
ip	Configure the IPv4 address and virtual routing and forwarding (VRF) instance of the portal server.
ip portal source-interface	Configure the portal communication source port.
port	Configure the communication port of the portal

	server.
redirect	Configure the encapsulation format of redirection packets.
show web-auth acl	Display whitelist configurations.
show web-auth app-config	Display app configurations.
show web-auth authmng	Display web authentication data.
show web-auth control	Display controlled authentication configurations.
show web-auth direct-arp	Display the straight-through ARP resource range.
show web-auth direct-host	Display the authentication-exempted user range.
show web-auth direct-site	Display the straight-through website range.
show web-auth ip-mapping	Display the mapping between servers and users.
show web-auth parameter	Display basic parameter configurations for web authentication.
show web-auth portal-check	Display portal-check parameters.
show web-auth rdport	Display the intercepted TCP ports.
show web-auth syslog ip	Display user online and offline records.
show web-auth template	Display the portal server configurations.
show web-auth user	Display online information of all users or a specified user, including the IP address, interface, and online time.
url	Configure the authentication page address of the portal server.
web-auth acl	Configure a whitelist.
web-auth apply-mapping	Apply the template mapping method on an interface.
web-auth dhcp-check	Enable Dynamic Host Configuration Protocol (DHCP) address check for web authentication.
web-auth dhcp-check vlan	Enable DHCP address check for web authentication on an interface.
web-auth dhcp-check disable	Disable DHCP address check on a VLAN.
web-auth direct-host	Configure the authentication-exempted user range.
web-auth enable	Enable web authentication on a port.
web-auth import-ssl	Upload the certificate and key files.

web-auth linkdown-timeout	Configure the authenticated user logout delay after a port is down.
web-auth logging enable	Configure the web authentication logging function.
web-auth mapping	Configure the webauth template mapping method.
web-auth portal direct-auth	Enable the function of adding the authentication page to Favorite.
web-auth portal extension	Enable portal specification extension.
web-auth portal key	Configure the communication key between the NAS and the portal server.
web-auth portal-check	Enable portal server detection.
web-auth portal-escape	Enable the portal escape function.
web-auth portal-import attr-26	Enable transparent transmission of RADIUS attributes.
web-auth portal-valid unique-name	Enable uniqueness check of portal authentication accounts.
web-auth radius-escape	Enable RADIUS server escape for web authentication.
web-auth ssl-policy https-redirect	Apply the HTTPS certificate and key files.
web-auth template	Create an authentication template and enter the authentication template configuration mode.
web-auth update-interval	Configure the interval for updating online user information.
web-auth vlan-control	Configure VLAN-based authentication on a port.

1.1 accounting

Function

Run the **accounting** command to configure the accounting method list used by a template.

Run the **no** form of this command to remove this configuration.

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

Syntax

accounting *method-list*

no accounting

Parameter Description

method-list: Name of the accounting method list used by a template.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

Before you configure an accounting method list, ensure that the accounting methods in the list have been configured on the Authentication, Authorization and Accounting (AAA) module and the method list name is the same as that configured in the AAA module.

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

Examples

The following example configures accounting method list mlist1 for template eportalv2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# accounting mlist1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa accounting network** (AAA)

1.2 app-name

Function

Run the **app-name** command to configure the app name used by a template.

Run the **no** form of this command to remove this configuration.

Syntax

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

no app-name

Parameter Description

APP_AUTH: Configures the gateway authentication app.

app-name: App name used by a template.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

The name of the app interworking with the web authentication module must be correctly configured.

Examples

The following example sets the app name used by a template to **appauth**.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template appauth
Hostname(config.tmplt.app)# app-name appauth
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **web-auth template**

1.3 authentication

Function

Run the **authentication** command to configure the authentication method list used by a template.

Run the **no** form of this command to remove this configuration.

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

Syntax

authentication *method-list*

no authentication

Parameter Description

method-list: Name of the authentication method list used by a template.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

The authentication method list name configured by running this command must be the same as that configured in the AAA module.

The first-generation web authentication does not support the configuration of an authentication method list.

Examples

The following example configures authentication method list mlist1 for template eportalv2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# authentication mlist1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **aaa authentication web-auth** (AAA)
- **web-auth template**

1.4 bindmode

Function

Run the **bindmode** command to configure the binding mode used by a template.

Run the **no** form of this command to remove this configuration.

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

Syntax

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

no bindmode

Parameter Description

ip-mac-mode: Specifies the IP address+MAC address binding mode. In this mode, both the IP address and media access control (MAC) address are used in the forwarding entry.

ip-only-mode: Specifies the IP address binding mode. In this mode, only the IP address is used in the forwarding entry. You are advised to use this binding mode in layer 3 (L3) networks because MAC address information in L3 networks is incorrect.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the binding mode used by template eportalv2 to IP address only.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# bindmode ip-only-mode
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **web-auth template**

1.5 clear web-auth acl

Function

Run the **clear web-auth acl** command to clear all whitelist configurations for web authentication.

Syntax

clear web-auth acl white-url

Parameter Description

white-url: Clears all whitelisted URLs.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears all whitelisted URLs for web authentication.

```
Hostname> enable
Hostname# clear web-auth acl white-url
```

Notifications

N/A

Platform Description

N/A

1.6 clear web-auth direct-arp

Function

Run the **clear web-auth direct-arp** command to clear all Address Resolution Protocol (ARP) resources.

Syntax

clear web-auth direct-arp

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears all ARP resources.

```
Hostname> enable
Hostname# clear web-auth direct-arp
```

Notifications

N/A

Platform Description

N/A

1.7 clear web-auth direct-host

Function

Run the **clear web-auth direct-host** command to clear all authentication-exempted users.

Syntax

clear web-auth direct-host

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears all authentication-exempted users.

```
Hostname> enable
Hostname# clear web-auth direct-host
```

Notifications

N/A

Platform Description

N/A

1.8 clear web-auth direct-site

Function

Run the **clear web-auth direct-site** command to clear all authentication-free network resources.

Syntax

clear web-auth direct-site

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears all authentication-free network resources.

```
Hostname> enable
Hostname# clear web-auth direct-site
```

Notifications

N/A

Platform Description

N/A

1.9 clear web-auth user

Function

Run the **clear web-auth user** command to force a user offline.

Syntax

clear web-auth user { **all** | **ip** *ipv4-address* | **mac** *mac-address* | **name** *name* }

Parameter Description

all: Forces all users offline.

ip *ipv4-address*: Forces users with specified IPv4 addresses offline.

mac *mac-address*: Forces users with specified MAC addresses offline.

name *name*: Forces users with specified usernames offline.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example forces all users offline.

```
Hostname> enable
Hostname# clear web-auth user all
```

Notifications

N/A

Platform Description

N/A

1.10 domain

Function

Run the **domain** command to enable automatic adding of domain information after usernames.

Run the **no** form of this command to remove this configuration.

No domain information is added after usernames by default.

Syntax

domain *domain-info*

no domain

Parameter Description

domain-info: Domain information to be automatically added after usernames. The value is a string of 1 to 63 bytes.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

Not all templates support automatic adding of domain information after usernames. Template eportalv1 does not support, while template eportalv2 supports.

Examples

The following example configures automatic adding of domain information "@wifi" after usernames.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# domain @wifi
```

Notifications

N/A

Platform Description

N/A

1.11 fmt

Function

Run the **fmt** command to configure the URL format of redirection packets.

Run the **no** form of this command to remove this configuration.

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

Syntax

URL format defined for the first-generation web authentication template:

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

URL format defined for the second-generation web authentication template:

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

Custom URL format:

fmt custom [**encry** { **md5** | **des** | **des_ecb** | **des_ecb3** | **none** }] [**user-ip** *user-ip-string*] [**user-mac** *user-mac-string* **mac-format** [**dot** | **line** | **none** | **5colon**]] [**user-vid** *user-vid-string*] [**user-id** *user-id-string*] [**nas-ip** *nas-ip-string*] [**nas-id** *nas-id-string*] [**nas-id2** *nas-id2-string*] [**ap-mac** *ap-mac-string* **mac-format** [**dot** | **line** | **none** | **5colon**]] [**url** *url-string*] [**ssid** *ssid-string*] [**port** *port-string*] [**ac-serialno** *ac-serialno-string*] [**ap-serialno** *ap-serinalno-string*] [**additional** *additional-string*] [**nas-name** *nas-name-string*]

no fmt

no fmt custom [**user-ip**] [**user-mac**] [**user-vid**] [**user-id**] [**nas-ip**] [**nas-id**] [**nas-id2**] [**ap-mac**] [**url**] [**ssid**] [**port**] [**ac-serialno**] [**ap-serialno**] [**additional**] [**nas-name**]

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

The URL format needs to be configured based on the interworking specifications of the portal server.

Examples

The following example sets the URL format of redirection packets to the CMCC extended format.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# fmt cmcc-ext1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.12 http redirect direct-arp

Function

Run the **http redirect direct-arp** command to configure a straight-through ARP resource range.

Run the **no** form of this command to remove this configuration.

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

Syntax

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

no http redirect direct- arp *ipv4-address* [*mask*]

Parameter Description

ipv4-address: IPv4 address configured as a straight-through ARP resource.

mask: Mask of the IPv4 address configured as a straight-through ARP resource.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

When ARP check is enabled, users cannot learn the ARP entries of the gateway or other devices. You can run this command to permit ARP learning for a specified address or network segment.

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.

Examples

The following example configures the website whose IP address is 172.16.0.1 as a straight-through ARP resource.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http redirect direct-arp 172.16.0.1
```

Notifications

When an invalid IP address/mask format is used, the following notification will be displayed:

```
%Error: Invalid IP address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.13 http redirect direct-site

Function

Run the **http redirect direct-site** command to configure an authentication-free network resource range.

Run the **no** form of this command to remove this configuration.

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

Syntax

http redirect direct-site *ipv4-address* [*mask*] [**arp** | *port-number*&<1-8>]
no http redirect direct-site *ipv4-address* [*mask*]

Parameter Description

ipv4-address: IPv4 address configured as an authentication-free network resource.

mask: Mask of the IPv4 address configured as an authentication-free network resource.

arp: Performs ARP binding for the authentication-free network resource range when the APR check function is enabled, that is, configures the **arp** keyword. This field is required only when IPv4 network resources are configured.

port-number&<1-8>: Authentication-free L4 port. &<1-8> indicates that the parameter can be entered for a maximum of eight times. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage 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.

Examples

The following example configures the website whose IPv4 address is 172.16.0.1 as an authentication-free network resource.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http redirect direct-site 172.16.0.1
```

The following example configures the website whose MAC address is 0000:5e00:0101 as an authentication-free network resource.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http redirect direct-site 0000:5e00:0101
```

Notifications

When an invalid IP address/mask format is used, the following notification will be displayed:

```
%Error: Invalid IP address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.14 http redirect port

Function

Run the **http redirect port** command to redirect HTTP requests with specified port numbers from users.

Run the **no** form of this command to remove this configuration.

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

Syntax

http redirect port *port-number*

no http redirect port *port-number*

Parameter Description

port-number: Port number in HTTP requests to be intercepted. The value range is from 1 to 65535.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The NAS needs to intercept HTTP packets with specified port numbers from users and redirect these HTTP packets to the authentication page to complete authentication. The port numbers can be configured.

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

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.

Examples

The following example redirects HTTP requests with destination port number 8080 from users.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http redirect port 8080
```

The following example does not redirect HTTP requests with destination port number 80 from users.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no http redirect port 80
```

Notifications

When HTTP requests with the destination port set to a well-known protocol port or internal reserved port, for example, port 23, are intercepted, the following notification will be displayed:

```
%Error: Can't set local reserved port(23) as redirection port.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.15 http redirect session-limit

Function

Run the **http redirect session-limit** command to configure the global maximum number of HTTP sessions allowed for an unauthenticated user.

Run the **no** form of this command to remove this configuration.

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

Syntax

http redirect session-limit *session-number*

no http redirect session-limit

Parameter Description

session-number: Global maximum number of HTTP sessions allowed for an unauthenticated user. The value range is from 1 to 255.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

TCP connection resources may be exhausted if unauthenticated users initiate excessive HTTP attacks. Therefore, it is necessary to restrict the maximum number of HTTP sessions allowed for unauthenticated users on the NAS. 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.

Examples

The following example sets the global maximum number of HTTP sessions allowed for an unauthenticated user to 4.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http redirect session-limit 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.16 http redirect timeout

Function

Run the **http redirect timeout** command to configure the redirection connection timeout time.

Run the **no** form of this command to remove this configuration.

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

Syntax

http redirect timeout *timeout*

no http redirect timeout

Parameter Description

timeout: Redirection connection timeout time, in seconds. The value range is from 1 to 10.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

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.

Examples

The following example sets the redirection connection timeout time to 4 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# http redirect timeout 4
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.17 ip

Function

Run the **ip** command to configure the IPv4 address and virtual routing and forwarding (VRF) instance of the portal server.

Run the **no** form of this command to remove this configuration.

No portal server IPv4 address or VRF instance is configured by default.

Syntax

ip [*ipv4-address* | **oob** | **vrf** *vrf-name*]

no ip [**oob** | **vrf**]

Parameter Description

ipv4-address: IPv4 address of the portal server.

oob: Uses the MGMT port for communication.

vrf *vrf-name*: Specifies the virtual private network (VPN) instance name.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the IP address of the portal server for redirection in template eportalv1 to 172.16.0.1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv1
Hostname(config.tmplt.eportalv1)# ip 172.16.0.1
```

Notifications

When the portal server IP address is changed directly, the following notification will be displayed:

```
%Error: Modify portal ip is unsupportted.
```

When an invalid IP address is set, the following notification will be displayed:

```
%Error: Invalid portal ip address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.18 ip portal source-interface

Function

Run the **ip portal source-interface** command to configure the portal communication source port.

Run the **no** form of this command to remove this configuration.

No portal communication source port is configured by default.

Syntax

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

no ip portal source-interface

Parameter Description

interface-type interface-number: Type and number of the interface used for portal communication.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

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.

Only one portal communication source port can be configured.

Examples

The following example configures Aggregateport 1 as the portal communication source port.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# ip portal source-interface aggregateport 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.19 port

Function

Run the **port** command to configure the communication port of the portal server.

Run the **no** form of this command to remove this configuration.

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

Syntax

port *port-number*

no port

Parameter Description

port-number: Communication port of the portal server. The value range is from 1 to 65535.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the communication port of the portal server to 10000.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# port 10000
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.20 redirect

Function

Run the **redirect** command to configure the encapsulation format of redirection packets.

Run the **no** form of this command to remove this configuration.

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

Syntax

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

no redirect

Parameter Description

http: Uses the HTTP 302 packet for URL redirection.

js: Uses the HTTP 200 packet with JS for URL redirection.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the encapsulation format of redirection packets to http.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv2
Hostname(config.tmplt.eportalv2)# redirect http
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.21 show web-auth acl

Function

Run the **show web-auth acl** command to display whitelist configurations.

Syntax

show web-auth acl white-url

Parameter Description

white-url: Displays whitelisted URLs.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays whitelist configurations.

```
Hostname> enable
```

```
Hostname# show web-auth acl white-url
White URL List:0
-----------------------------------------------------
```

Table 1-1Output Fields of the show web-auth acl Command

Field	Description
White URL List	Whitelisted URLs

Notifications

N/A

Platform Description

N/A

1.22 show web-auth app-config

Function

Run the **show web-auth app-config** command to display app configurations.

Syntax

show web-auth app-config *app-name*

Parameter Description

app-name: Name of the app whose configurations are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display app configurations.

Examples

The following example displays configurations of the app test_app.

```
Hostname> enable
Hostname# show web-auth app-config test_app
-----escape----
enable: ON
escape_online: 1
escape_url:
no_kick: 1
```

Table 1-1Output Fields of the show web-auth app-config test_app Command

Field	Description
enable	Whether the escape function is enabled
escape_online	Whether to allow users to go online automatically after escape is triggered
escape_url	URL to which a user is redirected after escape is triggered
no_kick	Whether to force online users offline when escape is triggered

Notifications

N/A

Platform Description

N/A

1.23 show web-auth authmng

Function

Run the **show web-auth authmng** command to display web authentication data.

Syntax

show web-auth authmng [**abnormal** | **statistic**]

Parameter Description

abnormal: Displays web authentication exceptions.

statistic: Displays web authentication statistics.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays web authentication statistics.

```
Hostname> enable
Hostname# show web-auth authmng statistic

Show web authentication information:
 current online number:.................................0.
 historical max online number:..........................0.
```

```
 aggregate online number:..............................0.

Web authentication redirect statistic:
 HTTP packet processing:
  number of users:.....................................0
  number of HTTP packets received:.....................0
 redirection time consumption for successful users:
  average time consumption:............................0ms.
  aggregate time consumption:..........................0ms.
  number of less than half one second:.................0(0.000%).
  number of between half and one second:...............0(0.000%).
  number of more than one second:......................0.

Web authentication statistic:
 authentication processing:
  number of authentication requests received:..........0.
  number of reauthentication requests received:........0.
  number of error password:............................0.
  number of authentication failures:...................0(0.000%).
   AAA timeout:........................................0(0.000%).
   authentication status timeout:......................0(0.000%).
   fail to set SCC:....................................0(0.000%).
   accounting reject:..................................0(0.000%).
   accounting dev timeout:.............................0(0.000%).
   user unexist:.......................................0(0.000%).
   portal timeout:.....................................0(0.000%).
   DHCPrelease pkt:....................................0(0.000%).
   sta move:...........................................0(0.000%).
   clear user:.........................................0(0.000%).
   config change:......................................0(0.000%).
   other:..............................................0.
 authentication time consumption for successful users:
  average time consumption:............................0ms.
  aggregate time consumption:..........................0ms.
  number of less than one second:......................0(0.000%).
  number of between one and three second:..............0(0.000%).
  number of more than three second:....................0(0.000%).
  number of less than one second(exclude server):.....0(0.000%).
  number of between one and three second(exclude server):0(0.000%).
  number of more than three second(exclude server):.....0(0.000%).

Web authentication offline information:
 number of offline count:.............................0.
  number of abnormal offline(rate):...................0(0.000%).
   number of portal timeout:..........................0(0.000%).
   number of set fail:................................0(0.000%).
```

```
   number of link change:.............................0.
  no flow:...........................................0.
  kick off:..........................................0.
  dhcp release:......................................0.
  STA delete:........................................0.
  STA move:..........................................0.
  active offline:....................................0.
  session timeout:...................................0.
  cli clear:.........................................0.
  no control:........................................0.
  interface default:.................................0.
  interface destroy:.................................0.
  dhcp ip check:.....................................0.
  vlan change:.......................................0.
  intfvlan change:...................................0.
  other:.............................................0.
 aggregate online time:.............................0min
 average online time of user:.......................0min

Station-move:
 move count:........................................0.
 move fail:.........................................0.

Other important process statistics:
Auth:
 average time consumption:..........................0ms.
 aggregate time consumption:........................0ms.
 number of less than one second:....................0(0.000%).
 number of more than one second:....................0.

AAA authentication:
 average time consumption:..........................0ms.
 aggregate time consumption:........................0ms.
 number of less than one second:....................0(0.000%).
 number of more than one second:....................0.

Radius authentication:
 average time consumption:..........................0ms.
 aggregate time consumption:........................0ms.
 number of less than one second:....................0(0.000%).
 number of more than one second:....................0.

Radius server authentication:
 average time consumption:..........................0ms.
 aggregate time consumption:........................0ms.
 number of less than one second:....................0(0.000%).
```

```
 number of more than one second:.....................0.

SCC:
 average time consumption:..........................0ms.
 aggregate time consumption:........................0ms.
 number of less than one second:.....................0(0.000%).
 number of more than one second:.....................0.

Accounting:
 average time consumption:..........................0ms.
 aggregate time consumption:........................0ms.
 number of less than one second:.....................0(0.000%).
 number of more than one second:.....................0.

AAA accounting:
 average time consumption:..........................0ms.
 aggregate time consumption:........................0ms.
 number of less than one second:.....................0(0.000%).
 number of more than one second:.....................0.

Radius accounting:
 average time consumption:..........................0ms.
 aggregate time consumption:........................0ms.
 number of less than one second:.....................0(0.000%).
 number of more than one second:.....................0.

Radius server accounting:
 average time consumption:..........................0ms.
 aggregate time consumption:........................0ms.
 number of less than one second:.....................0(0.000%).
 number of more than one second:.....................0.

Portal:
 average time consumption:..........................0ms.
 aggregate time consumption:........................0ms.
 number of less than one second:.....................0(0.000%).
 number of more than one second:.....................0.
```

Table 1-1Output Fields of the show web-auth authmng statistic Command

Field	Description
Show web authentication information	Web authentication information
current online number	Number of online users
historical max online number	Historical maximum number of online users

Field	Description
aggregate online number	Accumulated number of online users
Web authentication redirect statistic	User redirection statistics
HTTP packet processing	HTTP packet processing
number of users	Number of redirected users
number of HTTP packets received	Number of received HTTP packets
redirection time consumption for successful users	Time required for redirection
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than half one second	Number of users whose redirection time is less than 0.5s
number of between half and one second	Number of users whose redirection time is from 0.5s to 1s
number of more than one second	Number of users whose redirection time is greater than 1s
Web authentication statistic	Web authentication statistics
authentication processing	Authentication
number of authentication requests received	Number of authentication requests
number of reauthentication requests received	Number of re-authentication requests
number of error password	Number of authentication failures due to incorrect passwords
number of authentication failures	Number of authentication failures due to other causes
AAA timeout	Number of AAA timeout times
authentication status timeout	Number of authentication timeout times
fail to set SCC	Number of SCC configuration failures
accounting reject	Number of rejected accounting times
accounting dev timeout	Number of accounting timeout times
user unexist	Number of times with non-existent users
portal timeout	Number of portal server timeout times
DHCPrelease pkt	Number of DHCP release times

Field	Description
sta move	Number of user migration times
clear user	Number of user clearing times
config change	Number of configuration changes
other	Number of authentication failures due to other reasons
authentication time consumption for successful users	Time required for successful authentication
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose authentication time is less than 1s
number of between one and three second	Number of users whose authentication time is from 1s to 3s
number of more than three second	Number of users whose authentication time is greater than 3s
number of less than one second(exclude server)	Number of users whose authentication time is less than 1s excluding the time for interaction between the NAS and portal server
number of between one and three second(exclude server)	Number of users whose authentication time is from 1s to 3s excluding time for interaction between the NAS and the portal server
number of more than three second(exclude server)	Number of users whose authentication time is greater than 3s excluding time for interaction between the NAS and the portal server
Web authentication offline information	Web authentication user offline information
number of offline count	Total number of offline times
number of abnormal offline(rate)	Number of abnormal offline times
number of portal timeout	Number of portal server timeout times
number of set fail	Number of entry configuration failures
number of link change	Number of link changes
no flow	Number of offline times due to no traffic
kick off	Number of times being kicked off by the server
dhcp release	Number of DHCP release times
STA delete	Number of STA deletion times
STA move	Number of STA migration times

Field	Description
active offline	Number of offline times requested by users
session timeout	Number of times with the online duration expired
cli clear	Number of users cleared in the command-line interface (CLI)
no control	Number of users who go offline because web control is disabled
interface default	Number of users who go offline because an interface is restored to the default configuration
interface destroy	Number of users who go offline because an interface is deleted
dhcp ip check	Number of users who go offline because the DHCP IP address is changed
vlan change	Number of users who go offline due to VLAN changes
intfvlan change	Number of users who go offline due to L3 VLAN configuration changes
other	Number of users who go offline due to other causes
aggregate online time	Accumulated online duration
average online time of user	Average online duration of users
Station-move	User migration
move count	Total number of migrated users
move fail	Migration failed
Other important process statistics	Other important data
Auth	Authentication
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose authentication time is less than 1s
number of more than one second	Number of users whose authentication time is greater than 1s
AAA authentication	AAA Authentication
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose authentication time is less than 1s
number of more than one second	Number of users whose authentication time is greater than 1s

Field	Description
Radius authentication	RADIUS authentication
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose authentication time is less than 1s
number of more than one second	Number of users whose authentication time is greater than 1s
Radius server authentication	RADIUS server authentication
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose authentication time is less than 1s
number of more than one second	Number of users whose authentication time is greater than 1s
SCC	SCC
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose authentication time is less than 1s
number of more than one second	Number of users whose authentication time is greater than 1s
Accounting	Accounting
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose accounting time is less than 1s
number of more than one second	Number of users whose accounting time is greater than 1s
AAA accounting	AAA accounting
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose accounting time is less than 1s
number of more than one second	Number of users whose accounting time is greater than 1s
Radius accounting	RADIUS accounting
average time consumption	Average required time
aggregate time consumption	Accumulated time

Field	Description
number of less than one second	Number of users whose accounting time is less than 1s
number of more than one second	Number of users whose accounting time is greater than 1s
Radius server accounting	RADIUS accounting
average time consumption	Average required time
aggregate time consumption	Accumulated time
number of less than one second	Number of users whose accounting time is less than 1s
number of more than one second	Number of users whose accounting time is greater than 1s

The following example displays abnormal authentication data.

```
Hostname> enable
Hostname# show web-auth authmng abnormal
record num:0, value:3000, max-num:1000, clock:1
```

Table 1-2Output Fields of the show web-auth authmng abnormal Command

Field	Description
Record num	Number of abnormal records
value	Conditions for identifying abnormal records, that is, the timeout time. A record with 3s or longer authentication time is an abnormal record by default.
max-num	Maximum number of allowed records
clock	Time when a record is written to the flash memory. The default value is 01:00:00 [0–23].

Notifications

N/A

Platform Description

N/A

1.24 show web-auth control

Function

Run the **show web-auth control** command to display controlled authentication configurations.

Syntax

show web-auth control

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays controlled authentication configurations.

```
Hostname> enable
Hostname# show web-auth control
 Port                      Control  Server Name           Online User Count Arp-
detect Vlan Control List
 --------------------------- --------
 GigabitEthernet 0/1       On       eportalv2             1                 On
```

Table 1-1 Output Fields of the show web-auth control Command

Field	Description
Port	Name of a controlled port
Control	Whether web authentication is enabled for a port
Server Name	Customized server name on the port. <not configured> indicates that no server name is configured.
Online User Count	Number of online users on a port
Arp-detect	Whether ARP detection for user migration is enabled
Vlan Control List	List of VLANs that can be authenticated

Notifications

N/A

Platform Description

N/A

1.25 show web-auth direct-arp

Function

Run the **show web-auth direct-arp** command to display the straight-through ARP resource range.

Syntax

show web-auth direct-arp

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the straight-through ARP resource range.

```
Hostname> enable
Hostname# show web-auth direct-arp
Direct arps:
  Address         Mask
  ----- ----
  1.1.1.1         255.255.255.255
  2.2.2.2         255.255.255.255
```

Table 1-1 Output Fields of the show web-auth direct-arp Command

Field	Description
Address	IP address
Mask	Mask of an IP address

Notifications

N/A

Platform Description

N/A

1.26 show web-auth direct-host

Function

Run the **show web-auth direct-host** command to display the authentication-exempted user range.

Syntax

show web-auth direct-host

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all authentication-exempted users.

```
Hostname> enable
Hostname# show web direct-host
Direct hosts: 1
  Address         Mask            Port Binding   ARP Binding   Access Port List
  ----- ----- ---------- -----
  1.1.1.1         255.255.255.255 N/A            Off           1080
  Index      MAC-Address
  --------
```

Table 1-1Output Fields of the show web direct-host Command

Field	Description
Address	IP address of an authentication-exempted user
Mask	Mask of the IP address of an authentication-exempted user
Port Binding	Device port bound to the IP address of an authentication-exempted user
ARP Bining	Whether ARP binding is performed
Access Port List	Bound L4 port list

Notifications

N/A

Platform Description

N/A

1.27 show web-auth direct-site

Function

Run the **show web-auth direct-site** command to display the straight-through website range.

Syntax

show web-auth direct-site

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays all straight-through websites.

```
Hostname> enable
Hostname# show web-auth direct-site
Direct sites: 2
  Address                                 Mask            ARP Binding   Ports
  ------------ ----- --------
  1.1.1.1                                 255.255.255.255 Off           N/A
  2.2.2.2                                 255.255.255.255 Off           1080 2080
```

Table 1-1Output Fields of the show web-auth direct-site Command

Field	Description
Addres	IP address
Mask	Mask of an IP address
ARP Binding	Whether ARP binding is performed
Ports	L4 straight-through port

Notifications

N/A

Platform Description

N/A

1.28 show web-auth ip-mapping

Function

Run the **show web-auth ip-mapping** command to display the mapping between servers and users.

Syntax

show web-auth ip-mapping

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the mapping between servers and users.

```
Hostname> enable
Hostname# show web-auth ip-mapping
-------------------
  Name:       iportal
  Ip:         0.0.0.0
  Url:
  Ip-Mapping:
-------------------
  Name:       eportalv1
  Ip:         172.18.105.9
  Url:        http://172.18.105.9:8080/eportal/index.jsp
  Ip-Mapping:
              1.1.1.0-255.255.255.0           Global
```

Table 1-1 Output Fields of the show web-auth ip-mapping Command

Field	Description
Name	Mapping method name
Ip	Mapped IP address
Url	Mapped URL
Ip-Mapping	Mapped network segment

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.29 show web-auth parameter

Function

Run the **show web-auth parameter** command to display basic parameter configurations for web authentication.

Syntax

show web-auth parameter

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays HTTP redirection configurations.

```
Hostname> enable
Hostname# show web-auth parameter
  session-limit: 10
  timeout:         5
```

Table 1-1Output Fields of the show web-auth parameter Command

Field	Description
session-limit	Maximum number of HTTP sessions allowed for an unauthenticated user
timeout	Redirection connection timeout time

Notifications

N/A

Platform Description

N/A

1.30 show web-auth portal-check

Function

Run the **show web-auth portal-check** command to display portal-check parameters.

Syntax

show web-auth portal-check

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays portal-check parameters.

```
Hostname> enable
Hostname# show web portal-check
Check:         Enable
  Interval:    3s
  Timeout:     5s
  Retransmit:  3
Escape:        Enable
Nokick:        Disable
```

Table 1-1Output Fields of the show web portal-check Command

Field	Description
Check	Whether the portal-check function is enabled
Interval	Detection interval
Timeout	Detection timeout time
Retransmit	Number of retransmission times for each detection

Field	Description
Escape	Whether portal escape is enabled
Nokick	Whether to force online users offline if the portal server is unavailable after the escape function is enabled

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.31 show web-auth rdport

Function

Run the **show web-auth rdport** command to display the intercepted TCP ports.

Syntax

show web-auth rdport

Parameter Description

N/A

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the intercepted TCP ports.

```
Hostname> enable
Hostname# show web-auth rdport
Rd-Port:
80 443
```

Table 1-1 Output Fields of the show web-auth rdport Command

Field	Description
Rd-Port	Redirection port

Notifications

N/A

Platform Description

N/A

1.32 show web-auth syslog ip

Function

Run the **show web-auth syslog ip** command to display user online and offline records.

Syntax

show web-auth syslog ip *ipv4-address*

Parameter Description

ipv4-address: IPv4 address of a user whose online and offline records are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays online and offline records of a user whose IP address is 192.168.197.35.

```
Hostname> enable
Hostname# show web-auth syslog ip 192.168.197.35
Address: 192.168.197.35  Core-index 0 Current index 2
Index:            0
 Time:             2015-10-16 20:37:34
 Behavior:         ONLINE
 Mac:              00d0.f822.33e7
 Vid:              101
 Port:             Gi3/1
 Timeused:         0d 00:00:00
 Flow_up:          0
 Flow_down:        0
```

```
Index:            1
 Time:             2015-10-16 20:42:08
 Behavior:         OFFLINE
 Mac:              00d0.f822.33e7
 Vid:              101
 Port:             Gi3/1
 Timeused:         0d 00:04:27
 Flow_up:          2107872
 Flow_down:        2108224
```

Table 1-1 Output Fields of the show web-auth syslog ip Command

Field	Description
Index	Record No.
Time	Record occurrence time
Behavior	Online or offline action
MAC	MAC address of a user
Vid	VID of a user
Port	Port on the NAS used by user hosts to connect to the NAS
Timeused	Online time
Flow_up	Uplink traffic of a user
Flow_down	Downlink traffic of a user

Notifications

N/A

Platform Description

N/A

1.33 show web-auth template

Function

Run the **show web-auth template** command to display the portal server configurations.

Syntax

show web-auth template

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display the portal server configurations.

Examples

The following example displays portal server configurations.

```
Hostname> enable
Hostname# show web-auth template
Webauth Template Settings:
-------------------
  Name:      eportalv1
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-mac-mode
  Type:      v1
-------------------
  Name:      eportalv2
  Url:       http://17.17.1.21:8080/eportal/index.jsp
  Ip:        17.17.1.21
  BindMode:  ip-only-mode
  Type:      v2
  Port:      50100
  Acctmlist:
  Authmlist:
```

Table 1-1Output Fields of the show web-auth template Command

Field	Description
Name	Template name
Url	Homepage address of the portal server
Ip	IP address of the server
Type	Server type (v1 for first-generation web authentication, and v2 for second-generation web authentication)
Port	Communication port for protocol packets of the portal server (This parameter is valid only for the portal server of second-generation web authentication.)
Acctmlist	Accounting method list name (This parameter is valid only for second-generation web authentication.)

Field	Description
Authmlist	Authentication method list name (This parameter is valid only for second-generation web authentication.)

Notifications

N/A

Platform Description

N/A

1.34 show web-auth user

Function

Run the **show web-auth user** command to display online information of all users or a specified user, including the IP address, interface, and online time.

Syntax

show web-auth user { **all** | **ip** *ipv4-address* | **mac** *mac-address* | **name** *name* }

Parameter Description

all: Displays online information of all users.

ip *ipv4-address*: Specifies the IPv4 address of a user whose online information is displayed.

mac *mac-address*: Specifies the MAC address of a user whose online information is displayed.

name *name*: Specifies the username of a user whose online information is displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays online information of all users.

```
Hostname> enable
Hostname# show web user all
Current user num: 1, Online 1
Address                                 Online  Time Limit     Time Used
Status  Name
------------ --------------- -----
```

```
172.30.33.227                          On      240d 00:00:00  0d 00:01:19
Active  linlt
```

The following example displays online information of a user whose IP address is 192.168.0.11.

```
Hostname> enable
Hostname# show web-auth user ip 192.168.0.11
Address       :   192.168.0.11
 Mac            :   00d0.f800.2233
 Port           :   Gi0/2
 Online         :   On
 Time Limit     :   0d 01:00:00
 Time Used      :   0d 00:15:10
 Time Start     :   2009-02-22 20:05:10
 Status         :   Active
```

Table 1-1Output Fields of the show web-auth user Command

Field	Description
Address	IP address of a user
Mac	MAC address of a user
Port	Port on the user host used to connect to the NAS
Online	Whether a user is online
Time Limit	Limit of the available online time of a user (The value **0** indicates no limit.)
Time Used	User online duration
Time Start	Time when a user passes authentication and starts to get online
Status	User status, including: ● **Active**: A user gets online. ● **Create**: A user is created, and settings are not completed. ● **Destroy**: A user is deleted, and settings are not cleared.
Name	Username (This field is null for users authenticated using the first-generation web authentication solution.)

Notifications

N/A

Platform Description

N/A

1.35 url

Function

Run the **url** command to configure the authentication page address of the portal server.

Run the **no** form of this command to remove this configuration.

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

Syntax

url *url-string*

no url

Parameter Description

url-string: Authentication page address of the portal server, which must be started with "http://" or "https://". The value is a string of up to 255 characters.

Command Modes

Template configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example sets the authentication page address of the portal server in template eportalv1 to http://www.web-auth.net/login.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth template eportalv1
Hostname(config.tmplt.eportalv1)# url http://www.web-auth.net/login
```

Notifications

When an invalid URL format is used, the following notification will be displayed:

```
%Error: Invalid homepage URL.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.36 web-auth acl

Function

Run the **web-auth acl** command to configure a whitelist.

Run the **no** form of this command to remove this configuration.

No whitelist is configured by default.

Syntax

web-auth acl [**oob** | **vrf** *vrf-name*] **white-url** *white-url-name*
no web-auth acl [**oob** | **vrf** *vrf-name*] **white-url** *white-url-name*

Parameter Description

oob: Uses the MGMT port.

vrf *vrf-name*: Specifies the VPN instance name.

white-url *white-url-name*: Specifies whitelisted URLs.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

A whitelist allows users to access some network resources before authentication.

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.

Examples

The following example adds www.hostname.com to the whitelist.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth acl white-url www.hostname.com
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.37 web-auth apply-mapping

Function

Run the **web-auth apply-mapping** command to apply the template mapping method on an interface.

Run the **no** form of this command to remove this configuration.

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

Syntax

web-auth apply-mapping *mapping-method*

no web-auth apply-mapping

Parameter Description

mapping-method: Template mapping method.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

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

Examples

The following example applies template mapping method "test" on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)#web-auth apply-mapping test
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **web-auth mapping**

1.38 web-auth dhcp-check

Function

Run the **web-auth dhcp-check** command to enable Dynamic Host Configuration Protocol (DHCP) address check for web authentication.

Run the **no** form of this command to disable this feature.

DHCP address check is disabled for web authentication by default.

Syntax

web-auth dhcp-check

no web-auth dhcp-check

Parameter Description

N/A

Command Modes

Global configuration mode

Interface configuration mode

Default Level

14

Usage 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.

Examples

The following example enables DHCP address check for web authentication globally.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth dhcp-check
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.39 web-auth dhcp-check vlan

Function

Run the **web-auth dhcp-check vlan** command to enable DHCP address check for web authentication on an interface.

Run the **no** form of this command to disable this feature.

DHCP address check for web authentication is disabled on an interface by default.

Syntax

web-auth dhcp-check vlan *vlan-list*

no web-auth dhcp-check vlan *vlan-list*

Parameter Description

vlan *vlan-list*: Specifies the VLAN range on an interface for which DHCP address check needs to be enabled. The values are valid VIDs. Use commas (,) to separate different values. If a consecutive VLAN range exists, use a hyphen (-). For example, 3-5 indicates VLANs 3, 4, and 5.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

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

Examples

The following example enables DHCP address check for web authentication on GigabitEthernet 0/1 and sets the detected VLAN range to 1 and 3-5.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# web-auth dhcp-check vlan 1,3-5
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.40 web-auth dhcp-check disable

Function

Run the **web-auth dhcp-check disable** command to disable DHCP address check on a VLAN.

Run the **no** form of this command to remove this configuration.

DHCP address check is enabled on a VLAN by default.

Syntax

web-auth dhcp-check vlan disable

no web-auth dhcp-check vlan disable

Parameter Description

N/A

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example disables DHCP address check on a VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# web-auth dhcp-check vlan disable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.41 web-auth direct-host

Function

Run the **web-auth direct-host** command to configure the authentication-exempted user range.

Run the **no** form of this command to remove this configuration.

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

Syntax

web-auth direct-host *ipv4-address* [*mask*] [**arp** | *port-number*&<1-8>]
web-auth direct-host *mac-address*
no web-auth direct-host { *ipv4-address* [*mask*] }
no web-auth direct-host *mac-address*

Parameter Description

ipv4-address: IPv4 address of an authentication-exempted user.

mask: Mask of the IP address of an authentication-exempted user.

arp: Performs ARP binding for network resources of authentication-exempted users when the APR check function is enabled, that is, configures the **arp** keyword. This field is required only when IPv4 network resources are configured.

port-number&<1-8>: L4 port of an authentication-exempted user. &<1-8> indicates that the parameter can be entered for a maximum of eight times. The value range is from 1 to 65535.

mac-address: MAC address of a user exempted from authentication.

Command Modes

Global configuration mode

Default Level

14

Usage 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.

Examples

The following example configures the user whose IPv4 address is 172.16.0.1 as an authentication-exempted user.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth direct-host 172.16.0.1
```

The following example configures the user whose IPv6 address is FF02::/64 as an authentication-exempted user.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth direct-host FF02::/64
```

The following example configures the user whose MAC address is 0000:5e00:0101 as an authentication-exempted user.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth direct-host 0000:5e00:0101
```

Notifications

When an invalid IP address/mask format is used, the following notification will be displayed:

```
%Error: Invalid IP address.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.42 web-auth enable

Function

Run the **web-auth enable** command to enable web authentication on a port.

Run the **no** form of this command to disable this feature.

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

Syntax

web-auth enable [*template-name* | **appauth** | **eportalv1** | **eportalv2**]

no web-auth enable

Parameter Description

template-name: Custom template whose web authentication is enabled.

eportalv1: Enables first-generation web authentication.

eportalv2: Enables second-generation web authentication.

appauth: Enables app-based authentication.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

After web authentication is enabled, the first-generation web authentication template is used by default if no parameter is specified.

To apply web authentication successfully, you must configure the authentication page address.

Examples

The following example enables web authentication on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# web-auth enable
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.43 web-auth import-ssl

Function

Run the **web-auth import-ssl** command to upload the certificate and key files.

Syntax

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*]

Parameter Description

cert ftp:*path*: Configures the File Transfer Protocol (FTP) path for uploading certificate files.

cert tftp:*path*: Configures the Trivial FTP (TFTP) path for uploading certificate files.

cert oob_ftp:*path*: Configures the FTP path for uploading certificate files through the MGMT port.

cert oob_tftp:*path*: Configures the TFTP path for uploading certificate files through the MGMT port.

key ftp:*path*: Configures the FTP path for uploading key files.

Key tftp:*path*: Configures the TFTP path for uploading key files.

key oob_ftp:*path*: Configures the FTP path for uploading key files through the MGMT port.

key oob_tftp:*path*: Configures the TFTP path for uploading key files through the MGMT port.

vrf *vrf-name*: Configures the VRF instance used for uploading files.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

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.

Examples

The following example uploads the certificate and key files.

```
Hostname> enable
Hostname# configure terminal
Hostname# web-auth import-ssl cert tftp://182.168.1.1/cert.pem key
tftp://182.168.1.1/key.pem
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **web-auth ssl-policy https-redirect**

1.44 web-auth linkdown-timeout

Function

Run the **web-auth linkdown-timeout** command to configure the authenticated user logout delay after a port is down.

Run the **no** form of this command to remove this configuration.

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

Syntax

web-auth linkdown-timeout *linkdown-timeout*

no web-auth linkdown-timeout

Parameter Description

linkdown-timeout: Authenticated user logout delay after a port is down, in seconds. The value range is from 1 to 604800.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

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.

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

Examples

The following example sets the authenticated user logout delay after a port is down to 100 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth linkdown-timeout 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.45 web-auth logging enable

Function

Run the **web-auth logging enable** command to configure the web authentication logging function.

Run the **no** form of this command to disable this feature.

The web authentication logging function is disabled by default.

Syntax

web-auth logging enable *log-rate*

no web-auth logging enable

Parameter Description

log-rate: Number of logs printed every second. The value range is from 0 to 100. The value **0** indicates that the number of logs is not limited.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

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.

This command applies only to logs printed in normal cases and is invalid to abnormal or critical logs.

Examples

The following example enables web authentication logging and configures no rate limit for log printing.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth logging enable 0
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.46 web-auth mapping

Function

Run the **web-auth mapping** command to configure the webauth template mapping method.

Run the **no** form of this command to remove this configuration.

No webauth template mapping method is configured by default.

Syntax

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

no web-auth mapping *mapping-method* { **vlan** [*vlan-list*] | **ip-mapping** *ipv4-address mask* }

Parameter Description

mapping-method: Template mapping method.

vlan *vlan-list*: Specifies the VLAN list. The values are valid VIDs. Use commas (,) to separate different values. If a consecutive VLAN range exists, use a hyphen (-). For example, 3-5 indicates VLANs 3, 4, and 5.

ipv4-address mask: IPv4 network segment and mask that uses a template.

template *tmpltate-name*: Specifies the template name.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

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.

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

Examples

The following example configures template mapping method test1 for mapping between templates eportalv2 and VLANs 2-5 and VLAN 10.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth mapping test1 vlan 2-5,10 template eportalv2
```

The following example enables users in the network segment of 10.10.10.1 that uses template mapping method test1 to use template stu_1 for redirection.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth mapping map_test ip-mapping 10.10.10.1 255.255.255.0
template stu_1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- show web-auth ip-mapping

1.47 web-auth portal direct-auth

Function

Run the **web-auth portal direct-auth** command to enable the function of adding the authentication page to Favorite.

Run the **no** form of this command to disable this feature.

Adding the authentication page to favorite is disabled by default.

Syntax

web-auth portal direct-auth

no web-auth portal direct-auth

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The function of adding the authentication page to Favorite needs to query access interfaces of users by IP address and needs to be used together with ARP query or DHCP snooping.

Examples

The following example enables the function of adding the authentication page to Favorite.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth portal direct-auth
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- **ip dhcp snooping** (Security/DHCP Snooping)
- **Arp-check-check** (Security/ARP Check)

1.48 web-auth portal extension

Function

Run the **web-auth portal extension** command to enable portal specification extension.

Run the **no** form of this command to disable this feature.

Run the **default** form of this command to restore the default configuration.

Portal specification extension is enabled by default.

Syntax

web-auth portal extension

no web-auth portal extension

default web-auth portal extension

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

Portal specification extension is enabled to support Orion portal servers and portal servers that comply with the CMCC WLAN Service Portal Specification.

Examples

The following example disables portal specification extension.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# no web-auth portal extension
Hostname(config)# http redirect url-fmt ext1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.49 web-auth portal key

Function

Run the **web-auth portal key** command to configure the communication key between the NAS and the portal server.

Run the **no** form of this command to remove this configuration.

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

Syntax

web-auth portal key *key*

no web-auth portal key

Parameter Description

key: Communication key between the NAS and portal server. The value is a string of 1 to 255 characters.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To apply web authentication successfully, you must configure the communication key between the NAS and the portal server.

The communication key can be configured in global configuration mode only. Specifying a key for each server is not supported.

Examples

The following example sets the communication key between the NAS and the portal server to web-auth.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth portal key web-auth
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.50 web-auth portal-check

Function

Run the **web-auth portal-check** command to enable portal server detection.

Run the **no** form of this command to remove this configuration.

The portal server detection function is disabled by default.

Syntax

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

no web-auth porta-check

Parameter Description

interval *interval*: Specifies the detection interval, in seconds. The value range is from 1 to 1000. The default value is **10**.

timeout *timeout*: Specifies the packet timeout time, in seconds. The value range is from 1 to 1000. The default value is **5**.

retransmit *retransmit-times*: Configures the number of retransmission times upon timeout. The value range is from 1 to 100. The default value is **3**.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

In most networks, only one server is deployed and this function does not need to be configured.

If multiple portal servers exist, it is recommended that the detection interval and packet timeout time not be set to small values; otherwise, the NAS will send many packets within a short time, affecting performance.

Examples

The following example enables portal server detection and sets the detection interval to 20 seconds, the packet timeout time to 2 seconds, and the number of retransmission times upon timeout to 2.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth portal-check interval 20 timeout 2 retransmit 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.51 web-auth portal-escape

Function

Run the **web-auth portal-escape** command to enable the portal escape function.

Run the **no** form of this command to disable this feature.

Portal escape is disabled by default.

Syntax

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

no web-auth portal-escape

Parameter Description

nokick: Configures not to force online users offline if the portal server is unavailable after the escape function is enabled.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

You are advised to configure this command if some key services in the network need to be maintained when the portal server is faulty. The portal server detection function also needs to be configured. When all of the configured portal servers are unavailable, new users can access the Internet without authentication.

Examples

The following example enables the portal escape function.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth portal-escape
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- web-auth portal-check

1.52 web-auth portal-import attr-26

Function

Run the **web-auth portal-import attr-26** command to enable transparent transmission of RADIUS attributes.

Run the **no** form of this command to remove this configuration.

Transparent transmission of RADIUS attributes is disabled by default.

Syntax

web-auth portal-import attr-26

no web-auth portal-import attr-26

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

This command applies only to the Serverless Application Model (SAM) servers and Orion portal servers. If the NAS interworks with a portal server provided by other vendors, enabling this function may cause the portal server to fail to respond to packets.

Examples

The following example enables transparent transmission of RADIUS attributes.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)#web-auth portal-import attr-26
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.53 web-auth portal-valid unique-name

Function

Run the **web-auth portal-valid unique-name** command to enable uniqueness check of portal authentication accounts.

Run the **no** form of this command to disable this feature.

Uniqueness check of portal authentication accounts is disabled by default.

Syntax

web-auth portal-valid unique-name

no web-auth portal-vallid unique-name

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

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 a "Terminal Preemption" prompt to user hosts. Generally, this function is enabled when the portal server needs to push the "Terminal Preemption" prompt to users.

Examples

The following example enables uniqueness check of portal authentication accounts.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth portal-valid unique-name
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.54 web-auth radius-escape

Function

Run the **web-auth radius-escape** command to enable RADIUS server escape for web authentication.

Run the **no** form of this command to disable this feature.

RADIUS server escape for web authentication is disabled by default.

Syntax

web-auth radius-escape

no web-auth radius-escape

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

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

Examples

The following example enables RADIUS server escape for web authentication.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth radius-escape
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.55 web-auth ssl-policy https-redirect

Function

Run the **web-auth ssl-policy https-redirect** command to apply the HTTPS certificate and key files.

Run the **no** form of this command to remove this configuration.

No HTTPS certificate or key file is applied by default.

Syntax

web-auth ssl-policy https-redirect

no web-auth ssl-policy https-redurect

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

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.

Examples

The following example applies the HTTPS certificate and key files.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth ssl-policy https-redirect
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

- web-auth import-ssl

1.56 web-auth template

Function

Run the **web-auth template** command to create an authentication template and enter the authentication template configuration mode.

Run the **no** form of this command to remove this configuration.

No authentication template is configured by default.

Syntax

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

no web-auth template { **appauth** | **eportalv1** | **eportalv2** | *template-name* }

Parameter Description

appauth: Configures the default app-based authentication template.

eportalv1: Configures the default first-generation authentication template.

eportalv2: Configures the default second-generation authentication template.

template-name **app**: Custom app-based authentication template.

template-name **v1**: Custom first-generation authentication template.

template-name **v2**: Custom second-generation authentication template.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example configures the default first-generation authentication template.

```
Hostname> enable
Hostname(config)# web-auth template eportalv1
Hostname(config.tmplt.eportalv1)#
```

Notifications

When the template type is changed, the following notification will be displayed:

```
%Notice: Template has been created, it is a v2 template.
```

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.57 web-auth update-interval

Function

Run the **web-auth update-interval** command to configure the interval for updating online user information.

Run the **no** form of this command to remove this configuration.

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

Syntax

web-auth update-interval *update-interval*

no web-auth update-interval

Parameter Description

update-interval: Interval for updating online user information, in seconds. The value range is from 30 to 3600.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

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

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.

Examples

The following example sets the interval for updating online user information to 60 seconds.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# web-auth update-interval 60
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.58 web-auth vlan-control

Function

Run the **web-auth vlan-control** command to configure VLAN-based authentication on a port.

Run the **no** form of this command to remove this configuration.

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

Syntax

web-auth vlan-control *vlan-list*

no web-auth vlan-control

Parameter Description

vlan-list: List of VLANs for which authentication is allowed. The values are valid VIDs. Use commas (,) to separate different values. If a consecutive VLAN range exists, use a hyphen (-). For example, 3-5 indicates VLANs 3, 4, and 5.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

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

Examples

The following example allows authentication for VLAN 1.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# web-auth vlan-control 1
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A