Contents

Port security commands

display port-security

Use **display port-security** to display port security configuration, operation information, and statistics for ports.

Syntax

display port-security [**interface** *interface-type interface-number*]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number. If you do not specify a port, this command displays port security information for all ports.

Examples

Display port security information for all ports.

```
<Sysname> display port-security
Global port security parameters:
   Port security         : Enabled
   AutoLearn aging time   : 0 min
   Disableport timeout    : 20 s
   MAC move             : Denied
   Authorization fail     : Online
   NAS-ID profile        : Not configured
   Dot1x-failure trap     : Disabled
   Dot1x-logon trap      : Disabled
   Dot1x-logoff trap     : Enabled
   Intrusion trap        : Disabled
   Address-learned trap   : Enabled
   Mac-auth-failure trap  : Disabled
   Mac-auth-logon trap    : Enabled
   Mac-auth-logoff trap   : Disabled
   Open authentication    : Disabled
   OUI value list        :
    Index :  1         Value : 123401

 GigabitEthernet1/0/1 is link-up
   Port mode                   : userLogin
   NeedToKnow mode              : Disabled
   Intrusion protection mode     : NoAction
   Security MAC address attribute
      Learning mode            : Sticky
```

```
   Aging type              : Periodical
Max secure MAC addresses      : 32
Current secure MAC addresses   : 0
Authorization               : Permitted
NAS-ID profile              : Not configured
Free VLANs                  : Not configured
Open authentication         : Disabled
```

Table 1 Command output

Field	Description
Port security	Whether the port security feature is enabled.
AutoLearn aging time	Sticky MAC address aging timer, in minutes or seconds.
Disableport timeout	Silence period (in seconds) of the port that receives illegal packets.
MAC move	Status of MAC move: • If the feature is enabled, this field displays **Permitted**. • If the feature is disabled, this field displays **Denied**.
Authorization fail	Action to be taken for users that fail authorization: • **Online**—Allows the users to go online. • **Offline**—Logs off the users.
NAS-ID profile	NAS-ID profile applied globally.
Dot1x-failure trap	Whether SNMP notifications for 802.1X authentication failures are enabled.
Dot1x-logon trap	Whether SNMP notifications for 802.1X authentication successes are enabled.
Dot1x-logoff trap	Whether SNMP notifications for 802.1X authenticated user logoffs are enabled.
Intrusion trap	Whether SNMP notifications for intrusion protection are enabled. If they are enabled, the device sends SNMP notifications after illegal packets are detected.
Address-learned trap	Whether SNMP notifications for MAC address learning are enabled. If they are enabled, the device sends SNMP notifications after it learns a new MAC address.
Mac-auth-failure trap	Whether SNMP notifications for MAC authentication failures are enabled.
Mac-auth-logon trap	Whether SNMP notifications for MAC authentication successes are enabled.
Mac-auth-logoff trap	Whether SNMP notifications for MAC authentication user logoffs are enabled.
Open authentication	Whether global open authentication mode is enabled.
OUI value list	List of OUI values allowed for authentication.

Field	Description
Port mode	Port security mode: • noRestrictions. • autoLearn. • macAddressWithRadius. • macAddressElseUserLoginSecure. • macAddressElseUserLoginSecureExt. • secure. • userLogin. • userLoginSecure. • userLoginSecureExt. • macAddressOrUserLoginSecure. • macAddressOrUserLoginSecureExt. • userLoginWithOUI. For more information about port security modes, see *Security Configuration Guide*.
NeedToKnow mode	Need to know (NTK) mode: • **NeedToKnowOnly**—Allows only unicast packets with authenticated destination MAC addresses. • **NeedToKnowWithBroadcast**—Allows only unicast packets and broadcasts with authenticated destination MAC addresses. • **NeedToKnowWithMulticast**—Allows unicast packets, multicasts, and broadcasts with authenticated destination MAC addresses. • **Disabled**—NTK is disabled.
Intrusion protection mode	Intrusion protection action: • **BlockMacAddress**—Adds the source MAC address of the illegal packet to the blocked MAC address list. • **DisablePort**—Shuts down the port that receives illegal packets permanently. • **DisablePortTemporarily**—Shuts down the port that receives illegal packets for some time. • **NoAction**—Does not perform intrusion protection.
Learning mode	Secure MAC address learning mode: • **Dynamic**. • **Sticky**.
Aging type	Secure MAC address aging type: • **Periodical**—Timer aging only. • **Inactivity**—Inactivity aging feature together with the aging timer.
Max secure MAC addresses	Maximum number of secure MAC addresses (or online users) that port security allows on the port.
Current secure MAC addresses	Number of secure MAC addresses stored.
Authorization	Whether the authorization information from the authentication server (RADIUS server or local device) is ignored: • **Permitted**—Authorization information from the authentication server takes effect. • **Ignored**—Authorization information from the authentication server does not take effect.
NAS-ID profile	NAS-ID profile applied to the port.

Field	Description
Free VLANs	This field is not supported in the current software version. VLANs in which packets will not trigger authentication. If you do not configure free VLANs, this field displays **Not configured**.
Open authentication	Whether open authentication mode is enabled on the port.

display port-security mac-address block

Use **display port-security mac-address block** to display information about blocked MAC addresses.

Syntax

display port-security mac-address block [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its ID. The value range is 1 to 4094.

count: Displays only the count of the blocked MAC addresses.

Usage guidelines

If you do not specify any parameters, this command displays information about all blocked MAC addresses.

Examples

Display information about all blocked MAC addresses.

```
<Sysname> display port-security mac-address block
 MAC ADDR           Port                   VLAN ID
 000f-3d80-0d2d     GE1/0/1                30

 --- On slot 1, 1 MAC address(es) found ---

 --- 1 mac address(es) found ---
```

Display the count of all blocked MAC addresses.

```
<Sysname> display port-security mac-address block count

--- On slot 1, 1 MAC address(es) found ---

--- 1 mac address(es) found ---
```

Table 2 Command output

Field	Description
MAC ADDR	Blocked MAC address.
Port	Port having received frames with the blocked MAC address being the source address.
VLAN ID	ID of the VLAN to which the port belongs.
number mac address(es) found	Number of blocked MAC addresses.

Related commands

port-security intrusion-mode

display port-security mac-address security

Use **display port-security mac-address security** to display information about secure MAC addresses.

Syntax

display port-security mac-address security [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]

Views

Any view

Predefined user roles

network-admin

network-operator

Parameters

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies a VLAN by its ID. The value range is 1 to 4094.

count: Displays only the count of the secure MAC addresses.

Usage guidelines

Secure MAC addresses are those that are automatically learned by the port in autoLearn mode or configured by the **port-security mac-address security** command.

If you do not specify any parameters, this command displays information about all secure MAC addresses.

Examples

Display information about all secure MAC addresses.

```
<Sysname> display port-security mac-address security
 MAC ADDR        VLAN ID  STATE         PORT INDEX                AGING TIME
 0002-0002-0002  1        Security      GE1/0/1                    Not aged

 --- Number of secure MAC addresses: 1 ---
```

Display only the count of the secure MAC addresses.

```
<Sysname> display port-security mac-address security count
```

```
--- Number of secure MAC addresses: 1 ---
```

Table 3 Command output

Field	Description
MAC ADDR	Secure MAC address.
VLAN ID	ID of the VLAN to which the port belongs.
STATE	Type of the MAC address. This field displays **Security** for a secure MAC address.
PORT INDEX	Port to which the secure MAC address belongs.
AGING TIME	Period of time before the secure MAC address ages out. • If the secure MAC address is a static MAC address, this field displays **Not aged**. • If the secure MAC address is a sticky MAC address, this field displays the remaining lifetime. If the remaining lifetime is less than 60 seconds, the lifetime is counted in seconds. If the lifetime is not less than 60 seconds, the lifetime is counted in minutes. By default, sticky MAC addresses do not age out, and this field displays **Not aged**.
Number of secure MAC addresses	Number of secure MAC addresses stored.

Related commands

port-security mac-address security

port-security access-user log enable

Use **port-security access-user log enable** to enable logging for port security users.

Use **undo port-security access-user log enable** to disable logging for port security users.

Syntax

port-security access-user log enable [**failed-authorization** | **mac-learning** | **violation**] *

undo port-security access-user log enable [**failed-authorization** | **mac-learning** | **violation**] *

Default

All types of logging are disabled for port security users.

Views

System view

Predefined user roles

network-admin

Parameters

failed-authorization: Specifies logs generated for authorization failures of 802.1X or MAC authentication users.

mac-learning: Specifies logs generated for new MAC address learning.

violation: Specifies logs generated when intrusion protection is triggered.

Usage guidelines

As a best practice, disable this feature to prevent excessive output of logs for port security users.

If you do not specify any parameters, this command enables all types of logging for port security users.

Examples

Enable logging for intrusion protection.

```
<Sysname> system-view
[Sysname] port-security access-user log enable violation
```

Related commands

info-center source portsec logfile deny (*Network Management and Monitoring Command Reference*)

port-security authentication open

Use **port-security authentication open** to enable open authentication mode on a port.

Use **undo port-security authentication open** to disable open authentication mode on a port.

Syntax

port-security authentication open

undo port-security authentication open

Default

Open authentication mode is disabled on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command enables access users (802.1X or MAC authentication users) of a port to come online and access the network even if they use nonexistent usernames or incorrect passwords.

Access users that come online in open authentication mode are called open users. Authorization and accounting are not available for open users. To display open user information, use the following commands:

- **display dot1x connection open**.
- **display mac-authentication connection open**.

Open authentication mode does not affect the access of users that use correct user information on the port.

The open authentication mode setting has lower priority than the 802.1X Auth-Fail VLAN and the MAC authentication guest VLAN. Open authentication mode does not take effect on a port if the port is also configured with the 802.1X Auth-Fail VLAN or the MAC authentication guest VLAN.

For information about 802.1X authentication or MAC authentication, see *Security Configuration Guide*.

Examples

Enable open authentication mode on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security authentication open
```

Related commands

display dot1x connection

display mac-authentication connection

port-security authentication open global

port-security authentication open global

Use **port-security authentication open global** to enable global open authentication mode.

Use **undo port-security authentication open global** to disable global open authentication mode.

Syntax

port-security authentication open global

undo port-security authentication open global

Default

Global open authentication mode is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command enables access users (802.1X or MAC authentication users) to come online and access the network even if they use nonexistent usernames or incorrect passwords.

Access users that come online in open authentication mode are called open users. Authorization and accounting are not available for open users. To display open user information, use the following commands:

- **display dot1x connection open**.
- **display mac-authentication connection open**.

Open authentication mode does not affect the access of users that use correct user information.

The open authentication mode setting has lower priority than the 802.1X Auth-Fail VLAN and the MAC authentication guest VLAN. Open authentication mode does not take effect on a port if the port is also configured with the 802.1X Auth-Fail VLAN or the MAC authentication guest VLAN.

For information about 802.1X authentication or MAC authentication, see *Security Configuration Guide*.

Examples

Enable global open authentication mode.

```
<Sysname> system-view
[Sysname] port-security authentication open global
```

Related commands

display dot1x connection

display mac-authentication connection

port-security authentication open

port-security authorization ignore

Use **port-security authorization ignore** to configure a port to ignore the authorization information received from the authentication server (a RADIUS server or the local device).

Use **undo port-security authorization ignore** to restore the default.

Syntax

port-security authorization ignore

undo port-security authorization ignore

Default

A port uses the authorization information from the server.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

After a user passes RADIUS or local authentication, the server performs authorization based on the authorization attributes configured for the user account. For example, the server can assign a VLAN. If you do not want the port to use such authorization attributes for users, use this command to ignore the authorization information from the server.

Examples

Configure GigabitEthernet 1/0/1 to ignore the authorization information from the authentication server.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security authorization ignore
```

Related commands

display port-security

port-security authorization-fail offline

Use **port-security authorization-fail offline** to enable the authorization-fail-offline feature.

Use **undo port-security authorization-fail offline** to disable the authorization-fail-offline feature.

Syntax

port-security authorization-fail offline [**quiet-period**]

undo port-security authorization-fail offline

Default

The authorization-fail-offline feature is disabled. The device does not log off users that fail authorization.

Views

System view

Predefined user roles

network-admin

Parameters

quiet-period: Enables the quiet timer for 802.1X or MAC authentication users that are logged off by the authorization-fail-offline feature. The device adds these users to the 802.1X or MAC authentication quiet queue. Within the quiet timer, the device does not process packets from these users or authenticate them. If you do not specify this keyword, the quiet timer feature is disabled for users that are logged off by the authorization-fail-offline feature. The device immediately authenticates these users upon receiving packets from them.

Usage guidelines

The authorization-fail-offline feature logs off port security users that fail ACL or user profile authorization.

A user fails ACL or user profile authorization in the following situations:

- The device fails to authorize the specified ACL or user profile to the user.
- The server assigns a nonexistent ACL or user profile to the user.

If this feature is disabled, the device does not log off users that fail ACL or user profile authorization. However, the device outputs messages to report the failure.

For the **quiet-period** keyword to take effect, complete the following tasks:

- For 802.1X users, use the **dot1x quiet-period** command to enable the quiet timer and use the **dot1x timer quiet-period** command to set the timer.
- For MAC authentication users, use the **mac-authentication timer quiet** command to set the quiet timer for MAC authentication.

Examples

Enable the authorization-fail-offline feature.

```
<Sysname> system-view
[Sysname] port-security authorization-fail offline
```

Related commands

display port-security

dot1x quiet-period

dot1x timer quiet-period

mac-authentication timer

port-security enable

Use **port-security enable** to enable port security.

Use **undo port-security enable** to disable port security.

Syntax

port-security enable

undo port-security enable

Default

Port security is disabled.

Views

System view

Predefined user roles

network-admin

Usage guidelines

You must disable global 802.1X and MAC authentication before you enable port security on a port.

Enabling or disabling port security resets the following security settings to the default:

- 802.1X access control mode is MAC-based.
- Port authorization state is auto.

When online users are present on a port, disabling port security logs off the online users.

Examples

Enable port security.

```
<Sysname> system-view
[Sysname] port-security enable
```

Related commands

display port-security

dot1x

dot1x port-control

dot1x port-method

mac-authentication

port-security intrusion-mode

Use **port-security intrusion-mode** to configure the intrusion protection feature so the port takes the predefined actions when intrusion protection detects illegal frames on the port.

Use **undo port-security intrusion-mode** to restore the default.

Syntax

port-security intrusion-mode { **blockmac** | **disableport** | **disableport-temporarily** }

undo port-security intrusion-mode

Default

Intrusion protection is disabled.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

blockmac: Adds the source MAC addresses of illegal frames to the blocked MAC address list and discards frames with blocked source MAC addresses. This action implements illegal traffic filtering on the port. A blocked MAC address is restored to normal after being blocked for 3 minutes, which is not user configurable. To display the blocked MAC address list, use the **display port-security mac-address block** command.

disableport: Disables the port permanently upon detecting an illegal frame received on the port.

disableport-temporarily: Disables the port for a period of time whenever it receives an illegal frame. You can use the **port-security timer disableport** command to set the period.

Usage guidelines

To restore the connection of the port disabled by the intrusion protection feature, use the **undo shutdown** command.

Examples

Configure GigabitEthernet 1/0/1 to block the source MAC addresses of illegal frames after intrusion protection detects the illegal frames.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode blockmac
```

Related commands

display port-security

display port-security mac-address block

port-security timer disableport

port-security mac-address aging-type inactivity

Use **port-security mac-address aging-type inactivity** to enable inactivity aging for secure MAC addresses.

Use **undo port-security mac-address aging-type inactivity** to disable inactivity aging for secure MAC addresses.

Syntax

port-security mac-address aging-type inactivity

undo port-security mac-address aging-type inactivity

Default

The inactivity aging feature is disabled for secure MAC addresses.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

This command enables the device to periodically detect traffic data from secure MAC addresses.

If only the aging timer is configured, the aging timer counts up regardless of whether traffic data has been sent from the secure MAC addresses. When you use the aging timer together with the inactivity aging feature, the aging timer restarts once traffic data is detected from the secure MAC addresses. The secure MAC addresses age out only when no traffic data is detected within the aging timer.

The inactivity aging feature prevents the unauthorized use of a secure MAC address when the authorized user is offline. The feature also removes outdated secure MAC addresses so that new secure MAC addresses can be learned or configured.

If the aging timer is set to a value not less than 60 seconds, the traffic data detection interval is fixed at 30 seconds.

If the aging timer is set to a value less than 60 seconds, the traffic data detection interval is the effective aging period.

To set the aging timer for secure MAC addresses, use the **port-security timer autolearn aging** command.

This command takes effect only on sticky MAC addresses and dynamic secure MAC addresses.

Examples

Enable inactivity aging for secure MAC addresses on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-address aging-type inactivity
```

Related commands

display port-security

port-security mac-address dynamic

Use **port-security mac-address dynamic** to enable the dynamic secure MAC feature.

Use **undo port-security mac-address dynamic** to disable the dynamic secure MAC feature.

Syntax

port-security mac-address dynamic

undo port-security mac-address dynamic

Default

The dynamic secure MAC feature is disabled. Sticky MAC addresses can be saved to the configuration file. Once saved, they survive a device reboot.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Usage guidelines

The dynamic secure MAC feature converts sticky MAC addresses to dynamic and disables saving them to the configuration file.

After you execute this command, you cannot manually configure sticky MAC addresses, and secure MAC addresses learned by a port in autoLearn mode are dynamic. All dynamic MAC addresses are lost at reboot. Use this command when you want to clear all sticky MAC addresses after a device reboot.

You can display dynamic secure MAC addresses by using the **display port-security mac-address security** command.

The **undo port-security mac-address dynamic** command converts all dynamic secure MAC addresses on the port to sticky MAC addresses. You can manually configure sticky MAC addresses.

Examples

Enable the dynamic secure MAC feature on GigabitEthernet 1/0/1.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-address dynamic
```

Related commands

display port-security

display port-security mac-address security

port-security mac-address security

Use **port-security mac-address security** to add a secure MAC address.

Use **undo port-security mac-address security** to remove a secure MAC address.

Syntax

In Layer 2 Ethernet interface view:

port-security mac-address security [**sticky**] *mac-address* **vlan** *vlan-id*

undo port-security mac-address security [**sticky**] *mac-address* **vlan** *vlan-id*

In system view:

port-security mac-address security [**sticky**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo port-security mac-address security [[*mac-address* [**interface** *interface-type interface-number*]] **vlan** *vlan-id*]

Default

No manually configured secure MAC address entries exist.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

sticky: Specifies the MAC address type as sticky. If you do not specify this keyword, the command configures a static secure MAC address.

mac-address: Specifies a MAC address, in H-H-H format.

interface *interface-type interface-number*: Specifies a port by its type and number.

vlan *vlan-id*: Specifies the VLAN to which the secure MAC address belongs. The value range for the *vlan-id* argument is 1 to 4094.

Usage guidelines

Secure MAC addresses are MAC addresses configured or learned in autoLearn mode, and if saved, can survive a device reboot. You can bind a secure MAC address only to one port in a VLAN.

You can add important or frequently used MAC addresses as sticky or static secure MAC addresses to avoid the secure MAC address limit causing authentication failure. To successfully add secure MAC addresses on a port, first complete the following tasks:

- Enable port security on the port.

- Set the port security mode to autoLearn.
- Configure the port to permit packets of the specified VLAN to pass or add the port to the VLAN. Make sure the VLAN already exists.

Sticky MAC addresses can be manually configured or automatically learned in autoLearn mode. Sticky MAC addresses do not age out by default. You can use the **port-security timer autolearn aging** command to set an aging timer for the sticky MAC addresses. When the timer expires, the sticky MAC addresses are removed.

Static secure MAC addresses never age out unless you perform the following operations:

- Remove these MAC addresses by using the **undo port-security mac-address security** command.
- Change the port security mode.
- Disable the port security feature.

You cannot change the type of a secure address entry that has been added or add two entries that are identical except for their entry type. For example, you cannot add the **port-security mac-address security sticky 1-1-1 vlan 10** entry when a **port-security mac-address security 1-1-1 vlan 10** entry exists. To add the new entry, you must delete the old entry.

Examples

Enable port security, set GigabitEthernet 1/0/1 to operate in autoLearn mode, and configure the port to support a maximum number of 100 secure MAC addresses.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
[Sysname-GigabitEthernet1/0/1] port-security port-mode autolearn
```

Specify MAC address 0001-0002-0003 in VLAN 4 as a sticky MAC address.

```
[Sysname-GigabitEthernet1/0/1] port-security mac-address security sticky 0001-0002-0003
vlan 4
[Sysname-GigabitEthernet1/0/1] quit
```

In system view, specify MAC address 0001-0001-0002 in VLAN 10 as a secure MAC address for GigabitEthernet 1/0/1.

```
[Sysname] port-security mac-address security 0001-0001-0002 interface gigabitethernet
1/0/1 vlan 10
```

Related commands

display port-security

port-security timer autolearn aging

port-security mac-limit

Use **port-security mac-limit** to set the maximum number of MAC addresses that port security allows for specific VLANs on a port.

Use **undo port-security mac-limit** to restore the default.

Syntax

port-security mac-limit *max-number* **per-vlan** *vlan-id-list*

undo port-security mac-limit per-vlan *vlan-id-list*

Default

The maximum number is 2147483647.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-number: Specifies the maximum number of MAC addresses. The value range is 1 to 2147483647.

per-vlan *vlan-id-list*: Applies the maximum number to a VLAN list on per-VLAN basis. The *vlan-id-list* argument specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN by VLAN ID or specifies a range of VLANs in the form of *vlan-id1* **to** *vlan-id2*. The value range for the VLAN IDs is 1 to 4094. The value for the *vlan-id2* argument must be equal to or greater than the value for the *vlan-id1* argument.

Usage guidelines

This command limits the number of MAC addresses that port security allows to access a port through specific VLANs. Use this command to prevent resource contentions among MAC addresses and ensure reliable performance for each access user on the port. When the number of MAC addresses in a VLAN on the port reaches the upper limit, the device denies any subsequent MAC addresses in the VLAN on the port.

Port security allows the access of the following types of MAC addresses on a port:

- MAC addresses that pass 802.1X or MAC authentication.
- MAC addresses in the MAC authentication guest VLAN or MAC authentication critical VLAN.
- MAC addresses in the 802.1X guest VLAN, 802.1X Auth-Fail VLAN, or 802.1X critical VLAN.

On a port, the maximum number of MAC addresses in a VLAN cannot be smaller than the number of existing MAC addresses in the VLAN. If the specified maximum number is smaller, the setting does not take effect.

Examples

On GigabitEthernet 1/0/1, configure VLAN 1, VLAN 5, and VLANs 10 through 20 each to allow a maximum of 32 MAC authentication and 802.1X users.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security mac-limit 32 per-vlan 1 5 10 to 20
```

Related commands

display dot1x

display mac-authentication

port-security mac-move permit

Use **port-security mac-move permit** to enable MAC move on the device.

Use **undo port-security mac-move permit** to disable MAC move on the device.

Syntax

port-security mac-move permit

undo port-security mac-move permit

Default

MAC move is disabled on the device.

Views

System view

Predefined user roles

network-admin

Usage guidelines

This command takes effect on both 802.1X and MAC authentication users.

MAC move allows 802.1X or MAC authenticated users to move between ports on a device. For example, if an 802.1X-authenticated user moves to another 802.1X-enabled port on the device, the authentication session is deleted from the first port. The user is reauthenticated on the new port.

If MAC move is disabled, 802.1X or MAC users authenticated on one port cannot pass authentication after they move to another port.

802.1X or MAC authenticated users cannot move between ports on a device if the number of online users on the authentication server (local or remote) has reached the upper limit.

Examples

Enable MAC move.

```
<Sysname> system-view
[Sysname] port-security mac-move permit
```

Related commands

display port-security

port-security max-mac-count

Use **port-security max-mac-count** to set the maximum number of secure MAC addresses that port security allows on a port.

Use **undo port-security max-mac-count** to restore the default.

Syntax

port-security max-mac-count *max-count* [**vlan** [*vlan-id-list*]]

undo port-security max-mac-count [**vlan** [*vlan-id-list*]]

Default

Port security does not limit the number of secure MAC addresses on a port.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

max-count: Specifies the maximum number of secure MAC addresses that port security allows on the port. The value range is 1 to 2147483647.

vlan [*vlan-id-list*]: Specifies a space-separated list of up to 10 VLAN items. Each VLAN item specifies a VLAN ID or a range of VLAN IDs in the form of *start-vlan-id* **to** *end-vlan-id*. The end VLAN ID cannot be smaller than the start VLAN ID. The value range for

VLAN IDs is 1 to 4094. If you do not specify the **vlan** keyword, this command sets the maximum number of secure MAC addresses that port security allows on a port. If you do not specify the *vlan-id-list* argument, this command sets the maximum number of secure MAC addresses for each VLAN on the port. This option takes effect only on a port that operates in autoLearn mode.

Usage guidelines

For autoLearn mode, this command sets the maximum number of secure MAC addresses (both configured and automatically learned) on the port.

In any other mode that enables 802.1X, MAC authentication, or both, this command sets the maximum number of authenticated MAC addresses on the port. The actual maximum number of concurrent users that the port accepts equals the smaller of the following values:

- The value set by using this command.
- The maximum number of concurrent users allowed by the authentication mode in use.

For example, in userLoginSecureExt mode, if 802.1X allows more concurrent users than port security's limit on the number of MAC addresses, port security's limit takes effect.

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

- Make sure the maximum number of secure MAC addresses for a VLAN is not less than the number of MAC addresses currently saved for the VLAN.
- If you execute this command multiple times to set the maximum number of secure MAC addresses for the same VLAN, the most recent configuration takes effect.
- You cannot change port security's limit on the number of MAC addresses when the port is operating in autoLearn mode.

Examples

Set the maximum number of secure MAC address port security allows on GigabitEthernet 1/0/1 to 100.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security max-mac-count 100
```

Related commands

display port-security

port-security nas-id-profile

Use **port-security nas-id-profile** to apply a NAS-ID profile to global or port-based port security.

Use **undo port-security nas-id-profile** to restore the default.

Syntax

port-security nas-id-profile *profile-name*

undo port-security nas-id-profile

Default

No NAS-ID profile is applied to port security globally or on any port.

Views

System view

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

profile-name: Specifies a NAS-ID profile by its name. The argument is a case-insensitive string of 1 to 31 characters.

Usage guidelines

A NAS-ID profile defines NAS-ID and VLAN bindings. You can create a NAS-ID profile by using the **aaa nas-id profile** command.

The device selects a NAS-ID profile for a port in the following order:

1. The port-specific NAS-ID profile.
2. The NAS-ID profile applied globally.

If no NAS-ID profile is applied or no matching binding is found in the selected profile, the device uses the device name as the NAS-ID.

Examples

Apply NAS-ID profile **aaa** to GigabitEthernet 1/0/1 for port security.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security nas-id-profile aaa
```

Globally apply NAS-ID profile **aaa** to port security.

```
<Sysname> system-view
[Sysname] port-security nas-id-profile aaa
```

Related commands

aaa nas-id profile

port-security ntk-mode

Use **port-security ntk-mode** to configure the NTK feature.

Use **undo port-security ntk-mode** to restore the default.

Syntax

port-security ntk-mode { **ntk-withbroadcasts** | **ntk-withmulticasts** | **ntkonly** }

undo port-security ntk-mode

Default

The NTK feature is not configured on a port and all frames are allowed to be sent.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

ntk-withbroadcasts: Forwards only broadcast frames and unicast frames with authenticated destination MAC addresses.

ntk-withmulticasts: Forwards only broadcast frames, multicast frames, and unicast frames with authenticated destination MAC addresses.

ntkonly: Forwards only unicast frames with authenticated destination MAC addresses.

Usage guidelines

The NTK feature checks the destination MAC addresses in outbound frames. This feature allows frames to be sent only to devices passing authentication, preventing illegal devices from intercepting network traffic.

Examples

Set the NTK mode of GigabitEthernet 1/0/1 to **ntkonly**, allowing the port to forward received packets only to devices passing authentication.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

Related commands

display port-security

port-security oui

Use **port-security oui** to configure an OUI value for user authentication.

Use **undo port-security oui** to delete the OUI value with the specified OUI index.

Syntax

port-security oui index *index-value* **mac-address** *oui-value*

undo port-security oui index *index-value*

Default

No OUI values are configured.

Views

System view

Predefined user roles

network-admin

Parameters

index-value: Specifies the OUI index, in the range of 1 to 16.

oui-value: Specifies an OUI string, a 48-bit MAC address in the H-H-H format. The system uses only the 24 high-order bits as the OUI value.

Usage guidelines

You can configure multiple OUI values.

An OUI, the first 24 binary bits of a MAC address, is assigned by IEEE to uniquely identify a device vendor. Use this command to allow devices of specific vendors to access the network without being authenticated. For example, you can specify the OUIs of IP phones and printers.

The OUI values configured by this command apply only to the ports operating in userLoginWithOUI mode. In userLoginWithOUI mode, a port allows only one 802.1X user and one user whose MAC address matches one of the configured OUI values.

Examples

Configure an OUI value of 000d2a, and set the index to 4.

```
<Sysname> system-view
[Sysname] port-security oui index 4 mac-address 000d-2a10-0033
```

Related commands

display port-security

port-security port-mode

Use **port-security port-mode** to set the port security mode of a port.

Use **undo port-security port-mode** to restore the default.

Syntax

port-security port-mode { autolearn | mac-authentication | mac-else-userlogin-secure | mac-else-userlogin-secure-ext | secure | userlogin | userlogin-secure | userlogin-secure-ext | userlogin-secure-or-mac | userlogin-secure-or-mac-ext | userlogin-withoui }

undo port-security port-mode

Default

A port operates in noRestrictions mode, where port security does not take effect.

Views

Layer 2 Ethernet interface view

Predefined user roles

network-admin

Parameters

Keyword	Security mode	Description
autolearn	autoLearn	A port in this mode can learn MAC addresses. The automatically learned MAC addresses are not added to the MAC address table as dynamic MAC address. Instead, the MAC addresses are added to the secure MAC address table as secure MAC addresses. You can also configure secure MAC addresses by using the **port-security mac-address security** command. A port in autoLearn mode allows frames sourced from the following MAC addresses to pass: • Secure MAC addresses. • MAC addresses configured by using the **mac-address dynamic** and **mac-address static** commands. When the number of secure MAC addresses reaches the upper limit set by the **port-security max-mac-count** command, the port changes to **secure** mode.
mac-authentication	macAddressWithRadius	In this mode, a port performs MAC authentication for users and services multiple users.

Keyword	Security mode	Description
mac-else-userlogin-secure	macAddressElseUserLoginSecure	This mode is the combination of the macAddressWithRadius and userLoginSecure modes, with MAC authentication having a higher priority. In this mode, the port allows one 802.1X authentication user and multiple MAC authentication users to log in. • Upon receiving a non-802.1X frame, a port in this mode performs only MAC authentication. • Upon receiving an 802.1X frame, the port performs MAC authentication and then, if MAC authentication fails, 802.1X authentication.
mac-else-userlogin-secure-ext	macAddressElseUserLoginSecureExt	Same as the macAddressElseUserLoginSecure mode except that a port in this mode supports multiple 802.1X and MAC authentication users.
secure	secure	In this mode, MAC address learning is disabled on the port and you can configure MAC addresses by using the **mac-address static** and **mac-address dynamic** commands. The port permits only frames sourced from the following MAC addresses to pass: • Secure MAC addresses. • MAC addresses configured by using the **mac-address static** and **mac-address dynamic** commands.
userlogin	userLogin	In this mode, a port performs 802.1X authentication and implements port-based access control. If one 802.1X user passes authentication, all the other 802.1X users of the port can access the network without authentication.
userlogin-secure	userLoginSecure	In this mode, a port performs 802.1X authentication and implements MAC-based access control. The port services only one user passing 802.1X authentication.
userlogin-secure-ext	userLoginSecureExt	Same as the userLoginSecure mode, except that this mode supports multiple online 802.1X users.
userlogin-secure-or-mac	macAddressOrUserLoginSecure	This mode is the combination of the userLoginSecure and macAddressWithRadius modes. In this mode, the port allows one 802.1X authentication user and multiple MAC authentication users to log in. In this mode, the port performs 802.1X authentication first. By default, if 802.1X authentication fails, MAC authentication is performed. However, the port in this mode processes authentication differently when the following conditions exist: • The port is enabled with parallel processing of MAC authentication and 802.1X authentication. • The port is enabled with the 802.1X unicast trigger. • The port receives a packet from an unknown MAC address. Under such conditions, the port sends a unicast EAP-Request/Identity packet to the MAC address to initiate 802.1X authentication. After that, the port immediately processes MAC authentication without waiting for the 802.1X authentication result.

Keyword	Security mode	Description
userlogin-secure-or-mac-ext	macAddressOrUserLoginSecureExt	Same as the macAddressOrUserLoginSecure mode, except that a port in this mode supports multiple 802.1X and MAC authentication users.
userlogin-without-oui	userLoginWithOUI	Similar to the userLoginSecure mode. In addition, a port in this mode also permits frames from a user whose MAC address contains a specific OUI. In this mode, the port performs OUI check at first. If the OUI check fails, the port performs 802.1X authentication. The port permits frames that pass OUI check or 802.1X authentication.

Usage guidelines

To change the security mode for a port security enabled port, you must set the port in noRestrictions mode first. Do not change port security mode when the port has online users.

IMPORTANT:

If you are configuring the autoLearn mode, first set port security's limit on the number of secure MAC addresses by using the **port-security max-mac-count** command. You cannot change the setting when the port is operating in autoLearn mode.

When port security is enabled, you cannot enable 802.1X or MAC authentication, or change the access control mode or port authorization state. The port security automatically modifies these settings in different security modes.

As a best practice, do not enable the **mac-else-userlogin-secure** or **mac-else-userlogin-secure-ext** mode on the port where MAC authentication delay is enabled. The two modes are mutually exclusive with the MAC authentication delay feature. For more information about MAC authentication delay, see "MAC authentication commands."

Examples

Enable port security, and set GigabitEthernet 1/0/1 to operate in secure mode.

```
<Sysname> system-view
[Sysname] port-security enable
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security port-mode secure
```

Change the port security mode of GigabitEthernet 1/0/1 to userLogin.

```
[Sysname-GigabitEthernet1/0/1] undo port-security port-mode
[Sysname-GigabitEthernet1/0/1] port-security port-mode userlogin
```

Related commands

display port-security

port-security max-mac-count

port-security timer autolearn aging

Use **port-security timer autolearn aging** to set the secure MAC aging timer.

Use **undo port-security timer autolearn aging** to restore the default.

Syntax

port-security timer autolearn aging [**second**] *time-value*

undo port-security timer autolearn aging

Default

Secure MAC addresses do not age out.

Views

System view

Predefined user roles

network-admin

Parameters

second: Specifies the aging timer in seconds for secure MAC addresses. If you do not specify this keyword, the command sets the aging timer in minutes for secure MAC addresses.

time-value: Specifies the aging timer. The value range is 0 to 129600 if the unit is minute. To disable the aging timer, set the timer to 0. The value range is 10 to 7776000 if the unit is second.

Usage guidelines

The timer applies to all sticky secure MAC addresses and those automatically learned by a port.

The effective aging timer varies by the aging timer setting:

- If the aging timer is set in seconds, the effective aging timer can be either of the following values:
  - The nearest multiple of 30 seconds to the configured aging timer if the configured timer is not less than 60 seconds. The effective aging timer is not less than the configured aging timer.
  - The configured aging timer if the configured timer is less than 60 seconds.
- If the aging timer is set in minutes, the effective aging timer is the configured aging timer.

A short aging time improves port access security and port resource utility but affects online user stability. Set an appropriate secure MAC address aging timer according to your device performance and the network environment.

When a short aging time (less than 60 seconds) works with inactivity aging, do not assign a large value to the maximum number of secure MAC addresses on a port. A large value in this case might affect device performance.

Examples

Set the secure MAC aging timer to 30 minutes.

```
<Sysname> system-view
[Sysname] port-security timer autolearn aging 30
```

Set the secure MAC aging timer to 50 seconds.

```
<Sysname> system-view
[Sysname] port-security timer autolearn aging second 50
```

Related commands

display port-security

port-security mac-address security

port-security timer disableport

Use **port-security timer disableport** to set the silence period during which the port remains disabled.

Use **undo port-security timer disableport** to restore the default.

Syntax

port-security timer disableport *time-value*

undo port-security timer disableport

Default

The port silence period is 20 seconds.

Views

System view

Predefined user roles

network-admin

Parameters

time-value: Specifies the silence period in seconds during which the port remains disabled. The value is in the range of 20 to 300.

Usage guidelines

If you configure the intrusion protection action as disabling the port temporarily, use this command to set the silence period.

Examples

Configure the intrusion protection action on GigabitEthernet 1/0/1 as disabling the port temporarily, and set the port silence period to 30 seconds.

```
<Sysname> system-view
[Sysname] port-security timer disableport 30
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

Related commands

display port-security

port-security intrusion-mode

snmp-agent trap enable port-security

Use **snmp-agent trap enable port-security** to enable SNMP notifications for port security.

Use **undo snmp-agent trap enable port-security** to disable SNMP notifications for port security.

Syntax

snmp-agent trap enable port-security [**address-learned** | **dot1x-failure** | **dot1x-logoff** | **dot1x-logon** | **intrusion** | **mac-auth-failure** | **mac-auth-logoff** | **mac-auth-logon**] *

undo snmp-agent trap enable port-security [**address-learned** | **dot1x-failure** | **dot1x-logoff** | **dot1x-logon** | **intrusion** | **mac-auth-failure** | **mac-auth-logoff** | **mac-auth-logon**] *

Default

All port security SNMP notifications are disabled.

Views

System view

Predefined user roles

network-admin

Parameters

address-learned: Specifies notifications about MAC address learning.

dot1x-failure: Specifies notifications about 802.1X authentication failures.

dot1x-logoff: Specifies notifications about 802.1X user logoffs.

dot1x-logon: Specifies notifications about 802.1X authentication successes.

intrusion: Specifies notifications about illegal frame detection.

mac-auth-failure: Specifies notifications about MAC authentication failures.

mac-auth-logoff: Specifies notifications about MAC authentication user logoffs.

mac-auth-logon: Specifies notifications about MAC authentication successes.

Usage guidelines

To report critical port security events to an NMS, enable SNMP notifications for port security. For port security event notifications to be sent correctly, you must also configure SNMP on the device. For more information about SNMP configuration, see *Network Management and Monitoring Configuration Guide*.

If you do not specify a notification, this command enables all SNMP notifications for port security.

For this command to take effect, make sure the intrusion protection feature is configured.

Examples

Enable SNMP notifications about MAC address learning.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable port-security address-learned
```

Related commands

display port-security

port-security enable