目 录

1 IP Source Guard ····· 1-1
1.1 IP Source Guard简介 ····· 1-1
1.2 配置IP Source Guard ····· 1-2
1.3 配置对未知源IPv4 地址客户端数据报文的处理方式 ····· 1-2
1.4 IP Source Guard典型配置举例 ····· 1-3

1 IP Source Guard

1.1 IP Source Guard简介

IP Source Guard 功能用于对 AP 收到的报文进行过滤控制，以防止非法客户端的报文通过，从而限制了对网络资源的非法使用（比如非法客户端仿冒合法客户端 IP 接入网络），提高了无线网络的安全性。

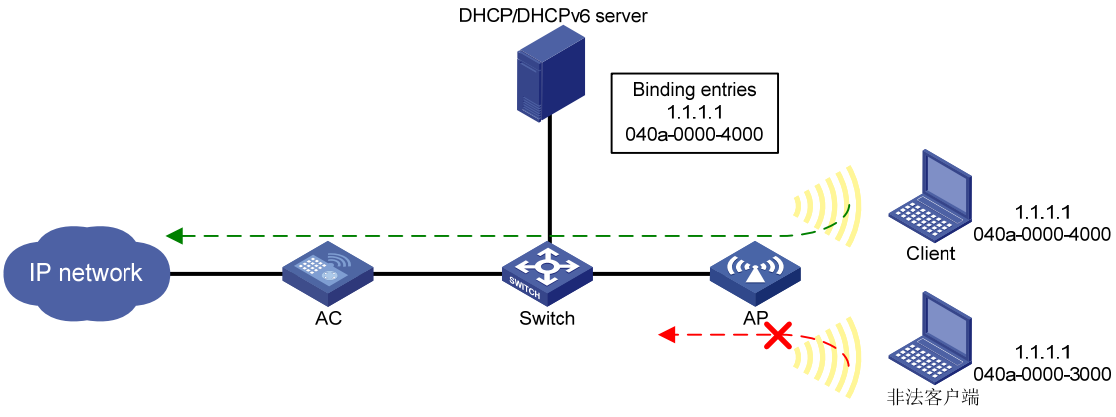
对于使用 IPv4 地址的客户端，AP 会监听客户端发送的 ARP 报文或者与 DHCP 服务器间交互的 DHCPv4 报文，从报文中获取到客户端的 IP 地址，并与客户端的 MAC 地址形成绑定表项。

对于使用 IPv6 地址的客户端，有以下两种方式可以形成绑定表项。

- DHCPv6 方式：AP 会监听客户端与 DHCPv6 服务器间交互的 DHCPv6 报文，从报文中获取到 DHCPv6 服务器为客户端分配的完整的 IPv6 地址，并与客户端的 MAC 地址形成绑定表项。如果从报文中获取到的是 DHCPv6 服务器为客户端分配的 IPv6 地址前缀，则无法与客户端的 MAC 地址形成绑定表项。
- ND（Neighbor Discovery，IPv6 邻居发现）方式：AP 会监听网络中的 RA（Router Advertisement，路由器通告消息）、NS（Neighbor Solicitation，邻居请求消息）、NA（Neighbor Advertisement，邻居通告消息）报文，从报文中获取 IPv6 地址，并与客户端的 MAC 地址形成绑定表项。

如 图 1-1 所示，开启IP Source Guard功能后，AP在收到客户端报文时，会查找IP源地址绑定表项，如果客户端发送报文的特征项（MAC地址+IP地址）与某个绑定表项匹配，则转发该报文，否则做丢弃处理。对于IPv4 地址匹配的条件，还要求客户端使用的IP地址是通过DHCP方式获取的，才转发报文，否则做丢弃处理。

图1-1 IP Source Guard 功能示意图



说明

- DHCP 功能的详细介绍请参考“三层技术配置指导”中的“DHCP”。
- DHCPv6 功能的详细介绍请参考“三层技术配置指导”中的“DHCPv6”。
- ND 功能的详细介绍请参考“三层技术配置指导”中的“IPv6 基础”。

1.2 配置IP Source Guard

IP Source Guard 功能是针对无线服务模板的，对某个无线服务模板配置了 IP Source Guard 功能后，仅对接入该无线服务模板的客户端报文进行 IP 源地址验证，通过其它无线服务模板接入的客户端不受影响。

表1-1 配置 IP Source Guard

操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-number*	-
开启IPv4源地址验证功能	**ip verify source**	缺省情况下，IPv4源地址验证功能处于关闭状态
开启IPv6源地址验证功能	**ipv6 verify source**	缺省情况下，IPv6源地址验证功能处于关闭状态

1.3 配置对未知源IPv4地址客户端数据报文的处理方式

设备开启 IP Source Guard 功能后，将通过 DHCP 方式学习到的 IPv4 地址视为已知源 IPv4 地址，将通过 ARP 方式学习到的 IPv4 地址或者未学习到的 IPv4 地址视为未知源 IPv4 地址。当设备接收到未知源 IPv4 地址客户端发送的数据报文时，可以对报文进行如下处理：

- 仅丢弃客户端的数据报文。
- 丢弃客户端的数据报文并向客户端发送解除认证报文强制其下线。

表1-2 配置对未知源 IPv4 地址客户端数据报文的处理方式

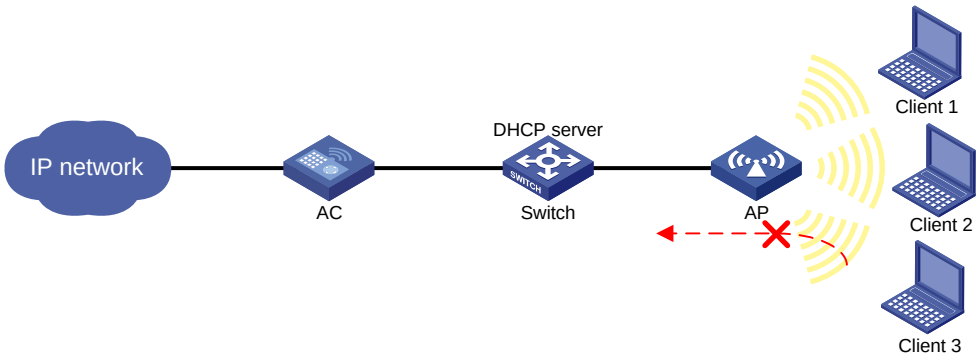
操作	命令	说明
进入系统视图	**system-view**	-
进入无线服务模板视图	**wlan service-template** *service-template-number*	-
配置对未知源IPv4地址客户端数据报文的处理方式	**ip verify unknown-ip** { **deauthenticate** | **drop** }	缺省情况下，丢弃未知源IPv4地址客户端数据报文并向客户端发送解除认证报文

1.4 IP Source Guard典型配置举例

1. 组网需求

- 如 图 1-2 所示，客户端通过名为service的SSID接入网络，Switch作为DHCP server会为接入的客户端动态分配IP地址。
- 要求对接入此 SSID 的客户端报文进行 IP 源地址验证，以防止非法客户端的报文通过。

图1-2 IPv4 源地址验证配置组网图



2. 配置步骤

创建无线服务模板 1，配置 SSID 为 service，并使能服务模版。

```
<AC> system-view
[AC] wlan service-template 1
[AC-wlan-st-1] ssid service
[AC-wlan-st-1] service-template enable
```

配置 IPv4 源地址验证功能。

```
[AC-wlan-st-1] ip verify source
[AC-wlan-st-1] quit
```

创建手工 AP，名称为 ap1，选择 AP 型号并配置序列号。

```
[AC] wlan ap ap1 model WA5320E-WiNet
[AC-wlan-ap-ap1] serial-id 219801A1FF8171E00361
```

将无线服务模板 1 绑定到 Radio 2 接口。

```
[AC-wlan-ap-ap1] radio 2
[AC-wlan-ap-ap1-radio-2] service-template 1
[AC-wlan-ap-ap1-radio-2] quit
[AC-wlan-ap-ap1] quit
```

3. 验证配置结果

Client 1（MAC 地址为 001d-0f31-87dd）和 Client 2（MAC 地址为 001c-f08f-f7f1）通过 DHCP 服务器申请到 IP 地址后，AP 上会生成 Client 1 和 Client 2 的绑定表项。当 AP 收到 Client 1 和 Client 2 发送的报文，检查绑定表项匹配后，AP 会转发这些报文，Client 3 为非法客户端（Client 3 伪造其 IP 地址为 Client 1 的 IP 地址），AP 无法查找到与其匹配的绑定表项，则会丢弃 Client 3 发送的报文。