H3C V7 无线产品通用优化操作

规范说明

新华三技术有限公司
http://www.h3c.com

资料版本：6W100-20191125

目 录

1 V7 无线产品通用优化操作规范

1.1 （必选）信号强度达标

1.1.1 应用说明

首先，信号覆盖的强度是第一位的，所有优化操作方式都以满足信号强度为基础。目标覆盖区域的信号覆盖强度要求不低于-65dBm。

特别，对于使用 500mW 大功率 AP 的场景，除了关注终端侧信号强度，也要同时关注 AP 侧检测的 RSSI 强度，确保上行和下行信号强度都能达标。一般 RSSI 大于 30 为良好，低于 20 为较差。

```
<AC>display wlan client verbose
Total number of clients: 64

 MAC address                     : 0cd6-bd00-a98e
 IPv4 address                    : N/A
 ……
 RSSI                            : 40
 Rx/Tx rate                      : 72.2/72.2
```

1.1.2 部署建议

在部署设备时，AP 或者天线要尽量部署在距离目标区域较近的位置，并保证无金属板、厚墙等削弱无线信号的障碍物。

对于宿舍或者教室类应用场景，不建议在楼道部署 AP，这种覆盖方式会导致两个方面的问题：

- AP 信号穿墙后，房间内的信号会较弱，可能无法满足终端的接入信号要求；
- AP 全楼道部署会导致 AP 之间覆盖区域重叠较多，干扰较难控制。

对于教室、会议室等高密接入场景，建议 AP 直接入室放装；对于宿舍、酒店、公寓楼等场景，可以考虑采用 X 分、面板等低成本部署方案。

1.2 （必选）信道规划和设置固定信道

1.2.1 应用说明

信道规划和功率调整将是 WLAN 网络的首要的、最先实施的优化方法。

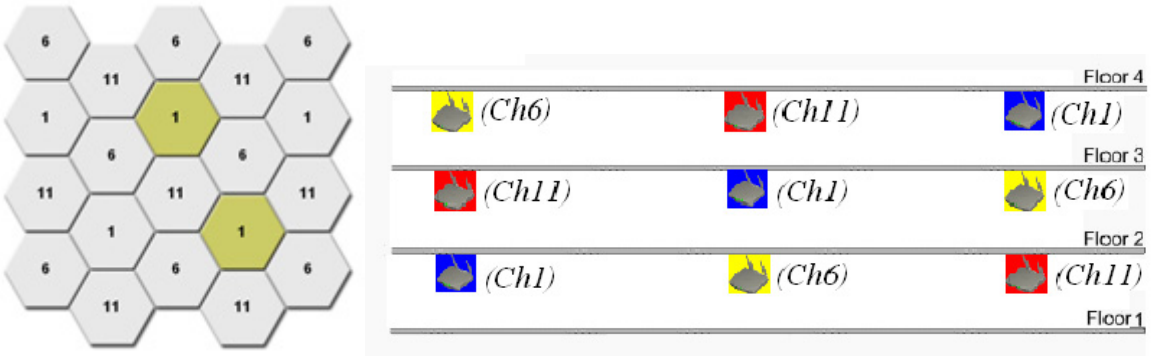
在实际的安装部署中，为了保证信号覆盖的质量，必须部署相应数量的 AP，就可能导致 AP 的覆盖范围出现重叠，AP 之间互相可见。如果所有的 AP 都工作在相同信道，这些 AP 只能共享一个信道的频率资源，造成整个 WLAN 网络性能较低。WLAN 协议本身提供了一些不重叠的物理信道，可以构建多个虚拟的独立的 WLAN 网络，各个网络独立使用一个信道的带宽，例如使用 2.4G 频段时，可以使用 1、6、11 三个非重叠信道构建 WLAN 网络。

同时信道规划调整需要考虑三维空间的信号覆盖情况，无论是水平方向还是垂直方向都要做到无线的蜂窝式覆盖，最大可能的避免同楼层和上下楼层间的同频干扰。

说明

- 802.11n 网络在实际部署时，无论是 2.4G 频段或 5G 频段，建议都采用 20MHz 模式进行覆盖，以加强信道隔离与复用，提升 WLAN 网络整体性能。
- 需要注意的是，我司 AP 在 5G 频段默认 802.11ac 射频模式的带宽为 80MHz，802.11an 射频模式的带宽为 40MHz。

图1-1 信道规划示意图



1.2.2 配置说明

【命令一】

channel *channel-number*

【参数】

channel-number：手动配置的射频工作信道。取值范围由国家码和射频模式决定。

【使用指导】

手工指定工作信道模式时，请不要使用雷达信道。

Radio 视图下配置的优先级高于 AP 组 Radio 视图下的配置。

【举例】

配置射频工作信道号为 149。（Radio 视图）

```
<Sysname> system-view
[Sysname] wlan ap ap1 model WA4320i-ACN
[Sysname-wlan-ap-ap1] radio 1
[Sysname-wlan-ap-ap1-radio-1] channel 149
```

配置射频工作信道号为 149。（AP 组 Radio 视图）

```
<Sysname> system-view
[Sysname] wlan ap-group apgroup1
[Sysname-wlan-ap-group-apgroup1] ap-model WA4320i-ACN
[Sysname-wlan-ap-group-apgroup1-ap-model-WA4320i-ACN] radio 1
[Sysname-wlan-ap-group-apgroup1-ap-model-WA4320i-ACN-radio-1] channel 149
```

【命令二】

channel band-width { **20** | **40** [**auto-switch**] | **80** | { **160** | **dual-80** } [**secondary-channel** *channel-number*] }

【参数】

20：将带宽模式设置成 20MHz。

40：将带宽模式设置成 40MHz。

80：将带宽模式设置成 80MHz。

auto-switch：允许在 20MHz 和 40MHz 之间自动切换。仅当 Radio 模式为 dot11gn 和 dot11gac 模式时，支持配置本参数。

160：将带宽模式设置成 160MHz。本参数的支持情况与 AP 的型号有关，请以设备的实际情况为准。

dual-80：将带宽模式设置成（80+80）MHz。本参数的支持情况与 AP 的型号有关，请以设备的实际情况为准。

secondary-channel *channel-number*：手工配置 160/(80+80)MHz 带宽模式下的辅信道。本参数的支持情况与 AP 的型号有关，请以设备的实际情况为准。

【使用指导】

该命令仅对 802.11n、802.11ac 和 802.11gac 类型的 Radio 有效。当 Radio 模式切换时，带宽恢复切换模式下的缺省值。

- 在指定带宽为 40MHz 情况下，如果找到两条可以绑定到一起的相邻信道，那么使用 40MHz 带宽；如果找不到可以绑定的相邻信道，那么实际只能使用 20MHz 带宽。
- 在指定带宽为 80MHz 情况下，如果找到一组可以绑定为 80MHz 的相邻信道，那么使用 80MHz 带宽；如果找不到可以绑定为 80MHz 的一组信道，但可以找到两条可以绑定为 40MHz 带宽的信道，那么使用 40MHz 带宽；如果找不到可以绑定的信道，那么实际只能使用 20MHz 带宽。
- 在指定带宽为 160MHz 情况下，如果找到一组可以绑定为 160MHz 的相邻信道，那么使用 160MHz 带宽；如果找不到可以绑定为 160MHz 的一组信道，但可以找到一组绑定为 80MHz 的相邻信道，那么使用 80MHz 带宽；如果找不到可以绑定为 80MHz 的一组信道，但可以找到一组绑定为 40MHz 带宽的信道，那么使用 40MHz 带宽；如果找不到可以绑定的信道，那么实际只能使用 20MHz 带宽。
- 在指定带宽为（80+80）MHz 情况下，如果找到一组可以绑定为 160MHz 的相邻信道，那么使用 160MHz 带宽；如果找不到可以绑定为 160MHz 的一组信道，但可以找到两组虽不相邻，但每组都可以绑定为 80MHz 的相邻信道，那么使用（80+80）MHz 带宽；如果找不到可以绑定为（80+80）MHz 的一组信道，但可以找到一组绑定为 80MHz 的相邻信道，那么使用 80MHz 带宽；如果找不到可以绑定为 80MHz 的一组信道，但可以找到一组绑定为 40MHz 带宽的信道，那么使用 40MHz 带宽；如果找不到可以绑定的信道，那么实际只能使用 20MHz 带宽。

根据协议规定，射频实际工作频宽一分为二，其中第一个频宽所处位置由主信道决定，第二个频宽所处位置由辅信道决定。主信道发送数据帧和所有的控制、管理帧；辅信道与主信道捆绑，仅发送数据帧。当使用 **channel** 命令配置了主信道，且射频的实际工作频宽为 160/(80+80)MHz 时，可使用 **secondary-channel** 参数指定第二个 80M 频宽的位置。其他情况下辅信道均由系统自动选择。

Radio 视图下配置的优先级高于 AP 组 Radio 视图下的配置。

如果带宽配置继承 AP 组，则辅信道也继承 AP 组，反之辅信道也不继承 AP 组。

【举例】

配置 Radio 1 的带宽为 40MHz。（Radio 视图）

```
<Sysname> system-view
[Sysname] wlan ap ap1 model WA4320i-ACN
[Sysname-wlan-ap-ap1] radio 1
[Sysname-wlan-ap-ap1-radio-1] type dot11an
[Sysname-wlan-ap-ap1-radio-1] channel band-width 40
```

配置 Radio 1 的带宽为 40MHz。（AP 组 Radio 视图）

```
<Sysname> system-view
[Sysname] wlan ap-group apgroup1
[Sysname-wlan-ap-group-apgroup1] ap-model WA4320i-ACN
[Sysname-wlan-ap-group-apgroup1-ap-model-WA4320i-ACN] radio 1
[Sysname-wlan-ap-group-apgroup1-ap-model-WA4320i-ACN-radio-1] type dot11an
[Sysname-wlan-ap-group-apgroup1-ap-model-WA4320i-ACN-radio-1] channel band-width 40
```

1.3 （必选）功率规划和设置固定功率

1.3.1 应用说明

信道规划完成后，虚拟 WLAN 网络的构建就已经同步完成了。此时需要关注每个虚拟 WLAN 网络中的 AP 发射功率，通过调整同一信道的 AP 的发射功率，降低这些 AP 之间的可见度，加强相同信道频谱资源的复用，以提高 WLAN 网络的整体性能。

1.3.2 配置说明

【命令】

max-power *radio-power*

【参数】

radio-power：射频的最大传输功率，其取值范围由国家码、信道、AP 型号、射频模式、天线类型、带宽等属性决定。

【使用指导】

射频的最大传输功率只能在射频支持的功率范围内进行选取，即保证射频的最大传输功率在合法范围内。射频支持的功率范围由国家码、信道、AP 型号、射频模式、天线类型、带宽等属性决定，修改上述属性，射频支持的功率范围和最大传输功率将自动调整为合法值。

如果开启了射频的功率锁定功能，则 AC 会将射频最大传输功率修改为射频当前传输功率。

Radio 视图下配置的优先级高于 AP 组 Radio 视图下的配置。

【举例】

配置射频最大传输功率为 15dBm。（Radio 视图）

```
<Sysname> system-view
[Sysname] wlan ap ap1 model WA4320i-ACN
```

```
[Sysname-wlan-ap-ap1] radio 1
[Sysname-wlan-ap-ap1-radio-1] max-power 15
```

配置射频最大传输功率为 15dBm。（AP 组 Radio 视图）

```
<Sysname> system-view
[Sysname] wlan ap-group apgroup1
[Sysname-wlan-ap-group-apgroup1] ap-model WA4320i-ACN
[Sysname-wlan-ap-group-apgroup1-ap-model-WA4320i-ACN] radio 1
[Sysname-wlan-ap-group-apgroup1-ap-model-WA4320i-ACN-radio-1] max-power 15
```

说明

不建议开启动态功率调整功能。由于终端本身会实时关注周围 AP 信号强度，如果开启动态功率调整，可能会导致终端无端漫游，使用效果变差。

1.4 （必选）为无线业务构建独立的VLAN

1.4.1 应用说明

WLAN 无线网络理论上就是实现一个二层的接入网络，而这个二层网络通常直接连接到现有的有线网络中。

而在无线网络中，广播/组播报文会使用最低速率发送广播报文，所以当广播报文比较多时，会相对较多地消耗信道空口资源，从而影响到整个无线网络性能和应用。一个广播报文通常会向 VLAN 内的所有 AP 发送，同时消耗所有 AP 的资源。所以在构建 WLAN 网络时，在条件允许的情况下，一定要为无线业务创建独立的 VLAN，不要和有线网络使用相同的 VLAN，这样即可以避免大量的广播/组播报文对无线网络的影响，又可以避免不必要的攻击。

此外，AC 有线口只放通必要的 VLAN，在本地转发情况下，不要放通无线业务 VLAN。

1.4.2 部署建议

在规划 WLAN 网络时，建议分配有线网络未使用的 VLAN 给 WLAN 接入业务使用。可以通过无线服务模板对应的接口配置对应的 VLAN，也可以在为 AP 绑定无线服务模板时指定 VLAN，还可以在无线客户端接入的时候下发授权 VLAN，具体配置请参考《H3C 无线控制器产品 配置指导》的“WLAN 接入配置指导”。

为了使网络规划更清晰，WLAN 网络仅作为一个新增的接入网络，所有的流量和接入都可以通过现有的有线网络设备进行监管和控制。可以将 WLAN 网络的构建、无线客户端接入管理等功能放在无线控制器上，而将业务 VLAN 的网关统一放在有线网络设备上，相当于在一个现有的有线网络设备上增加了一个独立的无线二层网络。

说明

由于无线控制器主要用于提供无线接入服务的功能，所以对于大型的综合型网络，建议业务 VLAN 的网关设置在无线控制器以外的设备上。

1.5 （必选）无线用户VLAN内二层隔离

1.5.1 应用说明

同一 VLAN 内，来自无线客户端的广播、组播报文会向所有放通该 VLAN 的 AP 上广播，而在空间介质中广播报文通常使用最低速率进行发送，因此当广播报文比较多时，会占用较多的空口资源，在一定程度上影响到整个网络性能。

无线用户 VLAN 内二层隔离可以在 AC 上控制无线用户只能访问网关设备，而不能互相之间访问。同时，通过配置 **undo user-isolation permit broadcast** 命令禁止有线用户（**user-isolation vlan permit-mac** 允许的 MAC 地址除外）发送广播、组播报文给无线用户，无线用户到有线用户的广播、组播报文不受限制。这样可以大量减少整个 WLAN 网络的广播流量，提高 WLAN 网络的整体性能。

1.5.2 配置说明

【命令一】

user-isolation vlan *vlan-list* **enable** [**permit-unicast**]

【参数】

vlan-list：VLAN 列表，表示开启用户隔离功能的 VLAN 的范围。表示方式为 *vlan-list* = { *vlan-id1* [**to** *vlan-id2*] }&<1-10>，*vlan-id* 的取值范围为 1～4094，*vlan-id2* 的值要大于或等于 vlan-id1 的值，&<1-10>表示前面的参数最多可以输入 10 次。

permit-unicast：表示不隔离单播，仅隔离广播和组播。如果未指定该参数，表示同时隔离单播、广播和组播。

【使用指导】

为了避免在指定 VLAN 上开启用户隔离功能后，出现断网情况，用户必须根据 **user-isolation vlan permit-mac** 命令先将用户网关的 MAC 地址加入到用户隔离允许列表中，再开启该 VLAN 的用户隔离功能。

如果多次执行 **user-isolation vlan enable** 命令，则开启用户隔离功能的 VLAN 是多次配置中指定的 VLAN 的合集；若同一 VLAN 多次配置，则最后一条配置生效。

【举例】

在 VLAN 1 上开启用户隔离功能。

```
<Sysname> system-view
[Sysname] user-isolation vlan 1 enable
```

【命令二】

user-isolation vlan *vlan-list* **permit-mac** *mac-list*

【参数】

vlan-list：VLAN 列表。表示方式为 *vlan-list* = { *vlan-id1* [**to** *vlan-id2*] }&<1-10>，*vlan-id* 的取值范围为 1～4094，*vlan-id2* 的值要大于或等于 *vlan-id1* 的值，&<1-10>表示前面的参数最多可以输入 10 次。

mac-list：MAC 地址允许转发列表，MAC 地址格式为 H-H-H。在一个 VLAN 内最多可以配置 64 个允许的 MAC 地址，该 MAC 地址不允许为广播或组播地址。

【使用指导】

配置指定 VLAN 的 MAC 地址允许转发列表，当在该 VLAN 内开启用户隔离功能后，所配置的 MAC 地址不会被隔离。

如果多次执行 **user-isolation vlan permit-mac** 命令，则指定 VLAN 允许的 MAC 地址为多次配置的 MAC 地址的集合。每一个 VLAN 内最多允许配置 64 个允许的 MAC 地址，一次最多允许配置 16 个允许的 MAC 地址。

【举例】

配置 VLAN 1 所允许 MAC 地址为 00bb-ccdd-eeff 和 0022-3344-5566。

```
<Sysname> system-view
[Sysname] user-isolation vlan 1 permit-mac 00bb-ccdd-eeff 0022-3344-5566
```

【命令三】

user-isolation permit-broadcast

undo user-isolation permit-broadcast

【使用指导】

当有线用户和无线用户属于同一 VLAN 或用户接入的 AC 设备工作于 IRF 环境时必须隔离有线用户发往无线用户的广播和组播报文，其他情况下允许接收有线用户发送给无线用户的广播和组播报文。

在本地转发组网下实施二层隔离需要通过 MAP 文件把相关配置下发到 AP 上。

【举例】

在 VLAN 10 上开启用户隔离功能，允许访问 MAC 地址为 00bb-ccdd-eeff 和 0022-3344-5566 的设备（允许的 MAC 地址通常为网关 MAC 地址），同时禁止有线用户（permit-mac 允许的 mac 地址除外）发送广播、组播报文给无线用户。

```
<AC> system-view
[AC] user-isolation vlan 10 enable
[AC] user-isolation vlan 10 permit-mac 00bb-ccdd-eeff 0022-3344-5566
[AC] undo user-isolation permit-broadcast
```

1.6 （强烈推荐）Vlan-group分配模式配置为静态

1.6.1 应用说明

无线 AC 可以通过使用 VLAN 组特性，将其 VLAN 成员分配给上线的各客户端，使各客户端均匀分布在各 VLAN，从而达到减小广播域的目的，同时还可以提高对非连续地址段的利用率。AC 默认 VLAN 组的 VLAN 分配方式为动态，即客户端首次上线时，无线服务模板绑定 Radio 时指定的 VLAN 组会为用户随机分配一个 VLAN。客户端再次上线时 VLAN 组再次随机为客户端分配 VLAN。采用该分配方式，客户端会被均衡地分配在 VLAN 组的所有 VLAN 中。对于终端而言，连接 SSID 不变的情况下，部分终端会出现地址更新慢，甚至不更新地址的情况，最终导致用户体验变差，因此当使用 VLAN 组特性时，如无特殊需求，强烈建议配置为静态分配方式，即终端再次上线时直接继承上次 VLAN 组分配的 VLAN。

1.6.2 配置说明

【命令】

client vlan-alloc { **dynamic** | **static** | **static-compatible** }

【参数】

dynamic：表示动态分配方式

static：表示静态分配方式

static-compatible：表示静态兼容分配方式。

【使用指导】

客户端首次上线时，AP 会为动态分配方式下的客户端随机分配无线服务模板绑定 Radio 时指定的 VLAN 组内的一个 VLAN，根据客户端的 MAC 地址为静态分配、静态兼容分配方式下的客户端分配 VLAN。客户端再次上线时被分配的 VLAN 将由配置的 VLAN 分配方式决定：

- 静态分配方式下，直接继承上次 VLAN 组分配的 VLAN。若客户端的 IP 地址在租约内，仍为客户端分配同一个 IP 地址。采用该分配方式，可以减少 IP 地址的消耗。
- 动态分配方式下，VLAN 组再次随机为客户端分配 VLAN。采用该分配方式，客户端会被均衡地分配在 VLAN 组的所有 VLAN 中。
- 静态兼容分配方式下，可以保证客户端在采用静态分配方式的 Comware V5 版本 AC 设备与 ComwareV7 版本的 AC 之间漫游时，被分配相同的 VLAN。

【举例】

配置客户端的 VLAN 分配方式为静态分配方式。

```
[AC] wlan service-template service1
[AC-wlan-st-service1] client vlan-alloc static
```

说明

- 不使用 VLAN 组特性时无需配置 VLAN 分配方式。
- 如果涉及 Comware V5、Comware V7 混合组网和漫游时，且均启用了 VLAN 组特性（V5 该功能为 VLAN 池），建议配置 VLAN 分配模式为 static-compatible。

1.7 （强烈推荐）禁止低速率

1.7.1 应用说明

在 WLAN 网络中，无线终端或 AP 通常是使用一个速率集发送空口报文（例如 802.11g 支持 1、2、5.5、11、6、9、12、18、24、36、48、54Mbps），实际无线终端或者 AP 在发送报文的时候会动态的在这些速率中选择一个速率进行发送。通常提到的 802.11g 可以达到速率主要指所有报文都采用 54M 速率进行发送的情况，而且是指的一个空口信道的能力。而实际上大量的广播报文和无线的管理报文都使用最低速率 1Mbps 进行发送，所以会消耗一定的空口资源。在无线网络中，不考虑信号传输距离的情况下，可以将 1、2、6 和 9Mbps 这类低速率禁用，这样可以整体上减少广播报文和管理报文对空口资源的占用。

对于信号强度比较弱的终端，或者距离比较远的终端，关闭低速率应用后可能会出现丢包现象。但是正常的室内覆盖，信号强度可以保证，所以要求在室内覆盖情况下关闭 WLAN 低速率。

1.7.2 配置说明

【命令】

rate disabled *rate-value*

【参数】

disabled：禁用速率。AP 禁用的速率。

rate-value：速率值，单位为 Mbps。可配置多个速率，用空格分隔。

- 802.11a/802.11an/802.11ac：可以取值 6、9、12、18、24、36、48、54。
- 802.11b：可以取值 1、2、5.5、11。
- 802.11g/802.1gn/802.11gac：可以取值 1、2、5.5、6、9、11、12、18、24、36、48、54。

【使用指导】

Radio 视图下配置的优先级高于 AP 组 Radio 视图下的配置。

【举例】

配置 802.11g 模式的禁用速率：1、2、5.5、6、9Mbps。（Radio 视图）

```
<Sysname> system-view
[AC] wlan ap test model WA4320i-ACN
[AC-wlan-ap-test] radio 2
[AC-wlan-ap-test-radio-2] rate disabled 1 2 5.5 6 9
```

配置 802.11g 模式的禁用速率：1、2、5.5、6、9Mbps。（AP 组 Radio 视图）

```
<Sysname> system-view
[AC] wlan ap-group test-group
[AC-wlan-ap-group-test-group] ap-model WA2620-AGN
[AC-wlan-ap-group-test-group-ap-model-WA2620-AGN] radio 2
[AC-wlan-ap-group-test-group-ap-model-WA2620-AGN-radio-2] rate disabled 1 2 5.5 6 9
```

1.8 （强烈推荐）开启无线用户限速

1.8.1 应用说明

WLAN 网络中每个 AP 提供的可用带宽是有限的，且由接入的无线客户端共享。如果个别的无线客户端通过 WLAN 使用网络工具下载文件，可能达到非常大的流量，进而直接耗尽当前共享带宽，造成其他无线客户端访问网络慢、Ping 抖动丢包等问题。通过配置用户限速功能，可以限制部分无线客户端对带宽的过多消耗，保证所有接入无线客户端均能正常使用网络业务。

基于无线客户端的速率限制功能有两种模式：动态模式和静态模式，其中静态模式为静态的配置每个客户端的速率，即配置的速率是同一个 AP 内，每个客户端的最大速率。

1.8.2 配置说明

【命令】

client-rate-limit { **inbound** | **outbound** } **mode** { **dynamic** | **static** } **cir** *cir*

【参数】

inbound：入方向，即限制客户端发送数据的速率。

outbound：出方向，即限制客户端接收数据的速率。

dynamic：配置限速模式为动态模式。在该模式下，单个客户端的限速速率为总限速速率/客户端总数。

static：配置限速模式为静态模式，所有客户端的限速速率为固定值。

cir *cir*：配置客户端限速速率。在静态模式下表示为所有客户端配置相同的限速速率；在动态模式下表示配置所有客户端的限速速率总和。*cir* 的取值范围为 16～1700000，单位为 Kbps。

【使用指导】

在同一视图下，开启了基于射频的客户端限速功能且配置了客户端速率限制，则该视图的客户端限速功能生效。

可以同时指定出方向和入方向的速率限制。

Radio 视图下客户端限速功能生效的优先级高于 AP 组 Radio 视图。

【举例】

配置客户端限速功能，使单个客户端发送数据的最大速率为 512Kbps，单个客户端接收数据的最大速率为 2048Kbps。（Radio 视图）

```
<AC> system-view
[AC] wlan ap ap1 model WA4320i-ACN
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-1] client-rate-limit enable
[AC-wlan-ap-ap1-1] client-rate-limit inbound mode static cir 512
[AC-wlan-ap-ap1-1] client-rate-limit outbound mode static cir 2048
```

配置客户端限速功能，使单个客户端发送数据的最大速率为 512Kbps，单个客户端接收数据的最大速率为 2048Kbps。（AP 组 Radio 视图）

```
<AC> system-view
[AC] wlan ap-group group1
[AC-wlan-ap-group-group1] ap-model WA4320i-ACN
[AC-wlan-ap-group-group1-ap-model-WA4320i-ACN] radio 1
[AC-wlan-ap-group-group1-ap-model-WA4320i-ACN-radio-1] client-rate-limit enable
[AC-wlan-ap-group-group1-ap-model-WA4320i-ACN-radio-1]client-rate-limit inbound mode
static cir 512
[AC-wlan-ap-group-group1-ap-model-WA4320i-ACN-radio-1]client-rate-limit outbound mode
static cir 2048
```

说明

用户限速功能与智能带宽保障功能不要同时启用。

1.9 （强烈推荐）无线终结单元下行有线口配置端口隔离

1.9.1 应用说明

无线终结者组网方案下，无线终结单元可能由于下行口之间连接网线造成广播风暴、私设路由器导致出现 DHCP 分配问题，影响用户体验。因此，需要在无线终结单元下行有线各端口间配置二层隔离，可以将不同的端口加入不同的 VLAN，但 VLAN 资源有限，因此建议采用端口隔离特性。用户只需要将端口加入到隔离组中，就可以实现隔离组内端口之间二层隔离，而不关心这些端口所属 VLAN，从而节省 VLAN 资源。无线终结单元的配置可以通过 map 文件下发或者远程到无线终结者上完成。

1.9.2 配置说明

【命令一】

slot *slot-number*

【参数】

slot-number：表示无线终结单元所在的槽位号。

【使用指导】

进入 slot 视图后，可以开启该 slot 的预配置功能。

【举例】

进入指定 slot 视图。

```
<WT1020> system-view
[WT1020] slot 2
[WT1020-slot-2]
```

【命令二】

provision model *model*

【参数】

model：表示设备支持的无线终结单元的类型。

【举例】

开启指定 slot 的预配置功能。

```
<WT1020> system-view
[WT1020] slot 2
[WT1020-slot-2] provision model WTU420H
```

【命令三】

port-isolate group *group-id*

【参数】

group-id：隔离组编号。

【举例】

创建隔离组 1。

```
<WT1020> system-view
[WT1020] port-isolate group 1
```

【命令四】

port-isolate enable group *group-id*

【参数】

group *group-id*：将端口加入到隔离组中的编号。

【举例】

进入无线终结者 WT1020 的 2 号槽位子卡 slot 视图进行预配置，将 slot2 下连接的 WTU420H 的下行口 1/2/1~1/2/4 加入端口隔离组 1（可通过 map 针对所有子卡进行下发）。

```
<WT1020> system-view
[WT1020] port-isolate group 1
[WT1020] slot 2
[WT1020-slot-2] provision model WTU420H
[WT1020-slot-2] quit
[WT1020] interface Ethernet 1/2/1
[WT1020-Ethernet1/2/1] port-isolate enable group 1
[WT1020] interface Ethernet 1/2/2
[WT1020-Ethernet1/2/1] port-isolate enable group 1
[WT1020] interface Ethernet 1/2/3
[WT1020-Ethernet1/2/1] port-isolate enable group 1
[WT1020] interface Ethernet 1/2/4
[WT1020-Ethernet1/2/1] port-isolate enable group 1
```

说明

只有创建 slot x，并预配置 **provision model** 后才能进入接口配置。

1.10 （强烈推荐）Portal配置用户闲置切断功能

1.10.1 应用说明

当 AC 作为接入设备，承载 Portal 认证业务时，如果服务器侧没有设置用户的闲置切断功能，会导致终端下线后，用户认证表项长期在设备上存在，如果此时终端重新接入，并获取到了新的 IP 地址，就有可能出现冲突，导致无法认证通过，此外大量的残留表项还会消耗设备的资源，因此无特殊需求的情况下，强烈建议开启设备上用户的闲置切断功能。

1.10.2 配置说明

【命令】

authorization-attribute idle-cut *minutes* [*flow*]

【参数】

minutes：指定用户的闲置切断时间。其中，*minutes* 的取值范围为 1～600，单位为分钟。

flow：用户在闲置切断时间内产生的数据流量，取值范围 1～10240000，单位为字节，缺省值为 10240。

【举例】

指定 ISP 域 test 下的用户闲置切断时间为 30 分钟，闲置切断时间内产生的流量为 10240 字节。

```
<AC> system-view
[AC] domain test
[AC-isp-test] authorization-attribute idle-cut 30 10240
```

1.11 （推荐）禁止AP回复广播Probe request

1.11.1 应用说明

WLAN 有两种探测机制：一种为无线终端被动的侦听 Beacon 帧之后，根据获取的无线网络情况，选择 AP 建立连接；另外一种为无线终端主动发送 Probe request 帧探测周围的无线网络，然后根据获取的 Probe Response 帧获取周围的无线网络信息，之后选择 AP 建立连接。

本功能主要针对 Probe 探测方式。

根据 Probe Request 帧（探测请求帧）是否携带 SSID，可以将主动扫描分为两种：

- 广播方式的 Probe 探测，客户端发送 Probe Request 帧（Probe Request 中 SSID 为空，也就是 SSID IE 的长度为 0）；
- 单播方式的 Probe 探测，客户端发送 Probe Request 帧（携带指定的 SSID）。

而大部分的无线终端都不会指定要连接的 SSID，这样就造成了无线终端会发送大量广播 Probe Request 探测，造成所有接收到该帧的 AP 设备都会回应 Probe Response 帧，而这些帧都使用低速率进行发送，会消耗一定的空口资源，因此，可以考虑关闭广播 Probe 探测功能，使 AP 针对 SSID 为空的探测请求不进行回复，有效降低空口的消耗，使整个 WLAN 网络性能得到一定的提升。

1.11.2 配置说明

【命令】

broadcast-probe reply disable

【使用指导】

广播 Probe request 报文即报文中不携带服务的 SSID，AP 收到广播报文后，将 AP 提供的所有服务的信息封装在 Probe response 报文中，回应给客户端。

配置禁止 AP 回复客户端的广播 Probe request 报文，可以减少 AP 回复的 Probe response 报文。

AP 视图下配置的优先级高于 AP 组视图下的配置。

【举例】

在 ap1 上开启禁止 AP 回应广播 Probe request 报文功能。（AP 视图）

```
<AC> system-view
[AC] wlan ap ap1 model WA4320i-ACN
[AC-wlan-ap-ap1] broadcast-probe reply disable
```

在 AP 组上开启禁止 AP 回应广播 Probe request 报文功能。（AP 组视图）

```
<AC> system-view
[AC] wlan ap-group group1
```

```
[AC-wlan-ap-group-group1] broadcast-probe reply disable
```

1.12 （推荐）加密方式设置

1.12.1 应用说明

在 WLAN 网络中，空口设置明文不加密，可以减少因加密带来的密钥协商时间开销，获取最大的无线空口性能。在 11n 网络中，如果因安全因素考虑必须设置加密，建议加密方式设置为 RSN+CCMP，不推荐使用 TKIP 或者 WEP 加密方式，这两种加密方式无法发挥 11n 网络的高带宽性能。

1.12.2 配置说明

【命令一】

akm mode { **dot1x** | **private-psk** | **psk** | **anonymous-dot1x** }

【参数】

dot1x：表示身份认证与密钥管理的模式是 802.1X 模式。

private-psk：表示身份认证与密钥管理的模式是 Private-PSK 模式。

psk：表示身份认证与密钥管理的模式是 PSK 模式。

anonymous-dot1x：表示身份认证与密钥管理的模式是 Wi-Fi 联盟匿名 802.1X 模式。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置，并且只能配置一种模式。

当 WLAN 网络采用 RSNA 安全机制时，必须配置身份认证与密钥管理。若配置了身份认证与密钥管理模式为 Wi-Fi 联盟匿名 802.1X 模式，则安全 IE 只能配置为 OSEN IE。

每一种身份认证模式都有互相依赖的用户认证方式：

- 802.1X 模式和 802.1X 用户认证模式相互依赖，必须同时配置。
- Private-PSK 模式和 MAC 地址认证模式相互依赖，必须同时配置。
- PSK 模式和 MAC 地址认证模式或 Bypass 用户认证模式相互依赖，必须同时配置。
- Wi-Fi 联盟匿名 802.1X 模式和 802.1X 用户认证模式相互依赖，必须同时配置。

【举例】

配置身份认证与密钥管理模式为 PSK 模式。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] akm mode psk
```

【命令二】

security-ie { **osen** | **rsn** | **wpa** }

【参数】

osen：设置在 AP 发送信标和探查响应帧时携带 OSEN IE。OSEN IE 通告了 AP 的 OSEN 能力。

rsn：设置在 AP 发送信标和探查响应帧时携带 RSN IE。RSN IE 通告了 AP 的 RSN 能力。

wpa：设置在 AP 发送信标和探查响应帧时携带 WPA IE。WPA IE 通告了 AP 的 WPA 能力。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置，并且必须要配置 CCMP 或 TKIP 加密套件。

当 WLAN 网络采用 RSNA 安全机制时，必须配置安全 IE。

若配置了安全 IE 为 OSEN IE，则只能配置认证密钥管理模式为 Wi-Fi 联盟匿名 802.1X 模式。

【举例】

配置信标帧和探查响应帧携带 RSN 信息元素。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] security-ie rsn
```

【命令三】

cipher-suite { **ccmp** | **tkip** | **wep40** | **wep104** | **wep128** }

【参数】

ccmp：AES-CCMP 加密套件。

tkip：TKIP 加密套件。

wep40：WEP40 加密套件。

wep104：WEP104 加密套件。

wep128：WEP128 加密套件。

【使用指导】

本命令只能在无线服务模板处于关闭状态时配置。

如果配置了安全 IE，则必须配置 TKIP 或者 CCMP 加密套件中的一种。当 WLAN 网络采用 RSNA 安全机制时，必须配置加密套件。

WEP 加密套件只能配置 WEP40/WEP104/WEP128 其中的一种，且需要配置与加密套件种类相对应的 WEP 密钥及 WEP 密钥 ID。

WEP128 和 CCMP 或 TKIP 不能同时配置。

【举例】

配置在帧加密时使用 TKIP 加密套件。

```
<Sysname> system-view
[Sysname] wlan service-template security
[Sysname-wlan-st-security] cipher-suite tkip
```

1.13 （推荐）禁止弱信号客户端接入

1.13.1 应用说明

在 WLAN 网络中，信号强度较弱的无线客户端，虽然也可以接入到网络中，但是所能够获取的网络性能和服务质量要比信号强度较强的无线客户端差很多。如果弱信号的无线客户端在接入到 WLAN 网络的同时还在大量地下载数据，就会占用较多的信道资源，最终必然对其他的无线客户端造成很大的影响。

禁止弱信号客户端接入功能，通过配置允许接入的无线客户端的最小信号强度门限值，可以直接拒绝信号强度低于指定门限的无线客户端接入到 WLAN 网络中，减少弱信号客户端对其他无线客户端的影响，从而提升整个 WLAN 网络的性能。

1.13.2 配置说明

【命令】

option client reject { **disable** | **enable** [**rssi** *rssi-value*] }

【参数】

rssi *rssi-value*：无线客户端信号强度门限值，取值范围为 5～100，缺省值为 10，建议值为 10。

【使用指导】

开启本功能后，当无线客户端信号强度低于门限值时，AP 将拒绝此类客户端接入。拒绝信号比较低的无线客户端接入到 WLAN 网络中，既可以避免低信号客户端占用较多的信道资源，同时可以减少对其他客户端的影响，提升整个 WLAN 网络的应用效果。

禁止弱信号客户端接入需要考虑场景覆盖信号强度情况，如场景覆盖信号强度偏弱，可能导致无线客户端无法正常接入。

【举例】

开启禁止弱信号客户端接入功能，并配置信号强度门限值为 10。（Radio 视图）

```
<AC> system-view
[AC] wlan ap ap1 model WA4320i-ACN
[AC-wlan-ap-ap1] radio 1
[AC-wlan-ap-ap1-radio-1] option client reject enable rssi 10
```

开启禁止弱信号客户端接入功能，并配置信号强度门限值为 10。（AP 组 Radio 视图）

```
<AC> system-view
[AC] wlan ap-group 1
[AC-wlan-ap-group-1] ap-model WA4320i-ACN
[AC-wlan-ap-group-1-ap-model-WA4320i-ACN] radio 1
[AC-wlan-ap-group-1-ap-model-WA4320i-ACN-radio-1] option client reject enable rssi 10
```

1.14 （必选）AC有线口只放通必要的VLAN

非业务广播报文进入 AC 会复制到所有 AP 空口，从而影响 AP 性能，甚至对 AC 造成冲击。为了防止不必要报文进入 AC，建议 AC 有线口以及对端互联的交换机端口只放通必要的 VLAN，禁止配置 **permit vlan all**。当组网为本地转发时，无线业务报文不经过 AC，所以 AC 有线口不需要放通本地转发业务 VLAN，防止报文迂回到 AC 影响性能。

1.15 （必选）AC-AP有线链路质量稳定

CAPWAP 隧道通过中间的有线链路承载，要求 AP 和 AC 之间 Ping 大于 1500 字节的数据包丢包率小于 1%，平均延迟小于 50ms。

1.16 （必选）IRF链路采用独立VLAN

1.16.1 应用说明

当 AC 通过二层交换机建立 IRF 时，要求 IRF 链路使用的 VLAN 独立于业务 VLAN。建议在交换机上将与 AC 的 IRF 堆叠口连接的端口配置为 Access 口，VLAN 独立规划。本优化不需要 AC 做配置调整。

1.16.2 配置说明

【命令一】

vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

【参数】

vlan-id1：VLAN 的编号，取值范围为 1～4094。

vlan-id1 **to** *vlan-id2*：指定 VLAN 的编号范围。*vlan-id1* 和 *vlan-id2* 为 VLAN 的编号，取值范围为 1～4094。*vlan-id2* 的值要大于或等于 *vlan-id1* 的值。

all：当设备允许创建的最大 VLAN 数小于 4094 时，不支持该参数。

【使用指导】

用户不能创建和删除缺省 VLAN（VLAN 1）

动态学习到的 VLAN，以及被其他应用锁定不让删除的 VLAN，都不能使用 **undo vlan** 命令直接删除。只有将相关配置删除之后，才能删除相应的 VLAN。

【举例】

创建 VLAN 2，并进入该 VLAN 视图。

```
<Sysname> system-view
[Sysname] vlan 2
```

【命令二】

port *interface-list*

【参数】

interface-list：以太网接口列表。表示方式为 *interface-list* = { *interface-type interface-number1* [**to** *interface-type interface-number2*] }&<1-10>，其中 *interface-type interface-number* 为端口类型和端口编号，*interface-number2* 的值要大于或等于 *interface-number1* 的值，&<1-10>表示前面的参数最多可以输入 10 次。

【使用指导】

通过本命令只能将 Access 端口加入到 VLAN 中，不能将 Trunk 和 Hybrid 端口加入到 VLAN 中。

设备上的所有端口的缺省链路类型都是 Access 类型，但用户可以自行切换端口类型，具体配置可参考命令 **port link-type**。

【举例】

向 VLAN2 中添加端口 GigabitEthernet1/0/1～GigabitEthernet1/0/2。

```
<Sysname> system-view
[Sysname] vlan 2
```

```
[Sysname-vlan2] port gigabitethernet 1/0/1 to gigabitethernet 1/0/2
```

1.17 （必选）IRF端口绑定多链路时采用静态聚合

1.17.1 应用说明

当 AC 通过二层交换机建立 IRF 时，IRF 堆叠口绑定了多个物理口，此时需要将交换机与 IRF 堆叠口连接的多个端口配置成静态聚合，不允许使用动态聚合。本优化不需要 AC 做配置调整。

1.17.2 配置说明

【命令一】

interface bridge-aggregation *interface-number*

【参数】

interface-number：指定二层聚合接口的编号。

【使用指导】

创建二层聚合接口后，系统将自动生成同编号的二层聚合组，且该聚合组缺省工作在静态聚合模式下。

删除二层聚合接口的同时会删除其对应的二层聚合组，如果该聚合组内有成员端口，那么这些成员端口将自动从该聚合组中退出。

【举例】

创建二层聚合接口 1，并进入二层聚合接口 1 的视图。

```
<Sysname> system-view
[Sysname] interface bridge-aggregation 1
```

【命令二】

port link-aggregation group *group-id*

【参数】

group-id：指定聚合组所对应聚合接口的编号。

【举例】

#创建二层聚合接口 2，并进入二层聚合接口 2 视图

```
[Switch] interface Bridge-Aggregation 2
```

#将 Switch 内联口 Ten-GigabitEthernet 1/2/0/1 加入到聚合组 2 中

```
[Switch] interface Ten-GigabitEthernet 1/2/0/1
[Switch-Ten-GigabitEthernet1/2/0/1] port link-aggregation group 2
```

1.18 （必选）IRF链路的对端交换机端口关闭STP功能

1.18.1 应用说明

当 AC 通过交换机建立 IRF 时，需要在交换机侧将与 IRF 堆叠口连接的端口关闭 STP 功能。同时，AC 上 IRF 堆叠物理口也需要关闭 STP 功能。

1.18.2 配置说明

【命令】

undo stp enable

【举例】

在端口 GigabitEthernet1/0/1 上关闭生成树协议。

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0/1
[Sysname-GigabitEthernet1/0/1] undo stp enable
```