1 SCC Commands

Command	Function
clear access-control packet statistics	Clear the statistics about packets filtered due to access control.
direct-vlan	Configure authentication-exempted VLANs.
nac-author-user maximum	Configure the IPv4 user capacity on a port.
show access-control packet statistics	Display the statistics about packets filtered due to access control.
show direct-vlan	Display authentication-exempted VLAN configurations.
show nac-author-user	Display the IPv4 user capacity limit and the current number of IPv4 users.
station-move permit	Enable authenticated user migration.

1.1 clear access-control packet statistics

Function

Run the **clear access-control packet statistics** command to clear the statistics about packets filtered due to access control.

Syntax

clear access-control packet statistics [**interface** *interface-type interface-number* | **vlan** *vlan-id*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface whose statistics about packets filtered due to access control are cleared.

vlan *vlan-id*: Specifies the virtual local area network (VLAN) whose statistics about packets filtered due to access control are cleared.

Command Modes

Privileged EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example clears statistics about packets filtered due to access control on all interfaces.

```
Hostname> enable
Hostname# clear access-control packet statistics
```

The following example clears statistics about packets filtered due to access control on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# clear access-control packet statistics interface GigabitEthernet 0/1
```

Notifications

N/A

Platform Description

N/A

1.2 direct-vlan

Function

Run the **direct-vlan** command to configure authentication-exempted VLANs.

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

No authentication-exempted VLAN is configured by default.

Syntax

direct-vlan *vlan-list*

no direct-vlan [*vlan-list*]

Parameter Description

vlan-list: List of authentication-exempted VLANs. Use commas (,) to separate different VLANs. If a consecutive VLAN range exists, use a hyphen (-). For example, 3-5 indicates VLANs 3, 4, and 5.

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

To enable users in a VLAN to access the Internet without 802.1x or web authentication, you can configure the VLAN as an authentication-exempted VLAN.

Examples

The following example configures VLAN 2 as an authentication-exempted VLAN.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# direct-vlan 2
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.3 nac-author-user maximum

Function

Run the **nac-author-user maximum** command to configure the IPv4 user capacity on a port.

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

The IPv4 user capacity on a port is not limited by default.

Syntax

nac-author-user maximum *max-user-number*

no nac-author-user maximum

Parameter Description

max-user-number: Maximum IPv4 user capacity. The value range is from 1 to 1024.

Command Modes

Interface configuration mode

Default Level

14

Usage Guidelines

IPv4 users include those generated through 802.1x authentication, web authentication, and other binding functions. IPv4 users on a port may be generated over the port or globally. For example, when a global IPv4 user is bound to a port by running the corresponding command, the user is also calculated as a user on the port.

Examples

The following example sets the IPv4 user capacity on GigabitEthernet 0/1 to 100.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# interface GigabitEthernet 0/1
Hostname(config-if-GigabitEthernet 0/1)# nac-author-user maximum 100
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Related Commands

N/A

1.4 show access-control packet statistics

Function

Run the **show access-control packet statistics** command to display the statistics about packets filtered due to access control.

Syntax

show access-control packet statistics [**interface** *interface-type interface-number* | **vlan** *vlan-id*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface whose statistics about packets filtered due to access control are displayed.

vlan *vlan-id*: Specifies the VLAN whose statistics about packets filtered due to access control are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

This command is used to display statistics about packets filtered due to access control.

Examples

The following example displays statistics about packets filtered due to access control on all interfaces.

```
Hostname> enable
Hostname# show access-control packet statistics
Interface      Discard             Passed
----   -------   ------
Gi0/1          575                 NA
Gi0/2          575                 NA
Gi0/3          575                 NA
Vl2000         575                 NA
```

The following example displays statistics about packets filtered due to access control on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show access-control packet statistics interface GigabitEthernet 0/1
Interface : GigabitEthernet 0/1
  Discard              : 14
  Passed               : NA
```

Table 1-1Output Fields of the show access-control packet statistics Command

Field	Description
Interface	Interface name
Discard	Number of discarded packets
Passed	Number of released packets

Notifications

N/A

Platform Description

N/A

1.5 show direct-vlan

Function

Run the **show direct-vlan** command to display authentication-exempted VLAN configurations.

Syntax

show direct-vlan

Parameter Description

N/A

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays authentication-exempted VLAN configurations.

```
Hostname> enable
Hostname# show direct-vlan
direct-vlan 5,7,100
```

Table 1-1Output Fields of the show direct-vlan Command

Field	Description
direct-vlan	Authentication-exempted VLAN range

Notifications

N/A

Platform Description

N/A

1.6 show nac-author-user

Function

Run the **show nac-author-user** command to display the IPv4 user capacity limit and the current number of IPv4 users.

Syntax

show nac-author-user [**interface** *interface-type interface-number*]

Parameter Description

interface *interface-type interface-number*: Specifies the interface whose IPv4 user capacity limit and the current number of IPv4 users are displayed.

Command Modes

All modes except the user EXEC mode

Default Level

14

Usage Guidelines

N/A

Examples

The following example displays the IPv4 user capacity limit and the current number of IPv4 users on GigabitEthernet 0/1.

```
Hostname> enable
Hostname# show nac-author-user interface GigabitEthernet 0/1
 Port      Cur_num  Max_num
 ----  ---  --
 Gi0/1     0         100
```

Table 1-1 Output Fields of the show nac-author-user Command

Field	Description
Port	Device port to be queried
Cur_num	Current number of IPv4 users
Max_num	IPv4 user capacity

Notifications

N/A

Platform Description

N/A

1.7 station-move permit

Function

Run the **station-move permit** command to enable authenticated user migration.

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

Authenticated user migration is disabled by default.

Syntax

station-move permit

no station-move permit

Parameter Description

N/A

Command Modes

Global configuration mode

Default Level

14

Usage Guidelines

The authenticated user migration function allows an online authenticated user to switch to another physical location to perform authentication and go online again without getting offline.

The authenticated user migration function requires a check of users' MAC addresses, and is invalid for users who have IP addresses only.

When both 802.1x authentication and port security are enabled on a port, and port security and 802.1x authentication users get online simultaneously, 802.1x authenticated users will fail to be migrated to another port to get online because the same MAC address cannot go online through different ports.

The user online detection function can kick users offline. When the authentication user migration function is not configured and a user does not proactively get offline, the user may be kicked offline by the online detection function and can implement authentication and get online in another physical location.

When an online authenticated user moves to a new physical location, the user needs to perform 802.1x or web authentication again.

Examples

The following example enables authenticated user migration.

```
Hostname> enable
Hostname# configure terminal
Hostname(config)# station-move permit
```

Notifications

N/A

Common Errors

N/A

Platform Description

N/A

Platform Description

N/A

Related Commands

N/A