Contents

Portal commands

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 enable

undo captive-bypass 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

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.

Examples

# Enable the captive-bypass feature.

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

Related commands

display portal web-server

default-logon-page

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

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

Syntax

default-logon-page *file-name*

undo default-logon-page

Default

The default authentication page file is **defaultfile.zip**.

Views

Local portal Web service view

Predefined user roles

network-admin

Parameters

file-name: 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

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.

As a best practice to ensure correct operation of the local portal service, use the predefined default authentication page file stored under the root directory of the device storage medium. If you want to customize authentication pages, follow the authentication page customization rules.

Examples

# Specify 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 interface *interface-type interface-number*

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

Examples

# Display portal configuration and portal running state on VLAN-interface 2.

```
<Sysname> display portal interface vlan-interface 2
 Portal information of Vlan-interface2
     NAS-ID profile: aaa
     Authorization : Strict checking
     ACL           : Enabled
     User profile  : Disabled
 IPv4:
     Portal status: Enabled
     Portal authentication method: Direct
     Portal web server: wbs
     Portal mac-trigger-server: Not configured
     Authentication domain: my-domain
     User-dhcp-only: Enabled
     Pre-auth IP pool: ab
     Max Portal users: Not configured
     Bas-ip: Not configured
     User detection : Type: ICMP  Interval: 300s  Attempts: 5   Idle time: 180s
     Action for server detection:
         Server type    Server name                        Action
         Web server     wbs                                fail-permit
         Portal server  pts                                fail-permit
     Layer3 source network:
         IP address               Mask
         1.1.1.1                  255.255.0.0

     Destination authentication subnet:
         IP address               Mask
         2.2.2.2                  255.255.255.0

 IPv6:
     portal status: Disabled
     Portal authentication method: Disabled
     Portal web server: Not configured
     Portal mac-trigger-server: Not configured
     Authentication 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
     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.
NAS-ID profile	NAS-ID profile on the interface.
Authorization	Authorization information type: ACL or 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 authentication method	Authentication mode enabled on the interface: • **Direct**—Direct authentication. • **Redhcp**—Re-DHCP authentication. • **Layer3**—Cross-subnet authentication.
Portal Web server	Name of the portal Web server specified on the interface.
Portal mac-trigger-server	This field is not supported in the current software version. Name of the MAC binding server specified on the interface.
Authentication domain	Mandatory authentication domain on the interface.
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.
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.
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.

Related commands

portal domain

portal enable

portal free-all except destination

portal ipv6 free-all except destination

portal ipv6 layer3 source

portal layer3 source

portal web-server

display portal packet statistics

Use **display portal packet statistics** to display packet statistics for portal authentication servers.

Syntax

display portal packet statistics [**server** *server-name*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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

Usage guidelines

This command displays statistics on packets the device sent to and received from portal authentication servers.

If you do not specify the **server** *server-name* option, this command displays packet statistics for all portal authentication 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
```

Table 2 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 packets that carry error information.
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 the portal authentication server sent to the access device.

Related commands

reset portal packet statistics

display portal rule

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

Syntax

display portal rule { **all** | **dynamic** | **static** } **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.

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 slot 1
Slot 1:
```

```
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
```

Table 3 Command output

Field	Description
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.
Protocol	Transport layer protocol permitted by the portal-free rule: • **Any**—Permits any transport layer protocol. • **TCP**—Permits TCP. • **UDP**—Permits UDP.
Status	Status of the portal filtering rule: • **Active**—The portal filtering rule is effective. • **Unactuated**—The portal filtering 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.

Field	Description
Interface	Layer 2 or Layer 3 interface on which the portal filtering rule is implemented.
VLAN	Source VLAN ID.
Protocol	Transport layer protocol permitted by the portal redirect rule. This field always displays **TCP**.
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.
Number	Number of the authorized ACL. This field displays **N/A** if the AAA server does not assign an ACL.

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 the portal authentication server **pts**.

```
<Sysname> display portal server pts
Portal server: pts
  Type                    : IMC
  IP                      : 192.168.0.111
  VPN instance            : Not configured
  Port                    : 50100
  Server detection        : Timeout 60s  Action: log
  User synchronization    : Timeout 200s
  Status                  : Up
```

Table 4 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	MPLS L3VPN instance where the portal authentication server resides.
Port	Listening port on the portal authentication server.
Server detection	Parameters for portal authentication server detection: - Detection timeout in seconds. - Action (**log**) 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: - **Up**—This value indicates one of the following conditions: ○ Portal authentication server detection is disabled. ○ Portal authentication server detection is enabled and the server is reachable. - **Down**—Portal authentication server detection is enabled and the server is unreachable.

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`** | **`interface`** *`interface-type interface-number`* | **`ip`** *`ipv4-address`* | **`ipv6`** *`ipv6-address`* } [**`verbose`**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

all: Displays information about all portal users.

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.

verbose: Displays detailed information about portal users.

Examples

# Display information about all portal users.

```
<Sysname> display portal user all
Total portal users: 2
Username: abc
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC               IP                 VLAN   Interface
  000d-88f8-0eab     2.2.2.2            100    Vlan-interface100
  Authorization information:
    DHCP IP pool: N/A
    User profile: abc (active)
    Session group profile: N/A
    ACL number: N/A
    Inbound CAR: N/A
    Outbound CAR: N/A

Username: def
  Portal server: pts
  State: Online
  VPN instance: N/A
  MAC               IP                 VLAN   Interface
  000d-88f8-0eac     3.3.3.3            200    Vlan-interface200
  Authorization information:
    DHCP IP pool: N/A
    User profile: N/A
    Session group profile: N/A
    ACL number: 3001
    Inbound CAR: N/A
    Outbound CAR: N/A
```

Table 5 Command output

Field	Description
Total portal users	Total number of portal users.
Username	Name of the user.
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. - **Waiting SetRule**—The user is waiting for authorization information. - **Authorizing**—The user is being authorized. - **Online**—The user is online. - **Waiting Traffic**—The last traffic of the user is to be collected. - **Stop Accounting**—Accounting for the user is stopped. - **Done**—The user goes offline successfully.
VPN instance	MPLS L3VPN instance to which the portal user belongs. If the portal user is on a public network, this field displays **N/A**.
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**—No user profile is authorized. - **active**—The authorized user profile is applied to the user access interface successfully. - **inactive**—The authorized user profile is not applied to the user access interface or the user profile does not exist on the device.
Session group profile	This field is not supported in the current software version. Authorized session group profile: - **N/A**—No session group profile is authorized. - **active**—The authorized session group profile is applied to the user access interface successfully. - **inactive**—The authorized session group profile is not applied to the user access interface or the session group profile does not exist on the device.
ACL number	Authorized ACL: - **N/A**—No ACL is authorized. - **active**—The authorized ACL is applied to the user access interface successfully. - **inactive**—The authorized ACL is not applied to the user access interface or the ACL does not exist on the device.
Inbound CAR	This field is not supported in the current software version. Authorized inbound CAR: - **CIR**—Committed information rate in bps. - **PIR**—Peak information rate in bps. - **active**—The authorized inbound CAR is applied to the user access interface successfully. - **inactive**—The authorized inbound CAR is not applied to the user access interface. - **N/A**—No inbound CAR is authorized.

Outbound CAR	This field is not supported in the current software version. Authorized outbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **active**—The authorized outbound CAR is applied to the user access interface successfully. • **inactive**—The authorized outbound CAR is not applied to the user access interface. • **N/A**—No outbound CAR is authorized.

# Display detailed information about the portal user with IP address 50.50.50.3.

```
<Sysname> display portal user ip 50.50.50.3 verbose
Basic:
  Current IP address: 50.50.50.3
  Original IP address: 30.30.30.2
  Username: user1@hrss
  User ID: 0x28000002
  Access interface: Vlan-interface20
  Service-VLAN/Customer-VLAN: -/-
  MAC address: 0000-0000-0001
  Domain: hrss
  VPN instance: N/A
  Status: Online
  Portal server: test
  Portal authentication method: Direct
AAA:
  Realtime accounting interval: 60s, retry times: 3
  Idle cut: 180 sec, 10240 bytes, direction: Inbound
  Session duration: 500 sec, remaining: 300 sec
  Remaining traffic: 10240000 bytes
  Login time: 2014-01-19  2:42:3 UTC
  ITA policy name: N/A
  DHCP IP pool: abc
ACL&QoS&Multicast:
  Inbound CAR: N/A
  Outbound CAR: N/A
  ACL number: 3000 (inactive)
  User profile: portal (active)
  Session group profile: N/A
  Max multicast addresses: 4
  Multicast address list: 1.2.3.1, 1.34.33.1, 3.123.123.3, 4.5.6.7
                          2.2.2.2, 3.3.3.3, 4.4.4.4
  User group: 1 (Id=1)
Flow statistic:
  Uplink   packets/bytes: 7/546
  Downlink packets/bytes: 0/0
ITA:
  Accounting merge: Disabled
  Traffic separate: Disabled
  Quota-out offline: Disabled
level-2 Session duration: N/A, remaining: N/A
        Remaining traffic: N/A
        Traffic action: Permit
        Inbound CAR: N/A
        Outbound CAR: N/A
        Uplink packets/bytes: 0/0
        Downlink packets/bytes: 0/0
```

Table 6 Command output

Field	Description
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.
Domain	ISP domain name for portal authentication.
VPN instance	MPLS L3VPN instance to which the portal user belongs. If the portal user is on a public network, this field displays **N/A**.
Status	Status of the portal user: • **Authenticating**—The user is being authenticated. • **Authorizing**—The user is being authorized. • **Waiting SetRule**—Deploying portal 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.
Portal authentication method	Portal authentication method on the access interface: • **Direct**—Direct authentication. • **Re-Dhcp**—Re-DHCP authentication. • **Layer3**—Cross-subnet authentication.
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**.
direction	Direction of user traffic: • **Both**—Inbound and outbound traffic. • **Inbound**—Inbound traffic.

	• **Outbound**—Outbound traffic.
Session duration	Session duration and the remaining session time. If the session duration is not authorized, this field displays **N/A**.
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	This field is not supported in the current software version. 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**.
Inbound CAR	This field is not supported in the current software version. Authorized inbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **active**—The authorized inbound CAR is applied to the user access interface successfully. • **inactive**—The authorized inbound CAR is not applied to the user access interface. • **N/A**—No inbound CAR is authorized.
Outbound CAR	This field is not supported in the current software version. Authorized outbound CAR: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **active**—The authorized outbound CAR is applied to the user access interface successfully. • **inactive**—The authorized outbound CAR is not applied to the user access interface. • **N/A**—No outbound CAR is authorized.
ACL number	Authorized ACL: • **N/A**—No ACL is authorized. • **active**—The authorized ACL is applied to the user access interface successfully. • **inactive**—The authorized ACL is not applied to the user access interface or the ACL does not exist on the device.
User profile	Authorized user profile: • **N/A**—No user profile is authorized. • **active**—The authorized user profile is applied to the user access interface successfully. • **inactive**—The authorized user profile is not applied to the user access interface or the user profile does not exist on the device.
Session group profile	This field is not supported in the current software version. Authorized session group profile: • **N/A**—No session group profile is authorized. • **active**—The authorized session group profile is applied to the user access interface successfully. • **inactive**—The authorized session group profile is not applied to the user access interface 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**.
User group	Name of the group where the portal user belongs. This field is invalid if the ID is 0xffffffff.
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.
ITA	This field is not supported in the current software version. ITA traffic statistics for the portal user.
Accounting merge	This field is not supported in the current software version. Status of the accounting merge feature: • **Enabled**—The accounting merge feature is enabled. The device merges the ITA traffic of all accounting rates in the ITA policy, and applies the lowest rate to the merged traffic. • **Disabled**—The accounting merge feature is disabled. The device sends separate traffic statistics for each accounting rate to the server.
Traffic separate	This field is not supported in the current software version. Whether to exclude the amount of ITA traffic from the overall traffic statistics sent to the accounting server: • **Enabled**—ITA traffic is excluded from the overall traffic statistics. • **Disabled**—ITA traffic is included in the overall traffic statistics.
Quota-out offline	This field is not supported in the current software version. Whether to prohibit the portal user from accessing the authorized IP subnets when the user has used up its ITA data quota: • **Enabled**—User cannot access the authorized IP subnets after its ITA data quota is used up. • **Disabled**—User can access the authorized IP subnets after its ITA data quota is used up.
level-2 Session duration	This field is not supported in the current software version. Authorized level *n* session duration and the remaining session duration. Level *n* represents the accounting level of the portal user in ITA. If the session duration is not authorized, this field displays **N/A**.
Remaining traffic	This field is not supported in the current software version. Remaining ITA traffic for the portal user.
Traffic action	This field is not supported in the current software version. Action for traffic destined for the authorized IP subnets when the portal user has used up its ITA data quota: • **Permit**—Permits traffic destined for the authorized IP subnets. • **Deny**—Denies traffic destined for the authorized IP subnets.
Inbound CAR	This field is not supported in the current software version. Authorized inbound CAR for ITA traffic: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **active**—The authorized inbound CAR is applied to the user access interface successfully. • **inactive**—The authorized inbound CAR is not applied to the user access interface. • **N/A**—No inbound CAR is authorized.

Outbound CAR	This field is not supported in the current software version. Authorized outbound CAR for ITA traffic: • **CIR**—Committed information rate in bps. • **PIR**—Peak information rate in bps. • **active**—The authorized outbound CAR is applied to the user access interface successfully. • **inactive**—The authorized outbound CAR is not applied to the user access interface. • **N/A**—No outbound CAR is authorized.
Uplink packets/bytes	This field is not supported in the current software version. Packet and byte statistics of the portal user's upstream ITA traffic.
Downlink packets/bytes	This field is not supported in the current software version. Packet and byte statistics of the portal user's downstream ITA traffic.

Related commands

portal enable

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
    IPv4 status      : Up
    IPv6 status      : Up
```

```
  Captive-bypass   : Disabled
  If-match         : original-url http://2.2.2.2 redirect-url http://192.168.56.2
```

Table 7 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 MPLS L3VPN where the portal Web server resides.
Server detection	Parameters for portal Web server detection: • Detection interval in seconds. • Maximum number of detection attempts. • Action (**log**) triggered by the reachability status change of the portal Web server.
IPv4 status	Current state of the IPv4 portal Web server: • **Up**—This value indicates one of the following conditions: ○ Portal Web server detection is disabled. ○ Portal Web server detection is enabled and the server is reachable. • **Down**—Portal Web server detection is enabled and the server is unreachable.
IPv6 status	Current state of the IPv6 portal Web server: • **Up**—This value indicates one of the following conditions: ○ Portal Web server detection is disabled. ○ Portal Web server detection is enabled and the server is reachable. • **Down**—Portal Web server detection is enabled and the server is unreachable.
Captive-bypass	Status of the captive-bypass feature: **Enabled** or **Disabled**.
If-match	Match rules configured for URL redirection. If no match rules are configured, this field displays **Not configured**.

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 interface *interface-type interface-number* [**slot** *slot-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

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
```

Table 8 Command output

Field	Description
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. - **Inactive**—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.
VLAN	Source VLAN. If not specified, this field displays **Any**.
Protocol	Transport layer protocol permitted by the Web redirect rule. This field always displays **TCP**.
Destination	Destination information in the Web redirect rule.
Port	Destination transport layer port number. The default port number is 80.

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 exist.

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

Usage guidelines

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

For a user to successfully access a redirection URL, configure a portal-free rule to allow HTTP or HTTPS 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.

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** and use **DES** to encrypt the parameters carried in this redirection URL.

```
<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 url-param-encryption des key simple 12345678
```

# 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 (portal authentication server view)

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

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

Syntax

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

undo ip

Default

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

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

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

vpn-instance *ipv4-vpn-instance-name*: Specifies the MPLS L3VPN instance to which the portal authentication server belongs. The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the portal authentication server belongs to the public network, do not specify this option.

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: 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 key. 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

A portal authentication server has only one IPv4 address. Therefore, in portal authentication server view, only one IPv4 address exists. If you execute this command multiple times, the most recent configuration takes effect.

Do not configure the same IPv4 address and MPLS L3VPN for different portal authentication servers.

Examples

# Specify **192.168.0.111** as the IPv4 address of portal authentication server **pts** and pliantext key **portal** as the shared key for communication with the portal authentication server.

```
<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 IPv6 address of a portal authentication server.

Use **`undo ipv6`** to restore the default.

Syntax

`ipv6` *`ipv6-address`* [**`vpn-instance`** *`vpn-instance-name`*] [**`key`** { **`cipher`** | **`simple`** } *`string`*]

`undo ipv6`

Default

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

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

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

`vpn-instance` *`ipv6-vpn-instance-name`*: Specifies the MPLS L3VPN instance to which the portal authentication server belongs. The *`ipv6-vpn-instance-name`* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters. If the portal authentication server belongs to the public network, do not specify this option.

`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`: Specifies a key in encrypted form.

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

`string`: Specifies the key. 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

A portal authentication server has only one IPv6 address. Therefore in portal authentication server view, only one IPv6 address exists. If you execute this command multiple times, the most recent configuration takes effect.

Do not configure the same IPv6 address and MPLS L3VPN for different portal authentication servers.

Examples

# Specify **2000::1** as the IPv6 address of portal authentication server **pts** and pliantext key **portal** as the shared key for communication with the portal authentication server.

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

Related commands

display portal server

portal 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 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 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 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 } (interface view)

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

Use **undo portal** { **bas-ip** | **bas-ipv6** } to restore the default.

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 packet's output interface. The BAS-IPv6 attribute of an IPv6 portal notification packet sent to the portal authentication server is the IPv6 address of the packet's output interface.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv4-address: Specifies BAS-IP for portal packets sent to the portal authentication server. This attribute must be the IPv4 address of an interface on the device. It cannot be 0.0.0.0, 1.1.1.1, a class D address, a class E address, or a loopback address.

ipv6-address: Specifies BAS-IPv6 for portal packets sent to the portal authentication server. This attribute must be the IPv6 address of an interface on the device. It cannot be a multicast address, an all-0 address, or a 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 address. Otherwise, the source IP address of the packets is the IP address of the packet output interface.

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

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

Examples

# On interface VLAN-interface 100, configure the BAS-IP attribute as **2.2.2.2** for portal packets sent to the portal authentication server.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
```

```
[Sysname–Vlan-interface100] portal bas-ip 2.2.2.2
```

Related commands

display portal

portal { ipv4-max-user | ipv6-max-user } (interface view)

Use **portal** { **ipv4-max-user** | **ipv6-max-user** } to set the maximum number of portal users allowed on an interface.

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 allowed on an interface is not limited.

Views

Interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of IPv4 or IPv6 portal users allowed on an interface, 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 the interface, the limit can be set successfully. The limit does not impact the online portal users. However, the device does not allow new portal users to log in from the interface until the number drops down below the limit.

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
```

Related commands

display portal user

portal max-user

portal apply web-server (interface view)

Use **portal** [**ipv6**] **apply web-server** to specify a portal Web server. The device redirects the HTTP requests sent by unauthenticated portal users to the portal Web server.

Use **undo portal** [**ipv6**] **apply web-server** to restore the default.

Syntax

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

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

Default

No portal Web server is specified.

Views

Interface 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.

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

fail-permit: Enables the portal fail-permit feature on the interface. The portal fail-permit feature allows portal users to access the Internet without authentication when the portal Web server is unreachable.

Usage guidelines

You can enable both IPv4 and IPv6 portal authentication on an interface. Therefore, you can specify both an IPv4 portal Web server and an IPv6 portal Web server on the interface.

When portal fail-permit is enabled for a portal authentication server and a portal Web server on the interface, portal authentication is disabled for users on the interface if either server is unreachable. Portal authentication resumes after both servers become reachable.

Examples

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

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

Related commands

display portal

portal fail-permit server

portal web-server

portal authorization strict-checking

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

Use **undo portal authorization strict-checking** to disable strict checking on portal authorization information.

Syntax

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

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

Default

Strict checking on portal authorization information is disabled. If an authorized ACL or user profile does not exist on the device or the user profile fails to be deployed, the user will not be logged out.

Views

Interface 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

The strict checking feature on an interface allows a portal user to stay online only when the authorization information for the user is successfully deployed. The strict checking fails if the authorized ACL or user profile does not exist on the device or the device fails to deploy the authorized user profile.

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

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
```

Related commands

display portal

portal delete-user

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

Syntax

portal delete-user { *ipv4-address* | **all** | **interface** *interface-type interface-number* | **ipv6** *ipv6-address* }

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.

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.

Examples

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

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

```
[Sysname] portal delete-user 1.1.1.1
```

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

A device is not configured with a device ID.

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 (interface view)

Use **portal** [**ipv6**] **domain** to specify a portal authentication domain on an interface. All portal users accessing through the 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 an interface.

Views

Interface 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 an interface.

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

Examples

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

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

Related commands

display portal

portal enable (interface view)

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

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

Syntax

portal enable method { **direct** | **layer3** | **redhcp** }

portal ipv6 enable method { **direct** | **layer3** }

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

Default

Portal authentication is disabled.

Views

Interface view

Predefined user roles

network-admin

Parameters

ipv6: Enables IPv6 portal authentication. Do not specify this keyword for IPv4 portal authentication.

method: Specifies an authentication mode:

- **direct**—Direct authentication.
- **layer3**—Cross-subnet authentication.
- **redhcp**—Re-DHCP authentication.

Usage guidelines

To modify the portal authentication mode, first execute the **undo portal** [**ipv6**] **enable** command to disable portal authentication and then execute the **portal** [**ipv6**] **enable** command.

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

IPv6 portal authentication does not support the re-DHCP authentication mode.

You can enable both IPv4 and IPv6 portal authentication on an interface.

Examples

# Enable direct IPv4 portal authentication on VLAN-interface 100.

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

Related commands

display portal

portal fail-permit server

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

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

Interface view

Predefined user roles

network-admin

Parameters

ipv6: Specifies an IPv6 portal authentication server. Do not specify this keyword for an 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 a portal Web server on an interface, the interface disables portal authentication for portal users if either server is unreachable. Portal authentication resumes on the interface when both servers become reachable. After portal authentication resumes, unauthenticated portal users need to pass authentication to access network resources. Portal users who has passed authentication can continue accessing network resources.

You can enable portal fail-permit for at most one portal authentication server and one portal Web server on an interface.

If you execute 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 free-all except destination

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

Use **`undo portal free-all except destination`** to delete the IPv4 portal authentication destination subnets on the 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 the interface. Portal users must pass portal authentication to access any subnet.

Views

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 the 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 command deletes all IPv4 portal authentication destination subnets on the interface.

Re-DHCP authentication does not support authentication destination subnets.

If you configure both an authentication source subnet and an authentication destination subnet on an interface, only the authentication destination subnet takes effect.

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** { *ipv4-address* { *mask-length* | *mask* } | **any** } [**tcp** *tcp-port-number* | **udp** *udp-port-number*] | **source ip** { *ipv4-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. The value range for this argument is 0 to 4294967295.

destination: Specifies the destination information.

source: Specifies the source information.

ip *ipv4-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 Layer 3 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 Layer 3 interface, the portal-free rule takes effect on all portal-enabled interfaces.

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

Examples

# Configure an IPv4-based portal-free rule:

- Set the rule number to 1.
- Specify the source IP address as 10.10.10.1/24, the destination IP address as 20.20.20.1, and the destination TCP port number as 23.
- Specify the interface where the rule is applied as VLAN-interface 1.

```
<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 1
```

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

# Configure an IPv6-based portal-free rule:

- Set the rule number to 2.
- Specify the source IP address as 2000::1/64, the destination IP address as 2001::1, and the destination TCP port number as 23.
- Specify the interface as VLAN-interface 1.

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

With this rule, users in subnet 2000::1/64 do not need to pass portal authentication on VLAN-interface 1 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. The value range for this argument is 0 to 4294967295.

destination: Specifies the destination host.

host-name: Specifies the destination host by its name, a case-insensitive string of 1 to 253 characters. Valid characters are letters, digits, hyphens (-), underscores (_), dots (.), and asterisks (*). The host name string cannot be **i**, **ip**, **ipv**, or **ipv6**.

all: Specifies all portal-free rules.

Usage guidelines

You can configure a host name in one of the following ways:

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

The fuzzy match feature takes effect only on HTTP or HTTPS requests initiated by Web browsers.

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: specify the rule number as **4** and host name as **www.h3c.com**. This rule allows the portal user who sends the HTTP/HTTPS request that carries the host name **www.h3c.com** to access network resources without 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 a specific or all portal-free rules.

Syntax

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

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

Default

No source-based portal-free rules exist.

Views

System view

Predefined user roles

network-admin

Parameters

rule-number: Specifies a portal-free rule number. The value range for this argument is 0 to 4294967295.

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. This option takes effect only on portal users that access the network through VLAN interfaces.

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.

Examples

# Configure source-based portal-free rule: specify the rule number as **3**, source MAC address as **1-1-1**, and source VLAN ID as **10**. This rule allows the portal user whose source MAC address is 1-1-1 from VLAN 10 to access network resources without authentication.

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

Related commands

display portal rule

portal ipv6 free-all except destination

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

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

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. Portal users must pass portal authentication to access any IPv6 subnet.

Views

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 the 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.

Re-DHCP authentication does not support authentication destination subnets.

If you configure both an authentication source subnet and an authentication destination subnet on an interface, only the authentication destination subnet takes effect.

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 layer3 source

Use **portal ipv6 layer3 source** to configure an IPv6 portal authentication source subnet.

Use **undo portal ipv6 layer3 source** to delete IPv6 portal authentication source subnets.

Syntax

portal ipv6 layer3 source *ipv6-network-address prefix-length*

undo portal ipv6 layer3 source [*ipv6-network-address*]

Default

No IPv6 portal authentication source subnet is configured. Portal users from any IPv6 subnet must pass portal authentication.

Views

Interface view

Predefined user roles

network-admin

Parameters

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

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

Usage guidelines

With IPv6 authentication source subnets configured, only packets from IPv6 users on the authentication source subnets can trigger portal authentication. If an unauthenticated IPv6 user is not on any authentication source subnet, the access device discards all the user's packets that do not match any portal-free rule.

If you do not specify the *ipv6-network-address* argument in the **undo portal ipv6 layer3 source** command, this command deletes all IPv6 portal authentication source subnets on the interface.

Only cross-subnet authentication supports authentication source subnets.

If you configure both an authentication source subnet and an authentication destination subnet on an interface, only the authentication destination subnet takes effect.

Examples

# Configure an IPv6 portal authentication source subnet of **1::1/16** on VLAN-interface 2. Only portal users from subnet 1::1/16 trigger portal authentication.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname–Vlan-interface2] portal ipv6 layer3 source 1::1 16
```

Related commands

display portal

portal ipv6 free-all except destination

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

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 idle timeout 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.

Direct authentication and re-DHCP authentication support both ND detection and ICMPv6 detection. Cross-subnet authentication only supports ICMPv6 detection.

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 layer3 source

Use **portal layer3 source** to configure an IPv4 portal authentication source subnet.

Use **undo portal layer3 source** to delete IPv4 portal authentication source subnets.

Syntax

portal layer3 source *ipv4-network-address* { *mask-length* | *mask* }

undo portal layer3 source [*ipv4-network-address*]

Default

No IPv4 portal authentication source subnet is configured. Portal users from any IPv4 subnet must pass portal authentication.

Views

Interface view

Predefined user roles

network-admin

Parameters

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

mask-length: Specifies the subnet mask length of the IPv4 address, in the range of 0 to 32.

mask: Specifies the subnet mask in dotted decimal format.

Usage guidelines

With IPv4 authentication source subnets configured, only packets from IPv4 users on the authentication source subnets can trigger portal authentication. If an unauthenticated IPv4 user is not on any authentication source subnet, the access device discards all the user's packets that do not match any portal-free rule.

If you do not specify the *ipv4-network-address* argument in the **undo portal layer3 source** command, this command deletes all IPv4 portal authentication source subnets on the interface.

Only cross-subnet authentication supports authentication source subnets.

If you configure both an authentication source subnet and an authentication destination subnet on an interface, only the authentication destination subnet takes effect.

Examples

# Configure an IPv4 portal authentication source subnet of **10.10.10.0/24** on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname–Vlan-interface2] portal layer3 source 10.10.10.0 24
```

Related commands

display portal

portal free-all except destination

portal local-web-server

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

Use **undo portal local-web-server** to delete the HTTP- or HTTPS-based local portal Web service.

Syntax

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

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

Default

No local portal Web services exist.

Views

System view

Predefined user roles

network-admin

Parameters

http: Specifies the HTTP-based local portal Web service, which uses HTTP to exchange authentication information with clients.

https: Specifies the HTTPS-based local portal Web service, which uses 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.

tcp-port *port-number*: Specifies the listening TCP port number for the HTTPS-based local portal Web service. The value range for the *port-number* argument is 1 to 65535. The default port number is 443.

Usage guidelines

In the local portal Web service, 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 an interface to use the local portal Web service, the URL of the portal Web server specified for the interface must meet the following requirements:

- The IP address in the URL must be a local IP address on the device.
- 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.

To specify a new SSL server policy for HTTPS, first execute the **undo** form of this command to delete the existing HTTPS-based local portal Web service.

When you specify the listening TCP port number for the HTTPS-based local portal Web service, follow these restrictions and guidelines:

- For the HTTPS-based local portal Web service and other services that use HTTPS:
    - If they use the same SSL server policy, they can use the same TCP port number to listen to HTTPS.
    - If they use different SSL server policies, they cannot use the same TCP port number to listen to HTTPS.
- Do not configure the HTTPS listening TCP port number as the port number used by a known protocol (except HTTPS) or other service. For example, do not specify port numbers 80 and 23, which are used by HTTP and Telnet, respectively.
- Do not configure the same TCP port number for HTTP and HTTPS local portal Web services.

Examples

# Create an HTTP-based local portal Web service and enter its view.

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

# Create an HTTPS-based local portal Web service and associate SSL server policy **policy1** with the service.

```
<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
```

# Create an HTTPS-based local portal Web service. In the service, the associated SSL server policy is **policy1** and the listening port number is 442.

```
<Sysname> system-view
[Sysname] portal local-web-server https ssl-server-policy policy1 tcp-port 442
[Sysname-portal-local-websvr-https] quit
```

Related commands

default-logon-page

portal local-web-server

ssl server-policy

portal log enable

Use **portal log enable** to enable logging for portal user logins and logouts.

Use **undo user log enable** to disable logging for portal user logins and logouts.

Syntax

portal log enable

undo portal 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, interface name, VLAN, 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
```

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 for this argument 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 total number of the maximum IPv4 and IPv6 portal users allowed on all interfaces 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 an 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 an interface.

Views

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.

Portal access matches only the inner VLAN ID of QinQ packets. For more information about QinQ, see *Layer 2—LAN Switching Configuration Guide*.

If an interface is specified with a NAS-ID profile, the interface prefers to use the bindings defined in the profile.

If no NAS-ID profile is specified for an interface or no matching binding is found in the specified profile, the device uses the device name as the interface NAS-ID.

Examples

# Specify 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.

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. This field is mainly used to carry CPE-side service information, identifying the further service type requirement. 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 SlotID00IfNOVlanID.

- **SlotID**—Slot number, a string of 2 characters.

- **IfNO**—Slot number, a string of 3 characters.
- **VlanID**—VLAN ID, a string of 9 characters.

Format 3 is SlotID00IfNOVlanIDDHCPoption.

- **SlotID**—Slot number, a string of 2 characters.
- **IfNO**—Interface number, a string of 3 characters.
- **VlanID**—VLAN ID, a string of 9 characters.
- **DHCPoption**—DHCP option 82 is appended for IPv4 users and DHCP option 1 is appended for IPv6.

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 pre-auth ip-pool

Use **portal** [**ipv6**] **pre-auth ip-pool** to specify a preauthentication IP address pool for portal users.

Use **undo portal** [**ipv6**] **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.

Views

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 if the following conditions exist:

- The interface does not have an IP address.
- Portal users that access the network through the interface 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.

The specified IP address pool takes effect when the following requirements are met:

- The direct portal authentication mode is used on the interface.
- The specified IP address pool must have existed and been correctly configured.

Examples

# Create 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 refresh enable

Use **portal refresh** { **arp** | **nd** } **enable** to enable the Rule ARP or ND entry feature for portal clients.

Use **undo portal refresh** { **arp** | **nd** } **enable** to disable the Rule ARP or ND entry feature for portal clients.

Syntax

portal refresh { **arp** | **nd** } **enable**

undo portal refresh { **arp** | **nd** } **enable**

Default

The Rule ARP or ND entry feature is enabled for portal clients.

Views

System view

Predefined user roles

network-admin

Parameters

arp: Enables the Rule ARP entry feature.

nd: Enables the Rule ND entry feature.

Usage guidelines

When the Rule ARP or ND entry feature is enabled for portal clients, ARP or ND entries for portal clients are Rule entries after the clients come online. The Rule ARP or ND entries will not age out and will be deleted immediately after the portal clients go offline.

If portal clients go offline and then try to come online before the ARP or ND entries are relearned for them, the clients will fail the authentication. In this case, disable this feature so that ARP or ND entries are dynamic entries after the clients come online. The dynamic ARP or ND entries are deleted only when they age out.

Enabling or disabling of this feature does not affect existing Rule/dynamic ARP or ND entries for portal users.

Examples

# Disable the Rule ARP entry feature 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

Portal roaming applies only to portal users that log in from VLAN interfaces.

This command cannot be executed when online 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.

For portal roaming to take effect, you must disable the Rule ARP or ND entry feature by using the **undo portal refresh** { **arp** | **nd** } **enable** command.

Examples

# Enable portal roaming.

```
<Sysname> system-view
[Sysname] portal roaming 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.
- Destination UDP port number used by the device to send unsolicited portal packets to the portal authentication server.
- MPLS L3VPN where the portal authentication server resides.
- Pre-shared key for communication between the access device and the server.
- Server detection feature.

You can configure multiple portal authentication servers for an access device.

Examples

# Create 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 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

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 idle timeout 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.

Direct authentication and re-DHCP authentication support both ARP detection and ICMP detection. Cross-subnet authentication only supports ICMP detection.

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 (interface view)

Use **portal user-dhcp-only** to allow only users 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 users with DHCP-assigned IP addresses and users with static IP addresses can pass portal authentication to come online.

Views

Interface view

Predefined user roles

network-admin

Parameters

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

Usage guidelines

With this feature enabled, users with static IP addresses cannot pass portal authentication to get online.

To ensure that IPv6 users can pass portal authentication when this feature is enabled, disable the temporary IPv6 address feature on terminal devices. Otherwise, IPv6 users will use temporary IPv6 addresses to access the IPv6 network and will fail portal authentication.

Examples

# Allow only users with DHCP-assigned IP addresses on VLAN-interface 100 to pass portal authentication.

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

Related commands

display portal

portal web-proxy port

Use **portal web-proxy port** to specify the port number of a Web proxy server.

Use **undo portal web-proxy port** to delete port numbers of Web proxy servers.

Syntax

portal web-proxy port *port-number*

undo portal web-proxy port { *port-number* | **all** }

Default

No port numbers of Web proxy servers are specified. Proxied HTTP requests are dropped.

Views

System view

Predefined user roles

network-admin

Parameters

port-number: Specifies the port number of a Web proxy server. The value range for this argument is 1 to 65535.

all: Specifies all port numbers of Web proxy servers.

Usage guidelines

To allow HTTP requests proxied by a Web proxy server to trigger portal authentication, specify the port number of the Web proxy server on the device. If a Web proxy server port is not specified on the device, HTTP requests proxied by the Web proxy server are dropped, and portal authentication cannot be triggered.

You can configure this command multiple times to specify multiple port numbers of Web proxy servers.

If a user's browser uses the Web Proxy Auto-Discovery (WPAD) protocol to discover Web proxy servers, you must perform the following tasks on the device:

- Specify the port numbers of the Web proxy servers on the device.
- Configure portal-free rules to allow user packets destined for the IP address of the WPAD server to pass without authentication.

If portal users enable Web proxy in their browsers, the users must add the IP address of the portal authentication server as a proxy exception in their browsers. Then, HTTP packets that the users send to the portal authentication server will not be sent to Web proxy servers.

You cannot specify Web proxy server port 443 on the device.

Examples

# Specify Web proxy server port 8080.

```
<Sysname> system-view
[Sysname] portal web-proxy port 8080
```

Related commands

`portal enable method`

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 a 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

reset portal packet statistics

Use **reset portal packet statistics** to clear packet statistics for portal authentication servers.

Syntax

reset portal packet statistics [**server** *server-name*]

Views

User 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

If you do not specify the **server** *server-name* option, this command clears packet statistics for all portal authentication servers.

Examples

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

```
<Sysname> reset portal packet statistics server pts
```

Related commands

display portal packet 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**

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: Configures the device to send a log message after detecting reachability status change of the portal authentication server. The log message contains the name, the original state, and the current state of the portal authentication server.

Usage guidelines

The portal authentication server detection feature takes effect only when the device has a portal-enabled interface.

To test server reachability by detecting heartbeat packets, you must enable the server heartbeat feature on the portal authentication server. Only the IMC portal authentication server supports sending heartbeat packets.

The detection timeout configured on the device must be greater than the server heartbeat interval configured on the portal authentication server.

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.

Examples

# Enable server detection for portal authentication server **pts**:

- Set the detection timeout to 600 seconds.
- Configure the device to send a log message if the server reachability status changes.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-detect timeout 600 log
```

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**

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 10 to 1200 seconds. The default is 20 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: Configures the device to send a log message after detecting reachability status change of the portal Web server. The log message contains the name, the original state, 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.

The portal Web server detection feature takes effect only when the URL of the portal Web server is specified and the device has a portal-enabled interface.

Examples

# Enable server detection for 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 after server reachability status changes.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] server-detect interval 600 retry 2 log
```

Related commands

portal web-server

server-register

Use **server-register** to configure the device to periodically send register packets to the 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 send register packets to a portal authentication server.

Views

Portal authentication server view

Predefined user roles

network-admin

Parameters

interval *interval-value*: Specifies the interval at which the device sends register packets to the portal authentication server, in seconds. The value range for the *interval* argument is 1 to 3600, and the default value is 600.

Usage guidelines

This feature is typically used in scenarios where a NAT device exists between a portal authentication server and a large number of access devices.

If this feature is disabled, you must configure a static NAT mapping for each access device on the NAT device. If this feature is enabled, the access device automatically sends a register packet to the portal authentication server. When 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.

This feature can work with only CMCC portal authentication servers.

Examples

# Configure the device to send register packets to portal authentication server **pts** at intervals of 120 seconds.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-register interval 120
```

Related commands

server-type

server-type (portal authentication/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** }

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.

Usage guidelines

Specify the portal server type on the device with the server type the device actually uses.

Examples

# Specify the type of portal authentication server as **imc**.

```
<Sysname> system-view
[Sysname] portal server pts
[Sysname-portal-server-pts] server-type imc
```

# Specify the type of portal Web server as **imc**.

```
<Sysname> system-view
[Sysname] portal web-server pts
[Sysname-portal-websvr-pts] server-type imc
```

Related commands

display portal server

tcp-port

Use **tcp-port** to configure a listening TCP port for the local portal Web service.

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 the TCP port number set by the **portal local-web-server** command.

Views

Local portal Web service 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 service, 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 service 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.
- For the HTTPS-based local portal Web service and other services that use HTTPS:
    - If they use the same SSL server policy, they can use the same TCP port number to listen to HTTPS.

- If they use different SSL server policies, they cannot use the same TCP port number to listen to HTTPS.

Examples

# Set the listening port number to 2331 for the HTTP-based local portal Web service.

```
<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 specify 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 a 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.

To redirect users' HTTPS requests to the portal Web server URL, you must specify the HTTPS redirect listening port number by using the **http-redirect https-port** command. For more information about this command, see HTTP redirect commands in *Layer 3—IP Services Command Reference*.

Examples

# Configure the URL for 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* { **original-url** | **source-address** | **source-mac** [**encryption** { **aes** | **des** } **key** { **cipher** | **simple** } *string*] | **value** *expression* }

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.

original-url: Specifies the URL of the original webpage that a portal user visits.

source-address: Specifies the user IP address.

source-mac: Specifies the user MAC address.

encryption: Specifies the encryption algorithm to encrypt the MAC address of the user.

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.

value *expression*: Specifies a custom case-sensitive string of 1 to 256 characters.

Usage guidelines

You can configure multiple URL parameters.

If you execute this command multiple times to configure the same URL parameter, 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 the 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 the 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
```

Related commands

display portal web-server

url

user-sync

Use **user-sync** to enable portal user synchronization for a portal authentication server.

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.

Usage guidelines

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.

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 execute this command multiple times, 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 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

vpn-instance

Use **vpn-instance** to specify an MPLS L3VPN instance for a portal Web server.

Use **undo vpn-instance** to restore the default.

Syntax

vpn-instance *vpn-instance-name*

undo vpn-instance

Default

A portal Web server belongs to the public network.

Views

Portal Web server view

Predefined user roles

network-admin

Parameters

vpn-instance-name: Specifies the MPLS L3VPN instance to which the portal Web server belongs, The *vpn-instance-name* argument represents the VPN instance name, a case-sensitive string of 1 to 31 characters.

Usage guidelines

A portal Web server belongs to only one MPLS L3VPN instance.

Examples

# Specify MPLS L3VPN instance **abc** for portal Web server **wbs**.

```
<Sysname> system-view
[Sysname] portal web-server wbs
[Sysname-portal-websvr-wbs] vpn-instance abc
```

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

The Web redirect feature is disabled.

Views

Interface 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. The default interval is 86400 seconds.

Usage guidelines

With Web direct enabled on an interface, a user on the interface is first redirected 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.

Web redirect does not work when both Web redirect and portal authentication are enabled.

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
```

Related commands

`display web-redirect rule`