目 录

1 端口安全配置命令

1.1 端口安全配置命令

1.1.1 display port-security

【命令】

display port-security [**interface** *interface-list*] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【参数】

interface *interface-list*：以太网端口列表，表示多个以太网端口。表示方式为 *interface-list* ＝ { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>。其中，*interface-type* 为端口类型，*interface-number* 为端口号。&<1-10>表示前面的参数最多可以输入 10 次。起始端口类型必须和终止端口类型一致，并且终止端口号必须大于起始端口号。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display port-security 命令用来显示端口安全的配置信息、运行情况和统计信息。

需要注意的是，如果不指定参数 **interface** *interface-list*，则显示所有端口的端口安全信息。

相关配置可参考命令 **port-security enable**、**port-security port-mode**、**port-security ntk-mode**、**port-security intrusion-mode**、**port-security max-mac-count**、**port-security mac-address security**、**port-security authorization ignore**、**port-security oui** 和 **port-security trap**。

【举例】

显示所有端口的端口安全状态。

```
<Sysname> display port-security
 Equipment port-security is enabled
 AddressLearn trap is enabled
 Intrusion trap is enabled
 Dot1x logon trap is enabled
 Dot1x logoff trap is enabled
```

```
 Dot1x logfailure trap is enabled
 RALM logon trap is enabled
 RALM logoff trap is enabled
 RALM logfailure trap is enabled
 Disableport Timeout: 20s
 OUI value:
   Index is 1,  OUI value is 000d1a
   Index is 2,  OUI value is 003c12

GigabitEthernet1/0/1 is link-down
    Port mode is userLoginWithOUI
    NeedToKnow mode is NeedToKnowOnly
    Intrusion Portection mode is DisablePort
    Max MAC address number is 50
    Stored MAC address number is 0
    Authorization is ignored
 GigabitEthernet1/0/2 is link-down
    Port mode is noRestriction
    NeedToKnow mode is disabled
    Intrusion mode is NoAction
    Max MAC address number is not configured
    Stored MAC address number is 0
    Authorization is permitted
```

表1-1 display port-security 命令显示信息描述表

字段	描述
Equipment port-security	端口安全的开启状态
AddressLearn trap	端口学习告警的开启状态。若为 enabled，则表示端口学习到新 MAC 地址时发出告警信息
Intrusion trap	入侵检测告警的开启状态。若为 enabled，则表示端口发现非法报文时发出告警信息
Dot1x logon trap	802.1X 认证成功告警的开启状态。若为 enabled，则表示 802.1X 用户认证成功时发出告警信息
Dot1x logoff trap	802. 1x 认证用户下线告警的开启状态。若为 enabled，则表示 802.1X 用户下线时发出告警信息
Dot1x logfailure	802. 1x 认证失败告警的开启状态。若为 enabled，则表示 802.1X 用户认证失败时发出告警信息
RALM logon trap	MAC 地址认证成功告警的开启状态。若为 enabled，则表示 MAC 地址认证成功时发出告警信息
RALM logoff trap	MAC 地址认证用户下线告警的开启状态。若为 enabled，则表示 MAC 地址认证用户下线时发出告警信息
RALM logfailure trap	MAC 地址认证失败告警的开启状态。若为 enabled，则表示 MAC 地址认证用户认证失败时发出告警信息
Disableport Timeout	收到非法报文的端口暂时被关闭的时间，单位为秒
OUI value	允许通过认证的用户的 24 位 OUI 值

字段	描述
Index	OUI 的索引
Port mode	• 端口安全模式，包括以下几种： • autoLearn • macAddressWithRadius • macAddressElseUserLoginSecure • macAddressElseUserLoginSecureExt • secure • userLogin • userLoginSecure • userLoginSecureExt • macAddressOrUserLoginSecure • macAddressOrUserLoginSecureExt • userLoginWithOUI
NeedToKnow mode	Need To Know 模式，包括以下三种： • NeedToKnowOnly：表示仅允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文通过 • NeedToKnowWithBroadcast：允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文或广播地址的报文通过 • NeedToKnowWithMulticast：允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文，广播地址或组播地址的报文通过
Intrusion mode	入侵检测特性模式，包括以下四种： • BlockMacAddress：表示将非法报文的源 MAC 地址加入阻塞 MAC 地址列表中 • DisablePort：表示将收到非法报文的端口永久关闭 • DisablePortTemporarily：表示将收到非法报文的端口暂时关闭一段时间 • NoAction：表示不进行入侵检测处理
Max MAC address number	端口下允许学习的安全 MAC 地址的最大数目
Stored MAC address number	端口下保存的安全 MAC 地址数目
Authorization	服务器的授权信息是否被忽略的情况 • permitted：表示当前端口应用 RADIUS 服务器下发的授权信息 • ignored：表示当前端口不应用 RADIUS 服务器下发的授权信息

1.1.2 display port-security mac-address block

【命令】

display port-security mac-address block [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【参数】

interface *interface-type interface-number*：显示指定端口的阻塞 MAC 地址信息。其中，*interface-type interface-number* 表示端口类型和端口编号。

vlan *vlan-id*：显示指定 VLAN 的阻塞 MAC 地址信息。其中，*vlan-id* 表示 VLAN 编号，取值范围为 1～4094。

count：统计符合条件的阻塞 MAC 地址个数。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display port-security mac-address block 命令用来显示阻塞 MAC 地址信息。

需要注意的是，如果不指定任何参数，则显示所有阻塞 MAC 地址的信息。

相关配置可参考命令 **port-security intrusion-mode**。

【举例】

显示所有阻塞 MAC 地址。

```
<Sysname> display port-security mac-address block
MAC ADDR             From Port                  VLAN ID

 --- On slot 0, no mac address found ---
000f-3d80-0d2d       GigabitEthernet1/0/1              30

--- On slot 4, 1 mac address(es) found ---

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

显示所有阻塞 MAC 地址计数。

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

--- On slot 0, no mac address found ---

--- On slot 4, 1 mac address(es) found ---

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

显示指定 VLAN 中的阻塞 MAC 地址。

```
<Sysname> display port-security mac-address block vlan 30
MAC ADDR             From Port                  VLAN ID

 --- On slot 0, no mac address found ---
000f-3d80-0d2d       GigabitEthernet1/0/1              30
```

```
--- On slot 1, 1 mac address(es) found ---

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

显示指定端口下的阻塞 MAC 地址。

```
<Sysname> display port-security mac-address block interface gigabitethernet1/0/1
MAC ADDR             From Port                  VLAN ID
000f-3d80-0d2d      GigabitEthernet1/0/1               30

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

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

显示指定端口下的在指定 VLAN 中的阻塞 MAC 地址。

```
<Sysname> display port-security mac-address block interface gigabitethernet 1/0/1 vlan 30
MAC ADDR             From Port                  VLAN ID

000f-3d80-0d2d       GigabitEthernet1/0/1               30
--- On slot 1, 1 mac address(es) found ---

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

表1-2 display port-security mac-address block 命令显示信息描述表

字段	描述
MAC ADDR	阻塞 MAC 地址
From Port	阻塞 MAC 地址所在端口
VLAN ID	端口所属 VLAN
2 mac address(es) found	当前阻塞 MAC 地址数目

1.1.3 display port-security mac-address security

【命令】

display port-security mac-address security [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**] [**|** { **begin** | **exclude** | **include** } *regular-expression*]

【视图】

任意视图

【缺省级别】

2：系统级

【参数】

interface *interface-type interface-number*：显示指定端口的安全 MAC 地址信息。其中，*interface-type interface-number* 表示端口类型和端口编号。

vlan *vlan-id*：显示指定 VLAN 的安全 MAC 地址信息。其中，*vlan-id* 表示 VLAN 编号，取值范围为 1～4094。

count：统计符合条件的安全 MAC 地址个数。

|：使用正则表达式对显示信息进行过滤。有关正则表达式的详细介绍，请参见“基础配置指导”中的“CLI”。

begin：从包含指定正则表达式的行开始显示。

exclude：只显示不包含指定正则表达式的行。

include：只显示包含指定正则表达式的行。

regular-expression：表示正则表达式，为 1～256 个字符的字符串，区分大小写。

【描述】

display port-security mac-address security 命令用来显示安全 MAC 地址信息。当端口工作于 autoLearn 模式时，端口上通过自动学习或者静态配置的安全 MAC 地址可通过该命令查看。

需要注意的是，如果不指定任何参数，则显示所有安全 MAC 地址的信息。

相关配置可参考命令 **port-security mac-address security**。

【举例】

显示所有安全 MAC 地址。

```
<Sysname> display port-security mac-address security
MAC ADDR        VLAN ID   STATE          PORT INDEX                      AGING TIME(s)
0002-0002-0002  1         Security       GigabitEthernet1/0/1            NOAGED
000d-88f8-0577  1         Security       GigabitEthernet1/0/1            NOAGED

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

显示所有安全 MAC 地址计数。

```
<Sysname> display port-security mac-address security count
 2 mac address(es) found
```

显示指定 VLAN 中的安全 MAC 地址。

```
<Sysname> display port-security mac-address security vlan 1
MAC ADDR        VLAN ID   STATE          PORT INDEX                      AGING TIME(s)
0002-0002-0002  1         Security       GigabitEthernet1/0/1            NOAGED
000d-88f8-0577  1         Security       GigabitEthernet1/0/1            NOAGED

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

显示指定端口下的安全 MAC 地址。

```
<Sysname> display port-security mac-address security interface gigabitethernet1/0/1
MAC ADDR        VLAN ID   STATE          PORT INDEX                      AGING TIME(s)
000d-88f8-0577  1         Security       GigabitEthernet1/0/1            NOAGED

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

显示指定端口下的在指定 VLAN 中的安全 MAC 地址。

```
<Sysname> display port-security mac-address security interface gigabitethernet 1/0/1 vlan
1
MAC ADDR        VLAN ID   STATE          PORT INDEX                      AGING TIME(s)
000d-88f8-0577  1         Security       GigabitEthernet1/0/1            NOAGED

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

表1-3 display port-security mac-address security 命令显示信息描述表

字段	描述
MAC ADDR	安全 MAC 地址
VLAN ID	端口所属 VLAN
STATE	添加的 MAC 地址类型 • Security：表示该项是安全 MAC 地址
PORT INDEX	安全 MAC 地址所在端口
AGING TIME(s)	安全 MAC 地址的存活时间 • NOAGED：表示该安全 MAC 地址不会被老化
2 mac address(es) found	当前保存的安全 MAC 地址数目

1.1.4 port-security authorization ignore

【命令】

port-security authorization ignore

undo port-security authorization ignore

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

无

【描述】

port-security authorization ignore 命令用来配置端口不应用 RADIUS 服务器下发的授权信息。

undo port-security authorization ignore 命令用来恢复缺省情况。

缺省情况下，端口应用 RADIUS 服务器下发的授权信息。

当用户通过 RADIUS 认证后，RADIUS 服务器会根据用户帐号配置的相关属性进行授权，比如动态下发 VLAN 等。

说明

本命令仅在 SAP 板工作在二层模式时支持。

相关配置可参考命令 **display port-security**。

【举例】

配置端口 GigabitEthernet1/0/1 不应用 RADIUS 服务器下发的授权信息。

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

```
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] port-security authorization ignore
```

1.1.5 port-security enable

【命令】

port-security enable

undo port-security enable

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

无

【描述】

port-security enable 命令用来使能端口安全功能。**undo port-security enable** 命令用来关闭端口安全功能。

缺省情况下，没有使能端口安全功能。

需要注意的是：

(1) 如果已全局开启了 802.1X 或 MAC 地址认证功能，则无法使能端口安全功能。

(2) 端口安全功能使能后，端口的如下配置会被自动恢复为（括弧内的）缺省情况，且以下配置不能再进行手动配置，只能随端口安全模式的改变由系统配置：

- 802.1X 认证（关闭）、端口接入控制方式（**macbased**）、端口接入控制模式（**auto**）；
- MAC 地址认证（关闭）。

(3) 端口安全功能关闭时，端口的如下配置会被自动恢复为（括弧内的）缺省情况：

- 端口安全模式（noRestrictions）；
- 802.1X 认证（关闭）、端口接入控制方式（**macbased**）、端口接入控制模式（**auto**）；
- MAC 地址认证（关闭）。

(4) 端口上有用户在线的情况下，端口安全功能无法关闭。

相关配置可参考命令 **display port-security**、“安全命令参考/802.1X”中的命令 **dot1x**、**dot1x port-method** 和 **dot1x port-control** 以及“安全命令参考/MAC 地址认证”中的命令 **mac-authentication**。

【举例】

使能端口安全功能。

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

1.1.6 port-security intrusion-mode

【命令】

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

undo port-security intrusion-mode

【视图】

二层以太网接口视图

【缺省级别】

2：系统级

【参数】

blockmac：表示将非法报文的源 MAC 地址加入阻塞 MAC 地址列表中，源 MAC 地址为阻塞 MAC 地址的报文将被丢弃，实现在端口上过滤非法流量的作用。此 MAC 地址在被阻塞 3 分钟（系统默认，不可配）后恢复正常。阻塞 MAC 地址列表可以通过 **display port-security mac-address block** 命令查看。

disableport：表示将收到非法报文的端口永久关闭。

disableport-temporarily：表示将收到非法报文的端口暂时关闭一段时间。关闭时长可通过 **port-security timer disableport** 命令配置。

【描述】

port-security intrusion-mode 命令用来配置入侵检测特性，对接收非法报文的端口采取相应的安全策略。**undo port-security intrusion-mode** 命令用来缺省情况。

缺省情况下，不进行入侵检测处理。

需要注意的是，可以通过执行 **undo shutdown** 命令将断开的端口连接恢复。

相关配置可参考命令 **display port-security**、**display port-security mac-address block** 和 **port-security timer disableport**。

说明

本命令仅在 SAP 板工作在二层模式时支持。

【举例】

配置端口 GigabitEthernet1/0/1 的入侵检测特性被触发后，将非法报文的源 MAC 地址置为阻塞 MAC。

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

1.1.7 port-security mac-address security

【命令】

在二层以太网接口视图下：

port-security mac-address security *mac-address* **vlan** *vlan-id*

在系统视图下：

port-security mac-address security *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*]

【视图】

二层以太网接口视图/系统视图

【缺省级别】

2：系统级

【参数】

mac-address：安全 MAC 地址，格式为 H-H-H。

interface *interface-type interface-number*：指定添加安全 MAC 地址的接口。其中，*interface-type interface-number* 表示接口类型和接口编号。

vlan *vlan-id*：指定安全 MAC 地址所属的 VLAN。其中，*vlan-id* 表示 VLAN 编号，取值范围为 1～4094。

【描述】

port-security mac-address security 命令用来添加安全 MAC 地址。**undo port-security mac-address security** 命令用来删除匹配的安全 MAC 地址。

缺省情况下，未配置安全 MAC 地址。

需要注意的是：

- 安全 MAC 地址的接口必须属于安全 MAC 地址所属的 VLAN。
- 此命令只有在端口安全功能打开（使用命令 **port-security enable**）且指定端口的端口安全模式为 autoLearn（使用命令 **port-security port-mode autolearn**）的时候才能配置成功。
- 删除安全 MAC 地址的命令只能在系统视图下执行。

相关配置可参考命令 **display port-security**。

【举例】

启动端口安全功能，配置端口 GigabitEthernet1/0/1 的安全模式为 autoLearn，并在系统视图下为该端口添加一条安全 MAC 地址：0001-0001-0002，该安全 MAC 地址属于 VLAN 10。

```
<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
[Sysname-GigabitEthernet1/0/1] quit
[Sysname] port-security mac-address security 0001-0001-0002 interface gigabitethernet 1/0/1
vlan 10
```

启动端口安全功能，配置端口 GigabitEthernet1/0/1 的安全模式为 autoLearn，并在接口视图下为该端口添加一条安全 MAC 地址：0001-0002-0003，该安全 MAC 地址属于 VLAN 4。

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

1.1.8 port-security max-mac-count

【命令】

port-security max-mac-count *count-value*

undo port-security max-mac-count

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

count-value：端口允许的最大安全 MAC 地址数，取值范围为 1～1024。

【描述】

port-security max-mac-count 命令用来设置端口允许转发的最大安全 MAC 地址数。**undo port-security max-mac-count** 命令用来恢复缺省情况。

缺省情况下，最大安全 MAC 地址数不受限制。

需要注意的是：

- 当端口工作于 autoLearn 模式时，无法更改端口允许的最大安全 MAC 地址数。
- 端口允许的最大安全 MAC 地址数仅包括端口上学习到的以及手工配置的安全 MAC 地址数目。
- 端口允许的最大安全 MAC 地址数不能小于当前端口下已保存的 MAC 地址数。

说明

本命令仅在 SAP 板工作在二层模式时支持。

相关配置可参考命令 **display port-security**。

【举例】

配置端口 GigabitEthernet1/0/1 允许的最大安全 MAC 地址数为 100。

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

1.1.9 port-security ntk-mode

【命令】

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

undo port-security ntk-mode

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

ntk-withbroadcasts：允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文或广播地址的报文通过。

ntk-withmulticasts：允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文，广播地址或组播地址的报文通过。

ntkonly：仅允许目的 MAC 地址为已通过认证的 MAC 地址的单播报文通过。

【描述】

port-security ntk-mode 命令用来配置端口 Need To Know 特性。**undo port-security ntk-mode** 命令用来恢复缺省配置。

缺省情况下，端口没有配置 Need To Know 特性，即所有报文都可成功发送。

Need To Know 特性通过检测从端口发出的数据帧的目的 MAC 地址，保证数据帧只能被发送到已经通过认证的设备上，从而防止非法设备窃听网络数据。

相关配置可参考命令 **display port-security**。

【举例】

配置端口 GigabitEthernet1/0/1 的 Need To Know 特性为 **ntkonly**，即仅发送目的地址为已认证的 MAC 地址的报文。

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

1.1.10 port-security oui

【命令】

port-security oui *oui-value* **index** *index-value*

undo port-security oui index *index-value*

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

oui-value：OUI 值，输入格式为 H-H-H 的 48 位 MAC 地址。系统会自动取输入的前 24 位做为 OUI 值，忽略后 24 位。

index-value：标识此 OUI 的索引值，取值范围为 1～16。

【描述】

port-security oui 命令用来配置用户认证的 OUI 值，在端口安全模式为 userLoginWithOUI 时使用。**undo port-security oui** 命令用来删除指定索引的 OUI 值。

缺省情况下，没有设置用户认证的 OUI 值。

OUI 指的是 MAC 地址的前 24 位（二进制），是 IEEE 为不同设备供应商分配的一个全球唯一的标识符。因此，当需要允许某些特殊设备的报文总是可以通过认证的情况下，就可以通过本命令来指定这些设备的 OUI 值，例如，某公司仅允许 A 厂商的 IP 电话在企业网中使用，则该值就为 A 厂商设备的 OUI。

需要注意的是，本命令设置的 OUI 值，只在端口安全模式为 userLoginWithOUI 时生效。

相关配置可参考命令 **display port-security**。

【举例】

配置 OUI 值为 000d2a，索引为 4。

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

1.1.11 port-security port-mode

【命令】

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

【视图】

以太网接口视图

【缺省级别】

2：系统级

【参数】

表1-4 安全模式的参数解释表

参数	安全模式	说明
autolearn	autoLearn	端口可通过手工配置或自动学习 MAC 地址。这些新的 MAC 地址被称为安全 MAC，并被添加到安全 MAC 地址表中 当端口下的安全 MAC 地址数超过端口允许学习的最大安全 MAC 地址数后，端口模式会自动转变为 secure 模式。之后，该端口停止添加新的安全 MAC，只有源 MAC 地址为安全 MAC 地址、手工配置的 MAC 地址的报文，才能通过该端口
mac-authentication	macAddressWithRadius	对接入用户采用 MAC 地址认证 此模式下，端口允许多个用户接入

参数	安全模式	说明
mac-else-userlogin-secure	macAddressElseUserLoginSecure	端口同时处于 macAddressWithRadius 模式和 userLoginSecure 模式，但 MAC 地址认证优先级大于 802.1X 认证； 非 802.1X 报文直接进行 MAC 地址认证。802.1X 报文先进行 MAC 地址认证，如果 MAC 地址认证失败再进行 802.1X 认证
mac-else-userlogin-secure-ext	macAddressElseUserLoginSecureExt	与 macAddressElseUserLoginSecure 类似，但允许端口下有多个 802.1X 和 MAC 地址认证用户
secure	secure	禁止端口学习 MAC 地址，只有源 MAC 地址为端口上的安全 MAC 地址、手工配置的 MAC 地址的报文，才能通过该端口
userlogin	userLogin	对接入用户采用基于端口的 802.1X 认证 此模式下，端口下的第一个 802.1X 用户认证成功后，其它用户无须认证就可接入
userlogin-secure	userLoginSecure	对接入用户采用基于 MAC 地址的 802.1X 认证 此模式下，端口最多只允许一个 802.1X 认证用户接入
userlogin-secure-ext	userLoginSecureExt	对接入用户采用基于 MAC 的 802.1X 认证，且允许端口下有多个 802.1X 用户
userlogin-secure-or-mac	macAddressOrUserLoginSecure	端口同时处于 userLoginSecure 模式和 macAddressWithRadius 模式 非 802.1X 报文直接进行 MAC 地址认证，802.1X 报文直接进行 802.1X 认证
userlogin-secure-or-mac-ext	macAddressOrUserLoginSecureExt	与 macAddressOrUserLoginSecure 类似，但允许端口下有多个 802.1X 和 MAC 地址认证用户
userlogin-withoui	userLoginWithOUI	与 userLoginSecure 模式类似，但端口上除了允许一个 802.1X 认证用户接入之外，还额外允许一个特殊用户接入，该用户报文的源 MAC 的 OUI 与设备上配置的 OUI 值相符 802.1X 报文进行 802.1X 认证，非 802.1X 报文直接进行 OUI 匹配，802.1X 认证成功和 OUI 匹配成功的报文都允许通过端口；

【描述】

port-security port-mode 命令用来配置端口安全模式。**undo port-security port-mode** 命令用来恢复缺省情况。

缺省情况下，端口处于 noRestrictions 模式，此时该端口下端口安全特性不生效。

- 端口安全模式与端口下的 802.1X 认证使能、端口接入控制方式、端口接入控制模式以及端口下的 MAC 地址认证使能配置互斥。
- 当端口安全已经使能且当前端口安全模式不是 noRestrictions 时，若要改变端口安全模式，必须首先执行 **undo port-security port-mode** 命令恢复端口安全模式为 noRestrictions 模式。
- 配置端口安全 autoLearn 模式时，首先需要通过命令 **port-security max-mac-count** 设置端口允许的最大安全 MAC 地址数。
- 端口上有用户在线的情况下，端口安全模式无法改变。

相关配置可参考命令 **display port-security**。

说明

本命令仅在 SAP 板工作在二层模式时支持。

【举例】

使能端口安全功能，并配置端口 GigabitEthernet1/0/1 的端口安全模式为 secure。

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

将端口 GigabitEthernet1/0/1 的端口安全模式改变为 userLogin。

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

1.1.12 port-security timer disableport

【命令】

port-security timer disableport *time-value*

undo port-security timer disableport

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

time-value：端口静默时间，取值范围为 20～300，单位为秒。

【描述】

port-security timer disableport 命令用来配置系统暂时关闭端口连接的时间。**undo port-security timer disableport** 命令用来恢复缺省情况。

缺省情况下，系统暂时关闭端口连接的时间为 20 秒。

当 **port-security intrusion-mode** 设置为 **disableport-temporarily** 模式时，系统暂时关闭端口连接的时间由该命令配置。

相关配置可参考命令 **display port-security**。

【举例】

配置端口 GigabitEthernet1/0/1 的入侵检测特性被触发后，收到非法报文的端口暂时关闭 30 秒。

```
<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
```

1.1.13 port-security trap

【命令】

port-security trap { **addresslearned** | **dot1xlogfailure** | **dot1xlogoff** | **dot1xlogon** | **intrusion** | **ralmlogfailure** | **ralmlogoff** | **ralmlogon** }

undo port-security trap { **addresslearned** | **dot1xlogfailure** | **dot1xlogoff** | **dot1xlogon** | **intrusion** | **ralmlogfailure** | **ralmlogoff** | **ralmlogon** }

【视图】

系统视图

【缺省级别】

2：系统级

【参数】

addresslearned：端口学习告警。在端口学习到新 MAC 地址时发出告警信息。

dot1xlogfailure：802.1X 认证失败告警。

dot1xlogon：802.1X 认证成功告警。

dot1xlogoff：802.1X 认证用户下线告警。

intrusion：发现非法报文告警。

ralmlogfailure：MAC 地址认证失败告警。

ralmlogoff：MAC 地址认证用户下线告警。

ralmlogon：MAC 地址认证成功告警。

说明

RALM（RADIUS Authenticated Login using MAC-address）是指基于 MAC 地址的 RADIUS 认证。

【描述】

port-security trap 命令用来打开指定告警信息的发送开关。**undo port-security trap** 命令用来关闭指定告警信息的发送开关。

缺省情况下，所有告警信息的发送开关处于关闭状态。

告警信息的发送过程使用了设备的 Trap 特性。Trap 特性是指当端口有特定的数据包（由非法入侵，用户不正常上下线等原因引起）传送时，设备将会发送 Trap 信息，便于用户对这些特殊的行为进行监控。

相关配置可参考命令 **display port-security**。

【举例】

打开端口学习告警信息开关。

```
<Sysname> system-view
[Sysname] port-security trap addresslearned
```