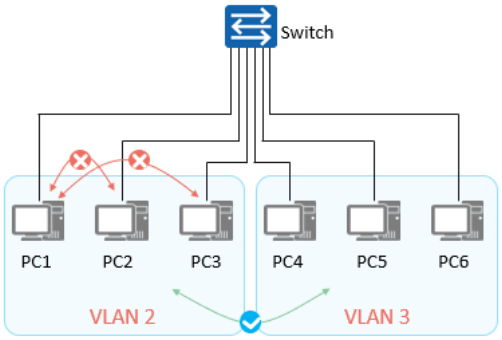
以太网交换安全

- 目前网络中以太网技术的应用非常广泛。然而，各种网络攻击的存在（例如针对 ARP、DHCP 等协议的攻击），不仅造成了网络合法用户无法正常访问网络资源，而且对网络信息安全构成严重威胁，因此以太网交换的安全性越来越重要。
- 本章节主要介绍常见的以太网交换安全技术，包括端口隔离、端口安全、MAC 地址漂移检测、风暴控制、端口限速、MAC 地址表安全、DHCP Snooping 及 IP Source Guard 等常见技术，以提高对以太网交换安全的理解和认识。

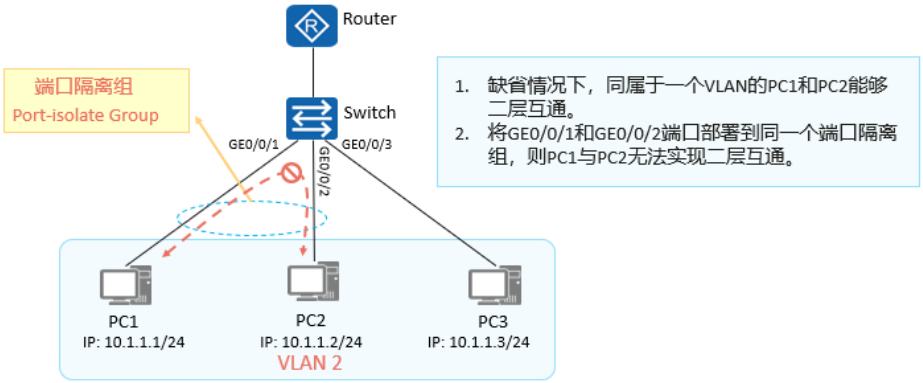
端口隔离技术背景

- 以太交换网络中为了实现报文之间的二层隔离，用户通常将不同的端口加入不同的VLAN，实现二层广播域的隔离。
- 大型网络中，业务需求种类繁多，只通过VLAN实现报文二层隔离，会浪费有限的VLAN资源。
- 如下图所示，由于某种业务需求，PC1与PC2虽然属于同一个VLAN ，但是要求它们在二层不能互通（但允许三层互通），PC1与PC3在任何情况下都不能互通，但是VLAN 3里的主机可以访问VLAN 2里的主机。 那么该如何解决这个问题呢?

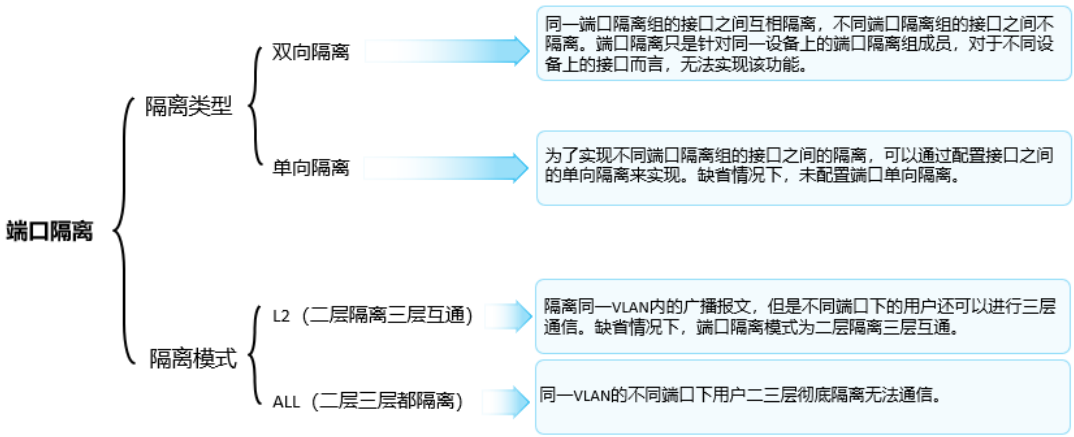


端口隔离技术概述

采用端口隔离功能，可以实现同一VLAN内端口之间的隔离。用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间二层数据的隔离。端口隔离功能为用户提供了更安全、更灵活的组网方案。



端口隔离技术原理



- 采用二层隔离三层互通的隔离模式时，在 VLANIF 接口上使能 VLAN 内 Proxy ARP 功能，配置 arp-proxy inner-sub-vlan-proxy enable，可以实现同一 VLAN 内主机通信。

端口隔离配置命令

1. 使能端口隔离功能

```
[Huawei-GigabitEthernet0/0/1] port-isolate enable [ group group-id ]
```

缺省情况下，未使能端口隔离功能。如果不指定*group-id*参数时，默认加入的端口隔离组为1。

2. (可选) 配置端口隔离模式

```
[Huawei] port-isolate mode { l2 | all }
```

缺省情况下，端口隔离模式为L2。

L2 端口隔离模式为二层隔离三层互通。

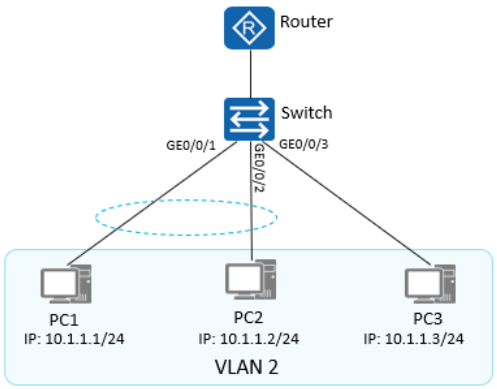
all 端口隔离模式为二层三层都隔离。

3. 配置端口单向隔离

```
[Huawei-GigabitEthernet0/0/1] am isolate {interface-type interface-number }&<1-8>
```

am isolate命令用来配置当前接口与指定接口的单向隔离。在接口A上配置与接口B之间单向隔离后，接口A发送的报文不能到达接口B，但从接口B发送的报文可以到达接口A。缺省情况下，未配置端口单向隔离。

端口隔离配置举例



如图所示：PC1、PC2和PC3属于VLAN 2，通过配置端口隔离，使PC3可以与PC1、PC2通信，但是PC1和PC2之间无法通信。

Switch配置如下：

```
[Switch] vlan 2
[Switch] port-isolate mode all
[Switch] interface GigabitEthernet 0/0/1
[Switch-GigabitEthernet0/0/1] port link-type access
[Switch-GigabitEthernet0/0/1] port default vlan 2
[Switch-GigabitEthernet0/0/1] port-isolate enable group 2
[Switch] interface GigabitEthernet 0/0/2
[Switch-GigabitEthernet0/0/2] port link-type access
[Switch-GigabitEthernet0/0/2] port default vlan 2
[Switch-GigabitEthernet0/0/2] port-isolate enable group 2
[Switch] interface GigabitEthernet 0/0/3
[Switch-GigabitEthernet0/0/3] port link-type access
[Switch-GigabitEthernet0/0/3] port default vlan 2
```

- display port-isolate group { group-id | all }，查看端口隔离组的配置。
- clear configuration port-isolate 命令一键式清除设备上所有的端口隔离配置。
- port-isolate exclude vlan 命令配置端口隔离功能生效时排除的 VLAN。

端口隔离配置验证

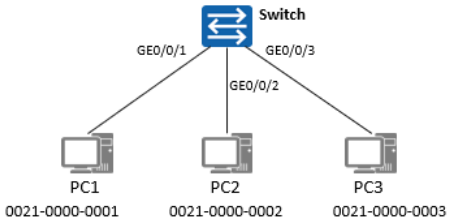
1.通过display port-isolate group *group-number*查看端口隔离组中的端口。

```
[SW]display port-isolate group 2
 The ports in isolate group 2:
GigabitEthernet0/0/1    GigabitEthernet0/0/2
```

2. 验证同一端口隔离组下主机网络不能互通。

```
PC1>ping 10.1.1.2
Ping 10.1.1.2: 32 data bytes, Press Ctrl_C to break
From 10.1.1.1: Destination host unreachable
From 10.1.1.1: Destination host unreachable
From 10.1.1.1: Destination host unreachable
From 10.1.1.1: Destination host unreachable
From 10.1.1.1: Destination host unreachable
--- 10.1.1.2 ping statistics ---
 5 packet(s) transmitted
 0 packet(s) received
 100.00% packet loss
```

MAC地址表项类型



[Switch]display mac-address

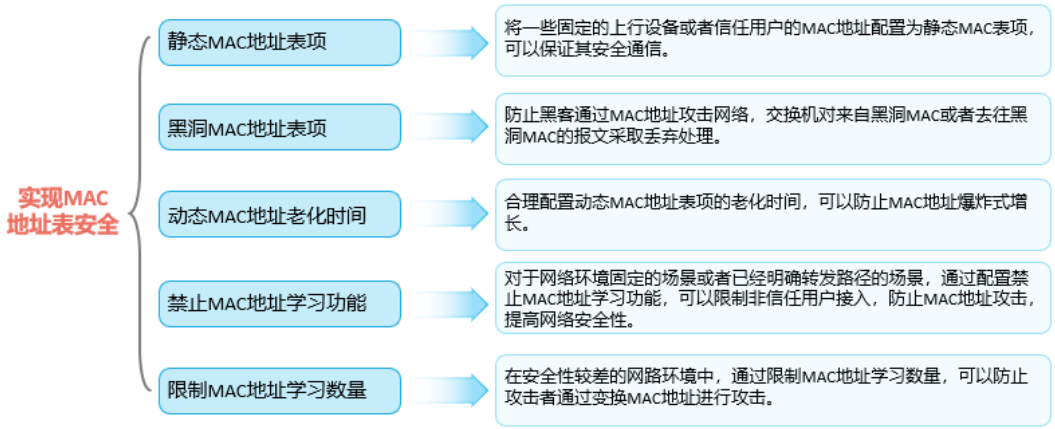
MAC地址	VLAN	接口	TYPE
0021-0000-0001	10	GE0/0/1	Static
0021-0000-0002	10	GE0/0/2	Blackhole
0021-0000-0003	10	GE0/0/3	Dynamic

MAC地址表项类型包括：

- **动态MAC地址表项**：由接口通过报文中的源MAC地址学习获得，表项可老化。在系统复位、接口板热插拔或接口板复位后，动态表项会丢失。
- **静态MAC地址表项**：由用户手工配置并下发到各接口板，表项不老化。在系统复位、接口板热插拔或接口板复位后，保存的表项不会丢失。接口和MAC地址静态绑定后，其他接口收到源MAC是该MAC地址的报文将会被丢弃。
- **黑洞MAC地址表项**：由用户手工配置，并下发到各接口板，表项不可老化。配置黑洞MAC地址后，源MAC地址或目的MAC地址是该MAC的报文将会被丢弃。

- MAC 地址表记录了交换机学习到的 MAC 地址与接口的对应关系，以及接口所属 VLAN 等信息。
- 设备在执行二层交换操作时，根据报文的目的 MAC 地址查询 MAC 地址表，如果 MAC 地址表中包含与报文目的 MAC 地址对应的表项，并且收到该报文的接口与对应的表项的接口不相同时，则直接通过该表项中的出接口转发该报文；如果相同，则丢弃该报文。
- 如果 MAC 地址表中没有包含报文目的 MAC 地址对应的表项时，设备将采取广播方式在所属 VLAN 内除接收接口外的所有接口转发该报文。

MAC地址表安全功能



- 为了防止一些关键设备（如各种服务器或上行设备）被非法用户恶意修改其 MAC 地址表项，可将这些设备的 MAC 地址配置为静态 MAC 地址表项，因为静态 MAC 地址表项优先于动态 MAC 地址表项，不易被非法修改。
- 为了防止无用 MAC 地址表项占用 MAC 地址表，同时为了防止黑客通过 MAC 地址攻击用户设备或网络，可将那些有着恶意历史的非信任 MAC 地址配置为黑洞 MAC 地址，使设备在收到目的 MAC 或源 MAC 地址为这些黑洞 MAC 地址的报文时，直接予以丢弃，不修改原有的 MAC 地址表项，也不增加新的 MAC 地址表项。
- 为了减轻手工配置静态 MAC 地址表项，华为 S 系列交换机缺省已使能了动态 MAC 地址表项学习功能。但为了避免 MAC 地址表项爆炸式增长，可合理配置动态 MAC 表项的老化时间，以便及时删除 MAC 地址表中的废弃 MAC 地址表项。
- 为了提高网络的安全性，防止设备学习到非法的 MAC 地址，错误地修改 MAC 地址表中的原 MAC 地址表项，可以选择关闭设备上指定接口或指定 VLAN 中所有接口的 MAC 地址学习功能，这样设备将不再从这些接口上学习新的 MAC 地址。
- 配置限制 MAC 地址学习数，当超过限制数时不再学习 M

AC 地址，同时可以配置当 MAC 地址数达到限制后对报文采取的动作，从而防止 MAC 地址表资源耗尽，提高网络安全性。

MAC地址表项配置

1. 配置静态MAC表项

   [Huawei] **mac-address static** *mac-address interface-type interface-number* **vlan** *vlan-id*

   指定的VLAN必须已经创建并且已经加入绑定的端口；指定的MAC地址，必须是单播MAC地址，不能是组播和广播MAC地址。

2. 配置黑洞MAC表项

   [Huawei] **mac-address blackhole** *mac-address* **[vlan** *vlan-id* **]**

   当设备收到目的MAC或源MAC地址为黑洞MAC地址的报文，直接丢弃。

3. 配置动态MAC表项的老化时间

   [Huawei] **mac-address aging-time** *aging-time*

禁止MAC地址学习功能

1. 关闭基于接口的MAC地址学习功能

   [Huawei-GigabitEthernet0/0/1] **mac-address learning disable [action { discard | forward }]**

   缺省情况下，接口的MAC地址学习功能是使能的：
   - 关闭MAC地址学习功能的缺省动作为forward，即对报文进行转发。
   - 当配置动作为discard时，会对报文的源MAC地址进行匹配，当接口和MAC地址与MAC地址表项匹配时，则对该报文进行转发。当接口和MAC地址与MAC地址表项不匹配时，则丢弃该报文。

2. 关闭基于VLAN的MAC地址学习功能

   [Huawei-vlan2] **mac-address learning disable**

   缺省情况下，VLAN的MAC地址学习功能是使能的。
   当同时配置基于接口和基于VLAN的禁止MAC地址学习功能时，基于VLAN的优先级要高于基于接口的优先级配置。

限制MAC地址学习数量

1. 配置基于接口限制MAC地址学习数

   [Huawei-GigabitEthernet0/0/1] **mac-limit maximum** *max-num*

   缺省情况下，不限制MAC地址学习数。

2. 配置当MAC地址数达到限制后，对报文应采取的动作

   [Huawei-GigabitEthernet0/0/1] **mac-limit action { discard | forward }**

   缺省情况下，对超过MAC地址学习数限制的报文采取丢弃动作。

3. 配置当MAC地址数达到限制后是否进行告警

   [Huawei-GigabitEthernet0/0/1] **mac-limit alarm { disable | enable }**

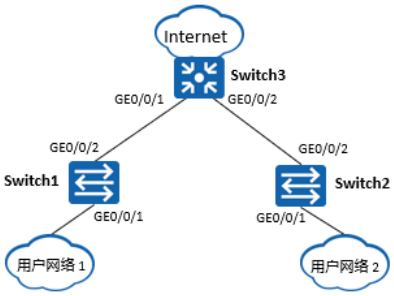
   缺省情况下，对超过MAC地址学习数限制的报文进行告警。

4. 配置基于VLAN限制MAC地址学习数

   [Huawei-vlan2] **mac-limit maximum** *max-num*

   缺省情况下，不限制MAC地址学习数。

MAC地址表安全配置举例



实验要求：

- 网络拓扑基本配置已完成，用户网络1属于VLAN 10，用户网络2属于VLAN 20。
- 在Switch3上配置禁止学习来自用户网络1的MAC地址。
- 在Switch3上配置限制用户网络2的MAC地址学习数量。

Switch3的配置如下：

配置方式一：在接口视图下配置

```
# 在接口GE0/0/1上配置禁止MAC地址学习
[Switch3-GigabitEthernet0/0/1] mac-address learning disable action
discard
#在接口GE0/0/2上配置限制MAC地址学习数量，超过阈值策略及告警
[Switch3-GigabitEthernet0/0/2] mac-limit maximum 100
[Switch3-GigabitEthernet0/0/2] mac-limit alarm enable
[Switch3-GigabitEthernet0/0/2] mac-limit action discard
```

配置方式二：在VLAN视图下配置

```
# 在VLAN 10上配置禁止MAC地址学习
[Switch3-vlan10] mac-address learning disable
#在VLAN 20上配置限制MAC地址学习数量与告警
[Switch3-vlan20] mac-limit maximum 100 alarm enable
```

配置验证

执行display mac-limit命令，查看MAC地址学习限制规则是否配置成功。

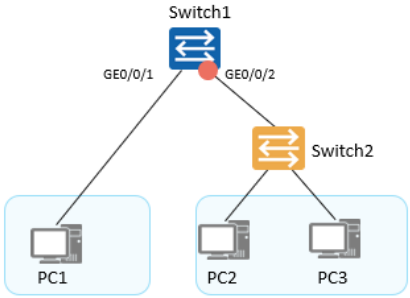
```
[Switch3]display mac-limit
MAC Limit is enabled
Total MAC Limit rule count : 2

PORT          VLAN/VSI/SI    SLOT  Maximum  Rate(ms)       Action       Alarm
------------------------------------------------------------------------------
GE0/0/2       -              -     100      -      forward    enable
-             20             -     100      -      forward    enable
```

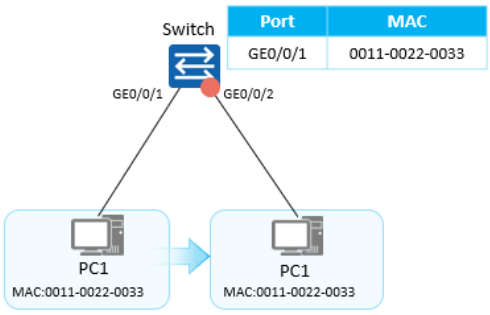
基于VLAN的MAC地址学习限制

基于接口的MAC地址学习限制

端口安全技术背景

- 企业要求接入层交换机上每个连接终端设备的接口均只允许一台PC接入网络（限制MAC地址接入数量）。如果有员工试图在某个接口下级联一台小交换机或集线器从而扩展上网接口，那么这种行为应该被发现或被禁止，如左图所示。
- 另一些企业还可能会要求只有MAC地址为可信任的终端发送的数据帧才允许被交换机转发到上层网络，员工不能私自更换位置（变更交换机的接入端口），如右图所示。
- 通过交换机的端口安全（port security）特性可以解决这些问题。





端口安全概述

- 通过在交换机的特定接口上部署端口安全，可以限制接口的 MAC 地址学习数量，并且配置出现越限时的惩罚措施。
- 端口安全通过将接口学习到的动态 MAC 地址转换为安全 MAC 地址（包括安全动态 MAC，安全静态 MAC 和 Sticky MAC），阻止非法用户通过本接口和交换机通信，从而增强设备的安全性。

端口安全技术原理

- 安全MAC地址分为以下类型：

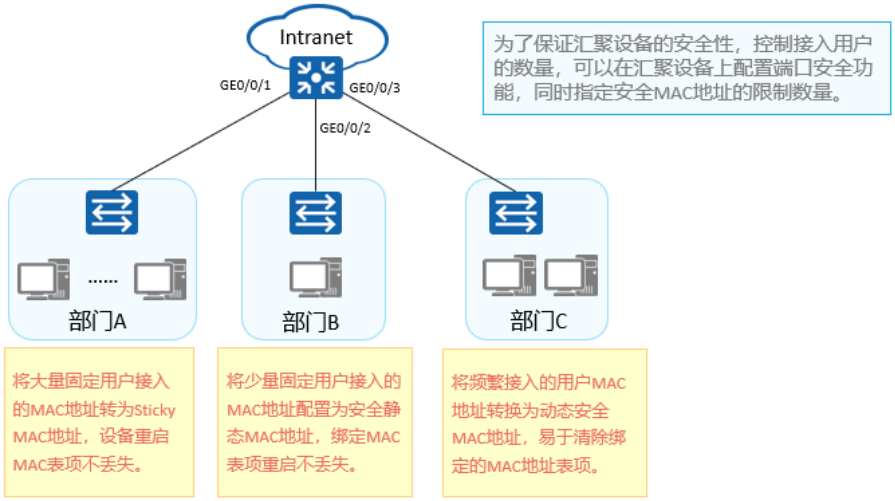
类型	定义	特点
安全动态MAC地址	使能端口安全而未使能Sticky MAC功能时转换的MAC地址。	设备重启后表项会丢失，需要重新学习。缺省情况下不会被老化，只有在配置安全MAC的老化时间后才可以被老化。
安全静态MAC地址	使能端口安全时手工配置的静态MAC地址。	不会被老化，手动保存配置后重启设备不会丢失。
Sticky MAC地址	使能端口安全后又同时使能Sticky MAC功能后转换到的MAC地址。	不会被老化，手动保存配置后重启设备不会丢失。

- 安全MAC地址通常与安全保护动作结合使用，常见的安全保护动作有：
  - Restrict：丢弃源MAC地址不存在的报文并上报告警。
  - Protect：只丢弃源MAC地址不存在的报文，不上报告警。
  - Shutdown：接口状态被置为error-down，并上报告警。

- 安全动态 MAC 地址的老化类型分为：绝对时间老化和相对时间老化。
- 如设置绝对老化时间为 5 分钟：系统每隔 1 分钟计算一次每个 MAC 的存在时间，若大于等于 5 分钟，则立即将该安全动态 MAC 地址老化。否则，等待下 1 分钟再检测计算。
- 如设置相对老化时间为 5 分钟：系统每隔 1 分钟检测一次是否有该 MAC 的流量。若没有流量，则经过 5 分钟后将该安全动态 MAC 地址老化。
- 默认情况下，接口关闭（error-down）后不会自动恢复，只能由网络管理人员在接口视图下使用 restart 命令重启接口进行恢复。
- 如果用户希望被关闭的接口可以自动恢复，则可在接口 error-down 前通过在系统视图下执行 error-down auto-recovery cause port-security interval interval-value 命令使能接口状态自动恢复为 Up 的功能，并设置接口自动恢复为 Up 的延时时间，使被关闭的接口经过延时时间后能够自动恢复。
- 当端口安全功能或者 Sticky MAC 功能使能/去使能时，接口上的 MAC 地址变化如下：
- 端口安全功能

- 使能之后，接口上之前学习到的动态 MAC 地址表项将被删除，之后学习到的 MAC 地址将变为安全动态 MAC 地址。
- 去使能之后，接口上的安全动态 MAC 地址将被删除，重新学习动态 MAC 地址。
- Sticky MAC 功能
- 使能之后，接口上的安全动态 MAC 地址表项将转化为 Sticky MAC 地址，之后学习到的 MAC 地址也变为 Sticky MAC 地址。
- 去使能之后，接口上的 Sticky MAC 地址，会转换为安全动态 MAC 地址。

端口安全技术应用



- 在对接入用户的安全性要求较高的网络中，可以配置端口安全功能及端口安全动态 MAC 学习的限制数量。此时接口学习到的 MAC 地址会被转换为安全 MAC 地址，接口学习的最大 MAC 数量达到上限后不再学习新的 MAC 地址，仅允许这些 MAC 地址和交换机通信。而且接口上安全 MAC 地址数达到限制后，如果收到源 MAC 地址不存在的报文，无论目的 MAC 地址是否存在，交换机即认为有非法用户攻击，就会根

据配置的动作对接口做保护处理。这样可以阻止其他非信任用户通过本接口和交换机通信，提高交换机与网络的安全性。

- 配置端口安全功能后，接口学习到的 MAC 地址会转换为安全 MAC 地址，接口学习的最大 MAC 数量达到上限后不再学习新的 MAC 地址，仅允许这些 MAC 地址和交换机通信。如果接入用户发生变动，可以通过设备重启或者配置安全 MAC 老化时间刷新 MAC 地址表项。对于相对比较稳定的接入用户，如果不希望后续发生变化，可以进一步使能接口 Sticky MAC 功能，这样在保存配置之后，MAC 地址表项不会刷新或者丢失。

端口安全配置命令

1. 使能端口安全功能

   ```
   [Huawei-GigabitEthernet0/0/1] port-security enable
   ```

   缺省情况下，未使能端口安全功能。

2. 配置端口安全动态MAC学习限制数量

   ```
   [Huawei-GigabitEthernet0/0/1] port-security max-mac-num max-number
   ```

   缺省情况下，接口学习的安全MAC地址限制数量为1。

3. (可选) 手工配置安全静态MAC地址表项

   ```
   [Huawei-GigabitEthernet0/0/1] port-security mac-address mac-address vlan vlan-id
   ```

4. (可选) 配置端口安全保护动作

   ```
   [Huawei-GigabitEthernet0/0/1] port-security protect-action { protect | restrict | shutdown }
   ```

   缺省情况下，端口安全保护动作为restrict。

- port-security protect-action 命令用来配置端口安全功能中接口学习到的 MAC 地址数超过限制或出现静态 MAC 地址漂移时的保护动作。
- protect
- 当学习到的 MAC 地址数超过接口限制数时，接口将丢弃源地址在 MAC 表以外的报文。
- 当出现静态 MAC 地址漂移时，接口将丢弃带有该 MAC 地址的报文。
- restrict
- 当学习到的 MAC 地址数超过接口限制数时，接口将丢弃

源地址在 MAC 表以外的报文，同时发出告警。

- 当出现静态 MAC 地址漂移时，接口将丢弃带有该 MAC 地址的报文，同时发出告警。
- shutdown
- 当学习到的 MAC 地址数超过接口限制数时，接口将执行 error down 操作，同时发出告警。
- 当出现静态 MAC 地址漂移时，接口将执行 error down 操作，同时发出告警。

端口安全配置命令

5. (可选) 配置接口学习到的安全动态MAC地址的老化时间

   [Huawei-GigabitEthernet0/0/1] **port-security aging-time** *time* [**type** { **absolute** | **inactivity** }]

   缺省情况下，接口学习的安全动态MAC地址不老化。

6. 使能接口Sticky MAC功能

   [Huawei-GigabitEthernet0/0/1] **port-security mac-address sticky**

   缺省情况下，接口未使能Sticky MAC功能。

7. 配置接口Sticky MAC学习限制数量。

   [Huawei-GigabitEthernet0/0/1] **port-security max-mac-num** *max-number*

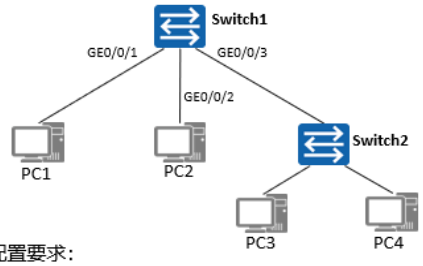
   使能接口Sticky MAC功能后，缺省情况下，接口学习的MAC地址限制数量为1。

8. (可选) 手动配置一条sticky-mac表项

   [Huawei-GigabitEthernet0/0/1] **port-security mac-address sticky** *mac-address* **vlan** *vlan-id*

- 查看安全 MAC 地址：
- 执行命令 display mac-address security [vlan vlan-id | interface-type interface-number] * [verbose]，查看安全动态 MAC 表项。
- 执行命令 display mac-address sec-config [vlan vlan-id | interface-type interface-number] * [verbose]，查看配置的安全静态 MAC 表项。
- 执行命令 display mac-address sticky [vlan vlan-id | interface-type interface-number] * [verbose]，查看 Sticky MAC 表项。

端口安全配置举例 - 安全动态MAC



- 配置要求：
  - 在Switch1上部署端口安全。
  - GE0/0/1及GE0/0/2接口将学习MAC地址的数量限制为1。当该接口连接多台PC时，Switch1需发出告警，且要求此时接口依然能正常转发合法PC的数据帧。
  - GE0/0/3接口将学习MAC地址的数量限制为2，并且当学习到的MAC地址数超出接口限制数时，交换机需发出告警，并且将接口关闭。

Switch1配置如下：

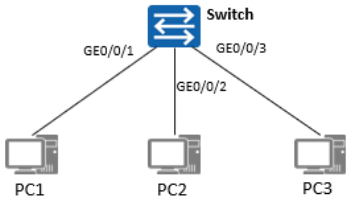
```
[Switch1] interface GigabitEthernet 0/0/1
[Switch1-GigabitEthernet 0/0/1] port-security enable
[Switch1-GigabitEthernet 0/0/1] port-security max-mac-num 1
[Switch1-GigabitEthernet 0/0/1] port-security protect-action restrict
[Switch1] interface GigabitEthernet 0/0/2
[Switch1-GigabitEthernet 0/0/2] port-security enable
[Switch1-GigabitEthernet 0/0/2] port-security max-mac-num 1
[Switch1-GigabitEthernet 0/0/2] port-security protect-action restrict
[Switch1] interface GigabitEthernet 0/0/3
[Switch1-GigabitEthernet 0/0/3] port-security enable
[Switch1-GigabitEthernet 0/0/3] port-security max-mac-num 2
[Switch1-GigabitEthernet 0/0/3] port-security protect-action shutdown
```

配置验证

执行命令display mac-address security ， 查看动态安全MAC表项。

```
[Switch1]display mac-address security
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/      PEVLAN CEVLAN Port          Type              LSP/LSR-ID
               VSI/SI                                                   MAC-Tunnel
-------------------------------------------------------------------------------
5489-98ac-71a9 1          -      -      GE0/0/3       security          -
5489-98b1-7b30 1          -      -      GE0/0/1       security          -
5489-9815-662b 1          -      -      GE0/0/2       security          -
-------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 3
```

端口安全配置举例 - Sticky MAC



Switch配置如下：

```
[Switch] interface GigabitEthernet 0/0/1
[Switch-GigabitEthernet 0/0/1] port-security enable
[Switch-GigabitEthernet 0/0/1] port-security max-mac-num 1
[Switch-GigabitEthernet 0/0/1] port-security mac-address sticky
[Switch] interface GigabitEthernet 0/0/2
[Switch-GigabitEthernet 0/0/2] port-security enable
[Switch-GigabitEthernet 0/0/2] port-security max-mac-num 1
[Switch-GigabitEthernet 0/0/2] port-security mac-address sticky
[Switch] interface GigabitEthernet 0/0/3
[Switch-GigabitEthernet 0/0/3] port-security enable
[Switch-GigabitEthernet 0/0/3] port-security max-mac-num 1
[Switch-GigabitEthernet 0/0/3] port-security mac-address sticky
[Switch-GigabitEthernet 0/0/3] port-security mac-address sticky 5489-98ac-71a9 vlan 1
```

- 配置要求：
  - 在Switch上部署端口安全。将GE0/0/1~G0/0/3都激活端口安全。
  - GE0/0/1及GE0/0/2接口都将学习MAC地址的数量限制为1，并将在这两个接口上学习到的动态安全MAC地址转换为Sticky MAC地址。
  - 对于GE0/0/3将学习MAC地址的数量限制为1，但是通过手工的方式为该接口创建一个sticky MAC地址表项，将该接口与MAC地址5489-98ac-71a9绑定。各接口违例惩罚保持缺省。

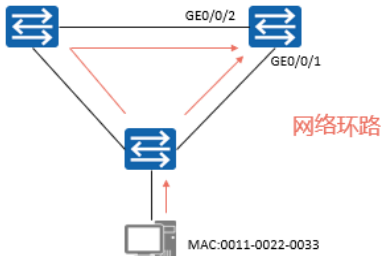
配置验证

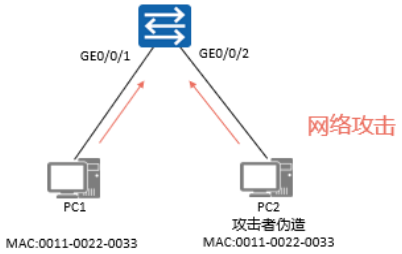
执行命令display mac-address sticky，查看Sticky MAC表项。

```
[Switch1]display mac-address sticky
MAC address table of slot 0:
-------------------------------------------------------------------------------
MAC Address    VLAN/      PEVLAN CEVLAN  Port        Type     LSP/LSR-ID
               VSI/SI                                         MAC-Tunnel
-------------------------------------------------------------------------------
5489-98ac-71a9 1          -      -       GE0/0/3     sticky   -
5489-98b1-7b30 1          -      -       GE0/0/1     sticky                -
5489-9815-662b 1          -      -       GE0/0/2     sticky   -
-------------------------------------------------------------------------------
Total matching items on slot 0 displayed = 3
```

MAC地址漂移概述

- MAC地址漂移是指交换机上一个VLAN内有两个端口学习到同一个MAC地址，后学习到的MAC地址表项覆盖原MAC地址表项的现象。
- 当一个MAC地址在两个端口之间频繁发生迁移时，即会产生MAC地址漂移现象。
- 正常情况下，网络中不会在短时间内出现大量MAC地址漂移的情况。出现这种现象一般都意味着网络中存在环路，或者存在网络攻击行为。



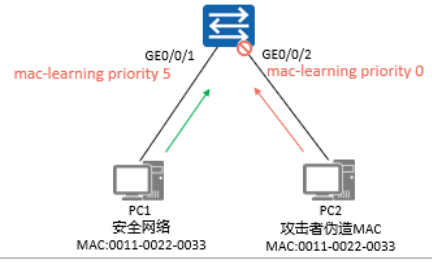


防止MAC地址漂移

如果是环路引发MAC地址漂移，治本的方法是部署防环技术，例如STP，消除二层环路。如果由于网络攻击等其他原因引起，则可使用如下MAC地址防漂移特性：

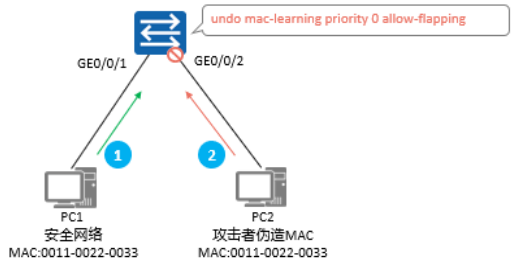
配置接口MAC地址学习优先级

当MAC地址在交换机的两个接口之间发生漂移时，可以将其中一个接口的MAC地址学习优先级提高。高优先级的接口学习到的MAC地址表项将覆盖低优先级接口学习到的MAC地址表项。



配置不允许相同优先级接口MAC地址漂移

当伪造网络设备所连接口的MAC地址优先级与安全的网络设备相同时，后学习到的伪造网络设备MAC地址表项不会覆盖之前正确的表项。



- 缺省时接口 MAC 地址学习的优先级均为 0，数值越大优先级越高。当同一个 MAC 地址被两个个接口学习到后，接口 MAC 地址学习优先级高的会被保留，MAC 地址学习优先级低的被覆盖。
- 在配置不允许相同优先级接口 MAC 地址漂移时，如果安全网络设备下电，则交换机仍会学习到伪造网络设备的 MAC 地址，当网络设备再次上电时将无法学习到正确的 MAC 地址。因此该特性需谨慎使用，如果交换机的接口连接的网络设备是服务器，当服务器下电后，另外的接口学习到与服务器相同的

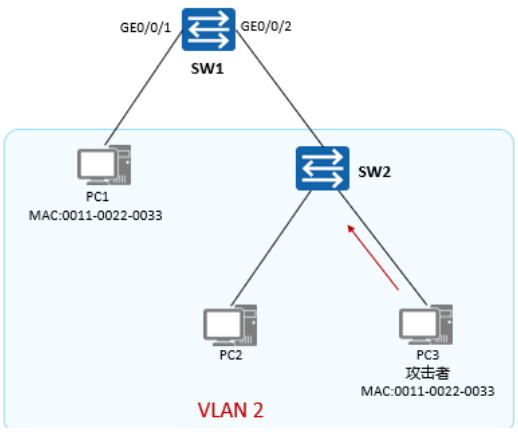
MAC 地址，当服务器再次上电后就不能学习到正确的 MAC 地址。

MAC 地址漂移检测

交换机支持 MAC 地址漂移检测机制，分为以下两种方式：

- 基于 VLAN 的 MAC 地址漂移检测
- 配置 VLAN 的 MAC 地址漂移检测功能可以检测指定 VLAN 下的所有的 MAC 地址是否发生漂移。
- 当 MAC 地址发生漂移后，可以配置指定的动作，例如告警、阻断接口或阻断 MAC 地址。
- 全局 MAC 地址漂移检测
- 该功能可以检测设备上的所有的 MAC 地址是否发生了漂移。
- 若发生漂移，设备会上报告警到网管系统。
- 用户也可以指定发生漂移后的处理动作，例如将接口关闭或退出 VLAN。

基于VLAN的MAC地址漂移检测



在配置基于VLAN的MAC地址漂移检测功能后，如果MAC地址发生漂移时，则可根据需求配置接口做出的动作有以下三种：

1. 发送告警，当检测到MAC地址发生漂移时只给网管发送告警。
2. 接口阻断，当检测到MAC地址发生漂移时，根据设置的阻塞时间对接口进行阻塞，并关闭接口收发报文的能力。
3. MAC地址阻断，当检测到MAC地址发生漂移时，只阻塞当前MAC地址，而不对物理接口进行阻塞，当前接口下的其他MAC的通信不受影响。

- MAC 地址发生漂移后的三种动作在上图中分别表示为：

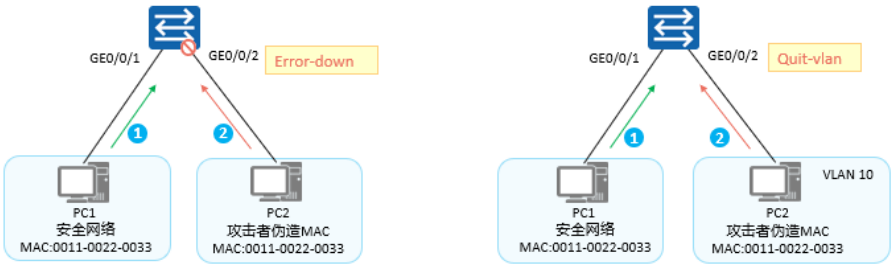
1.产生并上报告警；2.阻断 SW1 上的 GE0/0/2 接口的收发报文的能力；3.阻断 SW1 上的 GE0/0/2 接口上针对指定 MAC 地址报文的收发能力。

- 当配置接口阻塞时：
- 检测到 VLAN2 内产生 MAC 地址漂移时，将产生漂移后的接口直接阻塞。
- 接口将被阻塞 10 秒（该时长使用 block-time 关键字指定），接口被阻塞时是无法正常收发数据的。
- 10 秒之后接口会被放开并重新进行检测，此时该接口可以正常收发数据，如果 20 秒内没有再检测到 MAC 地址漂移，则接口的阻塞将被彻底解除；而如果 20 秒内再次检测到 MAC 地址漂移，则再次将该接口阻塞，如此重复 2 次（该次数使用 retry-times 关键字指定），如果交换机依然能检测到该接口发生 MAC 地址漂移，则永久阻塞该接口。

全局MAC地址漂移检测

当交换机检测到MAC地址漂移，在缺省情况下，它只是简单地上报告警，并不会采取其他动作。在实际网络部署中，可以根据网络需求，对检测到MAC地址漂移之后定义以下动作：

- error-down
  - 当配置了MAC地址漂移检测的端口检测到有MAC地址漂移时，将对应接口状态置为error-down，不再转发数据。
- quit-vlan
  - 当配置了MAC地址漂移检测的端口检测到有MAC地址漂移时，将退出当前接口所属的VLAN。



- 华为交换机默认开启全局 MAC 地址漂移检测功能，因此缺省时交换机便会对设备上的所有 VLAN 进行 MAC 地址漂移检测。
- 在某些场景下，需要对某些 VLAN 不进行 MAC 地址漂移

检测，可以通过配置 MAC 地址漂移检测的 VLAN 白名单来实现。

- 如果接口由于发生了 MAC 地址漂移从而被设置为 Error-Down，默认情况下是不会自动恢复的。
- 如果希望 Error-Down 的接口能够自动恢复，在系统视图下配置如下命令：

error-down auto-recovery cause mac-address-flapping interval *time-value*

- 如果接口由于发生了 MAC 地址漂移，被设置为离开 VLAN，如要实现接口自动恢复，可以在系统视图下配置如下命令：

mac-address flapping quit-vlan recover-time time-value

MAC地址漂移配置命令介绍 (1)

1. 配置接口学习MAC地址的优先级

   [Huawei-GigabitEthernet0/0/1] **mac-learning priority** *priority-id*

   缺省情况下，接口学习MAC地址的优先级为0，数值越大优先级越高。

2. 配置禁止MAC地址漂移时报文的处理动作为丢弃

   [Huawei-GigabitEthernet0/0/1] **mac-learning priority flapping-defend action discard**

   缺省情况下，禁止MAC地址漂移时报文的处理动作是转发。

3. 配置不允许相同优先级的接口发生MAC地址漂移

   [Huawei] **undo mac-learning priority** *priority-id* **allow-flapping**

   缺省情况下，允许相同优先级的接口发生MAC地址漂移。

4. 配置MAC地址漂移检测功能。

   [Huawei-vlan2] **mac-address flapping detection**

   缺省情况下，已经配置了对交换机上所有VLAN进行MAC地址漂移检测的功能。

MAC地址漂移配置命令介绍 (2)

1. (可选) 配置MAC地址漂移检测的VLAN白名单

```
[Huawei] mac-address flapping detection exclude vlan { vlan-id1 [ to vlan-id2 ] } &<1-10>
```

缺省情况下，没有配置MAC地址漂移检测的VLAN白名单。

2. (可选) 配置发生漂移后接口的处理动作

```
[Huawei-GigabitEthernet0/0/1] mac-address flapping action { quit-vlan | error-down }
```

缺省情况下，对超过MAC地址学习数限制的报文采取丢弃动作。

3. (可选) 配置MAC地址漂移表项的老化时间

```
[Huawei] mac-address flapping aging-time aging-time
```

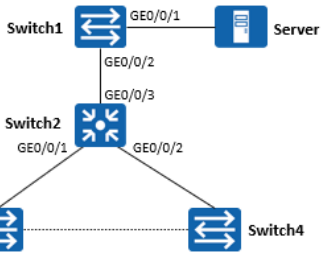
缺省情况下，MAC地址漂移表项的老化时间为300秒。

4. 配置MAC地址漂移检测功能

```
[Huawei-vlan2] loop-detect eth-loop { [ block-mac ] block-time block-time retry-times retry-times | alarm-only }
```

- 一些安全性较差的网络容易受到黑客的 MAC 地址攻击，由于 MAC 地址表的容量是有限的，当黑客伪造大量源 MAC 地址不同的报文并发送给交换机后，交换机的 MAC 表项资源就可能被耗尽。当 MAC 表被填满后，即使它再收到正常的报文，也无法学习到报文中的源 MAC 地址。
- 配置限制 MAC 地址学习数，当超过限制数时不再学习 MAC 地址，同时可以配置当 MAC 地址数达到限制后对报文采取的动作，从而防止 MAC 地址表资源耗尽，提高网络安全性。

MAC地址漂移配置举例



实验介绍：

- 网络基础配置已完成，Switch3与Switch4之间误接网线导致网络出现环路；
- 在Switch1的接口GE0/0/1上配置MAC地址防漂移功能，防止被非法用户攻击；
- 在Switch2上配置MAC地址漂移检测功能，判断网络中存在的环路，排除故障。

1.在Switch1与Server相连的接口GE0/0/1上配置MAC地址学习优先级高于其他接口，此优先级默认值为0。

```
[Switch1] interface GigabitEthernet 0/0/1
[Switch1-GigabitEthernet 0/0/1] mac-leaning priority 3
```

2.在Switch2上配置MAC地址漂移检测功能，并配置接口MAC地址漂移后的处理动作。

```
[Switch2] mac-address flapping detection
[Switch2] mac-address flapping aging-time 500
[Switch2-GigabitEthernet0/0/1] mac-address flapping action error-down
[Switch2-GigabitEthernet0/0/2] mac-address flapping action error-down
[Switch2] error-down auto-recovery cause mac-address-flapping interval 500
```

- 当 Switch3 与 Switch4 之间误连接之后，Switch2 的接口

GE0/0/1 的 MAC 地址漂移到接口 GE0/0/2 后，触发接口 error-down，接口 GE0/0/2 关闭。

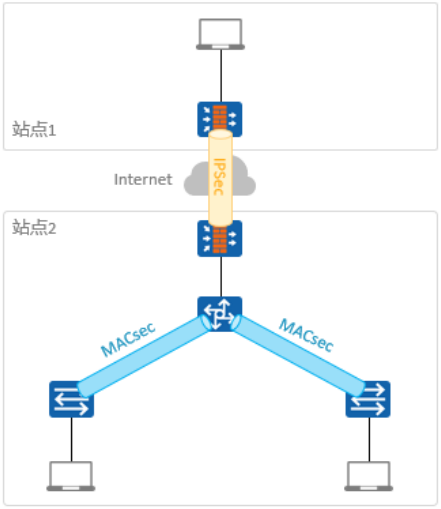
- 使用 display mac-address flapping record 可查看到漂移记录。

配置验证

配置完成后，当Switch2的接口GE0/0/1的MAC地址漂移到接口GE0/0/2后，接口GE0/0/2关闭；使用display mac-address flapping record可查看到漂移记录。

```
[Switch2] display mac-address flapping record
 S : start time
 E : end time
(Q) : quit vlan
(D) : error down
--------------------------------------------------------------------------------
Move-Time           VLAN MAC-Address    Original-Port   Move-Ports   MoveNum
--------------------------------------------------------------------------------
S:2020-06-22 17:22:36   1   5489-9815-662b  GE0/0/1      GE0/0/2(D)   83
E:2020-06-22 17:22:44
--------------------------------------------------------------------------------
Total items on slot 0: 1
```

MACsec，提供二层数据安全传输



背景

绝大部分数据在局域网链路中都是以明文形式传输的，在某些安全性要求较高的场景下存在安全隐患。

MACsec概述

MACsec定义了基于以太网的数据安全通信的方法，通过逐跳设备之间数据加密，保证数据传输安全性，对应的标准为802.1AE。

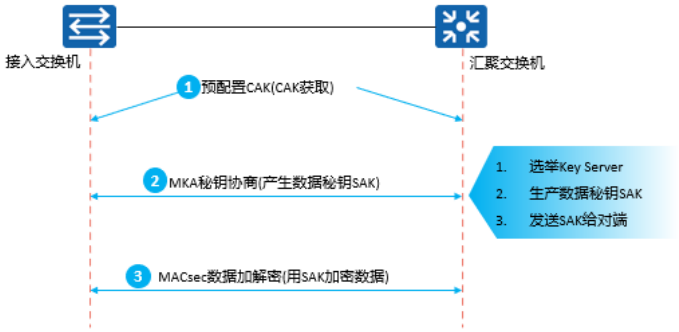
数据帧完整性检查 | 用户数据加密 | 数据源真实性校验 | 重放保护

典型应用场景

- 在交换机之间部署MACsec保护数据安全，例如在接入交换机与上联的汇聚或核心交换机之间部署。
- 当交换机之间存在传输设备时可部署MACsec保护数据安全。

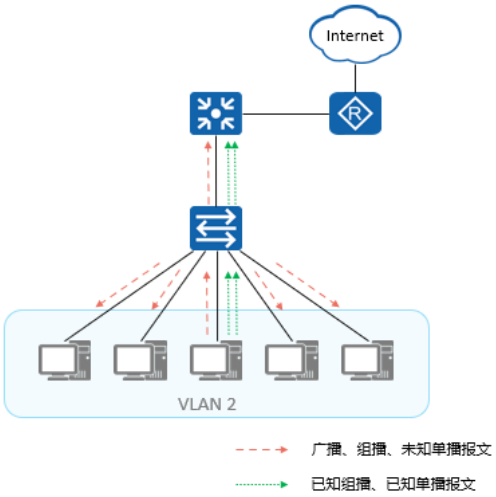
MACsec工作机制

在设备运行点到点MACsec时，网络管理员在两台设备上通过命令行预配置相同的CAK，两台设备会通过MKA协议选举出一个Key Server，Key Server决定加密方案，Key Server会根据CAK等参数使用某种加密算法生成SAK数据密钥，由Key Server将SAK分发给对端设备，这样两台设备拥有相同的SAK数据密钥，可以进行后续MACsec数据报文加解密收发。



- CAK（Secure Connectivity Association Key，安全连接关联密钥）不直接用于数据报文的加密，由它和其他参数派生出数据报文的加密密钥。CAK 可以在 802.1X 认证过程中下发，也可以由用户直接静态配置。
- MKA（MACsec Key Agreement protocol）用于 MACsec 数据加密密钥的协商协议。
- SAK（Secure Association Key，安全关联密钥）由 CAK 根据算法推导产生，用于加密安全通道间传输的数据。MKA 对每一个 SAK 可加密的报文数目有所限制，当使用某 SAK 加密的 PN 耗尽，该 SAK 会被刷新。例如，在 10Gbps 的链路上，SAK 最快 4.8 分钟刷新一次。
- Key Server 决定加密方案和进行密钥分发的 MKA 实体。

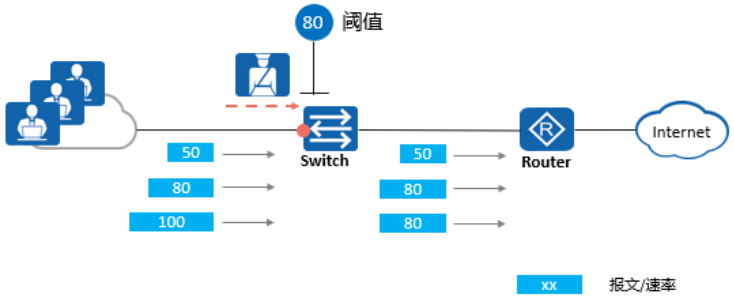
流量抑制概述



- **网络中存在的问题：**
  - 正常情况下，当设备某个二层以太接口收到广播、未知组播或未知单播报文时，会向同一VLAN内的其他二层以太接口转发这些报文，从而导致流量泛洪，降低设备转发性能。
  - 当设备某个以太接口收到已知组播或已知单播报文时，如果某种报文流量过大则可能会对设备造成冲击，影响其他业务的正常处理。
- **可用的解决方案：**
  - 流量抑制可以通过配置阈值来限制广播、未知组播、未知单播、已知组播和已知单播报文的速率，防止广播、未知组播报文和未知单播报文产生流量泛洪，阻止已知组播报文和已知单播报文的大流量冲击。

流量抑制工作原理 (1)

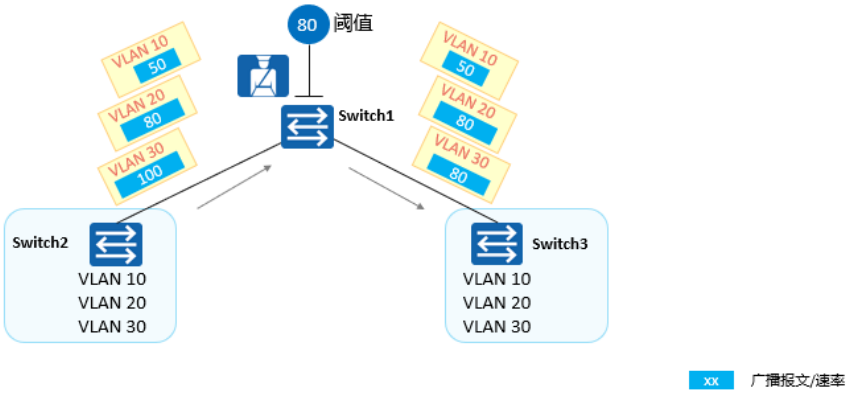
在接口入方向上，设备支持对广播、未知组播、未知单播、已知组播和已知单播报文按百分比、包速率和比特速率进行流量抑制。设备监控接口下的各类报文速率并和配置的阈值相比较，当入口流量超过配置的阈值时，设备会丢弃超额的流量。



- 在接口出方向上，设备支持对广播、未知组播和未知单播报文的阻塞（Block）。

流量抑制工作原理 (2)

在VLAN视图下，设备支持对广播报文按比特速率进行流量抑制。设备监控同一VLAN内广播报文的速率并和配置的阈值相比较，当VLAN内流量超过配置的阈值时，设备会丢弃超额的流量。



- 流量抑制还可以通过配置阈值的方式对 ICMP 报文进行限速，防止大量 ICMP 报文上送 CPU 处理，导致其他业务功能异常。

流量抑制的应用

流量抑制通过对不同类型的报文采取不同的限制措施，达到限制报文发送速率的目的。具体实施可分为以下三种情况：

1. 在交换机接口的入方向，例如下图中SW1的GE0/0/1入方向，通过流量抑制功能可以限制任意报文的发送速率。
2. 在交换机接口出方向，例如下图中SW1的GE0/0/1出方向，通过流量抑制功能可以阻塞广播，未知组播和未知单播报文。
3. 在交换机的VLAN视图下，通过配置VLAN 内流量抑制限制VLAN内广播报文。

- 流量抑制中，可以为接口入方向的报文流量配置阈值，当流量超过阈值时，系统将丢弃多余的流量，阈值范围内的报文可以正常通过，从而将流量限制在合理的范围内。
- 此外，流量抑制还支持对接口出方向的流量进行阻塞。
- 风暴控制中，只可以为接口入方向的报文流量配置阈值。当流量超过阈值时，系统会阻塞该接口收到的该类型报文流量或者直接将该接口关闭。

流量抑制配置命令介绍

1. (可选) 配置流量抑制模式

```
[Huawei] suppression mode { by-packets | by-bits }
```

缺省情况下，缺省的抑制模式为packets，在bits模式下，流量抑制的粒度更小、抑制更精确。

2. 配置流量抑制

```
[Huawei-GigabitEthernet0/0/1] { broadcast-suppression | multicast-suppression | unicast-suppression} { percent-value | cir cir-value [ cbs cbs-value ] | packets packets-per-second }
```

接口下配置流量抑制时，抑制模式需与全局的流量抑制模式保持一致。

3. 配置在接口出方向上阻塞报文

```
[Huawei-GigabitEthernet0/0/1] { broadcast-suppression | multicast-suppression | unicast-suppression } block outbound
```

4. 配置VLAN的广播抑制速率

```
[Huawei-vlan2] broadcast-suppression threshold-value
```

- display flow-suppression interface interface-type interface-number 查看流量抑制配置信息。
- 当在接口视图下的入方向和 VLAN 视图下同时配置流量抑制功能时，接口视图的配置优先于 VLAN 视图下的配置。

流量抑制配置举例

配置要求：

- 在GE0/0/1接口视图下配置流量抑制功能，限制二层网络转发的广播、未知组播和未知单播报文的能力。
- 配置广播流量抑制，按百分比抑制，百分比值为60%。
- 配置未知组播流量抑制，按百分比抑制，百分比值为70%。
- 配置未知单播流量抑制，按百分比抑制，百分比值为80%。

Switch配置如下：

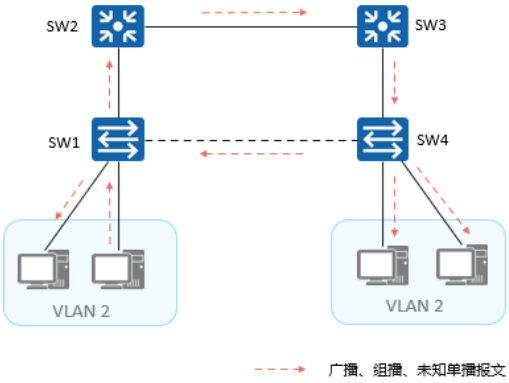
```
[Switch]suppression mode by-packets
[Switch-GigabitEthernet0/0/1] unicast-suppression 80
[Switch-GigabitEthernet0/0/1] multicast-suppression 70
[Switch-GigabitEthernet0/0/1] broadcast-suppression 60
```

配置验证

使用命令display flow-suppression interface 查看流量抑制配置信息。

```
[Switch]dis flow-suppression interface GigabitEthernet 0/0/1
 storm type            rate mode            set rate value
-------------------------------------------------------------------------------
 unknown-unicast       percent              percent: 80%
 multicast             percent              percent: 70%
 broadcast             percent              percent: 60%
-------------------------------------------------------------------------------
```

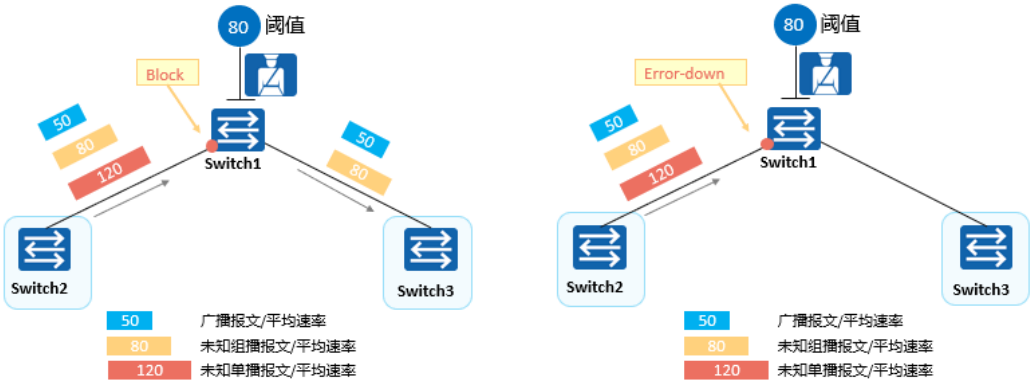
风暴控制概述



- **网络中存在的问题：**
  - 正常情况下，当设备某个二层以太接口收到广播、未知组播或未知单播报文时，会向同一VLAN内的其他二层以太接口转发这些报文，如果网络存在环路，则会导致广播风暴，严重降低设备转发性能。
- **可用的解决方案：**
  - 风暴控制可以通过阻塞报文或关闭端口来阻断广播、未知组播和未知单播报文的流量。

风暴控制工作原理

风暴控制可以用来防止广播、未知组播以及未知单播报文产生广播风暴。在风暴控制检测时间间隔内，设备监控接口下接收的三类报文的包平均速率与配置的最大阈值相比较。当报文速率大于配置的最大阈值时，风暴控制将根据配置的动作来对接口进行阻塞报文或关闭接口的处理。



- 流量抑制与风暴控制的主要区别是：风暴控制功能可以

对端口下发惩罚动作（block 和 shutdown），而流量抑制功能只是对端口流量进行限制。

风暴控制的应用

- 风暴控制与流量抑制相比的优势是可以同时监控接口下的广播报文、未知组播报文和未知单播报文各自的包平均速率，并根据阈值对接口采取阻塞相关报文或者关闭物理接口的惩罚动作。
- 本例中，Switch作为二层网络到路由器的衔接点，当需要限制二层网络转发过来的用户广播、未知组播和未知单播报文时，可以通过在Switch的GE0/0/1上配置风暴控制功能来实现。

- 流量抑制中，可以为接口入方向的报文流量配置阈值。当流量超过阈值时，系统将丢弃多余的流量，阈值范围内的报文可以正常通过，从而将流量限制在合理的范围内。此外，流量抑制还支持对接口出方向的流量进行阻塞。
- 风暴控制中，只可以为接口入方向的报文流量配置阈值。当流量超过阈值时，系统会阻塞该接口收到的该类型报文流量或者直接将该接口关闭。

风暴控制配置命令介绍

1. 配置接口对报文的风暴控制

   [Huawei-GigabitEthernet0/0/1] **storm-control { broadcast | multicast | unicast } min-rate** *min-rate-value* **max-rate** *max-rate-value*

   对接口上的广播、未知组播或未知单播报文进行风暴控制。
2. 配置风暴控制的动作

   [Huawei-GigabitEthernet0/0/1] **storm-control action { block | error-down }**
3. 配置风暴控制的检测时间间隔

   [Huawei-GigabitEthernet0/0/1] **storm-control interval** *interval-value*
4. 配置使能接口状态自动恢复

   [Huawei-GigabitEthernet0/0/1] **error-down auto-recovery cause storm-control interval** *interval-value*

   使能接口状态自动恢复为Up的功能，并设置接口自动恢复为Up的延时时间。
5. （可选）配置流量抑制及风暴控制白名单

   [Huawei] **storm-control whitelist protocol { arp-request | bpdu | dhcp | igmp | ospf }***

- display storm-control [interface interface-type interface-number]，查看接口的风暴控制信息。

- **min-rate** *min-rate-value*
- 指定包模式低阈值。如果指定了 *min-rate-value* 参数（单位 pps），在风暴控制检测时间间隔内，当接口接收报文的平均速率小于该值时，则将该接口的报文恢复到正常转发状态。
- **min-rate cir** *min-rate-value-cir*
- 指定字节模式低阈值。如果指定了 *min-rate-value-cir* 参数（单位 kbps），在风暴控制检测时间间隔内，当接口接收报文的平均速率小于该值时，则将该接口的报文恢复到正常转发状态。
- **min-rate percent** *min-rate-value-percent*
- 指定百分比模式低阈值。如果指定了 *min-rate-value-percent* 参数（百分比），在风暴控制检测时间间隔内，当接口接收报文的平均速率小于该值时，则将该接口的报文恢复到正常转发状态。
- **max-rate** *max-rate-value*
- 指定包模式高阈值。如果指定了 *max-rate-value* 参数（单位 pps），在风暴控制检测时间间隔内，当接口接收报文的平均速率大于该值时，则对该接口进行风暴控制。
- **max-rate cir** *max-rate-value-cir*
- 指定字节模式高阈值。如果指定了 *max-rate-value-cir* 参数（单位 kbps），在风暴控制检测时间间隔内，当接口接收报文的平均速率大于该值时，则对该接口进行风暴控制。
- **max-rate percent** *max-rate-value-percent*
- 指定百分比模式高阈值。如果指定了 *max-rate-value-percent* 参数，在风暴控制检测时间间隔内，当接口接收报文的平均速率大于该值时，则对该接口进行风暴控制。

风暴控制配置举例

- 配置需求
  - 在交换机Switch上需要配置防止二层网络转发的广播、未知组播和未知单播报文产生的广播风暴。
- 配置思路：
  - 通过在接口GE0/0/1上配置风暴控制限制二层网络的广播风暴的产生。

Switch配置如下：

```
[Switch] storm-control whitelist protocol arp-request
[Switch] interface gigabitethernet0/0/1
[Switch-GigabitEthernet0/0/1] storm-control broadcast min-rate 1000 max-rate 2000
[Switch-GigabitEthernet0/0/1] storm-control multicast min-rate 1000 max-rate 2000
[Switch-GigabitEthernet0/0/1] storm-control unicast min-rate 1000 max-rate 2000
[Switch-GigabitEthernet0/0/1] storm-control interval 90
[Switch-GigabitEthernet0/0/1] storm-control action block
[Switch-GigabitEthernet0/0/1] storm-control enable trap
#使能风暴控制上报告警
```

配置验证

执行命令display storm-control interface查看GE0/0/1接口下的风暴控制配置情况。

```
[Switch]display storm-control interface GigabitEthernet 0/0/1
PortName    Type      Rate          Mode    Action    Punish-  Trap Log Int    Last-
                      (Min/Max)             Status              Punish-Time
--------------------------------------------------------------------------------
GE0/0/1     Multicast 1000          Pps     Block     Normal   On   Off        90
                      /2000
GE0/0/1     Broadcast 1000          Pps     Block     Normal   On   Off        90
                      /2000
GE0/0/1     Unicast   1000          Pps     Block     Normal   On   Off        90
                      /2000
```

DHCP工作原理概述

- DHCP 无中继工作原理：
- 发现阶段，DHCP 客户端发送 DHCP DISCOVER 报文（广播）来发现 DHCP 服务器。DHCP DISCOVER 报文中携带了客户端的 MAC 地址（DHCP DISCOVER 报文中的 chaddr 字段）、需要请求的参数列表选项（Option55）、广播标志位（DHCP DISCOVER 报文中的 flags 字段，表示客户端请求服务器以单播或广播形式发送响应报文）等信息。
- 提供阶段，服务器接收到 DHCP DISCOVER 报文后，选择跟接收 DHCP DISCOVER 报文接口的 IP 地址处于同一网段的地址池，并且从中选择一个可用的 IP 地址，然后通过 DHCP OFFER 报文发送给 DHCP 客户端。
- 请求阶段，如果有多个 DHCP 服务器向 DHCP 客户端回应 DHCP OFFER 报文，则 DHCP 客户端一般只接收第一个收到的 DHCP OFFER 报文，然后以广播方式发送 DHCP REQUEST 报文，该报文中包含客户端想选择的 DHCP 服务器标识符（即 Option54）和客户端 IP 地址（即 Option50，填充了接收的 DHCP OFFER 报文中 yiaddr 字段的 IP 地址）。以广播方式发送 DHCP REQUEST 报文，是为了通知所有的 DHCP 服务器，它将选择某个 DHCP 服务器提供的 IP 地址，其他 DHCP 服务器可以重新将曾经分配给客户端的 IP 地址分配给其他客户端。
- 确认阶段，DHCP 客户端收到 DHCP ACK 报文，会广播发送免费 ARP 报文，探测本网段是否有其他终端使用服务器分配的 IP 地址。
- DHCP 有中继工作原理：
- DHCP 中继接收到 DHCP 客户端广播发送的 DHCP DISCOVER 报文后，主要动作含：检查 DHCP 报文中的 giaddr 字段。DHCP 报文中的 giaddr 字段标识客户端网关的 IP 地址。如果服务器和客户端不在同一个网段且中间存在多个 DHCP 中继，当客户端发出 DHCP 请求时，第一个 DHCP 中继会把

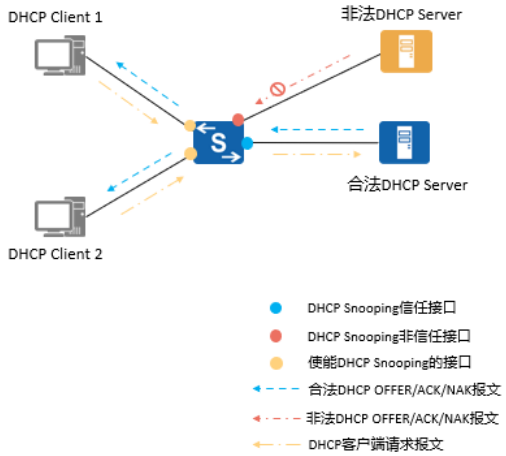
自己的 IP 地址填入此字段，后面的 DHCP 中继不修改此字段内容。DHCP 服务器会根据此字段来判断出客户端所在的网段地址，从而为客户端分配该网段的 IP 地址。

- 将 DHCP 报文的目的 IP 地址改为 DHCP 服务器或下一跳中继的 IP 地址，源地址改为中继连接客户端的接口地址，通过路由转发将 DHCP 报文单播发送到 DHCP 服务器或下一跳中继。
- DHCP 详细原理请参考《HCIP-Datacom-Core Technology》。

DHCP Snooping 概述

- 为了保证网络通信业务的安全性，引入了 DHCP Snooping 技术，在 DHCP Client 和 DHCP Server 之间建立一道防火墙，以抵御网络中针对 DHCP 的各种攻击。
- DHCP Snooping 是 DHCP 的一种安全特性，用于保证 DHCP 客户端从合法的 DHCP 服务器获取 IP 地址。DHCP 服务器记录 DHCP 客户端 IP 地址与 MAC 地址等参数的对应关系，防止网络上针对 DHCP 攻击。
- 目前 DHCP 协议在应用的过程中遇到很多安全方面的问题，网络中存在一些针对 DHCP 的攻击，如 DHCP Server 仿冒者攻击、DHCP Server 的拒绝服务攻击、仿冒 DHCP 报文攻击等。
- DHCP Snooping 主要是通过 DHCP Snooping 信任功能和 DHCP Snooping 绑定表实现 DHCP 网络安全。

DHCP Snooping信任功能

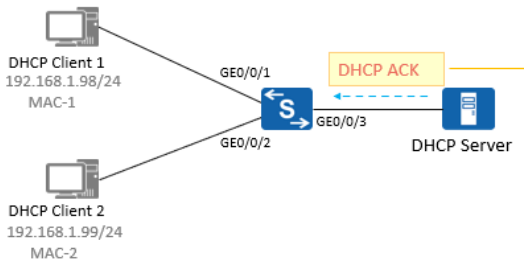


- DHCP Snooping的信任功能，能够保证DHCP客户端从合法的DHCP服务器获取IP地址。
- DHCP Snooping信任功能将接口分为信任接口和非信任接口：
  - 信任接口正常接收DHCP服务器响应的DHCP ACK、DHCP NAK和DHCP Offer报文。
  - 设备只将DHCP客户端的DHCP请求报文通过信任接口发送给合法的DHCP服务器，不会向非信任接口转发。
  - 非信任接口收到的DHCP Server发送的DHCP OFFER、DHCP ACK、DHCP NAK报文会被直接丢弃。

- 配置 dhcp snooping enable 命令的接口，收到 DHCP 请求报文后，转发给所有的信任接口；收到 DHCP 响应报文后丢弃。
- 配置 dhcp snooping trusted 命令的接口，收到 DHCP 请求报文后，转发给所有的信任接口，如果没有其他信任接口，则丢弃该 DHCP 请求报文；收到 DHCP 响应报文后，只转发给连接对应客户端的并且配置命令 dhcp snooping enable 的接口，如果查不到上述接口，则丢弃该 DHCP 响应报文。

DHCP Snooping绑定表

- 二层接入设备使能了DHCP Snooping功能后，从收到DHCP ACK报文中提取关键信息（包括PC的MAC地址以及获取到的IP地址、地址租期），并获取与PC连接的使能了DHCP Snooping功能的接口信息（包括接口编号及该接口所属的VLAN），根据这些信息生成DHCP Snooping绑定表。
- 由于DHCP Snooping绑定表记录了DHCP客户端IP地址与MAC地址等参数的对应关系，故通过对报文与DHCP Snooping绑定表进行匹配检查，能够有效防范非法用户的攻击。



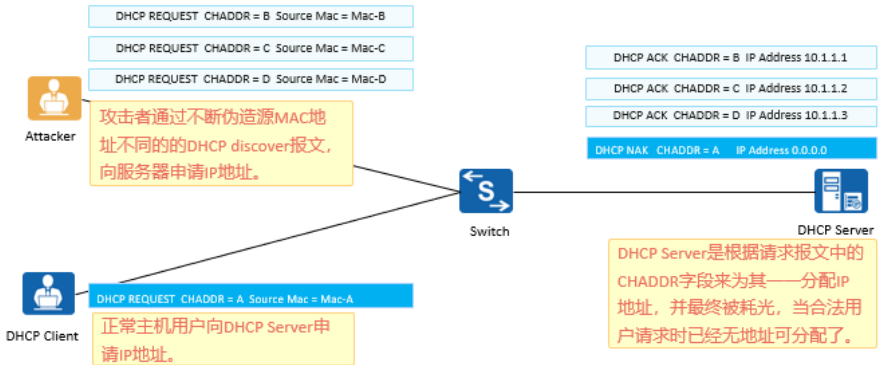
IP	MAC	VLAN	接口	Lease
192.168.1.98	MAC-1	1	GE0/0/1	1
192.168.1.99	MAC-2	1	GE0/0/2	1

- DHCP Snooping 绑定表根据 DHCP 租期进行老化或根据用户释放 IP 地址时发出的 DHCP Release 报文自动删除对

应表项。

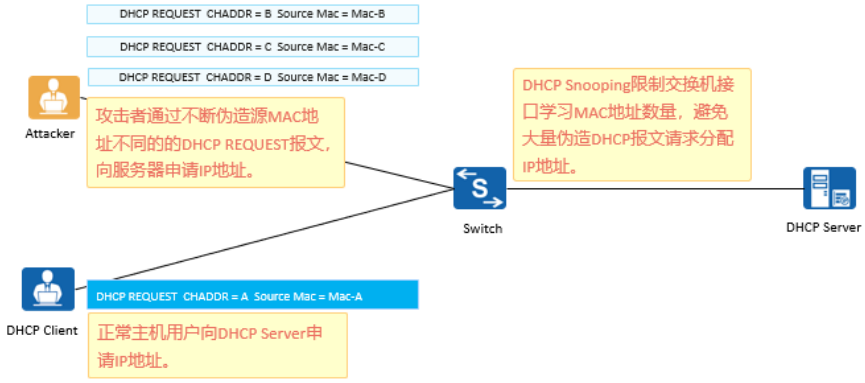
DHCP饿死攻击

- 攻击原理：攻击者持续大量地向DHCP Server申请IP地址，直到耗尽DHCP Server地址池中的IP地址，导致DHCP Server不能给正常的用户进行分配。
- 漏洞分析：DHCP Server向申请者分配IP地址时，无法区分正常的申请者与恶意的申请者。



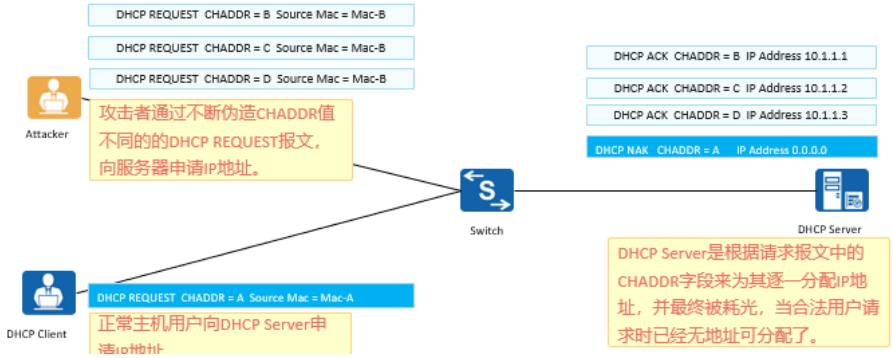
DHCP Snooping防饿死攻击

解决方法：对于饿死攻击，可以通过DHCP Snooping的MAC地址限制功能来防止。该功能通过限制交换机接口上允许学习到的最多MAC地址数目，防止通过变换MAC地址，大量发送DHCP请求。



改变CHADDR值的DoS攻击

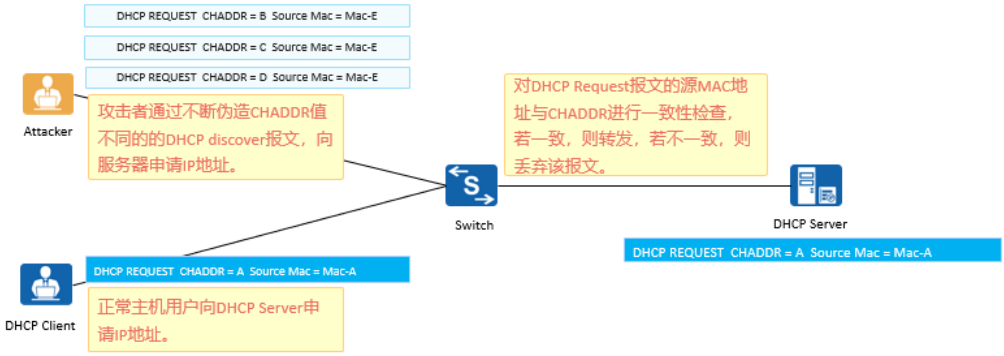
- 攻击原理：攻击者持续大量地向DHCP Server申请IP地址，直到耗尽DHCP Server地址池中的IP地址，导致DHCP Server不能给正常的用户进行分配。
- 漏洞分析：DHCP Server向申请者分配IP地址时，无法区分正常的申请者与恶意的申请者。



- DHCP 饿死攻击是攻击者通过持续大量地向 DHCP Server 申请 IP 地址来实现的，其目的是耗尽 DHCP Server 地址池中的 IP 地址，导致 DHCP Server 没有 IP 地址分配给正常的用户。DHCP 消息中有一个名叫 CHADDR（Client Hardware Address）的字段，该字段是由 DHCP 客户端填写的，表示的是客户端的硬件地址（也就是客户端的 MAC 地址）。DHCP Server 是针对 CHADDR 来分配 IP 地址的，对于不同的 CHADDR，DHCP Server 会分配不同的 IP 地址；DHCP Server 无法区分什么样的 CHADDR 是合法的，什么样的 CHADDR 是非法的。利用这个漏洞，攻击者每申请一个 IP 地址时，就在 DHCP 消息的 CHADDR 字段中填写一个不同的值，以此来冒充是不同的用户在申请 IP 地址。

DHCP Snooping防改变CHADDR值的DoS攻击

解决方法：为了避免受到攻击者改变CHADDR值的攻击，可以在设备上配置DHCP Snooping功能，检查DHCP Request报文中CHADDR字段。如果该字段跟数据帧头部的源MAC相匹配，转发报文；否则，丢弃报文。从而保证合法用户可以正常使用网络服务。

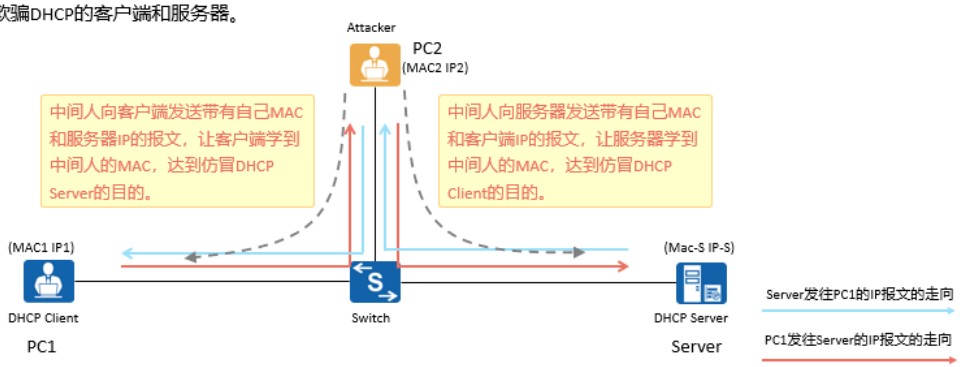


- DHCP 饿死攻击是攻击者通过持续大量地向 DHCP Server 申请 IP 地址来实现的，其目的是耗尽 DHCP Server 地址池中的 IP 地址，导致 DHCP Server 没有 IP 地址分配给正常的用户。DHCP 消息中有一个名叫 CHADDR（Client Hardware Address）的字段，该字段是由 DHCP 客户端填写的，表示的是客户端的硬件地址（也就是客户端的 MAC 地址）。DHCP Server 是针对 CHADDR 来分配 IP 地址的，对于不同的 CHADDR，DHCP Server 会分配不同的 IP 地址；DHCP Server 无法区分什么样的 CHADDR 是合法的，什么样的 CHADDR 是非法的。利用这个漏洞，攻击者每申请一个 IP 地址时，就在 DHCP 消息的 CHADDR 字段中填写一个不同的值，以此来冒充是不同的用户在申请 IP 地址。
- 为了弥补上述漏洞，从而阻止饿死攻击，DHCP Snooping 技术支持在端口下对 DHCP Request 报文的源 MAC 地址与 CHADDR 进行一致性检查：如果二者相同，则转发报文；如果二者不相同，则丢弃。如果要在某端口下实施源 MAC 地址与 CHADDR 的一致性检查，可以在该端口下使用命令 dhcp snooping check dhcp-chaddr enable。
- 还可能存在这样一种饿死攻击，就是攻击者不断同时变

换 MAC 地址和 CHADDR，并且每一次变换时，都让 CHADDR 与 MAC 地址相同，如此一来，便可以躲过上述源 MAC 地址与 CHADDR 的一致性检查！

DHCP中间人攻击

- 攻击原理：攻击者利用ARP机制，让Client学习到DHCP Server IP与Attacker MAC的映射关系，又让Server学习到Client IP与Attacker Mac的映射关系。如此一来，Client与Server之间交互的IP报文都会经过攻击者中转。
- 漏洞分析：从本质上讲，中间人攻击是一种Spoofing IP/MAC攻击，中间人利用了虚假的IP地址与MAC地址之间的映射关系来同时欺骗DHCP的客户端和服务器。

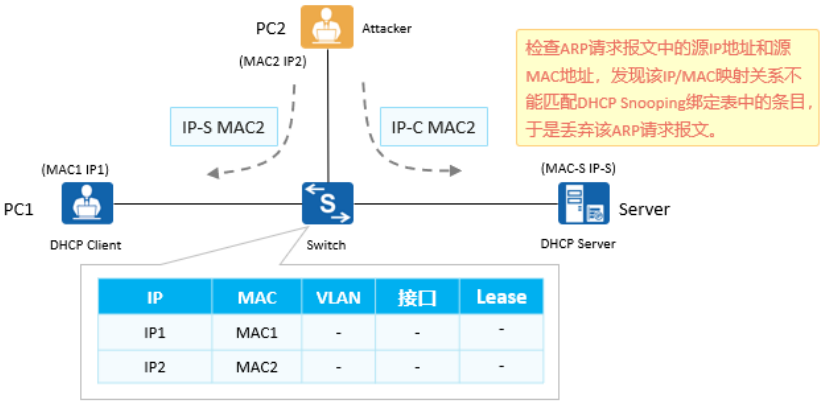


- 如图所示，攻击者利用 ARP 机制，让 PC1 学习到 IP-S 与 MAC2 的映射关系，又让 Server 学习到 IP1 与 MAC2 的映射关系。当 PC1 向 DHCP Server 发送 IP 报文时，目的 IP 地址为 IP-S，源 IP 地址为 IP1，而封装这个 IP 报文的帧的目的 MAC 地址为 MAC2，源 MAC 地址为 MAC1，所以这个帧会首先到达攻击者 PC2。攻击者收到这个帧后，将这个帧的目的 MAC 地址更换为 MAC-S，源 MAC 地址更换为 MAC2，然后将这个帧发往 Server。如此“偷梁换柱”，Server 是看不出任何破绽的。另一方面，当 DHCP Server 向 PC1 发送 IP 报文时，目的 IP 地址为 IP1，源 IP 地址为 IP-S，而封装这个 IP 报文的帧的目的 MAC 地址为 MAC2，源 MAC 地址为 MAC-S，所以这个帧也会首先到达攻击者 PC2。攻击者收到这个帧后，将这个帧的目的 MAC 地址更换为 MAC1，源 MAC 地址更换为 MAC2，然后将这个帧发往 PC1。同样，PC1 也是看不出任何破绽的。

- 由于往来于 PC1 与 DHCP Server 之间的 IP 报文都会经过攻击者（中间人）进行中转，攻击者便很容易窃取这些 IP 报文中的某些信息，并利用这些信息来进行其他的破坏行为。攻击者也可以很容易对往来于 PC1 与 DHCP Server 之间的 DHCP 消息（这些消息是封装在 UDP 报文中的，而 UDP 报文又是封装在 IP 报文中的）进行篡改，达到直接攻击 DHCP 的目的。

DHCP Snooping防DHCP中间人攻击

解决方法：为防御中间人攻击与IP/MAC Spoofing攻击，可使用DHCP Snooping的绑定表工作模式，当接口接收到ARP或者IP报文，使用ARP或者IP报文中的“源IP+源MAC”匹配DHCP Snooping绑定表。如果匹配就进行转发，如果不匹配就丢弃。



IP	MAC	VLAN	接口	Lease
IP1	MAC1	-	-	-
IP2	MAC2	-	-	-

- DHCP 中间人攻击本质上是一种 Spoofing IP/MAC 攻击。要想防止 DHCP 中间人攻击，其实就是要防止 Spoofing IP/MAC 攻击。
- 运行了 DHCP Snooping 的交换机会“侦听（Snooping）”往来于用户与 DHCP Server 之间的 DHCP 消息，并从中收集用户的 MAC 地址（这里的 MAC 地址是指 DHCP 消息中 CHADDR 字段的值）、用户的 IP 地址（这里的 IP 地址是指 DHCP Server 分配给相应 CHADDR 的 IP 地址）等信息，这些信息会集中存放在一个数据库中，该数据库也被称为 DHCP Snooping 绑定表。运行了 DHCP Snooping 的交换机会建立并动态维护 DHCP Snooping 绑定表，绑定表中除了包含了用户的 MAC 地址、用户的 IP 地址外，还包括 IP 地址租用期、VLAN

ID 等等信息。

- 如图所示，假设 DHCP Server 给 PC1 分配了 IP 地址 IP 1，给 PC2 分配了 IP 地址 IP2，那么 IP1 与 MAC1 就形成了绑定关系，IP2 与 MAC2 也形成了绑定关系，这种绑定关系都存放于 DHCP Snooping 绑定表中。攻击者为了让 Server 学习到 IP1 与 MAC2 的映射关系，会发送 ARP 请求报文（将 ARP 报文中的源 IP 地址填为 IP1，源 MAC 地址填为 MAC2）。交换机接收到 ARP 请求报文后，会检查该 ARP 请求报文中的源 IP 地址和源 MAC 地址，发现该 IP/MAC（IP1/MAC2）映射关系不能匹配 DHCP Snooping 绑定表中的条目，于是会丢弃该 ARP 请求报文，这样就有效地防止了 Spoofing IP/MAC 攻击。
- 如果需要使用上面所描述的防止 Spoofing IP/MAC 攻击（进而防止中间人）的方法，就必须在交换机的系统视图下执行配置命令 arp dhcp-snooping-detect enable。

DHCP Snooping配置命令介绍

1. 全局使能DHCP Snooping功能

   [Huawei] **dhcp snooping enable** [**ipv4** | **ipv6**]

2. VLAN视图下使能DHCP Snooping功能

   [Huawei-vlan2] **dhcp snooping enable**

   在VLAN视图下执行此命令，则对设备所有接口接收到的属于该VLAN的DHCP报文命令功能生效。

3. VLAN视图下配置接口为“信任”状态

   [Huawei-vlan2] **dhcp snooping trusted interface** *interface-type interface-number*

   在VLAN视图下执行此命令，则命令功能仅对加入该VLAN的接口收到的属于此VLAN的DHCP报文生效。

DHCP Snooping配置命令介绍

1. 接口视图下使能DHCP Snooping功能

```
[Huawei-GigabitEthernet0/0/1] dhcp snooping enable
```

2. 接口视图下配置接口为“信任”状态

```
[Huawei-GigabitEthernet0/0/1] dhcp snooping trusted
```

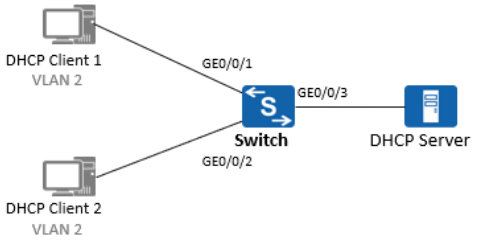
缺省情况下，设备接口为非信任状态。

3. (可选) 配置丢弃GIADDR字段非零的DHCP报文

```
[Huawei] dhcp snooping check dhcp-giaddr enable vlan { vlan-id1 [ to vlan-id2 ] }
```

使能检测DHCP Request报文中GIADDR字段是否非零的功能。此命令同时可以在VLAN视图或接口视图下进行配置。
在VLAN视图下执行此命令，则对设备所有接口接收到的属于该VLAN的DHCP报文命令功能生效；在接口下执行该命令，则对该接口下的所有DHCP报文命令功能生效。

DHCP Snooping配置举例



如图所示，DHCP和VLAN基础配置已完成，在Switch配置DHCP Snooping功能。

配置方式一：接口视图

```
[Switch] dhcp snooping enable ipv4
[Switch] interface GigabitEthernet 0/0/1
[Switch-GigabitEthernet0/0/1] dhcp snooping enable
[Switch] interface GigabitEthernet 0/0/2
[Switch-GigabitEthernet0/0/2] dhcp snooping enable
[Switch] interface GigabitEthernet 0/0/3
[Switch-GigabitEthernet0/0/3] dhcp snooping enable
[Switch-GigabitEthernet0/0/3] dhcp snooping trusted
```

配置方式二：VLAN视图

```
[Switch] dhcp snooping enable ipv4
[Switch] vlan 2
[Switch-vlan2] dhcp snooping enable
[Switch] interface GigabitEthernet 0/0/3
[Switch-GigabitEthernet0/0/3] dhcp snooping trusted
```

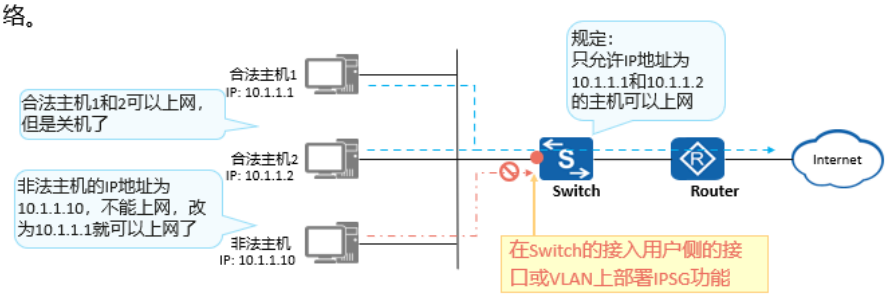
配置验证

执行命令display dhcp snooping interface，查看接口下的DHCP Snooping运行信息。

```
[Switch]display dhcp snooping interface GigabitEthernet 0/0/3
 DHCP snooping running information for interface GigabitEthernet0/0/3 :
 DHCP snooping                 : Enable
 Trusted interface             : Yes
 Dhcp user max number          : 1024    (default)
 Current dhcp user number      : 0
 Check dhcp-giaddr             : Disable  (default)
 Check dhcp-chaddr             : Disable  (default)
 Alarm dhcp-chaddr             : Disable  (default)
 Check dhcp-request            : Disable  (default)
 Alarm dhcp-request            : Disable  (default)
----- more ------
```

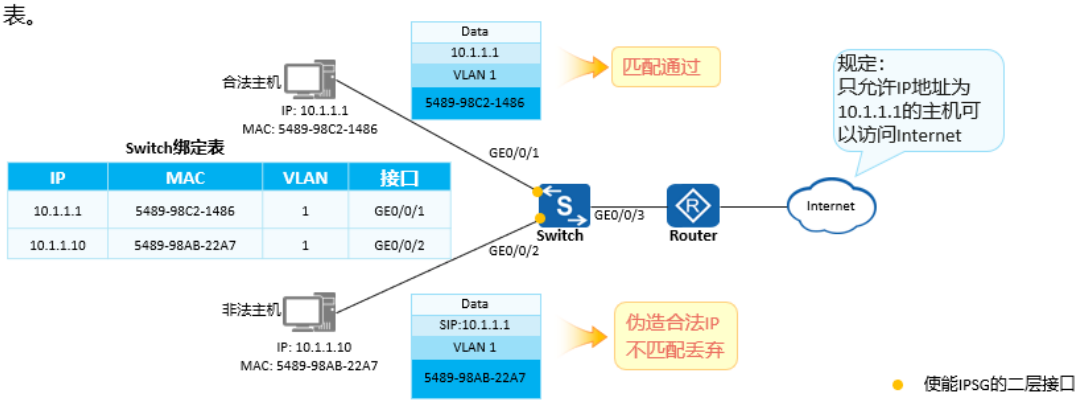
IPSG技术概述

- IP地址欺骗攻击中，攻击者通过伪造合法用户的IP地址获取网络访问权限，非法访问网络，甚至造成合法用户无法访问网络，或者信息泄露。IPSG针对IP地址欺骗攻击提供了一种防御机制，可以有效阻止此类网络攻击行为。
- IP源防攻击（IPSG，IP Source Guard）是一种基于二层接口的源IP地址过滤技术。它能够防止恶意主机伪造合法主机的IP地址来仿冒合法主机，还能确保非授权主机不能通过自己指定IP地址的方式来访问网络或攻击网络。



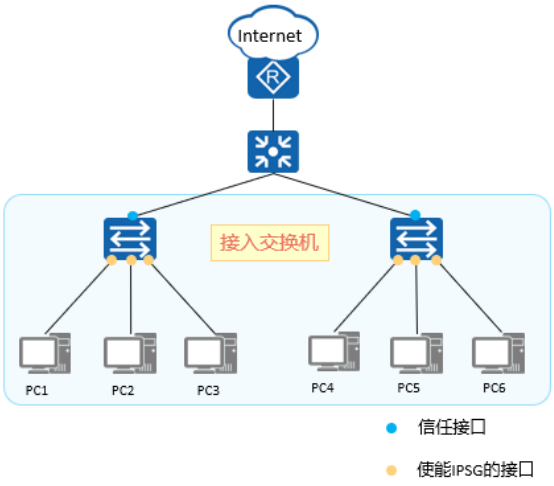
IPSG工作原理

IPSG利用绑定表（源IP地址、源MAC地址、所属VLAN、入接口的绑定关系）去匹配检查二层接口上收到的IP报文，只有匹配绑定表的报文才允许通过，其他报文将被丢弃。常见的绑定表有静态绑定表和DHCP Snooping动态绑定表。



- 绑定表生成后，IPSG 基于绑定表向指定的接口或者指定的 VLAN 下发 ACL，由该 ACL 来匹配检查所有 IP 报文。主机发送的报文，只有匹配绑定表才会允许通过，不匹配绑定表的报文都将被丢弃。当绑定表信息变化时，设备会重新下发 ACL。
- 缺省情况下，如果在没有绑定表的情况下使能了 IPSG，设备将拒绝除 DHCP 请求报文外的所有 IP 报文。
- 静态绑定表项包含：MAC 地址、IP 地址、VLAN ID、入接口。静态绑定表项中指定的信息均用于 IPSG 过滤接口收到的报文。
- 动态绑定表项包含：MAC 地址、IP 地址、VLAN ID、入接口。IPSG 依据该表项中的哪些信息过滤接口收到的报文，由用户设置的检查项决定，缺省是四项都进行匹配检查。常用的检查项有基于源 IP 地址过滤,基于源 MAC 地址过滤,基于源 IP 地址+源 MAC 地址过滤,基于源 IP 地址+源 MAC 地址+接口过滤,基于源 IP 地址+源 MAC 地址+接口+VLAN 过滤等。

IPSG应用场景



- 通过IPSG防止PC私自更改IP地址。
  - PC只能使用DHCP Server分配的IP地址或者管理员配置的静态地址，随意更改IP地址后无法访问网络，防止PC非法取得上网权限。
- 小型网络IP地址是静态分配时，通过IPSG限制非法PC接入。
  - 外来人员自带电脑不能随意接入内网，防止内网资源泄露。

IPSG配置命令介绍

1. 配置静态用户绑定表项

   [Huawei] **user-bind static { { { ip-address | ipv6-address } { *start-ip* [to *end-ip*] } &<1-10> | ipv6-prefix** *prefix/prefix-length* **} | mac-address** *mac-address* **} * [interface** *interface-type interface-number* **] [vlan** *vlan-id* **[ce-vlan** *ce-vlan-id* **]]**

   IPSG按照静态绑定表项进行完全匹配。

2. 使能IPSG功能

   [Huawei-GigabitEthernet0/0/1] **ip source check user-bind enable**

   使能接口或者VLAN的IP报文检查功能，VLAN视图配置与接口视图一致。

3. 使能IP报文检查告警功能

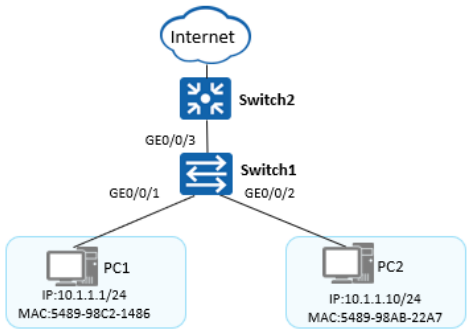
   [Huawei-GigabitEthernet0/0/1] **ip source check user-bind alarm enable**

4. 配置IP报文检查告警阈值

   [Huawei-GigabitEthernet0/0/1] **ip source check user-bind alarm threshold** *threshold*

   配置了IP报文检查告警功能后，当丢弃的IP报文超过告警阈值时，会产生告警提醒用户。

IPSG配置举例



Switch1配置如下：

```
#在接入交换机上配置静态绑定表
[Switch1] user-bind static ip-address 10.1.1.1 mac-address 5489-98C2-1486
[Switch1] user-bind static ip-address 10.1.1.10 mac-address 5489-98AB-22A7
#使能GE0/0/1接口IPSG和IP报文检查告警功能
[Switch1] interface GigabitEthernet 0/0/1
[Switch1-GigabitEthernet0/0/1] ip source check user-bind enable
[Switch1-GigabitEthernet0/0/1] ip source check user-bind alarm enable
[Switch1-GigabitEthernet0/0/1] ip source check user-bind alarm threshold 100
#接口GE0/0/2配置与GE0/0/1类似，此处省略
```

- 如图所示：网络终端设备通过手工方式配置静态IP地址统一管理，通过在接入交换机上配置IPSG，防止主机私自更改IP地址非法获取访问网络权限。
  - 配置静态绑定表
  - 使能IPSG及告警上报功能

配置验证

- 在Switch上执行display dhcp static user-bind all命令，可以查看静态绑定表信息。
- PC1和PC2使用管理员分配的固定IP地址可以正常访问网络，更改IP地址后无法访问网络。

```
[Switch1] display dhcp static user-bind all
DHCP static Bind-table:
Flags:O - outer vlan ,I - inner vlan ,P - Vlan-mapping
IP Address          MAC Address          VSI/VLAN(O/I/P) Interface
--------------------------------------------------------------------------------
10.1.1.1            5489-98C2-1486       -- /-- /--   --
10.1.1.10           5489-98AB-22A7       -- /-- /--   --
--------------------------------------------------------------------------------
Print count:      2      Total count:      2
```

思考题：

- （多选题）DHCP Snooping 是一种 DHCP 安全特性，可以用于防御多种攻击，其中包括（　　）
- 防御改变 CHADDR 值的饿死攻击
- 防御 DHCP 仿冒者攻击
- 防御 TCP flag 攻击
- 防御中间人攻击和 IP/MAC Spoofing 攻击

参考答案：

- ABD
-