目 录

1 用户隔离

1.1 用户隔离简介

用户隔离，即对使用同一公共无线服务或在同一 VLAN 进行通信的用户进行报文隔离，从而达到提高用户安全性、缓解设备转发压力和减少射频资源消耗的目的。

用户隔离包括基于 SSID 的用户隔离和基于 VLAN 的用户隔离：

- 基于 SSID 的用户隔离：用于隔离同一 SSID 下的无线用户。
- 基于 VLAN 的用户隔离：用于隔离同一 VLAN 内的有线用户和无线用户。

1.2 基于SSID的用户隔离

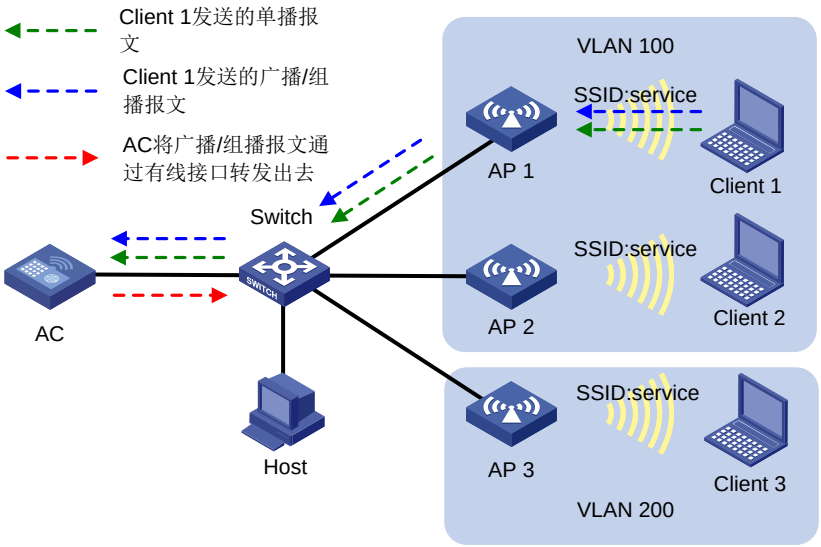
基于 SSID 的用户隔离功能适用于集中式转发和本地转发场景下，设备开启基于 SSID 的用户隔离功能后，通过该 SSID 接入无线服务且处于同一 VLAN 内的无线用户之间将不再能够互相访问。

1.2.1 集中式转发场景下基于SSID的用户隔离机制

如 图 1-1 所示，在集中式转发场景下，Client 1～Client 3 分别通过AP 1～AP 3 接入无线网络，Client 1 和Client 2 属于VLAN 100，Client 3 属于VLAN 200。在AC上开启基于SSID的用户隔离功能：

- Client 1 在 VLAN 100 内发送广播/组播报文，AC 收到广播/组播报文后，不再将广播/组播报文复制及转发给网络中的 AP，而是仅将去掉 CAPWAP 隧道封装的报文通过有线接口转发给 Switch。
- Client 1 在 VLAN 100 内向 Client 2 发送单播报文，AC 收到单播报文后，不将报文转发给 AP 2，而是直接丢弃该单播报文。

图1-1 集中式转发场景下报文路径转发示意图



1.2.2 本地转发场景下基于SSID的用户隔离机制

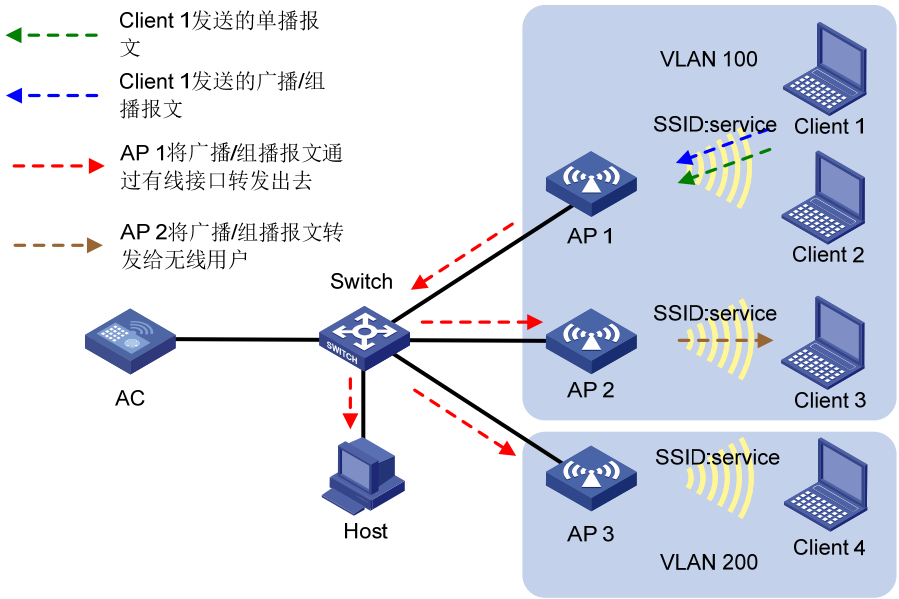
说明

该机制仅隔离同一 AP 下的无线客户端。

如 图 1-2 所示，在本地转发场景下，Client 1～Client 4 分别通过AP 1～AP 3 接入无线网络，Client 1～Client 3 属于VLAN 100，Client 4 属于VLAN 200。在AP 1 上开启基于SSID的用户隔离功能：

- Client 1 在 VLAN 100 内发送广播/组播报文，AP 1 收到广播/组播报文后，仅将报文通过有线接口转发给同一 VLAN 内的有线网络用户 AP 2、AP 3 和 Host，不再将报文转发给无线用户 Client 2。AP 2 接收到报文后转发给无线用户 Client 3，AP 3 接收到报文后不会将其转发给 Client 4。
- Client 1 在 VLAN 100 内向 Client 2 发送单播报文，AP 1 收到单播报文后，不将报文转发给 Client 2，而是直接丢弃该单播报文。

图1-2 本地转发场景下报文路径转发示意图



1.3 基于VLAN的用户隔离

基于VLAN的用户隔离功能适用于集中式转发和本地转发场景下，设备在指定VLAN内开启该功能后，该VLAN内的有线用户之间、有线用户和无线用户之间以及无线用户之间（无论无线用户是否使用同一SSID接入WLAN网络）的互相访问将按照 表 1-1 的机制进行隔离。

表1-1 基于 VLAN 的用户隔离处理机制

数据报文转发方式	收到单播报文	收到广播/组播报文
集中式转发	AC直接丢弃该单播报文	AC仅将报文转发给同一VLAN内的有线用户，不向同一VLAN内的无线用户转发

数据报文转发方式	收到单播报文	收到广播/组播报文
本地转发	Fit AP直接丢弃该单播报文	Fit AP仅将报文通过有线接口转发给同一VLAN内的有线或无线用户，不向同一VLAN内通过该AP接入的无线用户转发

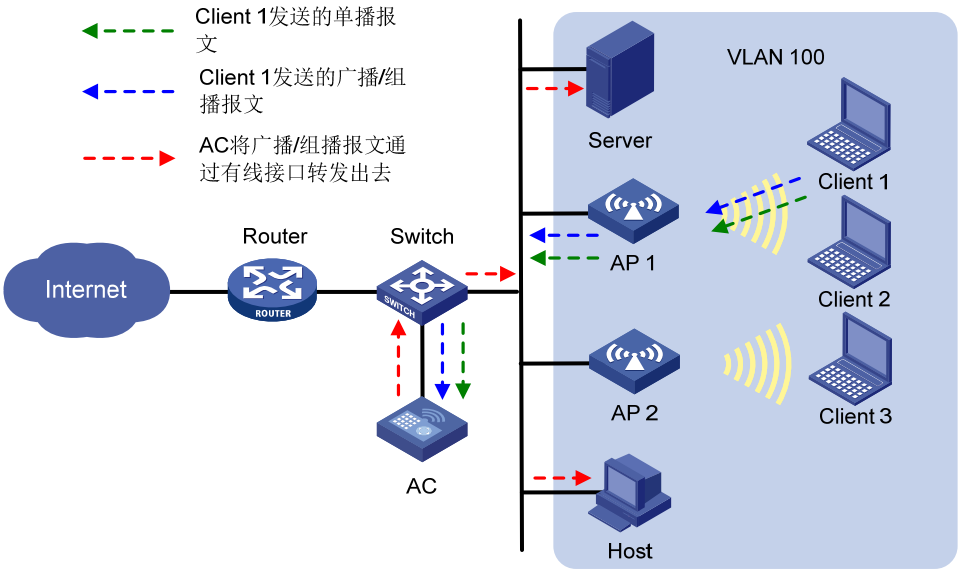
1.3.1 集中式转发场景下基于VLAN的用户隔离机制

1. AC接收无线用户发送的报文

如 图 1-3 所示，在集中式转发场景下，无线用户Client 1 和Client 2 通过AP 1 接入无线网络，Client 3 通过AP 2 接入无线网络，Client 1～Client 3 和有线用户Server、Host都属于VLAN 100。在AC上开启基于VLAN的用户隔离功能：

- Client 1 在 VLAN 100 内发送广播/组播报文，AC 收到广播/组播报文后，不再将广播/组播报文复制及转发给网络中的 AP，而是仅将去掉 CAPWAP 隧道封装的报文通过有线接口转发给同一 VLAN 内的有线用户 Host 和 Server。
- Client 1 在 VLAN 100 内向 Client 3 发送单播报文，AC 收到单播报文后，不将报文转发给 AP 2，而是直接丢弃该单播报文。

图1-3 无线用户报文路径转发示意图

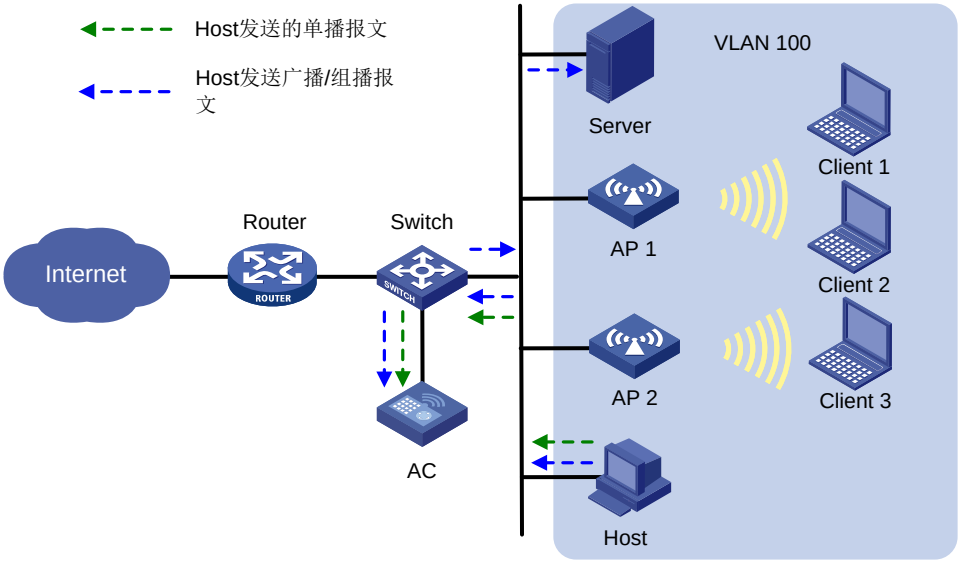


2. AC接收有线用户发送的报文

如 图 1-4 所示，在集中式转发场景下，无线用户Client 1 和Client 2 通过AP 1 接入无线网络，Client 3 通过AP 2 接入无线网络，Client 1～Client 3 和有线用户Server、Host都属于VLAN 100。在AC上开启基于VLAN的用户隔离功能：

- Host 在 VLAN 100 内发送广播/组播报文，该报文转发到有线网络用户 Server 和 AC，AC 收到该广播/组播报文后不再将广播/组播报文进行 CAPWAP 封装及转发给 AP，而是直接丢弃。
- Host 在 VLAN 100 内向 Client 3 发送单播报文，AC 收到单播报文后，不将报文转发给 AP 2，而是直接丢弃该单播报文。

图1-4 有线用户报文路径转发示意图



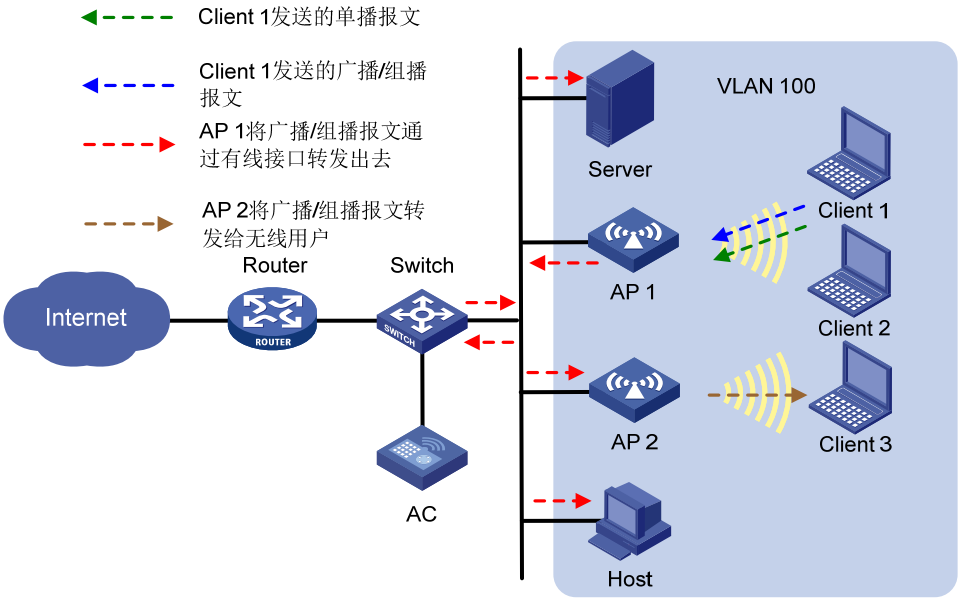
1.3.2 本地转发场景下基于VLAN的用户隔离机制

1. Fit AP接收无线用户发送的报文

如 图 1-5 所示，在本地转发场景下，无线用户Client 1 和Client 2 通过AP 1 接入无线网络，Client 3 通过AP 2 接入无线网络，Client 1～Client 3 和有线用户Server、Host都属于VLAN 100。在AP 1 上开启基于VLAN的用户隔离功能：

- Client 1 在 VLAN 100 内发送广播/组播报文，AP 1 接收到该报文后仅将报文通过有线接口转发给同一 VLAN 内的有线网络用户 Server、AP 2 和 Host。AP 2 接收到报文后转发给无线用户 Client 3，而 AP 1 不再将报文转发给无线用户 Client 2。
- Client 1 在 VLAN 100 内向 Client 3 发送单播报文，AP 1 收到单播报文后，不将报文转发给 AP 2，而是直接丢弃该单播报文。

图1-5 无线用户报文路径转发示意图

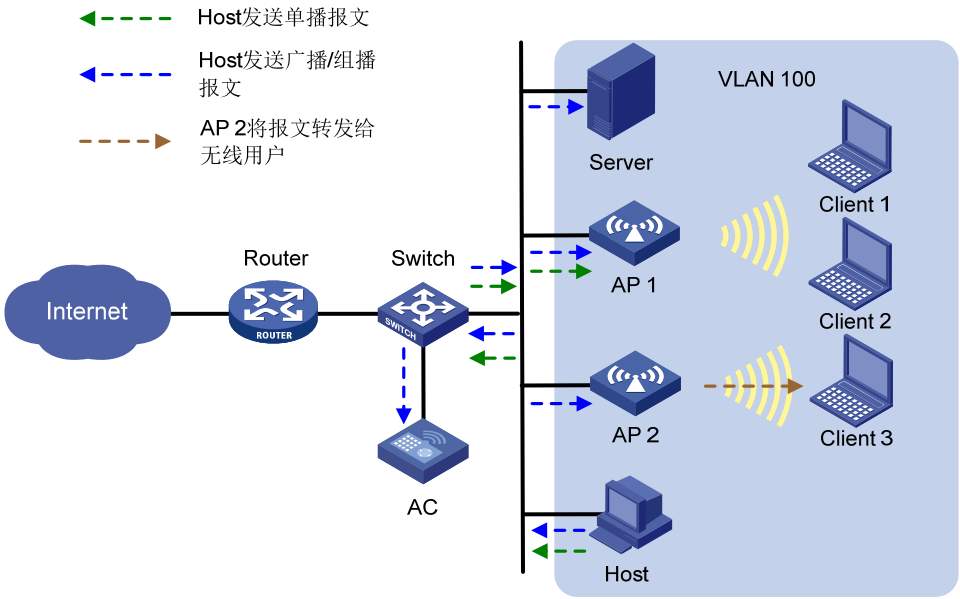


2. Fit AP接收有线用户发送的报文

如 图 1-6 所示，在本地转发场景下，无线用户Client 1 和Client 2 通过AP 1 接入无线网络，Client 3 通过AP 2 接入无线网络，Client 1～Client 3 和有线用户Server、Host都属于VLAN 100。在AP 1 上开启基于VLAN的用户隔离功能：

- Host 在 VLAN 100 内发送广播/组播报文，该报文由 Switch 转发到有线网络 Server、AC、AP 1 和 AP 2。AP 1 接收到报文后不再将广播报文转发给无线用户 Client 1 和 Client 2，而是直接丢弃；AP 2 接收到报文后转发给无线用户 Client 3。
- Host 在 VLAN 100 内向 Client 1 发送单播报文，AP 1 收到单播报文后，不将报文转发给 Client 1，而是直接丢弃该单播报文。

图1-6 有线用户报文路径转发示意图



1.4 配置基于SSID的用户隔离功能

表1-2 开启基于 SSID 的用户隔离功能

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-name*	-
开启基于SSID的用户隔离功能	**user-isolation enable**	缺省情况下，基于SSID的用户隔离功能处于关闭状态 可通过**display wlan service-template**查看基于SSID用户隔离的开启状态。关于该命令的详细介绍，请参见“WLAN命令参考”中的“WLAN接入”

1.5 配置基于VLAN的用户隔离功能

1.5.1 配置限制和指导

为了避免在指定 VLAN 上开启用户隔离功能后，出现通过用户网关无法访问外部网络的情况，必须先将该网关的 MAC 地址加入到用户隔离允许列表中，再开启该 VLAN 的用户隔离功能。

基于 VLAN 的用户隔离功能适用于集中式转发和本地转发应用场景：

- 在集中式转发应用场景下，仅需要直接在 AC 上开启该功能。

- 在本地转发应用场景下，需要通过 **map-configuration** 命令在 AC 上指定 AP 的配置文件来开启该功能。关于配置文件的相关介绍和配置，请参见“WLAN 配置指导”中的“WLAN 接入”。

1.5.2 配置步骤

表1-3 配置基于 VLAN 的用户隔离

操作	命令	说明
进入系统视图	**system-view**	-
（可选）配置指定VLAN的MAC地址允许转发列表	**user-isolation vlan** *vlan-list* **permit-mac** *mac-list*	缺省情况下，未配置指定VLAN的MAC地址允许转发列表 设备接收到该用户发送的单播/广播/组播报文或其他用户发送向该用户的单播报文可以正常进行转发
开启指定VLAN的用户隔离功能	**user-isolation vlan** *vlan-list* **enable** [**permit-unicast**]	缺省情况下，基于VLAN的用户隔离功能处于关闭状态 若指定**permit-unicast**参数，则允许该VLAN内所有用户的单播报文正常转发
（可选）配置允许转发指定VLAN内有线用户发送给无线用户的广播和组播报文	**user-isolation permit-broadcast**	缺省情况下，隔离有线用户发往无线用户的广播和组播报文

1.6 用户隔离显示与维护

在完成上述配置后，在任意视图下执行 **display** 命令可以查看显示信息验证配置的效果。

表1-4 用户隔离显示与维护

操作	命令
显示基于VLAN的用户隔离统计信息	**display user-isolation statistics** [**vlan** *vlan-id*]
清除基于VLAN的用户隔离统计信息	**reset user-isolation statistics** [**vlan** *vlan-id*]

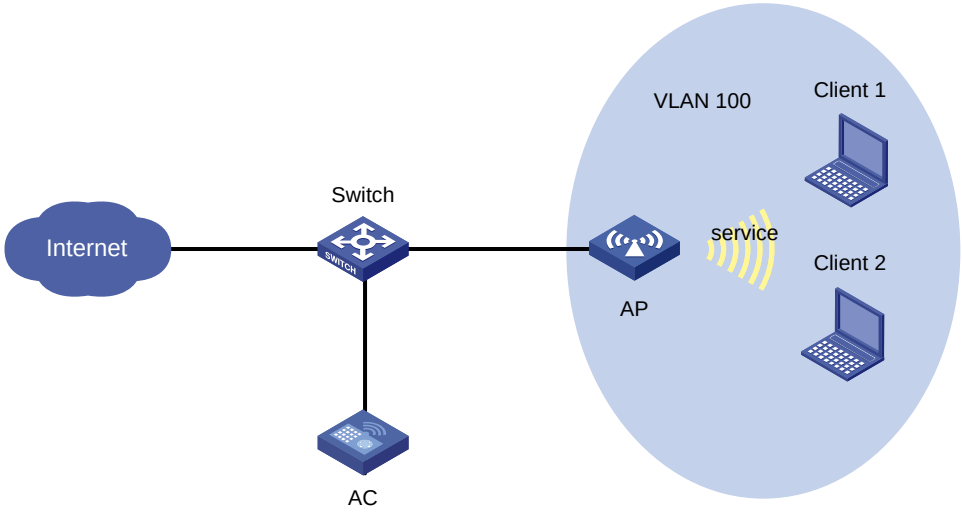
1.7 用户隔离典型配置举例

1.7.1 集中式转发场景下基于SSID的用户隔离

1. 组网需求

在集中式转发场景下，通过配置基于 SSID 的用户隔离，实现用户 Client 1 和 Client 2 可以通过同一个 SSID 访问网络，但是两者不能相互访问。

图1-7 集中式转发场景下基于 SSID 的用户隔离组网图



2. 配置步骤

配置 Client1 和 Client 2 通过无线网络接入 Internet。

配置步骤可参见“WLAN 配置指导”中的“AP 管理”和“WLAN 接入”，具体配置步骤略。

开启基于 SSID 的用户隔离功能。

```
<AC> system-view
[AC] wlan service-template service
[AC-wlan-st-service] user-isolation enable
[AC-wlan-st-service] quit
```

3. 验证配置

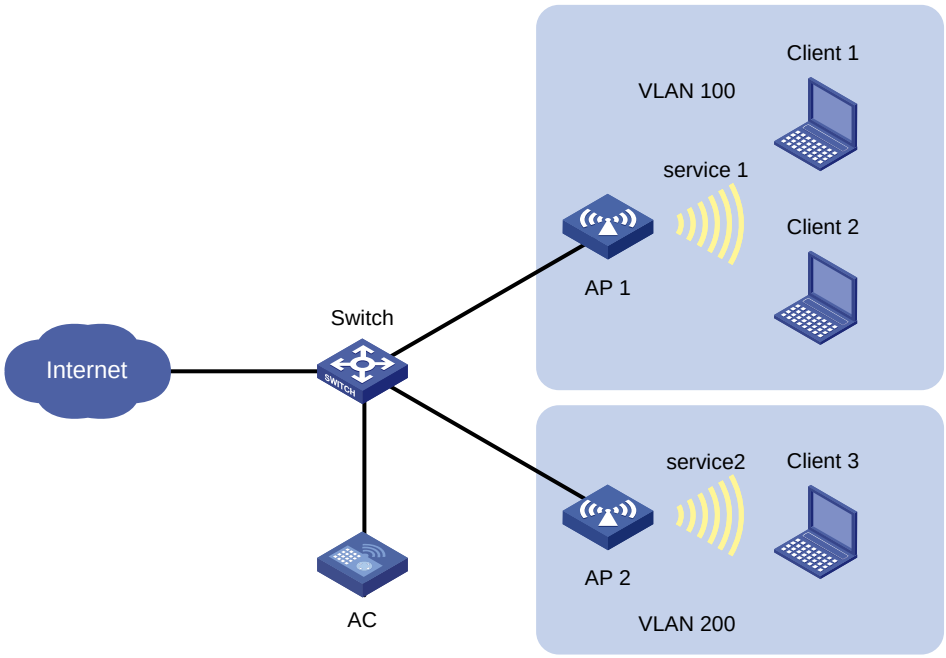
用户 Client 1 和 Client 2 都可以访问 Internet，但是不能相互访问。

1.7.2 本地转发场景下基于SSID的用户隔离

1. 组网需求

在本地转发场景下，通过配置基于 SSID 的用户隔离，实现用户 Client 1 和 Client 2 可以通过同一个 SSID 访问网络，但是两者不能相互访问。

图1-8 本地转发场景下基于 SSID 的用户隔离组网图



2. 配置步骤

配置 Client1 和 Client 2 通过无线网络接入 Internet。

配置步骤可参见“WLAN 配置指导”中的“AP 管理”和“WLAN 接入”，具体配置步骤略。

开启基于 SSID 的用户隔离功能。

```
<AC> system-view
[AC] wlan service-template service1
[AC-wlan-st-service1] user-isolation enable
[AC-wlan-st-service1] quit
```

3. 验证配置

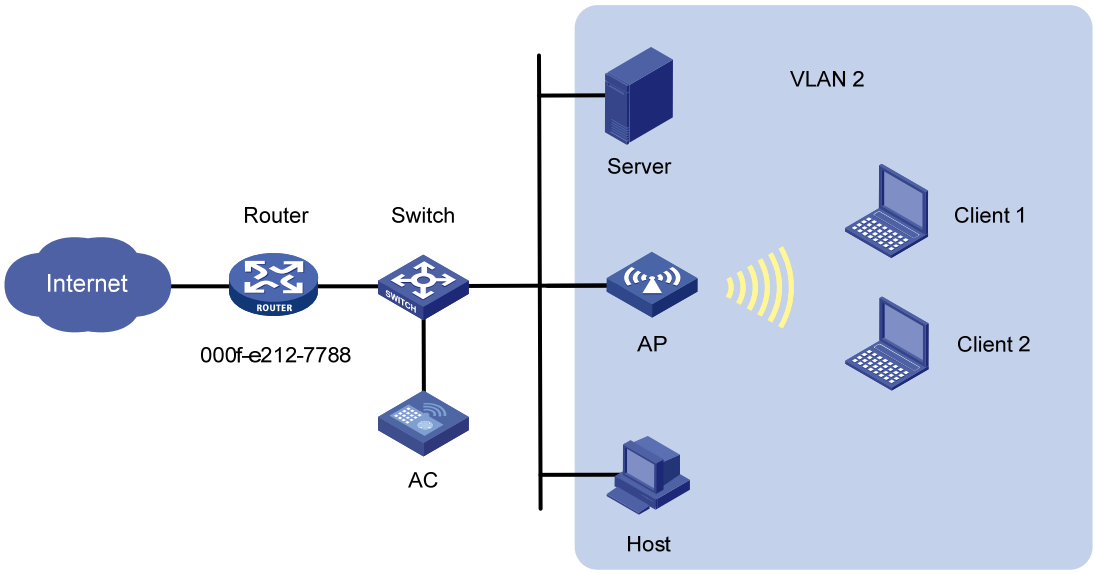
用户 Client 1 和 Client 2 都可以访问 Internet，但是不能相互访问。

1.7.3 集中式转发场景下基于VLAN的用户隔离

1. 组网需求

在集中式转发场景下，如 图 1-9 所示VLAN 2 用户的网关Router的MAC地址为 000f-e212-7788，通过配置基于VLAN的用户隔离，将网关的MAC地址加入到允许转发列表，实现VLAN 2 中的无线用户Client 1、Client 2 和有线用户Host、Server可以访问Internet。

图1-9 集中式转发场景下基于 VLAN 的用户隔离配置组网图



2. 配置步骤

配置 Client1 和 Client 2 通过无线网络接入 Internet。

配置步骤可参见“WLAN 配置指导”中的“AP 管理”和“WLAN 接入”，具体配置步骤略。

将 Router 与 AC 连接侧接口的 MAC 地址 000f-e212-7788 加入 VLAN 2 的允许转发列表。

```
<AC> system-view
[AC] user-isolation vlan 2 permit-mac 000f-e212-7788
```

在 VLAN 2 上开启基于 VLAN 的用户隔离功能。

```
[AC] user-isolation vlan 2 enable
```

3. 验证结果

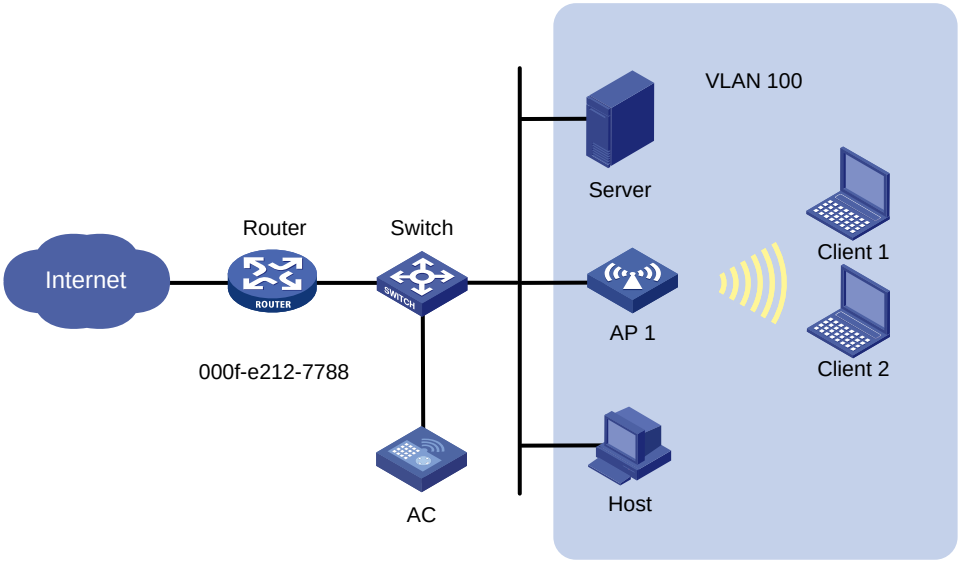
VLAN 2 中的用户 Client 1、Client 2、Host 和 Server 可以访问 Internet，但是不可以相互访问。

1.7.4 本地转发场景下基于VLAN的用户隔离配置举例

1. 组网需求

在本地转发场景下，如 图 1-10 所示VLAN 100 用户的网关Router的MAC地址为 000f-e212-7788，在AP 1 上配置基于VLAN的用户隔离，将网关的MAC地址加入到允许转发列表，实现VLAN 100 中的无线用户Client 1、Client 2 可以访问Internet。

图1-10 本地转发场景下基于 VLAN 的用户隔离配置组网图



2. 配置步骤

说明

AP 配置文件 apcfg.txt 的内容，要求为文本文件，按照命令行配置的顺序编写文本文件上传至 AC 即可，AC 与 AP 关联后，通过 **map-configuration** 命令下发至 AP 生效。从而完成对 AP 的配置。

配置 Client1 和 Client 2 通过无线网络接入 Internet。

配置步骤可参见“WLAN 配置指导”中的“AP 管理”和“WLAN 接入”，具体配置步骤略。

配置 apcfg.txt 配置文件，将 Router 与 AC 连接侧接口的 MAC 地址 000f-e212-7788 加入 VLAN 100 的允许转发列表，然后开启基于 VLAN 的用户隔离功能。

```
system-view
user-isolation vlan 100 permit-mac 000f-e212-7788
user-isolation vlan 100 enable
```

在 AC 上将配置文件 apcfg.txt 下发到 AP。

```
<AC> system-view
[AC] wlan ap ap1 model WA5320E-WiNet
[AC-wlan-ap-ap1] map-configuration apcfg.txt
```

3. 验证结果

VLAN 100 中的用户 Client 1 和 Client 2 可以访问 Internet。