交换机如何配置端口安全?

端口安全 樊凡 2019-01-01 发表

组网及说明

端口安全的主要功能是通过定义各种端口安全模式，让设备学习到合法的源MAC地址，以达到相应的网络管理效果。启动了端口安全功能之后，当发现非法报文时，系统将触发相应特性，并按照预先指定的方式进行处理，既方便用户的管理又提高了系统的安全性。 通过配置端口安全autolearn模式，实现对接入用户的控制。端口可通过手工配置或自动学习MAC地址，这些地址将被添加到安全MAC地址表中，称之为安全MAC地址。 当端口下的安全MAC地址数超过端口安全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、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。

问题描述

端口安全autolearn模式典型配置举例

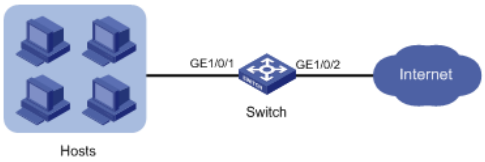
1. 组网需求

如图1所示，用户通过H3C交换机连接到网络。通过配置端口安全autolearn模式，实现对接入用户的控制，具体需求如下：

· 最多同时允许1个用户通过交换机接入到Internet，用户无需进行认证

· 当用户数量超过设定值后，新用户无法通过H3C交换机接入Internet

图1 端口安全autolearn模式配置组网图



过程分析

2. 配置思路

· 配置交换机与用户相连端口的安全模式为autolearn

· 为防止交换机与用户相连端口学习到的MAC地址的丢失，及安全MAC地址不老化会带来一些问题，需配置安全MAC地址并设定安全MAC地址老化时间（例如30分钟）

· 设置最大安全MAC地址数为1，当再有新的MAC地址接入时，交换机与用户相连端口被暂时断开连接，30秒后自动恢复端口的开启状态。(缺省情况下，系统暂时关闭端口连接的时间为20秒)

解决方法

3. 配置步骤

1）使能端口安全功能

<H3C> system-view

[H3C] port-security enable

2）设置Sticky MAC地址的老化时间为30分钟

[H3C] port-security timer autolearn aging 30

3）设置端口允许的最大安全MAC地址数为1

[H3C] interface GigabitEthernet 1/0/1

[H3C-GigabitEthernet1/0/1] port-security max-mac-count 1

4）设置端口安全模式为autoLearn

[H3C-GigabitEthernet1/0/1] port-security port-mode autolearn

5）设置触发入侵检测特性后的保护动作为暂时关闭端口，关闭时间为30秒

[H3C-GigabitEthernet1/0/1] port-security intrusion-mode disableport-temporarily

[H3C-GigabitEthernet1/0/1] quit

[H3C] port-security timer disableport 30

4. 验证配置

上述配置完成后，当学习到的MAC地址数达到1个后，用命令display port-security interface可以看到端口模式变为secure，再有新的MAC地址到达将触发入侵保护，可以用display命令显示端口安全配置情况，如下：

[H3C]display port-security interface gigabitethernet 1/0/1

```
Global port security parameters:
  Port security          : Enabled
  AutoLearn aging time   : 30 min
  Disableport timeout    : 30 s
  MAC move               : Denied
  Authorization fail     : Online
  NAS-ID profile         : Not configured
  Dot1x-failure trap     : Disabled
  Dot1x-logon trap       : Disabled
  Dot1x-logoff trap      : Disabled
  Intrusion trap         : Disabled
  Address-learned trap   : Disabled
  Mac-auth-failure trap  : Disabled
  Mac-auth-logon trap    : Disabled
  Mac-auth-logoff trap   : Disabled
  OUI value list         :

 GigabitEthernet1/0/1 is link-up
  Port mode                    : secure
  NeedToKnow mode              : Disabled
  Intrusion protection mode    : DisablePortTemporarily
  Security MAC address attribute
     Learning mode             : Sticky
     Aging type                : Periodical
  Max secure MAC addresses     : 1
  Current secure MAC addresses : 1
  Authorization                : Permitted
  NAS-ID profile               : Not configured
```

可以看到端口的最大安全MAC数为1,口模式为autoLearn，入侵保护动作为DisablePortTemporarily，入侵发生后端口禁用时间为30秒，学习到的MAC地址数可以用上述命令显示，如学习到1，那么存储的安全MAC地址数就为1

可以在端口视图下用display this命令查看学习到的MAC地址，如下：

```
[H3C-GigabitEthernet1/0/1]dis this
#
interface GigabitEthernet1/0/1
 port link-mode bridge
 combo enable copper
 port-security intrusion-mode disableport-temporarily
 port-security max-mac-count 1
 port-security port-mode autolearn
 port-security mac-address security sticky 1435-83d6-0306 vlan 1
#
```

当学习到的MAC地址数达到1个后，可以通过下述命令看到端口安全将此端口关闭

```
<H3C> display interface gigabitethernet 1/0/1
 gigabitEthernet1/0/1 current state: DOWN（ Port Security Disabled ）
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 0023-8927-ad7d
 Description: GigabitEthernet1/0/1 Interface .....
```

30秒后，端口状态恢复

```
[H3C-GigabitEthernet1/0/1] display interface gigabitethernet 1/0/1
 GigabitEthernet1/0/1 current state: UP
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-cb00-5558
 Description: GigabitEthernet1/0/1 Interface
 .....
```

此时，如通过命令undo port-security mac-address security手动删除几条安全MAC地址后，端口安全的状态重新恢复为autoLearn，可以继续学习MAC地址