目 录

1 系统功能配置举例

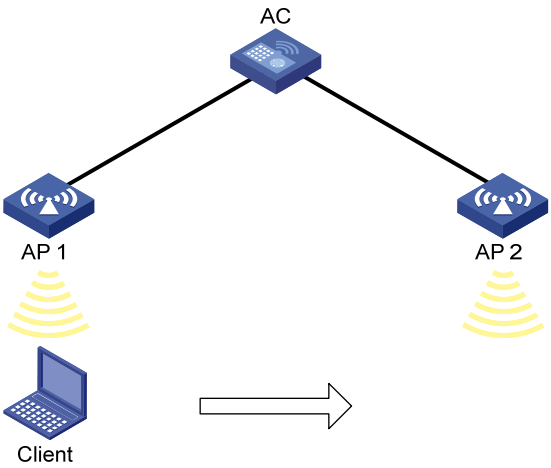
1.1 网络配置功能配置举例

1.1.1 AC内漫游配置举例

1. 组网需求

如 图 1-1 所示，仅有一台AC，要求客户端在AC内的不同AP间进行漫游。

图1-1 AC 内漫游配置组网图



2. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线网络”，进入“无线网络”页面配置无线服务，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 roaming。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。

3. 验证配置

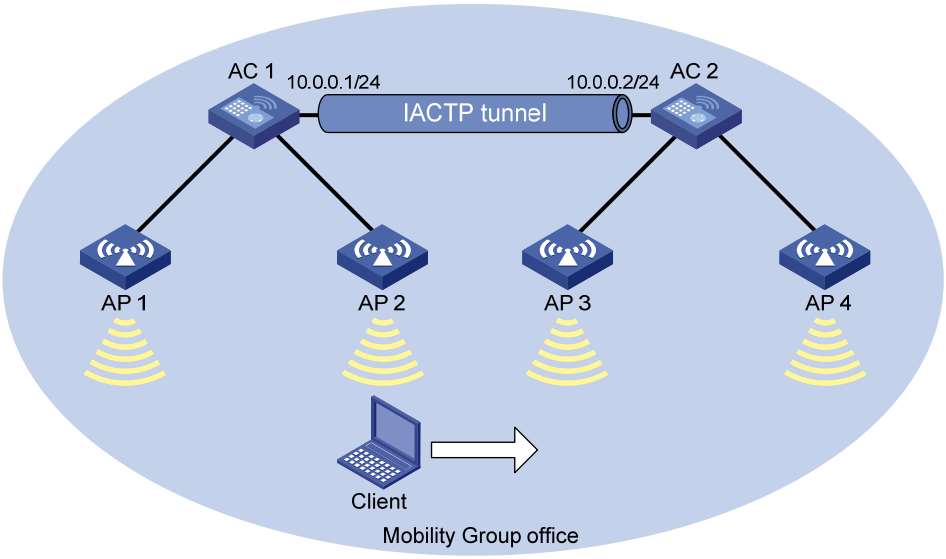
单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 漫游”，进入“漫游”页面查看客户端漫游前和漫游后所关联的 AC 和 AP。

1.1.2 AC间漫游配置举例

1. 组网需求

如 图 1-2 所示，在一个无线网络中，有两台AC，现要求客户端可以在AC内漫游，也可以跨AC漫游。

图1-2 AC 间漫游配置组网图



2. 配置步骤

(1) 配置 AC 1

配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线网络”，进入“无线网络”页面配置无线服务，配置步骤为：

- 创建一个无线服务，名称为 service 的。
- 配置 SSID 为 roaming。
- 开启无线服务。

配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。

配置漫游组

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 漫游”，进入“漫游”页面配置漫游，配置步骤为：

- 创建名称为 office 的漫游组。
- 选择隧道 IP 地址类型为 IPv4。
- 选择隧道的源 IPv4 地址为 10.0.0.1。
- 添加漫游组成员 IPv4 地址为 10.0.0.2。

- 配置漫游组状态为开启。

(2) 配置 AC 2

配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线网络”，进入“无线网络”页面配置无线服务，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 roaming。
- 开启无线服务。

配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 进入 AP 3 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 3 的射频。
- 进入 AP 4 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 4 的射频。

配置漫游组

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 漫游”，进入“漫游”页面配置漫游，配置步骤为：

- 创建名称为 office 的漫游组。
- 选择隧道 IP 地址类型为 IPv4。
- 选择隧道的源 IPv4 地址为 10.0.0.2。
- 添加漫游组成员 IPv4 地址为 10.0.0.1。
- 配置漫游组状态为开启。

3. 验证配置

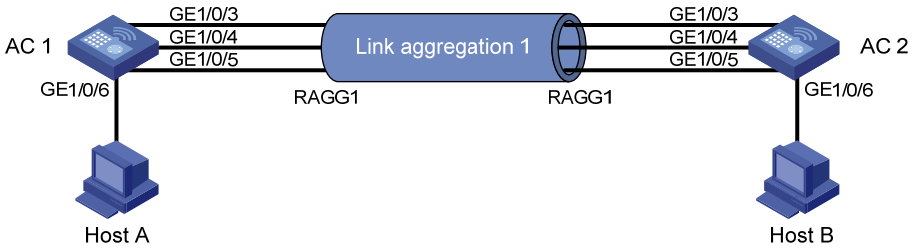
单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 漫游”，进入“漫游”页面查看客户端漫游前和漫游后所关联的 AC 和 AP。

1.1.3 二层以太网静态链路聚合配置举例

1. 组网需求

- AC 1 与 AC 2 通过各自的二层以太网接口 GigabitEthernet1/0/3～GigabitEthernet1/0/5 相互连接。
- 在 AC 1 和 AC 2 上分别配置二层静态链路聚合组，以提高链路的可靠性。

图1-3 以太网链路聚合配置组网图



2. 配置步骤

(1) 配置以太网链路聚合

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 接口”，进入“链路聚合”页面配置链路聚合，配置步骤为：

- 在 AC 1 上添加二层聚合组 1，指定聚合模式为静态聚合，将接口 GigabitEthernet1/0/3～GigabitEthernet1/0/5 加入到该聚合组中。
- AC 2 配置与 AC 1 相同。

(2) 配置 VLAN

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN，配置步骤为：

- 在 AC 1 上创建 VLAN 10。进入 VLAN 10 的详情页面，将与 Host A 相连的接口 GigabitEthernet1/0/6 加入 VLAN 10 的 Untagged 端口列表，将接口 GigabitEthernet1/0/3～GigabitEthernet1/0/5 加入 VLAN 10 的 Tagged 端口列表。
- AC 2 配置与 AC 1 相同。

3. 验证配置

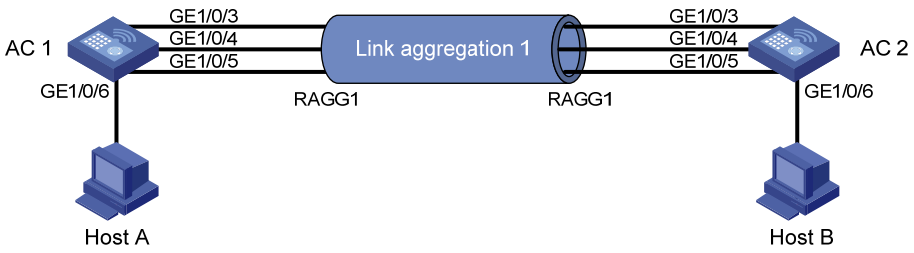
完成上述配置后，在“链路聚合”页面中可以看到 GigabitEthernet1/0/3～GigabitEthernet1/0/5 已经加入到静态聚合组 1。Host A 能够 Ping 通 Host B。AC 1 与 AC 2 之间的一条链路故障后，Host A 仍然能够 Ping 通 Host B。

1.1.4 二层以太网动态链路聚合配置举例

1. 组网需求

- AC 1 与 AC 2 通过各自的二层以太网接口 GigabitEthernet1/0/3～GigabitEthernet1/0/5 相互连接。
- 在 AC 1 和 AC 2 上分别配置二层动态链路聚合组，以提高链路的可靠性。

图1-4 以太网链路聚合配置组网图



2. 配置步骤

(1) 配置以太网链路聚合

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 接口”，进入“链路聚合”页面配置链路聚合，配置步骤为：

- 在 AC 1 上添加二层聚合组 1，指定聚合模式为动态聚合，将接口 GigabitEthernet1/0/3～GigabitEthernet1/0/5 加入到该聚合组中。

- AC 2 配置与 AC 1 相同。

(2) 配置 VLAN

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN，配置步骤为：

- 在 AC 1 上创建 VLAN 10。进入 VLAN 10 的详情页面，将与 Host A 相连的接口 GigabitEthernet1/0/6 加入 VLAN 10 的 Untagged 端口列表，将接口 GigabitEthernet1/0/3～GigabitEthernet1/0/5 加入 VLAN 10 的 Tagged 端口列表。
- AC 2 配置与 AC 1 相同。

3. 验证配置

完成上述配置后，在“链路聚合”页面中可以看到 GigabitEthernet1/0/3～GigabitEthernet1/0/5 已经加入到动态聚合组 1。Host A 能够 Ping 通 Host B。AC 1 与 AC 2 之间的一条链路故障后，Host A 仍然能够 Ping 通 Host B。

1.1.5 PPPoE Client配置举例

1. 组网需求

AC 作为 PPPoE 客户端通过 GigabitEthernet 1/0/1 连接到网络，要求：

- PPPoE 服务器与设备路由可达，GigabitEthernet 1/0/1 为三层物理口。
- PC 通过 Telnet 设备的 GE1/0/2 IP 连接到 Web 页面。

图1-5 PPPoE Client 组网图

2. 配置步骤

说明

- “链路空闲超时断线”中所设置的空闲时长为发报文空闲时长。
- 配置 PPPoE 客户端时需要勾选“删除该接口已存在的配置”选项，请根据实际情况选择合理三层物理接口。
- 完成 PPPoE 配置后请勿为该接口配置静态地址或者通过 DHCP 方式获取地址。

PPPoE 服务器为设备分配用户名和密码。（略）

配置 PPPoE 客户端。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 接口”，进入“接口”页面后，点击上方“PPPoE 配置”页签，进入 PPPoE 配置页面。配置步骤为：

(1) 点击左侧 按钮，进入添加配置页面。

(2) 选择需配置的三层物理接口，组网中为 GigabitEthernet 1/0/1。

(3) 输入用户名和密码，并选择在线方式。

(4) 选择开启 NAT 地址转换功能和删除该接口已存在的地址配置，并点击<确定>按钮，完成配置。

3. 验证配置

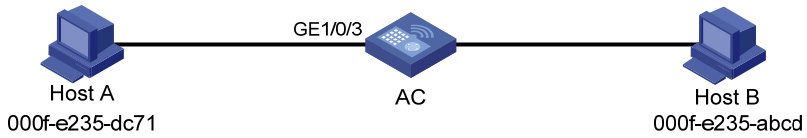
完成上述配置，可通过配置静态路由信息，并进行发送报文，查看流量信息进行验证。

1.1.6 MAC地址配置举例

1. 组网需求

- 现有一台用户主机 Host A，它的 MAC 地址为 000f-e235-dc71，属于 VLAN 1，连接 AC 的端口 GigabitEthernet1/0/3。为防止假冒身份的非法用户骗取数据，在设备的 MAC 地址表中为该用户主机添加一条静态表项。
- 另有一台用户主机 Host B，它的 MAC 地址为 000f-e235-abcd，属于 VLAN 1。由于该用户主机曾经接入网络进行非法操作，为了避免此种情况再次发生，在设备上添加一条黑洞 MAC 地址表项，使该用户主机接收不到报文。
- 配置设备的动态 MAC 地址表项老化时间为 500 秒。

图1-6 MAC 地址配置组网图



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“MAC”页面配置 MAC 地址，配置步骤为：

- 增加一条静态 MAC 地址表项，MAC 地址为 000f-e235-dc71，出接口为 GigabitEthernet1/0/3，且该接口属于 VLAN 1。
- 增加一条黑洞 MAC 地址表项，MAC 地址为 000f-e235-abcd，属于 VLAN 1。
- 进入配置页面，配置动态 MAC 地址表项的老化时间为 500 秒。

3. 验证配置

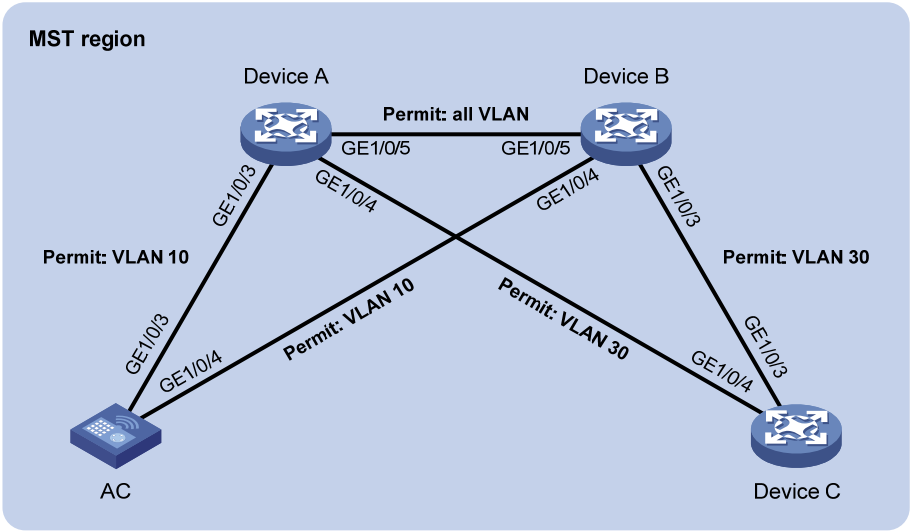
完成上述配置后，在“MAC 地址表”页面中可以看到已经创建的 MAC 地址表项，并且 Host B 无法 Ping 通 Host A。

1.1.7 MSTP配置举例

1. 组网需求

- 网络中所有设备都属于同一个 MST 域。Device A 和 Device B 为汇聚层设备，AC 和 Device C 为接入层设备。
- 通过配置 MSTP，使不同 VLAN 的报文按照不同的 MSTI 转发：VLAN 10 的报文沿 MSTI 1 转发，VLAN 30 沿 MSTI 2 转发。

图1-7 MSTP 配置组网图



2. 配置步骤

(1) 配置 VLAN

对于 AC 设备，单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN。

- Device A 上的配置：
  - 创建 VLAN 10 和 VLAN 30。
  - 进入 VLAN 10 的详情页面，将接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 加入 VLAN 10 的 Tagged 端口列表。
  - 进入 VLAN 30 的详情页面，将接口 GigabitEthernet1/0/4 和 GigabitEthernet1/0/5 加入 VLAN 30 的 Tagged 端口列表。
- Device B 上的配置：
  - 创建 VLAN 10 和 VLAN 30。
  - 进入 VLAN 10 的详情页面，将接口 GigabitEthernet1/0/4 和 GigabitEthernet1/0/5 加入 VLAN 10 的 Tagged 端口列表。
  - 进入 VLAN 30 的详情页面，将接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/5 加入 VLAN 30 的 Tagged 端口列表。
- AC 上的配置：
  - 创建 VLAN 10。
  - 进入 VLAN 10 的详情页面，将接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 加入 VLAN 10 的 Tagged 端口列表。
- Device C 上的配置：
  - 创建 VLAN 30。
  - 进入 VLAN 30 的详情页面，将接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 加入 VLAN 30 的 Tagged 端口列表。

(2) 配置 MSTP

对于 AC 设备，单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“STP”页面配置 MSTP，配置步骤为：

- Device A～Device C 和 AC 上开启 STP 功能，设置工作模式为 MSTP。
- Device A～Device C 和 AC 上，在域设置页面，配置 MST 域的域名为 Web，将 VLAN 10、30 分别映射到 MSTI 1、2 上，并配置 MSTP 的修订级别为 0。

3. 验证配置

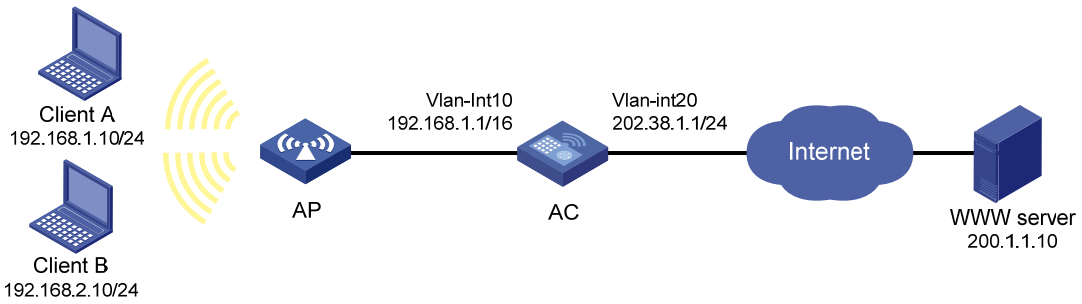
完成上述配置后，在生成树状态中可以看到各个接口的端口角色、端口状态等信息。

1.1.8 内网用户通过NAT地址访问外网（动态地址转换）

1. 组网需求

- 某公司内网使用的 IP 地址为 192.168.0.0/16。
- 该公司拥有 202.38.1.2 和 202.38.1.3 两个外网 IP 地址。
- 需要实现，内部网络中 192.168.1.0/24 网段的用户可以访问 Internet，其它网段的用户不能访问 Internet。使用的外网地址为 202.38.1.2 和 202.38.1.3。

图1-8 内网用户通过 NAT 访问外网



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > NAT”，进入“NAT”页面，单击“动态转换”后进行配置，配置步骤为：

- 添加 NAT 动态转换规则，并指定 ACL 2000，该 ACL 仅允许源 IP 地址为 192.168.1.0、通配符掩码为 0.0.0.255 的网段的用户进行地址转换。
- 添加编号为 0 的 NAT 地址组，起始地址为 202.38.1.2，结束地址为 202.38.1.3。
- 在接口 Vlan-interface20 上应用上述的 NAT 动态转换规则。

3. 验证配置

以上配置完成后，Client A 能够访问 WWW server，Client B 无法访问 WWW server。

1.1.9 外网用户通过外网地址访问内网服务器

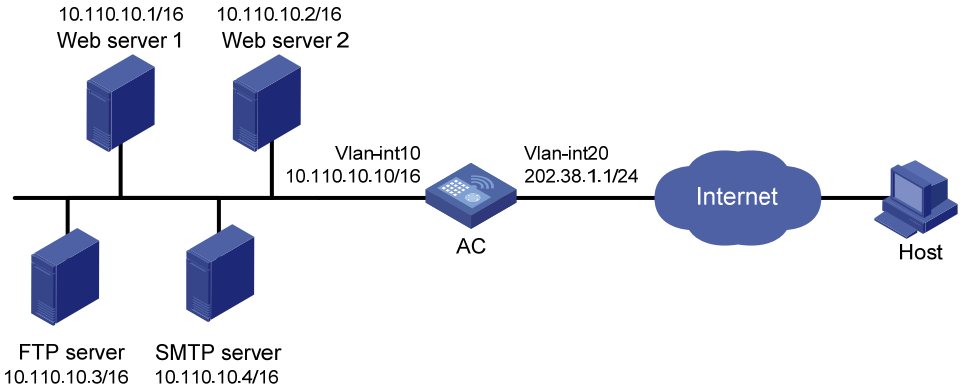
1. 组网需求

某公司内部对外提供 Web、FTP 和 SMTP 服务，而且提供两台 Web 服务器。公司内部网址为 10.110.0.0/16。其中，内部 FTP 服务器地址为 10.110.10.3/16，内部 Web 服务器 1 的 IP 地址为

10.110.10.1/16，内部 Web 服务器 2 的 IP 地址为 10.110.10.2/16，内部 SMTP 服务器 IP 地址为 10.110.10.4/16。公司拥有 202.38.1.1 至 202.38.1.3 三个公网 IP 地址。需要实现如下功能：

- 外部的主机可以访问内部的服务器。
- 选用 202.38.1.1 作为公司对外提供服务的 IP 地址，Web 服务器 2 对外采用 8080 端口。

图1-9 外网用户通过外网地址访问内网服务器



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > NAT”，进入“NAT”页面，单击“内部服务器”后进行配置，配置步骤为：

- 选择接口 Vlan-interface20。
- 添加 NAT 内部 FTP 服务器，指定 IP 协议类型为 TCP，映射方式为“外网地址单一，未使用外网端口或外网端口单一”，外网 IP 地址为 202.38.1.1，端口号为 21；内部服务器 IP 地址为 10.110.10.3，端口号为 21。
- 添加 NAT 内部 Web 服务器 1，指定 IP 协议类型为 TCP，映射方式为“外网地址单一，未使用外网端口或外网端口单一”，外网 IP 地址为 202.38.1.1，端口号为 80；内部服务器 IP 地址为 10.110.10.1，端口号为 80。
- 添加 NAT 内部 Web 服务器 2，指定 IP 协议类型为 TCP，映射方式为“外网地址单一，未使用外网端口或外网端口单一”，外网 IP 地址为 202.38.1.1，端口号为 80；内部服务器 IP 地址为 10.110.10.2，端口号为 80。
- 添加 NAT 内部 SMTP 服务器，指定 IP 协议类型为 TCP，映射方式为“外网地址单一，未使用外网端口或外网端口单一”，外网 IP 地址为 202.38.1.1，端口号为 25；内部服务器 IP 地址为 10.110.10.4，端口号为 25。

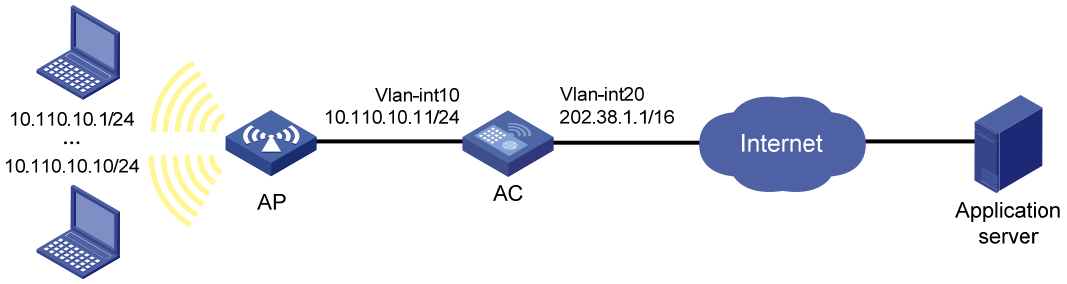
3. 验证配置

以上配置完成后，外网 Host 能够通过 NAT 地址访问各内网服务器。

1.1.10 NAT444 端口块静态映射配置举例

1. 组网需求

内部网络用户 10.110.10.1～10.110.10.10 使用外网地址 202.38.1.100 访问 Internet。内网用户地址基于 NAT444 端口块静态映射方式复用外网地址 202.38.1.100，外网地址的端口范围为 10001～15000，端口块大小为 500。



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > NAT”，进入“NAT”页面，单击“NAT444 静态转换”后进行配置，配置步骤为：

- 添加 NAT444 端口块组 1，指定公网地址的端口块范围为 10001～15000，端口块大小为 500，私网地址成员的起始 IP 地址为 10.110.10.1，结束地址为 10.110.10.10；公网地址成员的起始 IP 地址为 202.38.1.100。
- 在接口 Vlan-interface20 上引用端口块组 1。

3. 验证配置

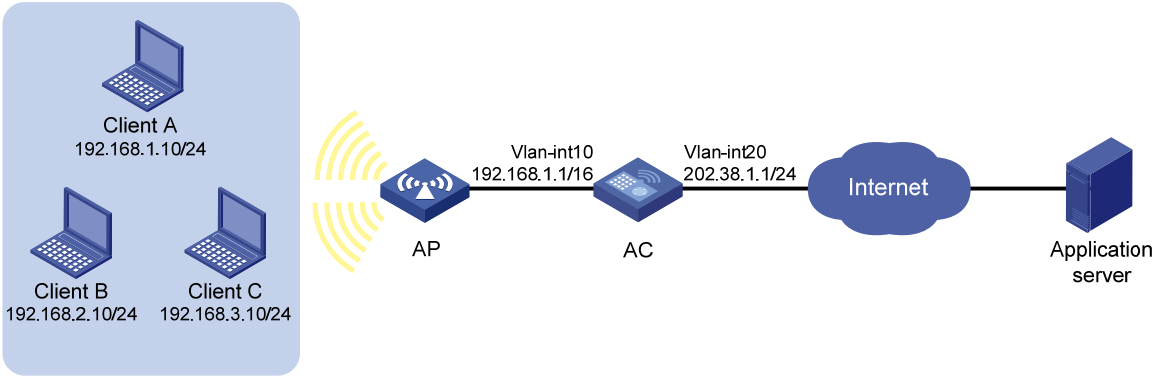
以上配置完成后，内网 Client 可以访问外网服务器。

1.1.11 NAT444 端口块动态映射配置举例

1. 组网需求

- 某公司内网使用的 IP 地址为 192.168.0.0/16。
- 该公司拥有 202.38.1.2 和 202.38.1.3 两个外网 IP 地址。

需要实现，内部网络中的 192.168.1.0/24 网段的用户可以访问 Internet，其它网段的用户不能访问 Internet。基于 NAT444 端口块动态映射方式复用两个外网地址 202.38.1.2 和 202.38.1.3，外网地址的端口范围为 1024～65535，端口块大小为 300。当为某用户分配的端口块资源耗尽时，再为其增量分配 1 个端口块。



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > NAT”，进入“NAT”页面，单击“NAT444 动态转换”后进行配置，配置步骤为：

- 添加 NAT444 地址组 0，指定端口范围为 1024～65535，端口块大小为 300，增量端口块数为 1，地址组成员的起始 IP 地址为 202.38.1.2，结束地址为 202.38.1.3。
- 添加 IPv4 ACL 2000，该 ACL 仅允许源 IP 地址为 192.168.1.0、通配符掩码为 0.0.0.255 的网段的用户进行地址转换。
- 在接口 Vlan-interface20 上使用 NAT444 地址组 0 中的地址对匹配 ACL 2000 的报文进行源地址转换。

3. 验证配置

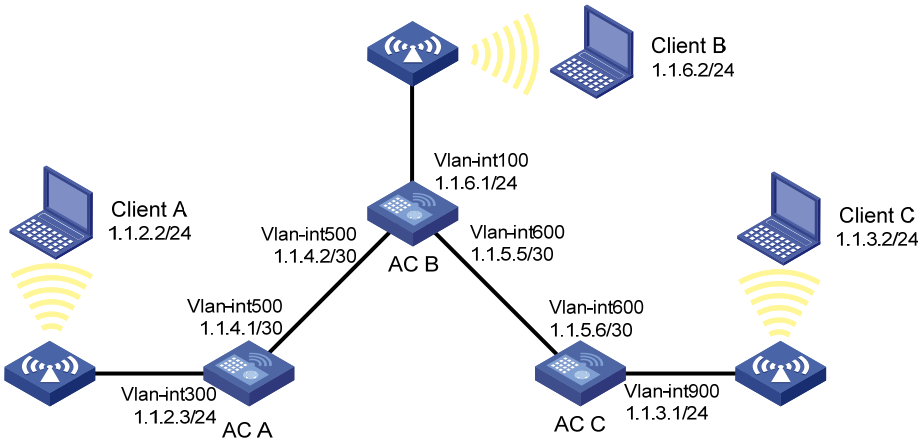
以上配置完成后，Client A 能够访问外网服务器，Client B 和 Client C 无法访问外网服务器。

1.1.12 IPv4 静态路由基本功能配置举例

1. 组网需求

AC各接口和无线客户端的IP地址和掩码如 图 1-10 所示。要求采用静态路由，使图中任意无线客户端之间都能互通。

图1-10 IPv4 静态路由配置组网图



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 >路由”，进入“静态路由”页面配置 IPv4 静态路由，三台 AC 上的配置分别为：

- 在 AC A 上创建一条 IPv4 静态路由表项，指定目的 IP 地址为 0.0.0.0，掩码长度为 0，下一跳地址为 1.1.4.2，该路由用来匹配所有的目的 IP 地址。
- 在 AC B 上创建到达 Client A 所在网段和 Client C 所在网段的两条 IPv4 静态路由表项：
  - 到达 Client C 所在网段的路由：目的 IP 地址为 1.1.3.0，掩码长度为 24，下一跳地址为 1.1.5.6；
  - 到达 Client A 所在网段的路由：目的 IP 地址为 1.1.2.0，掩码长度为 24，下一跳地址为 1.1.4.1。
- 在 AC C 上创建一条 IPv4 静态路由表项，指定目的 IP 地址为 0.0.0.0、掩码长度为 0、下一跳地址为 1.1.5.5，该路由用来匹配所有的目的 IP 地址。

3. 验证配置

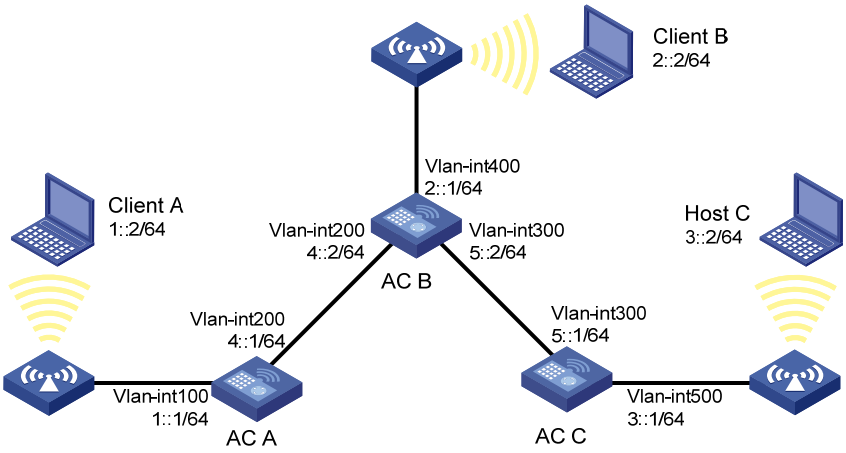
完成上述配置后，在任意一台无线客户端上都可以 ping 通另外两台无线客户端。

1.1.13 IPv6 静态路由基本功能配置举例

1. 组网需求

AC各接口和无线客户端的IPv6 地址和前缀长度如 图 1-11 所示。要求采用静态路由，使图中任意无线客户端之间都能互通。

图1-11 IPv6 静态路由配置组网图



2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 >路由”，进入“静态路由”页面配置 IPv6 静态路由，三台 AC 上的配置分别为：

- 在 AC A 上创建一条 IPv6 静态路由表项，指定目的 IPv6 地址为::，前缀长度为 0，下一跳地址为 4::2，该路由用来匹配所有的目的 IPv6 地址。
- 在 AC B 上创建到达 Client A 所在网段和 Client C 所在网段的两条 IPv6 静态路由表项：
  - 到达 Client C 所在网段的路由：目的 IPv6 地址为 3::2，前缀长度为 64，下一跳地址为 5::1；
  - 到达 Client A 所在网段的路由：目的 IPv6 地址为 1::2，前缀长度为 64，下一跳地址为 4::1。

- 在 AC C 上创建一条 IPv6 静态路由表项，指定目的 IPv6 地址为::，前缀长度为 0，下一跳地址为 5::2，该路由用来匹配所有的目的 IPv6 地址。

3. 验证配置

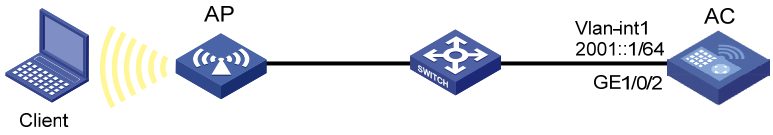
完成上述配置后，在任意一台无线客户端上都可以 ping 通另外两台无线客户端。

1.1.14 IPv6 地址静态配置举例

1. 组网需求

- 将 AP、AC 的以太网端口分别加入相应的 VLAN 里，在 VLAN 接口上配置 IPv6 地址，验证它们之间的互通性。
- AC 的 VLAN 接口 1 的全球单播地址为 2001::1/64。
- Client 上安装了 IPv6，根据 IPv6 邻居发现协议自动配置 IPv6 地址。

图1-12 IPv6 地址静态配置组网图



2. 配置步骤

(1) 配置 AC

配置 AC 基本功能（详细介绍请参见“WLAN 配置指导”中的“WLAN 接入”）（略）

(2) 配置 IPv6 地址

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > IP 服务”，进入“IPv6”页面配置 IPv6 地址，手工配置 VLAN1 接口地址为 2001::1，前缀长度为 64。

(3) 配置 VLAN 接口 1 允许发布 RA 消息

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务> ND”，进入“ND”页面，单击“高级设置 > 接口上的 RA 设置”，允许 VLAN 接口 1 发布 RA 消息。

(4) 配置 Client

Client 上安装 IPv6，根据 IPv6 邻居发现协议自动配置 IPv6 地址。

3. 验证配置

在 Client 上使用 Ping 测试和 AC 的互通性；在 AC 上使用 Ping 测试和 Client 的互通性。

1.1.15 DHCP服务器动态分配地址配置举例

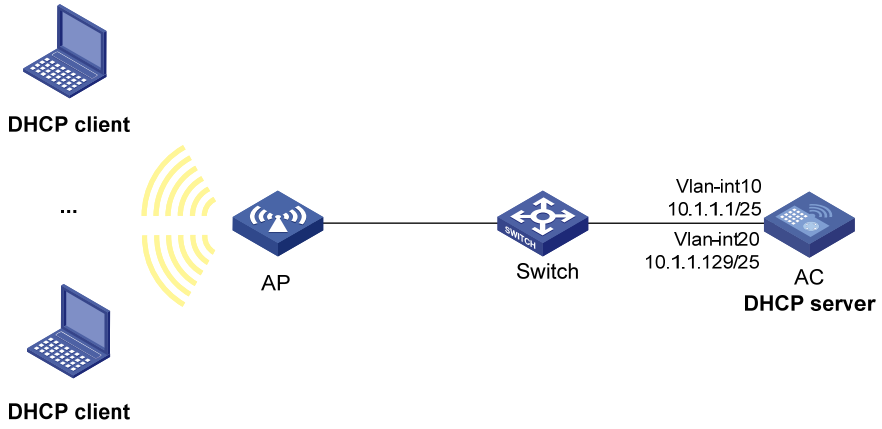
1. 组网需求

- 作为 DHCP 服务器的 AC 为网段 10.1.1.0/24 中的 AP 和客户端动态分配 IP 地址，该地址池网段分为两个子网网段：10.1.1.0/25 和 10.1.1.128/25；

- AC 的两个 VLAN 接口，VLAN 接口 10 和 VLAN 接口 20 的地址分别为 10.1.1.1/25 和 10.1.1.129/25；
- 为 AP 分配 10.1.1.0/25 网段的 IP 地址，为 DHCP client 分配 10.1.1.128/25 网段的 IP 地址。

2. 组网图

图1-13 DHCP 动态分配地址配置组网图



3. 配置步骤

在 AC 上创建 VLAN 10 和 VLAN 20，并配置 VLAN 接口 10 和 VLAN 接口 20 的地址。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面创建 VLAN 并配置 VLAN 接口，配置步骤为：

- 创建 VLAN10，配置 VLAN 接口 10 的 IP 地址为 10.1.1.1/25。
- 创建 VLAN20，配置 VLAN 接口 20 的 IP 地址为 10.1.1.129/25。

配置 DHCP 服务器。

单击“系统”菜单页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“DHCP”页面配置 DHCP 服务器，配置步骤为：

- 开启 DHCP 服务。
- 配置 VLAN 接口 10 和 VLAN 接口 20 工作在 DHCP 服务器模式。
- 在地址池页面，创建名称为 pool1 的地址池，配置该地址池动态分配的地址段为 10.1.1.0/25，在地址池选项中配置网关地址为 10.1.1.1。
- 在地址池页面，创建名称为 pool2 的地址池，配置该地址池动态分配的地址段为 10.1.1.128/25，在地址池选项中配置网关地址为 10.1.1.129。
- 在高级设置页面，配置冲突地址检查功能中的发送回显请求报文的最大数目为 1，等待回显响应报文的超时时间为 500 毫秒。

配置无线服务。

单击“网络”菜单页面左侧导航栏的“无线配置 > 无线网络”，进入“无线网络”页面配置无线服务，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 office。

- 配置缺省 VLAN 为 20。
- 开启无线服务。

配置 AP。

单击“网络”菜单页面左侧导航栏的“无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 添加一个 AP，配置 AP 名称为 AP 1，配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的 5GHz 射频。

配置 AP 射频。

单击“网络”菜单页面左侧导航栏的“无线配置 > AP 管理”，进入“AP”页面配置 AP 1 的 5GHz 射频状态为开启。

4. 验证配置

配置完成后，10.1.1.0/25 和 10.1.1.128/25 网段的 AP 和客户端可以从 DHCP 服务器 AC 申请到相应网段的 IP 地址和网络配置参数。

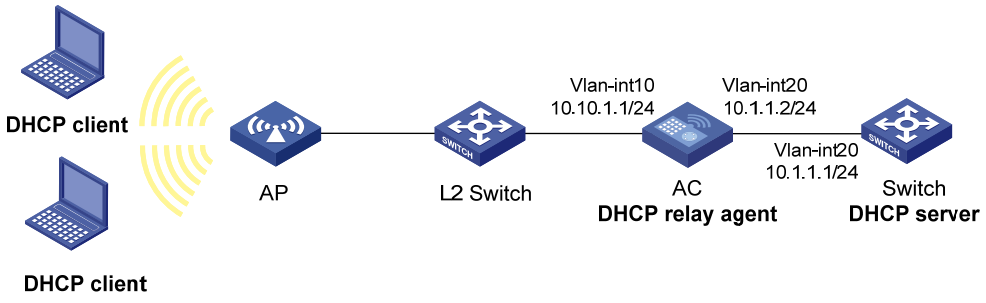
1.1.16 DHCP中继配置举例

1. 组网需求

- DHCP 客户端所在网段为 10.10.1.0/24，DHCP 服务器的 IP 地址为 10.1.1.1/24；
- 由于 DHCP 客户端和 DHCP 服务器不在同一网段，因此，需要在客户端所在网段设置 DHCP 中继设备，以便客户端可以从 DHCP 服务器申请到 10.10.1.0/24 网段的 IP 地址及相关配置信息；
- AC 作为 DHCP 中继通过端口（属于 VLAN10）连接到 DHCP 客户端所在的网络，VLAN 接口 10 的 IP 地址为 10.10.1.1/24，VLAN 接口 20 的 IP 地址为 10.1.1.2/24。

2. 组网图

图1-14 组网图



3. 配置步骤

配置各接口的 IP 地址。（略）

配置 DHCP 服务器。（略）

配置 AC 基本功能。（略）

配置 DHCP 中继。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“DHCP”页面配置 DHCP 中继，配置步骤为：

- 开启 DHCP 服务。
- 配置 VLAN 接口 10 为 DHCP 中继。
- 配置 DHCP 服务器 IP 地址为 10.1.1.1。

4. 验证配置

配置完成后，DHCP 客户端可以通过 DHCP 中继从 DHCP 服务器获取 IP 地址及相关配置信息。

1.1.17 DHCP Snooping配置举例

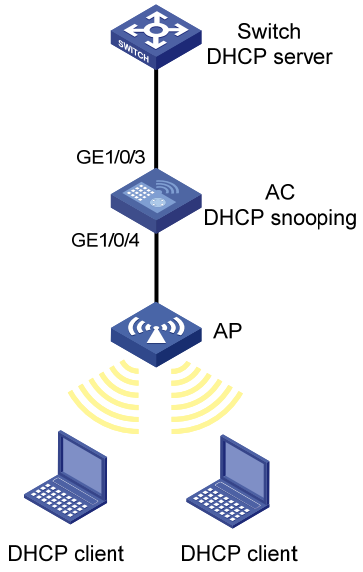
1. 组网需求

AC 通过以太网端口 GigabitEthernet 1/0/3 连接到 DHCP 服务器，通过以太网端口 GigabitEthernet 1/0/4 连接到 AP。要求：

- 与合法 DHCP 服务器相连的端口可以转发 DHCP 服务器的响应报文，而其他端口不转发 DHCP 服务器的响应报文。
- 记录 DHCP-REQUEST 报文和信任端口收到的 DHCP-ACK 报文中 DHCP 客户端 IP 地址及 MAC 地址的绑定信息。

2. 组网图

图1-15 DHCP Snooping 配置组网图



3. 配置步骤

配置 DHCP 服务器。（略）

配置 AC 基本功能。（略）

配置 DHCP Snooping。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“DHCP Snooping”页面配置 DHCP Snooping，配置步骤为：

- 开启 DHCP Snooping 功能。
- 设置 GigabitEthernet1/0/3 端口为信任端口。
- 在 GigabitEthernet1/0/4 上启用 DHCP Snooping 表项功能。

4. 验证配置

配置完成后，在 AC 上可查询到获取到的 DHCP Snooping 表项。

1.1.18 静态IPv4 DNS配置举例

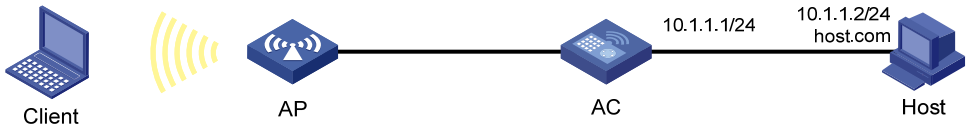
1. 组网需求

为了避免记忆复杂的 IP 地址，AC 希望通过便于记忆的主机名访问某一主机。在 AC 上手工配置 IP 地址对应的主机名，利用静态域名解析功能，就可以实现通过主机名访问该主机。

在本例中，AC 访问的主机 IP 地址为 10.1.1.2，主机名为 host.com。

2. 组网图

图1-16 静态 IPv4 DNS 配置举例组网图



3. 配置步骤

配置主机名 host.com 对应的 IP 地址为 10.1.1.2。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“IPv4 DNS”页面配置静态域名解析，配置步骤为：

配置静态域名解析：主机名为 host.com，对应的 IPv4 地址为 10.1.1.2。

4. 验证配置

在 AC 上执行 **ping host.com** 命令，可以解析到 host.com 对应的 IP 地址为 10.1.1.2，并能够 ping 通主机。

1.1.19 动态IPv4 DNS配置举例

1. 组网需求

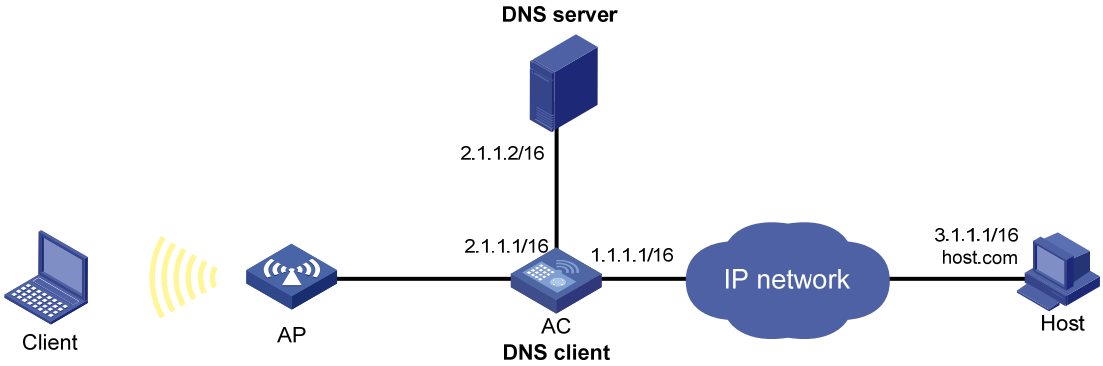
为了避免记忆复杂的 IP 地址，AC 希望通过便于记忆的域名访问某一主机。如果网络中存在域名服务器，则可以利用动态域名解析功能，实现通过域名访问主机。

在本例中：

- 域名服务器的 IP 地址是 2.1.1.2/16，域名服务器上包含域名“host”和 IP 地址 3.1.1.1/16 的对应关系。
- AC 作为 DNS 客户端，使用动态域名解析功能，将域名解析为 IP 地址。
- AC 上配置域名后缀 com，以便简化访问主机时输入的域名，例如通过输入 host 即可访问域名为 host.com、IP 地址为 3.1.1.1/16 的主机 Host。

2. 组网图

图1-17 动态 IPv4 DNS 配置举例组网图



3. 配置步骤

在 DNS 服务器上添加域名 host.com 和 IP 地址 3.1.1.1 的映射关系。（略）

在各设备上配置静态路由或动态路由协议，使得各设备之间路由可达。（略）

配置 DNS 客户端。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“IPv4 DNS”页面配置域名服务器，配置步骤为：

配置域名服务器地址为 2.1.1.2。在高级设置页面，配置域名后缀为 com。

4. 验证配置

完成上述配置后，在 AC 上执行 **ping host** 命令，可以解析到 host 对应的 IP 地址为 3.1.1.1，并能够 ping 通主机。

1.1.20 IPv4 DNS proxy配置举例

1. 组网需求

某局域网内拥有多台设备，每台设备上都指定了域名服务器的 IP 地址，以便直接通过域名访问外部网络。当域名服务器的 IP 地址发生变化时，网络管理员需要更改局域网内所有设备上配置的域名服务器 IP 地址，工作量将会非常巨大。

通过 DNS proxy 功能，可以大大减少网络管理员的工作量。当域名服务器 IP 地址改变时，只需更改 DNS proxy 上的配置，即可实现局域网内设备通过新的域名服务器解析域名。

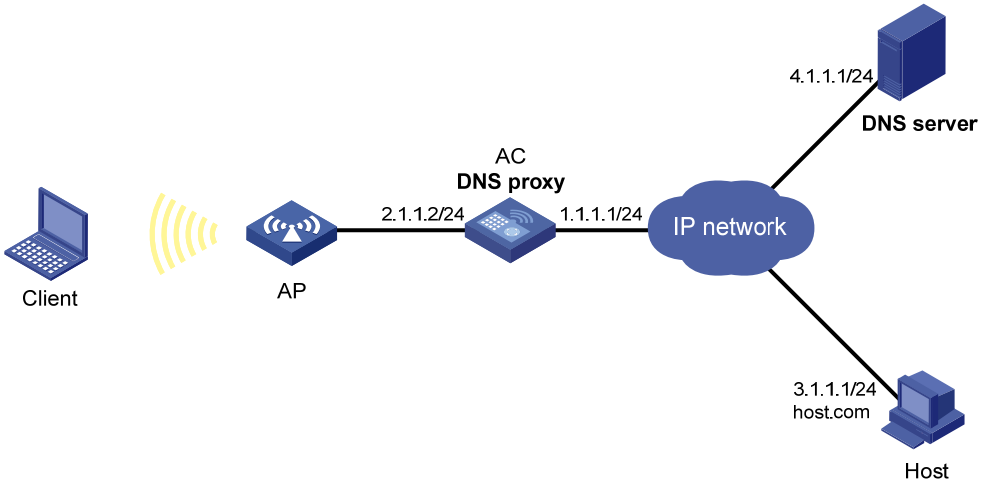
在本例中，具体配置步骤为：

(1) 局域网中的某台设备 AC 配置为 DNS proxy，DNS proxy 上指定域名服务器 IP 地址为真正的域名服务器的地址 4.1.1.1。

(2) 局域网中的其他设备上，域名服务器的 IP 地址配置为 DNS proxy 的地址，域名解析报文将通过 DNS proxy 转发给真正的域名服务器。

2. 组网图

图1-18 IPv4 DNS proxy 配置举例组网图



3. 配置步骤

在各设备上配置静态路由或动态路由协议，使得各设备之间路由可达。（略）

(1) 配置 DNS 服务器。（略）

(2) 配置 AC 作为 DNS proxy。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“IPv4 DNS”页面配置域名服务器，配置步骤为：

配置域名服务器的 IP 地址为 4.1.1.1。在高级设置页面，开启 DNS proxy 功能。

(3) 配置 DNS 客户端 Client，配置 DNS 服务器的 IP 地址为 2.1.1.2。

4. 验证配置

在 Client 上执行 **ping host.com** 命令，可以 ping 通主机，且对应的目的地址为 3.1.1.1。

1.1.21 静态IPv6 DNS配置举例

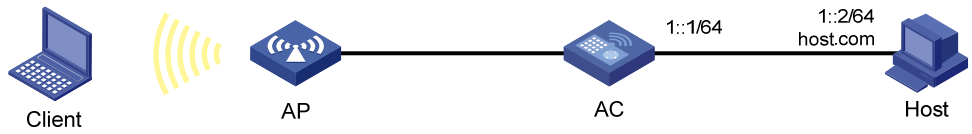
1. 组网需求

为了避免记忆复杂的 IPv6 地址，AC 希望通过便于记忆的主机名访问某一主机。在 AC 上手工配置 IPv6 地址对应的主机名，利用静态域名解析功能，就可以实现通过主机名访问该主机。

在本例中，AC 访问的主机 IP 地址为 1::2，主机名为 host.com。

2. 组网图

图1-19 静态 IPv6 DNS 配置举例组网图



3. 配置步骤

配置主机名 host.com 对应的 IPv6 地址为 1::2。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“IPv6 DNS”页面配置静态域名解析，配置步骤为：

配置静态域名解析：主机名为 host.com，对应的 IPv6 地址为 1::2。

4. 验证配置

在 AC 上执行 **ping ipv6 host.com** 命令，可以解析到 host.com 对应的 IPv6 地址为 1::2，并能够 ping 通主机。

1.1.22 动态IPv6 DNS配置举例

1. 组网需求

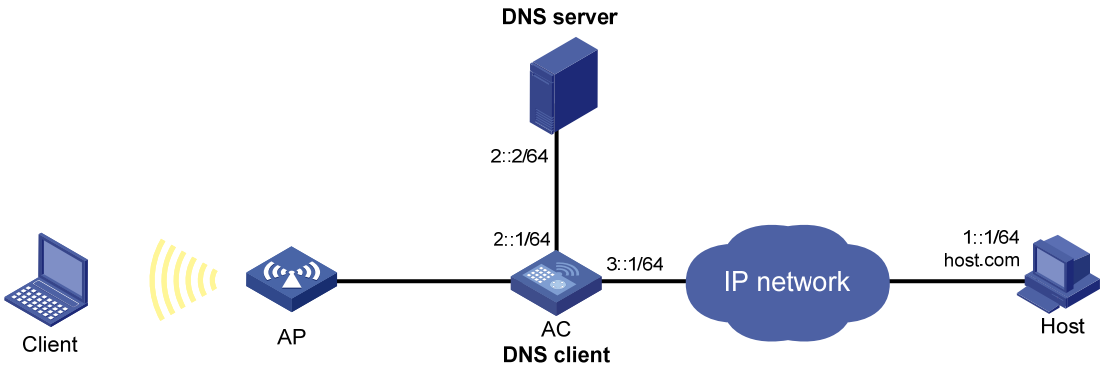
为了避免记忆复杂的 IPv6 地址，AC 希望通过便于记忆的域名访问某一主机。如果网络中存在域名服务器，则可以利用动态域名解析功能，实现通过域名访问主机。

在本例中：

- 域名服务器的 IPv6 地址是 2::2/64，域名服务器上包含域名“host”和 IPv6 地址 1::1/64 的对应关系。
- AC 作为 DNS 客户端，使用动态域名解析功能，将域名解析为 IPv6 地址。
- AC 上配置域名后缀 com，以便简化访问主机时输入的域名，例如通过输入 host 即可访问域名为 host.com、IPv6 地址为 1::1/64 的主机 Host。

2. 组网图

图1-20 动态 IPv6 DNS 配置举例组网图



3. 配置步骤

在 DNS 服务器上添加域名 host.com 和 IPv6 地址 1::1 的映射关系。（略）

在各设备上配置静态路由或动态路由协议，使得各设备之间路由可达。（略）

配置 DNS 客户端。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“IPv6 DNS”页面配置域名服务器，配置步骤为：

配置域名服务器地址为 2::2。在高级设置页面，配置域名后缀为 com。

4. 验证配置

完成上述配置后，在 AC 上执行 **ping ipv6 host** 命令，可以解析到 host 对应的 IPv6 地址为 1::1，并能够 ping 通主机。

1.1.23 IPv6 DNS proxy配置举例

1. 组网需求

某局域网内拥有多台设备，每台设备上都指定了域名服务器的 IPv6 地址，以便直接通过域名访问外部网络。当域名服务器的 IPv6 地址发生变化时，网络管理员需要更改局域网内所有设备上配置的域名服务器 IPv6 地址，工作量将会非常巨大。

通过 DNS proxy 功能，可以大大减少网络管理员的工作量。当域名服务器 IPv6 地址改变时，只需更改 DNS proxy 上的配置，即可实现局域网内设备通过新的域名服务器解析域名。

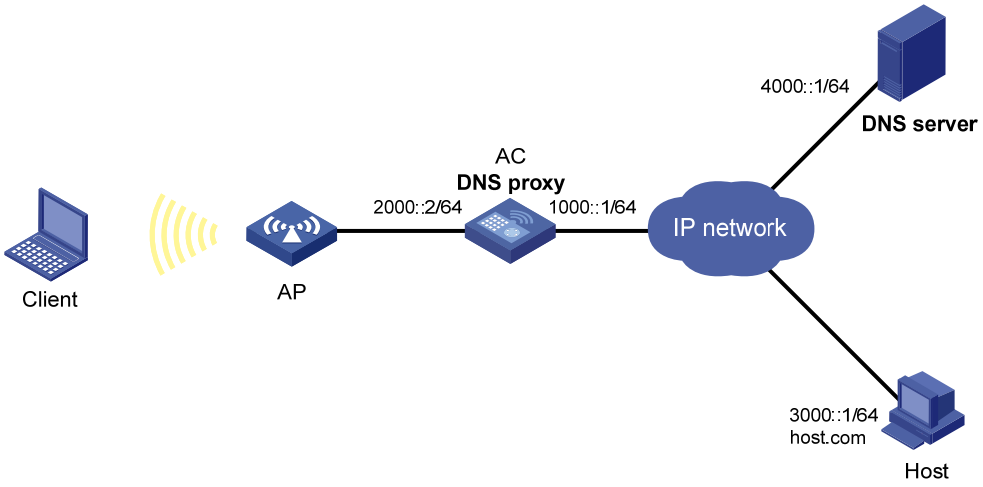
在本例中，具体配置步骤为：

(1) 局域网中的某台设备 AC 配置为 DNS proxy，DNS proxy 上指定域名服务器 IPv6 地址为真正的域名服务器的地址 4000::1

(2) 局域网中的其他设备上，域名服务器的 IPv6 地址配置为 DNS proxy 的地址，域名解析报文将通过 DNS proxy 转发给真正的域名服务器。

2. 组网图

图1-21 IPv6 DNS proxy 配置举例组网图



3. 配置步骤

在各设备上配置静态路由或动态路由协议，使得各设备之间路由可达。（略）

(1) 配置 DNS 服务器。（略）

(2) 配置 AC 作为 DNS proxy。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“IPv6 DNS”页面配置域名服务器，配置步骤为：

配置域名服务器的 IPv6 地址为 4000::1。在高级设置页面，开启 DNS proxy 功能。

(3) 配置 DNS 客户端 Client，配置 DNS 服务器的 IPv6 地址为 2000::2。

4. 验证配置

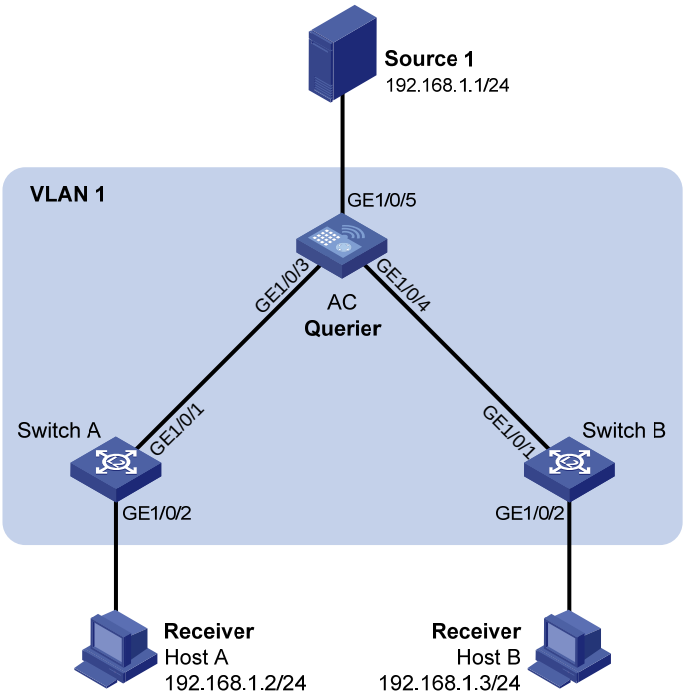
在 Client 上执行 **ping ipv6 host.com** 命令，可以 ping 通主机，且对应的目的地址为 3000::1。

1.1.24 IGMP Snooping配置举例

1. 组网需求

- 如下图所示，在一个没有三层网络设备的纯二层网络中，组播源 Source 1 向组播组 224.1.1.1 发送组播数据，Host A 和 Host B 都是该组播组的接收者，且都使用 IGMPv2。
- 由于该网络中没有可运行 IGMP 的三层网络设备，因此由 AC 来充当 IGMP 查询器，并将其发出的 IGMP 查询报文的源 IP 地址配置为非 0.0.0.0，以免影响 AC 和交换机上 IGMP snooping 转发表项的建立从而导致组播数据无法正常转发。
- 为防止 AC 和交换机在没有相应转发表项时将组播数据在 VLAN 内广播，在所有设备上都开启丢弃未知组播数据报文功能。

图1-22 IGMP Snooping 配置组网图



2. 配置步骤

(1) 配置 AC 作为 IGMP 查询器

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务> Multicast”，进入“IGMP Snooping”页面配置 IGMP Snooping，配置步骤为：

- 开启 IGMP Snooping 功能。
- 在 VLAN 1 内开启版本 2 的 IGMP snooping，并开启丢弃未知组播数据报文功能和充当 IGMP 查询器功能，然后将普遍组查询报文和特定组查询报文的源 IP 地址都配置为 192.168.1.10。

(2) 配置 Switch A 和 Switch B，在两台交换机的 VLAN 1 内开启版本 2 的 IGMP snooping，并开启丢弃未知组播数据报文功能。

3. 验证配置

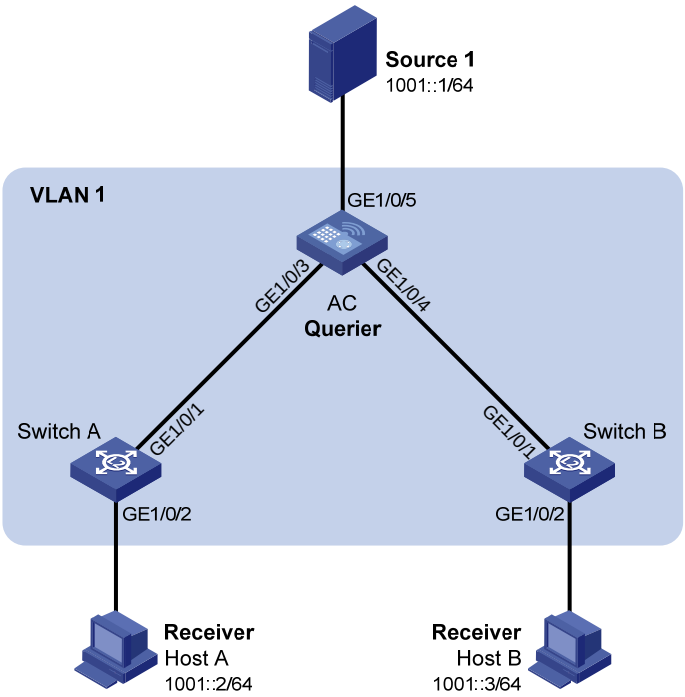
完成上述配置，并且接收者申请加入组播组 224.1.1.1 之后，在页面上可以看到该组播组对应的 IGMP snooping 转发表项。

1.1.25 MLD Snooping配置举例

1. 组网需求

- 如下图所示，在一个没有三层网络设备的纯二层网络中，组播源 Source 1 向 IPv6 组播组 FF1E::101 发送 IPv6 组播数据，Host A 和 Host B 都是该 IPv6 组播组的接收者，且都使用 MLDv1。
- 由于该网络中没有可运行 MLD 的三层网络设备，因此由 AC 来充当 MLD 查询器。
- 为防止 AC 和交换机在没有相应转发表项时将 IPv6 组播数据在 VLAN 内广播，在所有设备上都开启丢弃未知 IPv6 组播数据报文功能。

图1-23 MLD Snooping 配置组网图



2. 配置步骤

(1) 配置 AC 作为 MLD 查询器

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务> Multicast”，进入“MLD Snooping”页面配置 MLD Snooping，配置步骤为：

- 开启 MLD Snooping 功能。
- 在 VLAN 1 内开启版本 1 的 MLD snooping，并开启丢弃未知 IPv6 组播数据报文功能和充当 MLD 查询器功能。

(2) 配置 Switch A 和 Switch B，在两台交换机的 VLAN 1 内开启版本 1 的 MLD snooping，并开启丢弃未知 IPv6 组播数据报文功能。

3. 验证配置

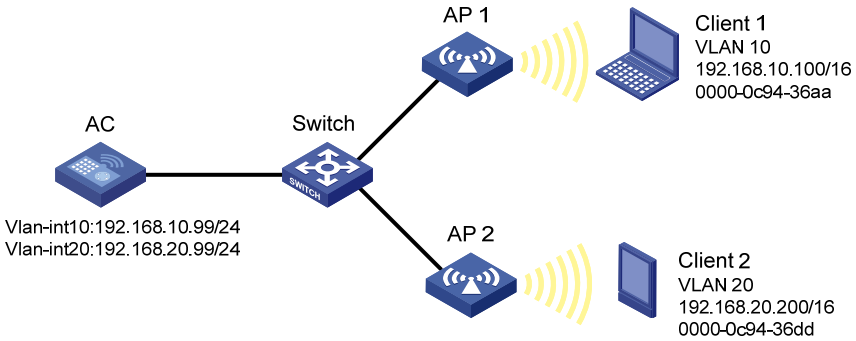
完成上述配置，并且接收者申请加入 IPv6 组播组 FF1E::101 之后，在页面上可以看到该 IPv6 组播组对应的 MLD snooping 转发表项。

1.1.26 代理ARP配置举例

1. 组网需求

- Client 1 和 Client 2 配置为同一网段的主机（Client 1 的 IP 地址是 192.168.10.100/16，Client 2 的 IP 地址是 192.168.20.200/16），但却被设备 AC 分在两个不同的子网（Client 1 属于 VLAN 10，Client 2 属于 VLAN 20）。
- Client 1 和 Client 2 没有配置缺省网关，要求在设备 AC 上开启代理 ARP 功能，使处在两个子网的 Client 1 和 Client 2 能互通。

图1-24 代理 ARP 配置组网图



2. 配置步骤

创建 VLAN 10 和 VLAN 20，并配置 VLAN 接口 10 和 VLAN 接口 20 的地址。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN，配置步骤为：

- 创建 VLAN 10，配置 VLAN 接口 10 的 IP 地址为 192.168.10.99/24。
- 创建 VLAN 20，配置 VLAN 接口 20 的 IP 地址为 192.168.20.99/24。

开启 VLAN 接口 10 和 VLAN 接口 20 的代理 ARP 功能。

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > ARP”，进入“ARP”页面，在“高级设置 > ARP 代理”页面开启 VLAN 接口 10 和 VLAN 接口 20 的代理 ARP 功能。

3. 验证配置

配置完成后，Client 1 和 Client 2 可以互相 ping 通。

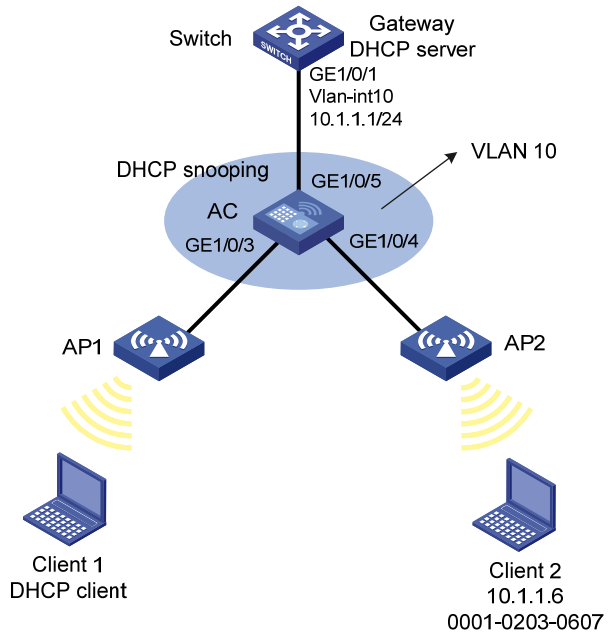
1.1.27 ARP攻击防御配置举例

1. 组网需求

- Switch 是 DHCP 服务器；

- Client 1 是 DHCP 客户端；用户 Client 2 的 IP 地址是 10.1.1.6，MAC 地址是 0001-0203-0607。
- AC 是 DHCP Snooping 设备，在 VLAN 10 内启用 ARP Detection 功能，对 DHCP 客户端和用户进行用户合法性检查和报文有效性检查。

图1-25 配置用户合法性检查和报文有效性检查组网图



2. 配置步骤

(1) 配置组网图中所有接口属于 VLAN 10 及 Switch 对应 VLAN 接口的 IP 地址（略）

(2) 配置 DHCP 服务器（略）

(3) 配置 DHCP 客户端 Client 1 和用户 Client 2（略）

(4) 配置 AC

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS”，进入“DHCP Snooping”页面，配置步骤为：

- 开启 DHCP Snooping 功能。
- 设置 GigabitEthernet1/0/5 端口为信任端口。
- 在 GigabitEthernet1/0/3 上启用 DHCP Snooping 表项记录功能。

单击“系统”菜单页面左侧导航栏的“网络配置 > 服务 > ARP”，进入“ARP”页面，在“高级设置 > ARP 攻击防御 > ARP Detection”页面开启 ARP Detection 功能，配置步骤为：

- 开启 VLAN10 的 ARP Detection 功能

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。

- 在高级设置页面，设置接口 gigabitethernet 1/0/5 状态为信任状态
- 在高级设置页面，开启源 MAC 地址的检查、目的 MAC 地址的检查和 IP 地址的检查

完成上述配置后，对于接口 GigabitEthernet1/0/3 和 GigabitEthernet1/0/4 收到的 ARP 报文，先进行报文有效性检查，然后基于 DHCP Snooping 安全表项进行用户合法性检查。

3. 验证配置

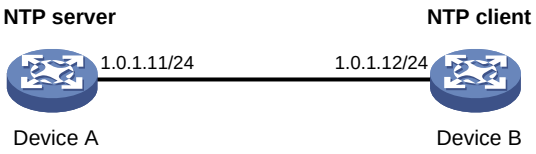
完成上述配置后，可在 AC 的“系统 > 网络配置 > 服务 > ARP”页面上看到 Client 1 的 ARP 表项，而无法看到 Client 2 的 ARP 表项。

1.1.28 NTP配置举例

1. 组网需求

- Device A 采用本地时钟作为参考时钟，使得自己的时钟处于同步状态。
- Device A 作为时间服务器为 Device B 提供时间同步。

图1-26 NTP 配置组网图



2. 配置步骤

(1) 配置 NTP 服务器 Device A

进入 Device A，单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 管理协议”，进入“NTP”页面配置 NTP 服务器，配置步骤为：

- 开启 NTP 服务。
- 配置本地时钟的 IP 地址为 127.127.1.0。
- 配置本地时钟所处的层数为 2。

(2) 配置 NTP 客户端 Device B

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“系统 > 管理”，进入“系统设置”页面配置系统时间，配置步骤为：

- 选择自动同步网络日期和时间，采用的协议为网络时间协议（NTP）。
- 指定 NTP 服务器（即时钟源）的 IP 地址为 1.0.1.11，并指定时钟源工作在服务器模式。

3. 验证配置

完成上述配置后，Device B 与 Device A 进行时间同步。此时 Device B 层数比 Device A 的层数大 1，为 3。

1.1.29 LLDP配置举例

1. 组网需求

通过在 AC 和 Switch 上配置 LLDP 功能，实现：

- AC 可以发现 Switch，并获取 Switch 的系统及配置等信息。
- Switch 不可以发现 AC。

图1-27 LLDP 配置组网图

2. 配置步骤

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 管理协议 > LLDP”，进入“LLDP”页面。两台设备上的配置分别为：

- 在 AC 上全局开启 LLDP 功能。进入接口状态页面，在接口 GigabitEthernet1/0/1 上开启 LLDP 功能。在接口设置页面，开启接口 GigabitEthernet1/0/1 的最近桥代理功能，并配置该接口的工作模式为 Rx：只接收 LLDP 报文，使得 AC 能够发现邻居。
- 在 Switch 上全局开启 LLDP 功能。进入接口状态页面，在接口 GigabitEthernet1/0/2 上开启 LLDP 功能。在接口设置页面，开启接口 GigabitEthernet1/0/2 的最近桥代理功能，并配置该接口的工作模式为 Tx：只发送 LLDP 报文，使得 Switch 不能够发现邻居。

3. 验证配置

完成上述配置后，在 AC 的 LLDP 邻居页面中可以看到 Switch 的信息，邻居关系建立；Switch 的 LLDP 邻居页面中没有邻居信息。

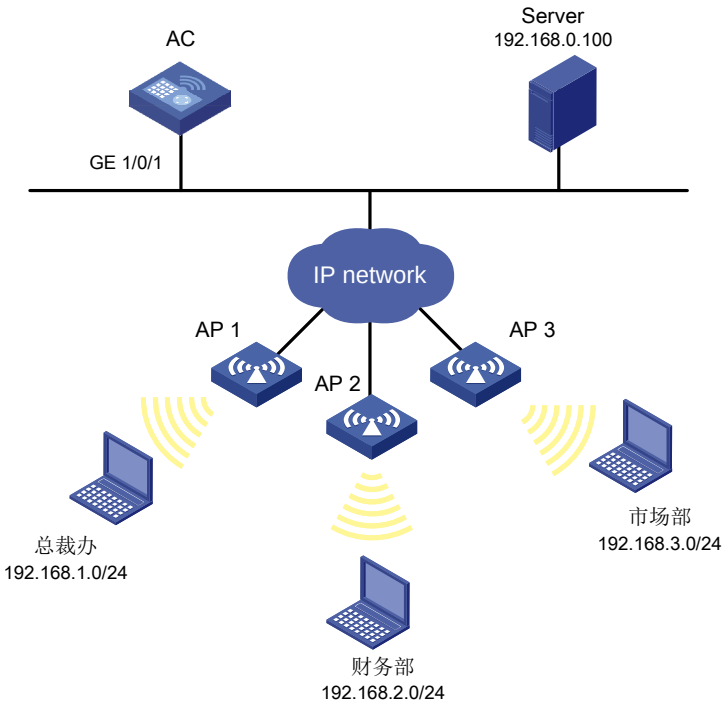
1.2 网络安全功能配置举例

1.2.1 通过ACL进行包过滤配置举例

1. 组网需求

某公司要求，允许总裁办在任意时间、财务部在工作时间（每周工作日的 8 点到 18 点）访问财务数据库服务器，禁止其它部门在任何时间、财务部在非工作时间访问该服务器。

图1-28 通过 ACL 进行包过滤配置组网图



2. 配置步骤

单击页面底部的<系统>按钮，然后单击左侧导航栏“网络安全 > 包过滤”，进入包过滤配置页面。配置步骤为：

- 创建接口包过滤策略，在 AC 的 VLAN 接口 10 的出方向上指定包过滤规则为 IPv4 ACL。
- 创建 IPv4 高级 ACL 3000，并按顺序制定三条规则：
  - 允许协议类型为 256（IP），源 IP 为 192.168.1.0、通配符掩码为 0.0.0.255，目的 IP 为 192.168.0.100、通配符掩码为 0 的报文通过。
  - 创建周期时间段 work，指定开始时间为 08：00，结束时间为 18：00，生效时间为每周一、周二、周三、周四和周五。允许协议类型为 256（IP），源 IP 为 192.168.2.0、通配符掩码为 0.0.0.255，目的 IP 为 192.168.0.100、通配符掩码为 0，生效时间段为 work 的报文通过。
  - 拒绝协议类型为 256（IP），目的 IP 为 192.168.0.100、通配符掩码为 0 的报文通过。
- 开启 ACL 规则的匹配统计功能。

3. 验证配置

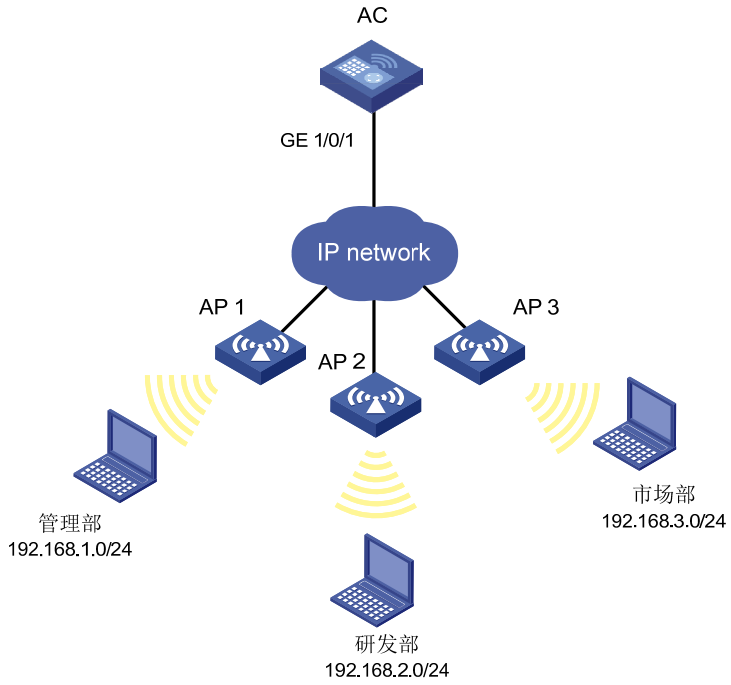
完成上述配置后，在页面上可以看到已经创建的 IPv4 高级 ACL 的规则状态和命中报文数。总裁办主机在任何时间都可以 ping 通财务数据库服务器；在工作时间财务部主机可以 ping 通该服务器；市场部在任何时间都不能 ping 通该服务器。

1.2.2 优先级映射配置举例

1. 组网需求

当三个部门访问 Internet 的流量发生拥塞时，要求按照依次发送管理部、市场部和研发部的流量。

图1-29 优先级映射配置组网图



2. 配置步骤

(1) 配置 QoS 策略

单击页面底部的<系统>按钮，然后单击左侧导航栏“网络安全 > 流策略”，进入 QoS 策略配置页面。在接口 GigabitEthernet1/0/2、GigabitEthernet1/0/3、GigabitEthernet1/0/4 的入方向上应用 QoS 策略后，修改应用的策略，创建如下三个 QoS 策略：

- 创建 IPv4 ACL 2001，添加一条允许源 IP 为 192.168.1.0、通配符掩码为 0.0.0.255 的报文通过的规则；定义匹配该 ACL 的类；指定流行为为重标记报文的 802.1p 优先级为 2。
- 创建 IPv4 ACL 2002，添加一条允许源 IP 为 192.168.2.0、通配符掩码为 0.0.0.255 的报文通过的规则；定义匹配该 ACL 的类；指定流行为为重标记报文的 802.1p 优先级为 0。
- 创建 IPv4 ACL 2003，添加一条允许源 IP 为 192.168.3.0、通配符掩码为 0.0.0.255 的报文通过的规则；定义匹配该 ACL 的类；指定流行为为重标记报文的 802.1p 优先级为 1。

(2) 配置优先级映射

完成上述配置后，单击页面上方的“优先级映射”，然后单击右上方的“端口优先级”，进入优先级映射配置页面。具体配置为：指定在接口 GigabitEthernet1/0/1、GigabitEthernet1/0/2、GigabitEthernet1/0/3、GigabitEthernet1/0/4 的优先级信任模式为信任 Dot1p 优先级。

单击<确定>后，返回优先级映射配置页面，然后单击右上方的“优先级映射表”，具体配置为：在 802.1p 优先级到本地优先级映射表中，输入值为 0、1、2 对应的输出值分别改为 0、1、2。

3. 验证配置

完成上述配置后，可以在 QoS 策略页面查看策略的应用状态。

1.3 系统功能配置举例

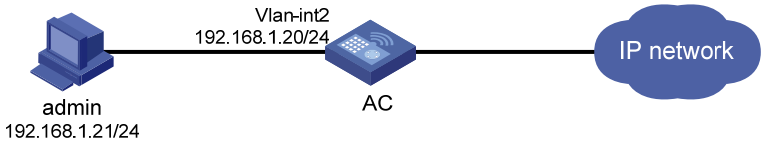
1.3.1 管理员配置举例

1. 组网需求

在 AC 上配置一个管理员帐户，用于用户采用 HTTP 方式登录 AC，具体要求如下：

- 用户使用管理员帐户登录时，AC 对其进行本地认证；
- 管理员帐户名称为 webuser，密码为 12345；
- 通过认证之后，用户被授予角色 network-admin。

图1-30 管理员配置组网图



2. 配置步骤

(1) 配置 VLAN 和 VLAN 接口

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入 VLAN 页面，创建 VLAN 2。进入 VLAN 2 的详情页面，将与管理员 PC 相连的接口加入 VLAN 2 的 Tagged 端口列表，并创建 VLAN 接口 2，配置 VLAN 接口 2 的 IP 地址为 192.168.1.20/24。

(2) 配置管理员账户

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“系统>管理员”，进入管理员页面，配置步骤为：

- 添加管理员。
- 配置用户名为 webuser，密码为 12345。
- 选择角色为 network-admin。
- 指定可用的服务为 HTTP 和 HTTPS。

3. 验证配置

(1) 完成上述配置后，在管理员页面上可以看到已成功添加的管理员帐户。

(2) 用户在 PC 的 Web 浏览器地址栏中输入 http://192.168.1.20 并回车后，浏览器将显示 Web 登录页面。用户在该登录页面中输入管理员帐户名称、密码以及验证码后，即可成功登录设备的 Web 页面进行相关配置。

2 网络功能配置举例

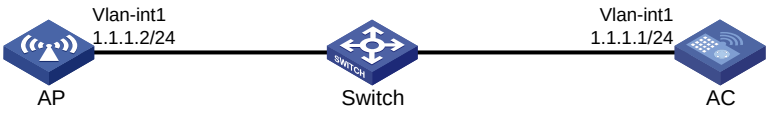
2.1 无线配置功能配置举例

2.1.1 配置通过DHCP发现方式建立CAPWAP隧道举例

1. 组网需求

如 图 2-1 所示，AP和AC通过交换机相连，AC作为DHCP服务器为AP提供DHCP服务。AP通过DHCP选项方式从DHCP服务器上获取AP和AC的IP地址，发现AC并与AC建立CAPWAP隧道连接。

图2-1 通过 DHCP 发现方式建立 CAPWAP 隧道典型组网图



2. 配置步骤

(1) 配置 AC 的 IP 地址

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN 接口 1 的 IP 地址为 1.1.1.1/24。

(2) 配置 DHCP 服务

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS > DHCP”，进入“DHCP”页面配置 DHCP 服务，配置步骤为：

- 开启 DHCP 服务。
- 配置 VLAN 接口 1 工作在 DHCP 服务器模式。
- 进入“地址池 > 地址分配”页面，创建名称为 pool1 的地址池，配置该地址池动态分配的地址段为 1.1.1.0/24，在地址池选项中配置网关地址为 1.1.1.1。
- 进入“地址池 > 地址池选项”页面”，配置 DHCP 选项 43 为客户端分配 AC 的 IP 地址，选项内容为 800700000101010101。

(3) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。

3. 验证配置

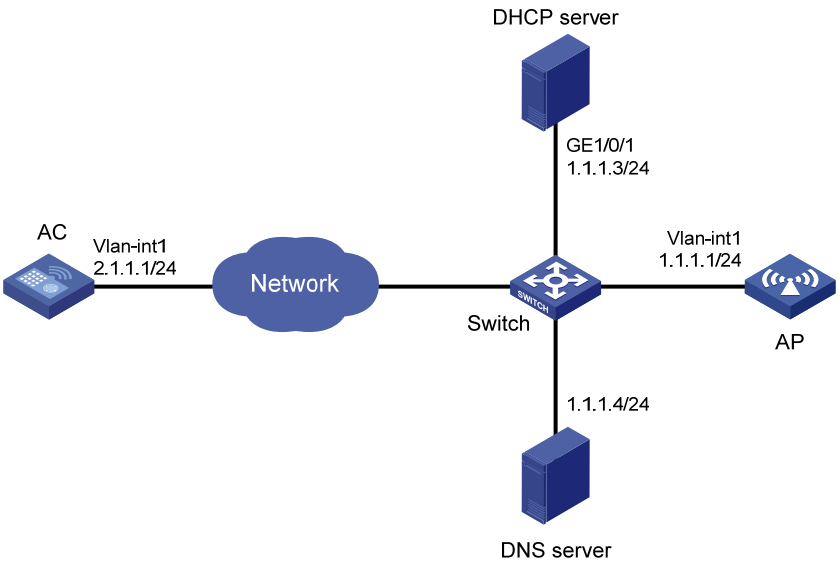
单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP”，进入“AP”页面可以查看到上线的 AP，通过查看详情可以看到 AP 获取到的 AP IP 地址、AC IP 地址和 AP 发现 AC 的方式。

2.1.2 配置通过DNS发现方式建立CAPWAP隧道举例

1. 组网需求

如 图 2-2 所示，DHCP server、DNS server、AP和AC通过交换机连接。由DHCP server为AP分配IP地址和AC的域名后缀，DNS server将AC的域名解析为AC的IP地址。

图2-2 通过 DNS 发现方式建立 CAPWAP 隧道典型组网图



2. 配置步骤

(1) 配置 DHCP server

在 DHCP server 上配置为 AP 分配 IP 地址和 AC 的域名后缀，分配的 IP 地址段为 1.1.1.0/24，AC 的域名后缀为 abc。（略）

(2) 配置 DNS server

在 DNS server 上添加 AC 域名和 AC IP 地址 1.1.1.1/24 的对应关系。（略）

(3) 配置 AC 的 IP 地址

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN 接口 1 的 IP 地址为 1.1.1.1/24。

(4) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。

3. 验证配置

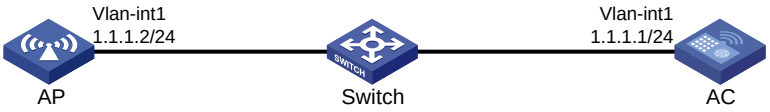
单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP”，进入“AP”页面可以查看到上线的 AP，通过查看上线 AP 的详细信息可以看到 AP 获取到的 AP IP 地址、AC IP 地址和 AP 发现 AC 的方式。

2.1.3 配置开启自动AP功能建立CAPWAP隧道举例

1. 组网需求

如 图 2-3 所示，AP和AC通过交换机相连。在AC上开启自动AP功能，MAC地址为 0011-2200-0101 的AP通过DHCP选项方式获取到AC的IP地址，AP通过获取到的AC的IP地址发现AC并与AC建立CAPWAP隧道连接。

图2-3 开启自动 AP 功能建立 CAPWAP 隧道典型组网图



2. 配置步骤

(1) 配置 AC 的 IP 地址

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > VLAN”，进入“VLAN”页面配置 VLAN 接口 1 的 IP 地址为 1.1.1.1/24。

(2) 配置 DHCP 服务

单击页面底部的<系统>按钮，进入“系统”菜单页面，然后单击页面左侧导航栏的“网络配置 > 服务 > DHCP/DNS > DHCP”，进入“DHCP”页面配置 DHCP 服务，配置步骤为：

- 开启 DHCP 服务。
- 配置 VLAN 接口 1 工作在 DHCP 服务器模式。
- 进入“地址池 > 地址分配”页面，创建名称为 pool1 的地址池，配置该地址池动态分配的地址段为 1.1.1.0/24，在地址池选项中配置网关地址为 1.1.1.1。
- 进入“地址池 > 地址池选项”页面”，配置 DHCP 选项 43 为客户端分配 AC 的 IP 地址，选项内容为 800700000101010101。

(3) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP 全局配置”，进入“AP 全局配置”页面开启自动 AP 功能。

3. 验证配置

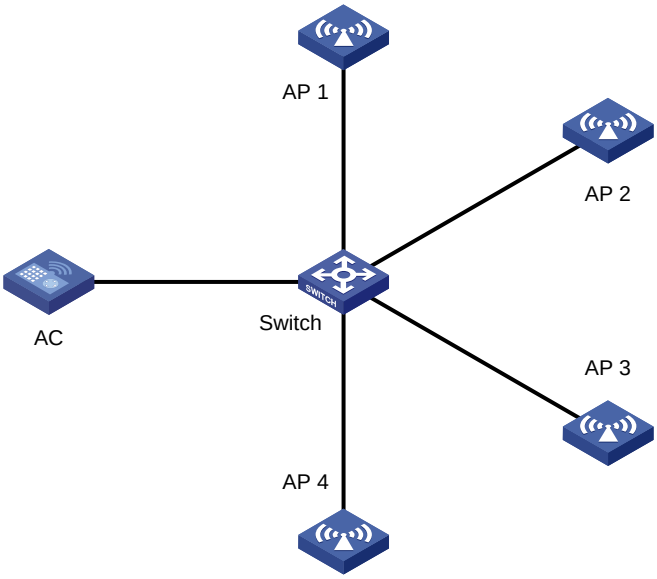
单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP”，进入“AP”页面可以查看到上线的自动 AP。

2.1.4 AP组配置举例

1. 组网需求

如 图 2-4 所示，AC通过交换机和AP 1、AP 2、AP 3、AP 4 相连；将AP1 加入group1，AP 2、AP 3 和AP 4 加入group2。AP 1、AP 2、AP 3 和AP4 名字分别为ap1、ap2、ap3 和ap4。

图2-4 AP 组配置举例



2. 配置步骤

(1) 配置 AP 通过 DHCP 方式获取 AP IP 地址及 AC IP 地址（略）。

(2) 配置 AP 组

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP 组”，进入“AP 组”页面，配置步骤为：

- 添加两个 AP 组，配置 AP 组名称为 group1 和 group2。
- 选中 AP 组，配置 AP 组 group1 的入组规则，创建 AP 名称入组规则，匹配数据为 ap1。
- 选中 AP 组，配置 AP 组 group2 的入组规则，创建 AP 名称入组规则，匹配数据为 ap2、ap3 和 ap4。

3. 验证配置

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理 > AP 组”，进入“AP 组”页面，选中 AP 组，查看 AP 组 group1 和 group2 的 AP 列表，可以看到 ap1 加入到 AP 组 group1 中，ap2、ap3 和 ap4 加入到 AP 组 group2 中。

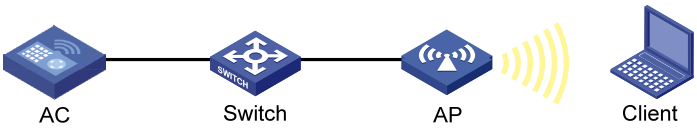
2.1.5 射频管理配置举例

1. 组网需求

如 图 2-5 所示，AP通过交换机与AC相连。对AP上的 5GHz射频进行配置，配置要求如下：

- 配置射频模式为 802.11ac，工作信道为 48，最大功率为 19dBm。
- 配置 802.11ac 的最大基本 NSS 为 2，最大支持 NSS 为 3，组播 NSS 为 2，VHT-MCS 索引值为 5。
- 配置 A-MPDU 功能、A-MSDU 功能来提高 AP 的吞吐量。

图2-5 射频管理基本功能配置组网图



2. 配置步骤

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 射频资源 > 射频管理”，进入“射频管理”页面，配置步骤为：

- 在“AP 组内所有 AP 的射频”中选择对应名称 AP 的 5GHz 射频进行编辑，在“基础”页面，配置射频模式为 802.11ac（5GHz），工作信道为 48，最大功率为 19dBm。
- 配置 802.11ac 的最大基本 NSS 为 2，最大支持 NSS 为 3，组播 NSS 为 2，组播 VHT-MCS 为 5。
- 开启 A-MPDU 和 A-MSDU 功能。
- 开启射频。

3. 验证配置

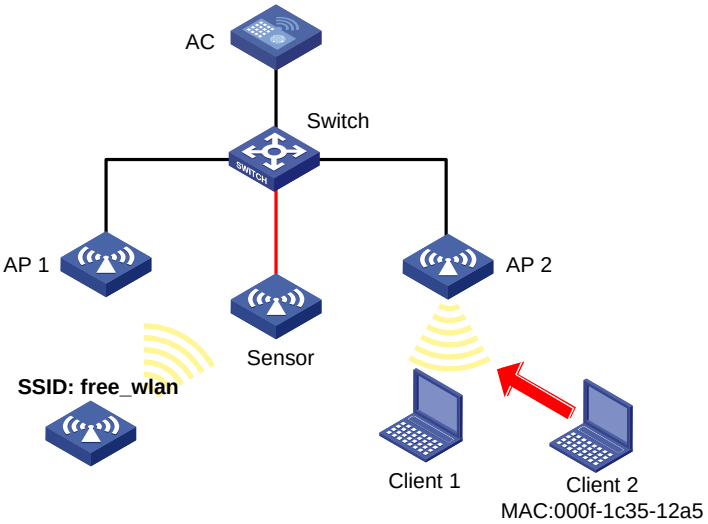
在 AP 节点导航栏中指定 AP 组下对应名称的 AP，单击页面左侧导航栏的“无线配置 > 射频管理”，进入“射频管理”页面，在“AP 组内所有 AP 的射频”中选择对应名称 AP 的 5GHz 射频，单击<编辑>按钮，可以查看 5GHz 射频上当前的配置。

2.1.6 WIPS分类与反制配置举例

1. 组网需求

如 图 2-6 所示，AP通过交换机与AC相连，AP 1 和AP 2 为Client提供无线服务，SSID为“abc”，在Sensor上开启WIPS功能，配置分类策略，将非法客户端的MAC地址（000f-1c35-12a5）添加到静态禁用列表中，将SSID“abc”添加到静态信任列表中，要求对检测到的潜在外部AP和非授权客户端进行反制。

图2-6 WIPS 分类与反制组网图



2. 配置步骤

(1) 配置手工 AP。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP 管理”页面，配置步骤为：

- 创建 AP 名称为 Sensor。
- 配置 AP 的型号、序列号。

(2) 配置 WIPS 功能。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线安全”，进入“无线安全”页面，配置步骤为：

- 在配置虚拟安全域的框里单击右上角的“+”：创建虚拟安全域 VSD_1。
- 单击开启 WIPS，编辑名称为 Sensor 的 AP，选择开启 WIPS 的射频接口，并加入虚拟安全域 VSD_1 中。
- 单击分类策略，创建分类策略 class1，将 Client 2 的 MAC 地址配置为禁用 MAC 地址，将 SSID abc 添加到信任 SSID 中。
- 单击反制策略，创建反制策略 protect，反制未授权客户端和潜在外部 AP。
- 编辑虚拟安全域 VSD_1，应用分类策略 class1 和反制策略 protect。

3. 验证配置

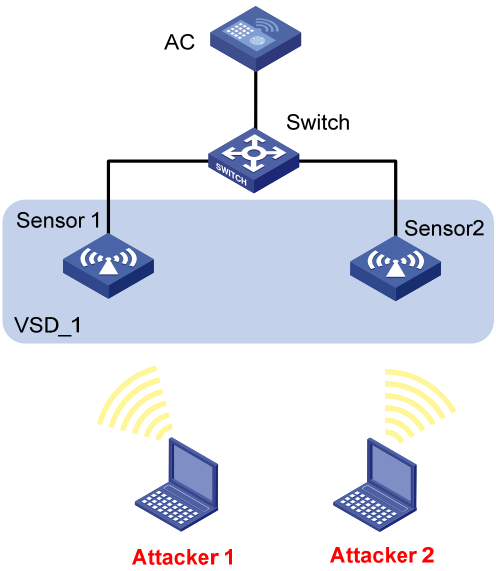
- 单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“监控 > 无线安全”，进入“无线安全”页面，在设备信息页面中可以查看无线设备的分类结果，在虚拟安全域 VSD_1，MAC 地址为 000f-e223-1616 的 AP 被分类成潜在外部 AP，MAC 地址为 000f-1c35-12a5 的客户端被分类为未授权的客户端。
- 单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“监控 > 无线安全”，进入“无线安全”页面，在反制记录页面中可以查看反制过的设备记录信息，在虚拟安全域 VSD_1，MAC 地址为 000f-1c35-12a5 的未授权客户端和 MAC 地址为 000f-e223-1616 的潜在外部 AP 被反制。

2.1.7 WIPS畸形报文检测和泛洪攻击检测配置举例

1. 组网需求

如 图 2-7 所示，AP通过交换机与AC相连，将两台AP分别配置为Sensor，配置虚拟安全域VSD_1，并配置两台Sensor属于这个虚拟安全域，当检测到攻击者对无线网络进行IE重复的畸形报文或Beacon帧泛洪攻击时，AP向AC发送告警信息。

图2-7 畸形报文检测和泛洪攻击检测组网图



2. 配置步骤

(1) 配置手工 AP。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP 管理”页面，配置步骤为：

- 创建 AP 名称为 Sensor 1 和 Sensor 2。
- 配置 AP 的型号、序列号。

(2) 配置 WIPS 功能。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线安全”，进入“无线安全”页面，配置步骤为：

- 在配置虚拟安全域的框里单击右上角的“+”：创建虚拟安全域 VSD_1。
- 单击开启 WIPS，编辑名称为 Sensor 1 和 Sensor 2 的 AP，选择开启 WIPS 的射频接口，并加入虚拟安全域 VSD_1。
- 单击攻击检测策略，创建攻击检测策略，配置当检测到 IE 重复的畸形报文和 Beacon 帧泛洪攻击时，向 AC 发送日志信息或告警信息。检测 IE 重复的畸形报文的静默时间为 50 秒，检测 Beacon 帧的统计周期为 100 秒，触发阈值为 200，静默时间为 50 秒。
- 编辑虚拟安全域 VSD_1，应用攻击检测策略。

3. 验证配置

- 单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“监控 > 无线安全”，进入“无线安全”页面，当网络中没有攻击者时，查看攻击统计信息，畸形报文和泛洪报文的统计个数为 0。
- 单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“监控 > 无线安全”，进入“无线安全”页面，当检测到 IE 重复的畸形报文和 Beacon 帧泛洪攻击时，查看攻击统计信息，可以查看到 IE 重复的畸形报文和 Beacon 帧泛洪攻击的统计个数。

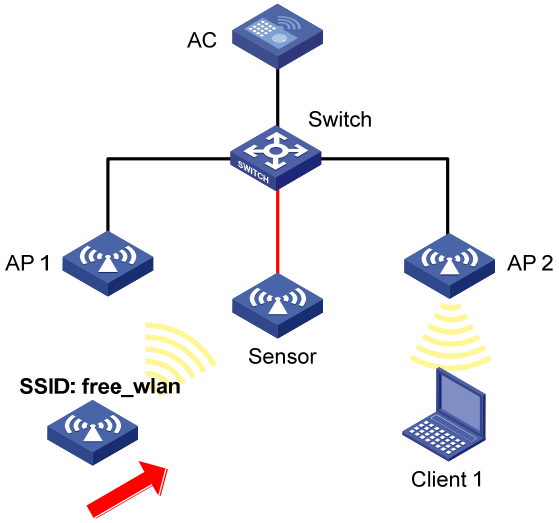
2.1.8 Signature检测配置举例

1. 组网需求

如 图 2-8 所示，AP通过交换机与AC相连，AP1 和AP2 为Client提供无线服务，SSID为“abc”，在Sensor上开启WIPS功能，配置Signature检测，检测无线环境中是否存在其他的无线服务，对SSID不是abc的Beacon帧进行检测， Sensor向AC发送告警信息。

2. 组网图

图2-8 WIPS 的攻击检测组网图



3. 配置步骤

(1) 配置手工 AP。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP 管理”页面，配置步骤为：

- 创建 AP 名称为 Sensor。
- 配置 AP 的型号、序列号。

(2) 配置 WIPS 功能。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线安全”，进入“无线安全”页面，配置步骤为：

- 在配置虚拟安全域的框里单击右上角的“+”：创建虚拟安全域 vsd1。

- 单击开启 WIPS，编辑名称为 Sensor 的 AP，选择开启 WIPS 的射频接口，并加入虚拟安全域 vsd1 中。
- 单击 Signature 规则，创建 Signature 规则 1，配置子规则对 SSID 不是 abc 的 Beacon 帧进行检测。
- 单击 Signature 策略，创建 Signature 策略 sig1，应用 Signature 规则 1，配置统计周期为 5 秒，发出告警后的静默时间为 60 秒，统计次数的阈值为 60。
- 编辑虚拟安全域 vsd1，应用 Signature 策略。

4. 验证配置

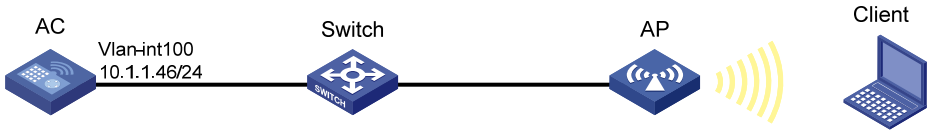
当检测到 SSID 为“free_wlan”的无线服务后，AC 会收到 Sensor 发送的告警信息。

2.1.9 共享密钥认证配置举例

1. 组网需求

AC 旁挂在 Switch 上，Switch 同时作为 DHCP server 为 AP 和 Client 分配 IP 地址。通过配置客户端在链路层使用 WEP 密钥 12345 接入无线网络。

图2-9 共享密钥认证配置组网图



2. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service1。
- 配置 SSID 为 service。
- 开启无线服务。

(2) 配置认证模式为静态 WEP 密钥

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，在“无线网络”页面单击 service1 的编辑按钮，进入“链路层认证”页面，配置步骤为：

- 选择认证模式为静态 WEP 密钥。
- 选择密钥类型为 Passphrase
- 选择加密套件为 WEP40。
- 配置明文密钥为 12345。

(3) 将无线服务绑定到 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 选中创建的无线服务 service1，单击“绑定到 AP”按钮，进入到“绑定到 AP”页面。

- 选中 AP 的 5GHz 射频单元，单击“快速绑定”。

(4) 验证配置

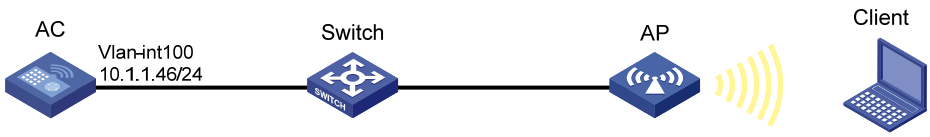
配置完成后，查看无线服务详情，可以看到已经创建的名称为 service1 无线服务以及配置的认证信息。

2.1.10 PSK身份认证与密钥管理模式和Bypass认证配置举例

1. 组网需求

- AC 旁挂在 Switch 上，Switch 同时作为 DHCP server 为 AP 和 Client 分配 IP 地址。通过配置客户端 PSK 密钥 12345678 接入无线网络。
- 客户端链路层认证使用开放式系统认证，用户接入认证使用 Bypass 认证的方式实现客户端可以不需要认证直接接入 WLAN 网络的目的。
- 通过配置客户端和 AP 之间的数据报文采用 PSK 身份认证与密钥管理模式来确保用户数据的传输安全。

图2-10 PSK+Bypass 认证配置组网图



2. 配置步骤

(1) 创建无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建无线服务，名称为 service1。
- 配置 SSID 为 service。
- 开启无线服务。

(2) 配置认证模式为静态 PSK 密钥

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，在“无线网络”页面单击 service1 的编辑按钮，进入“链路层认证”页面，配置步骤为：

- 选择认证模式为静态 PSK 密钥。
- 选择安全模式为 WPA。
- 选择加密套件为 CCMP。
- 选择密钥类型为 Passphrase，明文密钥为 12345678。

(3) 将无线服务绑定到 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 选中创建的无线服务 service1，单击“绑定到 AP”按钮，进入到“绑定到 AP”页面。
- 选中 AP 的 5GHz 射频单元，单击“快速绑定”。

3. 验证配置

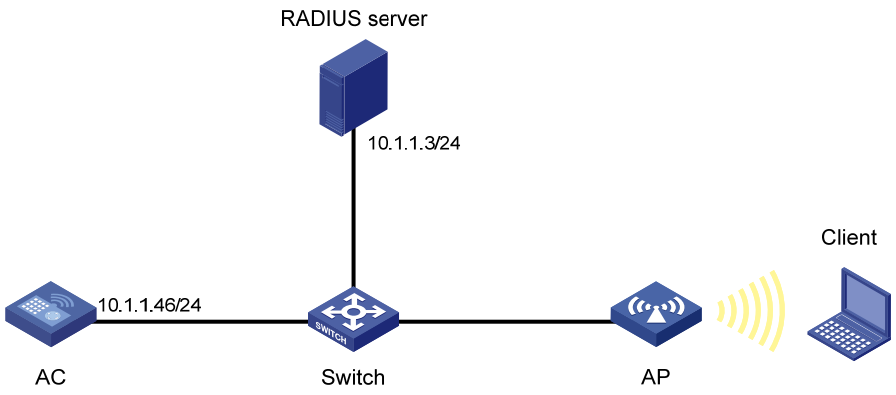
配置完成后，查看无线服务详情，可以看到已经创建的名称为 service1 无线服务以及配置的认证信息。

2.1.11 PSK身份认证与密钥管理模式和MAC地址认证配置举例

1. 组网需求

- AC 旁挂在 Switch 上，Switch 同时作为 DHCP server 为 AP 和 Client 分配 IP 地址。通过配置客户端 PSK 密钥 12345678 接入无线网络。
- 客户端链路层认证使用开放式系统认证，客户端通过 RADIUS 服务器进行 MAC 地址认证。
- 通过配置客户端和 AP 之间的数据报文采用 PSK 认证密钥管理模式来确保用户数据的传输安全。

图2-11 PSK 密钥管理模式和 MAC 认证配置组网图



2. 配置步骤

说明

- 在 RADIUS 服务器上配置，将 Client 的 MAC 地址作为认证的用户名和密码，且该 MAC 地址在配置时不能出现大写和连字符。完成 RADIUS 服务器的其它配置，并保证用户的认证/授权/计费功能正常运行。
- 完成设备上 RADIUS 和 Domain 域的配置。

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service1。
- 配置 SSID 为 service。
- 开启无线服务。

(2) 配置认证模式为静态 PSK 密钥和 MAC 地址认证

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，在“无线网络”页面单击 service1 的编辑按钮，进入“链路层认证”页面，配置步骤为：

- 选择认证模式为静态 PSK 密钥和 MAC 地址认证。
- 选择安全模式为 WPA。
- 选择加密套件为 CCMP。
- 选择密钥类型为 Passphrase，明文密钥为 12345678。
- 配置域名为 dom1。

(3) 将无线服务绑定到 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 选中创建的无线服务 service1，单击“绑定到 AP”按钮，进入到“绑定到 AP”页面。
- 选中 AP 的 5GHz 射频单元，单击“快速绑定”。

(4) 验证配置

配置完成后，查看无线服务详情，可以看到已经创建的名称为 service1 无线服务以及配置的认证信息。

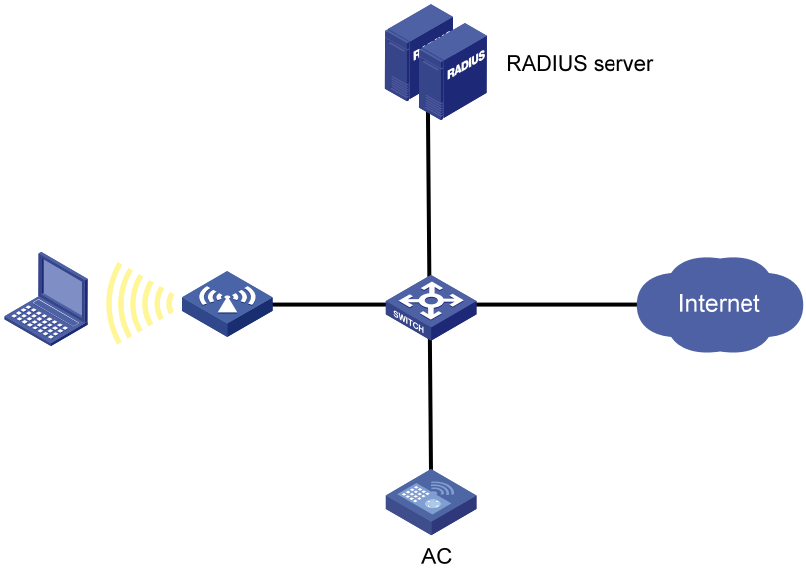
2.1.12 802.1X用户的RADIUS认证配置举例

1. 组网需求

用户接入无线网络，AC 对接入的用户进行 802.1X 认证以控制其访问 Internet，具体要求如下：

- RADIUS 服务器作为认证/授权/计费服务器与 AC 相连，其 IP 地址为 10.1.1.1/24。
- 端口 GigabitEthernet1/0/1 下的所有接入用户均需要单独认证，当某个用户下线时，也只有该用户无法使用网络。
- AC 对 802.1X 用户进行认证时，采用 RADIUS 认证方式，认证 ISP 域为 dm1X。
- AC 与 RADIUS 认证/授权和计费服务器交互报文时的共享密钥均为 name，认证/授权、计费的端口号分别为 1812 和 1813，向 RADIUS 服务器发送的用户名不携带域名。

图2-12 802.1X 用户的 RADIUS 认证配置组网图



2. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置 RADIUS 方案

单击页面底部的<网络>按钮，然后单击左侧导航栏“网络安全 > 认证”，然后单击“RADIUS”，再单击<添加>按钮，添加 RADIUS 方案，配置步骤为：

- 方案名称为 802.1X。
- 指定主认证服务器 IP 地址为 10.1.1.1，端口号为 1812，共享密钥为 name。设置主认证服务器状态为活动。
- 指定主计费服务器 IP 地址为 10.1.1.1，端口号为 1813，共享密钥为 name。设置主计费服务器状态为活动。
- 在显示高级设置里指定发送给 RADIUS 服务器的用户名格式为不携带域名。

(3) 配置 ISP 域

单击左侧导航栏“网络安全 > 认证”，进入“ISP 域”页面配置，配置步骤为：

- 添加 ISP 域，名称为 dm1X，并将该 ISP 域的状态设置为活动。
- 指定接入方式为 LAN 接入。
- 指定 LAN 接入 AAA 方案的认证、授权和计费的方法均为 RADIUS，方案都选择 802.1X。
- 单击<确定>按钮。

(4) 配置 802.1X

单击左侧导航栏“无线配置 > 无线网络”，进入无线网络页面配置，单击<添加>按钮，配置步骤为：

- 基础设置部分配置无线服务名称和 SSID。
- 安全认证部分认证模式选择 802.1X 认证。
- 域名为 dm1X。
- 单击<确定>按钮。

(5) 配置 RADIUS 服务器

在 RADIUS 服务器上添加用户帐户，保证用户的认证/授权/计费功能正常运行。具体配置方法请参考关于 RADIUS 服务器的配置说明。

3. 验证配置

(1) 单击左侧导航栏“网络安全 > 认证”，然后单击“RADIUS”页签，可以看到已添加成功的 RADIUS 方案 802.1X 的概要信息。

(2) 单击左侧导航栏“网络安全 > 认证”，在 ISP 域页面上，可以看到已添加成功的 ISP 域的 dm1X 的概要信息。

(3) 用户启动 802.1X 客户端，输入正确的用户名和密码之后，可以成功上线。

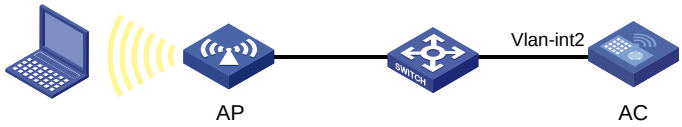
2.1.13 802.1X用户的本地认证配置举例

1. 组网需求

用户接入无线网络，AC 对接入的用户进行 802.1X 认证以控制其访问 Internet，具体要求如下：

- AC 对 802.1X 用户采用本地认证，认证域为 abc。
- 802.1X 用户的认证名为 dotuser，认证密码为 12345。

图2-13 802.1X 用户的本地认证配置组网图



2. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置本地用户

单击页面底部的<网络>按钮，然后单击左侧导航栏“网络安全 > 用户管理”，进入“本地认证”页面配置，配置步骤为：

- 添加用户，用户名为 dotuser，密码为 12345。
- 指定可用服务为 LAN 接入。

(3) 配置 ISP 域

单击左侧导航栏“网络安全 > 认证”，进入“ISP 域”页面配置，配置步骤为：

- 添加 ISP 域，名称为 abc，并将该 ISP 域的状态设置为活动。
- 指定接入方式为 LAN 接入。
- 指定 LAN 接入 AAA 方案的认证方法为本地认证，授权方法为本地授权，计费方法为不计费。

(4) 配置 802.1X

单击左侧导航栏“无线配置 > 无线网络”页面配置，配置步骤为：

- 基础设置部分配置无线服务名称和 SSID。
- 安全认证部分认证模式选择 802.1X 认证。
- 域名为 abc。

3. 验证配置

(1) 完成上述配置后，单击左侧导航栏“网络安全 > 用户管理”，在“本地认证”页面上可以看到已成功添加的本地用户。

(2) 单击左侧导航栏“网络安全 > 认证”，在“ISP 域”页面上可以看到已经成功添加的 ISP 域。

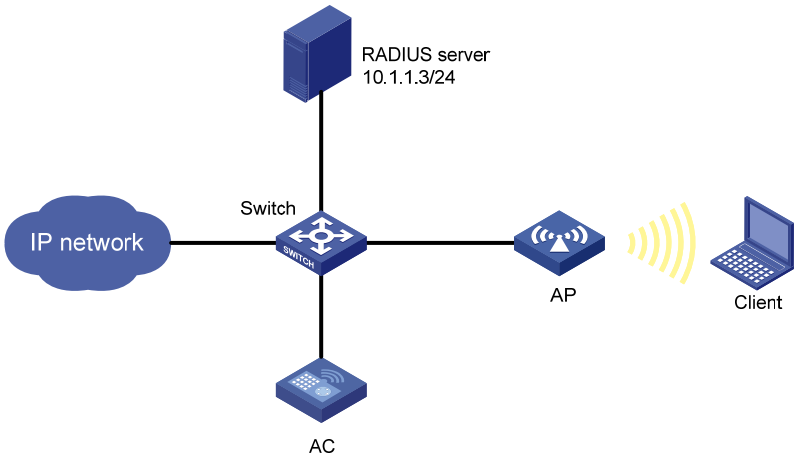
(3) 用户启动 802.1X 客户端，输入正确的用户名和密码之后，可以成功上线。

2.1.14 802.1X身份认证与密钥管理模式配置举例

1. 组网需求

- AP 旁挂在 Switch 上，Switch 同时作为 DHCP server 为 AP 和 Client 分配 IP 地址。
- 客户端链路层认证使用开放式系统认证，客户端通过 802.1X 接入认证的方式实现客户端可使用用户名 abcdef 和密码 123456 接入 WLAN 网络的目的。
- 通过配置客户端和 AP 之间的数据报文采用 802.1X 身份认证与密钥管理来确保用户数据的传输安全。

图2-14 802.1X 认证配置组网图



2. 配置步骤

说明

- 完成 RADIUS 服务器的配置，添加用户帐户，用户名为 abcedf，密码为 123456，并保证用户的认证/授权/计费功能正常运行。
- 完成设备上 RADIUS 和 Domain 域的配置。

(1) 配置无线服务

单击页面底部的<网络>按钮，然后单击左侧导航栏“无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 单击<添加>按钮，创建一个无线服务，无线服务名称为 service1。
- 配置 SSID 为 service。
- 无线服务状态选择“开启”。

- 单击<确定>按钮。

(2) 配置认证模式为 802.1X 认证

完成上述配置后，会返回“全部网络 > 无线配置 > 无线网络 > 无线网络”页面，单击无线名称为“service1”表项后面的<编辑>按钮，再单击页面上方的“链路层认证”页签，进入认证配置页面，配置步骤为：

- 选择认证模式为 802.1X 认证。
- 选择安全模式为 WPA。
- 选择加密套件为 CCMP。
- 配置域名为 dom1。
- 单击<确定>按钮。

(3) 将无线服务绑定到 AP

进入“全部网络 > 无线配置 > 无线网络 > 无线网络”页面，配置步骤：

- 选中创建的无线服务 service1，单击“绑定到 AP”按钮，进入到“绑定到 AP”页面。
- 选中 AP 的 5GHz 射频单元，单击“快速绑定”。

(4) 验证配置

配置完成后，查看无线服务详情，可以看到已经创建的名称为 service1 无线服务以及配置的认证信息。

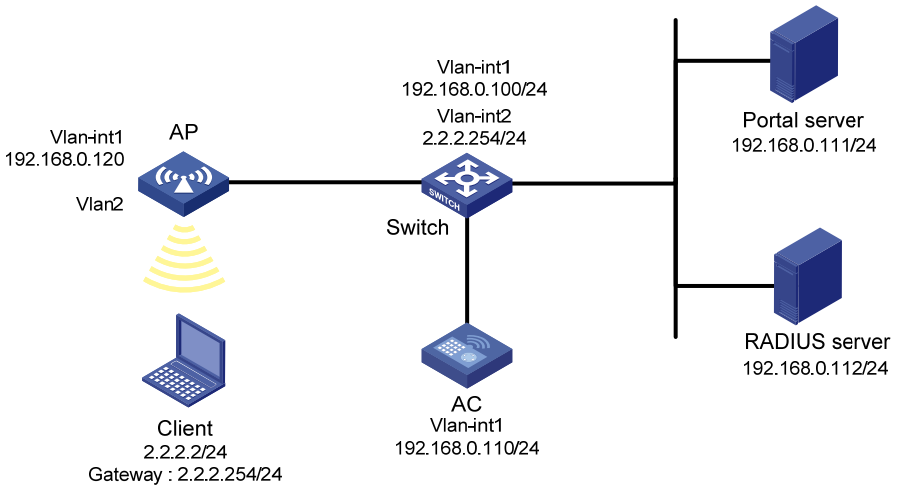
2.1.15 Portal直接认证配置举例

1. 组网需求

在本地转发模式下，对通过无线接入的用户采用直接认证方式。

- 无线客户端通过手工配置或 DHCP 获取的一个公网 IP 地址进行认证，在通过 Portal 认证前，只能访问 Portal Web 服务器；在通过 Portal 认证后，可以使用此 IP 地址访问非受限互联网资源。
- 采用一台 Portal 服务器承担 Portal 认证服务器和 Portal Web 服务器的职责。
- 采用 RADIUS 服务器作为认证/计费服务器。

图2-15 Portal 直接认证配置组网图



2. 配置步骤

说明

- 按照组网图配置设备各接口的 IP 地址，保证启动 Portal 之前各 Client、服务器和 AC 之间的路由可达。
- 完成 RADIUS 服务器上的配置，保证用户的认证/计费功能正常运行。
- 完成 AP 上的配置，保证 AP 与 AC 能够互通。
- 完成设备上 RADIUS 和 Domain 域的配置。

(1) 配置无线服务

单击页面底部的<网络>按钮，然后单击左侧导航栏“无线配置 > 无线网络”进入“无线网络”页面，配置步骤为：

- 单击<添加>按钮，创建一个无线服务，无线服务名称为 service1。
- 配置 SSID 为 service。
- 无线服务状态选择“开启”。
- 单击<确定>按钮。

(2) 配置认证模式为 Portal 认证

完成上述配置后，会返回“全部网络 > 无线配置 > 无线网络 > 无线网络”页面，单击无线名称为“service1”表项后面的<编辑>按钮，再单击页面上方的“链路层认证”，进入认证配置页面，配置步骤为：

- 选择认证模式为 Portal 认证。
- 配置域名为 dm1。
- 选择 Web 服务器名称为 newpt。
- 配置 BAS-IP 为 192.168.0.110。
- 单击<确定>按钮。

(3) 将无线服务绑定到 AP

进入“全部网络 > 无线配置 > 无线网络 > 无线网络”页面，配置步骤：

- 选中创建的无线服务 service1，单击“绑定到 AP”按钮，进入到“绑定到 AP”页面。
- 选中 AP 的 5GHz 射频单元，单击“绑定”按钮。
- 配置绑定到 VLAN 2，单击“确定”按钮。

(4) 验证配置

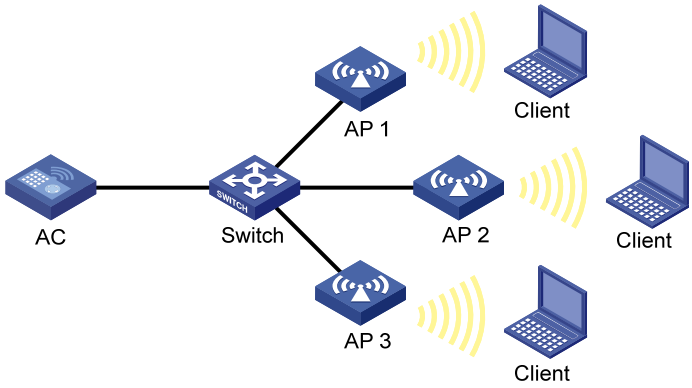
配置完成后，查看无线服务详情，可以看到已经创建的名称为 service1 无线服务以及配置的认证信息。

2.1.16 WLAN RRM信道调整配置举例

1. 组网需求

如 图 2-16 所示，客户端通过AP接入无线服务，当信道变差达到信道调整触发条件时，AC能自动切换信道，保证客户端的无线服务质量。要求AP 1 的Radio 1 避免进行频繁的信道调整。

图2-16 自动信道调整配置组网图



2. 配置步骤

(1) 配置 AP 射频的工作信道（缺省为自动选择，且信道不锁定）

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“射频配置”页面，配置 AP 1、AP 2、AP 3 上射频的工作信道为“自动选择不锁定”。

(2) 配置 RRM

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“射频优化”页面，配置步骤为：

- 在“AP RRM 配置”中开启 AP 1、AP 2、AP 3 上射频的自动信道调整功能，配置 CRC 错误门限为 30，信道干扰门限为 60，容限系数为 25。
- 在“RRM 保持调整组”中创建 ID 为 10 的 RRM 保持调整组，配置信道保持时长为 600 分钟，添加保持调整组成员为 AP 1 的 5GHz 射频单元。

3. 验证配置

(1) 调整周期超时后，如果某个 AP 的当前工作信道质量达到任意一个信道调整门限，AC 将为该 AP 进行信道调整。单击页面左侧导航栏的“ 监控 > 射频监控”，进入“射频优化”页面，可以查看信道调整前后，AP 所使用的信道和信道调整的详细信息。

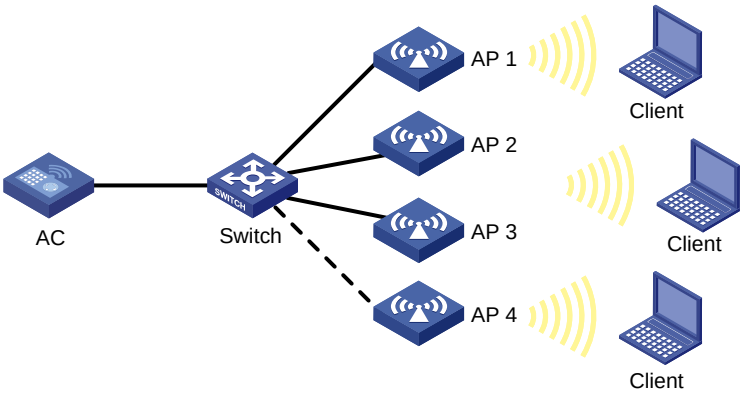
(2) 在调整周期超时后的 600 分钟内，AP 1 的 Radio 1 的信道不会进行调整。

2.1.17 WLAN RRM功率调整配置举例

1. 组网需求

如 图 2-17 所示，无线网络中原本存在AP 1～AP 3，每个AP上仅开启一个Radio，客户端通过AP 1接入无线网络。要求当AP 4 加入AC时，各AP能够自动调整发送功率，并且避免AP 1 的Radio 1 进行频繁的功率切换。

图2-17 自动功率调整配置组网图



2. 配置步骤

(1) 配置 AP 射频的功率锁定状态为关闭

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“射频配置”页面，配置 AP 1、AP 2、AP 3 和 AP 4 的功率锁定状态为关闭。

(2) 配置 RRM

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“射频优化”页面，配置步骤为：

- 在“AP RRM 配置”中开启 AP 1、AP 2、AP 3 和 AP 4 的自动功率调整功能，配置功率调整模式为自定义，最大邻居数为 3，功率调整门限为-70dBm，最小发射功率为 5dBm。
- 在“RRM 保持调整组”中创建 ID 为 10 的 RRM 保持调整组，配置功率保持时长为 100 分钟，添加保持调整组成员为 AP 1 的 5GHz 射频单元。

3. 验证配置

(1) 调整周期超时后，如果某个 AP 的当前发送功率达到功率调整门限，AC 将为该 AP 进行功率调整。单击页面左侧导航栏的“ 监控 > 射频监控”，进入“射频优化”页面，可以查看功率调整前后，AP 所使用的功率和功率调整的详细信息。

(2) 在调整周期超时后的 100 分钟内，AP 1 的 Radio 1 的功率不会进行调整。

2.1.18 会话模式的Radio负载均衡配置举例

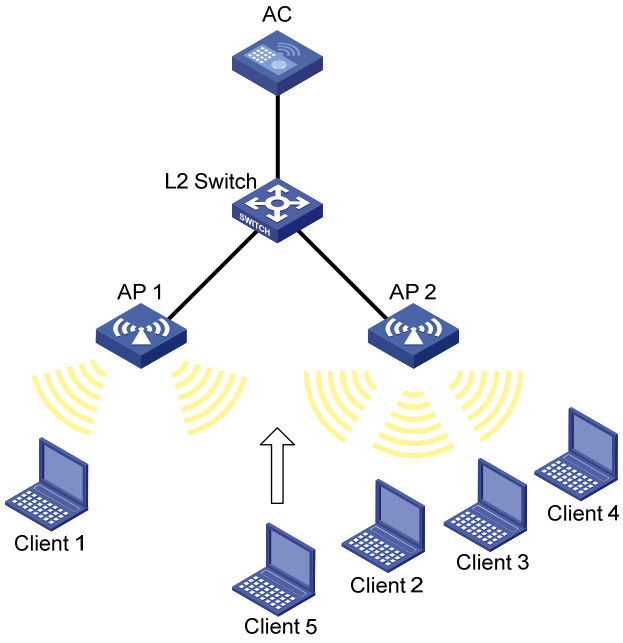
1. 组网需求

AC 连接了两个 AP，这两个 AP 的 Radio 覆盖区域有重叠，为了对这两个 AP 上 Radio 的接入载荷进行负载均衡，有以下要求：

- 负载均衡的评判依据为在线客户端数量。
- 当 Radio 上的在线客户端数量达到或超过 3，并且与另一个 Radio 上的在线客户端数量差值达到或超过 2，开始运行负载均衡。

2. 组网图

图2-18 会话模式的 Radio 负载均衡配置组网图



3. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 session-balance。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP2。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。

(3) 配置负载均衡

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“负载均衡”页面，配置步骤为：

- 点击“全局配置”的“更多”按钮进入“详细信息”页面，选择状态为“开启”。
- 选择模式为“会话模式”。

- 配置会话门限值为 3，会话差值门限值为 2。

4. 验证配置

当 Radio 上的在线客户端数量达到或超过 3，并且与另一个 Radio 上的在线客户端数量差值达到或超过 2，开始运行负载均衡。通过单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 Radio 2 和 AP 2 的 Radio 2 上关联的客户端数量达到均衡。

2.1.19 流量模式的Radio负载均衡配置举例

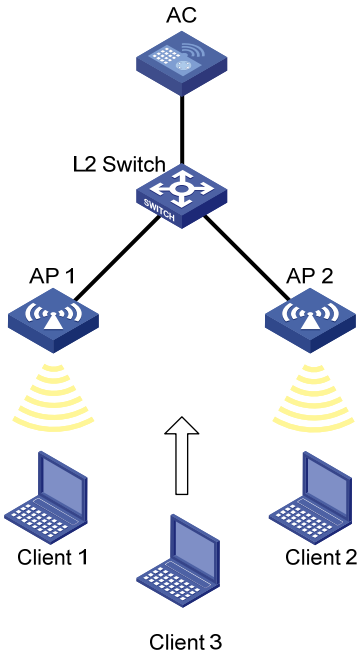
1. 组网需求

AC 连接了两个 AP，这两个 AP 的 Radio 覆盖区域有重叠，为了对这两个 AP 上 Radio 的接入载荷进行负载均衡，有以下要求：

- 负载均衡的评判依据为 Radio 的流量值。
- 当 Radio 上的流量达到或超过 30Mbps（即流量值为占 Radio 最大支持带宽的 20%），并且与另一个 Radio 上的流量差值达到或超过 15Mbps（即流量差值为占 Radio 最大支持带宽的 10%），开始运行负载均衡。

2. 组网图

图2-19 流量模式的 Radio 负载均衡配置组网图



3. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 traffic-balance。

- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP2。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。

(3) 配置负载均衡

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“负载均衡”页面，配置步骤为：

- 点击“全局配置”的“更多”按钮进入“详细信息”页面，选择状态为“开启”。
- 选择模式为“流量模式”。
- 配置流量门限值为 20，流量差值门限值为 10。

4. 验证配置

当 Radio 上的流量达到或超过 30Mbps，并且与另一个 Radio 上的流量差值达到或超过 15Mbps，开始运行负载均衡。通过单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 Radio 2 和 AP 2 的 Radio 2 上关联的客户端数量达到均衡。

2.1.20 带宽模式的Radio负载均衡配置举例

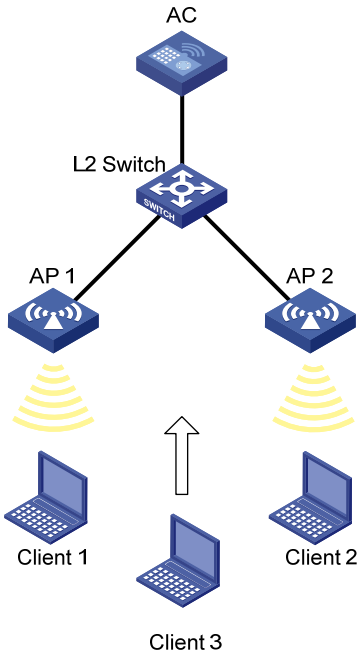
1. 组网需求

AC 连接了两个 AP，这两个 AP 的 Radio 覆盖区域有重叠，为了对这两个 AP 上 Radio 的接入载荷进行负载均衡，有以下要求：

- 负载均衡的评判依据为 Radio 的带宽值。
- 当 Radio 上的带宽达到或超过 12Mbps，并且与另一个 Radio 上的带宽差值达到或超过 3Mbps，开始运行负载均衡。

2. 组网图

图2-20 带宽模式的 Radio 负载均衡配置组网图



3. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 bandwidth-balance。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP2。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。

(3) 配置负载均衡

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“负载均衡”页面，配置步骤为：

- 点击“全局配置”的“更多”按钮进入“详细信息”页面，选择状态为“开启”。
- 选择模式为“带宽模式”。

- 配置带宽门限值为 12Mbps，带宽差值门限值为 3Mbps。

4. 验证配置

当 Radio 上的流量达到或超过 12Mbps，并且与另一个 Radio 上的流量差值达到或超过 3Mbps，开始运行负载均衡。通过单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 Radio 2 和 AP 2 的 Radio 2 上关联的客户端数量达到均衡。

2.1.21 会话模式的负载均衡组配置举例

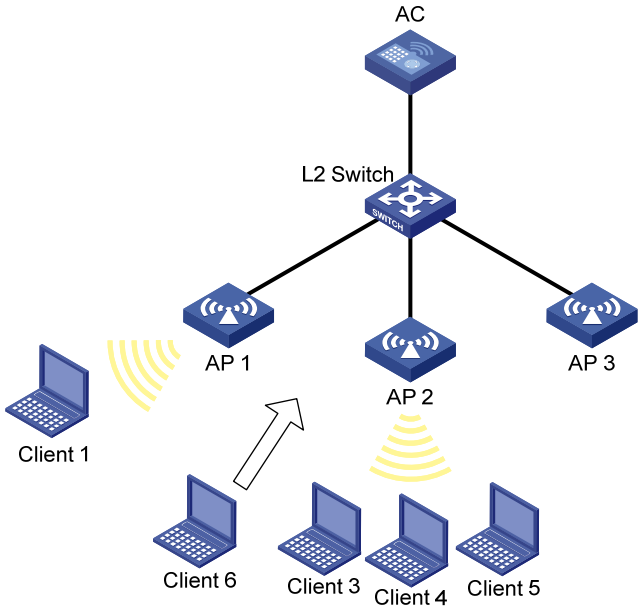
1. 组网需求

AC 连接了三个 AP，这三个 AP 的 radio 覆盖区域有重叠，为了对这三个 AP 上 Radio 的接入载荷进行负载均衡，有以下要求：

- 负载均衡的评判依据为在线客户端数量。
- 仅需要对 AP 1 的 Radio 2 和 AP 2 的 Radio 2 进行负载均衡。
- 当 Radio 上的在线客户端数量达到或超过 3，并且与另一个 Radio 上的在线客户端数量差值达到或超过 2，开始运行负载均衡。

2. 组网图

图2-21 会话模式的负载均衡组配置组网图



3. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 session-balance。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP2。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP3。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。
- 进入 AP 3 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 3 的射频。

(3) 配置负载均衡

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“负载均衡”页面，配置步骤为：

- 点击“全局配置”的“更多”按钮进入“详细信息”页面，选择状态为“开启”。
- 选择模式为“会话模式”。
- 配置会话门限值为 3，会话差值门限值为 2。
- 进入负载均衡组配置页面，创建负载均衡组 1
- 将 AP 1 的 Radio 2 和 AP 2 的 Radio 2 绑定到负载均衡组中。

4. 验证配置

AP 1 的 Radio 2 和 AP 2 的 Radio 2 在同一个负载均衡组中，AP 3 的 Radio 2 没有加入负载均衡组。由于负载均衡只对组内的 Radio 生效，所以 AP 3 的 Radio 2 不参与负载均衡。

当参与运行负载均衡的某个 Radio 上的在线客户端数量达到或超过 3，并且与另一个 Radio 上的在线客户端数量差值达到或超过 2，开始运行负载均衡。通过单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 Radio 2 和 AP 2 的 Radio 2 上关联的客户端数量达到均衡。

2.1.22 流量模式的负载均衡组配置举例

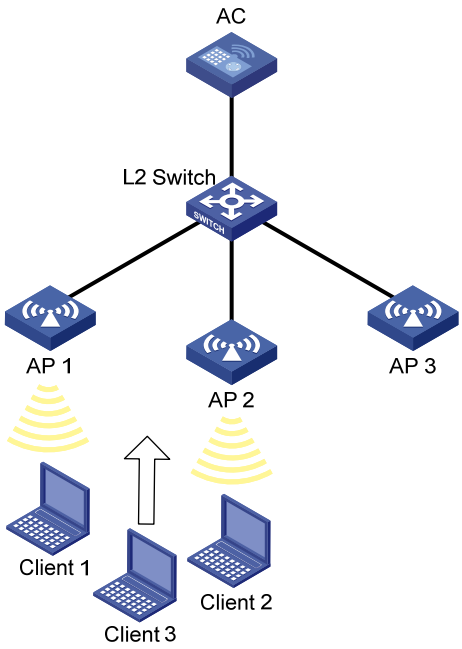
1. 组网需求

AC 连接了三个 AP，这三个 AP 的 radio 覆盖区域有重叠，为了对这三个 AP 上 Radio 的接入载荷进行负载均衡，有以下要求：

- 负载均衡的评判依据为 Radio 的流量值。
- 仅需要对 AP 1 的 Radio 2 和 AP 2 的 Radio 2 进行负载均衡。
- 当 Radio 上的流量达到或超过 30Mbps（即流量值为占 Radio 最大支持带宽的 20%），并且与另一个 Radio 上的流量差值达到或超过 15Mbps（即流量差值为占 Radio 最大支持带宽的 10%），开始运行负载均衡。

2. 组网图

图2-22 流量模式的负载均衡组网图



3. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 traffic-balance。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP2。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP3。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。
- 进入 AP 3 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 3 的射频。

(3) 配置负载均衡

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“负载均衡”页面，配置步骤为：

- 点击“全局配置”的“更多”按钮进入“详细信息”页面，选择状态为“开启”。
- 选择模式为“流量模式”。
- 配置流量门限值为 20，流量差值门限值为 10。
- 进入负载均衡组配置页面，创建负载均衡组 1
- 将 AP 1 的 Radio 2 和 AP 2 的 Radio 2 绑定到负载均衡组中。

4. 验证配置

AP 1 的 Radio 2 和 AP 2 的 Radio 2 在同一个负载均衡组中，AP 3 的 Radio 2 没有加入负载均衡组。由于负载均衡只对组内的 Radio 生效，所以 AP 3 的 Radio 2 不参与负载均衡。

当参与运行负载均衡的某个 Radio 上的流量达到或超过 30Mbps，并且与另一个 Radio 上的流量差值达到或超过 15Mbps，开始运行负载均衡。通过单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 Radio 2 和 AP 2 的 Radio 2 上关联的客户端数量达到均衡。

2.1.23 带宽模式的负载均衡组配置举例

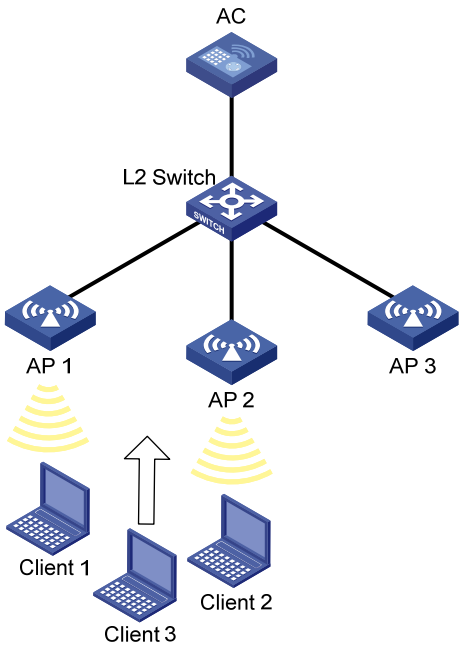
1. 组网需求

AC 连接了三个 AP，这三个 AP 的 radio 覆盖区域有重叠，为了对这三个 AP 上 Radio 的接入载荷进行负载均衡，有以下要求：

- 负载均衡的评判依据为 Radio 的带宽值。
- 仅需要对 AP 1 的 Radio 2 和 AP 2 的 Radio 2 进行负载均衡。
- 当 Radio 上的带宽达到或超过 12Mbps，并且与另一个 Radio 上的带宽差值达到或超过 3Mbps，开始运行负载均衡。

2. 组网图

图2-23 带宽模式的负载均衡组网图



3. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 bandwidth-balance。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP2。
- 配置 AP 型号及序列号。
- 配置 AP 名称为 AP3。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的射频。
- 进入 AP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 2 的射频。
- 进入 AP 3 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 3 的射频。

(3) 配置负载均衡

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“负载均衡”页面，配置步骤为：

- 点击“全局配置”的“更多”按钮进入“详细信息”页面，选择状态为“开启”。
- 选择模式为“带宽模式”。
- 配置带宽门限值为 12Mbps，带宽差值门限值为 3Mbps。
- 进入负载均衡组配置页面，创建负载均衡组 1
- 将 AP 1 的 Radio 2 和 AP 2 的 Radio 2 绑定到负载均衡组中。

4. 验证配置

AP 1 的 Radio 2 和 AP 2 的 Radio 2 在同一个负载均衡组中，AP 3 的 Radio 2 没有加入负载均衡组。由于负载均衡只对组内的 Radio 生效，所以 AP 3 的 Radio 2 不参与负载均衡。

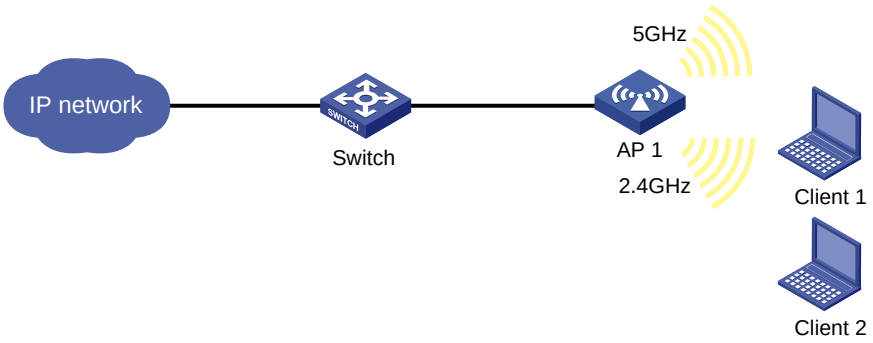
当参与运行负载均衡的某个 Radio 上的带宽达到或超过 12Mbps，并且与另一个 Radio 上的带宽差值达到或超过 3Mbps，开始运行负载均衡。通过单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 Radio 2 和 AP 2 的 Radio 2 上关联的客户端数量达到均衡。

2.1.24 频谱导航配置举例

1. 组网需求

如 图 2-24 所示，AP通过交换机与AC相连，并开启 5GHz射频和 2.4GHz射频。由于网络中有些客户端仅支持 2.4GHz频段，有些客户端支持双频，就有可能导致 2.4GHz射频过载，5GHz射频相对空余。为了防止上述情况的出现，平衡两个频段的射频负载，开启频谱导航功能和频谱导航负载均衡功能。

图2-24 频谱导航配置组网图



2. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 band-navigation。
- 开启无线服务。
- 关闭快速关联。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > AP 管理”，进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 AP 1 的 5GHz 射频和 2.4GHz 射频。

(3) 配置频谱导航

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 无线配置 > 射频管理”，进入“频谱导航”页面，配置步骤为：

- 在“全局配置”页面，配置全局频谱导航状态为开启，频谱导航负载均衡的连接数门限为 5，连接数差值门限为 2。
- 在“AP 配置”页面，配置 AP 频谱导航状态为开启。

3. 验证配置

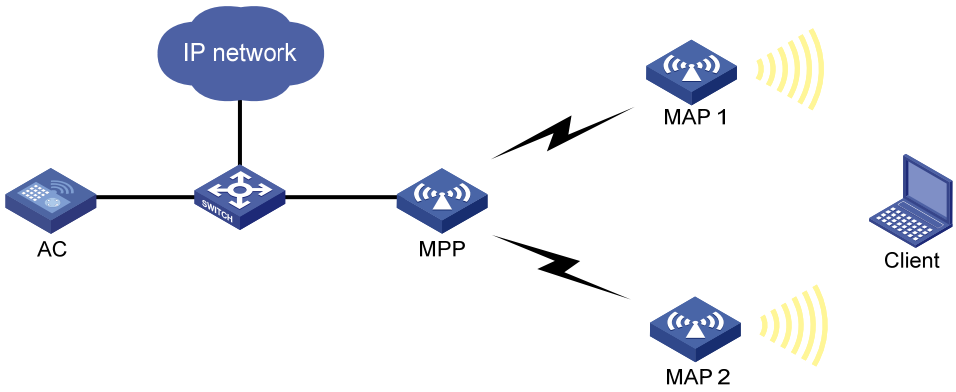
单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 监控 > 客户端”，进入“客户端”页面，可以查看到 AP 1 的 5GHz 射频和 2.4GHz 射频上关联的客户端数量处于均衡状态。

2.1.25 Mesh服务配置举例

1. 组网需求

组建一个 Mesh 网络，MPP 通过交换机与 AC 连接，在 MPP 和 MAP 1、MPP 和 MAP 2 之间使用射频工作模式为 802.11n（5GHz），工作信道号为 149 来建立 Mesh 链路，客户端能够通过 MAP 接入网络并访问网络资源。

图2-25 集中式 Mesh 网络配置组网图



2. 配置步骤

(1) 配置无线服务

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 创建一个无线服务，名称为 service。
- 配置 SSID 为 mesh-network。
- 开启无线服务。

(2) 配置 AP

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP 管理”页面，配置步骤为：

- 配置 AP，名称为 MPP。
- 配置 AP，名称为 MAP1。
- 配置 AP，名称为 MAP2。

分别进入 MPP、MAP 1、MAP 2 的配置页面，在“无线服务配置”页面中将无线服务 service 绑定到 MPP、MAP 1、MAP 2 的射频 1。

(3) 配置 Mesh Profile

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 应用 > Mesh 服务”，进入“Mesh 服务”页面，配置步骤为：

- 在 Mesh Profile 的框里单击右上角的“+”：创建 Mesh Profile。
- 指定 Profile 索引为 1。
- 指定 Profile 状态为开启。
- 指定 Mesh ID 为 1。
- 指定身份认证和密钥管理模式为 SAE。
- 指定密钥为 12345678。
- 其它配置项为缺省配置。

(4) 配置将 Mesh Profile 绑定到射频

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 应用 > Mesh 服务 > 绑定信息”，进入“绑定信息”页面，对 MPP、MAP 1、MAP 2 进行绑定操作，绑定的 Profile 索引为 1。

(5) 配置 MPP 停止发送邻居探测请求

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 应用 > Mesh 服务 > 邻居探测请求发送功能”，进入“邻居探测请求发送功能”页面，开启 MPP 的邻居探测请求发送功能。

(6) 配置邻居白名单

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 应用 > Mesh 服务 > 邻居白名单统计”，进入“邻居白名单统计”页面，配置步骤为：

- 配置 MAP 1 的邻居白名单表项为 MPP 的 MAC 地址，使 MAP1 仅与 MPP 建立 Mesh 连接，以避免环路的产生。
- 配置 MAP 2 的邻居白名单表项为 MPP 的 MAC 地址，使 MAP2 仅与 MPP 建立 Mesh 连接，以避免环路的产生。

(7) 配置工作信道

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 射频管理 > 射频配置 > AP 组内所有 AP 的射频”，进入“AP 组内所有 AP 的射频”页面，配置 MPP、MAP 1、MAP 2 的射频 1 的工作信道为 149。

(8) 配置射频模式

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 射频管理 > 射频配置 > AP 组内所有 AP 的射频”，进入“AP 组内所有 AP 的射频”页面，配置 MPP、MAP 1、MAP 2 的射频 1 的射频模式为 802.11n（5GHz）。

(9) 开启射频

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 射频管理 > 射频配置 > AP 组内所有 AP 的射频”，进入“AP 组内所有 AP 的射频”页面，开启 MPP、MAP 1、MAP 2 的射频 1。

3. 验证配置

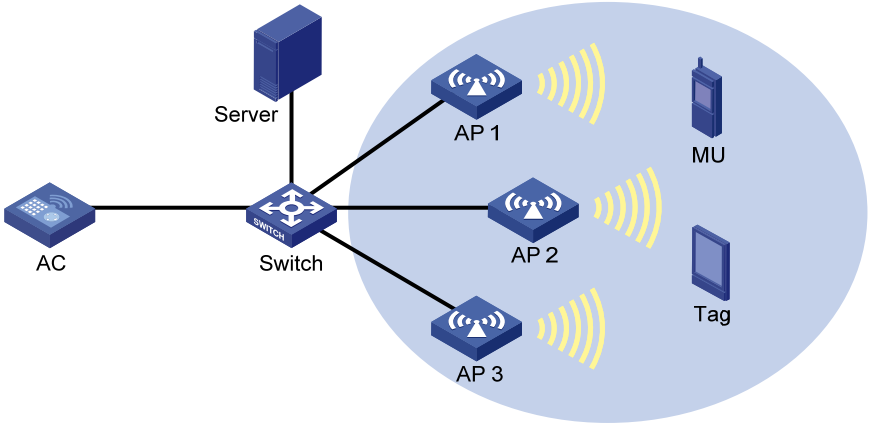
Mesh 网络建立完成后，当客户端接入网络并访问网络资源时，可通过 Mesh 链路统计信息页面查看到 Mesh 链路上的报文统计信息。

2.1.26 无线定位服务典型配置举例

1. 组网需求

在如下图所示的无线环境中，通过 AP 1、AP 2 和 AP 3 搜集 Tag 和 Mobile 设备的定位信息，然后提供给定位服务器进行定位。

图2-26 无线定位配置组网组



2. 配置步骤

(1) 配置定位服务器

- 在定位服务器上手工配置 AP 1～AP 3 的 IP 地址，或者选择广播方式发现 AP。
- 在定位服务器上完成和定位相关的配置。

(2) 配置 AP

在 AC 上，对 AP 1～AP 3 进行配置。这里以 AP 1 为例。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 无线网络”，进入“无线网络”页面配置无线服务，配置步骤为：

- 创建一个无线服务，名称为 market。
- 开启无线服务。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > AP 管理”，进入“AP”页面配置 AP，配置步骤为：

- 配置 AP 名称为 AP1。
- 配置 AP 型号及序列号。
- 进入 AP 1 的配置页面，在“无线服务配置”页面中将无线服务 market 绑定到 AP 1 的 Radio1 射频。

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“无线配置 > 应用”，进入“无线定位”页面配置无线定位，配置步骤为：

- 单击“全局配置”的“更多”按钮，在“Aeroscout 定位配置”页面下开启 Aeroscout 定位。
- 单击“AP 配置”的“更多”按钮，对 AP1 进行编辑，在“通用配置”页面下开启忽略 Beacon 帧功能。在 Aeroscout 定位配置下，开启 Aeroscout 定位功能，配置 Radio1 为开启并且客户端类型选择 Mobile 设备和 TAG 设备。

3. 验证配置

在图形软件上用户可以通过地图、表格或者报告等形式获取到无线网络中 MU 和 Tag 设备的位置。

2.2 网络安全功能配置举例

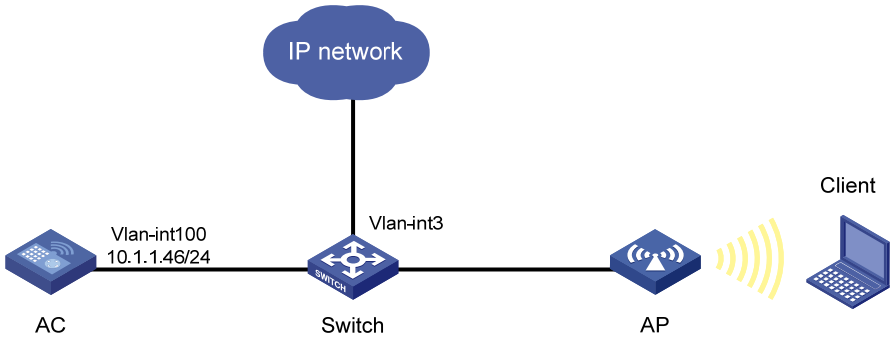
2.2.1 BYOD配置举例

1. 组网需求

用户通过 AC 接入网络，AC 对用户进行 802.1X 认证以控制其访问权限，具体要求如下：

- 802.1X 用户的认证名为 dotuser，认证密码为 12345。
- AC 使用开放式系统对 802.1X 用户进行本地认证、授权，认证域为 abc
- 终端类型为 Microsoft Windows 8 的 802.1X 用户通过认证后将被授权访问 VLAN 3。

图2-27 支持本地 BYOD 授权的 802.1X 用户认证、授权配置组网图



2. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置无线服务

单击页面底部的<网络>按钮，然后单击左侧导航栏“无线配置 > 无线网络”，进入“无线网络”页面，配置步骤为：

- 单击<添加>按钮，创建一个无线服务，无线服务名称为 service1。
- 配置 SSID 为 service。
- 无线服务状态选择“开启”。
- 单击<确定>按钮。

(3) 配置认证模式为 802.1X 认证

完成上述配置后，会返回“全部网络 > 无线配置 > 无线网络 > 无线网络”页面，单击无线名称为“service1”表项后面的<编辑>按钮，再单击页面上方的“链路层认证”，进入认证配置页面，配置步骤为：

- 选择认证模式为 802.1X 认证。
- 选择安全模式为 WPA。
- 选择加密套件为 CCMP。
- 配置域名为 abc。
- 单击<确定>按钮。

(4) 将无线服务绑定到 AP

进入“全部网络 > 无线配置 > 无线网络 > 无线网络”页面，配置步骤为：

- 选中创建的无线服务 service1，单击“绑定到 AP”按钮，进入到“绑定到 AP”页面。
- 选中 AP 的 5GHz 射频单元，单击“快速绑定”。

(5) 配置 ISP 域

单击左侧导航栏“网络安全 > 认证”，进入“ISP 域”配置页面，配置步骤为：

- 单击<添加>按钮，添加 ISP 域，域名为 abc，并将该 ISP 域的状态设置为活动。
- 指定接入方式为 LAN 接入。
- 指定 LAN 接入 AAA 方案的认证方法为本地认证，授权方法为本地授权，计费方法为不计费。
- 单击<确定>按钮。

(6) 配置本地用户

单击左侧导航栏“网络安全 > 用户管理”，进入“本地认证”配置页面，配置步骤为：

- 单击页面右上方<用户组>按钮，然后单击<添加>按钮，添加用户组，用户组名为 windows8。
- 单击<确定>按钮，返回本地用户页面。
- 单击页面右上方<用户>按钮，然后单击<添加>按钮，添加用户，用户名为 dotuser，密码为 12345。
- 指定可用服务为 LAN 接入。
- 指定授权用户组为 windows8。
- 单击<确定>按钮。

(7) 配置 BYOD 授权

单击左侧导航栏“网络安全 > BYOD”，然后单击页面上方“BYOD 授权”，进入 BYOD 授权配置页面，单击用户组 windows8 表项后面的<编辑>按钮，为用户组 windows8 配置授权属性：设备类型为 Microsoft Windows 8、ACL 编号为 2000，授权 VLAN 为 VLAN 3。

然后单击表项右侧的<添加>按钮，最后单击<确定>。

(8) 配置 BYOD 规则

完成上述配置后会返回到 BYOD 授权页面，单击“BYOD 规则”，新建一条自定义 BYOD 规则：DHCP Option 55 为 1,15,3,6,44,46,47,31,33,121,249,252,43.33，终端类型为 Microsoft Windows 8。

3. 验证配置

以上配置完成后，使用 Microsoft Windows 8 终端的 802.1X 用户通过认证后，可访问 VLAN 3 中的网络资源。

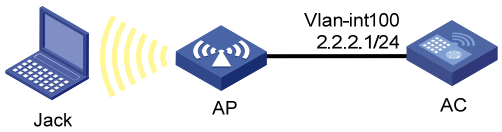
2.2.2 来宾用户管理配置举例

1. 组网需求

在 AC 上配置来宾管理功能，并为来宾 Jack 创建来宾用户 user1。具体要求如下：

- 为来宾 Jack 创建一个本地来宾用户 user1，并设置密码、所属用户组、个人相关信息、有效期、以及接待人信息。
- 配置设备为来宾用户业务发送电子邮件使用的 SMTP 服务器地址、发件人地址、来宾管理员的电子邮件地址。
- 配置设备发送给来宾用户、来宾接待人、来宾管理员的邮件标题和内容。
- 来宾用户账户过期后系统自动将其删除。

图2-28 来宾用户管理配置组网图



2. 配置步骤

(1) 配置各接口的 IP 地址（略）

(2) 配置无线服务（略）

(3) 添加来宾用户

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 网络安全 > 来宾管理”，进入“来宾用户”页面，配置步骤为：

- 添加用户，账号为 user1，密码为 123456。
- 指定来宾用户所属的用户组。（请根据实际需求选择）
- 配置来宾用户的姓名、公司名称、电子邮箱、联系电话、描述信息。（请根据实际情况配置）
- 配置来宾接待人的姓名、所属部门、电子邮箱。（请根据实际情况配置）
- 配置来宾用户的有效期。（请根据实际情况配置）

(4) 配置来宾业务参数

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 网络安全 > 来宾管理”，进入“来宾业务参数”页面，配置步骤为：

- 开启自动删除失效来宾用户功能。
- 配置发送电子邮件使用的 SMTP 服务器地址为 smtp://192.168.0.112/smtp。
- 配置发件人电子邮箱为 bbb@ccc.com。
- 配置来宾管理员电子邮箱为 guest-manager@ccc.com。

- 配置发送给来宾用户的通知邮件标题为 Guest account information，邮件内容为 A guest account has been created for your use. The username, password, and valid dates for the account are given below.。
- 配置发送给来宾管理员的通知邮件标题为 Guest register information，邮件内容为 A guest account has been registered. The username for the account is given below. Please approve the register information.。
- 配置发送给来宾接待人的通知邮件标题为 Guest account information，邮件内容为 A guest account has been created. The username, password, and valid dates for the account are given below.。

3. 验证配置

Jack 使用用户名 user1 和密码 123456 在账户有效期内进行本地认证，可以认证通过并接入网络。

2.3 工具功能配置举例

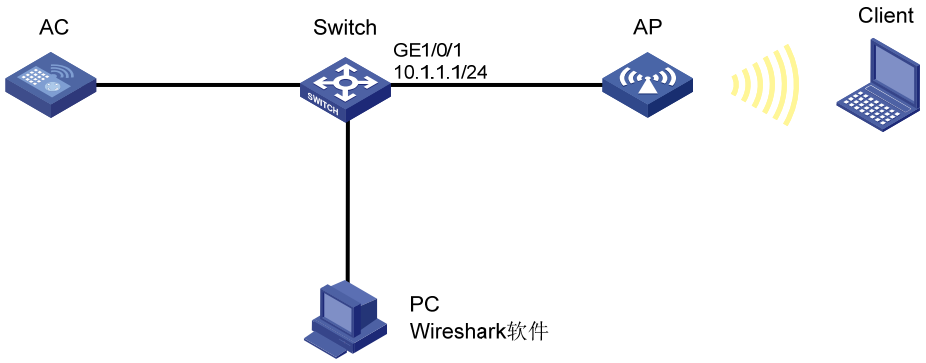
2.3.1 本地报文捕获配置举例

1. 组网需求

- 在 AP 的 Radio 1 上开启本地报文捕获功能，要求捕获 1KB 的协议类型为 TCP，且报文的源 IP 地址为 192.168.20.173 的报文。
- Switch 做为 FTP 服务器，保存 AP 发送的被捕获报文。

2. 组网图

图2-29 本地报文捕获组网图



3. 配置步骤

(1) 配置 Switch

在 Switch 上添加一个 FTP 用户 abc，并设置其认证密码为 123456，访问时使用的用户角色为 network-admin，授权访问目录为 Flash 的根目录，可以使用的服务类型为 FTP。

启动 Switch 的 FTP 服务功能。

(2) 在 AC 上配置本地报文捕获功能

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 工具 > 无线报文捕获”，进入“无线报文捕获”页面，配置步骤为：

- 选择 AP 的 Radio 1，开启本地报文捕获功能。
- 指定过滤规则为"src 192.168.20.173 and tcp"，捕获报文最大长度为 8000，存储捕获报文的文件大小为 1KB，FTP 服务器的 URL 地址为 ftp://10.1.1.1，登录 FTP 服务器的用户名为 abc，用户密码为 123456。

4. 验证配置

报文捕获成功后，在 PC 上使用 wireshark 软件与 FTP 服务器建立连接，可以解析报文文件。

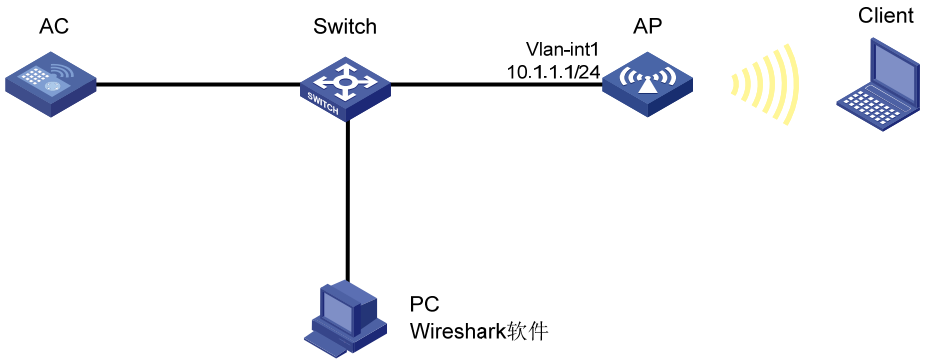
2.3.2 远程报文捕获配置举例

1. 组网需求

在 AP 的 Radio 1 上开启远程报文捕获功能，将捕获的报文上送到 Wireshark 软件上解析。

2. 组网图

图2-30 远程报文捕获组网图



3. 配置步骤

(1) 配置远程报文捕获功能

单击页面底部的<网络>按钮，进入“网络”菜单页面，然后单击页面左侧导航栏的“ 工具 > 无线报文捕获”，进入“无线报文捕获”页面，配置步骤为：

- 选择 AP 的 Radio 1，开启远程报文捕获功能。
- 指定 RPCAP 服务端口号为 2014。

(2) 配置 PC

- 在 PC 上打开 Wireshark 软件，菜单栏选择 Capture，在弹出的下拉菜单中选择 Options，弹出 Capture Options 对话框后，选择 remote 捕获方式，输入捕获地址 10.1.1.1 和端口号 2014，单击“OK”按钮，再单击“Start”按钮，此时在弹出的报文捕获窗口会看到捕获的报文。

图2-31 Wireshark 软件报文捕获窗口