# 目　录

# 1 端口安全

## 1.1 端口安全配置命令

### 1.1.1 display port-security

**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。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

**interface** *interface-type interface-number*：显示指定端口的端口安全相关信息。*interface-type interface-number* 表示端口类型和端口编号。若不指定本参数，则显示所有端口的端口安全信息。

【举例】

# 显示所有端口的端口安全相关状态。

```
<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
   OUI value list        :
    Index :  1          Value : 123401
```

```
Ten-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
```

表1-1 display port-security 命令显示信息描述表

| 字段 | 描述 |
| --- | --- |
| Port security | 端口安全的开启状态 |
| AutoLearn aging time | Sticky MAC地址的老化时间，单位为分钟 |
| Disableport timeout | 收到非法报文的端口暂时被关闭的时间，单位为秒 |
| MAC move | MAC迁移功能的开启状态<br>• 如果 MAC 迁移功能处于开启状态，则显示 Permitted<br>• 如果 MAC 迁移功能处于关闭状态，则显示 Denied |
| Authorization fail | 授权失败后用户的状态，包括下线（Offline）和保持在线（Online）两种类型 |
| NAS-ID profile | 全局引用的 NAS-ID Profile |
| Dot1x-failure trap | 802.1X用户认证失败的告警功能开启状态 |
| Dot1x-logon trap | 802.1X用户认证成功的告警功能开启状态 |
| Dot1x-logoff trap | 802.1X用户认证下线的告警功能开启状态 |
| Intrusion trap | 发现非法报文的告警功能开启状态 |
| Address-learned trap | 端口学习到新MAC地址的告警功能开启状态 |
| Mac-auth-failure trap | MAC地址认证用户认证失败的告警功能开启状态 |
| Mac-auth-logon trap | MAC地址认证用户认证成功的告警功能开启状态 |
| Mac-auth-logoff trap | MAC地址认证用户认证下线的告警功能开启状态 |
| OUI value list | 允许通过认证的用户的24位OUI值 |
| Index | OUI的索引 |
| Value | OUI值 |
| Port mode | 端口安全模式，包括以下几种：<br>• noRestriction<br>• autoLearn<br>• macAddressWithRadius<br>• macAddressElseUserLoginSecure |

| 字段 | 描述 |
| --- | --- |
| | • macAddressElseUserLoginSecureExt<br>• secure<br>• userLogin<br>• userLoginSecure<br>• userLoginSecureExt<br>• macAddressOrUserLoginSecure<br>• macAddressOrUserLoginSecureExt<br>• userLoginWithOUI<br>关于各模式的具体涵义，请参考端口安全配置手册 |
| NeedToKnow mode | Need To Know模式，包括以下几种：<br>• 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<br>• 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<br>• 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<br>• Disabled：表示不进行 NTK 处理 |
| Intrusion protection mode | 入侵检测特性模式，包括以下几种：<br>• BlockMacAddress：表示将非法报文的源 MAC 地址加入阻塞 MAC 地址列表中<br>• DisablePort：表示将收到非法报文的端口永久关闭<br>• DisablePortTemporarily：表示将收到非法报文的端口暂时关闭一段时间<br>• NoAction：表示不进行入侵检测处理 |
| Security MAC address attribute | 安全MAC地址的相关属性 |
| Security MAC address learning mode | 安全MAC地址的学习方式：<br>• Dynamic：动态类型<br>• Sticky：Sticky 类型 |
| Security MAC address aging type | 安全MAC地址的老化方式：<br>• Periodical：按照配置的老化时间间隔进行老化<br>• Inactivity：无流量命中时老化 |
| Max secure MAC addresses | 端口安全允许的最大安全MAC地址数目或上线用户数 |
| Current secure MAC addresses | 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<br>• Permitted：表示当前端口应用 RADIUS 服务器或本地设备下发的授权信息<br>• Ignored：表示当前端口不应用 RADIUS 服务器或本地设备下发的授权信息 |
| NAS-ID profile | 端口下引用的 NAS-ID Profile |

### 1.1.2 display port-security mac-address block

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

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

**interface** *interface-type interface-number*：显示指定端口的阻塞 MAC 地址信息。*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**：显示阻塞 MAC 地址的个数。

【使用指导】

如果不指定任何参数，则显示所有阻塞 MAC 地址的信息。

【举例】

# 显示所有阻塞 MAC 地址。（独立运行模式）

```
<Sysname> display port-security mac-address block
 MAC ADDR           Port                   VLAN ID
 000f-3d80-0d2d     XGE1/0/1               30

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

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

# 显示所有阻塞 MAC 地址计数。（独立运行模式）

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

--- 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 |

| 字段 | 描述 |
| --- | --- |
| Port | 阻塞MAC地址所在端口 |
| VLAN ID | 端口所属VLAN |
| *number* mac address(es) found | 当前阻塞MAC地址数目为*number*个 |

【相关命令】

- **port-security intrusion-mode**

### 1.1.3 display port-security mac-address security

**display port-security mac-address security** 命令用来显示安全 MAC 地址信息。

【命令】

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

【视图】

任意视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【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。

【使用指导】

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。

如果不指定任何参数，则显示所有安全 MAC 地址的信息。

【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
 0002-0002-0002  1        Security      XGE1/0/1                  NOAGED

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

# 显示所有安全 MAC 地址计数。

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

 ---  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<br>• Security：表示该项是安全 MAC 地址 |
| PORT INDEX | 安全MAC地址所在端口 |
| AGING TIME | 安全MAC地址的剩余存活时间<br>• 对于静态 MAC 地址，显示为 NOAGED<br>• 对于 Sticky MAC 地址，显示为具体的剩余存活时间，单位为分钟。缺省情况下为不进行老化，显示为 NOAGED |
| *number* mac address(es) found | 当前保存的安全MAC地址数目为*number*个 |

【相关命令】

- **port-security mac-address security**

## 1.1.4 port-security authorization ignore

**port-security authorization ignore** 命令用来配置端口不应用 RADIUS 服务器或设备本地下发的授权信息。

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

【命令】

**port-security authorization ignore**

**undo port-security authorization ignore**

【缺省情况】

端口应用 RADIUS 服务器或设备本地下发的授权信息。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

当用户通过 RADIUS 认证或本地认证后，RADIUS 服务器或设备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。若不希望接受这类动态下发的属性，则可通过配置本命令来忽略。

【举例】

# 配置端口 Ten-GigabitEthernet1/0/1 不应用 RADIUS 服务器或设备本地下发的授权信息。

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

【相关命令】

- **display port-security**

### 1.1.5 port-security authorization-fail offline

**port-security authorization-fail offline** 命令用来开启授权失败用户下线功能。

**undo port-security authorization-fail offline** 命令用来关闭授权失败用户下线功能。

【命令】

**port-security authorization-fail offline**

**undo port-security authorization-fail offline**

【缺省情况】

授权失败用户下线功能处于关闭状态，即授权失败后用户保持在线。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

如果配置为授权失败用户下线，当下发的授权 ACL 不存在或者 ACL 下发失败时，将强制用户下线。

如果配置为授权失败用户保持在线，当下发的授权 ACL 不存在或者 ACL 下发失败时，用户保持在线，授权 ACL 不生效，设备打印 LOG 信息。

【举例】

# 开启授权失败用户下线功能。

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

【相关命令】

- **display port-security**

### 1.1.6 port-security enable

**port-security enable** 命令用来使能端口安全。

**undo port-security enable** 命令用来关闭端口安全。

【命令】

**port-security enable**

**undo port-security enable**

【缺省情况】

端口安全功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

如果已全局开启了 802.1X 或 MAC 地址认证，则无法使能端口安全。

执行使能或关闭端口安全的命令后，端口上的相关配置将会恢复为如下情况：

- 802.1X 端口接入控制方式恢复为 **macbased**；
- 802.1X 端口的授权状态恢复为 **auto**。

端口上有用户在线的情况下，若关闭端口安全，则在线用户将会下线。

【举例】

# 使能端口安全。

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

【相关命令】

- **display port-security**
- **dot1x**（安全命令参考/802.1X）
- **dot1x port-control**（安全命令参考/802.1X）
- **dot1x port-method**（安全命令参考/802.1X）
- **mac-authentication**（安全命令参考/MAC 地址认证）

### 1.1.7 port-security intrusion-mode

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

**undo port-security intrusion-mode** 命令用来恢复缺省情况。

【命令】

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

**undo port-security intrusion-mode**

【缺省情况】

对接收到非法报文的端口不进行入侵检测处理。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【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。

【使用指导】

可以通过执行 **undo shutdown** 命令重新开启被入侵检测特性临时或永久断开的端口。

【举例】

# 配置端口 Ten-GigabitEthernet1/0/1 的入侵检测特性检测到非法报文后，将非法报文的源 MAC 地址置为阻塞 MAC。

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

【相关命令】

- **display port-security**
- **display port-security mac-address block**
- **port-security timer disableport**

### 1.1.8 port-security mac-address aging-type inactivity

**port-security mac-address aging-type inactivity** 命令用来配置安全 MAC 地址的老化方式为无流量老化。

**undo port-security mac-address aging-type inactivity** 命令用来恢复缺省情况。

【命令】

**port-security mac-address aging-type inactivity**

**undo port-security mac-address aging-type inactivity**

【缺省情况】

安全 MAC 地址按照配置的老化时间进行老化，即在安全 MAC 地址的老化时间到达后立即老化，不论该安全 MAC 地址是否还有流量产生。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

无流量老化方式下，设备会定期检测（检测周期不可配）端口上的安全 MAC 地址是否有流量产生，若某安全 MAC 地址在配置的老化时间内没有任何流量产生，则才会被老化，否则该安全 MAC 地址不会被老化，并在下一个老化周期内重复该检测过程。下一个周期内若还有流量产生则继续保持该安全 MAC 地址的学习状态，该方式可有效避免非法用户通过仿冒合法用户 MAC 地址乘机在合法用户的安全 MAC 地址老化时间到达之后占用端口资源。

此命令仅对于 Sticky MAC 地址以及动态类型的安全 MAC 地址有效。

【举例】

# 配置端口 Ten-GigabitEthernet1/0/1 的安全 MAC 地址的老化方式为无流量老化。

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

【相关命令】

- **display port-security**

### 1.1.9 port-security mac-address dynamic

**port-security mac-address dynamic** 命令用来将 Sticky MAC 地址设置为动态类型的安全 MAC 地址。

**undo port-security mac-address dynamic** 命令用来恢复缺省情况。

【命令】

**port-security mac-address dynamic**

**undo port-security mac-address dynamic**

【缺省情况】

端口学习到的是 Sticky 类型的安全 MAC，它能够被保存在配置文件中，设备重启后也不会丢失。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

动态类型的安全 MAC 地址不会被保存在配置文件中，可通过执行 **display port-security mac-address security** 命令查看到，设备重启之后会丢失。在不希望设备上保存重启之前端口上已有的 Sticky MAC 地址的情况下，可将其设置为动态类型的安全 MAC 地址。

本命令成功执行后，指定端口上的 Sticky MAC 地址会立即被转换为动态类型的安全 MAC 地址，且将不能手工添加 Sticky MAC 地址。之后，若成功执行对应的 **undo** 命令，该端口上的动态类型的安全 MAC 地址会立即转换为 Sticky MAC 地址，且用户可以手工添加 Sticky MAC 地址。

【举例】

# 将端口 Ten-GigabitEthernet1/0/1 上的 Sticky MAC 地址设置为动态类型的安全 MAC 地址。

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

【相关命令】

- **display port-security**
- **display port-security mac-address security**

### 1.1.10 port-security mac-address security

**port-security mac-address security** 命令用来添加安全 MAC 地址。

**undo port-security mac-address security** 命令用来删除指定的安全 MAC 地址。

【命令】

在二层以太网接口视图下：

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

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

在系统视图下：

**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* ]

【缺省情况】

未配置安全 MAC 地址。

【视图】

系统视图

二层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

**sticky**：表示要添加一个可老化的安全 MAC 地址（Sticky MAC 地址）。若不指定本参数，则表示添加的是一个不老化的静态安全 MAC 地址。

*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。

【使用指导】

Sticky MAC 地址的老化时间可通过 **port-security timer autolearn aging** 命令配置。当 Sticky MAC 地址的老化时间到达时，Sticky MAC 地址即被删除。

手工配置添加的安全 MAC 地址在保存配置并设备重启后，不会被删除。因此，可以将网络中一些已知的、固定要接入某端口的主机或设备的 MAC 地址添加为安全 MAC 地址，这样在端口处于 autoLearn 安全模式时，此类源 MAC 地址为安全 MAC 地址的主机或设备的报文将被允许通过指定端口，而且还可避免与其它通过自动方式学习到端口上的 MAC 地址的报文争夺资源而被拒绝接收。

成功添加安全 MAC 地址的前提为：端口安全处于开启状态；端口的端口安全模式为 autoLearn；当前的接口允许指定的 VLAN 通过或已加入该 VLAN，且该 VLAN 已存在。

已添加的安全 MAC 地址，除非首先将其删除，否则不能重复添加或者修改其地址类型，例如已经在某端口上添加了一条安全 MAC 地址 **port-security mac-address security** 1-1-1 **vlan** 10，则不能再添加一条安全 MAC 地址 **port-security mac-address security sticky** 1-1-1 **vlan** 10。

所有的静态安全 MAC 地址均不老化，除非被管理员通过命令行手工删除，或因为配置的改变（端口的安全模式被改变，或端口安全功能被关闭）而被系统自动删除。

【举例】

# 使能端口安全，配置端口 Ten-GigabitEthernet1/0/1 的安全模式为 autoLearn，并指定端口安全允许的最大 MAC 地址数为 100。

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

# 为该端口添加一条 Sticky MAC 地址 0001-0002-0003，该安全 MAC 地址属于 VLAN 4。

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

# 在系统视图下为端口 Ten-GigabitEthernet1/0/1 添加一条安全 MAC 地址 0001-0001-0002，该安全 MAC 地址属于 VLAN 10。

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

【相关命令】

- **display port-security**
- **port-security timer autolearn aging**

### 1.1.11 port-security mac-move permit

**port-security mac-move permit** 命令用来开启允许 MAC 迁移功能。

**undo port-security mac-move permit** 命令用来关闭允许 MAC 迁移功能。

【命令】

**port-security mac-move permit**

**undo port-security mac-move permit**

【缺省情况】

允许 MAC 迁移功能处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【使用指导】

该功能对系统中的所有 802.1X 认证用户和 MAC 地址认证用户生效。

MAC 迁移功能处于关闭状态时，如果用户从某一端口上线成功，则该用户在未从当前端口下线的情况下无法在设备的其它端口上（无论该端口是否与当前端口属于同一 VLAN）发起认证，也无法上线。

MAC 迁移功能处于开启状态时，如果用户从某一端口上线成功，则允许该在线用户在设备的其它端口上（无论该端口是否与当前端口属于同一 VLAN）发起认证。如果该用户在后接入的端口上认证成功，则当前端口会将该用户立即进行下线处理，保证该用户仅在一个端口上处于上线状态。如果服务器在线用户数已达到上限，将无法进行 MAC 地址迁移。

【举例】

# 开启允许 MAC 迁移功能。

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

【相关命令】

- **display port-security**

### 1.1.12 port-security max-mac-count

**port-security max-mac-count** 命令用来设置端口安全允许的最大安全 MAC 地址数。

**undo port-security max-mac-count** 命令用来恢复缺省情况。

【命令】

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

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

【缺省情况】

端口安全不限制本端口可保存的最大安全 MAC 地址数。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

*max-count*：端口允许的最大安全 MAC 地址数，取值范围为 1～4294967295。端口安全允许的最大安全 MAC 地址数不能小于当前端口下已保存的 MAC 地址数。

**vlan** [ *vlan-id-list* ]：指定端口所属 VLAN。*vlan-id-list* 是 VLAN 列表，表示方式为 *vlan-id-list* = { *vlan-id1* [ to *vlan-id2* ] }&<1-10>，*vlan-id* 取值范围为 1～4094，&<1-10>表示前面的参数最多可以重复输入 10 次。*vlan-id2* 的值必须大于或等于 *vlan-id1* 的值。

【使用指导】

对于 autoLearn 安全模式，端口允许的最大安全 MAC 地址数由本命令配置，包括端口上学习到的以及手工配置的安全 MAC 地址数；对于采用 802.1X、MAC 地址认证或者两者组合形式的认证类安全模式，端口允许的最大用户数取本命令配置的值与相应模式下允许认证用户数的最小值。例如，userLoginSecureExt 模式下，端口下所允许的最大安全 MAC 地址数为配置的端口安全允许的最大安全 MAC 地址数与 802.1X 认证所允许的最大用户数的最小值。

当端口工作于 autoLearn 模式时，无法更改端口安全允许的最大安全 MAC 地址数。

当配置 VLAN 内的最大安全 MAC 地址数时，如果指定 *vlan-id*，则表示限制该 VLAN 内的最大安全 MAC 地址数；否则表示限制端口允许通过的每个 VLAN 内的最大安全 MAC 地址数。此功能仅对端口安全的 autolearn 模式生效。

端口允许的 VLAN 内最大安全 MAC 地址数不能小于当前 VLAN 内已保存的 MAC 地址数。

同一 VLAN，后配置的最大安全 MAC 地址数覆盖前面配置的最大安全 MAC 地址数。

【举例】

# 在端口 Ten-GigabitEthernet1/0/1 上配置端口安全允许的最大安全 MAC 地址数为 100。

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

【相关命令】

- **display port-security**

### 1.1.13 port-security nas-id-profile

**port-security nas-id-profile** 命令用来指定全局/端口引用的 NAS-ID Profile。

**undo port-security nas-id-profile** 命令用来恢复缺省情况。

【命令】

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

**undo port-security nas-id-profile**

【缺省情况】

未指定引用的 NAS-ID Profile。

【视图】

系统视图

二层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

*profile-name*：标识指定 VLAN 和 NAS-ID 绑定关系的 Profile 名称，为 1～31 个字符的字符串，不区分大小写。

【使用指导】

本命令引用的 NAS-ID Profile 由命令 **aaa nas-id profile** 配置，具体情况请参考“安全命令参考”中的“AAA”。

NAS-ID Profile 可以在系统视图下或者接口视图下进行配置引用，接口上的配置优先，若接口上没有配置，则使用系统视图下的全局配置。

如果指定了 NAS-ID Profile，则此 Profile 中定义的绑定关系优先使用；如果未指定 NAS-ID Profile 或指定的 Profile 中没有找到匹配的绑定关系，则使用设备名作为 NAS-ID。

【举例】

# 在接口 Ten-GigabitEthernet1/0/1 上指定名为 aaa 的 NAS-ID Profile。

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

# 在系统视图下指定名为 aaa 的 NAS-ID Profile。

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

【相关命令】

- **aaa nas-id profile**（安全命令参考/AAA）

### 1.1.14 port-security ntk-mode

**port-security ntk-mode** 命令用来配置端口 Need To Know 特性。

**undo port-security ntk-mode** 命令用来恢复缺省情况。

【命令】

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

**undo port-security ntk-mode**

【缺省情况】

端口未配置 Need To Know 特性，即所有报文都可成功发送。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【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。

【使用指导】

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。

【举例】

# 配置端口 Ten-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 ten-gigabitethernet 1/0/1
[Sysname-Ten-GigabitEthernet1/0/1] port-security ntk-mode ntkonly
```

【相关命令】

- **display port-security**

### 1.1.15 port-security oui

**port-security oui** 命令用来配置允许通过认证的用户的 OUI 值。

**undo port-security oui** 命令用来删除指定索引的 OUI 值。

【命令】

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

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

【缺省情况】

不存在允许通过认证的用户 OUI 值。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

*index-value*：标识此 OUI 的索引值，取值范围为 1～16。

*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 位作为 OUI 值，忽略后 24 位。

【使用指导】

OUI 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。当需要允许某些厂商的设备（如 IP 电话或打印机）无需认证即可接入网络时，则可以通过本命令来指定这些设备的 OUI 值。

可通过多次执行本命令，配置多个 OUI 值。

配置的 OUI 值只在端口安全模式为 userLoginWithOUI 时生效。在 userLoginWithOUI 模式下，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 地址的 OUI 与设备上配置的某个 OUI 值相符。

【举例】

# 配置一个允许通过认证的用户 OUI 值为 000d2a，索引为 4。

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

【相关命令】

- **display port-security**

## 1.1.16 port-security port-mode

**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。

【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**

【缺省情况】

端口处于 noRestrictions 模式，此时该端口的安全功能关闭，端口处于不受端口安全限制的状态。

【视图】

二层以太网接口视图

【缺省用户角色】

network-admin

mdc-admin

【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。手工配置或自动学习到的MAC地址被称为安全MAC，并被添加到安全MAC地址表中<br>当端口下的安全MAC地址数超过端口安全允许的最大安全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 |

| 参数 | 安全模式 | 说明 |
| --- | --- | --- |
| | | 加新的安全MAC，只有源MAC地址为安全MAC地址、通过命令**mac-address dynamic**或**mac-address static**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<br>此模式下，端口允许多个用户接入 |
| **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。允许端口下一个802.1X认证用户及多个MAC地址认证用户接入<br>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<br>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<br>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，且允许一个802.1X认证用户及多个MAC地址认证用户接入<br>此模式下，802.1X认证优先级大于MAC地址认证：报文首先触发802.1X认证，默认情况下，如果802.1X认证失败再进行MAC地址认证；若开启了端口的MAC地址认证和802.1X认证并行处理功能，则端口配置了802.1X单播触发功能的情况下，当端口收到源MAC地址未知的报文，会向该MAC地址单播发送EAP-Request帧来触发802.1X认证，但不等待802.1X认证处理完成，就同时进行MAC地址认证 |
| **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<br>此模式下，报文首先进行OUI匹配，OUI匹配失败的报文再进行802.1X认证，OUI匹配成功和802.1X认证成功的报文都允许通过端口 |

【使用指导】

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、端口授权状态以及端口下的 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** 设置端口安全允许的最大安全 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。

开启了 MAC 地址认证延迟功能的接口上不建议同时配置端口安全的模式为 **mac-else-userlogin-secure** 或 **mac-else-userlogin-secure-ext**，否则 MAC 地址认证延迟功能不生效。MAC 地址认证延迟功能的具体配置请参见“安全命令参考”中的“MAC 地址认证”。

【举例】

# 使能端口安全，并配置端口 Ten-GigabitEthernet1/0/1 的端口安全模式为 secure。

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

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

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

【相关命令】

- **display port-security**
- **port-security max-mac-count**

## 1.1.17 port-security timer autolearn aging

**port-security timer autolearn aging** 命令用来配置安全 MAC 地址的老化时间。

**undo port-security timer autolearn aging** 命令用来恢复缺省情况。

【命令】

**port-security timer autolearn aging** *time-value*

**undo port-security timer autolearn aging**

【缺省情况】

安全 MAC 地址不会老化。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

*time-value*：安全 MAC 地址的老化时间，取值范围为 0～129600，单位为分钟，取值为 0 表示不会老化。

【使用指导】

安全 MAC 地址的老化时间对所有端口学习到的安全 MAC 地址以及手工添加的 Sticky MAC 地址均有效。

较短的老化时间可提高端口接入的安全性和端口资源的利用率，但也会影响在线用户的在线稳定性，因此需要结合当前的网络环境和设备的性能合理设置老化时间。

【举例】

# 配置安全 MAC 地址的老化时间为 30 分钟。

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

【相关命令】

- **display port-security**
- **port-security mac-address security**

### 1.1.18 port-security timer disableport

**port-security timer disableport** 命令用来配置系统暂时关闭端口的时间。

**undo port-security timer disableport** 命令用来恢复缺省情况。

【命令】

**port-security timer disableport** *time-value*

**undo port-security timer disableport**

【缺省情况】

系统暂时关闭端口的时间为 20 秒。

【视图】

系统视图

【缺省用户角色】

network-admin

mdc-admin

【参数】

*time-value*：端口关闭的时间，取值范围为 20～300，单位为秒。

【使用指导】

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

【举例】

# 配置端口 Ten-GigabitEthernet1/0/1 的入侵检测特性检测到非法报文后，将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 ten-gigabitethernet 1/0/1
```

```
[Sysname-Ten-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily
```

【相关命令】

- **display port-security**
- **port-security intrusion-mode**

### 1.1.19 snmp-agent trap enable port-security

**snmp-agent trap enable port-security** 命令用来开启端口安全告警功能。

**undo snmp-agent trap enable port-security** 命令用来关闭指定的端口安全告警功能。

【命令】

**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** ] *

【缺省情况】

端口安全的所有告警功能均处于关闭状态。

【视图】

系统视图

【缺省用户角色】

network-admin

network-operator

mdc-admin

mdc-operator

【参数】

**address-learned**：表示端口学习到新 MAC 地址时的告警功能。

**dot1x-failure**：表示 802.1X 用户认证失败时的告警功能。

**dot1x-logon**：表示 802.1X 用户认证成功时的告警功能。

**dot1x-logoff**：表示 802.1X 用户认证下线时的告警功能。

**intrusion**：表示发现非法报文时的告警功能。

**mac-auth-failure**：表示 MAC 地址认证用户认证失败时的告警功能。

**mac-auth-logoff**：表示 MAC 地址认证用户认证下线时的告警功能。

**mac-auth-logon**：表示 MAC 地址认证用户认证成功时的告警功能。

【使用指导】

如果不指定任何参数，则表示开启或关闭所有类型的端口安全告警功能。

开启端口安全模块的告警功能后，该模块会生成告警信息，用于报告该模块的重要事件。生成的告警信息将发送到设备的 SNMP 模块，通过设置 SNMP 中告警信息的发送参数，来决定告警信息输出的相关属性。有关告警信息的详细介绍，请参见“网络管理和监控配置指导”中的“SNMP”。

【举例】

# 开启端口学习到新 MAC 地址时的告警功能。

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

【相关命令】

- **display port-security**
- **port-security enable**