# 目 录

# 1 ARP 攻击防御

## 1.1 ARP攻击防御简介

设备提供了多种 ARP 攻击防御技术对局域网中的 ARP 攻击和 ARP 病毒进行防范、检测和解决。常见的 ARP 攻击方式包括：

- 攻击者通过向设备发送大量目标 IP 地址不能解析的 IP 报文，使得设备试图反复地对目标 IP 地址进行解析，导致 CPU 负荷过重及网络流量过大。
- 攻击者向设备发送大量 ARP 报文，对设备的 CPU 形成冲击。
- 攻击者可以仿冒用户、仿冒网关发送伪造的 ARP 报文，使网关或主机的 ARP 表项不正确，从而对网络进行攻击。

## 1.2 ARP攻击防御配置任务简介

如下所有配置均为可选，请根据实际情况选择配置。

- 防止泛洪攻击
  - 配置 ARP 防止 IP 报文攻击功能
  - 配置源 MAC 地址固定的 ARP 攻击检测功能
- 防止仿冒用户、仿冒网关攻击
  - 配置 ARP 报文源 MAC 地址一致性检查功能
  - 配置 ARP 主动确认功能
  - 配置授权 ARP 功能
  - 配置 ARP Detection 功能
  - 配置 ARP 自动扫描、固化功能
  - 配置 ARP 网关保护功能
  - 配置 ARP 过滤保护功能

## 1.3 配置ARP防止IP报文攻击功能

### 1.3.1 功能简介

如果网络中有主机通过向设备发送大量目标 IP 地址不能解析的 IP 报文来攻击设备，则会造成下面的危害：

- 设备向目的网段发送大量 ARP 请求报文，加重目的网段的负载。
- 设备会试图反复地对目标 IP 地址进行解析，增加了 CPU 的负担。

为避免这种 IP 报文攻击所带来的危害，设备提供了下列两个功能：

- ARP 源抑制功能：如果发送攻击报文的源是固定的，可以采用 ARP 源抑制功能。开启该功能后，如果网络中每 5 秒内从某 IP 地址向设备某接口发送目的 IP 地址不能解析的 IP 报文超过

了设置的阈值，则设备将不再处理由此 IP 地址发出的 IP 报文直至该 5 秒结束，从而避免了恶意攻击所造成的危害。

- ARP 黑洞路由功能：无论发送攻击报文的源是否固定，都可以采用 ARP 黑洞路由功能。开启该功能后，一旦接收到目标 IP 地址不能解析的 IP 报文，设备立即产生一个黑洞路由，并同时发起 ARP 主动探测，如果在黑洞路由老化时间内 ARP 解析成功，则设备马上删除此黑洞路由并开始转发去往该地址的报文，否则设备直接丢弃该报文。在删除黑洞路由之前，后续去往该地址的 IP 报文都将被直接丢弃。用户可以通过命令配置 ARP 请求报文的发送次数和发送时间间隔。等待黑洞路由老化时间过后，如有报文触发则再次发起解析，如果解析成功则进行转发，否则仍然产生一个黑洞路由将去往该地址的报文丢弃。这种方式能够有效地防止 IP 报文的攻击，减轻 CPU 的负担。

### 1.3.2 配置 ARP 源抑制功能

(1) 进入系统视图。

**system-view**

(2) 开启 ARP 源抑制功能。

**arp source-suppression enable**

缺省情况下，ARP 源抑制功能处于关闭状态。

(3) 配置 ARP 源抑制的阈值。

**arp source-suppression limit** *limit-value*

缺省情况下，ARP 源抑制的阈值为 10。

### 1.3.3 配置 ARP 黑洞路由功能

#### 1. 配置限制和指导

当用户配置的 ARP 主动探测总时长（发送次数×发送时间间隔）大于黑洞路由老化时间时，系统只会取小于等于该老化时间的最大值作为真正的探测总时长。

当发起 ARP 主动探测过程结束且生成的黑洞路由还未老化时，设备无法主动对黑洞路由对应的设备进行 ARP 解析，为了缓解该问题，用户可以配置较大的发送 ARP 请求报文次数。

#### 2. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 开启 ARP 黑洞路由功能。

**arp resolving-route enable**

缺省情况下，ARP 黑洞路由功能处于开启状态。

(3) （可选）配置发送 ARP 请求报文的次数。

**arp resolving-route probe-count** *count*

缺省情况下，发送 ARP 请求报文的次数为 3 次。

(4) （可选）配置发送 ARP 请求报文的时间间隔。

**arp resolving-route probe-interval** *interval*

缺省情况下，发送 ARP 请求报文的时间间隔为 1 秒。

### 1.3.4 ARP 防止 IP 报文攻击显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 ARP 源抑制的运行情况，通过查看显示信息验证配置的效果。

表1-1 ARP 防止 IP 报文攻击显示和维护

| 操作 | 命令 |
| --- | --- |
| 显示ARP源抑制的配置信息 | **display arp source-suppression** |

## 1.4 配置源MAC地址固定的ARP攻击检测功能

### 1.4.1 功能简介

本特性根据 ARP 报文的源 MAC 地址对上送 CPU 的 ARP 报文进行统计，在 5 秒内，如果收到同一源 MAC 地址（源 MAC 地址固定）的 ARP 报文超过一定的阈值，则认为存在攻击，系统会将此 MAC 地址添加到攻击检测表项中。当开启了 ARP 日志信息功能（配置 **arp check log enable** 命令），且在该攻击检测表项老化之前，如果设置的检查模式为过滤模式，则会打印日志信息并且将该源 MAC 地址发送的 ARP 报文过滤掉；如果设置的检查模式为监控模式，则只打印日志信息，不会将该源 MAC 地址发送的 ARP 报文过滤掉。

对于已添加到源 MAC 地址固定的 ARP 攻击检测表项中的 MAC 地址，在等待设置的老化时间后，会重新恢复成普通 MAC 地址。

关于 ARP 日志信息功能的详细描述，请参见“网络互通配置指导”中的“ARP”。

### 1.4.2 配置限制和指导

切换源 MAC 地址固定的 ARP 攻击检查模式时，如果从监控模式切换到过滤模式，过滤模式马上生效；如果从过滤模式切换到监控模式，已生成的攻击检测表项，到表项老化前还会继续按照过滤模式处理。

对于网关或一些重要的服务器，可能会发送大量 ARP 报文，为了使这些 ARP 报文不被过滤掉，可以将这类设备的MAC地址配置成保护MAC地址，这样，即使该设备存在攻击也不会被检测或过滤。

### 1.4.3 配置步骤

(1) 进入系统视图。

**system-view**

(2) 开启源 MAC 地址固定的 ARP 攻击检测功能，并选择检查模式。

**arp source-mac** { **filter** | **monitor** }

缺省情况下，源 MAC 地址固定的 ARP 攻击检测功能处于关闭状态。

(3) 配置源 MAC 地址固定的 ARP 报文攻击检测的阈值。

**arp source-mac threshold** *threshold-value*

缺省情况下，源 MAC 地址固定的 ARP 报文攻击检测的阈值 30

(4) 配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间。

**arp source-mac aging-time** *time*

缺省情况下，源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 300 秒，即 5 分钟。

(5) （可选）配置保护 MAC 地址。

**arp source-mac exclude-mac** *mac-address*&<1-n>

缺省情况下，未配置任何保护 MAC 地址。

### 1.4.4 源 MAC 地址固定的 ARP 攻击检测显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后源 MAC 地址固定的 ARP 攻击检测的运行情况，通过查看显示信息验证配置的效果。

说明

由于 WX2500H-WiNet 系列、WAC 系列、WX2500H-LI 系列和 AC1000 系列不支持 IRF 功能，因此不支持 IRF 模式的命令行配置。

表1-2 源 MAC 地址固定的 ARP 攻击检测显示和维护

| 操作 | 命令 |
|---|---|
| 显示检测到的源MAC地址固定的ARP攻击检测表项 | （独立运行模式）<br>**display arp source-mac** [ **interface** *interface-type interface-number* ]<br>（IRF模式）<br>**display arp source-mac** { **interface** *interface-type interface-number* \| **slot** *slot-number* } |

### 1.4.5 源 MAC 地址固定的 ARP 攻击检测功能配置举例

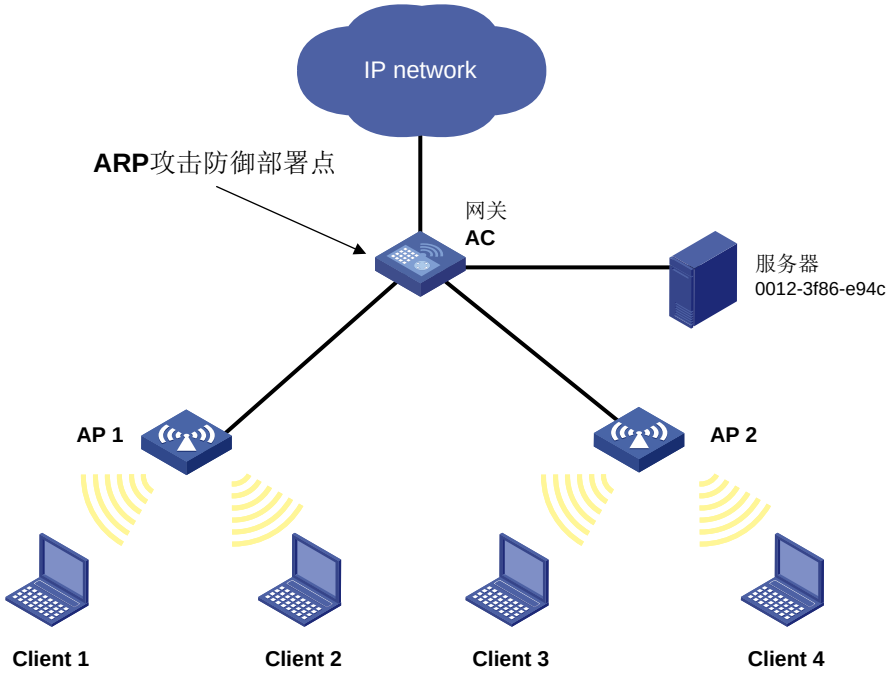
#### 1. 组网需求

某局域网内客户端通过网关与外部网络通信，网络环境如图 1-1 所示。

网络管理员希望能够防止因恶意用户对网关发送大量 ARP 报文，造成设备瘫痪，并导致其它用户无法正常地访问外部网络；同时，对于正常的大量 ARP 报文仍然会进行处理。

### 2. 组网图

图1-1 源 MAC 地址固定的 ARP 攻击检测功能配置组网图




### 3. 配置步骤

# 开启源 MAC 固定 ARP 攻击检测功能，并选择过滤模式。

```
<AC> system-view
[AC] arp source-mac filter
```

# 配置源 MAC 固定 ARP 报文攻击检测阈值为 30 个。

```
[AC] arp source-mac threshold 30
```

# 配置源 MAC 地址固定的 ARP 攻击检测表项的老化时间为 60 秒。

```
[AC] arp source-mac aging-time 60
```

# 配置源 MAC 固定攻击检查的保护 MAC 地址为 0012-3f86-e94c。

```
[AC] arp source-mac exclude-mac 0012-3f86-e94c
```

## 1.5 配置ARP报文源MAC地址一致性检查功能

### 1. 功能简介

ARP 报文源 MAC 地址一致性检查功能主要应用于网关设备上，防御以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同的 ARP 攻击。

配置本特性后，网关设备在进行 ARP 学习前将对 ARP 报文进行检查。如果以太网数据帧首部中的源 MAC 地址和 ARP 报文中的源 MAC 地址不同，则认为是攻击报文，将其丢弃；否则，继续进行 ARP 学习。

### 2. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 开启 ARP 报文源 MAC 地址一致性检查功能。

**arp valid-check enable**

缺省情况下，ARP 报文源 MAC 地址一致性检查功能处于关闭状态。

## 1.6 配置ARP主动确认功能

### 1. 功能简介

ARP 的主动确认功能主要应用于网关设备上，防止攻击者仿冒用户欺骗网关设备。ARP 主动确认功能分为非严格模式和严格模式，这两种模式的实现如下：

- 配置非严格模式的 ARP 主动确认功能时，处理方式如下：
  - 收到目标 IP 地址为自己的 ARP 请求报文时，设备会发送 ARP 应答报文，但先不建立对应的表项。同时，设备立即向 ARP 请求报文的发送端 IP 地址发送 ARP 请求，在一个探测周期内如果收到发送端 IP 地址对应的设备回复的 ARP 应答报文，则建立 ARP 表项。
  - 收到 ARP 应答报文时，需要确认本设备是否在当前探测时间周期内对该报文中的源 IP 地址发起过 ARP 请求：
    - 若发起过请求，则设备建立该 ARP 表项；
    - 若未发起过请求，则不建立 ARP 表项。同时，设备立即向 ARP 应答报文的发送端 IP 地址发送 ARP 请求，在一个探测周期内如果收到发送端 IP 地址对应的设备回复的 ARP 应答报文，则建立 ARP 表项。
- 配置严格模式的 ARP 主动确认功能时，处理方式如下：
  - 收到目标 IP 地址为自己的 ARP 请求报文时，设备会发送 ARP 应答报文，但不建立 ARP 表项；
  - 收到 ARP 应答报文时，需要确认本设备是否在当前探测时间周期内对该报文中的源 IP 地址发起过 ARP 请求：若发起过请求，则设备建立该 ARP 表项；若未发起过请求，则设备丢弃该报文，不建立表项。

### 2. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 开启 ARP 主动确认功能。

**arp active-ack [ strict ] enable**

缺省情况下，ARP 主动确认功能处于关闭状态。

在严格模式下，只有 ARP 黑洞路由功能处于开启状态，ARP 主动确认功能才能生效。

## 1.7 配置授权ARP功能

### 1.7.1 功能简介

所谓授权 ARP（Authorized ARP），就是动态学习 ARP 的过程中，只有和 DHCP 服务器生成的租约或 DHCP 中继生成的安全表项一致的 ARP 报文才能够被学习。关于 DHCP 服务器和 DHCP 中继的介绍，请参见“网络互通配置指导”中的“DHCP”。

配置接口的授权 ARP 功能后，可以防止用户仿冒其他用户的 IP 地址或 MAC 地址对网络进行攻击，保证只有合法的用户才能使用网络资源，增加了网络的安全性。

### 1.7.2 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。

**interface** *interface-type interface-number*

支持的接口类型包括三层以太网接口、三层以太网子接口和 VLAN 接口视图。

(3) 开启授权 ARP 功能。

**arp authorized enable**

缺省情况下，接口下的授权 ARP 功能处于关闭状态。

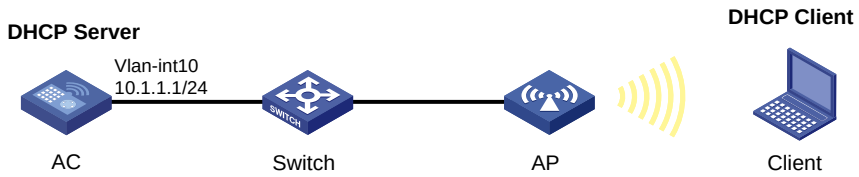
### 1.7.3 授权 ARP 功能在 DHCP 服务器上的典型配置举例

#### 1. 组网需求

- AC 是 DHCP 服务器，为同一网段中的客户端动态分配 IP 地址，地址池网段为 10.1.1.0/24。通过在 AC 接口上启用授权 ARP 功能来保证客户端的合法性。
- Client 是 DHCP 客户端，通过 DHCP 协议从 DHCP 服务器获取 IP 地址。

#### 2. 组网图

图1-2 授权 ARP 功能典型配置组网图




#### 3. 配置步骤

# 开启 DHCP 服务。

```
<AC> system-view
[AC] dhcp enable
[AC] dhcp server ip-pool 1
[AC-dhcp-pool-1] network 10.1.1.0 mask 255.255.255.0
[AC-dhcp-pool-1] quit
```

# 创建 VLAN 10，并配置接口 VLAN-interface10 的 IP 地址为 10.1.1.1/24。

```
[AC] vlan 10
[AC-vlan10] quit
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 10.1.1.1 24
```

# 开启接口 VLAN-interface10 的授权 ARP 功能。

```
[AC-Vlan-interface10] arp authorized enable
```

```
[AC-Vlan-interface10] quit
```

#### 4. 验证配置

# Client 通过 DHCP 申请地址后，可以在 AC 上查看相应的授权信息。

```
[AC] display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule   I-Invalid
IP address      MAC address    VLAN/VSI name Interface/Link ID        Aging Type
10.1.1.2        0012-3f86-e94c --            WLAN-BSS1/0/85703        20    D
```

从以上信息可以获知 AC 为 Client 动态分配的 IP 地址为 10.1.1.2。

此后，Client 与 AC 通信时采用的 IP 地址、MAC 地址等信息必须和授权 ARP 表项中的一致，否则将无法通信，从而保证了客户端的合法性。

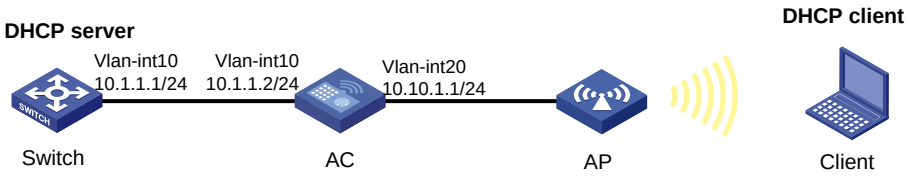
### 1.7.4 授权 ARP 功能在 DHCP 中继上的典型配置举例

#### 1. 组网需求

- Switch 充当 DHCP 服务器，为不同网段中的客户端动态分配 IP 地址，地址池网段为 10.10.1.0/24。
- AC 是 DHCP 中继，通过在接口 Vlan-interface10 上启用授权 ARP 功能来保证客户端的合法性。
- Client 是 DHCP 客户端，通过 DHCP 中继从 DHCP 服务器获取 IP 地址。

#### 2. 组网图

图1-3 授权 ARP 功能典型配置组网图




#### 3. 配置步骤

(1) 配置 Switch

# 配置接口的 IP 地址。

```
<Switch> system-view
[Switch] interface vlan-interface 10
[Switch-Vlan-interface10] ip address 10.1.1.1 24
[Switch-Vlan-interface10] quit
```

# 启用 DHCP 服务。

```
[Switch] dhcp enable
[Switch] dhcp server ip-pool 1
[Switch-dhcp-pool-1] network 10.10.1.0 mask 255.255.255.0
[Switch-dhcp-pool-1] gateway-list 10.10.1.1
[Switch-dhcp-pool-1] quit
[Switch] ip route-static 10.10.1.0 24 10.1.1.2
```

(2) 配置 AC

# 启用 DHCP 服务。

```
<AC> system-view
[AC] dhcp enable
```

# 配置 Vlan-interface10 以及 Vlan-interface20 接口的 IP 地址。

```
[AC] interface vlan-interface 10
[AC-Vlan-interface10] ip address 10.1.1.2 24
[AC-Vlan-interface10] quit
[AC] interface vlan-interface 20
[AC-Vlan-interface20] ip address 10.10.1.1 24
```

# 配置 Vlan-interface20 接口工作在 DHCP 中继模式。

```
[AC-Vlan-interface20] dhcp select relay
```

# 配置 DHCP 服务器的地址。

```
[AC-Vlan-interface20] dhcp relay server-address 10.1.1.1
```

# 启用接口授权 ARP 功能。

```
[AC-Vlan-interface20] arp authorized enable
[AC-Vlan-interface20] quit
```

# 开启 DHCP 中继用户地址表项记录功能。

```
[AC] dhcp relay client-information record
```

#### 4. 验证配置

# 用户通过 DHCP 申请地址后，在 AC 上查看授权 ARP 信息。

```
[AC] display arp
  Type: S-Static   D-Dynamic   O-Openflow   R-Rule  I-Invalid
IP address      MAC address    VLAN/VSI name Interface/Link ID        Aging Type
10.10.1.2       0012-3f86-e94c --            WLAN-BSS1/0/85703        20    D
```

从以上信息可以获知 AC 为 Client 动态分配的 IP 地址为 10.10.1.2。

此后，Client 与 AC 通信时采用的 IP 地址、MAC 地址等信息必须和授权 ARP 表项中的一致，否则将无法通信，从而保证了客户端的合法性。

## 1.8 配置ARP Detection功能

### 1.8.1 功能简介

ARP Detection 功能主要应用于接入设备上，通过检测并丢弃非法用户的 ARP 报文来防止仿冒用户、仿冒网关的攻击，具体包括以下几个功能：

- 用户合法性检查；
- ARP 报文有效性检查；
- ARP 报文强制转发；
- ARP Detection 日志功能。

如果既配置了报文有效性检查功能，又配置了用户合法性检查功能，那么先进行报文有效性检查，然后进行用户合法性检查。

### 1.8.2 用户合法性检查

#### 1. 功能简介

对于 ARP 信任接口，不进行用户合法性检查；对于 ARP 非信任接口，需要进行用户合法性检查，以防止仿冒用户的攻击。

用户合法性检查是根据 ARP 报文中源 IP 地址和源 MAC 地址检查用户是否是所属 VLAN 所在接口上的合法用户，包括基于用户合法性规则检查、基于 DHCP Snooping 表项的检查和基于 802.1X 安全表项的检查。

设备收到 ARP 报文后，首先进行基于用户合法性规则检查，如果找到与报文匹配的规则，则按照该规则对报文进行处理；如果未找到与报文匹配的规则，则继续进行基于 DHCP Snooping 表项的检查和基于 802.1X 安全表项的检查：

- 只要符合两者中的任何一个，就认为该 ARP 报文合法，进行转发。转发时查询报文目的 IP 地址对应的 DHCP Snooping 表项和 802.1X 安全表项：
  - 如果查询到两者中的任何一个，且和源 IP 地址对应表项的接口不一致，则将报文从目的 IP 地址对应的表项中的接口发送出去；
  - 如果查询到两者中的任何一个，且和源 IP 地址对应表项的接口一致，则将报文进行二层转发；
  - 如果未查到任何表项，则将报文进行二层转发。
- 如果所有检查都没有找到匹配的表项，则认为是非法报文，直接丢弃。

DHCP Snooping 安全表项通过 DHCP Snooping 功能自动生成，详细介绍请参见“网络互通配置指导”中的“DHCP Snooping”。

802.1X 安全表项通过 802.1X 功能产生，802.1X 用户需要使用支持将 IP 地址上传的客户端，用户通过了 802.1X 认证并且将 IP 地址上传至配置 ARP Detection 的设备后，设备自动生成可用于 ARP Detection 的用户合法性检查的 802.1X 安全表项。802.1X 的详细介绍请参见“用户接入与认证配置指导”中的“802.1X”。

#### 2. 配置限制和指导

配置用户合法性检查功能时，必须至少配置用户合法性规则或者 DHCP Snooping 功能和 802.1X 功能三者之一，否则所有从 ARP 非信任接口收到的 ARP 报文都会被正常转发。

#### 3. 配置步骤

(1) 进入系统视图。

**system-view**

(2) （可选）配置用户合法性检查规则。

**arp detection rule** *rule-id* { **deny** | **permit** } **ip** { *ip-address* [ *mask* ] | **any** } **mac** { *mac-address* [ *mask* ] | **any** } [ **vlan** *vlan-id* ]

缺省情况下，未配置用户合法性检查规则。

(3) 进入 VLAN 视图。

**vlan** *vlan-id*

(4) 开启 ARP Detection 功能。

**arp detection enable**

缺省情况下，ARP Detection 功能处于关闭状态，即不进行用户合法性检查。

(5) （可选）将不需要进行用户合法性检查的接口配置为 ARP 信任接口。

a. 退回系统视图。

**quit**

b. 进入接口视图。

**interface** *interface-type interface-number*

支持的接口类型包括二层以太网接口和二层聚合接口视图。

c. 将不需要进行用户合法性检查的接口配置为 ARP 信任接口。

**arp detection trust**

缺省情况下，接口为 ARP 非信任接口。

### 1.8.3 ARP 报文有效性检查

#### 1. 功能简介

对于 ARP 信任接口，不进行报文有效性检查；对于 ARP 非信任接口，需要根据配置对 MAC 地址和 IP 地址不合法的报文进行过滤。可以选择配置源 MAC 地址、目的 MAC 地址或 IP 地址检查模式。

- 源 MAC 地址的检查模式：会检查 ARP 报文中的源 MAC 地址和以太网报文头中的源 MAC 地址是否一致，一致则认为有效，否则丢弃报文；
- 目的 MAC 地址的检查模式（只针对 ARP 应答报文）：会检查 ARP 应答报文中的目的 MAC 地址是否为全 0 或者全 1，是否和以太网报文头中的目的 MAC 地址一致。全 0、全 1、不一致的报文都是无效的，需要被丢弃；
- IP 地址检查模式：会检查 ARP 报文中的源 IP 或目的 IP 地址，如全 1、或者组播 IP 地址都是不合法的，需要被丢弃。对于 ARP 应答报文，源 IP 和目的 IP 地址都进行检查；对于 ARP 请求报文，只检查源 IP 地址。

#### 2. 配置准备

配置本功能前需保证已经配置了“1.8.2 用户合法性检查”。

#### 3. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入 VLAN 视图。

**vlan** *vlan-id*

(3) 开启 ARP Detection 功能。

**arp detection enable**

缺省情况下，ARP Detection 功能处于关闭状态，即不进行报文有效性检查。

(4) 开启 ARP 报文有效性检查功能。

a. 退回系统视图。

**quit**

b. 开启 ARP 报文有效性检查功能。

**arp detection validate** { **dst-mac** | **ip** | **src-mac** } *

ARP 报文有效性检查功能处于关闭状态。

(5) （可选）将不需要进行 ARP 报文有效性检查的接口配置为 ARP 信任接口。

a. 进入接口视图。

**interface** *interface-type interface-number*

支持的接口类型包括二层以太网接口和二层聚合接口。

b. 将不需要进行 ARP 报文有效性检查的接口配置为 ARP 信任接口。

**arp detection trust**

缺省情况下，接口为 ARP 非信任接口。

## 1.8.4 ARP 报文强制转发

### 1. 功能简介

对于从 ARP 信任接口接收到的 ARP 报文不受此功能影响，按照正常流程进行转发；对于从 ARP 非信任接口接收到的并且已经通过用户合法性检查的 ARP 报文的处理过程如下：

- 对于 ARP 请求报文，通过信任接口进行转发；
- 对于 ARP 应答报文，首先按照报文中的以太网目的 MAC 地址进行转发，若在 MAC 地址表中没有查到目的 MAC 地址对应的表项，则将此 ARP 应答报文通过信任接口进行转发。

### 2. 配置限制和指导

ARP 报文强制转发功能不支持目的 MAC 地址为多端口 MAC 的情况。

### 3. 配置准备

配置本功能前需保证已经配置了“1.8.2 用户合法性检查”。

### 4. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入 VLAN 视图。

**vlan** *vlan-id*

(3) 开启 ARP 报文强制转发功能。

**arp restricted-forwarding enable**

缺省情况下，ARP 报文强制转发功能处于关闭状态。

## 1.8.5 ARP Detection 显示和维护

在完成上述配置后，在任意视图下执行 **display** 命令可以显示配置后 ARP Detection 的运行情况，通过查看显示信息验证配置的效果。

在用户视图下，用户可以执行 **reset** 命令清除 ARP Detection 的统计信息。

表1-3 ARP Detection 显示和维护

| 操作 | 命令 |
| --- | --- |
| 显示开启了ARP Detection功能的VLAN | **display arp detection** |

| 操作 | 命令 |
| --- | --- |
| 显示ARP Detection丢弃报文的统计信息 | **display arp detection statistics** [ **interface** *interface-type interface-number* ] |
| 清除ARP DetectionARP Detection的报文丢弃统计信息 | **reset arp detection statistics** [ **interface** *interface-type interface-number* ] |

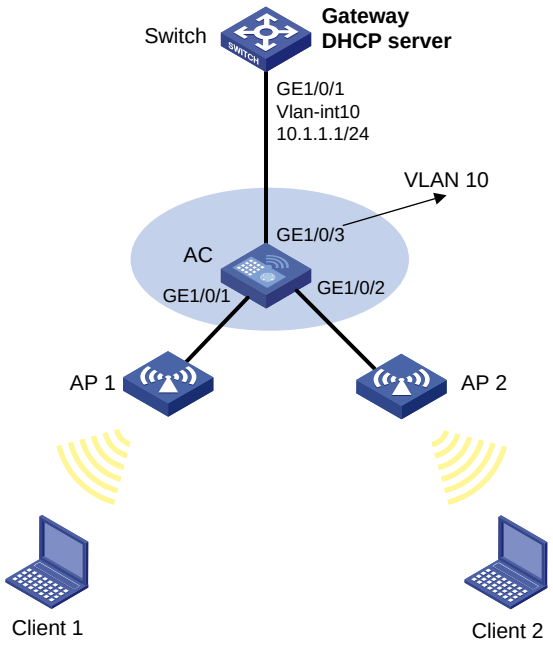
## 1.8.6 用户合法性检查配置举例

### 1. 组网需求

- Switch 是 DHCP 服务器；AC 是支持 802.1X 的设备，在 VLAN 10 内启用 ARP Detection 功能，对认证客户端进行保护，保证合法用户可以正常转发报文，否则丢弃。
- Client 1 和 Client 2 是本地 802.1X 接入用户，且支持 IP 地址上传。

### 2. 组网图

图1-4 配置用户合法性检查组网图




### 3. 配置步骤

(1) 配置组网图中所有接口属于 VLAN 及 Switch 对应 VLAN 接口的 IP 地址（略）

(2) 配置 DHCP 服务器 Switch，创建 DHCP 地址池 0

```
<Switch> system-view
[Switch] dhcp enable
[Switch] dhcp server ip-pool 0
[Switch-dhcp-pool-0] network 10.1.1.0 mask 255.255.255.0
```

(3) 配置客户端 Client 1 和 Client 2（略）。

(4) 配置 AC

# 配置 802.1X 认证方式为 CHAP。

```
<AC> system-view
[AC] dot1x authentication-method chap
```

# 配置名称为 local 的 ISP 域，并将认证、授权和计费的方式配置为本地。

```
[AC] domain local
[AC-isp-local] authentication lan-access local
[AC-isp-local] authorization lan-access local
[AC-isp-local] accounting lan-access local
[AC-isp-local] quit
```

# 配置无线服务模板，名称为 wlas_local_chap，用户认证方式为 802.1X，ISP 域为 local，SSID 为 wlas_local_chap。

```
[AC] wlan service-template wlas_local_chap
[AC-wlan-st-wlas_local_chap] client-security authentication-mode dot1x
[AC-wlan-st-wlas_local_chap] dot1x domain local
[AC-wlan-st-wlas_local_chap] ssid wlas_local_chap
```

# 使能无线服务模板。

```
[AC-wlan-st-wlas_local_chap] service-template enable
[AC-wlan-st-wlas_local_chap] quit
```

# 创建 ap1，并配置序列号。

```
[AC] wlan ap ap1 model WA4320i-ACN
[AC-wlan-ap-ap 1] serial-id 210235A1BSC123000050
[AC-wlan-ap-ap 1] quit
```

# 配置 Radio 信道为 149，并使能射频。

```
[AC] wlan ap ap1
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] channel 149
[AC-wlan-ap-ap1-radio-1] radio enable
```

# 将无线服务模板 wlas_local_chap 绑定到 radio1 上。

```
[AC-wlan-ap-ap1-radio-1] service-template wlas_local_chap
[AC-wlan-ap-ap1-radio-1] quit
[AC-wlan-ap-ap1] quit
```

# 添加本地接入用户。

```
[AC] local-user test class network
[AC-luser-network-test] service-type lan-access
[AC-luser-network-test] password simple test
[AC-luser-network-test] quit
```

# 开启 ARP Detection 功能，对用户合法性进行检查。

```
[AC] vlan 10
[AC-vlan10] arp detection enable
```

# 接口状态缺省为非信任状态，上行接口配置为信任状态，下行接口按缺省配置。

```
[AC-vlan10] interface gigabitethernet 1/0/3
[AC-GigabitEthernet1/0/3] arp detection trust
[AC-GigabitEthernet1/0/3] quit
```

#### 4. 验证配置

完成上述配置后，对于接口 GigabitEthernet1/0/1 和 GigabitEthernet1/0/2 收到的 ARP 报文，需基于 802.1X 安全表项进行用户合法性检查。

## 1.9 配置ARP自动扫描、固化功能

#### 1. 功能简介

建议在网吧这种环境稳定的小型网络中使用 ARP 自动扫描、固化功能。ARP 自动扫描功能一般与 ARP 固化功能配合使用：

- 配置 ARP 自动扫描功能后，设备会对局域网内的邻居自动进行扫描（向邻居发送 ARP 请求报文，获取邻居的 MAC 地址，从而建立动态 ARP 表项）。
- ARP 固化用来将当前的 ARP 动态表项（包括 ARP 自动扫描生成的动态 ARP 表项）转换为静态 ARP 表项。通过对动态 ARP 表项的固化，可以有效防止攻击者修改 ARP 表项。

固化后的静态 ARP 表项与配置产生的静态 ARP 表项相同。

#### 2. 配置限制和指导

- 对于已存在 ARP 表项的 IP 地址不进行扫描。
- 扫描操作可能比较耗时，用户可以通过<Ctrl_C>来终止扫描（在终止扫描时，对于已经收到的邻居应答，会建立该邻居的动态 ARP 表项）。
- 固化生成的静态 ARP 表项数量同样受到设备可以支持的静态 ARP 表项数目的限制，由于静态 ARP 表项数量的限制可能导致只有部分动态 ARP 表项被固化。
- 通过 **arp fixup** 命令将当前的动态 ARP 表项转换为静态 ARP 表项后，后续学习到的动态 ARP 表项可以通过再次执行 **arp fixup** 命令进行固化。
- 通过固化生成的静态 ARP 表项，可以通过命令行 **undo arp** *ip-address* 逐条删除，也可以通过命令行 **reset arp all** 或 **reset arp static** 全部删除。

#### 3. 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。

**interface** *interface-type interface-number*

(3) 开启 ARP 自动扫描功能。

**arp scan** [ *start-ip-address* **to** *end-ip-address* ]

(4) 退回系统视图。

**quit**

(5) 将设备上的动态 ARP 表项转化成静态 ARP 表项。

**arp fixup**

# 1.10 配置ARP网关保护功能

## 1.10.1 功能简介

在设备上不与网关相连的接口上配置此功能，可以防止伪造网关攻击。

在接口上开启此功能后，当接口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址是否和配置的被保护网关的 IP 地址相同。如果相同，则认为此报文非法，将其丢弃；否则，认为此报文合法，继续进行后续处理。

## 1.10.2 配置限制和指导

- 每个接口最多支持配置 8 个被保护的网关 IP 地址。
- 不能在同一接口下同时配置命令 **arp filter source** 和 **arp filter binding**。
- 本功能与 ARP Detection 和 ARP 快速应答功能配合使用时，先进行本功能检查，本功能检查通过后才会进行其他配合功能的处理。

## 1.10.3 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。

**interface** *interface-type interface-number*

支持的接口类型包括二层以太网接口和二层聚合接口。

(3) 开启 ARP 网关保护功能，配置被保护的网关 IP 地址。

**arp filter source** *ip-address*

缺省情况下，ARP 网关保护功能处于关闭状态。

## 1.10.4 ARP 网关保护功能配置举例

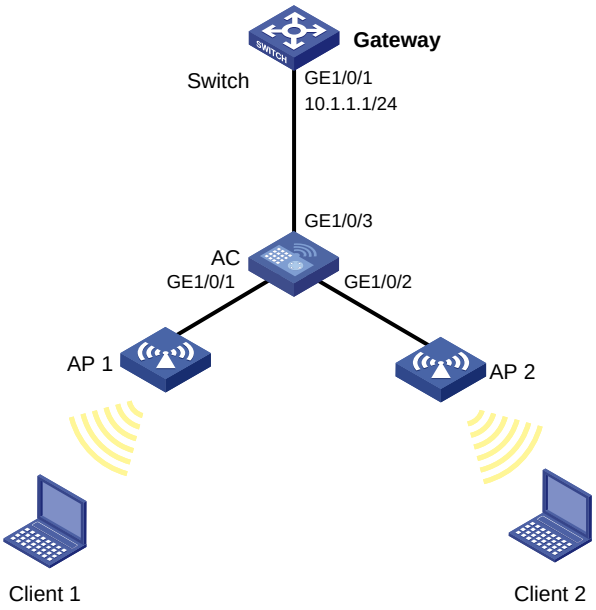
### 1. 组网需求

与 AC 相连的无线客户端 Client 2 进行了仿造网关 Switch（IP 地址为 10.1.1.1）的 ARP 攻击，接入 AC 的无线客户端 Client 1 错误地将与网关 Switch 通信的流量发往了 Client 2。

要求：通过配置防止这种仿造网关攻击。

### 2. 组网图

图1-5 配置 ARP 网关保护功能组网图




### 3. 配置步骤

# 在 AC 上配置 ARP 网关保护功能。

```
<AC> system-view
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] arp filter source 10.1.1.1
[AC-GigabitEthernet1/0/1] quit
[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] arp filter source 10.1.1.1
```

### 4. 验证配置

完成上述配置后，对于 Client 2 发送的伪造源 IP 地址为网关 IP 地址的 ARP 报文将会被丢弃，不会再被转发。

## 1.11 配置ARP过滤保护功能

### 1.11.1 功能简介

本功能用来限制接口下允许通过的 ARP 报文，可以防止仿冒网关和仿冒用户的攻击。

在接口上配置此功能后，当接口收到 ARP 报文时，将检查 ARP 报文的源 IP 地址和源 MAC 地址是否和允许通过的 IP 地址和 MAC 地址相同：

- 如果相同，则认为此报文合法，继续进行后续处理；
- 如果不相同，则认为此报文非法，将其丢弃。

### 1.11.2 配置限制和指导

- 每个接口最多支持配置 8 组允许通过的 ARP 报文的源 IP 地址和源 MAC 地址。
- 不能在同一接口下同时配置命令 **arp filter source** 和 **arp filter binding**。
- 本功能与 ARP Detection 和 ARP 快速应答功能配合使用时，先进行本功能检查，本功能检查通过后才会进行其他配合功能的处理。

### 1.11.3 配置步骤

(1) 进入系统视图。

**system-view**

(2) 进入接口视图。

**interface** *interface-type interface-number*

支持的接口类型包括二层以太网接口和二层聚合接口。

(3) 开启 ARP 过滤保护功能，配置允许通过的 ARP 报文的源 IP 地址和源 MAC 地址。

**arp filter binding** *ip-address mac-address*

缺省情况下，ARP 过滤保护功能处于关闭状态。

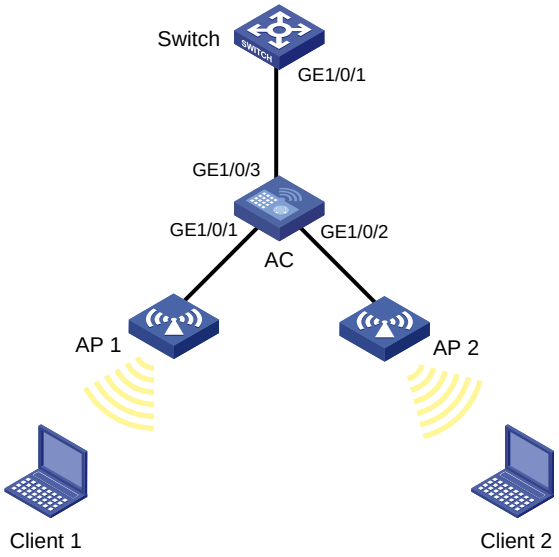
### 1.11.4 ARP 过滤保护功能配置举例

#### 1. 组网需求

- Client 1 的 IP 地址为 10.1.1.2，MAC 地址为 000f-e349-1233。
- Client 2 的 IP 地址为 10.1.1.3，MAC 地址为 000f-e349-1234。
- 限制 AC 的 GigabitEthernet1/0/1、GigabitEthernet1/0/2 接口只允许指定用户接入，不允许其他用户接入。

## 2. 组网图

图1-6 配置 ARP 过滤保护功能组网图




## 3. 配置步骤

# 配置 AC 的 ARP 过滤保护功能。

```
<AC> system-view
[AC] interface gigabitethernet 1/0/1
[AC-GigabitEthernet1/0/1] arp filter binding 10.1.1.2 000f-e349-1233
[AC-GigabitEthernet1/0/1] quit
[AC] interface gigabitethernet 1/0/2
[AC-GigabitEthernet1/0/2] arp filter binding 10.1.1.3 000f-e349-1234
```

## 4. 验证配置

完成上述配置后，接口 GigabitEthernet1/0/1 收到 Client 1 发出的源 IP 地址为 10.1.1.2、源 MAC 地址为 000f-e349-1233 的 ARP 报文将被允许通过，其他 ARP 报文将被丢弃；接口 GigabitEthernet1/0/2 收到 Client 2 发出的源 IP 地址为 10.1.1.3、源 MAC 地址为 000f-e349-1234 的 ARP 报文将被允许通过，其他 ARP 报文将被丢弃。