Contents

Portal commands

The WX1800H series, WX2500H series, and WH3000H series access controllers do not support the slot keyword or the slot-number argument.

aaa-fail nobinding enable

Use **aaa-fail nobinding enable** to enable AAA failure unbinding.

Use **undo aaa-fail nobinding enable** to restore the default.

Syntax

aaa-fail nobinding enable

undo aaa-fail nobinding enable

Default

AAA failure unbinding is disabled.

Views

MAC binding server view

Predefined user roles

network-admin

Usage guidelines

If a portal user fails AAA in MAC-trigger authentication, the user cannot trigger authentication before the MAC-trigger entry of the user ages out. After the MAC-trigger entry ages out, the user triggers MAC-trigger authentication when it accesses the network.

After this feature is enabled, the device sets the MAC-trigger entry state for a user to unbound immediately after the user fails AAA in MAC-trigger authentication. Before the user's MAC-trigger entry ages out, the user can trigger normal portal authentication.

Examples

# Enable AAA failure unbinding for MAC binding server **mts**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] aaa-fail nobinding enable
```

Related commands

display portal mac-trigger-server

aging-time

Use **aging-time** to set the aging time for MAC-trigger entries.

Use **undo aging-time** to restore the default.

Syntax

aging-time *seconds*

undo aging-time

Default

The aging time for MAC-trigger entries is 300 seconds.

Views

MAC binding server view

Predefined user roles

network-admin

Parameters

seconds: Specifies the aging time for MAC-trigger entries. The value range is 60 to 7200 seconds.

Usage guidelines

With MAC-based quick portal authentication enabled, the device generates a MAC-trigger entry for a user when the device detects traffic from the user for the first time. The MAC-trigger entry records the following information:

- MAC address of the user
- Interface index
- VLAN ID
- Traffic statistics
- Aging timer

When the aging time expires, the device deletes the MAC-trigger entry. The device re-creates a MAC-trigger entry for the user when it detects the user's traffic again.

Examples

# Set the aging time to 300 seconds for MAC-trigger entries.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] aging-time 300
```

Related commands

display portal mac-trigger-server

app-id

Use **app-id** to specify the APP ID for QQ authentication.

Use **undo app-id** to restore the default.

Syntax

app-id *app-id*

undo app-id

Default

An APP ID for QQ authentication exists.

Views

QQ authentication server view

Predefined user roles

network-admin

Parameters

app-id: Specifies the APP ID for QQ authentication.

Usage guidelines

To use QQ authentication for portal users, you must go to the Tencent Open Platform (**http://connect.qq.com/intro/login**) to finish the following tasks:

1. Register as a developer by using a valid QQ account.
2. Apply the access to the platform for your website. The website is the webpage to which users are redirected after passing QQ authentication.

You will obtain the APP ID and APP key from the Tencent Open Platform after your application succeeds.

After a portal user passes QQ authentication, the QQ authentication server sends the authorization code of the user to the portal Web server. After the portal Web server receives the authorization code, it sends the authorization code of the user, the APP ID, and the APP key to the QQ authentication server for verification. If the information is verified as correct, the device determines that the user passes QQ authentication.

Examples

# Specify 101235509 as the APP ID for QQ authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server qq
[Sysname-portal-extend-auth-server-qq] app-id 101235509
```

Related commands

display portal extend-auth-server

app-key

Use **app-key** to specify the APP key for QQ authentication.

Use **undo app-key** to restore the default.

Syntax

app-key { **cipher** | **simple** } *app-key*

undo app-key

Default

An APP key for QQ authentication exists.

Views

QQ authentication server view

Predefined user roles

network-admin

Parameters

cipher: Specifies the APP key in encrypted form.

simple: Specifies the APP key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

app-key: Specifies the APP key string. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 1 to 117 characters.

Usage guidelines

To use QQ authentication for portal users, you must go to the Tencent Open Platform (**http://connect.qq.com/intro/login**) to finish the following tasks:

1. Register as a developer by using a valid QQ account.

2. Apply the access to the platform for your website. The website is the webpage to which users are redirected after passing QQ authentication.

You will obtain the APP ID and APP key from the Tencent Open Platform after your application succeeds.

After a portal user passes QQ authentication, the QQ authentication server sends the authorization code of the user to the portal Web server. After the portal Web server receives the authorization code, it sends the authorization code of the user, the APP ID, and the APP key to the QQ authentication server for verification. If the information is verified as correct, the device determines that the user passes QQ authentication.

Examples

# Specify **8a5428e6afdc3e2a2843087fe73f1507** in plaintext form as the APP key for QQ authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server qq
[Sysname-portal-extend-auth-server-qq] app-key simple 8a5428e6afdc3e2a2843087fe73f1507
```

Related commands

display portal extend-auth-server

authentication-timeout

Use **authentication-timeout** to set the authentication timeout, which is the maximum amount of time the device waits for portal authentication to complete after receiving the MAC binding query response.

Use **undo authentication-timeout** to restore the default.

Syntax

authentication-timeout *minutes*

undo authentication-timeout

Default

The authentication timeout time is 3 minutes.

Views

MAC binding server view

Predefined user roles

network-admin

Parameters

minutes: Specifies the authentication timeout in the range of 1 to 15 minutes.

Usage guidelines

On receiving the MAC binding query response from the MAC binding server, the device starts the timeout timer for portal authentication.

If the user passes portal authentication before the timer expires, the device immediately deletes the MAC-trigger entry for the user. If the user does not pass portal authentication within the authentication timeout, the device deletes the MAC-trigger entry after the entry expires.

Examples

# Set the authentication timeout to 10 minutes.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
```

```
[Sysname-portal-mac-trigger-server-mts] authentication-timeout 10
```

Related commands

display portal mac-trigger-server

auth-url

Use **auth-url** to specify the URL of the QQ authentication server.

Use **undo auth-url** to delete the URL of the QQ authentication server.

Syntax

auth-url *url-string*

undo auth-url

Default

The URL of QQ authentication server is **https://graph.qq.com**.

Views

QQ authentication server view

Predefined user roles

network-admin

Parameters

url-string: Specifies the URL of the QQ authentication server, a case-sensitive string of 1 to 256 characters. Make sure that you specify the actual URL of the QQ authentication server.

Examples

# Specify **http://oauth.qq.com** as the URL of the QQ authentication server.

```
<Sysname> system-view
[Sysname] portal extend-auth-server qq
[Sysname-portal-extend-auth-server-qq] auth-url http://oauth.qq.com
```

Related commands

display portal extend-auth-server

binding-retry

Use **binding-retry** to set the maximum number of attempts and the interval for sending MAC binding queries to the MAC binding server.

Use **undo binding-retry** to restore the default.

Syntax

binding-retry { *retries* | **interval** *interval* } *

undo binding-retry

Default

The maximum number of query attempts is 3 and the query interval is 1 second.

Views

MAC binding server view

Predefined user roles

network-admin

Parameters

retries: Specifies the maximum number of MAC binding query attempts, in the range of 1 to 10.

interval *interval*: Specifies the query interval in the range of 1 to 60 seconds.

Usage guidelines

If the device does not receive a response from the MAC binding server after the maximum number is reached, the device determines that the MAC binding server is unreachable. The device performs normal portal authentication for the user. The user needs to enter the username and password for authentication.

If you execute this command multiple times in the same MAC binding server view, the most recent configuration takes effect.

Examples

# Set the maximum number of MAC binding query attempts to 3 and the query interval to 60 seconds.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] binding-retry 3 interval 60
```

Related commands

display portal mac-trigger-server

captive-bypass enable

Use **captive-bypass enable** to enable the captive-bypass feature.

Use **undo captive-bypass enable** to disable the captive-bypass feature.

Syntax

captive-bypass [**android | ios** [**optimize**]] **enable**

undo captive-bypass [**android | ios** [**optimize**]] **enable**

Default

The captive-bypass feature is disabled. The device automatically pushes the portal authentication page to the iOS devices and some Android devices when they are connected to the network.

Views

Portal Web server view

Predefined user roles

network-admin

Parameters

android: Enables the captive-bypass feature for Android users.

ios: Enables the captive-bypass feature for iOS users.

optimize: Enables the optimized captive-bypass feature.

Usage guidelines

With this feature enabled, the device does not automatically push the portal authentication page to iOS devices and some Android devices when they are connected to the network. The device pushes the portal authentication page only when the user accesses the Internet by using a browser or other methods.

The optimized captive-bypass feature applies only to iOS mobile clients. The device automatically pushes the portal authentication page to iOS mobile devices when they are connected to the network. Users can perform authentication on the page or press the home button to return to the desktop without performing authentication, and the Wi-Fi connection is not terminated.

You can repeat this command to enable the captive-bypass feature for both Android and iOS users.

If you do not specify any parameters, this command enables the captive-bypass feature for both Android and iOS users.

Examples

# Enable the captive-bypass feature.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] captive-bypass enable
```

# Enable the optimized captive-bypass feature for iOS users.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] captive-bypass ios optimize enable
```

# Enable the captive-bypass feature for Android users.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] captive-bypass android enable
```

Related commands

- **display portal web-server**
- **display portal captive-bypass statistics**

default-logon-page

Use **default-logon-page** to specify the default authentication page file for the local portal Web server.

Use **undo default-logon-page** to restore the default.

Syntax

default-logon-page *filename*

undo default-logon-page

Default

No default authentication page file is specified for the local portal Web server.

Views

Local portal Web server view

Predefined user roles

network-admin

Parameters

filename: Specifies the default authentication page file by the file name (without the file storage directory). The file name is a case-sensitive string of 1 to 91 characters. Valid characters are letters, digits, dots (.) and underscores (_).

Usage guidelines

You must edit the default authentication pages, compress them to a .zip file, and then upload the file to the root directory of the storage medium of the device.

After you use the **default-logon-page** command to specify the file, the device decompresses the file to get the authentication pages. The device then sets them as the default authentication pages for local portal authentication.

For successful local portal authentication, you must specify the default portal authentication page file for the local portal Web server.

Examples

# Specify the file **pagefile1.zip** as the default authentication page file for local portal authentication.

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] default-logon-page pagefile1.zip
```

Related commands

portal local-web-server

display portal

Use **display portal** to display portal configuration and portal running state.

Syntax

display portal { **ap** *ap-name* [**radio** *radio-id*] **|** **interface** *interface-type interface-number* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ap *ap-name*: Specifies an AP by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, underscores (_), left brackets ([), right brackets (]), slashes (/), and minus signs (-).

radio *radio-id*: Specifies a radio by its ID. The value range for the radio ID varies by device model. If you do not specify a radio, this command displays portal configuration and portal running state for all radios of the AP.

interface-type interface-number: Specifies an interface by its type and number.

Examples

# Display portal configuration and portal running state on AP **ap1**.

```
<Sysname> display portal ap ap1
 Portal information of ap1
 Radio ID: 1
 SSID: portal
     Authorization : Strict checking
     ACL           : Disable
     User profile  : Disable
 IPv4:
     Portal status: Enabled
     Portal authentication method: Direct
     Portal Web server: wbs(active)
     Secondary portal Web server: wbs sec
     Portal mac-trigger-server: mts
     Authentication domain: my-domain
     Extend-auth domain: def
     User-dhcp-only: Enabled
     Max portal users: 1024
     Bas-ip: 2.2.2.2
     Action for sever detection:
         Server type      Server name           Action
         Web server       wbs                   fail-permit
         Portal server    pts                   fail-permit
     Destination authentication subnet:
         IP address                             Mask
         2.2.2.2                                255.255.0.0
 IPv6:
     Portal status: Enabled
     Portal authentication method: Direct
     Portal Web server: wbsv6(active)
     Secondary portal Web server: Not configured
     Authentication domain: my-domain
     Extend-auth domain: Not configured
     User-dhcp-only: Disabled
     Max portal users: 512
     Bas-ipv6: 2000::1
     Action for sever detection:
         Server type      Server name           Action
         Web server       wbsv6                 fail-permit
         Portal server    ptsv6                 fail-permit
     Destination authentication subnet:
         IP address                             Prefix length
         3000::1                                64
```

# Display portal configuration and portal running state on VLAN-interface 30.

```
<Sysname> display portal interface Vlan-interface 30
 Portal information of Vlan-interface30
     NAS-ID profile: Not configured
     Authorization : Strict checking
     ACL           : Disable
     User profile  : Disable
 IPv4:
     Portal status: Enabled
     Portal authentication method: Direct
     Portal Web server: pt
     Secondary portal Web server: wbs sec(active)
     Authentication domain: test
     Pre-auth domain: Not configured
     User-dhcp-only: Disabled
```

```
    Pre-auth IP pool: Not configured
    Max portal users: Not configured
    Bas-ip: Not configured
    User detection: Not configured
    Portal temp-pass: Enabled       Period: 30s
    Action for server detection:
        Server type    Server name                        Action
        --             --                                 --
    Layer3 source network:
        IP address               Mask
    Destination authentication subnet:
        IP address               Mask
IPv6:
    Portal status: Disabled
    Portal authentication method: Disabled
    Portal Web server: Not configured
    Secondary portal Web server: Not configured
    Authentication domain: Not configured
    Pre-auth domain: Not configured
    User-dhcp-only: Disabled
    Pre-auth IP pool: Not configured
    Max portal users: Not configured
    Bas-ipv6: Not configured
    User detection: Not configured
    Portal temp-pass: Disabled
    Action for server detection:
        Server type    Server name                        Action
        --             --                                 --
    Layer3 source network:
        IP address                                        Prefix length
    Destination authentication subnet:
        IP address                                        Prefix length
```

Table 1 Command output

Field	Description
Portal information of interface	Portal configuration on the interface.
Radio ID	ID of the radio.
SSID	Service set identifier.
NAS-ID profile	NAS-ID profile on the interface.
VSRP instance	Name of the VSRP instance on the interface.
VSRP state	VSRP state of the interface: • **Master**—The device acts as the master in the VSRP instance. • **Backup**—The device acts as the backup in the VSRP instance. • **Down**—The device is not running in the VSRP instance.

Field	Description
	This state occurs in either of the following conditions: ○ The associated VRRP group is in **Initial** state. ○ The VSRP instance does not exist or is not correctly configured on the device. • **N/A**—The interface is not associated with any VSRP instance.
Authorization	Authorization information type: • ACL • User profile
Strict checking	Whether strict checking is enabled on portal authorization information.
IPv4	IPv4 portal configuration.
IPv6	IPv6 portal configuration.
Portal status	Portal authentication status on the interface: • **Disabled**—Portal authentication is disabled. • **Enabled**—Portal authentication is enabled. • **Authorized**—The portal authentication server or portal Web server is unreachable. The interface allows users to have network access without authentication.
Portal VSRP status	Status of the portal VSRP on the interface: • **M_Initial**—The master device is in initial state. • **M_Delay**—The master device is in delayed state. (The device will switch to the master state after the delay time.) • **M_Alone**—The master device is in standalone state. This state occurs when the master device and the backup device cannot communicate with each other. A typical reason is that the failover link is disconnected. • **M_Hello**—The master device is building a TCP connection with the backup device (negotiating the VSRP state and portal enabling state on the interface). • **M_Collect**—The master device is waiting for portal user information from the backup device. • **M_Sync**—The master device is sending portal user information to the backup device. • **M_Synced**—The master device has synchronized the portal user information to the backup device. • **B_Initial**—The backup device is in initial state. • **B_Alone**—The backup device is in standalone state. This state occurs when the backup device and the master device cannot communicate with each other. A typical reason is that the failover link is disconnected. • **B_Hello**—The backup device is building a TCP connection with the master device (negotiating the VSRP state and portal enabling state on the interface). • **B_Report**—The backup device is sending portal user information to the master device. • **B_Sync**—The backup device is receiving portal user information from the master device. • **B_Synced**—The backup device has synchronized the portal information with the master device. • **Down**—The device is not running in the VSRP instance. This field does not appear when the interface is not enabled with

Field	Description
	portal or not associated with a VSRP instance.
Portal authentication method	Authentication mode enabled on the interface. This field displays **Direct** if direct authentication is enabled.
Portal Web server	Name of the primary portal Web server specified on the interface. This field displays the **(active)** flag next to the server name if the server is being used.
Secondary portal Web server	Name of the backup portal Web server specified on the interface. This field displays the **(active)** flag next to the server name if the server is being used.
Portal mac-trigger-server	Name of the MAC binding server specified on the interface.
Authentication domain	Mandatory authentication domain on the interface.
Pre-auth domain	Preauthentication domain for portal users on the interface.
Extend-auth domain	Authentication domain configured for third-party authentication on an interface or service template.
User-dhcp-only	Status of the user-dhcp-only feature: • **Enabled**: Only users with IP addresses obtained through DHCP can perform portal authentication. • **Disabled**: Both users with IP addresses obtained through DHCP and users with static IP addresses can pass authentication to get online.
Pre-auth ip-pool	Name of the IP address pool specified for portal users before authentication.
Max portal users	Maximum number of portal users allowed on an interface.
Bas-ip	BAS-IP attribute of the portal packets sent to the portal authentication server.
Bas-ipv6	BAS-IPv6 attribute of the portal packets sent to the portal authentication server.
User detection	Configuration for online detection of portal users on the interface, including detection method (ARP, ICMP, ND, or ICMPv6), detection interval, maximum number of detection attempts, and user idle time.
Portal temp-pass	Status of the temporary pass feature: • **Enabled**—The temporary pass feature is enabled. • **Disabled**—The temporary pass feature is disabled. • **Period**—Temporary pass period during which a user can access the Internet temporarily. This field is displayed only if the temporary pass feature is enabled.
Action for server detection	Portal server detection configuration on the interface: • **Server type**—Type of the server. **Portal server** represents the portal authentication server, and **Web server** represents the portal Web server. • **Server name**—Name of the server. • **Action**—Action triggered by the result of server detection. This field displays **fail-permit** when the portal fail-permit feature is enabled.
Layer3 source subnet	Information of the portal authentication source subnet.

Field	Description
Destination authentication subnet	Information of the portal authentication destination subnet.
IP address	IP address of the portal authentication subnet.
Mask	Subnet mask of the portal authentication subnet.
Prefix length	Prefix length of the IPv6 portal authentication subnet address.

display portal auth-error-record

Use **display portal auth-error-record** to display portal authentication error records.

Syntax

display portal auth-error-record { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **start-time** *start-date start-time* **end-time** *end-date end-time* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Specifies all portal authentication error records.

ipv4 *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2100. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

Examples

# Display all portal authentication error records.

```
<Sysname> display portal auth-error-record all
Total authentication error records: 2
User MAC                : 0016-ecb7-a879
Interface               : WLAN-BSS1/0/1
User IP address         : 192.168.0.188
AP                      : ap1
SSID                    : byod
Auth error time         : 2016-03-04 16:49:07
Auth error reason       : The maximum number of users already reached.

User MAC                : 0016-ecb7-a235
Interface               : WLAN-BSS1/0/1
User IP address         : 192.168.0.10
AP                      : ap1
```

```
SSID                   : byod
Auth error time        : 2016-03-04 16:51:07
Auth error reason      : The maximum number of users already reached.
```

# Display portal authentication error records for the portal user whose IPv4 address is 192.168.0.188.

```
<Sysname> display portal auth-error-record ip 192.168.0.188
User MAC               : 0016-ecb7-a879
Interface              : WLAN-BSS1/0/1
User IP address        : 192.168.0.188
AP                     : ap1
SSID                   : byod
Auth error time        : 2016-03-04 16:49:07
Auth error reason      : The maximum number of users already reached.
```

# Display portal authentication error records for the portal user whose IPv6 address is 2000::2.

```
<Sysname> display portal auth-error-record ipv6 2000::2
User MAC               : 0016-ecb7-a879
Interface              : WLAN-BSS1/0/1
User IP address        : 2000::2
AP                     : ap1
SSID                   : byod
Auth error time        : 2016-03-04 16:49:07
Auth error reason      : The maximum number of users already reached.
```

# Display portal authentication error records with the error time in the range of 2016/3/4 14:20 to 2016/3/4 14:23.

```
<Sysname> display portal auth-error-record start-time 2016/3/4 14:20 end-time 2016/3/4
14:23
User MAC               : 0016-ecb7-a879
Interface              : WLAN-BSS1/0/1
User IP address        : 192.168.0.188
AP                     : ap1
SSID                   : byod
Auth error time        : 2016-03-04 14:22:25
Auth error reason      : The maximum number of users already reached.
```

Table 2 Command output

Field	Description
Total authentication error records	Total number of portal authentication error records.
User MAC	MAC address of the portal user.
Interface	Access interface of the portal user.
User IP address	IP address of the portal user.
AP	AP name.
SSID	Service set identifier.
Auth error time	Time when the portal user encountered an authentication error, in the format of YYYY-MM-DD hh:mm:ss.
Auth error reason	Reason for the authentication error:

Field	Description
	• The maximum number of users already reached. • Failed to obtain user physical information. • Failed to receive the packet because packet length is 0. • Packet source unknown. Server IP:X.X.X.X, VRF index:0. • Packet validity check failed because packet length and version don't match. • Packet type invalid. • Packet validity check failed due to invalid authenticator. • Memory insufficient. • Portal is disabled on the interface. • The maximum number of users on the interface already reached. • Failed to get the access token of the cloud user. • Failed to get the user information of the cloud user. • Failed to get the access token of the QQ user. • Failed to get the openID of the QQ user. • Failed to get the user information of the QQ user. • Email authentication failed.

Related commands

- **portal auth-error-record enable**
- **reset auth-error-record**

display portal auth-fail-record

Use **display portal auth-fail-record** to display portal authentication failure records.

Syntax

display portal auth-fail-record { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **start-time** *start-*date *start-time* **end-time** *end-date end-time* | **username** *username* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Specifies all portal authentication failure records.

ipv4 *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2100. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

username *username*: Specifies the username of a portal user, a case-sensitive string of 1 to 253 characters. The username cannot contain the domain name.

Examples

# Display all portal authentication failure records.

```
<Sysname> display portal auth-fail-record all
Total authentication fail records: 2
User name              : test@abc
User MAC               : 0016-ecb7-a879
Interface              : WLAN-BSS1/0/1
User IP address        : 192.168.0.188
AP                     : ap1
SSID                   : byod
Auth failure time      : 2016-03-04 16:49:07
Auth failure reason    : Authorization information does not exist.

User name              : coco
User MAC               : 0016-ecb7-a235
Interface              : WLAN-BSS1/0/1
User IP address        : 192.168.0.10
AP                     : ap1
SSID                   : byod
Auth failure time      : 2016-03-04 16:50:07
Auth failure reason    : Authorization information does not exist.
```

# Display portal authentication failure records for the portal user whose IPv4 address is 192.168.0.8.

```
<Sysname> display portal auth-fail-record ip 192.168.0.188
User name              : test@abc
User MAC               : 0016-ecb7-a879
Interface              : WLAN-BSS0/1
User IP address        : 192.168.0.188
AP                     : ap1
SSID                   : byod
Auth failure time      : 2016-03-04 16:49:07
Auth failure reason    : Authorization information does not exist.
```

# Display portal authentication failure records for the portal user whose IPv6 address is 2000::2.

```
<Sysname> display portal auth-fail-record ipv6 2000::2
User name              : test@abc
User MAC               : 0016-ecb7-a879
Interface              : WLAN-BSS1/0/1
User IP address        : 2000::2
AP                     : ap1
SSID                   : byod
Auth failure time      : 2016-03-04 16:49:07
Auth failure reason    : Authorization information does not exist.
```

# Display portal authentication failure records for the portal user whose username is **chap1**.

```
<Sysname> display portal auth-fail-record username chap1
User name              : chap1
User MAC               : 0016-ecb7-a879
Interface              : WLAN-BSS1/0/1
User IP address        : 192.168.0.188
```

```
AP                      : ap1
SSID                    : byod
Auth failure time       : 2016-03-04 16:49:07
Auth failure reason     : Authorization information does not exist.
```

# Display portal authentication failure records with the failure time in the range of 2016/3/4 14:20 to 2016/3/4 14:23.

```
<Sysname> display portal auth-fail-record start-time 2016/3/4 14:20 end-time 2016/3/4
14:23
User name               : chap1
User MAC                : 0016-ecb7-a879
Interface               : WLAN-BSS1/0/1
User IP address         : 192.168.0.188
AP                      : ap1
SSID                    : byod
Auth failure time       : 2016-03-04 14:22:25
Auth failure reason     : Authorization information does not exist.
```

Table 3 Command output

Field	Description
Total authentication fail records	Total number of portal authentication failure records.
User name	Username of the portal user.
User MAC	MAC address of the portal user.
Interface	Access interface of the portal user.
User IP address	IP address of the portal user.
AP	AP name.
SSID	Service set identifier.
Auth failure time	Time when the portal user failed authentication, in the format of YYYY/MM/DD hh:mm:ss.
Auth failure reason	Reason why the user failed portal authentication.

Related commands

- **portal auth-fail-record enable**
- **reset portal auth-fail-record**

display portal captive-bypass statistics

Use **display portal captive-bypass statistics** to display packet statistics for portal captive-bypass.

Syntax

display portal captive-bypass statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command displays portal captive-bypass packet statistics for all cards.

Examples

# Display portal captive-bypass packets on slot 1.

```
<Sysname> display portal captive-bypass statistics slot 1
Slot 1:
User type  Packets
iOS     :  1
Android :  0
```

Table 4 Command output

Field	Description
User type	Type of users: • iOS. • Android.
Packets	Number of portal captive-bypass packets sent to the users.

Related commands

captive-bypass enable

display portal dns free-rule-host

Use **display portal dns free-rule-host** to display IP addresses corresponding to host names in destination-based portal-free rules.

Syntax

display portal dns free-rule-host [*host-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

host-name: Specifies a host name, a case-insensitive string of 1 to 253 characters. Valid characters include letters, digits, hyphens (-), underscores (_), dots (.), and asterisks (*). The host name cannot be **ip** or **ipv6**. If you do not specify a host name, this command displays IP addresses corresponding to all host names in destination-based portal-free rules.

Examples

# Display IP addresses corresponding to host name **www.baidu.com** in a destination-based portal-free rule.

```
<Sysname> display portal dns free-rule-host www.baidu.com
 Host name                      IP
 www.baidu.com                  10.10.10.10
```

# Display IP addresses corresponding to host name ***abc.com** in a destination-based portal-free rule.

```
<Sysname> display portal dns free-rule-host *abc.com
 Host name                      IP
 *abc.com                       12.12.12.12
                                111.8.33.100
                                3.3.3.3
```

Table 5 Command output

Field	Description
Host name	Host name specified in a destination-based portal-free rule.
IP	IP addresses corresponding to the host name.

display portal extend-auth-server

Use **display portal extend-auth-server** to display information about third-party authentication servers.

Syntax

display portal extend-auth-server { **all** | **qq** | **mail** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Specifies all third-party authentication servers.

qq: Specifies the QQ authentication server.

mail: Specifies the email authentication server.

Examples

# Display information about all third-party authentication servers.

```
<Sysname> display portal extend-auth-server all
Portal extend-auth-server: qq
   Authentication URL : http://graph.qq.com
   APP ID            : 101235509
   APP key           : ******
   Redirect URL      : http://h3crd-lvzhou3.chinacloudapp.cn/portal/qqlogin.html
Portal extend-auth-server: mail
   Mail protocol      : POP3
   Mail domain name   : @qq.com
```

Table 6 Command output

Field	Description
Portal extend-auth-server	Type of the third-party authentication server.

Field	**Description**
Authentication URL	URL of the QQ authentication server.
APP ID	APP ID for QQ authentication.
APP key	APP key for QQ authentication.
Redirect URL	Redirection URL for QQ authentication success.
Mail protocol	Protocols of the email authentication service.
Mail domain name	Email domain name of the email authentication service.

Related commands

portal extend-auth-server

display portal local-binding mac-address

Use **display portal local-binding mac-address** to display information about local MAC-account binding entries.

Syntax

display portal local-binding mac-address { *mac-address* | **all** }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

mac-address: Specifies the MAC address of a portal user, in the format of H-H-H.

all: Specifies all local MAC-account binding entries.

Examples

# Display information about all local MAC-account binding entries.

```
<Sysname> display portal local-binding mac-address all
Total MAC addresses: 5
MAC address                Username            Aging(hh:mm:ss)
0015-e9a6-7cfe             wlan_user1          00:41:38
0000-e27c-6e80             wlan_user2          00:41:38
000f-e212-ff01             wlan_user3          00:41:38
001c-f08f-f804             wlan_user4          00:41:38
000f-e233-9000             wlan_user5          00:41:38
```

# Display information about the local MAC-account binding entry for the user with MAC address 0015-e9a6-7cfe.

```
<Sysname> display portal local-binding mac-address 0015-e9a6-7cfe
Total MAC addresses: 1
MAC address                Username           Aging(hh:mm:ss)
0015-e9a6-7cfe             wlan_user1         00:41:38
```

Table 7 Command output

Field	Description
MAC address	MAC address of a portal user.
Username	Username of a portal user.
Aging	Remaining lifetime of the local MAC-account binding entry.

Related commands

local-binding enable

display portal logout-record

Use **display portal logout-record** to display portal user offline records.

Syntax

display portal logout-record { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **start-time** *start-date start-time* **end-time** *end-date end-time* | **username** *username* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Specifies all portal user offline records.

ipv4 *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2100. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

username *username*: Specifies the username of a portal user, a case-sensitive string of 1 to 253 characters. The username cannot contain the domain name.

Examples

# Display all portal user offline records.

```
<Sysname> display portal logout-record all
Total logout records: 2
User name                : test@abc
User MAC                 : 0016-ecb7-a879
Interface                : WLAN-BSS1/0/1
User IP address          : 192.168.0.8
AP                       : ap1
SSID                     : byod
User login time          : 2016-03-04 14:20:19
User logout time         : 2016-03-04 14:22:05
Logout reason            : Admin Reset
```

```
User name              : coco
User MAC               : 0016-ecb7-a235
Interface              : WLAN-BSS1/0/1
User IP address        : 192.168.0.10
AP                     : ap1
SSID                   : byod
User login time        : 2016-03-04 14:10:15
User offline time      : 2016-03-04 14:22:05
Offline reason         : Admin Reset
```

# Display offline records for the portal user whose IP address is 192.168.0.8.

```
<Sysname> display portal logout-record ip 192.168.0.8
User name              : test@abc
User MAC               : 0016-ecb7-a879
Interface              : WLAN-BSS1/0/1
User IP address        : 192.168.0.8
AP                     : ap1
SSID                   : byod
User login time        : 2016-03-04 14:26:12
User logout time       : 2016-03-04 14:27:35
Logout reason          : Admin Reset
```

# Display offline records for the portal user whose username is **chap1**.

```
<Sysname> display portal logout-record username chap1
User name              : chap1
User MAC               : 0016-ecb7-a879
Interface              : WLAN-BSS1/0/1
User IP address        : 192.168.0.8
AP                     : ap1
SSID                   : byod
User login time        : 2016-03-04 17:20:19
User logout time       : 2016-03-04 17:22:05
Logout reason          : Admin Reset
```

# Display portal user offline records with the logout time in the range of 2016/3/4 14:20 to 2016/3/4 14:23.

```
<Sysname> display portal logout-record start-time 2016/3/4 14:20 end-time 2016/3/4 14:23
User name              : test@abc
User MAC               : 0016-ecb7-a879
Interface              : WLAN-BSS1/0/1
User IP address        : 192.168.0.8
AP                     : ap1
SSID                   : byod
User login time        : 2016-03-04 14:20:19
User logout time       : 2016-03-04 14:22:05
Logout reason          : Admin Reset
```

Table 8 Command output

Field	Description
Total logout records	Total number of portal user offline records.
User name	Username of the portal user.
User MAC	MAC address of the portal user.
Interface	Access interface of the portal user.
User IP address	IP address of the portal user.
AP	AP name.
SSID	Service set identifier.
User login time	Time when the portal user came online, in the format of YYYY-MM-DD hh:mm:ss.
User logout time	Time when the portal user went offline, in the format of YYYY-MM-DD hh:mm:ss.
Logout reason	Reason why the portal user went offline: • User Request. • Carrier Lost. • Service Lost. • Admin Reset. • NAS Request. • Idle Timeout. • Port Suspended. • Port Error. • Admin Reboot. • Session Timeout. • User Error. • Service Unavailable. • NAS Error. • Other Errors.

Related commands

- **portal logout-record enable**
- **reset portal logout-record**

display portal mac-trigger-server

Use **display portal mac-trigger-server** to display information about MAC binding servers.

Syntax

display portal mac-trigger-server { **all** | **name** *server-name* }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Specifies all MAC binding servers.

name *server-name*: Specifies a MAC binding server by its name, a case-sensitive string of 1 to 32 characters.

Examples

# Display information about all MAC binding servers.

```
<Sysname> display portal mac-trigger-server all
Portal mac-trigger server: ms1
  Version                     : 2.0
  Server type                 : CMCC
  IP                          : 10.1.1.1
  Port                        : 100
  VPN instance                : vpn1
  Aging time                  : 120 seconds
  Free-traffic threshold      : 1000 bytes
  NAS-Port-Type               : 255
  Binding retry times         : 5
  Binding retry interval      : 2 seconds
  Authentication timeout      : 5 minutes
  Excluded attribute list     : 1
  Local-binding               : Disabled
  Local-binding aging time    : 12 hours
  AAA-fail nobinding          : Disabled
Portal mac-trigger server: mts
  Version                     : 1.0
  Server type                 : IMC
  IP                          : 4.4.4.2
  Port                        : 50100
  VPN instance                : Not configured
  Aging time                  : 300 seconds
  Free-traffic threshold      : 0 bytes
  NAS-Port-Type               : Not configured
  Binding retry times         : 3
  Binding retry interval      : 1 seconds
  Authentication timeout      : 3 minutes
  Excluded attribute list     : 1
  Local-binding               : Disabled
  Local-binding aging-time    : 12 hours
  AAA-fail nobinding          : Disabled
```

# Display information about MAC binding server **ms1**.

```
<Sysname> display portal mac-trigger-server name ms1
Portal mac-trigger server: ms1
  Version                     : 2.0
  Server type                 : CMCC
  IP                          : 10.1.1.1
  Port                        : 100
  VPN instance                : vpn1
  Aging time                  : 120 seconds
  Free-traffic threshold      : 1000 bytes
  NAS-Port-Type               : 255
  Binding retry times         : 5
  Binding retry interval      : 2 seconds
  Authentication timeout      : 5 minutes
  Excluded attribute list     : 1
  Local-binding               : Disabled
  Local-binding aging-time    : 12 hours
  AAA-fail nobinding          : Disabled
```

Table 9 Command output

Field	Description
Portal mac-trigger-server	Name of the MAC binding server.
Version	Version of the portal protocol: • **1.0**—Version 1. • **2.0**—Version 2. • **3.0**—Version 3.
Server type	Type of the MAC binding server: • **CMCC**—CMCC server. • **IMC**—H3C IMC server or H3C CAMS server.
IP	IP address of the MAC binding server.
Port	UDP port number on which the MAC binding server listens for MAC binding query packets.
VPN instance	MPLS L3VPN where the MAC binding server resides. Support for this field depends on the device model.
Aging time	Aging time in seconds. A MAC-trigger entry is aged out when the aging time expires.
Free-traffic threshold	Free-traffic threshold in bytes. If a user's traffic is below the threshold, the user can access the network without authentication.
NAS-Port-Type	NAS-Port-Type attribute value in RADIUS request packets sent to the RADIUS server.
Binding retry times	Maximum number of attempts for sending MAC binding queries to the MAC binding server.
Binding retry interval	Interval at which the device sends MAC binding queries to the MAC binding server.
Authentication timeout	Maximum amount of time that the device waits for portal authentication to complete after receiving the MAC binding query response.
Excluded attribute list	Numbers of attributes excluded from portal protocol packets.
Local-binding	Status of local MAC-trigger authentication: • Disabled. • Enabled.
Local-binding aging-time	Aging time for local MAC-account binding entries, in hours.

Field	Description
AAA-fail nobinding	Status of the AAA failure unbinding feature: • Disabled. • Enabled.

display portal packet statistics

Use **display portal packet statistics** to display packet statistics for portal authentication servers and MAC binding servers.

Syntax

display portal packet statistics [**extend-auth-server** { **cloud** | **mail** | **qq** | **wechat** } | **mac-trigger-server** *server-name* | **server** *server-name*] *

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

extend-auth-server: Specifies a third-party authentication server.

cloud: Specifies the lvzhou cloud authentication server.

mail: Specifies the email authentication server.

qq: Specifies the QQ authentication server.

wechat: Specifies the WeChat authentication server.

mac-trigger-server *server-name*: Specifies a MAC binding server by its name, a case-sensitive string of 1 to 32 characters.

server *server-name*: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify any parameters, this command displays packet statistics for all third-party authentication servers, portal authentication servers, and MAC binding servers.

Examples

# Display packet statistics for portal authentication server **pts**.

```
<Sysname> display portal packet statistics server pts
 Portal server :  pts
 Invalid packets: 0
 Pkt-Type                            Total    Drops    Errors
 REQ_CHALLENGE                       3        0        0
 ACK_CHALLENGE                       3        0        0
 REQ_AUTH                            3        0        0
 ACK_AUTH                            3        0        0
 REQ_LOGOUT                          1        0        0
 ACK_LOGOUT                          1        0        0
 AFF_ACK_AUTH                        3        0        0
 NTF_LOGOUT                          1        0        0
 REQ_INFO                            6        0        0
 ACK_INFO                            6        0        0
 NTF_USERDISCOVER                    0        0        0
 NTF_USERIPCHANGE                    0        0        0
 AFF_NTF_USERIPCHAN                  0        0        0
 ACK_NTF_LOGOUT                      1        0        0
 NTF_HEARTBEAT                       0        0        0
 NTF_USER_HEARTBEAT                  2        0        0
 ACK_NTF_USER_HEARTBEAT              0        0        0
 NTF_CHALLENGE                       0        0        0
 NTF_USER_NOTIFY                     0        0        0
 AFF_NTF_USER_NOTIFY                 0        0        0
```

# Display packet statistics for MAC binding server **newpt**.

```
<Sysname> display portal packet statistics mac-trigger-server newpt
 MAC-trigger server: newpt
 Invalid packets: 0
 Pkt-Type                            Total    Drops    Errors
 REQ_MACBIND                         1        0        0
 ACK_MACBIND                         1        0        0
 NTF_MTUSER_LOGON                    1        0        0
 NTF_MTUSER_LOGOUT                   0        0        0
 REQ_MTUSER_OFFLINE                  0        0        0
```

# Display packet statistics for the lvzhou cloud authentication server.

```
<Sysname> display portal packet statistics extend-auth-server cloud
Extend-auth server:  cloud
 Update interval:  60s
  Pkt-Type               Success    Error      Timeout    Conn-failure
  REQ_ACCESSTOKEN        1          0          0          0
  REQ_USERINFO           1          0          0          0
  RESP_ACCESSTOKEN       1          0          0          0
  RESP_USERINFO          1          0          0          0
  POST_ONLINEDATA        0          0          0          0
  RESP_ONLINEDATA        0          0          0          0
  POST_OFFLINEUSER       1          0          0          0
  AUTHENTICATION         0          1          0          0
```

Table 10 Command output

Field	Description
Portal server	Name of the portal authentication server.
Invalid packets	Number of invalid packets.
Pkt-Type	Packet type.
Total	Total number of packets.
Drops	Number of dropped packets.
Errors	Number of erroneous packets.

Field	Description
REQ_CHALLENGE	Challenge request packet the portal authentication server sent to the access device.
ACK_CHALLENGE	Challenge acknowledgment packet the access device sent to the portal authentication server.
REQ_AUTH	Authentication request packet the portal authentication server sent to the access device.
ACK_AUTH	Authentication acknowledgment packet the access device sent to the portal authentication server.
REQ_LOGOUT	Logout request packet the portal authentication server sent to the access device.
ACK_LOGOUT	Logout acknowledgment packet the access device sent to the portal authentication server.
AFF_ACK_AUTH	Affirmation packet the portal authentication server sent to the access device after receiving an authentication acknowledgment packet.
NTF_LOGOUT	Forced logout notification packet the access device sent to the portal authentication server.
REQ_INFO	Information request packet.
ACK_INFO	Information acknowledgment packet.
NTF_USERDISCOVER	User discovery notification packet the portal authentication server sent to the access device.
NTF_USERIPCHANGE	User IP change notification packet the access device sent to the portal authentication server.
AFF_NTF_USERIPCHAN	User IP change success notification packet the portal authentication server sent to the access device.
ACK_NTF_LOGOUT	Forced logout acknowledgment packet the portal authentication server sent to the access device.
NTF_HEARTBEAT	Server heartbeat packet the portal authentication server periodically sent to the access device.
NTF_USER_HEARTBEAT	User synchronization packet the portal authentication server sent to the access device.
ACK_NTF_USER_HEARTBEAT	User synchronization acknowledgment packet the access device sent to the portal authentication server.
NTF_CHALLENGE	Challenge request packet the access device sent to the portal authentication server.
NTF_USER_NOTIFY	User information notification packet the access device sent to the portal authentication server.
AFF_NTF_USER_NOTIFY	NTF_USER_NOTIFY acknowledgment packet

Field	Description
	the portal authentication server sent to the access device.
MAC-trigger server	Name of the MAC binding server.
REQ_MACBIND	MAC binding request packet the access device sent to the MAC binding server.
ACK_MACBIND	MAC binding acknowledgment packet the MAC binding server sent to the access device.
NTF_MTUSER_LOGON	User logon notification packet the access device sent to the MAC binding server.
NTF_MTUSER_LOGOUT	User logout notification packet the access device sent to the MAC binding server.
REQ_MTUSER_OFFLINE	User offline request packet that the MAC binding server sent to the access device for forcible logout of a user.
Extend-auth server	Type of the third-party authentication server: • **qq**—QQ authentication server. • **mail**—Email authentication server. • **wechat**—WeChat authentication server. • **cloud**—Lvzhou cloud authentication server.
Update interval	Interval at which the device sends online user information to the lvzhou cloud server, in seconds. This field is displayed if the third-party authentication server is the lvzhou cloud authentication server.
Success	Number of packets that have been successfully sent or received.
Timeout	Number of packets that timed out of establishing a connection to the third-party authentication server.
Conn-failure	Number of packets that failed to establish a connection to the third-party authentication server.
Deny	Number of packets denied access to the third-party authentication server. This field is displayed if the third-party authentication server is the email authentication server.
REQ_ACCESSTOKEN	Access token request packets the access device sent to the third-party authentication server. This field is displayed if the third-party authentication server is QQ, lvzhou cloud, or WeChat authentication server.
REQ_OPENID	Open ID request packets the access device sent to the third-party authentication server. This field is displayed if the third-party authentication server is the QQ authentication server.

Field	Description
REQ_USERINFO	User information request packets the access device sent to the third-party authentication server. This field is displayed if the third-party authentication server is the QQ, lvzhou cloud, or WeChat authentication server.
RESP_ACCESSTOKEN	Access token response packets the access device received from the third-party authentication server. This field is displayed if the third-party authentication server is the QQ, lvzhou cloud, or WeChat authentication server.
RESP_OPNEID	Open ID response packets the access device received from the third-party authentication server. This field is displayed if the third-party authentication server is the QQ authentication server.
RESP_USERINFO	User information response packets the access device received from the third-party authentication server. This field is displayed if the third-party authentication server is the QQ, lvzhou cloud, or WeChat authentication server.
REQ_POP3	POP3 authentication request packets the access device sent to the third-party authentication server. This field is displayed if the third-party authentication server is the email authentication server.
REQ_IMAP	IMAP authentication request packets the access device sent to the third-party authentication server. This field is displayed if the third-party authentication server is the email authentication server.
POST_ONLINEDATA	Cloud user information request packets the access device sent to the third-party authentication server. This field is displayed if the third-party authentication server is the lvzhou cloud authentication server.
RESP_ONLINEDATA	Cloud user information response packets the access device received from the third-party authentication server. This field is displayed if the third-party authentication server is the lvzhou cloud authentication server.
POST_OFFLINEUSER	Cloud user offline packets the access device sent to the third-party authentication server. This field is displayed if the third-party authentication server is the lvzhou cloud or WeChat authentication server.

Field	Description
AUTHENTICATION	Result of third-party authentication.

Related commands

reset portal packet statistics

display portal permit-rule statistics

Use **display portal permit-rule statistics** to display statistics for portal permit rules.

Syntax

display portal permit-rule statistics

Views

Any view

Predefined user roles

network-admin

network-operator

Usage guidelines

Portal permit rules refer to category 1 and category 2 portal filtering rules, which permit user packets to pass.

Examples

# Display statistics for portal permit rules.

```
<Sysname> display portal permit-rule statistics
Interface              Free rules           Fuzzy rules            User rules
WLAN-BSS1/0/1          2                      5                    10
WLAN-BSS2/0/1          2                      3                    6
```

Table 11 Command output

Field	Description
Interface	Interface on which portal permit rules are used.
Free rules	Number of permit rules generated based on configured portal-free rules, excluding permit rules generated based on fuzzy matches of destination-based portal-free rules.
Fuzzy rules	Number of permit rules generated based on fuzzy matches of destination-based portal-free rules.
User rules	Number of permit rules generated after portal users pass authentication.

display portal redirect statistics

Use **display portal redirect statistics** to display portal redirect packet statistics.

Syntax

display portal redirect statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays portal redirect packet statistics for all member devices.

Examples

# Display portal redirect packet statistics on the specified slot.

```
<Sysname> display portal redirect statistics slot 1
Slot 1:
HttpReq: 3
HttpResp: 3
HttpsReq: 6
HttpsResp: 6
```

Table 12 Command output

Field	Description
HttpReq	Total number of HTTP redirect requests.
HttpResp	Total number of HTTP redirect responses.
HttpsReq	Total number of HTTPS redirect requests.
HttpsResp	Total number of HTTPS redirect responses.

Related commands

reset portal redirect statistics

display portal rule

Use **display portal rule** to display portal filtering rules.

Syntax

display portal rule { **all** | **dynamic** | **static** } { **ap** *ap-name* [**radio** *radio-id*] | **interface** *interface-type interface-number* [**slot** *slot-number*] }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays all portal filtering rules, including dynamic and static portal filtering rules.

dynamic: Displays dynamic portal filtering rules, which are generated after users pass portal authentication. These rules allow packets with specific source IP addresses to pass the interface.

static: Displays static portal filtering rules, which are generated after portal authentication is enabled. The interface filters packets by these rules when portal authentication is enabled.

ap *ap-name*: Specifies an AP by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, underscores (_), left brackets ([), right brackets (]), slashes (/), and minus signs (-).

radio *radio-id*: Specifies a radio by its ID. The value range for the radio ID varies by device model. If you do not specify a radio, this command displays portal filtering rules for all radios of the AP.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays portal filtering rules for all member devices.

Examples

# Display all portal filtering rules on VLAN-interface 100.

```
<Sysname> display portal rule all interface vlan-interface 100
IPv4 portal rules on Vlan-interface100:
Rule 1
 Type                : Static
 Action              : Permit
 Protocol            : Any
 Status              : Active
 Source:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0
    Port           : Any
    MAC            : 0000-0000-0000
    Interface      : Vlan-interface100
    VLAN           : 100
 Destination:
    IP             : 192.168.0.111
    Mask           : 255.255.255.255
    Port           : Any

Rule 2
 Type                : Dynamic
 Action              : Permit
 Status              : Active
 Source:
    IP             : 2.2.2.2
    MAC            : 000d-88f8-0eab
    Interface      : Vlan-interface100
    VLAN           : 100
 Author ACL:
    Number         : 3001

Rule 3
 Type                : Static
 Action              : Redirect
 Status              : Active
 Source:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0
    Interface      : Vlan-interface100
    VLAN           : 100
    Protocol       : TCP
 Destination:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0
    Port           : 80

Rule 4:
 Type                : Static
 Action              : Deny
 Status              : Active
 Source:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0
    Interface      : Vlan-interface100
    VLAN           : Any
 Destination:
    IP             : 0.0.0.0
    Mask           : 0.0.0.0

IPv6 portal rules on Vlan-interface100:
Rule 1
 Type                : Static
 Action              : Permit
 Protocol            : Any
 Status              : Active
 Source:
    IP              : ::
    Prefix length   : 0
    Port            : Any
    MAC             : 0000-0000-0000
    Interface       : Vlan-interface100
    VLAN            : 100
 Destination:
    IP               : 3000::1
    Prefix length    : 64
    Port             : Any

Rule 2
 Type                : Dynamic
 Action              : Permit
 Status              : Active
 Source:
    IP              : 3000::1
    MAC             : 0015-e9a6-7cfe
    Interface       : Vlan-interface100
    VLAN            : 100
 Author ACL:
    Number          : 3001

Rule 3
 Type                : Static
 Action              : Redirect
 Status              : Active
 Source:
    IP              : ::
    Prefix length   : 0
    Interface       : Vlan-interface100
    VLAN            : 100
    Protocol        : TCP
 Destination:
    IP              : ::
    Prefix length   : 0
    Port            : 80

Rule 4:
 Type                : Static
 Action              : Deny
 Status              : Active
 Source:
    IP             : ::
    Prefix length  : 0
    Interface      : Vlan-interface100
    VLAN           : 100
 Destination:
    IP             : ::
    Prefix length  : 0
Author ACL:
    Number          : 3001

Rule 5:
 Type                : Static
 Action              : Match pre-auth ACL
 Status              : Active
 Source:
    Interface      : Vlan-interface100
Pre-auth ACL:
    Number          : 3002
```

# Display all portal filtering rules on AP **ap1**.

```
<Sysname> display portal rule all ap ap1
IPv4 portal rules on ap1:
Radio ID : 1
SSID     : portal
```

```
Rule 1
 Type                : Static
 Action              : Permit
 Protocol            : Any
 Status              : Active
 Source:
    IP        : 0.0.0.0
    Mask      : 0.0.0.0
    Port      : 23
    MAC       : 0000-0000-0000
    Interface : WLAN-BSS1/0/1
    VLAN      : any
 Destination:
    IP        : 192.168.0.111
    Mask      : 255.255.255.255
    Port      : Any

Rule 2
 Type                : Static
 Action              : Redirect
 Status              : Active
 Source:
    IP        : 0.0.0.0
    Mask      : 0.0.0.0
    Port      : Any
    MAC       : 0000-0000-0000
    Interface : WLAN-BSS1/0/1
    VLAN      : any
    Protocol  : TCP
 Destination:
    IP        : 0.0.0.0
    Mask      : 0.0.0.0
    Port      : 80

Rule 3
 Type                : Dynamic
 Action              : Permit
 Status              : Active
 Source:
    IP        : 2.2.2.2
    Mask      : 255.255.255.255
    MAC       : 000d-88f8-0eab
    Interface : WLAN-BSS1/0/1
    VLAN      : 2
 Destination:
    IP        : 0.0.0.0
    Mask      : 0.0.0.0
```

Table 13 Command output

Field	Description
Radio ID	ID of the radio.
SSID	Service set identifier.
Rule	Number of the portal filtering rule. IPv4 portal filtering rules and IPv6 portal filtering rules are numbered separately.
Type	Type of the portal filtering rule: • **Static**—Static portal filtering rule. • **Dynamic**—Dynamic portal filtering rule.
Action	Action triggered by the portal filtering rule: • **Permit**—The interface allows packets to pass. • **Redirect**—The interface redirects packets. • **Deny**—The interface forbids packets to pass. • **Match pre-auth ACL**—The interface matches packets against the authorized ACL rules in the preauthentication domain.
Protocol	Transport layer protocol permitted by the portal filtering rule: • **Any**—Permits any transport layer protocol. • **TCP**—Permits TCP. • **UDP**—Permits UDP.
Status	Status of the portal filtering rule: • **Active**—The portal rule is effective. • **Unactuated**—The portal rule is not activated.
Source	Source information of the portal filtering rule.
IP	Source IP address.
Mask	Subnet mask of the source IPv4 address.
Prefix length	Prefix length of the source IPv6 address.
Port	Source transport layer port number.
MAC	Source MAC address.
Interface	Interface on which the portal filtering rule is implemented.
VLAN	Source VLAN ID.
Protocol	Protocol type for the portal filtering rule.
Destination	Destination information of the portal filtering rule.
IP	Destination IP address.
Port	Destination transport layer port number.
Mask	Subnet mask of the destination IPv4 address.
Prefix length	Prefix length of the destination IPv6 address.
Author ACL	Authorized ACL assigned to authenticated portal users. This field is displayed only for a dynamic portal filtering rule.
Pre-auth ACL	Authorized ACL assigned to preauthentication portal users. This field is displayed only for the **Match pre-auth ACL** action.
Number	Number of the authorized ACL. This field displays **None** if the AAA server does not assign an ACL.

display portal safe-redirect statistics

Use **display portal safe-redirect statistics** to display portal safe-redirect packet statistics.

Syntax

display portal safe-redirect statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays statistics for all member devices.

Examples

# Display portal safe-redirect packet statistics on the specified slot.

```
<Sysname> display portal safe-redirect statistics slot 1
Slot 1:
Redirect statistics:
  Success: 7
  Failure: 8
  Total  : 15

Method statistics:
  Get    : 11
  Post   : 1
  Others : 3

User agent statistics:
Safari: 3
Chrome: 2

Forbidden URL statistics:
www.qq.com: 4

Forbidden filename extension statistics:
.jpg: 0
```

Table 14 Command output

Field	Description
Success	Number of packets redirected successfully.
Failure	Number of packets failed redirection.
Total	Total number of packets.
Method statistics	Statistics of HTTP request methods.

Field	Description
Get	Number of packets with the **GET** request method.
Post	Number of packets with the **POST** request method.
Other	Number of packets with other request methods.
User agent statistics	Browser types (in HTTP User Agent) allowed by portal safe-redirect, and packet statistics for the browsers.
Forbidden URL statistics	URLs forbidden by portal safe-redirect, and packet statistics for the URLs.
Forbidden filename extension statistics	Filename extensions forbidden by portal safe-redirect, and packet statistics for the filename extensions.

Related commands

reset portal safe-redirect statistics

display portal server

Use **display portal server** to display information about portal authentication servers.

Syntax

display portal server [*server-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

server-name: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify the *server-name* argument, this command displays information about all portal authentication servers.

Examples

# Display information about portal authentication server **pts**.

```
<Sysname> display portal server pts
Portal server: pts
  Type                    : IMC
  IP                      : 192.168.0.111
  VPN instance            : vpn1
  Port                    : 50100
  Server detection        : Timeout 60s  Action: log, trap
  User synchronization    : Timeout 200s
  Status                  : Up
  Exclude-attribute       : Not configured
  Logout notification     : Retry 3 interval 5s
```

Table 15 Command output

Field	Description
Type	Portal authentication server type: • **CMCC**: CMCC server. • **IMC**: IMC server.
Portal server	Name of the portal authentication server.
IP	IP address of the portal authentication server.
VPN instance	Name of the VPN instance to which the portal authentication server belongs. This field is not supported in the current software version.
Port	Listening port on the portal authentication server.
Server detection	Parameters for portal authentication server detection: • Detection timeout in seconds. • Actions (**log** and **trap**) triggered by the reachability status change of the portal authentication server.
User synchronization	User idle timeout in seconds for portal user synchronization.
Status	Reachability status of the portal authentication server: • **N/A**—Portal authentication server detection is disabled. Reachability status of the server is unknown. • **Up**—Portal authentication server detection is enabled. The server is reachable. • **Down**—Portal authentication server detection is enabled. The server is unreachable.
Exclude-attribute	Attributes that are not carried in portal protocol packets sent to the portal authentication server.
Logout-notification	Maximum number of times and the interval (in seconds) for retransmitting a logout notification packet.

Related commands

- **portal enable**
- **portal server**
- **server-detect** (portal authentication server view)
- **user-sync**

display portal user

Use **display portal user** to display information about portal users.

Syntax

display portal user { **all** | **ap** *ap-name* [**radio** *radio-id*] | **auth-type** { **cloud** | **email** | **local** | **normal** | **qq** | **wechat** } | **interface** *interface-type interface-number* | **ip** *ip-address* | **ipv6** *ipv6-address* | **mac** *mac-address* | **pre-auth** [**interface** *interface-type interface-number* | **ip** *ip-address* | **ipv6** *ipv6-address*] | **username** *username* } [**brief** | **verbose**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays information about all portal users.

ap *ap-name*: Specifies an AP by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, underscores (_), left brackets ([), right brackets (]), slashes (/), and minus signs (-).

radio *radio-id*: Specifies a radio by its ID. The value range for the radio ID varies by device model. If you do not specify a radio, this command displays information about portal users for all radios of the AP.

auth-type: Specifies an authentication type.

cloud: Specifies the cloud authentication (a cloud portal authentication server performs portal authentication on portal users).

email: Specifies the email authentication.

local: Specifies the local authentication (a local portal authentication server performs portal authentication on portal users).

normal: Specifies the normal authentication (a remote portal authentication server performs portal authentication on portal users).

qq: Specifies QQ authentication.

wechat: Specifies WeChat authentication.

interface *interface-type interface-number*: Displays information about portal users on the specified interface.

ip *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

mac *mac-address*: Specifies the MAC address of a portal user, in the format of H-H-H.

username *username*: Specifies the username of a portal user, a case-sensitive string of 1 to 253 characters. The username cannot contain the domain name.

pre-auth: Displays information about preauthentication portal users. A preauthentication user is a user who is authorized with the authorization attributes in a preauthentication domain before portal authentication. If you do not specify the **pre-auth** keyword, this command displays information about authenticated portal users.

brief: Displays brief information about portal users.

verbose: Displays detailed information about portal users.

Usage guidelines

If you specify neither the **brief** nor the **verbose** keyword, this command displays portal authentication-related information for all portal users.

Examples

# Display information about all portal users.

```
<Sysname> display portal user all
Total portal users: 1
Username: def
  AP name: ap1
  Radio ID: 1
  SSID: portal
  Portal server: pts
  State: Online
  VPN instance: vpn1
  MAC               IP                 VLAN   Interface
  000d-88f8-0eac    4.4.4.4            2     Bss1/2
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: 3000
```

# Display information about portal users that perform normal portal authentication.

```
<Sysname> display portal user auth-type normal
Total normal users: 1
Username: abc
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC               IP                 VLAN   Interface
  000d-88f8-0eab    2.2.2.2            2      WLAN-BSS1/0/1
  Authorization information:
    DHCP IP pool: N/A
    User profile: abc (active)
    Session group profile: cd (inactive)
    ACL number: N/A
```

# Display information about the portal user whose MAC address is 000d-88f8-0eab.

```
<Sysname> display portal user mac 000d-88f8-0eab
Username: abc
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC               IP                 VLAN   Interface
  000d-88f8-0eab    2.2.2.2            2      WLAN-BSS1/0/1
  Authorization information:
    DHCP IP pool: N/A
    User profile: abc (active)
    Session group profile: cd (inactive)
    ACL number: N/A
```

# Display information about the portal user whose username is **abc**.

```
<Sysname> display portal user username abc
Username: abc
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC               IP                 VLAN   Interface
  000d-88f8-0eab    2.2.2.2            2      WLAN-BSS1/0/1
  Authorization information:
    DHCP IP pool: N/A
    User profile: abc (active)
    Session group profile: cd (inactive)
    ACL number: N/A
```

Table 16 Command output

Field	Description
Total portal users	Total number of portal users.
Total normal users	Total number of portal users that perform normal authentication.
Total local users	Total number of portal users that perform local authentication.
Total email users	Total number of portal users that perform email authentication.
Total cloud users	Total number of portal users that perform cloud authentication.
Total QQ users	Total number of portal users that perform QQ authentication.
Total WeChat users	Total number of portal users that perform WeChat authentication.
Username	Name of the user.
AP name	Name of the AP.
Radio ID	ID of the radio.
SSID	Service set identifier.
Portal server	Name of the portal authentication server.
State	Current state of the portal user: • **Initialized**—The user is initialized and ready for authentication. • **Authenticating**—The user is being authenticated. • **Authorizing**—The user is being authorized. • **Online**—The user is online.
VPN instance	Name of the VPN instance to which the portal user belongs. If the portal user is on a public network, this field displays **N/A**. This field is not supported in the current software version.
MAC	MAC address of the portal user.
IP	IP address of the portal user.
VLAN	VLAN where the portal user resides.
Interface	Access interface of the portal user.
Authorization information	Authorization information for the portal user.
DHCP IP pool	Name of the authorized IP address pool. If no IP address pool is authorized for the portal user, this field displays **N/A**.
User profile	Authorized user profile: • **N/A**—The AAA server authorizes no user profile. • **active**—The AAA server has authorized the user profile successfully. • **inactive**—The AAA server failed to authorize the user profile or the user profile does not exist on the device.
ACL number	Authorized ACL:

Field	Description
	• **N/A**—The AAA server authorizes no ACL. • **active**—The AAA server has authorized the ACL successfully. • **inactive**—The AAA server failed to authorize the ACL or the ACL does not exist on the device.

# Display detailed information about the portal user with IP address with IP address 18.18.0.20.

```
<Sysname> display portal user ip 18.18.0.20 verbose
Basic:
AP name: ap1
  Radio ID: 1
  SSID: portal
  Current IP address: 18.18.0.20
  Original IP address: 18.18.0.20
  Username: chap1
  User ID: 0x10000001
  Access interface: WLAN_BSS1/0/1
  Service-VLAN/Customer-VLAN: 50/-
  MAC address: 7854-2e1c-c59e
  Authentication type: Normal
  Domain name: portal
  VPN instance: N/A
  Status: Online
  Portal server: pt
  Vendor: Apple
  Portal authentication method: Direct
AAA:
  Realtime accounting interval: 720s, retry times: 5
  Idle cut: N/A
  Session duration: 0 sec, remaining: 0 sec
  Remaining traffic: N/A
  Login time: 2014-12-25 10:47:53 UTC
  Online duration (hh:mm:ss): 1:53:7
  DHCP IP pool: N/A
ACL&Multicast:
  ACL number: N/A
  User profile: N/A
  Session group profile: N/A
  Max multicast addresses: 4
Flow statistic:
  Uplink packets/bytes: 6/412
  Downlink packets/bytes: 0/0
```

Table 17 Command output

Field	Description
AP name	Name of the AP.
Radio ID	Radio ID.

Field	Description
SSID	Service set identifier.
Current IP address	IP address of the portal user after passing authentication.
Original IP address	IP address of the portal user during authentication.
Username	Name of the portal user.
User ID	Portal user ID.
Access interface	Access interface of the portal user.
Service-VLAN/Customer-VLAN	Public VLAN/Private VLAN to which the portal user belongs. If no VLAN is configured for the portal user, this field displays **-/-**.
MAC address	MAC address of the portal user.
Authentication type	Type of portal authentication: • **Normal**—Normal authentication. • **Local**—Local authentication. • **Email**—Email authentication. • **Cloud**—Cloud authentication. • **QQ**—QQ authentication. • **WeChat**—WeChat authentication.
Domain	ISP domain name for portal authentication.
VPN instance	MPLS L3VPN to which the portal user belongs. If the portal user is on a public network, this field displays **N/A**. This field is not supported in the current software version.
Status	Status of the portal user: • **Authenticating**—The user is being authenticated. • **Authorizing**—The user is being authorized. • **Waiting SetRule**—Deploying portal filtering rules to the user. • **Online**—The user is online. • **Waiting Traffic**—Waiting for traffic from the user. • **Stop Accounting**—Stopping accounting for the user. • **Done**—The user is offline.
Portal server	Name of the portal server.
Vendor	Vendor name of the endpoint.
Portal authentication method	Portal authentication method on the access interface. This field displays **Direct** if direct authentication is enabled.
AAA	AAA information about the portal user.
Realtime accounting interval	Interval for sending real-time accounting updates, and the maximum number of accounting attempts. If the real-time accounting is not authorized, this field displays **N/A**.
Idle-cut	Idle timeout period and the minimum traffic threshold. If idle-cut is not authorized, this field displays **N/A**.
Session duration	Session duration and the remaining session time. If the session duration is not authorized, this field displays **N/A**.

Field	Description
Remaining traffic	Remaining traffic for the portal user. If the remaining traffic is not authorized, this field displays **N/A**.
Login time	Time when the user logged in. The field uses the device time format, for example, 2023-1-19 2:42:30 UTC.
ITA policy name	Name of the intelligent target accounting policy.
DHCP IP pool	Authorized DHCP IP address pool. If no DHCP IP address pool is authorized for the portal user, this field displays **N/A**.
ACL number	Authorized ACL: • **N/A**—The AAA server authorizes no ACL. • **active**—The AAA server has authorized the ACL successfully. • **inactive**—The AAA server failed to authorize the ACL or the ACL does not exist on the device.
User profile	Authorized user profile: • **N/A**—The AAA server authorizes no user profile. • **active**—The AAA server has authorized the user profile successfully. • **inactive**—The AAA server failed to authorize the user profile or the user profile does not exist on the device.
Session group profile	Authorized session group profile: • **N/A**—The AAA server authorizes no session group profile. • **active**—The AAA server has authorized the session group profile successfully. • **inactive**—The AAA server failed to authorize the session group profile or the session group profile does not exist on the device.
Max multicast addresses	Maximum number of multicast groups the portal user can join.
Multicast address list	Multicast group list the portal user can join. If no multicast group is authorized, this field displays **N/A**.
Flow statistic	Flow statistics for the portal user.
Uplink packets/bytes	Packet and byte statistics of the upstream traffic.
Downlink packets/bytes	Packet and byte statistics of the downstream traffic.

# Display brief information about all portal users.

```
<Sysname> display portal user all brief
IP address        MAC address       Online duration       Username
4.4.4.4           000d-88f8-0eac    1:53:7                def
```

Table 18 Command output

Field	Description
IP address	IP address of the portal user.
MAC address	MAC address of the portal user.
Online duration	Online duration of the portal user, in hh:ss:mm.
Username	Username of the portal user.

Related commands

portal enable

display portal user count

Use **display portal user count** to display the number of portal users.

Syntax

display portal user count

Views

Any view

Predefined user roles

network-admin

Examples

# Display the number of portal users.

```
<Sysname> display portal user count
Total number of users: 1
```

Related commands

- **portal enable**
- **portal delete-user**

display portal web-server

Use **display portal web-server** to display information about portal Web servers.

Syntax

display portal web-server [*server-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

server-name: Specifies a portal Web server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify the *server-name* argument, this command displays information about all portal Web servers.

Examples

# Display information about portal Web server **wbs**.

```
<Sysname> display portal web-server wbs
Portal Web server: wbs
    Type             : IMC
    URL              : http://www.test.com/portal
    URL parameters   : userurl=http://www.test.com/welcome
                       userip=source-address
    VPN instance     : Not configured
    Server detection : Interval: 120s  Attempts: 5  Action: log, trap
    IPv4 status      : Up
    IPv6 status      : N/A
    Captive-bypass   : Enabled
    If-match        : original-url:  http://2.2.2.2, redirect-url:  http://192.168.56.2
```

Table 19 Command output

Field	Description
Type	Portal Web server type: • **CMCC**—CMCC server. • **IMC**—IMC server.
Portal Web server	Name of the portal Web server.
URL	URL of the portal Web server.
URL parameters	URL parameters for the portal Web server.
VPN instance	Name of the VPN instance to which the portal Web server belongs. This field is not supported in the current software version.
Server detection	Parameters for portal Web server detection: • Detection interval in seconds. • Maximum number of detection attempts. • Actions (**log** and **trap**) triggered by the reachability status change of the portal Web server.
IPv4/IPv6 status	Current state of the portal Web server: • **N/A**—Portal Web server detection is disabled. Reachability status of the server is unknown. • **Up**—Portal Web server detection is enabled. The server is reachable. • **Down**—Portal Web server detection is enabled. The server is unreachable.
Captive-bypass	Status of the captive-bypass feature: • **Disabled**—Captive-bypass is disabled. • **Enabled**—Captive-bypass is enabled. • **Optimize Enabled**—Optimized captive-bypass is enabled.
If-match	Match rules configured for URL redirection.

Related commands

- **portal enable**
- **portal web-server**
- **server-detect** (portal Web server view)

display web-redirect rule

Use **display web-redirect rule** to display information about Web redirect rules.

Syntax

display web-redirect rule { **ap** *ap-name* [**radio** *radio-id*] **|** **interface** *interface-type interface-number* [**slot** *slot-number*] }

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

ap *ap-name*: Specifies an AP by its name, a case-insensitive string of 1 to 64 characters. The string can contain letters, digits, underscores (_), left brackets ([), right brackets (]), forward slashes (/), and hyphens (-).

radio *radio-id*: Specifies a radio by its ID. The value range for this argument varies by device model. If you do not specify this option, the command displays Web redirect rules for all radios of the AP.

interface *interface-type interface-number*: Specifies an interface by its type and number.

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command displays Web redirect rules for the master device.

Examples

# Display all Web redirect rules on VLAN-interface 100.

```
<Sysname> display web-redirect rule interface vlan-interface 100
IPv4 web-redirect rules on vlan-interface 100:
Rule 1:
 Type                 : Dynamic
 Action               : Permit
 Status               : Active
 Source:
    IP              : 192.168.2.114
    VLAN            : Any

Rule 2:
 Type                 : Static
 Action               : Redirect
 Status               : Active
 Source:
    VLAN            : Any
    Protocol        : TCP
 Destination:
    Port            : 80

IPv6 web-redirect rules on vlan-interface 100:
Rule 1:
 Type                 : Static
 Action               : Redirect
 Status               : Active
 Source:
    VLAN            : Any
    Protocol       : TCP
 Destination:
    Port           : 80
```

# Display all Web redirect rules on AP **ap1**.

```
<Sysname> display web-redirect rule ap ap1
IPv4 web-redirect rules on ap1:
Radio ID: 1
SSID     : portal
Rule 1:
Type                : Dynamic
 Action              : Permit
 Status              : Active
 Source:
    IP             : 192.168.2.114
    VLAN           : Any

Rule 2:
 Type                : Static
 Action              : Redirect
 Status              : Active
 Source:
    VLAN           : Any
    Protocol       : TCP
 Destination:
    Port           : 80
```

Table 20 Command output

Field	Description
Radio ID	ID of the radio.
SSID	Service set identifier.
Rule	Number of the Web redirect rule.
Type	Type of the Web redirect rule: • **Static**—Static Web redirect rule, generated when the Web redirect feature takes effect. • **Dynamic**—Dynamic Web redirect rule, generated when a user visits a redirect webpage.
Action	Action in the Web redirect rule: • **Permit**—Allows packets to pass. • **Redirect**—Redirects the packets.
Status	Status of the Web redirect rule: • **Active**—The Web redirect rule is effective. • **Deactive**—The Web redirect rule is not effective.
Source	Source information in the Web redirect rule.
IP	Source IP address.
Mask	Subnet mask of the source IPv4 address.
Prefix length	Prefix length of the source IPv6 address.

Field	Description
VLAN	Source VLAN. If not specified, this field displays **Any**.
Protocol	Transport layer protocol in the Web redirect rule: - **Any**—No transport layer protocol is limited. - **TCP**—Transmission Control Protocol.
Destination	Destination information in the Web redirect rule.
Port	Destination transport layer port number. The default port number is 80.

exclude-attribute (MAC binding server view)

Use **exclude-attribute** to exclude an attribute from portal protocol packets.

Use **undo exclude-attribute** to not exclude an attribute from portal protocol packets.

Syntax

exclude-attribute *attribute-number*

undo exclude-attribute *attribute-number*

Default

No attributes are excluded from portal protocol packets.

Views

MAC binding server view

Predefined user roles

network-admin

Parameters

attribute-number: Specifies an attribute by its number in the range of 1 to 255.

Usage guidelines

Support of the portal authentication server for portal protocol attributes varies by the server type. During MAC-trigger authentication, the device and the server cannot communicate if the device sends the portal authentication server a packet that contains an attribute unsupported by the server.

To address this issue, you can configure this command to exclude the unsupported attributes from portal protocol packets sent to the portal authentication server.

You can specify multiple excluded attributes.

Table 21 describes all attributes of the portal protocol.

Table 21 Portal attributes

Name	Number	Description
UserName	1	Name of the user to be authenticated.
PassWord	2	User password in plaintext form.
Challenge	3	Random challenge for CHAP authentication.
ChapPassWord	4	CHAP password encrypted by MD5.
TextInfo	5	The device uses this attribute to transparently transport prompt information of a RADIUS server

Name	Number	Description
		or packet error information to the portal authentication server. The attribute value can be any string excluding the end character '\0'. This attribute can exist in any packet from the device to the portal server. A packet can contain multiple TextInfo attributes. As a best practice, carry only one TextInfo attribute in a packet.
UpLinkFlux	6	Uplink (output) traffic of the user, an 8-byte unsigned integer, in KB.
DownLinkFlux	7	Downlink (input) traffic of the user, an 8-byte unsigned integer, in KB.
Port	8	Port information, a string excluding the end character '\0'.
IP-Config	9	The device uses this attribute in ACK_LOGOUT (Type=0x06) and NTF_LOGOUT (Type=0x08) packets to indicate that the current user IP address must be released. The portal server must notify the user to release the public IP address through DHCP. The device will reallocate a private IP address to the user.
BAS-IP	10	IP address of the access device.
Session-ID	11	Identification of a portal user. Generally, the value of this attribute is the MAC address of the portal user.
Delay-Time	12	Delay time for sending a packet. This attributes exists in NTF_LOGOUT (Type=0x08) packets.
User-List	13	List of IP addresses of an IPv4 portal user.
EAP-Message	14	An EAP attribute that needs to be transported transparently. This attribute is applicable to EAP TLS authentication. Multiple EAP-Message attributes can exist in a portal authentication packet.
User-Notify	15	Value of the hw_User_Notify attribute in a RADIUS accounting response. This attribute needs to be transported transparently.
BAS-IPv6	100	IPv6 address of the access device.
UserIPv6-List	101	List of IPv6 addresses of an IPv6 portal user.

Examples

# Exclude the BAS-IP attribute (number 10) from portal packets sent to MAC binding server 123.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server 123
[Sysname-portal-mac-trigger-server-123] exclude-attribute 10
```

Related commands

display portal server

exclude-attribute (portal authentication server view)

Use **exclude-attribute** to exclude an attribute from portal protocol packets.

Use **undo exclude-attribute** to not exclude an attribute from portal protocol packets.

Syntax

exclude-attribute *number* { **ack-auth** | **ack-logout** | **ntf-logout** }

undo exclude-attribute *number* { **ack-auth** | **ack-logout** | **ntf-logout** }

Default

No attributes are excluded from portal protocol packets.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

number: Specifies an attribute by its number in the range of 1 to 255.

ack-auth: Excludes the attribute from ACK_AUTH packets.

ack-logout: Excludes the attribute from ACK_LOGOUT packets.

ntf-logout: Excludes the attribute from NTF_LOGOUT packets.

Usage guidelines

Support of the portal authentication server for portal protocol attributes varies by the server type. If the device sends the portal authentication server a packet that contains an attribute unsupported by the server, the device and the server cannot communicate.

To address this issue, you can configure this command to exclude the unsupported attributes from specific portal protocol packets sent to the portal authentication server.

You can specify multiple excluded attributes. For an excluded attribute, you can specify multiple types of portal protocol packets (**ack-auth**, **ntf-logout**, and **ack-logout**).

Table 21 describes all attributes of the portal protocol.

Examples

# Exclude the UpLinkFlux attribute (number 6) from portal ACK_AUTH packets.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] exclude-attribute 6 ack-auth
```

Related commands

display portal server

free-traffic threshold

Use **free-traffic threshold** to set the free-traffic threshold for portal users.

Use **undo free-traffic threshold** to restore the default.

Syntax

free-traffic threshold *value*

undo free-traffic threshold

Default

The free-traffic threshold is 0 bytes.

Views

MAC binding server view

Predefined user roles

network-admin

Parameters

value: Specifies the free-traffic threshold in the range of 0 to 10240000 bytes. If the free-traffic threshold is set to 0, the device immediately triggers MAC-based quick portal authentication for a user once the user's traffic is detected.

Usage guidelines

A user can access the network without authentication if the user's network traffic (sent and received) is below the free-traffic threshold. When the user's network traffic reaches the threshold, the device triggers MAC-based quick portal authentication for the user.

If the user passes portal authentication, the device clears the user traffic statistics. If the user fails authentication, the device does not trigger MAC-based quick authentication for the user before the MAC-trigger entry ages out. When the MAC-trigger entry ages out, the device clears the user traffic statistics.

After traffic statistics are cleared for a user, the device repeats the MAC-based portal authentication procedure for the user. For more information about the MAC-based portal authentication procedure, see *Security Configuration Guide*.

In wireless networks where APs are configured to forward client data traffic, APs report traffic statistics to the AC at a regular interval. The AC can determine whether a user's traffic exceed the free-traffic threshold only after receiving the traffic statistics report from the associated AP. To set the interval for APs to report traffic statistics to the AC, use the **portal client-traffic-report interval** command.

Examples

# Set the free-traffic threshold for portal users to 10240 bytes.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] free-traffic threshold 10240
```

Related commands

display portal mac-trigger-server

if-match

Use **if-match** to configure a match rule for URL redirection.

Use **undo if-match** to delete a URL redirection match rule.

Syntax

if-match { **original-url** *url-string* **redirect-url** *url-string* [**url-param-encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string*] | **user-agent** *string* **redirect-url** *url-string* }

undo if-match { **original-url** *url-string* | **user-agent** *user-agent* }

Default

No URL redirection match rules exists.

Views

Portal Web server view

Predefined user roles

network-admin

Parameters

original-url *url-string*: Specifies a URL string to match the URL in HTTP requests of a portal user. The specified URL must be a complete URL starting with **http://** or **https://**, a case-sensitive string of 1 to 256 characters.

redirect-url *url-string*: Specifies the URL to which the user is redirected. The specified URL must be a complete URL starting with **http://** or **https://**, a case-sensitive string of 1 to 256 characters.

url-param-encryption: Specifies an encryption algorithm to encrypt the parameters carried in the redirection URL. If you do not specify an encryption algorithm, the parameters carried in the redirection URL are not encrypted.

aes: Specifies the AES algorithm.

des: Specifies the DES algorithm.

key: Specifies a key for encryption.

cipher: Specifies a key in encrypted form.

simple: Specifies a key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the case-sensitive key string. The string length varies by the selected encryption method:

- If **des cipher** is specified, the string length is 41 characters.
- If **des simple** is specified, the string length is 8 characters.
- If **aes cipher** is specified, the string length is 1 to 73 characters.
- If **aes simple** is specified, the string length is 1 to 31 characters.

user-agent *user-agent*: Specifies a user agent string to match the HTTP User-Agent string in HTTP requests. The user agent string is a case-sensitive string of 1 to 255 characters. HTTP User-Agent string in HTTP requests includes information about hardware manufacturer, operating system, browser, and search engine.

Usage guidelines

A URL redirection match rule matches HTTP requests by user-requested URL or User-Agent information, and redirects the matching HTTP requests to the specified redirection URL.

For a user to successfully access a redirection URL, configure a portal-free rule to allow HTTP requests destined for the redirection URL to pass. For information about configuring portal-free rules, see the **portal free-rule** command.

For a portal Web server, you can configure the **url** command and the **if-match** command for URL redirection. The **url** command redirects all HTTP or HTTPS requests from unauthenticated users to the portal Web server for authentication. The **if-match** command allows for flexible URL redirection by redirecting specific HTTP or HTTPS requests to specific redirection URLs. If both commands are executed, the **if-match** command takes priority to perform URL redirection.

If you configure encryption for parameters in the redirection URL, you must add an encryption prompt field after the redirection URL address. For example, to redirect HTTP requests to URL 10.1.1.1 with encrypted URL parameters, specify the redirection URL as http://10.1.1.1?yyyy=. The value of yyyy depends on the portal Web server configuration. For more information, see the portal Web server configuration guide.

Examples

# Configure a match rule to redirect HTTP requests destined for the URL **http://www.abc.com.cn** to the URL **http://192.168.0.1**.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match original-url http://www.abc.com.cn redirect-url
http://192.168.0.1
```

# Configure a match rule to redirect HTTP requests that carry the user agent string **5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36** to the URL **http://192.168.0.1.**

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] if-match user-agent
5.0(WindowsNT6.1)AppleWebKit/537.36(KHTML,likeGecko)Chrome/36.0.1985.125Safari/537.36
redirect-url http://192.168.0.1
```

Related commands

- **display portal web-server**
- **portal free-rule**
- **url**
- **url-parameter**

ip (MAC binding server view)

Use **ip** to specify the IP address of a MAC binding server.

Use **undo ip** to restore the default.

Syntax

ip *ipv4-address* [**key** { **cipher | simple** } *string*]

undo ip

Default

The IP address of the MAC binding server is not specified.

Views

MAC binding server view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IP address of a MAC binding server.

key: Specifies a shared key to be used to authenticate packets between the device and the MAC binding server. If you do not specify a shared key, the device and MAC binding server do not authenticate the packets between them.

cipher: Specifies a shared key in encrypted form.

simple: Specifies a shared key in plaintext form. For security purposes, the key specified in plaintext form will be stored in encrypted form.

string: Specifies the shared key. Its plaintext form is a case-sensitive string of 1 to 64 characters. Its encrypted form is a case-sensitive string of 33 to 117 characters.

Usage guidelines

Portal packets exchanged between the device and MAC binding server carry an authenticator that is generated with the shared key. The receiver uses the authenticator to verify the correctness of the received portal packets.

If you execute this command multiple times in the same MAC binding server view, the most recent configuration takes effect.

Examples

# Specify the IP address of the MAC binding server as **192.168.0.111** and the plaintext key as **portal**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] ip 192.168.0.111 key simple portal
```

Related commands

display portal mac-trigger-server

ip (portal authentication server view)

Use **ip** to specify the IP address of an IPv4 portal authentication server.

Use **undo ip** to delete the IP address of the IPv4 portal authentication server.

Syntax

ip *ipv4-address* [**key** { **cipher** | **simple** } *string*]

undo ip

Default

The IP address of the IPv4 portal authentication server is not specified.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IP address of the IPv4 portal authentication server.

key: Specifies a shared key for communication with the portal authentication server. Portal packets exchanged between the access device and the portal authentication server carry an authenticator that is generated with the shared key. The receiver uses the authenticator to check the correctness of the received portal packets.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

string: Specifies the shared key. A plaintext shared key is a case-sensitive string of 1 to 64 characters. A ciphertext shared key is a case-sensitive string of 33 to 117 characters.

Usage guidelines

A portal authentication server has only one IP address. Therefore, in portal authentication server view, only one IP address exists. A newly configured IP address (IPv4 or IPv6) overrides the old address.

For security purposes, all keys, including keys specified in plain text, are saved in cipher text.

Examples

# Configure the IP address of the IPv4 portal authentication server **pts** as **192.168.0.111** and the plaintext key as **portal**.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] ip 192.168.0.111 key simple portal
```

Related commands

- **display portal server**
- **portal server**

ipv6

Use **ipv6** to specify the IP address of an IPv6 portal authentication server.

Use **undo ipv6** to delete the IP address of the IPv6 portal authentication server.

Syntax

ipv6 *ipv6-address* [**key** { **cipher** | **simple** } *string*]

undo ipv6

Default

The IP address of the IPv6 portal authentication server is not specified.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

ipv6-address: Specifies the IP address of the IPv6 portal authentication server.

key: Specifies a shared key for communication with the portal authentication server. Portal packets exchanged between the access device and the portal authentication server carry an authenticator that is generated with the shared key. The receiver uses the authenticator to check the correctness of the received portal packets.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

string: Specifies the shared key. A plaintext shared key is a case-sensitive string of 1 to 64 characters. A ciphertext shared key is a case-sensitive string of 33 to 117 characters.

Usage guidelines

A portal authentication server has only one IP address. Therefore in portal authentication server view, only one IP address exists. A newly configured IP address (IPv4 or IPv6) overrides the old address.

For security purposes, all keys, including keys specified in plain text, are saved in cipher text.

Examples

# Configure the IP address of the IPv6 portal authentication server **pts** as **2000::1** and the plaintext key as **portal**.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] ipv6 2000::1 key simple portal
```

Related commands

- **display portal server**
- **portal server**

local-binding aging-time

Use **local-binding aging-time** to set the aging time for local MAC-account binding entries.

Use **undo local-binding aging-time** to restore the default.

Syntax

local-binding aging-time *minutes*

undo local-binding aging-time

Default

The aging time for local MAC-account binding entries is 720 minutes.

Views

MAC binding server view

Predefined user roles

network-admin

Parameters

minutes: Specifies the aging time for local MAC-account binding entries. The value range for this argument is 60 to 129600 minutes.

Usage guidelines

The local MAC-account binding entry of a portal user is deleted when the entry ages out. If the device detects traffic for the user next time, the device creates a local MAC-trigger entry for the user.

If you disable local MAC-trigger authentication, the device does not delete existing local MAC-account binding entries. These entries are automatically deleted when they age out.

Examples

# Set the aging time of local MAC-account binding entries to 240 minutes for MAC binding server **mts**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] local-binding aging-time 240
```

Related commands

- **display portal mac-trigger-server**
- **local-binding enable**

local-binding enable

Use **local-binding enable** to enable local MAC-trigger authentication.

Use **undo local-binding enable** to disable local MAC-trigger authentication.

Syntax

local-binding enable

undo local-binding enable

Default

Local MAC-trigger authentication is disabled.

Views

MAC binding server view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to act as a local MAC binding server to provide local MAC-trigger authentication for local portal users.

After a user passes portal authentication for the first time, the access device (local MAC binding server) generates a local MAC binding entry for the user. The local MAC binding entry records the MAC address and authentication information (username and password) of the user. Then, the user can be automatically connected to the network without manual authentication for subsequent network access attempts.

Examples

# Enable local MAC-trigger authentication for MAC binding server **mts**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] local-binding enable
```

Related commands

- **display portal mac-trigger-server**
- **local-binding aging-time**

logon-page bind

Use **logon-page bind** to bind an SSID, endpoint name, or endpoint type to an authentication page file.

Use **undo logon-page bind** to unbind the SSID, endpoint name, or endpoint type from the authentication page file.

Syntax

logon-page bind { **device-type** { **computer** | **pad** | **phone** } | **device-name** *device-name* | **ssid** *ssid-name* } * **file** *file-name*

undo logon-page bind { **all** | **device-type** { **computer** | **pad** | **phone** } | **device-name** *device-name* | **ssid** *ssid-name* } *

Default

No SSID, endpoint name, or endpoint type is bound to an authentication page file.

Views

Local portal Web server view

Predefined user roles

network-admin

Parameters

all: Specifies all SSIDs, endpoint names, and endpoint types.

device-type *type-name*: Specifies an endpoint type.

computer: Specifies the endpoint type as computer.

pad: Specifies the endpoint type as tablet.

phone: Specifies the endpoint type as mobile phone.

device-name *device-name*: Specifies an endpoint by its name, a case-sensitive string of 1 to 127 characters. The specified endpoint name must have been predefined on the device. Otherwise, the bound authentication page file does not take effect.

ssid *ssidname*: Specifies an SSID by its name, a case-insensitive string of 1 to 32 characters. An SSID string can contain letters, digits, and spaces, but the start and end characters cannot be spaces. An SSID string cannot be **f**, **fi**, **fil**, or **file**.

file *filename*: Specifies an authentication page file by the file name (without the file storage directory). A file name is a string of 1 to 91 characters, and can contain letters, digits, and underscores (_). You must edit the authentication pages, compress them to a .zip file, and then upload the file to the root directory of the storage medium of the device.

Usage guidelines

This command implements customized authentication page pushing for portal users. After you configure this command, the device pushes authentication pages to users according to the user SSID, endpoint name, or endpoint type.

When a Web user triggers local portal authentication, the device searches for a binding that matches the user's SSID, endpoint name, and endpoint type.

- If the binding exists, the device pushes the bound authentication pages to the user.
- If multiple matching binding entries are found, the device selects an entry in the following order:
  - **a.** The entry that specifies the SSID, endpoint name, and endpoint type.
  - **b.** The entry that specifies the SSID and endpoint name.
  - **c.** The entry that specifies the SSID and endpoint type.
  - **d.** The entry that specifies only the SSID.
  - **e.** The entry that specifies the endpoint name and endpoint type.
  - **f.** The entry that specifies only the endpoint name.
  - **g.** The entry that specifies only the endpoint type.
- If the binding does not exist, the device pushes the default authentication pages to the user. If the default authentication page file is not specified (by using the **default-logon-page** command), the user cannot perform local portal authentication.

When you configure this command, follow these restrictions and guidelines:

- If the name or contents of the file in a binding entry are changed, you must reconfigure the binding.
- To reconfigure or modify a binding, simply re-execute this command, without canceling the existing binding.
- If you execute this command multiple times to bind an SSID, endpoint name, or endpoint type to different authentication page files, the most recent configuration takes effect.
- You can configure multiple binding entries on the device.

Examples

# Create a local portal Web server and specify HTTP to exchange information with clients.

```
<Sysname> system-view
[Sysname] portal local-web-server http
```

# Bind SSID **SSID1** to authentication page file **file1.zip**.

```
[Sysname-portal-local-websvr-http] logon-page ssid SSID1 file file1.zip
```

# Bind endpoint type **phone** to authentication page file **file2.zip**.

```
[Sysname-portal-local-websvr-http] logon-page device-type phone file file2.zip
```

Related commands

- **default-logon-page**
- **portal local-web-server**

logout-notify

Use **logout-notify** to set the maximum number of times and the interval for retransmitting a logout notification packet.

Use **undo logout-notify** to restore the default.

Syntax

logout-notify retry *retries* **interval** *interval*

undo logout-notify

Default

The device does not retransmit a logout notification packet.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

retry *retries*: Specifies the maximum number of retries, in the range of 1 to 5.

interval *interval*: Specifies the retry interval, in the range of 1 to 10 seconds.

Usage guidelines

A logout notification packet is a UDP packet that the device sends to the portal authentication server for forcibly logging out a portal user. To increase the delivery reliability, you can set the maximum number of times and the interval for retransmitting a logout notification packet.

After the device sends a logout notification packet for logging out a portal user, it waits for a response from the portal authentication server. If the device receives a response within the specified period of time (maximum number of retries × retry interval), it logs out and deletes the user immediately. If the device does not receive a response within the period of time, the device logs out and deletes the user when the period of time elapses.

Examples

# Set the maximum number of times for retransmitting a logout notification packet to 3 and the retry interval to 5 seconds.

```
<Sysname> system-view
[Sysname] portal server pt
[Sysname-portal-server-pt] logout-notify retry 3 interval 5
```

Related commands

display portal server

mail-domain-name

Use **mail-domain-name** to specify an email domain name for email authentication.

Use **undo mail-address** to restore the default.

Syntax

mail-domain-name *string*

undo mail-domain-name [*string*]

Default

No email domain names are specified for email authentication.

Views

Email authentication server view

Predefined user roles

network-admin

Parameters

string: Specifies an email domain name for email authentication, a case-sensitive string of 1 to 255 characters, in the format of @XXX.XXX.

Usage guidelines

After you configure this command, the device performs email authentication only on portal users that use the specified email domain names.

You can specify a maximum of 16 email domain names for email authentication.

Examples

# Specify **@qq.com** and **@sina.com** email domain names for email authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server mail
[Sysname-portal-extend-auth-server-mail] mail-domain-name @qq.com
[Sysname-portal-extend-auth-server-mail] mail-domain-name @Sina.com
```

Related commands

display portal extend-auth-server

mail-protocol

Use **mail-protocol** to specify protocols for email authentication.

Use **undo mail-protocol** to restore the default.

Syntax

mail-protocol { **imap** | **pop3** } *

undo mail-protocol

Default

No protocols are specified for email authentication.

Views

Email authentication server view

Predefined user roles

network-admin

Parameters

imap: Specifies the Internet Message Access Protocol (IMAP).

pop3: Specifies the Post Office Protocol 3 (POP3).

Usage guidelines

This command specifies email protocols that the device uses to interact with the email authentication server to perform authentication and authorization on portal users who uses email authentication.

Examples

# Specify the POP3 protocol for email authentication.

```
<Sysname> system-view
[Sysname] portal extend-auth-server mail
[Sysname-portal-extend-auth-server-mail] mail-protocol pop3
```

Related commands

display portal extend-auth-server

nas-port-type

Use **nas-port-type** to specify the NAS-Port-Type value carried in RADIUS requests sent to the RADIUS server.

Use **undo nas-port-type** to restore the default.

Syntax

nas-port-type *value*

undo nas-port-type

Default

The NAS-Port-Type value carried in RADIUS requests is 0.

Views

MAC binding server view

Predefined user roles

network-admin

Parameters

value: Specifies the NAS-Port-Type value in the range of 1 to 255.

Usage guidelines

Some MAC binding servers identify MAC-based quick portal authentication by a specific NAS-Port-Type value in received RADIUS requests. To communicate with such a MAC binding server, you must configure the device to use the NAS-Port-Type value required by the MAC binding server.

Examples

# Set the NAS-Port-Type value to 30 for RADIUS requests sent to MAC binding server **mts**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] nas-port-type 30
```

Related commands

display portal mac-trigger-server

port (MAC binding server view)

Use **port** to set the UDP port number the MAC binding server uses to listen for MAC binding query packets.

Use **undo port** to restore the default.

Syntax

port *port-number*

undo port

Default

The MAC binding server listens for MAC binding query packets on UDP port 50100.

Views

MAC binding server view

Predefined user roles

network-admin

Parameters

port-number: Specifies the listening UDP port number in the range of 1 to 65534.

Usage guidelines

The specified port number must be the same as the query listening port number configured on the MAC binding server.

Examples

# Set the UDP port number to **1000** for MAC binding server **pts** to listen for MAC binding query packets.

```
<sysname> system-view
[sysname] portal mac-trigger-server mts
[sysname-portal-mac-trigger-server-mts] port 1000
```

Related commands

display portal mac-trigger-server

port (portal authentication server view)

Use **port** to set the destination UDP port number used by the device to send unsolicited portal packets to the portal authentication server.

Use **undo port** to restore the default.

Syntax

port *port-number*

undo port

Default

The access device uses 50100 as the destination UDP port number for unsolicited portal packets.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

port-number: Specifies a destination UDP port number the access device uses to send unsolicited portal packets to the portal authentication server. The value range for this argument is 1 to 65534.

Usage guidelines

The specified port must be the port that listens to portal packets on the portal authentication server.

Examples

# Set the destination UDP port number to **50000** for the device to send unsolicited portal packets to the portal authentication server **pts**.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] port 50000
```

Related commands

portal server

portal { bas-ip | bas-ipv6 }

Use **portal** { **bas-ip** | **bas-ipv6** } to configure the BAS-IP or BAS-IPv6 attribute carried in the portal packets sent to a portal authentication server.

Use **undo portal** { **bas-ip** | **bas-ipv6** } to delete the BAS-IP or BAS-IPv6 attribute setting.

Syntax

portal { **bas-ip** *ipv4-address* | **bas-ipv6** *ipv6-address* }

undo portal { **bas-ip** | **bas-ipv6** }

Default

The BAS-IP attribute of an IPv4 portal reply packet sent to the portal authentication server is the source IPv4 address of the packet. The BAS-IPv6 attribute of an IPv6 portal reply packet sent to the portal authentication server is the source IPv6 address of the packet.

The BAS-IP attribute of an IPv4 portal notification packet sent to the portal authentication server is the IPv4 address of the interface. The BAS-IPv6 attribute of an IPv6 portal notification packet sent to the portal authentication server is the IPv6 address of the interface.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

bas-ip *ipv4-address*: Specifies BAS-IP for portal packets sent by the interface. The *ipv4-address* argument must be the IPv4 address of the device, and cannot be an all-zero address, all-one address, class D address, class E address, or loopback address.

bas-ip6 *ipv6-address*: Specifies BAS-IPv6 for portal packets sent by the interface. The *ipv6-address* argument must be the IPv6 address of the device, and cannot be a multicast address, all-zero address, or link-local address.

Usage guidelines

If the device runs Portal 2.0, unsolicited portal packets (such as a logout notification packet) sent to the portal authentication server must carry the BAS-IP attribute. If the device runs Portal 3.0, unsolicited portal packets sent to the portal authentication server must carry the BAS-IP or BAS-IPv6 attribute.

After this command takes effect, the source IP address for unsolicited notification portal packets the device sends to the portal authentication server is the configured BAS-IP or BAS-IPv6. Otherwise the source IP address of the packets is the IP address of the interface.

You must configure the BAS-IP or BAS-IPv6 attribute on a portal authentication-enabled interface or service template if the following conditions are met:

- The portal authentication server is an H3C IMC server.
- The portal device IP address specified on the portal authentication server is not the IP address of the portal packet output interface.

Examples

# Configure the BAS-IP attribute of outgoing portal packets as **2.2.2.2** on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal bas-ip 2.2.2.2
```

# Configure the BAS-IP attribute of outgoing portal packets as **2.2.2.2** on service template **service1**.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] portal bas-ip 2.2.2.2
```

Related commands

display portal

portal { ipv4-max-user | ipv6-max-user }

Use **portal** { **ipv4-max-user** | **ipv6-max-user** } to set the maximum number of portal users allowed on a VLAN interface or a service template.

Use **undo portal** { **ipv4-max-user** | **ipv6-max-user** } to restore the default.

Syntax

portal { **ipv4-max-user** | **ipv6-max-user** } *max-number*

undo portal { **ipv4-max-user** | **ipv6-max-user** }

Default

The maximum number of portal users on a VLAN interface or a service template is not limited.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of portal users allowed on a VLAN interface or a service template, in the range of 1 to 4294967295.

Usage guidelines

If the specified maximum number is smaller than the number of current online portal users on a VLAN interface or a service template, the limit can be set successfully and does not impact the online portal users. However, the device does not allow new portal users to log in from the interface or service template until the number drops down below the limit.

Make sure the maximum combined number of IPv4 and IPv6 portal users specified on all VLAN interfaces or service templates does not exceed the system-allowed maximum number. Otherwise, the exceeding portal users will not be able to log in to the device.

Examples

# Set the maximum number of IPv4 portal users to 100 on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal ipv4-max-user 100
```

# Set the maximum number of IPv4 portal users to 100 on service template **service1**.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal ipv4-max-user 100
```

Related commands

- **display portal user**
- **portal max-user**

portal apply mac-trigger-server

Use **portal apply mac-trigger-server** to specify a MAC binding server.

Use **undo portal apply mac-trigger-server** to restore the default.

Syntax

portal apply mac-trigger-server *server-name*

undo portal apply mac-trigger-server

Default

No MAC binding server is specified.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

server-name: Specifies a MAC binding server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

For MAC-based quick portal authentication to take effect, perform the following tasks:

- Configure normal portal authentication.
- Configure a MAC binding server.
- Specify the MAC binding server on a portal enabled VLAN interface or service template.

Examples

# Specify MAC binding server **mts** on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal apply mac-trigger-server mts
```

Related commands

portal mac-trigger-server

portal apply web-server

Use **portal** [**ipv6**] **apply web-server** to specify a portal Web server on a VLAN interface or a service template. The device redirects the HTTP or HTTPS requests sent by unauthenticated portal users to the portal Web server.

Use **undo portal** [**ipv6**] **apply web-server** to delete the portal Web server specified on the VLAN interface or service template.

Syntax

portal [**ipv6**] **apply web-server** *server-name* [**secondary**]

undo portal [**ipv6**] **apply web-server** [*server-name*]

Default

No portal Web server is specified on a VLAN interface or a service template.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an IPv6 portal Web server. If the server is an IPv4 portal Web server, do not specify this keyword.

secondary: Specifies the backup portal Web server. If you do not specify this keyword, the specified server is the primary portal Web server.

server-name: Specifies a portal Web server to be specified on the interface by its name, a case-sensitive string of 1 to 32 characters. The name must already exist. If you do not specify a server name in the **undo** form of this command, all portal Web servers on the interface or service template are removed.

Usage guidelines

IPv4 and IPv6 portal authentication can both be enabled on a VLAN interface or on a service template. You can specify both a primary portal Web server and a backup portal Web server after enabling each type (IPv4 or IPv6) of portal authentication.

The device first uses the primary portal Web server for portal authentication. When the primary portal Web server is unreachable but the backup portal Web server is reachable, the device uses the backup portal Web server. When the primary portal Web server becomes reachable, the device switches back to the primary portal Web server for portal authentication.

To automatically switch between the primary portal Web server and the backup portal Web server, configure portal Web server detection on both servers.

Examples

# Specify portal Web server **wbs** as the primary portal Web server on VLAN-interface 100 for portal authentication.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal apply web-server wbs
```

# Specify portal Web server **wbs** as the backup portal Web server on service template **service1** for portal authentication.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] portal apply web-server wbs secondary
```

Related commands

- **display portal**
- **portal fail-permit server**
- **portal web-server**
- **server-detect** (portal web-server view)

portal auth-error-record enable

Use **portal auth-error-record enable** to enable portal authentication error recording.

Use **undo portal auth-error-record enable** to disable portal authentication error recording.

Syntax

portal auth-error-record enable

undo portal auth-error-record enable

Default

Portal authentication error recording is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to save all portal authentication error records and to periodically send the records to the lvzhou cloud server or other servers.

Examples

# Enable portal authentication error recording.

```
<Sysname> system-view
[Sysname] portal auth-error-record enable
```

Related commands

display portal auth-error-record

portal auth-error-record export

Use **portal auth-error-record export** to export portal authentication error records to a path.

Syntax

portal auth-error-record export url *url-string* [**start-time** *start-date start-time* **end-time** *end-date end-time*]

Views

System view

Predefined user roles

network-admin

Parameters

url *url-string*: Specifies the URL to which portal authentication error records are exported. The URL is a case-insensitive string of 1 to 255 characters.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2100. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

Usage guidelines

The device supports FTP, TFTP, and HTTP file transfer methods. Table 22 describes the valid URL format for each method.

Table 22 URL formats

Protocol	URL format	Remarks
FTP	ftp://*username*[:*password*]@*server-address*[:*port-number*]/*file-path* Example: **ftp://a:1@1.1.1.1/authfail/**	The username and password must be the same as those on the server. If the server authenticates only the username, no password is required.
TFTP	tftp://*server-address*[:*port-number*]/*file-path* Example: **tftp://1.1.1.1/ autherror/**	N/A
HTTP	http://*username*[:*password*]@*server-address*[:*port-number*]/*file-path* Example: **http://1.1.1.1/autherror/**	The username and password must be the same as those on the server. If the server authenticates only the username, no password is required.

If the server address is an IPv6 address, bracket the IPv6 address to distinguish the IPv6 address from the port number. For example, if the server address is **2001::1** and the port number is 21, the URL is **ftp://test:test@[2001::1]:21/test/**.

Examples

# Export all portal authentication error records to path **tftp://1.1.1.1/record/autherror/**.

```
<Sysname> system-view
[Sysname] portal auth-error-record export tftp://1.1.1.1/record/autherror/
```

# Export portal authentication error records in the time range from 2016/3/4 14:20 to 2016/3/4 15:00 to path **tftp://1.1.1.1/record/autherror/**.

```
<Sysname> system-view
[Sysname] portal auth-error-record export tftp://1.1.1.1/record/autherror/ start-time
2016/3/4 14:20 end-time 2016/3/4 15:00
```

Related commands

- **display portal auth-error-record**

- **portal auth-error-record enable**
- **reset portal auth-error-record**

portal auth-error-record max

Use **portal auth-error-record max** to set the maximum number of portal authentication error records.

Use **undo portal auth-error-record max** to restore the default.

Syntax

portal auth-error-record max *number*

undo portal auth-error-record max

Default

The maximum number of portal authentication error records is 32000.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of portal authentication error records, in the range of 1 to 4294967295.

Usage guidelines

When the maximum number of portal authentication error records is reached, the new record overwrites the oldest one.

Examples

# Set the maximum number of portal authentication error records to 50.

```
<Sysname> system-view
[Sysname] portal auth-error-record max 50
```

Related commands

display portal auth-error-record

portal auth-fail-record enable

Use **portal auth-fail-record enable** to enable portal authentication failure recording.

Use **undo portal auth-fail-record enable** to disable portal authentication failure recording.

Syntax

portal auth-fail-record enable

undo portal auth-fail-record enable

Default

Portal authentication failure recording is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to save portal authentication failure records and to periodically send the records to the lvzhou cloud server or other servers.

Examples

# Enable portal authentication failure recording.

```
<Sysname> system-view
[Sysname] portal auth-fail-record enable
```

Related commands

display portal auth-fail-record

portal auth-fail-record export

Use **portal auth-fail-record export** to export portal authentication failure records to a path.

Syntax

portal auth-fail-record export url *url-string* [**start-time** *start-date start-time* **end-time** *end-date end-time*]

Views

System view

Predefined user roles

network-admin

Parameters

url *url-string*: Specifies the URL to which portal authentication failure records are exported. The URL is a case-insensitive string of 1 to 255 characters.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2100. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

Usage guidelines

The device supports FTP, TFTP, and HTTP file transfer methods. Table 23 describes the valid URL format for each method.

Table 23 URL formats

Protocol	URL format	Remarks
FTP	ftp://*username*[:*password*]@*server-address*[:*port-number*]/*file-path* Example: **ftp://a:1@1.1.1.1/authfail/**	The username and password must be the same as those on the server. If the server authenticates only the username, no password is required.
TFTP	tftp://*server-address*[:*port-number*]/*file-path* Example: **tftp://1.1.1.1/ autherror/**	N/A
HTTP	http://*username*[:*password*]@*server-address*[:*port-number*]/*file-path*	The username and password must be the same as those on the server.

Protocol	URL format	Remarks
	Example: **http://1.1.1.1/autherror/**	If the server authenticates only the username, no password is required.

If the server address is an IPv6 address, bracket the IPv6 address to distinguish the IPv6 address from the port number. For example, if the server address is **2001::1** and the port number is 21, the URL is **ftp://test:test@[2001::1]:21/test/**.

Examples

# Export all portal authentication failure records to path **tftp://1.1.1.1/record/authfail/**.

```
<Sysname> system-view
[Sysname] portal auth-fail-record export url tftp://1.1.1.1/record/authfail/
```

# Export portal authentication failure records in the time range from 2016/3/4 14:20 to 2016/3/4 15:00 to path **tftp://1.1.1.1/record/authfail/**.

```
<Sysname> system-view
[Sysname] portal auth-fail-record export tftp://1.1.1.1/record/authfail/ start-time
2016/3/4 14:20 end-time 2016/3/4 15:00
```

Related commands

- **display portal auth-fail-record**
- **portal auth-fail-record enable**
- **reset portal auth-fail-record**

portal auth-fail-record max

Use **portal auth-fail-record max** to set the maximum number of portal authentication failure records.

Use **undo portal auth-fail-record max** to restore the default.

Syntax

portal auth-fail-record max *number*

undo portal auth-fail-record max

Default

The maximum number of portal authentication failure records is 32000.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of portal authentication failure records, in the range of 1 to 4294967295.

Usage guidelines

When the maximum number of portal authentication failure records is reached, the new record overwrites the oldest one.

Examples

# Set the maximum number of portal authentication failure records to 50.

```
<Sysname> system-view
[Sysname] portal auth-fail-record max 50
```

Related commands

display portal auth-fail-record

portal authorization strict-checking

Use **portal authorization strict-checking** to enable strict checking on portal authorization information.

Use **undo portal authorization strict-checking** to restore the default.

Syntax

portal authorization { **acl** | **user-profile** } **strict-checking**

undo portal authorization { **acl** | **user-profile** } **strict-checking**

Default

The strict checking mode is disabled. If an authorized ACL or user profile does not exist on the device or the ACL or user profile fails to be deployed, the user will not be logged out.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

acl: Enables strict checking on authorized ACLs.

user-profile: Enables strict checking on authorized user profiles.

Usage guidelines

You can enable strict checking on authorized ACLs, authorized user profiles, or both. If you enable both strict ACL checking and user profile checking, the user will be logged out if either checking fails.

An ACL/user profile checking fails when the authorized ACL/user profile does not exist on the device or the ACL/user profile fails to be deployed.

Examples

# Enable strict checking on authorized ACLs on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal authorization acl strict-checking
```

# Enable strict checking on authorized ACLs on service template **service1**.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] portal authorization acl strict-checking
```

Related commands

display portal

portal captive-bypass optimize delay

Use **portal captive-bypass optimize delay** to set the captive-bypass detection timeout time.

Use **undo portal captive-bypass optimize delay** to restore the default.

Syntax

portal captive-bypass optimize delay *seconds*

undo portal captive-bypass optimize delay

Default

The captive-bypass detection timeout time is 6 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

seconds: Specifies the captive-bypass detection timeout time, in the range of 6 to 60 seconds.

Usage guidelines

This command applies only to iOS mobile clients.

With optimized captive-bypass enabled, the device automatically pushes the portal authentication page to iOS mobile devices when they are connected to the network. Users can perform authentication on the page or press the home button to return to the desktop without performing authentication, and the Wi-Fi connection is not disabled.

Optimized captive-bypass might fail in some conditions. For example, when the network condition is poor, the device cannot receive a server detection packet from an iOS mobile device within the captive-bypass detection timeout time. Therefore, the Wi-Fi connection might be terminated on the iOS mobile device. To avoid such failure, you can set a longer captive-bypass detection timeout time when the network condition is poor.

Examples

# Set the captive-bypass detection timeout time to 20 seconds.

```
<Sysname> system-view
[Sysname] portal captive-bypass optimize delay 20
```

Related commands

captive-bypass enable

portal client-gateway interface

Use **portal client-gateway interface** to configure the gateway for portal clients to access the AC during authentication.

Use **undo portal client-gateway interface** to restore the default.

Syntax

portal client-gateway interface *interface-type interface-number*

undo portal client-gateway interface

Default

No gateway is specified for portal clients to access the AC during authentication.

Views

System view

Predefined user roles

network-admin

Parameters

interface-type interface-number: Specifies an interface by its type and number.

Usage guidelines

When the client traffic forwarding location is at APs, execute this command to specify the gateway for portal clients to access the AC during authentication.

Examples

# Configure VLAN-interface 100 as the gateway for portal clients to access the AC during authentication.

```
<Sysname> system-view
[Sysname] portal client-gateway interface vlan-interface 10
```

portal client-traffic-report interval

Use **portal client-traffic-report interval** to set the interval at which an AP reports traffic statistics to the AC.

Use **undo portal client-traffic-report interval** to restore the default.

Syntax

portal client-traffic-report interval *interval*

undo portal client-traffic-report *interval*

Default

An AP reports traffic statistics to the AC at an interval of 60 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the interval at which an AP reports traffic statistics to the AC, in the range of 1 to 3600 seconds.

Usage guidelines

Before you execute this command, make sure the client traffic forwarding location is at APs.

Examples

# Set the interval at which an AP reports traffic statistic to the AC to 120 seconds.

```
<Sysname> system-view
[Sysname] portal client-traffic-report interval 120
```

Related commands

client forwarding-location (*WLAN Command Reference*)

portal delete-user

Use **portal delete-user** to log out online portal users.

Syntax

portal delete-user { *ipv4-address* **| all | auth-type** { **cloud | email | local | normal | qq | wechat** } **| interface** *interface-type interface-number* **| ipv6** *ipv6-address* **| mac** *mac-address* **| username** *username* }

Views

System view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies the IP address of an IPv4 online portal user.

all: Specifies IPv4 and IPv6 online portal users on all interfaces.

auth-type: Specifies online portal users by the authentication type.

cloud: Specifies the cloud authentication.

email: Specifies the email authentication.

local: Specifies the local authentication.

normal: Specifies the normal authentication.

qq: Specifies the QQ authentication.

wechat: Specifies the WeChat authentication.

interface *interface-type interface-number*: Specifies an interface by its type and number. If you specify this option, this command logs out all IPv4 and IPv6 online portal users on the interface.

ipv6 *ipv6-address*: Specifies the IP address of an IPv6 online portal user.

mac *mac-address*: Specifies the MAC address of an online portal user, in the format of H-H-H.

username *username*: Specifies the username of an online portal user, a case-sensitive string of 1 to 253 characters. The username cannot contain the domain name.

Examples

# Log out the portal user whose IP address is 1.1.1.1.

```
<Sysname> system-view
[Sysname] portal delete-user 1.1.1.1
```

# Log out the portal user whose MAC address is 000d-88f8-0eab.

```
<Sysname> system-view
[Sysname] portal delete-user mac 000d-88f8-0eab
```

# Log out all portal users that come online through email authentication.

```
<Sysname> system-view
[Sysname] portal delete-user auth-type email
```

# Log out the portal user whose username is **abc**.

```
<Sysname> system-view
[Sysname] portal delete-user username abc
```

Related commands

display portal user

portal device-id

Use **portal device-id** to specify the device ID.

Use **undo portal device-id** to restore the default.

Syntax

portal device-id *device-id*

undo portal device-id

Default

No device ID is specified for the device.

Views

System view

Predefined user roles

network-admin

Parameters

device-id: Specifies a device ID for the device, a case-sensitive string of 1 to 63 characters.

Usage guidelines

The portal authentication server uses device IDs to identify the devices that send protocol packets to the portal server.

Make sure the configured device ID is different than any other access devices communicating with the same portal authentication server.

Examples

# Set the device ID of the device to **0002.0010.100.00**.

```
<Sysname> system-view
[Sysname] portal device-id 0002.0010.100.00
```

portal domain

Use **portal** [**ipv6**] **domain** to configure a portal authentication domain on a VLAN interface or a service template. All portal users accessing through the VLAN interface must use the authentication domain.

Use **undo portal** [**ipv6**] **domain** to delete the configured portal authentication domain.

Syntax

portal [**ipv6**] **domain** *domain-name*

undo portal [**ipv6**] **domain**

Default

No portal authentication domain is configured on a VLAN interface or a service template.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an authentication domain for IPv6 portal users. Do not specify this keyword for IPv4 portal users.

domain-name: Specifies an ISP authentication domain by its name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

You can specify both an IPv4 portal authentication domain and an IPv6 portal authentication domain on a VLAN interface or on a service template.

Do not specify the **ipv6** keyword for IPv4 portal users.

Examples

# Configure the authentication domain for IPv4 portal users as **my-domain** on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal domain my-domain
```

# Configure the authentication domain for IPv4 portal users as **my-domain** on service template **service1**.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] portal domain my-domain
```

Related commands

display portal

portal enable

Use **portal** [**ipv6**] **enable** to enable portal authentication.

Use **undo portal** [**ipv6**] **enable** to disable portal authentication.

Syntax

In VLAN interface view:

portal enable method direct

portal ipv6 enable method direct

undo portal [**ipv6**] **enable**

In service template view:

portal [**ipv6**] **enable method direct**

undo portal [**ipv6**] **enable**

Default

Portal authentication is disabled.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

ipv6: Enables IPv6 portal authentication. If you do not specify this keyword, IPv4 portal authentication is enabled.

Usage guidelines

Make sure the device supports IPv6 ACL and IPv6 forwarding before you enable IPv6 portal authentication.

You can enable both IPv4 and IPv6 portal authentication on a VLAN interface or on a service template.

Do not enable portal authentication on both a VLAN interface and a service template.

Examples

# Enable IPv4 portal authentication on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal enable method direct
```

# Enable IPv4 portal authentication on service template **service1**.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] portal enable method direct
```

Related commands

display portal

portal extend-auth domain

Use **portal extend-auth domain** to specify the authentication domain for third-party authentication.

Use **undo portal extend-auth domain** to remove the authentication domain for third-party authentication.

Syntax

portal extend-auth domain *domain-name*

undo portal extend-auth domain

Default

No authentication domain is specified for third-party authentication.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

domain-name: Specifies an ISP domain by its name, a case-insensitive string of 1 to 255 characters.

Usage guidelines

The specified ISP domain takes effect only on IPv4 portal users that use third-party authentication.

Examples

# Specify authentication domain **my-domain** for third-party authentication on service template **service1**.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] portal extend-auth domain my-domain
```

Related commands

display portal

portal extend-auth-server

Use **portal extend-auth-server** to create a third-party authentication server and enter its view, or enter the view of an existing third-party authentication server.

Use **undo portal extend-auth-server** to delete a third-party authentication server.

Syntax

portal extend-auth-server { **qq** | **mail** }

undo portal extend-auth-server { **qq** | **mail** }

Default

No third-party authentication servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

qq: Specifies the QQ authentication server.

mail: Specifies the email authentication server.

Usage guidelines

The device supports using the QQ or email authentication server as a third-party portal authentication server for portal authentication. A portal user can use a QQ or email account instead of a portal account to perform portal authentication. If the user passes third-party authentication, the third-party server notifies the third-party authentication success of the user to the device. Then, the device interacts with the local portal Web server to complete the remaining process of portal authentication.

Examples

# Create a QQ authentication server and enter its view.

```
<Sysname> system-view
[Sysname] portal extend-auth-server qq
[Sysname-portal-extend-auth-server-qq]
```

# Create an email authentication server and enter its view.

```
<Sysname> system-view
[Sysname] portal extend-auth-server mail
[Sysname-portal-extend-auth-server-mail]
```

Related commands

display portal extend-auth-server

portal fail-permit server

Use **portal** [**ipv6**] **fail-permit server** to enable the portal fail-permit feature for a portal authentication server.

Use **undo portal** [**ipv6**] **fail-permit server** to disable the portal fail-permit feature for the portal authentication server.

Syntax

portal [**ipv6**] **fail-permit server** *server-name*

undo portal [**ipv6**] **fail-permit server**

Default

Portal fail-permit is disabled for the portal authentication server.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an IPv6 portal authentication server. If you do not specify this keyword, the specified authentication server is IPv4 portal authentication server.

server-name: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

When portal fail-permit is enabled for a portal authentication server and portal Web servers on a VLAN interface, the interface disables portal authentication in either of the following conditions:

- All portal Web servers are unreachable.
- The specified portal authentication server is unreachable.

Portal authentication resumes on the VLAN interface when the specified portal authentication server and a minimum of one portal Web server becomes reachable. After portal authentication resumes, users who failed portal authentication and unauthenticated portal users need to pass authentication to access network resources. Portal users who have passed authentication can continue accessing network resources.

If you configure this command multiple times, the most recent configuration takes effect.

Examples

# Enable portal fail-permit for portal authentication server **pts1** on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal fail-permit server pts1
```

Related commands

display portal

portal fail-permit web-server

Use **portal** [**ipv6**] **fail-permit web-server** to enable the portal fail-permit feature for portal Web servers.

Use **undo portal** [**ipv6**] **fail-permit web-server** to disable the portal fail-permit feature for portal Web servers.

Syntax

portal [**ipv6**] **fail-permit web-server**

undo portal [**ipv6**] **fail-permit web-server**

Default

Portal fail-permit is disabled for portal Web servers.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

ipv6: Specifies IPv6 portal Web servers. If you do not specify this keyword, IPv4 portal Web servers are specified.

Usage guidelines

When portal fail-permit is enabled for a portal authentication server and portal Web servers, the VLAN interface or service template disables portal authentication in either of the following conditions:

- All portal Web servers are unreachable.
- The specified portal authentication server is unreachable.

Portal authentication resumes on the VLAN interface or service template when the specified portal authentication server and a minimum of one portal Web server becomes reachable. After portal authentication resumes, users who failed portal authentication and unauthenticated portal users need to pass authentication to access network resources. Portal users who have passed authentication can continue accessing network resources.

On the same VLAN interface or service template, the portal Web server is unreachable when both the primary and backup portal Web servers are unreachable.

Examples

# Enable portal fail-permit for the portal Web servers on service template **service1**.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] portal fail-permit web-server
```

Related commands

display portal

portal free-all except destination

Use **portal free-all except destination** to configure an IPv4 portal authentication destination subnet on a VLAN interface.

Use **undo portal free-all except destination** to delete the IPv4 portal authentication destination subnets on the VLAN interface.

Syntax

portal free-all except destination *ipv4-network-address* { *mask-length* | *mask* }

undo portal free-all except destination [*ipv4-network-address*]

Default

No IPv4 portal authentication destination subnet is configured on a VLAN interface. Portal users must pass portal authentication to access any subnet.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

ipv4-network-address: Specifies an IPv4 portal authentication subnet address.

mask-length: Specifies the subnet mask length for the authentication subnet address, in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal format.

Usage guidelines

Portal users on a VLAN interface are authenticated when accessing the specified authentication destination subnet (except IP addresses and subnets specified in portal-free rules). The users can access other subnets without portal authentication.

You can configure multiple authentication destination subnets.

If you do not specify the *ipv4-network-address* argument in the **undo portal free-all except destination** command, this commands deletes all IPv4 portal authentication destination subnets on the interface.

Examples

# Configure an IPv4 portal authentication destination subnet of **11.11.11.0/24** on VLAN-interface 2. Portal users need to pass authentication to access this subnet and can access other subnets without authentication.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname–Vlan-interface2] portal free-all except destination 11.11.11.0 24
```

Related commands

display portal

portal free-rule

Use **portal free-rule** to configure an IP-based portal-free rule.

Use **undo portal free-rule** to delete portal-free rules.

Syntax

portal free-rule *rule-number* { **destination ip** { *ip-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **source ip** { *ip-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } * [**interface** *interface-type interface-number*]

portal free-rule *rule-number* { **destination ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-numbe*r | **udp** *udp-port-number*] | **source ipv6** { *ipv6-address prefix-length* | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] } * [**interface** *interface-type interface-number*]

undo portal free-rule { *rule-number* | **all** }

Default

No IP-based portal-free rule is configured.

Views

System view

Predefined user roles

network-admin

Parameters

rule-number: Specifies a portal-free rule number in the range of 1 to 4294967295.

destination: Specifies the destination information.

source: Specifies the source information.

ip *ip-address*: Specifies an IPv4 address for the portal-free rule.

{ *mask-length* | *mask* }: Specifies the subnet mask of the IPv4 address. The value range for the *mask-length* argument is 0 to 32. The *mask* argument is in dotted decimal format.

ipv6 *ipv6-address*: Specifies an IPv6 address for the portal-free rule.

prefix-length: Specifies the prefix length of the IPv6 address, in the range of 0 to 128.

ip any: Represents any IPv4 address.

ipv6 any: Represents any IPv6 address.

tcp *tcp-port-number*: Specifies a TCP port number for the portal-free rule, in the range of 0 to 65535.

udp *udp-port-number*: Specifies a UDP port number for the portal-free rule, in the range of 0 to 65535.

all: Specifies all portal-free rules.

interface *interface-type interface-number*: Specifies a VLAN interface on which the portal-free rule takes effect.

Usage guidelines

You can specify both the **source** and **destination** keyword for a portal-free rule. If you specify only one keyword, the other keyword does not act as a filtering criterion.

If you specify both a source port number and a destination port number for a portal-free rule, the two port numbers must belong to the same transport layer protocol.

If you do not specify a VLAN interface, the portal-free rule takes effect on all portal-enabled VLAN interfaces.

You cannot configure two portal-free rules with the same filtering criteria.

Examples

# Configure an IPv4-based portal-free rule: specify the rule number as **1**, the source IP address as **10.10.10.1**/**24**, the destination IP address as **20.20.20.1**, the destination TCP port number as **23**, and the interface as VLAN-interface 100.

```
<Sysname> system-view
[Sysname] portal free-rule 1 destination ip 20.20.20.1 32 tcp 23 source ip 10.10.10.1 24
interface vlan-interface 100
```

With this rule, users in subnet 10.10.10.1/24 do not need to pass portal authentication through GigabitEthernet 1/0/1 when they access services provided on TCP port 23 of host 20.20.20.1.

# Configure an IPv6-based portal-free rule: specify the rule number as **2**, the source IP address as **2000::1**/**64**, the destination IP address as **2001::1**, the destination TCP port number as **23**, and the interface as VLAN-interface 100.

```
<Sysname> system-view
[Sysname] portal free-rule 2 destination ipv6 2001::1 128 tcp 23 source ip 2000::1 64
interface vlan-interface 100
```

With this rule, users in subnet 2000::1/64 do not need to pass portal authentication through VLAN-interface 100 when they access services provided on TCP port 23 of host 2001::1.

Related commands

display portal rule

portal free-rule destination

Use **portal free-rule destination** to configure a destination-based portal-free rule.

Use **undo portal free-rule** to delete portal-free rules.

Syntax

portal free-rule *rule-number* **destination** *host-name*

undo portal free-rule { *rule-number* | **all** }

Default

No destination-based portal-free rule is configured.

Views

System view

Predefined user roles

network-admin

Parameters

rule-number: Specifies a portal-free rule number in the range of 1 to 4294967295.

destination: Specifies the destination host.

host-name: Specifies the destination host by its name, a case-insensitive string that can contain letters, digits, hyphens (-), underscores (_), dots (.), and asterisks (*).

all: Specifies all portal-free rules.

Usage guidelines

You can configure a hostname in one of the following ways:

- **For exact match**—Specify a complete hostname. For example, if you configure the hostname as **abc.com.cn** in the portal-free rule, only packets that contain the hostname **abc.com.cn** match the rule. Packets that carry any other hostnames (such as **dfabc.com.cn**) do not match the rule.
- **For fuzzy match**—Specify a hostname by placing the asterisk (*) wildcard character at the beginning or end of the hostname string. For example, if you configure the hostname as ***abc.com.cn**, **abc***, or ***abc***, packets that carry the hostname ending with **abc.com.cn**, starting with **abc**, or including **abc** match the rule.

The asterisk (*) wildcard character represents any characters. The device treats multiple consecutive asterisks as one.

The configured hostname cannot contain only asterisks (*).

You cannot configure two destination-based portal-free rules with the same destination information. Otherwise the system prompts you that the same rule already exists.

Examples

# Configure a destination-based portal-free rule numbered **4** to allow portal users whose HTTP/HTTPS requests carry hostname **www.h3c.com** to access network resources without portal authentication.

```
<Sysname> system-view
```

```
[Sysname] portal free-rule 4 destination www.h3c.com
```

Related commands

display portal rule

portal free-rule source

Use **portal free-rule source** to configure a source-based portal-free rule. The filtering criteria include source MAC address, source interface, and source VLAN.

Use **undo portal free-rule** to delete portal-free rules.

Syntax

portal free-rule *rule-number* **source** { **ap** *ap-name* **|** { **interface** *interface-type interface-number* **| mac** *mac-address* **| vlan** *vlan-id* } * }

undo portal free-rule { *rule-number* **| all** }

Default

No source-based portal-free rule is configured.

Views

System view

Predefined user roles

network-admin

Parameters

rule-number: Specifies a portal-free rule number in the range of 1 to 4294967295.

ap *ap-name*: Specifies an AP by its name, a case-insensitive string of 1 to 64 characters. Valid characters are letters, digits, underscores (_), left brackets ([), right brackets (]), slashes (/), and minus signs (-). This option is applicable only when portal authentication is enabled on a service template.

interface *interface-type interface-number*: Specifies a source interface by its type and number for the portal-free rule.

mac *mac-address*: Specifies a source MAC address for the portal-free rule, in the form of H-H-H.

vlan *vlan-id*: Specifies a source VLAN ID for the portal-free rule.

all: Specifies all portal-free rules.

Usage guidelines

If you specify both the source VLAN and the source Layer 2 interface, the interface must be in the VLAN.

If portal users have come online before source-based portal-free rules are configured, the device keeps accounting on traffic of the users even if they match these rules.

Examples

# Configure a source-based portal-free rule numbered 3 to allow the portal user whose source MAC address is 1-1-1 from VLAN 10 to access network resources without portal authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 3 source mac 1-1-1 vlan 10
```

# Configure a source-based portal-free rule numbered 4 to allow portal users on AP 10 to access network resources without portal authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 4 source ap ap10
```

Related commands

display portal rule

portal host-check enable

Use **portal host-check enable** to enable validity check on wireless portal clients.

Use **undo portal host-check enable** to disable validity check on wireless portal clients.

Syntax

portal host-check enable

undo portal host-check enable

Default

The device checks wireless portal client validity according to ARP entries only.

Views

System view

Predefined user roles

network-admin

Usage guidelines

In wireless networks where the AP forwards client traffic, the AC does not have ARP entries for clients. Therefore, the AC cannot check the validity of portal clients by using ARP entries. To ensure that valid users can perform portal authentication, you must enable wireless client validity check on the AC.

This feature enables the AC to validate a client by looking up the client information in the WLAN snooping table, DHCP snooping table, and ARP table. If the client information exists, the AC determines the client to be valid for portal authentication.

Examples

# Enable validity check on wireless portal clients.

```
<Sysname> system-view
[Sysname] portal host-check enable
```

portal ipv6 free-all except destination

Use **portal ipv6 free-all except destination** to configure an IPv6 portal authentication destination subnet.

Use **undo portal ipv6 free-all except destination** to delete IPv6 portal authentication destination subnets.

Syntax

portal ipv6 free-all except destination *ipv6-network-address prefix-length*

undo portal ipv6 free-all except destination [*ipv6-network-address*]

Default

No IPv6 portal authentication destination subnet is configured on a VLAN interface. Portal users must pass portal authentication to access any IPv6 subnet.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

ipv6-network-address: Specifies an IPv6 portal authentication destination subnet.

prefix-length: Specifies the prefix length of the IPv6 subnet, in the range of 0 to 128.

Usage guidelines

Portal users on a VLAN interface are authenticated when accessing the specified authentication destination subnet (except IP addresses and subnets specified in portal-free rules). The users can access other subnets without portal authentication.

You can configure multiple authentication destination subnets.

If you do not specify the *ipv6-network-address* argument in the **undo portal ipv6 free-all except destination** command, this command deletes all IPv6 portal authentication destination subnets on the interface.

Examples

# Configure an IPv6 portal authentication destination subnet of **1::2/16** on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname–Vlan-interface2] portal ipv6 free-all except destination 1::2 16
```

Related commands

display portal

portal ipv6 user-detect

Use **portal ipv6 user-detect** to enable online detection of IPv6 portal users.

Use **undo portal user-detect** to disable online detection of IPv6 portal users.

Syntax

portal ipv6 user-detect type { **icmpv6 | nd** } [**retry** *retries*] [**interval** *interval*] [**idle** *time*]

undo portal ipv6 user-detect

Default

Online detection of IPv6 portal users is disabled.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

type: Specifies the detection type.

- **icmpv6**—ICMPv6 detection.
- **nd**—ND detection.

retry *retries*: Sets the maximum number of detection attempts, in the range of 1 to 10. The default value is 3.

interval *interval*: Sets a detection interval in the range of 1 to 1200 seconds. The default interval is 3 seconds.

idle *time*: Sets the user idle timeout in the range of 60 to 3600 seconds. The default is 180 seconds. When the timeout expires, online detection of portal users is started.

Usage guidelines

If the device receives no packets from a portal user within the idle time, the device detects the user's online status as follows:

- **ICMPv6 detection**—Sends ICMPv6 requests to the user at configurable intervals to detect the user status.
  - If the device receives a reply within the maximum number of detection attempts, it considers that the user is online and stops sending detection packets. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the device receives no reply after the maximum number of detection attempts, the device logs out the user.
- **ND detection**—Sends ND requests to the user and detects the ND entry status of the user at configurable intervals.
  - If the ND entry of the user is refreshed within the maximum number of detection attempts, the device considers that the user is online and stops detecting the user's ND entry. Then the device resets the idle timer and repeats the detection process when the timer expires.
  - If the ND entry of the user is not refreshed after the maximum number of detection attempts, the device logs out the user.

If firewall policies on the access device filter out ICMPv6 packets, ICMPv6 detection might fail and result in the logout of portal users. Make sure the access device does not block ICMPv6 packets before you enable ICMPv6 detection on an interface.

Examples

# Enable online detection of IPv6 portal users on VLAN-interface 100. Configure the detection type as **ND**, the maximum number of detection attempts as 5, the detection interval as 10 seconds, and the user idle timeout as 300 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal ipv6 user-detect type nd retry 5 interval 10 idle 300
```

Related commands

display portal

portal local-web-server

Use **portal local-web-server** to create a local portal Web server and enter its view, or enter the view of an existing local portal Web server.

Use **undo portal local-web-server** to delete the local portal Web server.

Syntax

portal local-web-server { **http** | **https** [**ssl-server-policy** *policy-name*] }

undo portal local-web-server { **http** | **https** }

Default

No local portal Web servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

http: Configures the local portal Web server to use HTTP to exchange authentication information with clients.

https: Configures the local portal Web server to use HTTPS to exchange authentication information with clients.

ssl-server-policy *policy-name*: Specifies an existing SSL server policy for HTTPS. The policy name is a case-insensitive string of 1 to 31 characters. If you do not specify this option, HTTPS is associated with the SSL server policy that uses the self-signed certificate. That SSL server policy supports all cipher suites.

Usage guidelines

After a local portal Web server is configured on the access device, the access device also acts as the portal Web server and the portal authentication server. No external portal Web server and portal authentication server are needed.

For a VLAN interface to use the local portal Web server, the URL of the portal Web server specified for the VLAN interface must meet the following requirements:

- The IP address in the URL must be a local IP address on the device (except the IP address 127.0.0.1).
- The URL must be ended with **/portal/**. For example: **http://1.1.1.1/portal/**.

You cannot delete an SSL server policy by using the **undo ssl server-policy** command when the policy is associated with HTTPS.

You cannot change the associated SSL server policy for HTTPS by executing this command repeatedly. To change the SSL server policy for HTTPS:

1. Delete the local portal Web server by using the **portal local-web-server https ssl-server-policy** command.
2. Re-create the local portal Web server and specify a new SSL server policy by using the **portal local-web-server https ssl-server-policy** command.

Examples

# Configure a local portal Web server. Use HTTP to exchange authentication information with clients.

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] quit
```

# Configure a local portal Web server. Use HTTPS to exchange authentication information with clients, and specify SSL server policy **policy1** for HTTPS.

```
<Sysname> system-view
[Sysname] portal local-web-server https ssl-server-policy policy1
[Sysname-portal-local-websvr-https] quit
```

# Change the SSL server policy to **policy2**.

```
[Sysname] undo portal local-web-server https
[Sysname] portal local-web-server https ssl-server-policy policy2
[Sysname-portal-local-websvr-https] quit
```

Related commands

- **default-logon-page**
- **portal local-web-server**
- **ssl server-policy**

portal logout-record enable

Use **portal logout-record enable** to enable portal user offline recording.

Use **undo portal logout-record enable** to disable portal user offline recording.

Syntax

portal logout-record enable

undo portal logout-record enable

Default

Portal user offline recording is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature enables the device to save all portal user offline records and to periodically send the records to the lvzhou cloud server or other servers.

Examples

# Enable portal user offline recording.

```
<Sysname> system-view
[Sysname] portal logout-record enable
```

Related commands

display portal logout-record

portal logout-record export

Use **portal logout-record export** to export portal user offline records to a path.

Syntax

portal logout-record export url *url-string* [**start-time** *start-date start-time* **end-time** *end-date end-time*]

Views

System view

Predefined user roles

network-admin

Parameters

url *url-string*: Specifies the URL to which portal user offline records are exported. The URL is a case-insensitive string of 1 to 255 characters.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2100. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

Usage guidelines

The device supports FTP, TFTP, and HTTP file transfer methods. Table 24 describes the valid URL format for each method.

Table 24 URL formats

Protocol	URL format	Remarks
FTP	ftp://*username*[:*password*]@*server-address*[:*port-number*]/*file-path* Example: **ftp://a:1@1.1.1.1/authfail/**	The username and password must be the same as those on the server. If the server authenticates only the username, no password is required.
TFTP	tftp://*server-address*[:*port-number*]/*file-path* Example: **tftp://1.1.1.1/ autherror/**	N/A
HTTP	http://*username*[:*password*]@*server-address*[:*port-number*]/*file-path* Example: **http://1.1.1.1/autherror/**	The username and password must be the same as those on the server. If the server authenticates only the username, no password is required.

If the server address is an IPv6 address, bracket the IPv6 address to distinguish the IPv6 address from the port number. For example, if the server address is **2001::1** and the port number is 21, the URL is **ftp://test:test@[2001::1]:21/test/**.

Examples

# Export all portal user offline records to path **tftp://1.1.1.1/record/logout/**.

```
<Sysname> system-view
[Sysname] portal logout-record export url tftp://1.1.1.1/record/logout/
```

# Export portal user offline records in the time rang of 2016/3/4 14:20 to 2016/3/4 15:00 to path **tftp://1.1.1.1/record/logout/**.

```
<Sysname> system-view
[Sysname] portal logout-record export tftp://1.1.1.1/record/logout/ start-time 2016/3/4
14:20 end-time 2016/3/4 15:00
```

Related commands

display portal logout-record

portal logout-record enable

reset portal logout-record

portal logout-record max

Use **portal logout-record max** to set the maximum number of portal user offline records.

Use **undo portal logout-record max** to restore the default.

Syntax

portal logout-record max *number*

undo portal logout-record max

Default

The maximum number of portal user offline records is 32000.

Views

System view

Predefined user roles

network-admin

Parameters

number: Specifies the maximum number of portal user offline records, in the range of 1 to 4294967295.

Usage guidelines

When the maximum number of portal user offline records is reached, the new record overwrites the oldest one.

Examples

# Set the maximum number of portal user offline records to 50.

```
<Sysname> system-view
[Sysname] portal logout-record max 50
```

Related commands

display portal logout-record

portal mac-trigger-server

Use **portal mac-trigger-server** to create a MAC binding server and enter its view, or enter the view of an existing MAC binding server.

Use **undo portal mac-trigger-server** to delete the MAC binding server.

Syntax

portal mac-trigger-server *server-name*

undo portal mac-trigger-server *server-name*

Default

No MAC binding servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies a MAC binding server name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

After you create a MAC binding server, you can configure MAC binding server parameters, such as the server's IP address and the free-traffic threshold.

Examples

# Create MAC binding server **mts** and enter its view.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts]
```

Related commands

- **display portal mac-trigger-server**
- **portal apply mac-trigger-server**

portal max-user

Use **portal max-user** to set the maximum number of total portal users allowed in the system.

Use **undo portal max-user** to restore the default.

Syntax

portal max-user *max-number*

undo portal max-user

Default

The total number of portal users allowed in the system is not limited.

Views

System view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of total portal users in the system. The value range is 1 to 4294967295.

Usage guidelines

If you configure the maximum total number smaller than the number of current online portal users on the device, this command still takes effect. The online users are not affected by this command, but the system forbids new portal users to log in.

This command sets the maximum number of online IPv4 and IPv6 portal users in all.

Make sure the maximum combined number of IPv4 and IPv6 portal users specified on all interfaces or service templates does not exceed the system-allowed maximum number. Otherwise, the exceeding portal users will not be able to log in to the device.

Examples

# Set the maximum number of online portal users allowed in the system to 100.

```
<Sysname> system-view
[Sysname] portal max-user 100
```

Related commands

- **display portal user**
- **portal** { **ipv4-max-user | ipv6-max-user** }

portal nas-id profile

Use **portal nas-id-profile** to specify a NAS-ID profile for a VLAN interface.

Use **undo portal nas-id-profile** to restore the default.

Syntax

portal nas-id-profile *profile-name*

undo portal nas-id-profile

Default

No NAS-ID profile is specified for a VLAN interface.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies the name of a NAS-ID profile, a case-insensitive string of 1 to 31 characters.

Usage guidelines

A NAS-ID profile defines the binding relationship between VLANs and NAS-IDs. To configure a NAS-ID profile, use the **aaa nas-id profile** command. For more information, see "AAA commands."

If a VLAN interface is specified with a NAS-ID profile, the VLAN interface prefers to use the bindings defined in the profile.

If no NAS-ID profile is specified for a VLAN interface or no matching binding is found in the specified profile, the device uses the device name as the interface NAS-ID.

Examples

# Specify the NAS-ID profile **aaa** for VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal nas-id-profile aaa
```

Related commands

aaa nas-id profile

portal nas-port-id format

Use **portal nas-port-id format** to specify the NAS-Port-Id attribute format.

Use **undo portal nas-port-id format** to restore the default.

Syntax

portal nas-port-id format { **1** | **2** | **3** | **4** }

undo portal nas-port-id format

Default

The format for the NAS-Port-Id attribute is format 2.

Views

System view

Predefined user roles

network-admin

Parameters

1: Uses format 1 for the NAS-Port-Id attribute.

2: Uses format 2 for the NAS-Port-Id attribute.

3: Uses format 3 for the NAS-Port-Id attribute.

4: Uses format 4 for the NAS-Port-Id attribute.

Usage guidelines

The NAS-Port-Id format supported by RADIUS servers varies by vendor. Use this command to specify the format of the NAS-Port-Id attribute in the RADIUS packets sent for portal users to the RADIUS server. The device then automatically constructs a value for the NAS-Port-Id attribute in the specified format to meet the RADIUS server requirements.

Format 1 contains three space-separated strings: *interface-type port-location access-node-id*. Spaces are not allowed within a string.

- The *interface-type* string specifies the interface type of the NAS port. Available options include:
  - **atm**—ATM interface.
  - **eth**—Common Ethernet interface.
  - **trunk**—Ethernet trunk interface.
  - **0**—The interface type information will be reported by the access node to the BRAS.
- The *port-location* string represents the location of the access line on the BRAS. Its format is NAS_slot/NAS_subslot/NAS_port:XPI.XCI.

Field	Description
NAS_slot	Slot number of the BRAS, in the range of 0 to 31.
NAS_subslot	Subslot number of the BRAS, in the range of 0 to 31.
NAS_Port	Port number of the BRAS, in the range of 0 to 63.
XPI.XCI	For ATM interfaces: • XPI is VPI in the range of 0 to 255. • XCI is VCI in the range of 0 to 65535. For Ethernet interfaces or Ethernet trunk interfaces: • XPI is PVLAN in the range of 0 to 4095. This field is set to 4096 if there is no PVLAN. • XCI is CVLAN in the range of 0 to 4095. This field is set to 4096 if the user is not assigned to a VLAN as in the situation where the end user device is directly connected to a BRAS port.

  For the access node to report its access line information to the BRAS, all fields will be set to 0s except for the XPI and XCI fields.

- The *access-node-id* string specifies the attributes the of BRAS. Its format is AccessNodeIdentifier/ANI_rack/ANI_frame/ANI_slot/ANI_subslot/ANI_port:ANI_XPI.ANI_XCI, in which the :ANI_XPI.ANI_XCI portion is optional.

Field	Description
AccessNodeIdentifier	Identifier description of the access node, a string not longer than 50 characters without spaces.
ANI_rack	Rack number of the access node, in the range of 0 to 15.
ANI_frame	Frame number of the access node, in the range of 0 to 31.
ANI_slot	Slot number of the access node, in the range of 0 to 127.
ANI_subslot	Subslot number of the access node, in the range of 0 to 31.
ANI_port	Port number of the access node, in the range of 0 to 255.
ANI_XPI.ANI_XCI	Optional.

Field	Description
	This field is mainly used to carry CPE-side service information, identifying the further service type requirement. For example, use this field to identify specific services in a multi-PVC scenario. For ATM interfaces: • ANI_XPI is VPI in the range of 0 to 255 • ANI_XCI is VCI in the range of 0 to 65535. For Ethernet interfaces or Ethernet trunk interfaces: • ANI_XPI is PVLAN in the range of 0 to 4095. This field is set to 4096 if there is no PVLAN. • ANI_XCI is CVLAN in the range of 0 to 4095. This field is set to 4096 if the user is not assigned to a VLAN as in the situation where the end user device is directly connected to a BRAS port.

If the device does not have rack, frame, or subslot information, 0 is padded in the corresponding field.

For ATM interfaces, all fields in the access-node-id string are filled with 0s except for the ANI_XPI and ANI_XCI fields.

- Examples of format 1:

NAS-Port-Id	Description
atm 31/31/7:255.65535 0/0/0/0/0/0	The subscriber interface is an ATM interface. The slot number is 31, the BRAS subslot number is 31, the BRAS port number is 7, the VPI is 255, and the VCI is 65535.
eth 31/31/7:1234.2345 0/0/0/0/0/0	The subscriber interface is an Ethernet interface. The slot number is 31, the subslot number is 31, the port number is 7, the PVLAN is 1234, and the CVLAN is 2345. If there is no PVLAN, 1234 will be replaced with 4096.
eth 31/31/7:4096.2345 guangzhou001/1/31/63/31/127	The subscriber interface is an Ethernet interface. The slot number is 31, the subslot number is 31, the port number is 7, and the VLAN ID is 2345. The access node identifier of the DSLAM is guangzhou001, the rack number is 1, the frame number is 31, the slot number is 63, subslot number is 31, and the port number is 127.
0 0/0/0:4096.1234 guangzhou001/0/31/63/31/127	The 0 and 0/0/0 strings indicate that BRAS does not have access line information and will use the information received from the access node. After receiving access line information from the access node, the BRAS transparently delivers the information or complements the BRAS access link information as configured. For example, the BRAS complements the access line information as eth 31/31/7:4096.1234 guangzhou001/0/31/63/31/127.

Format 2 is SlotID/00/IfNO/VlanID.

- **SlotID**—The number of the slot the user accesses, a string of 2 characters.
- **IFNO**—The number of the interface the user accesses, a string of 3 characters.
- **VlanID**—The number of VLAN the user accesses, a string of 9 characters.

Format 3 is SlotID/00/IfNO/VlanID/DHCP option.

- **SlotID**—The number of the slot the user accesses, a string of 2 characters.
- **IFNO**—The number of the interface the user accesses, a string of 3 characters.
- **VlanID**—The number of VLAN the user accesses, a string of 9 characters.
- **DHCP option**—DHCP option 82 is appended for IPv4 users and DHCP option 18 is appended for IPv6 users.

Format 4 is slot=**;subslot=**;port=**;vlanid=**;vlanid2=**;.

- For non-VLAN interfaces, the slot=**;subslot=**;port=**;vlanid=0; format is used.
- For interfaces that terminate only the outermost VLAN tag, the slot=**;subslot=**;port=**;vlanid=**; format is used.

Examples

# Set the format of the NAS-Port-Id attribute to format 1.

```
<Sysname> system-view
[Sysname] portal nas-port-id format 1
```

portal nas-port-type

Use **portal nas-port-type** to specify the NAS-Port-Type value carried in RADIUS requests sent to the RADIUS server.

Use **undo portal nas-port-type** to restore the default.

Syntax

portal nas-port-type { **ethernet | wireless** }

undo portal nas-port-type

Default

The NAS-Port-Type value carried in RADIUS requests is the user's access interface type value obtained by the access device.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

ethernet: Specifies the NAS-Port-Type attribute value as Ethernet (number 15).

wireless: Specifies the NAS-Port-Type attribute value as WLAN-IEEE 802.11 (number 19).

Usage guidelines

As the access device, the BAS might not be able to correctly obtain a user's interface type when multiple network devices exist between the BAS and the portal client. For example, the access interface type obtained by the BAS for a wireless portal user might be the type of the wired interface that authenticated the user. For the BAS to send correct user interface type to the RADIUS server, use this command to specify the correct NAS-Port-Type value.

Examples

# Specify the NAS-Port-Type value in RADIUS requests sent to RADIUS server as WLAN-IEEE 802.11 on VLAN-interface 2.

```
<Sysname> system-view
```

```
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] portal nas-port-type wireless
```

# Specify the NAS-Port-Type value in RADIUS requests sent to RADIUS server as WLAN-IEEE 802.11 on service template **service1**.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] portal nas-port-type wireless
```

Related commands

display portal interface

portal oauth user-sync interval

Use **portal oauth user-sync interval** to set the user synchronization interval for portal authentication using OAuth.

Use **undo portal oauth user-sync interval** to restore the default.

Syntax

portal oauth user-sync interval *interval*

undo portal oauth user-sync interval

Default

The user synchronization interval is 60 seconds for portal authentication using OAuth.

Views

System view

Predefined user roles

network-admin

Parameters

interval: Specifies the user synchronization interval, in seconds. The value for this argument can be 0 or in the range of 60 to 3600.

Usage guidelines

If portal authentication uses OAuth, the device periodically reports user information to the portal authentication server for user synchronization on the server. To disable user synchronization from the device to the portal authentication server, set the user synchronization interval to 0 seconds on the device.

Examples

# Set the user synchronization interval to 120 seconds for portal authentication using OAuth.

```
<Sysname> system-view
[Sysname] portal oauth user-sync interval 120
```

portal outbound-filter enable

Use **portal** [**ipv6**] **outbound-filter enable** to enable outgoing packets filtering.

Use **undo portal** [**ipv6**] **outbound-filter enable** to disable outgoing packets filtering.

Syntax

portal [**ipv6**] **outbound-filter enable**

undo portal [**ipv6**] **outbound-filter enable**

Default

Outgoing packets filtering is disabled. A portal-enabled interface can send any packets.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

ipv6: Specifies outgoing IPv6 packets. If you do not specify this keyword, the command is for outgoing IPv4 packets.

Usage guidelines

When you enable this feature on a portal-enabled VLAN interface or service template, the device permits the interface or service template to send the following packets:

- Packets whose destination IP addresses are IP addresses of authenticated portal users.
- Packets that match portal-free rules.

Other outgoing packets on the VLAN interface or service template are dropped.

Examples

# Enable outgoing packets filtering on VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 20
[Sysname–Vlan-interface20] portal outbound-filter enable
```

# Enable outgoing packets filtering on service template **service1**.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] portal outbound-filter enable
```

Related commands

portal enable

portal packet log enable

Use **portal packet log enable** to enable logging for portal protocol packets.

Use undo **portal packet log enable** to disable logging for portal protocol packets.

Syntax

portal packet log enable

undo portal packet log enable

Default

Portal protocol packet logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature logs information about portal protocol packets, including the username, IP address, authentication type, packet type, SSID, and AP MAC. For portal log messages to be sent correctly, you must also configure the information center on the device. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

# Enable logging for portal protocol packets.

```
<Sysname> system-view
[Sysname] portal packet log enable
```

Related commands

portal redirect log enable

portal user log enable

portal pre-auth domain

Use **portal** [**ipv6**] **pre-auth domain** to specify a preauthentication domain for portal users on a VLAN interface.

Use **undo portal** [**ipv6**] **pre-auth domain** to restore the default.

Syntax

portal [**ipv6**] **pre-auth domain** *domain-name*

undo portal [**ipv6**] **pre-auth domain**

Default

No preauthentication domain is specified on a VLAN interface.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies IPv6 portal users. Do not specify this keyword for IPv4 portal users.

domain-name: Specifies an existing ISP domain by its name, a case-insensitive string of 1 to 255 characters. The string cannot contain the following characters: slashes (/), backslashes (\), vertical bars (|), quotation marks ("), colons (:), asterisks (*), question marks (?), left angle brackets (<), right angle brackets (>), and at signs (@).

Usage guidelines

Make sure you specify an existing ISP domain as a preauthentication domain. If the specified ISP domain does not exist, the device might operate incorrectly.

You must delete a preauthentication domain (by using the **undo portal** [**ipv6**] **pre-auth domain** command) and reconfigure it in the following situations:

- You create the ISP domain after specifying it as the preauthentication domain.
- You delete the specified ISP domain and then re-create it.

The preauthentication domain takes effect only on portal users with IP addresses assigned by DHCP or DHCPv6.

After you configure a preauthentication domain on a portal-enabled VLAN interface, the device authorizes users on the VLAN interface as follows:

1. After an unauthenticated user obtains an IP address, the user is assigned with authorization attributes configured for the preauthentication domain.

   The authorization attributes in a preauthentication domain include ACL, user profile, and CAR.

   An unauthenticated user who is authorized with the authorization attributes in a preauthentication domain is called a preauthentication user.
2. After the user passes portal authentication, the user is assigned with new authorization attributes from the AAA server.
3. After the user goes offline, the user is reassigned with the authorization attributes in the preauthentication domain.

If you change the preauthentication domain on a VLAN interface, the VLAN interface uses the new preauthentication domain for both new and existing preauthentication users.

If authorization attributes in the preauthentication domain are modified, the modified attributes take effect only on new preauthentication users. Existing preauthentication users use the original authorization attributes.

If the ACL in the preauthentication domain does not exist or the ACL has no rules, the device does not control user access. Users can access any network resources without passing portal authentication.

Follow these guidelines when you configure a preauthentication ACL rule:

- Do not specify a source address. If you specify a source address, users cannot trigger portal authentication.
- Do not set the destination address to **any**. All packets will be permitted to pass and therefore users can access any resources before portal authentication.

Examples

# Create the preauthentication domain **abc** for VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] portal pre-auth domain abc
```

Related commands

display portal

portal pre-auth ip-pool

Use **portal pre-auth ip-pool** to specify a preauthentication IP address pool for portal users on a VLAN interface.

Use **undo portal pre-auth ip-pool** to restore the default.

Syntax

portal [**ipv6**] **pre-auth ip-pool** *pool-name*

undo portal [**ipv6**] **pre-auth ip-pool**

Default

No preauthentication IP address pool is specified for portal users on a VLAN interface.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies IPv6 portal users. Do not specify this keyword for IPv4 portal users.

pool-name: Specifies an IP address pool by its name, a case-insensitive string of 1 to 63 characters.

Usage guidelines

You must use this command to specify a preauthentication IP address pool on a portal-enabled interface in the following situation:

- Portal users access the network through a subinterface of the portal-enabled interface.
- The subinterface does not have an IP address.
- Portal users need to obtain IP addresses through DHCP.

DHCP assigns an IP address from the specified IP address pool to a user. Then, the user can use this IP address to perform portal authentication.

Make sure the specified IP address pool exists and is correctly configured.

Examples

# Create the IPv4 address pool **abc** for VLAN-interface 100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal pre-auth ip-pool abc
```

Related commands

- **dhcp server ip-pool** (*Layer 3—IP Services Command Reference*)
- **display portal**
- **ipv6 dhcp pool** (*Layer 3—IP Services Command Reference*)

portal redirect log enable

Use **portal redirect log enable** to enable logging for portal redirect.

Use **undo portal redirect log enable** to disable logging for portal redirect.

Syntax

portal redirect log enable

undo portal redirect log enable

Default

Portal redirect logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature logs information about portal redirect packets, including the user IP address, MAC address, SSID, BAS IP, and Web server IP address. For portal log messages to be sent correctly, you must also configure the information center on the device. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

# Enable logging for portal redirect.

```
<Sysname> system-view
[Sysname] portal redirect log enable
```

Related commands

portal packet log enable

portal user log enable

portal refresh enable

Use **portal refresh** { **arp** | **nd** } **enable** to enable ARP or ND entry conversion for portal clients.

Use **undo portal refresh** { **arp** | **nd** } **enable** to disable ARP or ND entry conversion.

Syntax

portal refresh { **arp** | **nd** } **enable**

undo portal refresh { **arp** | **nd** } **enable**

Default

ARP or ND entry conversion is enabled for portal clients.

Views

System view

Predefined user roles

network-admin

Parameters

arp: Specifies the ARP entries.

nd: Specifies the ND entries.

Usage guidelines

When you enable this feature at a time:

- ARP or ND entries for portal users who pass authentication after the time are converted to Rule ARP or ND entries. Rule ARP or ND entries will not be aged.
- ARP or ND entries for portal users who pass authentication before the time will be aged when their respective aging timers expire.

When you disable this feature at a time:

- ARP or ND entries for portal users who pass authentication after the time will be aged when their respective aging timers expire.
- Rule ARP or ND entries created for portal users before the time are still Rule ARP or ND entries.

Examples

# Disable ARP entry conversion for portal clients.

```
<Sysname> system-view
[Sysname] undo portal refresh arp enable
```

portal roaming enable

Use **portal roaming enable** to enable portal roaming.

Use **undo portal roaming enable** to disable portal roaming.

Syntax

portal roaming enable

undo portal roaming enable

Default

Portal roaming is disabled. An online portal user cannot roam in its VLAN.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command applies only to portal users that log in from VLAN interfaces.

This command cannot be executed when online users or preauthentication portal users are present on the device.

If portal roaming is enabled, an online portal user can access network resources from any Layer 2 port in its local VLAN. If portal roaming is disabled, the portal user can access network resources only from the Layer 2 port on which it passes authentication.

Examples

# Enable portal roaming.

```
<Sysname> system-view
[Sysname] portal roaming enable
```

portal safe-redirect enable

Use **portal safe-redirect enable** to enable the portal safe-redirect feature.

Use **undo portal safe-redirect enable** to disable the portal safe-redirect feature.

Syntax

portal safe-redirect enable

undo portal safe-redirect enable

Default

The portal safe-redirect feature is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

Portal redirects all HTTP requests except HTTP requests that match portal-free rules to the portal Web server, which might overload the server.

Portal safe-redirect filters HTTP requests by HTTP request method, browser type (in HTTP User Agent), and destination URL, and redirects only the permitted HTTP requests.

As a best practice to avoid server overload and improve security, enable portal safe-redirect on the device.

Examples

# Enable the portal safe-redirect feature.

```
<Sysname> system-view
[Sysname] portal safe-redirect enable
```

Related commands

portal safe-redirect forbidden-url

portal safe-redirect method

portal safe-redirect user-agent

portal safe-redirect forbidden-file

Use **portal safe-redirect forbidden-file** to configure a filename extension forbidden by portal safe-redirect. If the URL of an HTTP request includes the specified filename extension, the device does not redirect the HTTP request.

Use **undo portal safe-redirect forbidden-file** to delete a portal safe-redirect forbidden filename extension.

Syntax

portal safe-redirect forbidden-file *filename-extension*

undo portal safe-redirect forbidden-file *filename-extension*

Default

No forbidden filename extensions are configured. The device redirects HTTP requests regardless of the filename extension in the URL.

Views

System view

Predefined user roles

network-admin

Parameters

filename-extension: Specifies a filename extension forbidden by portal safe-redirect, a case sensitive string of 1 to 16 characters.

Usage guidelines

You can configure multiple portal safe-redirect forbidden filename extensions.

Before you execute this command, make sure the portal safe-redirect feature is enabled.

Examples

# Specify **.jpg** as a portal safe-redirect forbidden filename extension.

```
<Sysname> system-view
[Sysname] portal safe-redirect forbidden-file .jpg
```

Related commands

portal safe-redirect enable

portal safe-redirect forbidden-url

Use **portal safe-redirect forbidden-url** to configure a URL forbidden by portal safe-redirect.

Use **undo portal safe-redirect forbidden-url** to delete a portal safe-redirect forbidden URL.

Syntax

portal safe-redirect forbidden-url *user-url-string*

undo portal safe-redirect forbidden-url *user-url-string*

Default

No forbidden URLs are configured. The device can redirect HTTP requests with any URLs.

Views

System view

Predefined user roles

network-admin

Parameters

user-url-string: Specifies a URL forbidden by portal safe-redirect, a case sensitive string of 1 to 256 characters.

Usage guidelines

You can execute this command multiple times to configure multiple portal safe-redirect forbidden URLs. The device does not redirect HTTP requests destined for the specified URLs to the portal Web server.

Before you execute this command, make sure the portal safe-redirect feature is enabled.

Examples

# Specify **http://www.abc.com** as a portal safe-redirect forbidden URL.

```
<Sysname> system-view
[Sysname] portal safe-redirect forbidden-url  http://www.abc.com
```

Related commands

portal safe-redirect enable

portal safe-redirect method

Use **portal safe-redirect method** to specify HTTP request methods permitted by portal safe-redirect.

Use **undo portal safe-redirect method** to delete HTTP request methods permitted by portal safe-redirect.

Syntax

portal safe-redirect method { **get** | **post** }*

undo portal safe-redirect method { **get** | **post** }*

Default

After portal safe-redirect is enabled, the device redirects only HTTP requests with the GET method.

Views

System view

Predefined user roles

network-admin

Parameters

get: Specifies the GET request method.

post: Specifies the POST request method.

Usage guidelines

After you specify HTTP request methods for portal safe-redirect, the device redirects only the HTTP requests with the specified methods to the portal Web server.

Before you execute this command, make sure the portal safe-redirect feature is enabled.

If you configure this command multiple times, the most recent configuration takes effect.

Examples

# Specify the GET request method for portal safe-redirect.

```
<Sysname> system-view
[Sysname] portal safe-redirect method get
```

Related commands

portal safe-redirect enable

portal safe-redirect user-agent

Use **portal safe-redirect user-agent** to specify a browser type for portal safe-redirect.

Use **undo portal safe-redirect user-agent** to delete a browser type for portal safe-redirect.

Syntax

portal safe-redirect user-agent *user-agent-string*

undo portal safe-redirect user-agent *user-agent-string*

Default

After portal safe-redirect is enabled, the device redirects the HTTP packets matching any browser types in Table 25.

Views

System view

Predefined user roles

network-admin

Parameters

user-agent-string: Specifies a browser type in HTTP User Agent, a case-sensitive string of 1 to 255 characters. You can specify the browser types as shown in Table 25.

Table 25 Browser type and description

Browser type	Description
Safari	Apple browser
Chrome	Google browser
Firefox	Firefox browser
UC	UC browser
QQBrowser	QQ browser
LBBROWSER	Cheetah browser
TaoBrowser	Taobao browser

Browser type	Description
Maxthon	Maxthon browser
BIDUBrowser	Baidu browser
MSIE 10.0	Microsoft IE 10.0 browser
MSIE 9.0	Microsoft IE 9.0 browser
MSIE 8.0	Microsoft IE 8.0 browser
MSIE 7.0	Microsoft IE 7.0 browser
MSIE 6.0	Microsoft IE 6.0 browser
MetaSr	Sogou browser

Usage guidelines

You can execute this command for multiple times to specify multiple browser types. The device redirects an HTTP request only when its User-Agent string contains a specified browser type.

Before you execute this command, make sure the portal safe-redirect feature is enabled.

Examples

# Specify browser types **Chrome** and **Safari** for portal safe-redirect.

```
<Sysname> system-view
[Sysname] portal safe-redirect user-agent Chrome
[Sysname] portal safe-redirect user-agent Safari
```

Related commands

portal safe-redirect enable

portal server

Use **portal server** to create a portal authentication server and enter its view, or enter the view of an existing portal authentication server.

Use **undo portal server** to delete the specified portal authentication server.

Syntax

portal server *server-name*

undo portal server *server-name*

Default

No portal authentication servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

In portal authentication server view, you can configure the following parameters and features for the portal authentication server:

- IP address of the server.
- Pre-shared key for communication between the access device and the server.
- Destination UDP port number used by the device to send unsolicited portal packets to the portal authentication server.
- Server detection feature.

You can configure multiple portal authentication servers for an access device.

Examples

# Create the portal authentication server **pts** and enter its view.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts]
```

Related commands

display portal server

portal temp-pass enable

Use **portal temp-pass enable** to enable portal temporary pass and set the temporary pass period.

Use **undo portal temp-pass enable** to disable portal temporary pass.

Syntax

portal temp-pass [**period** *period-value*] **enable**

undo portal temp-pass enable

Default

Portal temporary pass is disabled.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

period *period-value*: Specifies the temporary pass period. The value range for the *period-value* argument is 10 to 180 seconds, and the default is 30 seconds.

Usage guidelines

Typically, a portal user cannot access the network before passing portal authentication. This feature allows a user to access the Internet temporarily if the user uses a WeChat account to perform portal authentication. During the temporary pass period, the user provides WeChat authentication information to the WeChat server for the server to interact with the access device to finish portal authentication.

Examples

# On service template **service1**, enable portal temporary pass and set the temporary pass period to 25 seconds.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] portal temp-pass period 25 enable
```

Related commands

display portal

portal user-detect

Use **portal user-detect** to enable online detection of IPv4 portal users.

Use **undo portal user-detect** to disable online detection of IPv4 portal users.

Syntax

portal user-detect type { **arp** | **icmp** } [**retry** *retries*] [**interval** *interval*] [**idle** *time*]

undo portal user-detect

Default

Online detection of IPv4 portal users is disabled.

Views

VLAN interface view

Predefined user roles

network-admin

Parameters

type: Specifies the detection type.

- **arp**—ARP detection.
- **icmp**—ICMP detection.

retry *retries*: Sets the maximum number of detection attempts, in the range of 1 to 10. The default value is 3.

interval *interval*: Sets a detection interval in the range of 1 to 1200 seconds. The default interval is 3 seconds.

idle *time*: Sets a user idle timeout in the range of 60 to 3600 seconds. The default is 180 seconds. When the timeout expires, online detection of IPv4 portal users is started.

Usage guidelines

If the device receives no packets from a portal user within the configured idle time, the device detects the user's online status as follows:

- **ICMP detection**—Sends ICMP requests to the user at configurable intervals to detect the user status.
    - If the device receives a reply within the maximum number of detection attempts, it considers that the user is online and stops sending detection packets. Then the device resets the idle timer and repeats the detection process when the timer expires.
    - If the device receives no reply after the maximum number of detection attempts, the device logs out the user.
- **ARP detection**—Sends ARP requests to the user and detects the ARP entry status of the user at configurable intervals.
    - If the ARP entry of the user is refreshed within the maximum number of detection attempts, the device considers that the user is online and stops detecting the user's ARP entry. Then the device resets the idle timer and repeats the detection process when the timer expires.

- If the ARP entry of the user is not refreshed after the maximum number of detection attempts, the device logs out the user.

If firewall policies on the access device filter out ICMP packets, ICMP detection might fail and result in the logout of portal users. Make sure the access device does not block ICMP packets before you enable ICMP detection on an interface.

Examples

# Enable online detection of IPv4 portal users on VLAN-interface 100. Configure the detection type as **ARP**, the maximum number of detection attempts as **5**, the detection interval as **10** seconds, and the user idle timeout as **300** seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] portal user-detect type arp retry 5 interval 10 idle 300
```

Related commands

display portal

portal user-dhcp-only

Use **portal user-dhcp-only** to allow only portal clients with DHCP-assigned IP addresses to pass portal authentication.

Use **undo portal user-dhcp-only** to restore the default.

Syntax

portal [**ipv6**] **user-dhcp-only**

undo portal [**ipv6**] **user-dhcp-only**

Default

Both portal clients with DHCP-assigned IP addresses and portal clients with static IP addresses can pass portal authentication.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

ipv6: Specifies IPv6 portal clients. Do not specify this keyword for IPv4 portal clients.

Usage guidelines

After this command is configured, portal clients with static IP addresses cannot pass portal authentication.

To ensure that IPv6 portal clients can pass portal authentication when this feature is configured, disable the temporary IPv6 address feature on terminal devices. Otherwise, IPv6 portal clients will use temporary IPv6 addresses to access the IPv6 network and will fail portal authentication.

Examples

# Configure VLAN-interface 100 to allow only portal clients with DHCP-assigned IP addresses to pass portal authentication.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname–Vlan-interface100] portal user-dhcp-only
```

# Configure service template **service1** to allow only portal clients with DHCP-assigned IP addresses to pass portal authentication.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] portal user-dhcp-only
```

Related commands

display portal

portal user-logoff after-client-offline enable

Use **portal user-logoff after-client-offline enable** to automatically log out portal users after the wireless clients go offline.

Use **undo portal user-logoff after-client-offline enable** to restore the default.

Syntax

portal user-logoff after-client-offline enable

undo portal user-logoff after-client-offline enable

Default

Automatic logout is disabled for wireless portal users. Portal users will not be automatically logged out after the wireless clients are disconnected from the wireless network.

Views

System view

Predefined user roles

network-admin

Usage guidelines

After automatic logout is enabled for wireless portal users, the device will automatically log out a portal user after the user is disconnected from the wireless network.

Examples

# Enable automatic logging out of portal users after the wireless clients go offline.

```
<Sysname> system-view
[Sysname] portal user-logoff after-client-offline enable
```

portal user log enable

Use **portal user log enable** to enable logging for portal user logins and logouts.

Use **undo portal user log enable** to disable logging for portal user logins and logouts.

Syntax

portal user log enable

undo portal user log enable

Default

Portal user login and logout logging is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This feature logs information about portal user login and logout events, including the username, IP address, user's MAC address, name of the access interface, VLAN, SSID, AP's MAC address, and reason for login failure. For portal log messages to be sent correctly, you must also configure the information center on the device. For more information about information center configuration, see *Network Management and Monitoring Configuration Guide*.

Examples

# Enable logging for portal user logins and logouts.

```
<Sysname> system-view
[Sysname] portal user log enable
```

Related commands

portal packet log enable

portal redirect log enable

portal web-server

Use **portal web-server** to create a portal Web server and enter its view, or enter the view of an existing portal Web server.

Use **undo portal web-server** to delete the specified portal Web server.

Syntax

portal web-server *server-name*

undo portal web-server *server-name*

Default

No portal Web servers exist.

Views

System view

Predefined user roles

network-admin

Parameters

server-name: Specifies a portal Web server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

The portal Web server pushes portal authentication pages to portal users during authentication. The access device redirects HTTP requests of unauthenticated portal users to the portal Web server. In portal Web server view, you can configure the URL and URL parameters for the portal Web server and the portal Web server detection feature.

Examples

# Create portal Web server **wbs** and enter its view.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs]
```

Related commands

- **display portal web-server**
- **portal apply web-server**

redirect-url

Use **redirect-url** to specify the redirection URL for QQ authentication success.

Use **undo redirect-url** to restore the default.

Syntax

redirect-url *url-string*

undo redirect-url

Default

The redirection URL for QQ authentication success is **http://lvzhou.h3c.com/portal/qqlogin.html**.

Views

QQ authentication server view

Predefined user roles

network-admin

Parameters

url-string: Specifies the redirection URL for QQ authentication success, a case-sensitive string of 1 to 256 characters.

Usage guidelines

After a portal user passes QQ authentication, the user is redirected to the specified webpage to complete portal authentication.

You must enable DNS proxy and specify the IP address of an interface on the device as the DNS server.

Examples

# Specify **http://www.abc.com/portal/qqlogin.html** as the redirection URL for QQ authentication success.

```
<Sysname> system-view
[Sysname] portal extend-auth-server qq
[Sysname-portal-extend-auth-server-qq] redirect-url
http://www.abc.com/portal/qqlogin.html
```

Related commands

display portal extend-auth-server

reset portal auth-error-record

Use **reset portal auth-error-record** to clear portal authentication error records.

Syntax

reset portal auth-error-record { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **start-time** *start-date start-time* **end-time** *end-date end-time* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all portal authentication error records.

ipv4 *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2100. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

Examples

# Clear all portal authentication error records.

```
<Sysname> reset portal auth-error-record all
```

# Clear portal authentication error records for the portal user whose IPv4 address is 11.1.0.1.

```
<Sysname> reset portal auth-error-record ipv4 11.1.0.1
```

# Clear portal authentication error records for the portal user whose IPv6 address is 2000::2.

```
<Sysname> reset portal auth-error-record ipv6 2000::2
```

# Clear portal authentication error records with the error time in the range of 2016/3/4 14:20 to 2016/3/4 16:23.

```
<Sysname> reset portal auth-error-record start-time 2016/3/4 14:20 end-time 2016/3/4 16:23
```

Related commands

display portal auth-error-record

reset portal auth-fail-record

Use **reset portal auth-fail-record** to clear portal authentication failure records.

Syntax

reset portal auth-fail-record { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **start-time** *start-date start-time* **end-time** *end-date end-time* | **username** *username* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all portal authentication failure records.

ipv4 *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2100. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

username *username*: Specifies the username of a portal user, a case-sensitive string of 1 to 253 characters. The username cannot contain the domain name.

Examples

# Clear all portal authentication failure records.

```
<Sysname> reset portal auth-fail-record all
```

# Clear portal authentication failure records for the portal user whose IPv4 address is 11.1.0.1.

```
<Sysname> reset portal auth-fail-record ipv4 11.1.0.1
```

# Clear portal authentication failure records for the portal user whose IPv6 address is 2000::2.

```
<Sysname> reset portal auth-fail-record ipv6 2000::2
```

# Clear portal authentication failure records for the portal user whose username is **abc**.

```
<Sysname> reset portal auth-fail-record username abc
```

# Clear portal authentication failure records with the failure time in the range of 2016/3/4 14:20 to 2016/3/4 16:23.

```
<Sysname> reset portal auth-fail-record start-time 2016/3/4 14:20 end-time 2016/3/4 16:23
```

Related commands

display portal auth-fail-record

reset portal captive-bypass statistics

Use **reset portal captive-bypass statistics** to clear portal captive-bypass packet statistics.

Syntax

reset portal captive-bypass statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies a card by its slot number. If you do not specify a card, this command clears portal captive-bypass packet statistics for all cards.

Examples

# Clear portal captive-bypass packet statistics on slot 1.

```
<Sysname> reset portal captive-bypass statistics slot 0
```

Related commands

display portal captive-bypass statistics

reset portal local-binding mac-address

Use **reset portal local-binding mac-address** to clear local MAC-account binding entries.

Syntax

reset portal local-binding mac-address { *mac-address* | **all** }

Views

User view

Predefined user roles

network-admin

Parameters

mac-address: Specifies the MAC address of a portal user, in the format of H-H-H.

all: Specifies all local MAC-account binding entries.

Examples

# Clear all local MAC-account binding entries.

```
<Sysname> reset portal local-binding mac-address all
```

Related commands

- **display portal local-binding mac-address**
- **local-binding aging-time**

reset portal logout-record

Use **reset portal logout-record** to clear portal user offline records.

Syntax

reset portal logout-record { **all** | **ipv4** *ipv4-address* | **ipv6** *ipv6-address* | **start-time** *start-date start-time* **end-time** *end-date end-time* | **username** *username* }

Views

User view

Predefined user roles

network-admin

Parameters

all: Specifies all portal user offline records.

ipv4 *ipv4-address*: Specifies the IPv4 address of a portal user.

ipv6 *ipv6-address*: Specifies the IPv6 address of a portal user.

start-time *start-date start-time* **end-time** *end-date end-time*: Specifies a time range. The start date and end date must be in the format of MM/DD/YYYY or YYYY/MM/DD. The value range for MM is 1 to 12. The value range for DD varies with the specified month. The value range for YYYY is 1970 to 2100. The start time and end time must be in the format of hh:mm. The value range for the start time and end time is 00:00 to 23:59.

username *username*: Specifies the username of a portal user, a case-sensitive string of 1 to 253 characters. The username cannot contain the domain name.

Examples

# Clear all portal user offline records.

```
<Sysname> reset portal logout-record all
```

# Clear offline records for the portal user whose IPv4 address is 11.1.0.1.

```
<Sysname> reset portal logout-record ipv4 11.1.0.1
```

# Clear offline records for the portal user whose IPv6 address is 2000::2.

```
<Sysname> reset portal logout-record ipv6 2000::2
```

# Clear offline records for the portal user whose username is **abc**.

```
<Sysname> reset portal logout-record username abc
```

# Clear portal user offline records with the logout time in the range of 2016/3/4 14:20 to 2016/3/4 16:23.

```
<Sysname> reset portal logout-record start-time 2016/3/4 14:20 end-time 2016/3/4 16:23
```

Related commands

display portal logout-record

reset portal packet statistics

Use **reset portal packet statistics** to clear packet statistics for portal authentication servers.

Syntax

reset portal packet statistics [**extend-auth-server** { **cloud** | **mail** | **qq** | **wechat** } | **mac-trigger-server** *server-name* **|** **server** *server-name*]

Views

User view

Predefined user roles

network-admin

Parameters

extend-auth-server server-name: Specify a third-party authentication server.

cloud: Specify the lvzhou cloud authentication server.

mail: Specify the email authentication server.

qq: Specify the QQ authentication server.

wechat: Specify the WeChat authentication server.

mac-trigger-server: Specify a MAC binding server by its name, a case-sensitive string of 1 to 32 characters. If you do not specify a MAC binding server, this command clears packet statistics for the specified portal authentication server.

server *server-name*: Specifies a portal authentication server by its name, a case-sensitive string of 1 to 32 characters.

Usage guidelines

If you do not specify any parameters, this command clears packet statistics for all third-party authentication server, MAC binding server, and portal authentication servers.

Examples

# Clear packet statistics for the portal authentication server **pts**.

```
<Sysname> reset portal packet statistics server pts
```

# Clear packet statistics for MAC binding server **newps**.

```
<Sysname> reset portal packet statistics mac-trigger-server newpt
```

# Clear packet statistics for the lvzhou cloud authentication server.

```
<Sysname> reset portal packet statistics extend-auth-server cloud
```

Related commands

display portal packet statistics

reset portal redirect statistics

Use **reset portal redirect statistics** to reset portal redirect packet statistics.

Syntax

reset portal redirect statistics [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears portal redirect packet statistics for all member devices.

Examples

# Clear redirect packet statistics on the specified slot.

```
<Sysname> reset portal redirect statistics slot 0
```

Related commands

display portal safe-redirect statistics

reset portal safe-redirect statistics

Use **reset portal safe-redirect statistics** to clear portal safe-redirect packet statistics.

Syntax

reset portal safe-redirect statistics [**slot** *slot-number*]

Views

User view

Predefined user roles

network-admin

Parameters

slot *slot-number*: Specifies an IRF member device by its member ID. If you do not specify a member device, this command clears statistics for all member devices.

Examples

# Clear portal safe-redirect packet statistics on the specified slot.

```
<Sysname> reset portal safe-redirect statistics slot 0
```

Related commands

display portal safe-redirect statistics

server-detect (portal authentication server view)

Use **server-detect** to enable portal authentication server detection. After server detection is enabled for a portal authentication server, the device periodically detects portal packets from the server to identify its reachability status.

Use **undo server-detect** to disable portal authentication server detection.

Syntax

server-detect [**timeout** *timeout*] { **log** | **trap** } *

undo server-detect

Default

Portal authentication server detection is disabled.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

timeout *timeout*: Specifies the detection timeout in the range of 10 to 3600 seconds. The default is 60 seconds.

{ **log** | **trap** } *: Specifies the action to be taken after the device detects reachability status change of the portal authentication server. You can select one of the following options or both:

- **log**—When reachability status of the portal authentication server changes, the device sends a log message. The log message contains the name, the original state, and the current state of the portal authentication server.
- **trap**—When reachability status of the portal authentication server changes, the device sends a trap message to the NMS. The trap message contains the name and the current state of the portal authentication server.

Usage guidelines

The portal authentication server detection feature is effective only when the portal authentication server supports server heartbeat. Now only the IMC portal authentication server supports server heartbeat.

If the device receives portal packets from the portal authentication server before the detection timeout expires and verifies the correctness of the packets, the device considers the portal authentication server is reachable. Otherwise, the device considers the portal authentication server is unreachable.

The detection timeout configured on the device must be greater than the server heartbeat interval configured on the portal authentication server.

Examples

# Enable server detection for the portal authentication server **pts**:

- Set the detection timeout to **600** seconds.
- Configure the device to send a log message and a trap message if the server reachability status changes.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-detect timeout 600 log trap
```

Related commands

portal server

server-detect (portal Web server view)

Use **server-detect** to enable portal Web server detection.

Use **undo server-detect** to disable portal Web server detection.

Syntax

server-detect [**interval** *interval*] [**retry** *retries*] { **log** | **trap** } *

undo server-detect

Default

Portal Web server detection is disabled.

Views

Portal Web server view

Predefined user roles

network-admin

Parameters

interval *interval*: Specifies a detection interval in the range of 1 to 1200 seconds. The default is 5 seconds.

retry *retries*: Specifies the maximum number of consecutive detection failures, in the range of 1 to 10. The default is 3. If the number of consecutive failed detections reaches this threshold, the device considers the server as unreachable.

{ **log** | **trap** } *: Specifies the action to be taken after the device detects reachability status change of the portal Web server. You can select one of the following options or both:

- **log**—When reachability status of the portal Web server changes, the device sends a log message. The log message contains the name, the original state, and the current state of the portal Web server.
- **trap**—When reachability status of the portal Web server changes, the device sends a trap message to the NMS. The trap message contains the name and the current state of the portal Web server.

Usage guidelines

The access device performs server detection independently. No configuration on the portal Web server is required for the detection.

Examples

# Enable server detection for the portal Web server **wbs**:

- Set the detection interval to **600** seconds.
- Set the maximum number of consecutive detection failures to 2.
- Configure the device to send a log message and a trap massage after server reachability status changes.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] server-detect interval 600 retry 2 log trap
```

Related commands

portal web-server

server-register

Use **server-register** to set the interval at which the device registers with a portal authentication server.

Use **undo server-register** to restore the default.

Syntax

server-register [**interval** *interval-value*]

undo server-register

Default

The device does not register with a portal authentication server.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

interval *interval-value*: Specifies the register interval in the range of 1 to 3600 seconds. The default interval is 600 seconds.

Usage guidelines

This feature is typically used in scenarios where a NAT device exists between a portal authentication server and an access device.

After this feature is enabled, the access device automatically sends register packets to the portal authentication server. The register packet contains the access device name. After the server receives the register packet, it records register information for the access device, including the device name and the IP address and port number after NAT. The register information is used for subsequent authentication information exchanges between the server and the access device. The access device updates its register information on the server by sending register packets at regular intervals.

Only CMCC portal authentication servers support this feature.

Examples

# Configure the device to register with the portal authentication server at an interval of 120 seconds.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-register interval 120
```

Related commands

server-type

server-type (MAC binding server view)

Use **server-type** to specify the type of a MAC binding server.

Use **undo server-type** to restore the default.

Syntax

server-type { **cmcc** | **imc** }

undo server-type

Default

The type of the MAC binding server is IMC.

Views

MAC binding server view

Predefined user roles

network-admin

Parameters

cmcc: Specifies the MAC binding server type as CMCC.

imc: Specifies the MAC binding server type as IMC.

Examples

# Specify the type of the MAC binding server as **cmcc**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] server-type cmcc
```

server-type (portal server view/portal web-server view)

Use **server-type** to specify the type of a portal authentication server or portal Web server.

Use **undo server-type** to restore the default.

Syntax

server-type { **cmcc** | **imc** | **oauth** }

undo server-type

Default

The type of the portal authentication server and portal Web server is IMC.

Views

Portal authentication server view

Portal Web server view

Predefined user roles

network-admin

Parameters

cmcc: Specifies the portal server type as CMCC.

imc: Specifies the portal server type as IMC.

oauth: Specifies the portal server type as lvzhou cloud. This keyword is supported only in portal Web server view.

Usage guidelines

Specify the portal server type on the device with the server type the device actually uses.

Examples

# Specify the type of the portal authentication server as **cmcc**.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-type cmcc
```

# Specify the type of the portal Web server as **cmcc**.

```
<Sysname> system-view
[Sysname] web-server pts
[Sysname-portal-websvr-pts] server-type cmcc
```

Related commands

display portal server

tcp-port

Use **tcp-port** to configure a listening TCP port for the local portal Web server.

Use **undo tcp-port** to restore the default.

Syntax

tcp-port *port-number*

undo tcp-port

Default

The listening TCP port number for HTTP is 80 and that for HTTPS is 443.

Views

Local portal Web server view

Predefined user roles

network-admin

Parameters

port-number: Specifies the listening TCP port number in the range of 1 to 65535.

Usage guidelines

To use the local portal Web server, make sure the port number in the portal Web server URL and the port number configured in this command are the same.

For successful local portal authentication, follow these guidelines:

- Do not configure the listening TCP port number for a local portal Web server as the port number used by a known protocol. For example, do not specify port numbers 21 and 23, which are used by FTP and Telnet, respectively.
- Do not configure the HTTP listening port number as the default HTTPS listening port number 443.
- Do not configure the HTTPS listening port number as the default HTTP listening port number 80.
- Do not configure the same listening port number for HTTP and HTTPS.

Examples

# Set the HTTP service listening port number to 2331 for the local portal Web server.

```
<Sysname> system-view
[Sysname] portal local-web-server http
[Sysname-portal-local-websvr-http] tcp-port 2331
```

Related commands

portal local-web-server

url

Use **url** to configure a URL for a portal Web server.

Use **undo url** to restore the default.

Syntax

url *url-string*

undo url

Default

No URL is specified for the portal Web server.

Views

Portal Web server view

Predefined user roles

network-admin

Parameters

url-string: Specifies a URL for the portal Web server, a case-sensitive string of 1 to 256 characters.

Usage guidelines

This command specifies a URL that can be accessed through standard HTTP or HTTPS. The URL should start with http:// or https://. If the URL you specify does not start with http:// or https://, the system considers the URL begins with http:// by default.

Examples

# Configure the URL for the portal Web server **wbs** as **http://www.test.com/portal**.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url http://www.test.com/portal
```

Related commands

display portal web-server

url-parameter

Use **url-parameter** to configure the parameters carried in the URL of a portal Web server. The access device redirects a portal user by sending the URL with the parameters to the user.

Use **undo url-parameter** to delete the parameters carried in the URL of the portal Web server.

Syntax

url-parameter *param-name* { **nas-id** | **nas-port-id** | **original-url** | **source-address** | **ssid** | { **ap-mac** | **source-mac** } [**encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string*] | **value** *expression* | **vlan** }

undo url-parameter *param-name*

Default

No URL parameters are configured for a portal Web server.

Views

Portal Web server view

Predefined user roles

network-admin

Parameters

param-name: Specifies a URL parameter name, a case-sensitive string of 1 to 32 characters. Content of the parameter is determined by the following keyword you specify.

nas-id: Specifies the NAS-ID.

nas-port-id: Specifies the NAS-Port-Id.

original-url: Specifies the URL of the original webpage that a portal user visits.

source-address: Specifies the user IP address.

ssid: Specifies the SSID of the AP.

ap-mac: Specifies the MAC address of the AP.

source-mac: Specifies the user MAC address.

aes: Specifies AES to encrypt the specified URL parameter.

des: Specifies DES to encrypt the specified URL parameter.

cipher: Sets a ciphertext shared key.

simple: Sets a plaintext shared key.

string: Specifies the case-sensitive key string. The string length varies by the selected encryption method:

- For a DES-encrypted ciphertext key, the string length is 41 characters.
- For a DES-encrypted plaintext key, the string length is 8 characters.
- For an AES-encrypted ciphertext key, the string length is 1 to 73 characters.
- For an AES-encrypted plaintext key, the string length is 1 to 31 characters.

value *expression*: Specifies a custom case-sensitive string of 1 to 256 characters.

vlan: Specifies the user VLAN ID.

Usage guidelines

You can configure multiple URL parameters.

If you configure a URL parameter multiple times, the most recent configuration takes effect.

After you configure the URL parameters, the access device sends the portal Web server URL with these parameters to portal users. For example, assume that the URL of a portal Web server is http://www.test.com/portal, and you execute the **url-parameter userip source-address** and **url-parameter userurl value http://www.abc.com/welcome** commands. Then, the access device sends to the user whose IP address is 1.1.1.1 the URL http://www.test.com/portal?userip=1.1.1.1&userurl=http://www.abc.com/welcome.

When you configure the *param-name* argument in this command, you must use the URL parameter name supported by the actual portal server. Different portal server types support different URL parameter names.

For example, the IMC server supports parameter names **userurl**, **userip**, and **usermac** for the keywords **original-url**, **source-address**, and **source-mac**, respectively. To carry the user IP information in the portal Web server URL, you must configure the parameter name as **userip** and specify the **source-address** keyword.

If you specify the encryption algorithm for a parameter, the redirection URL carries the encrypted value for the parameter. Execute the **url-parameter usermac source-mac encryption des key simple 12345678** command. Then the access device sends to the user with MAC address 1111-1111-1111 the URL http://www.test.com/portal?usermac=xxxxxxxxx&userip=1.1.1.1&userurl= http://www.test.com/welcome, where xxxxxxxxx represents the encrypted user MAC address.

Examples

# Configure URL parameters **userip** and **userurl** for portal Web server **wbs**. Configure the value of the **userip** parameter as **source-address** (the IP addresses of users) and that of the **userurl** parameter as **http://www.abc.com/welcome**.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url-parameter userip source-address
[Sysname-portal-websvr-wbs] url-parameter userurl value http://www.abc.com/welcome
```

# Configure URL parameter **usermac** for portal Web server **wbs**. Configure the value of the **usermac** parameter as **source-mac** (the MAC addresses of users) and specify DES to encrypt the MAC addresses.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url-parameter usermac source-mac encryption des key simple
12345678
```

# Configure URL parameter **uservlan** for portal Web server **wbs**. Configure the value of the **uservlan** parameter as the **vlan** (the VLAN IDs of users.)

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] url-parameter uservlan vlan
```

Related commands

- **display portal web-server**
- **url**

user-sync

Use **user-sync** to enable portal user synchronization for a portal authentication server. After this feature is enabled, the device replies to and periodically detects the synchronization packets from the portal authentication server. In this way, information about online portal users on the device and on the portal authentication server remains consistent.

Use **undo user-sync** to disable portal user synchronization for a portal authentication server.

Syntax

user-sync timeout *timeout*

undo user-sync

Default

Portal user synchronization is disabled for a portal authentication server.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

timeout *timeout*: Sets a detection timeout for synchronization packets, in the range of 60 to 18000 seconds. The default is 1200 seconds.

Usage guidelines

Portal user synchronization requires that the portal authentication server support the portal user heartbeat feature. Now, only the IMC portal authentication server supports portal user heartbeat. To implement portal user synchronization, you need to configure the user heartbeat feature on the portal authentication server. Make sure the user heartbeat interval configured on the portal authentication server is not greater than the synchronization detection timeout configured on the access device.

Deleting a portal authentication server on the device also deletes the user synchronization configuration for the server.

If you configure portal user synchronization multiple times for a portal authentication server, the most recent configuration takes effect.

For information of the users considered as nonexistent on the portal authentication server, the device deletes the information after the configured detection timeout expires.

If the user information from the portal authentication server does not exist on the device, the device encapsulates IP addresses of the users in user heartbeat reply packets to the server. The portal authentication server then deletes the users.

Examples

# Enable portal user synchronization for the portal authentication server **pts** and set the detection timeout to **600** seconds. If a use has not appeared in the synchronization packets sent by the portal authentication server for 600 seconds, the access device logs out the user.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] user-sync timeout 600
```

Related commands

portal server

version

Use **version** to specify the version of the portal protocol.

Use **undo version** to restore the default.

Syntax

version *version-number*

undo version

Default

The version of the portal protocol is 1.

Views

MAC binding server view

Predefined user roles

network-admin

Parameters

version-number: Specifies the portal protocol version in the range of 1 to 3.

Usage guidelines

The specified portal protocol version must be the that required by the MAC binding server.

Examples

# Configure the device to use portal protocol version 2 to communicate with the MAC binding server **mts**.

```
<Sysname> system-view
[Sysname] portal mac-trigger-server mts
[Sysname-portal-mac-trigger-server-mts] version 2
```

Related commands

- **display portal mac-trigger-server**
- **portal mac-trigger-server**

web-redirect url

Use **web-redirect url** to enable the Web redirect feature.

Use **undo web-redirect url** to disable the Web redirect feature.

Syntax

web-redirect [**ipv6**] **url** *url-string* [**interval** *interval*]

undo web-redirect [**ipv6**]

Default

Web redirect is disabled.

Views

VLAN interface view

Service template view

Predefined user roles

network-admin

Parameters

ipv6: Specifies the IPv6 Web redirect feature. Do not specify this keyword for the IPv4 Web redirect feature.

url *url-string*: Specifies the URL to which the user is redirected. The URL is required to be complete and begins with **http://** or **https://**, a string of 1 to 256 characters.

interval *interval*: Specifies the time interval at which the user is redirected to the specified URL. It is in the range of 60 to 86400 seconds.

Usage guidelines

This feature redirects a user on a VLAN interface or a service template to the specified URL before the user can access an external network through a Web browser. After the specified interval, the user is redirected to the specified URL again.

On a service template, both Web redirect and portal authentication can be enabled and will take effect at the same time.

The Web redirect feature takes effect only on HTTP packets that use the default port number 80.

Examples

# Configure IPv4 Web redirect on VLAN-interface 100. Set the redirect URL to **http://192.0.0.1** and the interval to 3600 seconds.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname–Vlan-interface100] web-redirect url http://192.0.0.1 interval 3600
```

# Configure IPv4 Web redirect on service template **service1**. Set the redirect URL to **http://192.0.0.1** and the interval to 3600 seconds.

```
<Sysname> system-view
[Sysname] wlan service-template service1
[Sysname-wlan-st-service1] web-redirect url http://192.0.0.1 interval 3600
```

Related commands

display web-redirect rule