大型 WLAN 组网介绍与部署

- 目前，大多数企业办公环境同时使用有线和无线网络来支撑业务。办公区在提供有线网口的同时，也采用全 Wi-Fi 覆盖，办公环境更为开放和智能。未来，企业云桌面办公、智真会议、4K 视频等大带宽业务将从有线网络迁移至无线网络，而 VR/AR、虚拟助手、自动化工厂等新技术将直接基于无线网络部署。新的应用场景对企业 WLAN 的设计与规划提出更高的要求。
- 本课程介绍大型 WLAN 组网的典型应用、关键技术原理以及大型 WLAN 组网的配置。

- 云桌面又称桌面虚拟化、云电脑，是替代传统电脑的一种新模式；采用云桌面后，用户无需再购买电脑主机，用户安装客户端后通过特有的通信协议访问后端服务器上的虚拟机主机来实现交互式操作，达到与电脑一致的体验效果；同时，云桌面不仅支持用于替换传统电脑，还支持手机、平板等其他智能设备在互联网上访问，也是移动办公的最新解决方案。
- 智真会议是通过高分辨率摄像头和语音设备，提供真人大小面对面、眼对眼的视频会议。
- VR：Virtual Reality，虚拟现实，指用计算机模拟三维环境，用户常常借助手套和眼镜就能直接交互操作。
- AR：Augmented Reality，增强现实，在虚拟现实的基础上发展起来的新技术，也被称为混合现实。是通过计算机系统提供的信息增加用户对现实世界感知的技术，将虚拟的信息应用到真实世界，并将计算机生成的虚拟物体、场景或系统提示信息叠加到真实场景中，从而实现对现实的增强。AR 通常是以透过式头盔显示系统和注册（AR 系统中用户观察点和计算机生成的虚拟物体的定位）系统相结合的形式来实现的。

大型WLAN组网的应用

- 高新科技园区会使用大量的新兴技术，比如 IoT、5G 融合、自动驾驶等等技术。

大型WLAN组网特点

华为大型WLAN方案功能

设备统一管理

全网设备统一纳管，配置自动备份，告警实时上报，网管不再有烦恼。

漫游&业务随行

无缝漫游，用户在园区网络内移动时，只要身份不变，则其网络访问权限及体验将随之而动

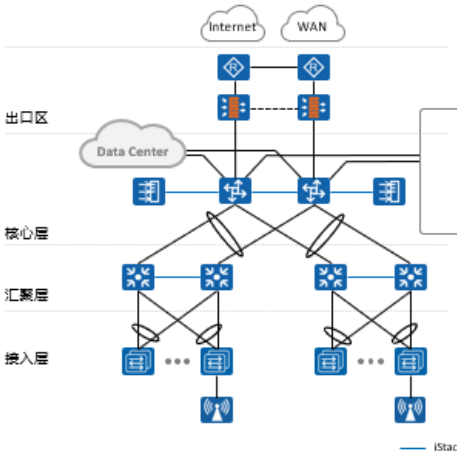
接入&终端安全保障

准入控制技术以及终端安全防护确保安全无死角。

高可靠性技术

双机冷备、双机热备、N+1备份等多种高可靠性技术保障WLAN网络稳定运行。

WLAN网络解决方案



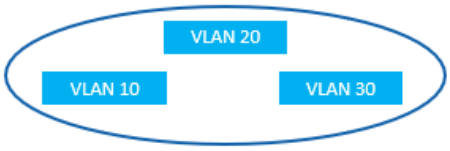
WLAN配合SDN控制器使用，由SDN控制器统一管理和配置，能够实现业务发放自动化、网络全生命周期管理，结合大数据和AI技术可实现园区网络的智能、极简和安全。园区网络更具备有线与无线的深度融合能力。

大型WLAN网络关键技术

技术	作用
VLAN Pool	通过VLAN Pool把接入的用户分配到不同的VLAN，可以减少广播域，减少网络中的广播报文，提升网络性能。
DHCP Option 43 & 52	当AC和AP间是三层组网时，AP通过发送广播请求报文的方式无法发现AC，这时需要通过DHCP服务器回应给AP的报文中携带的Option43字段（IPv4）或Option52（IPv6）来通告AC的IP地址。
漫游技术	WLAN漫游是指STA在不同AP覆盖范围之间移动且保持用户业务不中断的行为。
高可靠性技术	为了保证WLAN业务的稳定运行，保证在主设备故障时业务能够顺利切换到备份设备的技术。
准入控制	准入控制技术是通过对接入网络的客户端和用户的认证来保证网络的安全，是一种“端到端”的安全技术。

VLAN Pool 概念

- 现有网络面临的挑战
  - 无线网络终端的移动性导致特定区域IP地址请求较多。
  - 通过情况下，一个SSID只能对应一个业务VLAN，如果通过扩大子网增加IP地址则会导致广播域扩大，大量的广播报文造成网络拥塞。
- VLAN Pool是一种把多个VLAN放在一个池中并提供分配算法的VLAN分配技术，又称为VLAN池。



VLAN Pool

- 通过 VLAN Pool 把接入的用户分配到不同的 VLAN，可以减少广播域，减少网络中的广播报文，提升网络性能。
- 由于无线终端的移动性，在无线网络中经常有大量用户从某个区域接入后，随着用的移动，再漫游到其他区域，导致该区域的用户接入多，对 IP 地址数目要求大。比如：场馆入口、酒店的大堂等。目前一个 SSID 只能对应一个 VLAN，一个 VLAN 对应一个子网，如果大量用户从某一区域接入，只能扩大 VLAN 的子网，保证用户能够获取到 IP 地址。这样带来的问题就是广播域扩大，导致大量的广播报文（如：ARP、

DHCP 等）带来严重的网络拥塞。

- 基于此问题考虑，一个 SSID 需要能够对应多个 VLAN，把大量用户分散到不同的 VLAN 减少广播域。VLAN Pool 提供多个 VLAN 的管理和分配算法，实现 SSID 对应多个 VLAN 的方案。

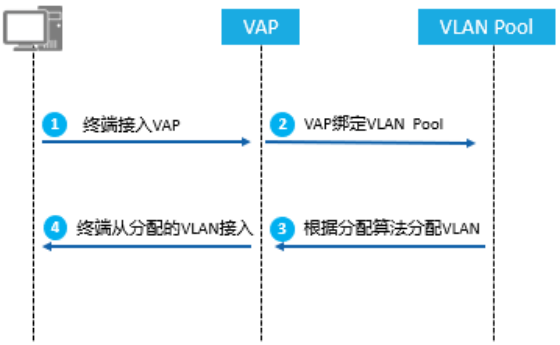
VLAN Pool分配VLAN的算法

- 顺序分配算法：把用户按上线顺序依次划分到不同的VLAN中。
- HASH分配算法：根据用户MAC地址HASH值分配VLAN。
- 两种分配方式的比较：

分配算法	优点	缺点
顺序分配	各个VLAN用户数目划分均匀	重新上线VLAN容易变更、IP变化
HASH分配	用户多次上线可分配相同的VLAN、IP不变	各个VLAN用户数划分不均衡

- 顺序分配算法：把用户按上线顺序依次划分到不同的 VLAN 中，用户上下线用户 VLAN 容易变化，IP 地址变更。
- HASH 分配算法：根据用户 MAC 地址 HASH 值分配 VLAN，用户分配的 VLAN 固定，可能导致 VLAN 间用户划分不均匀，有的 VLAN 用户较多，有的较少。

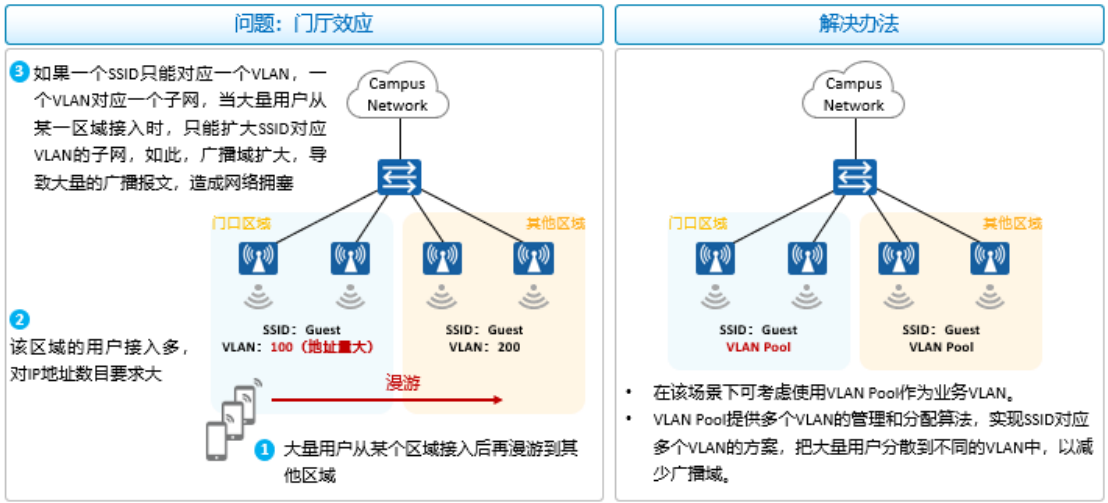
分配VLAN流程



1. 用户终端从某个VAP接入，判断VAP是否有判断VLAN Pool。
2. 如果该VAP对应的模板绑定了VLAN Pool，使用VLAN Pool的分配算法分配一个VLAN，VLAN Pool有顺序分配和hash分配两种分配算法。
3. 给终端分配一个VLAN。
4. 终端从VLAN Pool分配的VLAN上线。

- 虚拟接入点 VAP（Virtual Access Point）：VAP 就是在一个物理实体 AP 上虚拟出多个 AP，每一个被虚拟出的 AP 就是一个 VAP，每个 VAP 提供和物理实体 AP 一样的功能。用户可以在一个 AP 上创建不同的 VAP 来为不同的用户群体提供无线接入服务。

VLAN Pool应用示例



配置介绍

1. 创建VLAN Pool并进入VLAN Pool视图。

   [AC] **vlan pool** *pool-name*

2. 将指定VLAN添加到VLAN Pool中。

   [AC-vlan-pool-pool-name] **vlan { start-vlan [to end-vlan] } &<1-10>**

3. 配置VLAN Pool中的VLAN分配算法。

   [AC-vlan-pool-pool-name] **assignment { even | hash }**

4. 配置VAP的业务VLAN。

   [AC] **wlan**
   [AC-wlan-view] **vap-profile name** *profile-name*
   [AC-wlan-vap-prof-*profile-name*] **service-vlan vlan-pool** *pool-name*

- VLAN pool 中可以配置 VLAN 分配算法。assignment { even | hash }
- VLAN 分配算法为 even 时，VLAN pool 根据 STA 的上线顺序为 STA 分配业务 VLAN，VLAN pool 尽量保证所有 VLAN 分配给 STA 的 IP 地址数目相近。但同一个 STA 如果多次上线，每次获取的地址通常都不相同。
- VLAN 分配算法为 hash 时，VLAN pool 根据 STA 的 MAC 地址进行哈希运算后的结果为 STA 分配业务 VLAN，只要 VLAN pool 里面的 VLAN 不发生变化，通常 STA 都会获取到固定的业务 VLAN，STA 重新上线时也会被尽量优先分配到之前使用过的 IP 地址。

配置案例 (1)

- AC是STA的DHCP服务器，已开启DHCP功能；
- DHCP服务器地址包含两个网段，分别为10.1.2.0/24以及10.1.3.0/24；
- DHCP客户机能够动态获取服务器分配的IP地址，IP地址池地址范围为10.1.2.0以及10.1.3.0网段地址，且网关地址为10.1.2.254，10.1.3.254。

AC的VLAN Pool配置如下：

```
[AC] vlan pool STA
[AC-vlan-pool-STA] vlan 20 30
[AC-vlan-pool-STA] assignment hash
[AC-vlan-pool-STA] quit
```

```
[AC] wlan
[AC-wlan-view] vap-profile name huawei
[AC-wlan-vap-prof-huawei] service-vlan vlan-pool STA
Info: This operation may take a few seconds, please wait. Done.
```

配置案例 (2)

1. 在AC上查看所有VLAN pool下的简要配置信息：

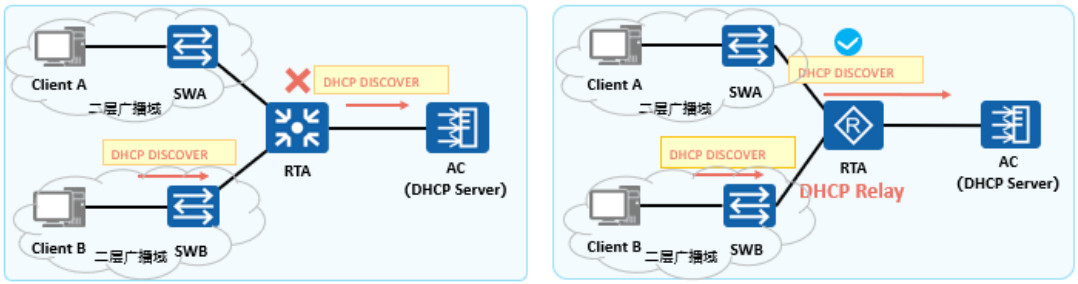
```
<AC> display vlan pool all
--------------------------------------------------------------------------------
Name                Assignment          VLAN total
--------------------------------------------------------------------------------
STA                 hash                2
--------------------------------------------------------------------------------
Total: 2
```

2. 在AC上查看STA VLAN Pool下的详细配置信息：

```
<AC> display vlan pool name STA
--------------------------------------------------------------------------------
Name                : STA
Total               : 2
Assignment  : hash
VLAN ID             : 20 30
```

DHCP中继

- DHCP客户端使用IP广播来寻找同一网段上的DHCP服务器。当服务器和客户段处在不同网段，即被路由器分割开来时，路由器是不会转发这样的广播包。
- DHCP中继能够跨网段“透传”DHCP报文，使得一个DHCP服务器同时为多个网段服务成为可能。



- 随着网络规模的不断扩大，网络设备不断增多，企业内不同的用户可能分布在不同的网段，一台 DHCP 服务器在正常情况下无法满足多个网段的地址分配需求。企业内网各个网段通常都没有与 DHCP Server 在同一个二层广播域内，如果还需要通过 DHCP 服务器分配 IP 地址，则需要跨网段发送 DHCP 协议报文。

配置介绍

1. 使能接口的DHCP中继功能

```
[Huawei-GigabitEthernet0/0/0]dhcp select relay
```

2. 在接口视图下配置DHCP服务器的IP地址

```
[Huawei-GigabitEthernet0/0/0]dhcp relay server-ip ip-address
```

3. 创建DHCP服务器组

```
[Huawei]dhcp server group group-name
```

4. 在DHCP服务器组中配置DHCP服务器成员

```
[Huawei-dhcp-server-group-HW]dhcp-server ip-address [ ip-address-index ]
```

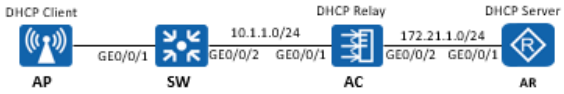
5. 配置接口应用的DHCP服务器组

```
[Huawei-GigabitEthernet0/0/0]dhcp relay server-select group-name
```

6. 开启接口下的DHCP Client功能

```
[Huawei-GigabitEthernet0/0/0]ip address dhcp-alloc
```

配置案例 (1)



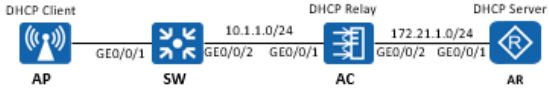
- WLAN的管理VLAN是VLAN 10，AP通过DHCP获取IP地址。
- 在SW、AC和AR上配置基础互通参数。
- 将AP、AC和AR分别配置为DHCP的客户端、DHCP中继以及DHCP服务器，开启DHCP功能。
- AC上开启DHCP Relay功能，并且指定DHCP Server的IP地址为172.21.1.2。
- 在AR上创建地址池“AP”，地址范围为10.1.1.0/24，网关为10.1.1.2。

SW和AC的配置如下：

```
[SW] vlan 10
[SW-vlan10] quit
[SW] interface GigabitEthernet 0/0/1
[SW-GigabitEthernet0/0/1] port link-type access
[SW-GigabitEthernet0/0/1] port default vlan 10
[SW-GigabitEthernet0/0/1] quit
[SW] interface GigabitEthernet 0/0/2
[SW-GigabitEthernet0/0/2] port link-type trunk
[SW-GigabitEthernet0/0/2] port trunk allow-pass vlan 10
[SW-GigabitEthernet0/0/2] quit
[SW] interface Vlanif 10
[SW-Vlanif10] ip address 10.1.1.1 24
```

```
[AC] vlan batch 10 20
[AC] interface GigabitEthernet 0/0/1
[AC-GigabitEthernet0/0/1] port link-type trunk
[AC-GigabitEthernet0/0/1] port trunk allow-pass vlan 10
[AC-GigabitEthernet0/0/1] quit
[AC] interface GigabitEthernet 0/0/2
[AC-GigabitEthernet0/0/1] port link-type access
[AC-GigabitEthernet0/0/1] port default vlan 20
```

配置案例 (2)



- WLAN的管理VLAN是VLAN 10，AP通过DHCP获取IP地址。
- 在SW、AC和AR上配置基础互通参数。
- 将AP、AC和AR分别配置为DHCP的客户端、DHCP中继以及DHCP服务器，已开启DHCP功能。
- AC上开启DHCP Relay功能，并且指定DHCP Server的IP地址为172.21.1.2。
- 在AR上创建地址池“AP”，地址范围为10.1.1.0/24，网关为10.1.1.2。

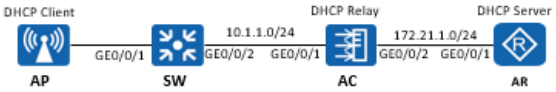
AC和AR的配置如下：

```
[AC] interface Vlanif 10
[AC-Vlanif10] ip address 10.1.1.2 24
[AC-Vlanif10] quit
[AC] interface Vlanif 20
[AC-Vlanif20] ip address 172.21.1.1 24
[AC-Vlanif20] quit
```

```
[AR] interface GigabitEthernet 0/0/1
[AR-GigabitEthernet0/0/1] ip address 172.21.1.2 24
[AR-GigabitEthernet0/0/1] quit
```

```
[AC] dhcp server group AP
[AC-dhcp-server-group-AP] dhcp-server 172.21.1.2
[AC-dhcp-server-group-AP] quit
[AC] interface Vlanif 10
[AC-Vlanif10] dhcp select relay
[AC-Vlanif10] dhcp relay server-select AP
[AC-Vlanif10] quit
```

配置案例 (3)



- WLAN的管理VLAN是VLAN 10，AP通过DHCP获取IP地址。
- 在SW、AC和AR上配置基础互通参数。
- 将AP、AC和AR分别配置为DHCP的客户端、DHCP中继以及DHCP服务器，已开启DHCP功能。
- AC上开启DHCP Relay功能，并且指定DHCP Server的IP地址为172.21.1.2。
- 在AR上创建地址池“AP”，地址范围为10.1.1.0/24，网关为10.1.1.2，并添加静态路由，确保AR能够访问到10.1.1.0网段。

AR的配置如下：

```
[AR] ip pool AP
[AR-ip-pool-AP] network 10.1.1.0 mask 24
[AR-ip-pool-AP] gateway-list 10.1.1.2
[AR-ip-pool-AP] excluded-ip-address 10.1.1.1
[AR-ip-pool-AP] quit
[AR] interface GigabitEthernet 0/0/1
[AR-GigabitEthernet0/0/1] dhcp select global
[AR-GigabitEthernet0/0/1] quit
[AR] ip route-static 10.1.1.0 255.255.255.0 172.21.1.1
```

配置案例 (4)

在AR上查看DHCP地址池分配情况：

```
[AR] display ip pool name AP used
.....
Network section :
-------------------------------------------------------------------------------
 Index    IP            MAC               Lease   Status
-------------------------------------------------------------------------------
 253      10.1.1.254    00e0-fcca-1150    2181    Used
-------------------------------------------------------------------------------
[AR]
```

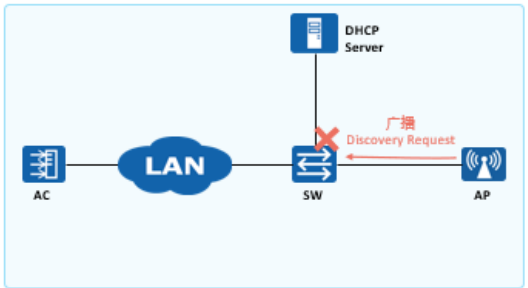
从上图可以看到DHCP服务器已分配IP地址给AP。

在AC上查看DHCP Relay信息：

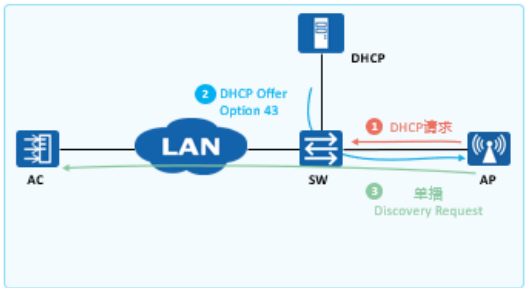
```
<AC> display dhcp relay all
 DHCP relay agent running information of interface Vlanif10 :
 Server group name      : AP
 Gateway address in use : 10.1.1.2
```

WLAN三层组网AC发现机制

当AC和AP间是三层组网时，AP通过发送广播请求报文的方式无法发现AC，这时需要通过DHCP服务器回应给AP的报文中携带的Option43字段（IPv4）或Option52（IPv6）来通告AC的IP地址。



WLAN三层组网场景，AP的广播Discovery Request报文无法发现AC，导致CAPWAP隧道无法建立。

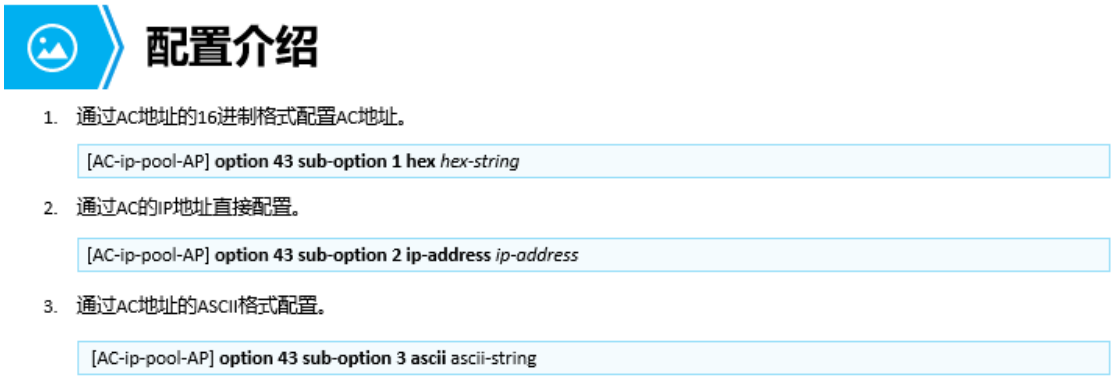


WLAN三层组网场景，配置DHCP Option 43后，在AP获取IP地址阶段，同时获取了AC的IP地址，直接通过单播与AC建立联系。

- 在 AC 和 AP 间是二层组网的情况下，也可以配置 Option 43，AP 会根据 Option43 的内容先向指定 IP 地址的 AC 发送

单播请求报文，如果发送十次报文，AP 都没有收到回应，则 AP 会继续以广播的方式来发现同一网段的 AC。所以在二层组网的情况下 Option 43 不是必配的参数，但在三层组网的情况下则是必配的。

- Option 43 即为 Type 值为 43（0x2B）的 Option 字段，又称为厂商特定信息选项，DHCP 服务器和 DHCP 客户端通过 Option43 交换厂商特定的信息。当 DHCP 服务器接收到请求 Option43 信息的 DHCP 请求报文后，将在回复报文中携带 Option43，为 DHCP 客户端分配厂商指定的信息（本文中特指 AC 的 IP 地址）。

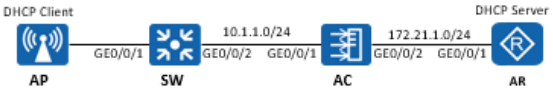


- 以 AC 或交换机配置 DHCP 服务器为例。大型组网中，通常都是使用独立的 DHCP 服务器，实际上 AC 或交换机也可以作为 DHCP 服务器。然后选择下面的一条命令配置 Option43 就可以了。
- option 43 sub-option 1 hex C0A80001C0A80002 配置设备为 AP 指定 AC 的 IP 地址为 192.168.0.1 和 192.168.0.2。其中，“C0A80001”表示 IP 地址 192.168.0.1 的十六进制格式，“C0A80002”表示 IP 地址 192.168.0.2 的十六进制格式。
- option 43 sub-option 2 ip-address 192.168.0.1 192.168.0.2 配置设备为 AP 指定 AC 的 IP 地址为 192.168.0.1 和 192.1

68.0.2。

- option 43 sub-option 3 ascii 192.168.0.1,192.168.0.2 配置设备为 AP 指定 AC 的 IP 地址为 192.168.0.1 和 192.168.0.2，选项使用 ASCII 字符串类型时，如果要配置多个 IP 地址，IP 地址之间要使用“,”隔开。

配置案例 (1)



- WLAN的管理VLAN是VLAN 10，AP通过DHCP获取IP地址。
- SW、AC以及AR的基础配置及DHCP Relay配置均已完成，AP能够正常获取到IP地址10.1.1.254，AC的IP地址为100.100.100.100。
- 在AR上创建地址池“AP”，地址范围为10.1.1.0/24，网关为10.1.1.2，并添加静态路由，确保AR能够访问到10.1.1.0网段。

AR和AC配置如下：

```
[AR] ip pool AP
[AR-ip-pool-ap] option 43 sub-option 3 ascii 100.100.100.100
[AR-ip-pool-ap] quit
```

```
[AC] interface LoopBack 0
[AC-LoopBack0] ip address 100.100.100.100 32
[AC-LoopBack0] quit
[AC] capwap source interface LoopBack 0
```

配置案例 (2)

在AR上查看DHCP地址池的配置情况：

```
[AR] display ip pool name AP
Pool-name      : AP
 Pool-No       : 0
 Lease         : 1 Days 0 Hours 0 Minutes
 Option-code   : 43
 Option-subcode : 3
 Option-type   : ascii
 Option-value  : 100.100.100.100
……
 Position      : Local      Status      : Unlocked
 Gateway-0     : 10.1.1.2
 Mask          : 255.255.255.0
……
```

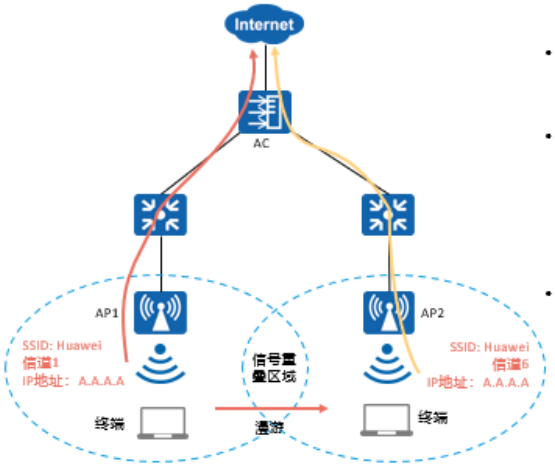
从上图可以看到option字段已经成功配置。

在AC上查看AP能否正常发现AP。

```
[AC] display ap unauthorized record
Unauthorized AP record:
Total number: 1
----------------------------------------------------------------------
AP type: AP4030TN
AP SN: 210235448310C92A877C
AP MAC address: 00e0-fcca-1150
AP IP address: 10.1.1.254
Record time: 2020-06-18 11:51:34
----------------------------------------------------------------------
[AC]
```

从上图可以看到AP已经成功发现AC，在AC上可以随时将AP添加到AC上。

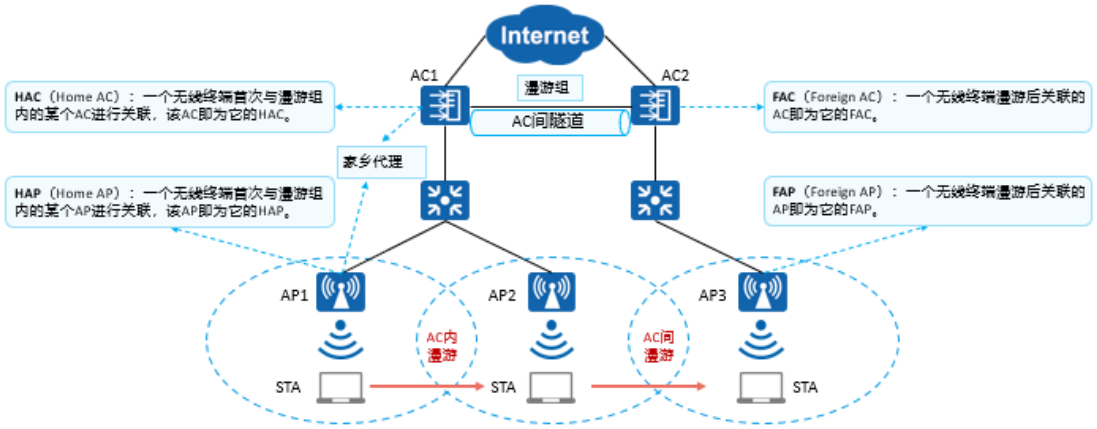
WLAN漫游概述



- WLAN漫游是指STA在不同AP覆盖范围之间移动且保持用户业务不中断的行为。
- 实现WLAN漫游的两个AP必须使用相同的SSID和安全模板（安全模板名称可以不同，但是安全模板下的配置必须相同），认证模板的认证方式和认证参数也要配置相同。
- WLAN漫游策略主要解决以下问题：
  - 避免漫游过程中的认证时间过长导致丢包甚至业务中断。
  - 保证用户授权信息不变。
  - 保证用户IP地址不变。

- 终端在移动过程中，终端在移动过程中， 如果逐渐远离接入 AP，则链路的信号质量也会逐步下降。当终端感知到信号质量降低一定程度（漫游门限）时，终端会主动漫游到附近 AP 来提高信号质量。
- 如图所示，漫游一般包括如下动作：
- 终端已经与 AP1 建链，终端在各种信道中发送 Probe Request。AP2 在信道 6（AP2 使用的信道）中收到请求后，通过在信道 6 中发送应答来进行响应。终端收到应答后，对其进行评估，确定同哪个 AP 关联最合适。此时通过评估，终端与 AP2 关联最合适。
- 终端通过信道 6 向 AP2 发送关联请求，AP2 使用关联响应做出应答，建立用户与 AP2 间的关联，至此，用户与 AP1 的关联一直保持。
- 删除用户与 AP1 现有的关联。终端通过信道 1（AP1 使用的信道）向 AP1 发送 802.11 解除关联信息，解除用户与 AP1 间的关联。

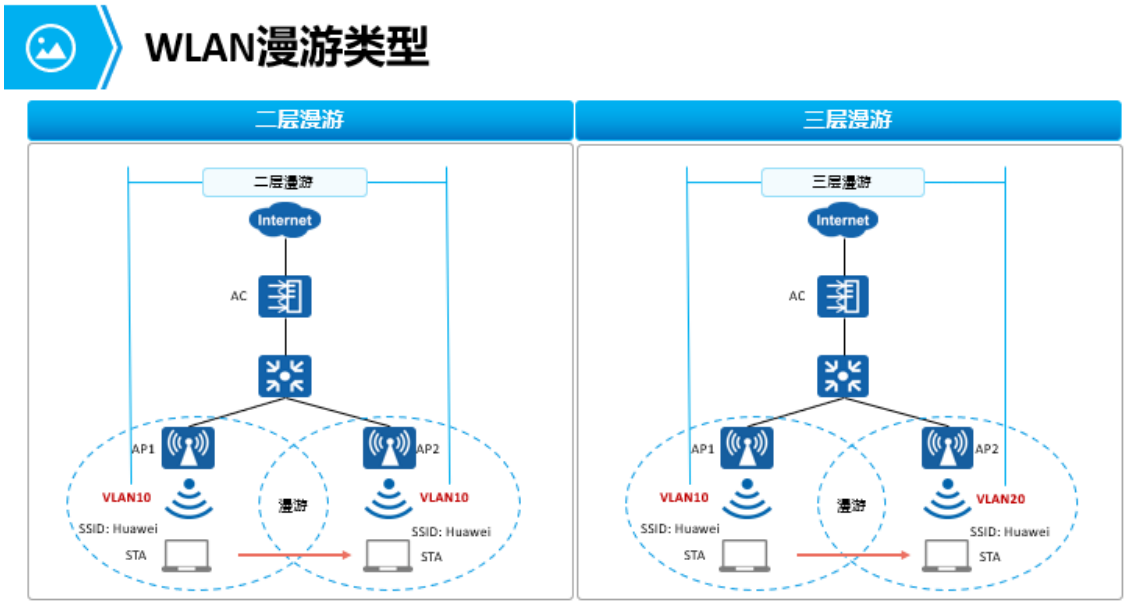
WLAN漫游的相关术语



- AC 内漫游：如果漫游过程中关联的是同一个 AC，这次漫游就是 AC 内漫游。
- AC 间漫游：如果漫游过程中关联的不是同一个 AC，这次漫游就是 AC 间漫游。
- AC 间隧道：为了支持 AC 间漫游，漫游组内的所有 AC 需要同步每个 AC 管理的 STA 和 AP 设备的信息，因此在 AC 间建立一条隧道作为数据同步和报文转发的通道。AC 间隧道也是利用 CAPWAP 协议创建的。如图所示，AC1 和 AC2 间建立 AC 间隧道进行数据同步和报文转发。
- 漫游组服务器
- STA 在 AC 间进行漫游，通过选定一个 AC 作为漫游组服务器，在该 AC 上维护漫游组的成员表，并下发到漫游组内的各 AC，使漫游组内的各 AC 间相互识别并建立 AC 间隧道。
- 漫游组服务器既可以是漫游组外的 AC，也可以是漫游组内选择的一个 AC。
- 一个 AC 可以同时作为多个漫游组的漫游组服务器，但是自身只能加入一个漫游组。
- 漫游组服务器管理其他 AC 的同时不能被其他的漫游组服务器管理。也就是说如果一个 AC 是作为漫游组服务器角色负责向其他 AC 同步漫游配置的，则它无法再作为被管理者接

受其他 AC 向其同步漫游配置（即配置了漫游组就不能再配置漫游组服务器）。

- 漫游组服务器作为一个集中配置点，不需要有特别强的数据转发能力，只需要能够和各个 AC 互通即可。
- 家乡代理
- 能够和 STA 家乡网络的网关二层互通的一台设备。为了支持 STA 漫游后仍能正常访问家乡网络，需要将 STA 的业务报文通过隧道转发到家乡代理，再由家乡代理中转。STA 的家乡代理由 HAC 或 HAP 兼任，如图所示，用户可以选取 AC 1 或 AP1 作为 STA 的家乡代理。



- 二层漫游：1 个无线客户端在 2 个 AP（或多个 AP）之间来回切换连接无线，前提是这些 AP 都绑定的是同 1 个 SSID 并且业务 VLAN 都在同 1 个 VLAN 内（在同一个 IP 地址段），漫游切换的过程中，无线客户端的接入属性（比如无线客户端所属的业务 VLAN、获取的 IP 地址等属性）不会有任何变化，直接平滑过渡，在漫游的过程中不会有丢包和断线重连的现象。
- 三层漫游：漫游前后 SSID 的业务 VLAN 不同，AP 所提供的业务网络为不同的三层网络，对应不同的网关。此时，为

保持漫游用户 IP 地址不变的特性，需要将用户流量迂回到初始接入网段的 AP，实现跨 VLAN 漫游。

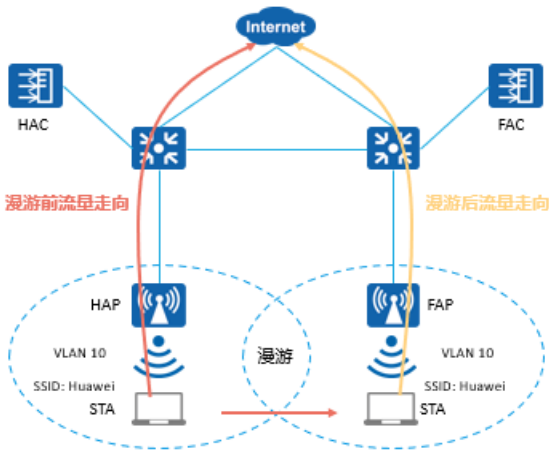
- 网络中有时候会出现以下情况：两个业务 VLAN 的 VLAN ID 相同，但是这两个子网又属于不同的子网。此时为了避免系统仅仅依据 VLAN ID 将用户在两个子网间的漫游误判为二层漫游，需要通过漫游域来确定设备是否在同一个子网内，只有当 VLAN 相同且漫游域也相同的时候才是二层漫游，否则是三层漫游。

WLAN漫游流量转发模型

根据WLAN数据转发类型以及跨三层与否，可将漫游流量转发模型划分为四种：

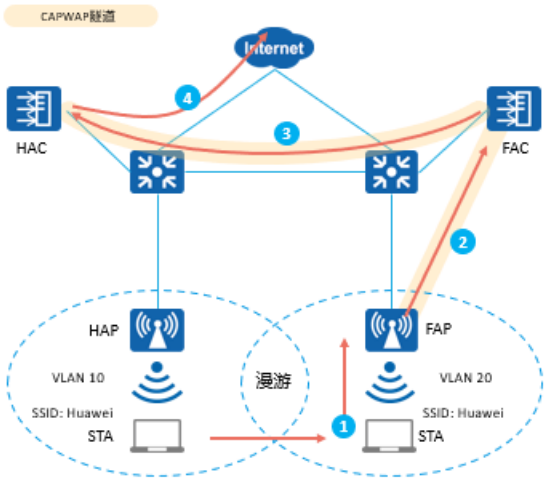
转发模型	特点
二层漫游直接转发	由于二层漫游后STA仍然在原来的子网中，所以FAP/FAC对二层漫游用户的流量转发和平台新上线的用户没有区别，直接在FAP/FAC本地的网络转发，不需要通过隧道转发回家乡代理中转。
二层漫游隧道转发	
三层漫游直接转发	HAP和HAC之间的业务报文不通过CAPWAP隧道封装，无法判定HAP和HAC是否在同一个子网内，此时设备默认报文需返回到HAP进行中转。
三层漫游隧道转发	HAP和HAC之间的业务报文通过CAPWAP隧道封装，此时可以将HAP和HAC看作在同一个子网内，所以报文无需返回HAP，可直接通过HAC中转到上层网络。

AC间二层漫游 - 直接转发



- 漫游前：
  - STA发送业务报文给HAP。
  - HAP接收到业务报文后经由网关（交换机）发送给上层网络。
- 漫游后：
  - STA发送业务报文给FAP。
  - FAP接收到业务报文后经由网关（交换机）发送给上层网络。

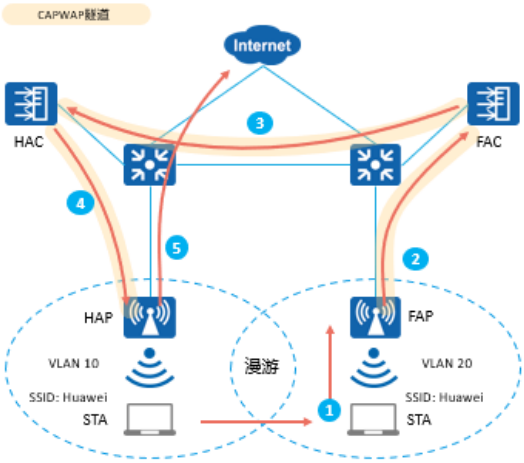
- AC 间二层漫游隧道转发与直接转发流量走向一致，不再赘述。



- 漫游前：
  1. STA发送业务报文给HAP。
  2. HAP接收到业务报文后通过CAPWAP隧道发送给HAC。
  3. HAC直接将业务报文经过交换机发送给上层网络。
- 漫游后：
  1. STA发送业务报文给FAP。
  2. FAP接收到业务报文后通过CAPWAP隧道发送给FAC 。
  3. FAC通过HAC和FAC之间的AC间隧道将业务报文转发给HAC。
  4. HAC直接将业务报文经由交换机发送给上层网络。

- 三层漫游时，用户漫游前后不在同一个子网中，为了使用户漫游后仍能正常访问漫游前的网络，需要将用户流量通过隧道中转到原来的子网。
- 隧道转发模式下，HAP 和 HAC 之间的业务报文通过 CAPWAP 隧道封装，此时可以将 HAP 和 HAC 看作在同一个子网内，报文无需返回到 HAP， 直接通过 HAC 进行中转到上层网络。

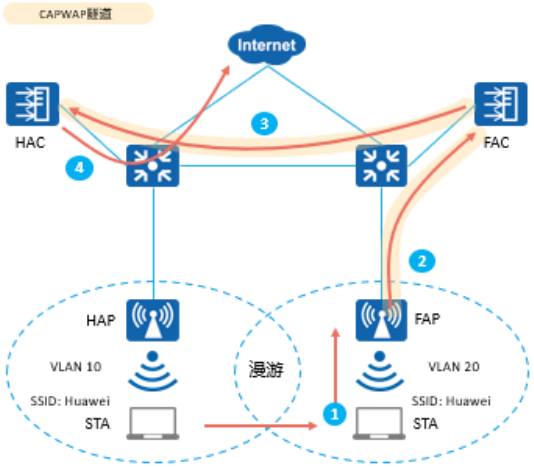
AC间三层漫游 - 直接转发（HAP为家乡代理）



- 漫游前：
  1. STA发送业务报文给HAP。
  2. HAP接收到业务报文后直接将业务报文经过交换机发送给上层网络。
- 漫游后：
  1. STA发送业务报文给FAP。
  2. FAP接收到STA发送的业务报文并通过CAPWAP隧道发送给FAC。
  3. FAC通过HAC和FAC之间的AC间隧道将业务报文转发给HAC。
  4. HAC通过CAPWAP隧道将业务报文发送给HAP。
  5. HAP直接将业务报文发送给上层网络。

- 直接转发模式下，HAP 和 HAC 之间的业务报文不通过 CAPWAP 隧道封装，无法判定 HAP 和 HAC 是否在同一个子网内，此时设备默认报文需要返回到 HAP 进行中转。如果 HAP 和 HAC 在同一个子网时，可以将家乡代理设置为性能更强的 HAC，减少 HAP 的负荷并提高转发效率。

AC间三层漫游 - 直接转发（HAC为家乡代理）



- 漫游前：
  1. STA发送业务报文给HAP。
  2. HAP接收到业务报文后直接将业务报文经过交换机发送给上层网络。
- 漫游后：
  1. STA发送业务报文给FAP。
  2. FAP接收到STA发送的业务报文并通过CAPWAP隧道发送给FAC。
  3. FAC通过HAC和FAC之间的AC间隧道将业务报文转发给HAC。
  4. HAC直接将业务报文发送给上层网络。

- 直接转发模式下，HAP 和 HAC 之间的业务报文不通过 CAPWAP 隧道封装，无法判定 HAP 和 HAC 是否在同一个子网内，此时设备默认报文需要返回到 HAP 进行中转。如果 HAP

和 HAC 在同一个子网时，可以将家乡代理设置为性能更强的 HAC，减少 HAP 的负荷并提高转发效率。

AC间漫游配置介绍

1. 创建漫游组

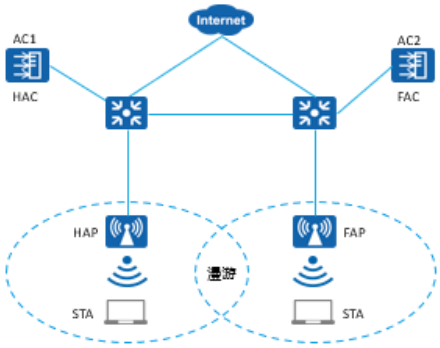
```
[AC-wlan-view] mobility-group name group-name
```

2. 向漫游组中添加成员，此处添加的AC的IP地址为AC的源IP地址。

```
[AC-mc-mg-group-name] member { ip-address ipv4-address | ipv6-address ipv6-address } [ description description ]
```

- 配置漫游组。
- 如果指定了漫游组服务器，则需要在漫游组服务器上配置漫游组。
- 如果没有指定漫游组服务器，则各成员 AC 均需配置漫游组。

配置案例 (1)



配置AC1和AC2的WLAN漫游功能：

```
[AC1-wlan-view] mobility-group name mobility
[AC1-mc-mg-mobility] member ip-address 10.1.201.100
[AC1-mc-mg-mobility] member ip-address 10.1.201.200
[AC1-mc-mg-mobility] quit
```

```
[AC2-wlan-view] mobility-group name mobility
[AC2-mc-mg-mobility] member ip-address 10.1.201.100
[AC2-mc-mg-mobility] member ip-address 10.1.201.200
[AC2-mc-mg-mobility] quit
```

- HAP与HAC，FAP与FAC之间的组网方式为三层组网。
- 配置HAC和FAC形成漫游组，保证STA的业务流量正常。

配置案例 (2)

STA漫游后在AC上查看STA的漫游轨迹：

```
<AC> display station roam-track sta-mac 28b2-bd35-4af3
Access SSID:huawei-guest1
Rx/Tx: Rx-Rate/Tx-Rate Mbps
-------------------------------------------------------------------------------
L2/L3    AC IP          AP name    Radio ID  BSSID          TIME                In Rx/Tx  RSSI   Out Rx/Tx  RSSI
-------------------------------------------------------------------------------
--       10.1.201.100   ap1        1         cccc-8110-2250 2020/06/18 14:09:06 130/130   -44    130/130    -44
L3       10.1.201.200   ap2        1         cccc-8110-22b0 2020/06/18 14:12:24 130/6     -42    -/-
-------------------------------------------------------------------------------
Number of roam track: 1
```

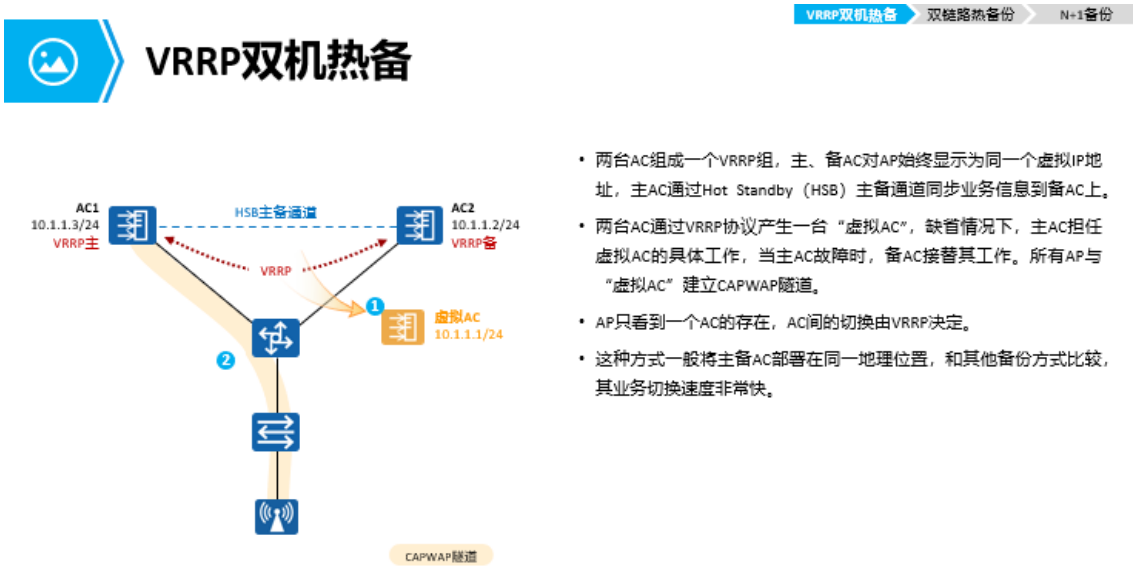
AC 高可靠性概述

- 在 WLAN 组网中，为保证组网可靠性，常见的备份技术有：
- VRRP 双机热备份（主备）
- 双链路冷备份
- 双链路热备份（主备&负载分担）
- N+1 备份
- 为了保证 WLAN 业务的稳定运行，热备份（Hot-Standby Backup）机制可以保证在主设备故障时业务能够不中断的顺利切换到备份设备。

- 热备份是指，当两台设备在确定主用（Master）设备和备用（Backup）设备后，由主用设备进行业务的转发，而备用设备处于监控状态，同时主用设备实时向备用设备发送状态信息和需要备份的信息，当主用设备出现故障后，备用设备及时接替主用设备的业务运行。
- VRRP 双机热备份
- 主备 AC 两个独立的 IP 地址，通过 VRRP 对外虚拟为同一个 IP 地址，单个 AP 和虚拟 IP 建立一条 CAPWAP 链路。
- 主 AC 备份 AP 信息、STA 信息和 CAPWAP 链路信息，

并通过 HSB 主备服务将信息同步给备 AC。主 AC 故障后，备 AC 直接接替工作。

- 双链路热备份
- 单个 AP 分别和主备 AC 建立 CAPWAP 链路，一条主链路，一条备链路。
- 主 AC 仅备份 STA 信息，并通过 HSB 主备服务将信息同步给备 AC。主 AC 故障后，AP 切换到备链路上，备 AC 接替工作。
- 双链路冷备份
- 单个 AP 分别和主备 AC 建立 CAPWAP 链路，一条主链路，一条备链路。
- AC 不备份同步信息。主 AC 故障后，AP 切换到备链路上，备 AC 接替工作。
- N+1 备份
- 单个 AP 只和一个 AC 建立 CAPWAP 链路。
- AC 不备份同步信息。主 AC 故障后，AP 重新与备 AC 建链 CAPWAP 链路，备 AC 接替工作。



- AC 目前支持 VRRP 单实例整机热备，不支持负载均衡。

整机热备具有以下特点:

- 上行链路可以互为备份，主备 VRRP 可以 track 上行口状态，AC 整机主备状态可能与各下行链路通断状态不一致。
- 下行多条链路(包括有线、无线) 采用 MSTP 破环，MSTP 状态变更时会自动清除链路上的 MAC/ARP 表。

HSB 相关概念

- HSB（Hot Standby，热备份）是华为主备公共机制。
- 主备服务（HSB service）：建立和维护主备通道，为各个主备业务模块提供通道通断事件和报文发送/接收接口。
- 主备备份组（HSB group）：HSB 备份组内部绑定 HSB service，为各个主备业务模块提供数据备份通道。HSB 备份组与一个 VRRP 实例绑定，借用 VRRP 机制协商出主备实例。同时，HSB 备份组还负责通知各个业务模块处理批量备份、实时备份、主备切换等事件。

- 基于 VRRP 的双机热备，热备相关的业务都注册到同一个 HSB 备份组，HSB 备份组内部绑定 HSB 服务，同时 HSB 备份组与一个 VRRP 实例绑定，从而业务通过 HSB 备份组获知当前用户的主备状态、以及主备切换等事件，并通过 HSB 组的接口进行备份数据的接收和发送。

- HSB 主备服务负责在两个互为备份的设备间建立主备备份通道，维护主备通道的链路状态，为其他业务提供报文的收发服务，并在备份链路发生故障时通知主备业务备份组进行相应的处理。
- HSB 主备服务主要包括两个方面：

- 建立主备备份通道
- 维护主备通道的链路状态
- HSB 主备服务主要包括两个方面： 建立主备备份通道：通过配置主备服务本端和对端的 IP 地址和端口号，从而建立主备机制报文发送的 TCP 通道，为其他业务提供报文的收发以及链路状态变化通知服务。
- 维护主备通道的链路状态：通过发送主备服务报文和重传等机制来防止 TCP 较长时间中断但协议栈没有检测到该连接中断。如果在主备服务报文时间间隔与重传次数乘积的时间内还未收到对端发送的主备服务报文，设备则会收到异常通知，并且准备重建主备备份通道。

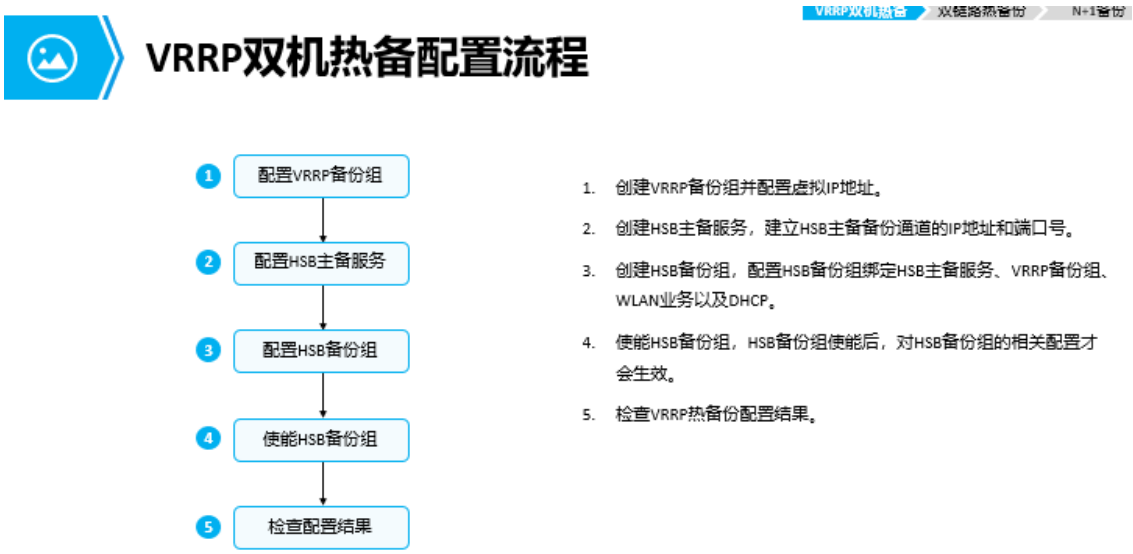
数据同步

基于 VRRP 双机热备备份信息包括用户表项、CAPWAP 链路信息以及 AP 表项等信息，备份的方式有实时备份，批量备份，定时备份。

- 批量备份：主用设备会将已有的会话表项一次性同步到新加入的备份设备上，使主备 AC 信息对齐，这个过程称为批量备份。批量备份会在 AC 主备确立时进行触发。
- 实时备份：主用设备在产生新表项或表项变化后会及时备份到备份设备上。
- 定时同步：备用设备会每隔 30 分钟检查其已有的会话表项与主用设备是否一致，若不一致则将主用设备上的会话表项同步到备用设备。
- 当主用设备出现故障，流量切换到备份设备时，要求主用设备和备份设备的会话表项完全一致，否则有可能导致会话中断。因此，需要一种机制在主用设备上会话建立或表项变化时将相关信息同步保存到备份设备上。HSB 主备服务处理模块可以提供数据的备份功能，它负责在两个互为备份的设备间

建立主备通道，并维护主备通道的链路状态，提供报文的收发服务。

- HSB 业务实时备份：
- 用户数据信息备份
- CAPWAP 隧道信息备份
- AP 表项备份
- DHCP 地址信息备份
- HSB 主备通道，可通过两台 AC 之间的直连物理链路承载，也可通过交换机承载，例如复用 VRRP 报文交互所处的物理通道。



配置介绍 (1)

1. 在对应的接口视图下，创建VRRP备份组并配置虚拟IP地址。

```
[AC-GigabitEthernet0/0/1] vrrp vrid virtual-router-id virtual-ip virtual-address
```

2. 配置设备在VRRP备份组中的优先级，默认为100，主设备的优先级要大于备设备。

```
[AC-GigabitEthernet0/0/1] vrrp vrid virtual-router-id priority priority-value
```

3. 创建HSB主备服务并进入HSB主备服务视图。

```
[AC] hsb-service service-index
```

4. 配置建立HSB主备备份通道的IP地址和端口号。

```
[AC-hsb-service-0] service-ip-port local-ip { local-ipv4-address | local-ipv6-address } peer-ip { peer-ipv4-address | peer-ipv6-address } local-data-port local-port peer-data-port peer-port
```


配置介绍 (2)

1. 创建HSB备份组并进入HSB备份组视图。

```
[AC] hsb-group group-index
```

2. 配置HSB备份组绑定的HSB主备服务。

```
[AC-hsb-group-0] bind-service service-index
```

3. 配置HSB备份组绑定的VRRP备份组。

```
[AC-hsb-group-0] track vrrp vrid virtual-router-id interface interface-type interface-number
```

4. 配置WLAN业务绑定HSB备份组。

```
[AC] hsb-service-type ap hsb-group group-index
```

5. 配置DHCP业务绑定HSB备份组。

```
[AC] hsb-service-type dhcp hsb-group group-index
```

6. 配置准入控制用户绑定HSB备份组。

```
[AC] hsb-service-type access-user hsb-group group-index
```


配置介绍 (3)

1. 使能HSB备份组。

```
[AC-hsb-group-0] hsb enable
```

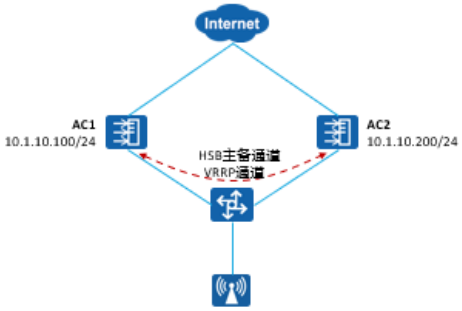
2. 查看HSB备份组的信息。

```
[AC] display hsb-group group-index
```

3. 查看HSB主备服务的信息。

```
[AC] display hsb-service service-index
```

配置案例 (1)



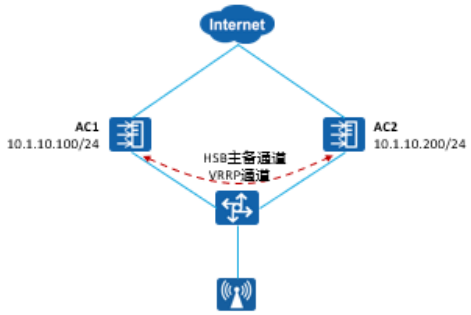
- AC1和AC2通过VLANIF10建立VRRP主备关系，VRRP的虚拟IP为10.1.10.1，AC1为主设备，且优先级为120；
- 使用HSB技术实现双机热备。

AC的VRRP配置如下：

```
[AC1]interface Vlanif10
[AC1-Vlanif10]ip address 10.1.10.100 255.255.255.0
[AC1-Vlanif10]vrrp vrid 1 virtual-ip 10.1.10.1
[AC1-Vlanif10]vrrp vrid 1 priority 120
```

```
[AC2]interface Vlanif10
[AC2-Vlanif10]ip address 10.1.10.200 255.255.255.0
[AC2-Vlanif10]vrrp vrid 1 virtual-ip 10.1.10.1
```


配置案例 (2)



- AC1和AC2通过VLANIF10建立VRRP主备关系，VRRP的虚拟IP为10.1.10.1，AC1为主设备，且优先级为120；
- 使用HSB技术实现双机热备。

AC的HSB配置如下：

```
[AC1]hsb-service 0
[AC1-hsb-service-0]service-ip-port local-ip 10.1.10.100 peer-ip 10.1.10.200 local-data-port 10241 peer-data-port 10241
[AC1-hsb-service-0]quit
```

```
[AC1]hsb-group 0
[AC1-hsb-group-0]bind-service 0
[AC1-hsb-group-0]track vrrp vrid 1 interface Vlanif10
[AC1-hsb-group-0]quit
```

```
[AC1]hsb-service-type access-user hsb-group 0
[AC1]hsb-service-type dhcp hsb-group 0
[AC1]hsb-service-type ap hsb-group 0
```

```
[AC1]hsb-group 0
[AC1-hsb-group-0]hsb enable
```

- AC2 配置与 AC1 相同，此处不再赘述。

配置案例 (3)

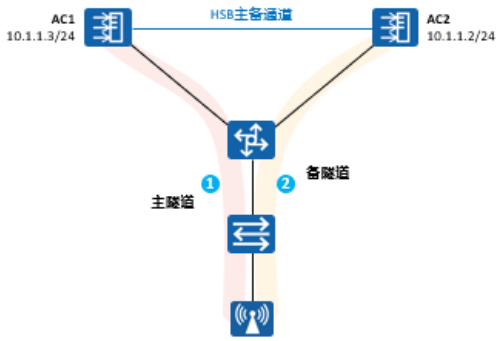
在AC上查看主备服务的建立情况。

```
[AC1] display hsb-service 0
Hot Standby Service Information:
-------------------------------------------------------
Local IP Address      : 10.1.10.100
Peer IP Address       : 10.1.10.200
Source Port           : 10241
Destination Port      : 10241
Keep Alive Times      : 2
Keep Alive Interval   : 1
Service State         : Connected
Service Batch Modules :
Shared-key            : -
-------------------------------------------------------
```

在AC上查看HSB备份组的运行情况。

```
[AC1] display hsb-group 0
Hot Standby Group Information:
-------------------------------------------------------
HSB-group ID                : 0
Vrrp Group ID               : 1
Vrrp Interface              : Vlanif10
Service Index               : 0
Group Vrrp Status           : Master
Group Status                : Active
Group Backup Process        : Realtime
Peer Group Device Name      : AirEngine 9700-M
Peer Group Software Version : V200R019C00
Group Backup Modules        : Access-user
                              DHCP
                              AP
```

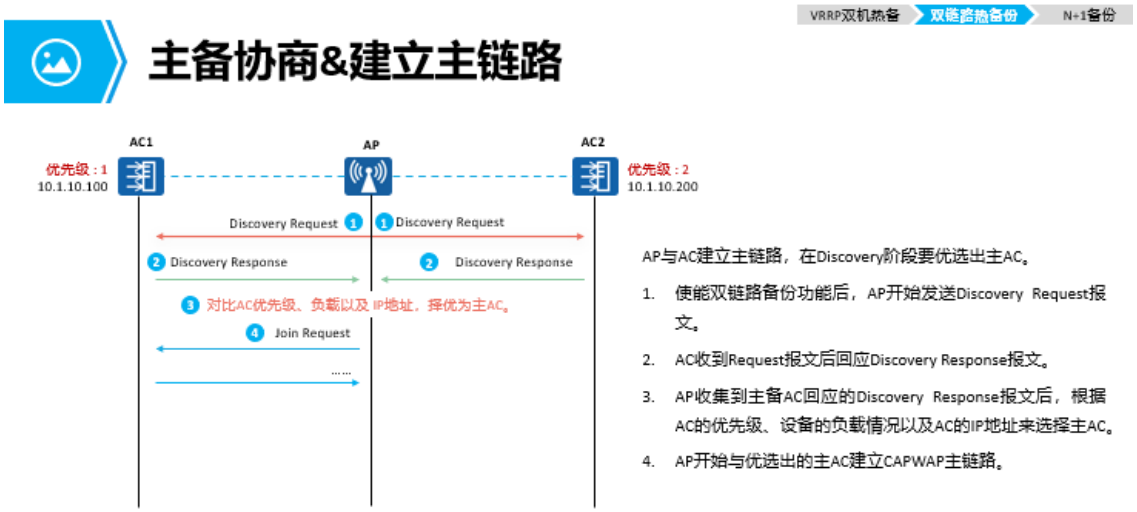

双链路双机热备



- 双链路双机热备场景下，业务直接绑定HSB备份服务，这样HSB对业务仅提供备份数据收发的功能，用户的主备状态由双链路机制进行维护。
- AP同时与主备AC之间分别建立CAPWAP隧道，AC间的业务信息通过HSB主备通道同步。
- 当AP和主AC间链路断开，AP会通知备AC切换成主AC。

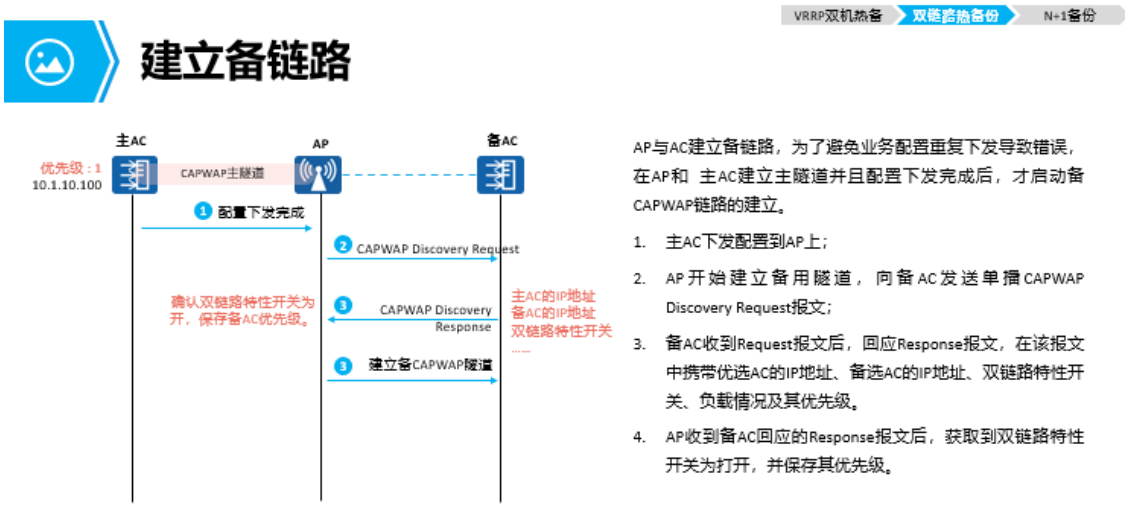
- 该方案除了支持主备备份之外，还支持负载分担模式。负载分担模式下可以指定一部分 AP 的主 AC 为 AC1，与其建立 CAPWAP 主链路，一部分 AP 的主 AC 为 AC2，与其建立 CAPWAP 主链路。
- 双链路双机热备的主备 AC 不受地理位置限制，部署灵活，可进行负载分担，有效利用资源，但业务切换速度较慢。
- 图中，AC1 和 AC2 经过部署为双链路双机热备，只绑定 HSB 主备服务，提供双机热备份 HSB 隧道。AP 需依次与两台 AC 建立 CAPWAP 隧道，通过 AC 下发的 CAPWAP 报文

中的优先级判断主用 AC 与备用 AC。



- 建立主链路时，除了 Discovery 阶段要优选出主 AC，其他过程跟正常情况下的 CAPWAP 隧道建立过程一致。
- 在 Discovery 阶段，使能双链路备份功能后，AP 开始发送 Discovery Request 报文，分为单播方式和广播方式：
- 如果预先通过静态方式、DHCP 服务器方式或 DNS 方式指定了主备 AC 的 IP 地址，AP 向 AC 发送单播 Discovery Request 报文请求与主备 AC 关联。
- 如果没有配置 AC 的静态 IP 地址或者单播没有回应时，AP 将发送广播 Discovery Request 报文请求同网段内可关联的 AC。
- 不管是单播发现还是广播发现，如果主备 AC 都正常，都会回应 Discovery Response 报文，并在该报文中携带双链路特性开关、优先级、负载情况以及 IP 地址。
- AP 收集到主备 AC 回应的 Discovery Response 报文后，根据 AC 的优先级、设备的负载情况以及 AC IP 地址来选择主 AC 并开始与其建立 CAPWAP 主链路，优选顺序如下：
- 比较 AC 的优先级，优先级值小的为主 AC，默认优先级为 0，最大值为 7，优先级取值越小，优先级越高。；

- 优先级相同情况下，比较 AC 设备的负载情况，即 AP 个数和 STA 个数，负载轻的为主 AC。优先选择当前可接入 AP 数大的 AC 为主 AC，如果当前可接入 AP 数相同，则选择当前可接入 STA 数大的 AC 为主 AC；
- 负载相同情况下，比较 IP 地址，IP 地址小的为主 AC。
- 说明：当前可接入 AP 数=可接入的最大 AP 数-当前已接入的 AP 数，当前可接入 STA 数=可接入的最大 STA 数-当前已接入的 STA 数。



- 说明：如果该 AC 的优先级修改为比步骤 1 已经建立好 CAPWAP 链路的 AC 优先级高，也不进行主备倒换，待建立隧道完成后再进行倒换。
- AP 发送的 Join Request 中，会携带一个自定义消息类型，告诉备 AC 配置已经下发过了，不需要再下发。AC 收到 Join Request，获取到该自定义消息时，在配置下发阶段，会跳过配置下发流程，避免对 AP 重复下发配置。
- 备链路建立完成后，AP 重新根据两个链路的优先级决策出主备 AC。
- 缺省情况下，CAPWAP 心跳检测的间隔时间为 25 秒，心跳检测报文次数为 6。如果开启了双链路备份功能，则 CAPWAP 心跳检测的间隔时间为 25 秒，心跳检测报文次数为 3。

- 说明：
- 如果在配置双链路备份时需要使用 WDS 或 Mesh，建议配置 CAPWAP 心跳检测的间隔时间为 25 秒，心跳检测报文次数至少为 6 次。否则由于双链路备份时缺省的心跳报文间隔时间为 25 秒，心跳检测报文次数为 3 次，会导致 WDS 或 Mesh 链路不稳定，无法保证用户正常接入。
- 配置 CAPWAP 心跳检测间隔时间和次数低于默认值会影响 CAPWAP 链路可靠性，请谨慎修改，建议使用默认值。

配置介绍 (2)

1. 创建HSB主备服务并进入HSB主备服务视图。

```
[AC] hsb-service service-index
```

2. 配置建立HSB主备备份通道的IP地址和端口号。

```
[AC] service-ip-port local-ip { local-ipv4-address | local-ipv6-address } peer-ip { peer-ipv4-address | peer-ipv6-address } local-data-port local-port peer-data-port peer-port
```

3. 配置WLAN业务绑定HSB备份组。

```
[AC] hsb-service-type ap hsb-group group-index
```

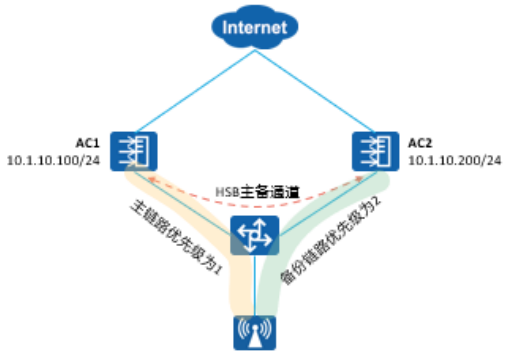
4. 配置DHCP业务绑定HSB备份组。

```
[AC] hsb-service-type dhcp hsb-group group-index
```

5. 配置准入控制用户绑定HSB备份组。

```
[AC] hsb-service-type access-user hsb-service service-index
```


配置案例 (1)



- AC1和AC2配置双链路双机热备，AC1为主设备，优先级为1，AC2为备设备，优先级为2；
- 使用HSB技术实现双机热备。

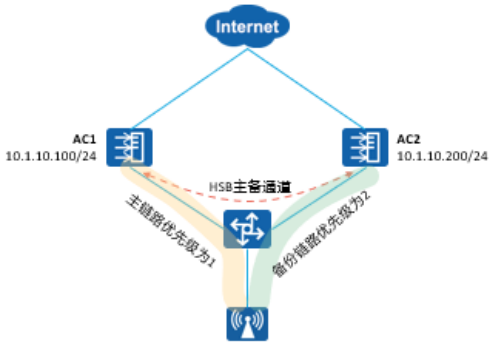
AC1的配置如下：

```
[AC1] wlan
[AC1-wlan-view] ac protect enable
[AC1-wlan-view] ac protect protect-ac 10.1.10.200 priority 1
```

```
[AC1] hsb-service 0
[AC1-hsb-service-0] service-ip-port local-ip 10.1.10.100 peer-ip 10.1.10.200 local-data-port 10241 peer-data-port 10241
[AC1-hsb-service-0] quit
```

```
[AC1] hsb-service-type access-user hsb-group 0
[AC1] hsb-service-type dhcp hsb-group 0
[AC1] hsb-service-type ap hsb-group 0
```


配置案例 (2)



- AC1和AC2配置双链路双机热备，AC1为主设备，优先级为1，AC2为备设备，优先级为2；
- 使用HSB技术实现双机热备。

AC2的配置如下：

```
[AC2] wlan
[AC2-wlan-view] ac protect enable
[AC2-wlan-view] ac protect protect-ac 10.1.10.100 priority 2
```

```
[AC2] hsb-service 0
[AC2-hsb-service-0] service-ip-port local-ip 10.1.10.200 peer-ip 10.1.10.100 local-data-port 10241 peer-data-port 10241
[AC2-hsb-service-0] quit
```

```
[AC2] hsb-service-type access-user hsb-group 0
[AC2] hsb-service-type dhcp hsb-group 0
[AC2] hsb-service-type ap hsb-group 0
```

配置案例 (3)

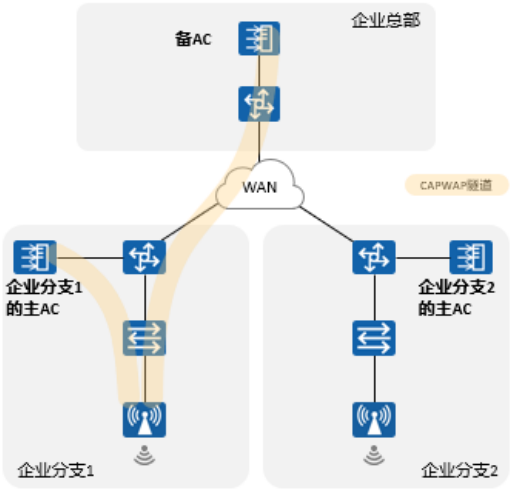
在AC上查看双链路备份的配置信息。

```
[AC1] display ac protect
------------------------------------------------------------
Protect state          : enable
Protect AC IPv4        : 10.1.10.200
Protect AC IPv6        : -
Priority               : 0
Protect restore        : enable
...
```

在AC上查看主备服务的建立情况。

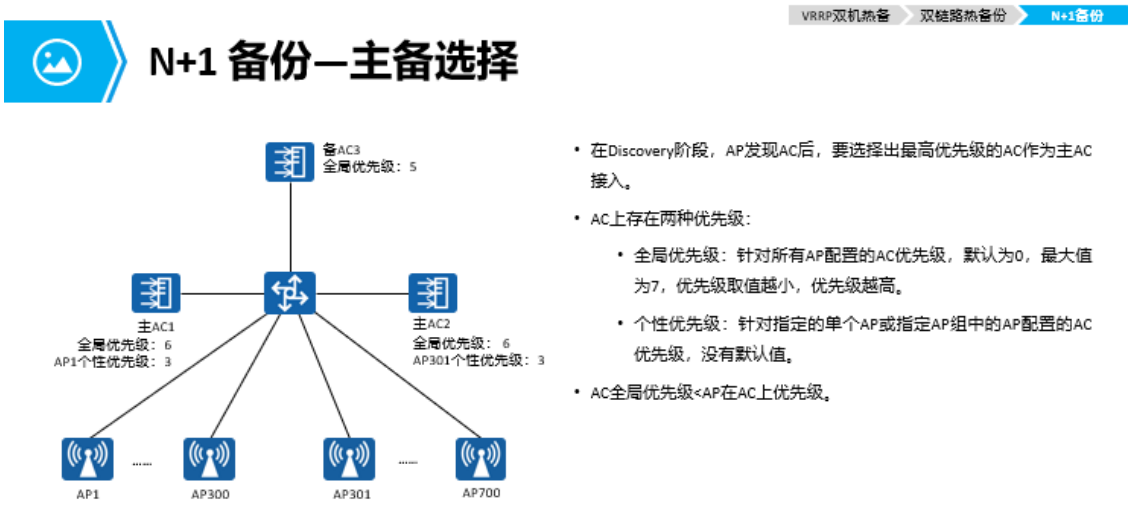
```
[AC1] display hsb-service 0
Hot Standby Service Information:
------------------------------------------------------------
 Local IP Address       : 10.1.10.100
 Peer IP Address        : 10.1.10.200
 Source Port            : 10241
 Destination Port       : 10241
 Keep Alive Times       : 5
 Keep Alive Interval    : 3
 Service State          : Connected
 Service Batch Modules  : AP
                          Access-user
                          DHCP
.....
```


AC可靠性：N+1



- N+1备份是指在AC+FIT AP的网络架构中，使用一台AC作为备AC，为多台主AC提供备份服务的一种解决方案。
- 网络正常情况下，AP只与各自所属的主AC建立CAPWAP链路。
- 当主AC故障或主AC与AP间CAPWAP链路故障时，备AC替代主AC来管理AP，备AC与AP间建立CAPWAP链路，为AP提供业务服务。
- 支持主备倒换，支持主备回切。

- 当 AP 与主用 AC 之间的 CAPWAP 隧道中断时，将触发 AP 与备用 AC 建立 CAPWAP 隧道，此时 AP 会重新与该 AC 建链、重启并获取配置，在该过程中，业务将会受影响。



- 当 AC 收到 AP 发送的 Discovery Request 报文时，如果 AC 没有为该 AP 配置个性优先级，则在回应的 Discovery Response 报文中携带全局优先级；
- 如果 AC 已为该 AP 配置了个性优先级，则在回应的 Discovery Response 报文中携带个性优先级。
- 正确配置主 AC 和备 AC 的不同优先级，可以控制 AP 能够在指定的主 AC 或备 AC 上线
- 优选顺序如下：
- AP 查看优选 AC，如果只有一个优选 AC，则此 AC 作为主 AC。如果存在多个优选 AC，则选择负载最轻的 AC 作为主 AC，如果负载相同选择 IP 地址最小的作为主 AC；
- 负载的比较方式：比较 AC 设备的负载情况，即 AP 个数和 STA 个数，负载轻的为主 AC。优先选择当前可接入 AP 数大的 AC 为主 AC，如果当前可接入 AP 数相同，则选择当前可接入 STA 数大的 AC 为主 AC；
- 如果没有优选 AC，查看备选 AC，如果只有一个备选 AC，则此 AC 作为主 AC，如果存在多个备选 AC，则选择负载最轻的 AC 作为主 AC，如果负载相同选择 IP 地址最小的作为主 AC；
- 如果没有备选 AC，比较 AC 的优先级，优先级最高的作

为主 AC。优先级取值越小，优先级越高。优先级的具体判断方式参考主备优先级；

- 优先级相同情况下，则选择负载最轻的 AC 作为主 AC；
- 负载相同情况下，继续比较 IP 地址，IP 地址小的为主 AC。

配置介绍 (1)

1. 创建AP系统模板，并进入模板视图。

   [AC-wlan-view] **ap-system-profile name** *profile-name*

2. 配置优选AC的IP地址。

   [AC-wlan-ap-system-prof-huawei] **primary-access** { **ip-address** *ip-address* | **ipv6-address** *ipv6-address* }

3. 配置备选AC的IP地址。

   [AC-wlan-ap-system-prof-huawei] **backup-access** { **ip-address** *ip-address* | **ipv6-address** *ipv6-address* }

4. 在AP组中引用AP系统模板。

   [AC-wlan-ap-group-huawei] **ap-system-profile** *profile-name*

5. 在AP中引用AP系统模板。

   [AC-wlan-ap-0] **ap-system-profile** *profile-name*

6. 重启AP，使双链路备份功能生效。

   [AC-wlan-view] **ap-reset** { **all** | **ap-name** *ap-name* | **ap-mac** *ap-mac* | **ap-id** *ap-id* | **ap-group** *ap-group* | **ap-type** { **type** *type-name* | **type-id** *type-id* } }

配置介绍 (2)

1. 使能全局回切功能

   [AC-wlan-view] **undo ac protect restore disable**

2. 配置CAPWAP心跳检测的间隔时间以及次数。

   [AC] **capwap echo** { **interval** *interval-value* | **times** *times-value* }

3. 使能N+1备份功能。

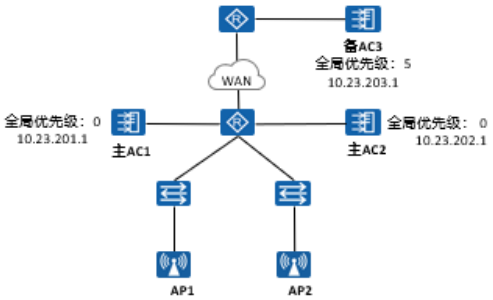
   [AC-wlan-view] **undo ac protect enable**

   ac protect enable命令用来使能全局双链路备份功能并去使能N+1备份功能。

   undo ac protect enable命令用来去使能全局双链路备份功能并使能N+1备份功能。

   缺省情况下，全局双链路备份功能未使能，N+1备份功能使能。

配置案例 (1)



- 已经完成各个AC和其它网络设备实现网络互通的配置。
- AC1作为AP1的主AC，AC2作为AP2的主AC，在主AC上配置主备AC信息。
- AC3作为AP1和AP2的备AC，在备AC上配置两个AP组，保持WLAN基本业务，业务配置和主AC保持一致。
- 先后在主备AC上配置N+1备份功能。配置完成后需要重启所有AP。

AC1的配置如下：

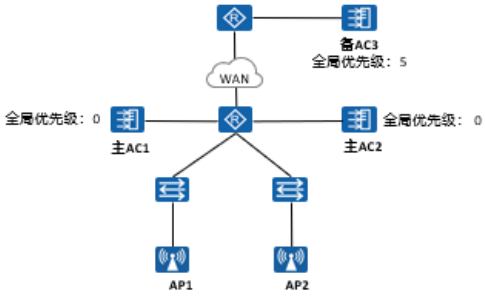
```
[AC1-wlan-view] ap-system-profile name ap-system1
[AC1-wlan-ap-system-prof-ap-system1] primary-access ip-address 10.23.201.1
[AC1-wlan-ap-system-prof-ap-system1] backup-access ip-address 10.23.203.1
[AC1-wlan-ap-system-prof-ap-system1] quit
[AC1-wlan-view] ap-group name ap-group1
[AC1-wlan-ap-group-ap-group1] ap-system-profile ap-system
[AC1-wlan-ap-group-ap-group1] quit
```

AC2的配置如下：

```
[AC2-wlan-view] ap-system-profile name ap-system2
[AC2-wlan-ap-system-prof-ap-system2] primary-access ip-address 10.23.202.1
[AC2-wlan-ap-system-prof-ap-system2] backup-access ip-address 10.23.203.1
[AC2-wlan-ap-system-prof-ap-system2] quit
[AC2-wlan-view] ap-group name ap-group2
[AC2-wlan-ap-group-ap-group2] ap-system-profile ap-system2
[AC2-wlan-ap-group-ap-group2] quit
```

VRRP双机热备 双链路热备份 N+1备份

配置案例 (2)



- 已经完成各个AC和其它网络设备实现网络互通的配置。
- AC1作为AP1的主AC，AC2作为AP2的主AC，在主AC上配置主备AC信息。
- AC3作为AP1和AP2的备AC，在备AC上配置两个AP组，保持WLAN基本业务，业务配置和主AC保持一致。
- 先后在主备AC上配置N+1备份功能。配置完成后需要重启所有AP。

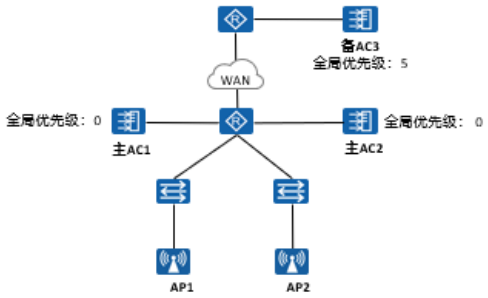
AC3的配置如下：

```
[AC3-wlan-view] ap-system-profile name ap-system1
[AC3-wlan-ap-system-prof-ap-system1] primary-access ip-address 10.23.201.1
[AC3-wlan-ap-system-prof-ap-system1] backup-access ip-address 10.23.203.1
[AC3-wlan-ap-system-prof-ap-system1] quit
```

```
[AC3-wlan-view] ap-system-profile name ap-system2
[AC3-wlan-ap-system-prof-ap-system2] primary-access ip-address 10.23.202.1
[AC3-wlan-ap-system-prof-ap-system2] backup-access ip-address 10.23.203.1
[AC3-wlan-ap-system-prof-ap-system2] quit
```

```
[AC3-wlan-view] ap-group name ap-group1
[AC3-wlan-ap-group-ap-group1] ap-system-profile ap-system1
[AC3-wlan-ap-group-ap-group1] quit
[AC3-wlan-view] ap-group name ap-group2
[AC3-wlan-ap-group-ap-group2] ap-system-profile ap-system2
[AC3-wlan-ap-group-ap-group2] quit
```

配置案例 (3)



- 已经完成各个AC和其它网络设备实现网络互通的配置。
- AC1作为AP1的主AC，AC2作为AP2的主AC，在主AC上配置主备AC信息。
- AC3作为AP1和AP2的备AC，在备AC上配置两个AP组，保持WLAN基本业务，业务配置和主AC保持一致。
- 先后在主备AC上配置N+1备份功能。配置完成后需要重启所有AP。

AC的配置如下：

```
[AC1-wlan-view] undo ac protect enable
Info: Backup function has already disabled.
[AC1-wlan-view] ap-reset all
Warning: Reset AP(s), continue?[Y/N]: y
```

```
[AC2-wlan-view] undo ac protect enable
Info: Backup function has already disabled.
[AC2-wlan-view] ap-reset all
Warning: Reset AP(s), continue?[Y/N]: y
```

```
[AC3-wlan-view] undo ac protect restore disable
Info: Protect restore has already enabled.
[AC3-wlan-view] undo ac protect enable
Info: Backup function has already disabled.
[AC3-wlan-view] ap-reset all
Warning: Reset AP(s), continue?[Y/N]: y
```

- 缺省情况下，全局回切功能处于使能状态，执行命令 undo ac protect restore disable 会提示 Info。
- 缺省情况下，N+1 备份功能开启，执行命令 undo ac protect enable 会提示 Info。需要在主 AC 上继续执行命令 ap-reset all 重启所有 AP，AP 重启后，N+1 备份功能开始生效。

配置案例 (4)

在主AC1上查看AC上N+1备份信息。

```
[AC1] display ac protect
-------------------------------------------------------------
Protect state       : disable
Protect AC IPv4     : -
Protect AC IPv6     : -
Priority            : 0
Protect restore     : enable
```

```
[AC1] display ap-system-profile name ap-system
-------------------------------------------------------------
AC priority         : -
Protect AC IP address : -
Primary AC          : 10.23.201.1
Backup AC           : 10.23.203.1
```

在主AC2上查看AC上N+1备份信息。

```
[AC2] display ac protect
-------------------------------------------------------------
Protect state       : disable
Protect AC IPv4     : -
Protect AC IPv6     : -
Priority            : 0
Protect restore     : enable
```

```
[AC2] display ap-system-profile name ap-system
-------------------------------------------------------------
AC priority         : -
Protect AC IP address : -
Primary AC          : 10.23.202.1
Backup AC           : 10.23.203.1
```

配置案例 (5)

在备AC3上，查看AC上N+1备份信息。

```
[AC3] display ac protect
------------------------------------------------------------
Protect state        : disable
Protect AC IPv4      : -
Protect AC IPv6      : -
Priority             : 0
Protect restore      : enable
...
```

```
[AC3-wlan-view] display ap-system-profile name ap-system1
------------------------------------------------------------------------------
AC priority                 : -
Protect AC IP address       : -
Primary AC                  : 10.23.201.1
Backup AC                   : 10.23.203.1
...
```

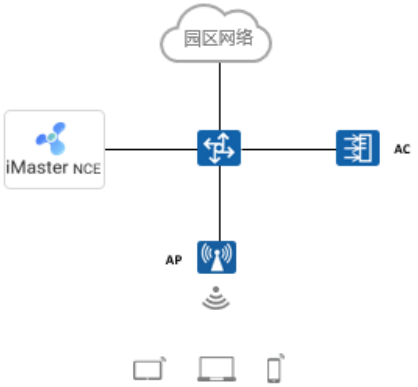
```
[AC3-wlan-view] display ap-system-profile name ap-system2
------------------------------------------------------------------------------
AC priority                 : -
Protect AC IP address       : -
Primary AC                  : 10.23.202.1
Backup AC                   : 10.23.203.1
...
```

AC可靠性：小结

对比项	VRRP双机热备	双链路双机热备	N+1备份
切换速度	主备切换速度快，对业务影响小。通过配置VRRP抢占时间，相比于其他备份方式实现更快的切换	AP状态切换慢，需等待检测到CAPWAP断链超时后才会切换，主备切换后终端不需要重新上线	AP状态切换慢，需等待检测到CAPWAP断链超时后才会切换，AP、终端均需要重新上线，业务会出现短暂中断
主备AC异地部署	不建议主备AC异地部署	支持	支持
约束条件	主备AC的型号和软件版本需完全一致。 一台备AC只支持为一台主AC提供备份。	主备AC的型号和软件版本需完全一致。 一台备AC只支持为一台主AC提供备份。	主备AC产品形态可以不同，AC的软件版本必须一致。 一台备AC支持为多台主AC提供备份，能降低购买设备的成本。
适用范围	对可靠性要求高，且无须异地部署主备AC的场景	对可靠性要求高，且要求异地部署主备AC的场景	对可靠性要求较低，对成本控制要求较高的场景

NAC概述

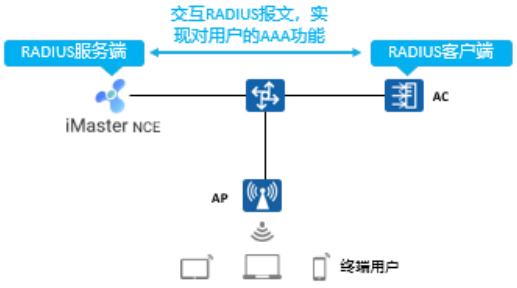
NAC（Network Admission Control）称为网络接入控制，通过对接入网络的客户端和用户的认证保证网络的安全，是一种“端到端”的安全技术。



- NAC：
  - 用于用户和接入设备之间的交互。
  - NAC负责控制用户的接入方式（802.1X，MAC或Portal认证），接入过程中的各类参数和定时器。
  - 确保合法用户和接入设备建立安全稳定的连接。

RADIUS概述

- AAA可以通过多种协议来实现，在实际应用中，最常使用RADIUS协议。
- RADIUS是一种分布式的、客户端/服务器结构的信息交互协议，能保护网络不受未授权访问的干扰，常应用在既要求较高安全性、又允许远程用户访问的各种网络环境中。
- 该协议定义了基于UDP（User Datagram Protocol）的RADIUS报文格式及其传输机制，并规定UDP端口1812、1813分别作为默认的认证、计费端口。
- RADIUS协议的主要特征如下：
  - 客户端/服务器模式
  - 安全的消息交互机制
  - 良好的扩展性

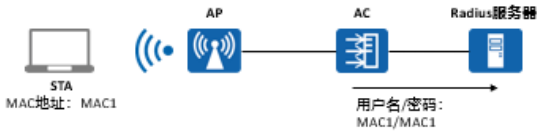


802.1X认证

- 802.1X是IEEE制定的关于用户接入网络的认证标准，主要解决以太网内认证和安全方面的问题。
- 802.1X认证系统为典型的Client/Server结构，包括3个实体：请求方、认证方和认证服务器。
- 认证服务器通常是RADIUS服务器，用于对申请者进行认证、授权和计费。
- 对于大中型企业的员工，推荐使用802.1X认证。

- 802.1X 认证系统使用可扩展认证协议（Extensible Authentication Protocol，EAP）来实现申请者、认证者和认证服务器之间的信息交互。常用的 802.1X 认证协议有防护扩展验证协议（Protected Extensible Authentication Protocol，PEAP）和传输层安全性协议（Transport Layer Security，TLS），其区别如下：
- PEAP：管理员给用户分配用户名、密码。用户在接入 WLAN 时输入用户名、密码进行认证。
- TLS：用户使用证书进行认证，此认证方式一般结合企业 App 使用，如华为的 EasyAccess。
- 对于大中型企业的员工，推荐使用 802.1X 认证。

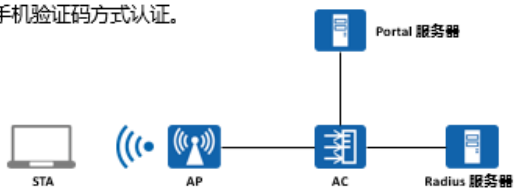
MAC认证



- MAC认证是一种基于MAC地址对用户的网络访问权限进行控制的认证方法，它不需要用户安装任何客户端软件。
- 接入设备在启动了MAC认证的接口上首次检测到用户的MAC地址后，即启动对该用户的认证操作。
- 认证过程中，不需要用户手动输入用户名或者密码。
- MAC认证常用于哑终端（如打印机）的接入认证，或者结合认证服务器完成MAC优先的Portal认证，用户首次认证通过后，一定时间内免认证再次接入。

Portal认证

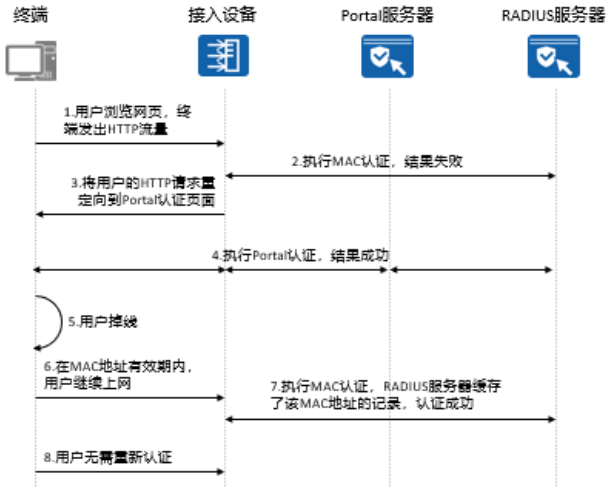
- Portal认证通常也称为Web认证，将浏览器作为认证客户端，不需要安装单独的认证客户端。
- 用户上网时，必须在Portal页面进行认证，只有认证通过后才可以使用网络资源，同时服务提供商可以在Portal页面上开展业务拓展，如展示商家广告等。
- 对于大中型企业的访客、商业会展和公共场所，推荐使用Portal认证。
- 常用的Portal认证方式如下：
  - 用户名和密码方式：由前台管理员给访客申请一个临时账号，访客使用临时账号认证。
  - 短信认证：访客通过手机验证码方式认证。



- 定义
- Portal 认证通常也称为 Web 认证，一般将 Portal 认证网站称为门户网站。用户上网时，必须在门户网站进行认证，如果未认证成功，仅可以访问特定的网络资源，认证成功后，才可以访问其他网络资源。
- 优点
- 一般情况下，客户端不需要安装额外的软件，直接在 Web 页面上认证，简单方便。
- 便于运营，可以在 Portal 页面上进行业务拓展，如广告推送、企业宣传等。

- 技术成熟，被广泛应用于运营商、连锁快餐、酒店、学校等网络。
- 部署位置灵活，可以在接入层或关键数据的入口作访问控制。
- 用户管理灵活，可基于用户名与 VLAN/IP 地址/MAC 地址的组合对用户进行认证。

MAC优先的Portal认证



技术背景

用户进行Portal认证成功后，如果断开网络，重新连接时需要再次输入用户名、密码，体验差。

MAC优先的Portal认证

- 用户进行Portal认证成功后，在一定时间内断开网络重新连接，能够直接通过MAC认证接入，无需输入用户名密码重新进行Portal认证。
- 该功能需要在设备配置MAC+Portal的混合认证，同时在认证服务器上开启MAC优先的Portal认证功能并配置MAC地址有效时间。

三种认证方式比较

NAC包括三种认证方式：802.1X认证、MAC认证和Portal认证。由于三种认证方式认证原理不同，各自适合的场景也有所差异，实际应用中，可以根据场景部署某一种合适的认证方式，也可以部署几种认证方式组成的混合认证，混合认证的组合方式以设备实际支持为准。

对比项	802.1X认证	MAC认证	Portal认证
适合场景	新建网络、用户集中、信息安全要求严格的场景	打印机、传真机等哑终端接入认证的场景	用户分散、用户流动性大的场景
客户端需求	需要	不需要	不需要
优点	安全性高	无需安装客户端	部署灵活
缺点	部署不灵活	需登记MAC地址，管理复杂	安全性不高

思考题：

- （简答题）在部署 WLAN 三层组网的时候，需要配置 D

HCP Option43，那么 Option43 的作用是什么？

- （简答题）二层漫游和三层漫游的最大的区别是什么？
- （简答题）WLAN 双机热备份数据同步的方式有几种，分别应用在什么场景下？

答案：

- AP 发送的 DHCP 广播请求报文是二层报文，不能在三层组网中传输，所以广播发现不了三层组网中 AC，必须通过 Option43 来通告 AC 的 IP 地址，否则 AP 获取不到 AC 的 IP 地址，后续 AP 无法上线。
- 二层漫游和三层漫游的最大的区别是什么？
- 区别在于漫游前后关联的 AP 的服务集上的 VLAN 不同。
- 二层漫游是指客户端在同一子网内漫游。
- 三层漫游是指客户端在不同子网间漫游。
- 数据同步的方式有批量备份、实时备份和定时同步：
- 批量备份：在配置双机热备份功能后，先运行的主用设备会将已有的会话表项一次性同步到新加入的备份设备上。
- 实时备份：主用设备在产生新表项或表项变化后会及时备份到备份设备上。
- 定时同步：备用设备会每隔 30 分钟检查其已有的会话表项与主用设备是否一致，若不一致则将主用设备上的会话表项同步到备用设备。