目 录

1 无线配置

1.1 无线网络

1.1.1 无线接入

无线网络为用户提供 WLAN 接入服务。无线服务的骨干网通常使用有线电缆作为线路连接安置在固定网络，接入点设备安置在需要覆盖无线网络的区域，用户在该区域内就可以通过无线接入的方式接入无线网络。

1. 无线服务

无线服务即一类无线服务属性的集合，如无线网络的 SSID、认证方式（开放系统认证或者共享密钥认证）等。

2. SSID

SSID（Service Set Identifier，服务集标识符），就是无线网络的名称。

3. 隐藏SSID

AP 将 SSID 置于 Beacon 帧中向外广播发送。若 BSS（Basic Service Set，基本服务集）的客户端数量已达到上限或 BSS 一段时间内不可用即客户端不能上线，不希望其它客户端上线，则可以配置隐藏 SSID。若配置了隐藏 SSID，AP 不将 SSID 置于 Beacon 帧中，还可以借此保护网络免遭攻击。为了进一步保护无线网络，AP 对于广播 Probe Request 帧也不会回复。此时客户端若想连接此 BSS，则需要手工指定该 SSID，这时客户端会直接向该 AP 发送认证及关联报文连接该 BSS。

4. 数据转发

可以在 AC 上将客户端数据报文转发位置配置在 AC 或者 AP 上。

- 将数据报文转发位置配置在 AC 上时，为集中式转发，客户端的数据流量由 AP 通过 CAPWAP 隧道透传到 AC，由 AC 转发数据报文；
- 将数据报文转发位置配置在 AP 上时，为本地转发，客户端的数据流量直接由 AP 进行转发。将转发位置配置在 AP 上缓解了 AC 的数据转发压力；
- 将转发位置配置在 AP 上时，可以指定 VLAN，即只有处于指定 VLAN 的客户端，在 AP 上转发其数据流量。

5. 绑定无线服务

无线服务跟 AP 的 Radio 存在多对多的映射关系，将无线服务绑定在某个 AP 的射频上，AP 会根据射频上绑定的无线服务的属性创建 BSS。BSS 是无线服务提供服务的基本单元。在一个 BSS 的服务区域内（这个区域是指射频信号覆盖的范围），客户端能够通过同一个 SSID 访问网络。

绑定无线服务时，可以进行如下配置：

- 可以为该 BSS 指定一个 VLAN 组，该 BSS 下连接的客户端会被均衡地分配在 VLAN 组的所有 VLAN 中，既能将客户端划分在不同广播域中，又能充分利用不连续的地址段为客户端分配 IP 地址。
- 可以绑定 NAS-Port-ID 和 NAS-ID，用于网络服务提供者标识客户端的接入位置，区分流量来源。按照网络服务提供者的标准，不同的 NAS-Port-ID 对应不同的位置信息。

- 可以配置 SSID 隐藏。

1.1.2 链路层认证

最初 802.11 的安全机制被称为 Pre-RSNA 安全机制，它的认证机制不完善，容易被攻破，存在安全隐患，且在 WEP 加密机制中，由于连接同一 BSS 下的所有客户端都使用同一加密密钥和 AP 进行通信，一旦某个用户的密钥泄露，那么所有用户的数据都可能被窃听或篡改，所以 IEEE 制订了 802.11i 协议来加强无线网络的安全性。

但 802.11i 仅对无线网络的数据报文进行加密保护，而不对管理帧进行保护，所以管理帧的机密性、真实性、完整性无法保证，容易受到仿冒或监听，例如：恶意攻击者通过获取设备的 MAC 地址并仿冒设备恶意拒绝客户端认证或恶意结束设备与客户端的关联。802.11w 无线加密标准建立在 802.11i 框架上，通过保护无线网络的管理帧来解决上述问题，进一步增强无线网络的安全性。

1. Pre-RSNA安全机制

Pre-RSNA 安全机制采用开放式系统认证（Open system authentication）和共享密钥认证（Shared key authentication）两种认证方式来进行客户端认证，并且采用 WEP 加密方式对数据进行加密来保护数据机密性，以对抗窃听。WEP 加密使用 RC4 加密算法（一种流加密算法）实现数据报文的加密，WEP 加密支持 WEP40、WEP104 和 WEP128 三种密钥长度。

2. RSNA安全机制

802.11i 安全机制又被称为 RSNA（Robust Security Network Association，健壮安全网络连接）安全机制，包括 WPA（Wi-Fi Protected Access，Wi-Fi 保护访问）和 RSN（Robust Security Network，健壮安全网络）两种安全模式，采用 AKM（Authentication and Key Management，身份认证与密钥管理）对用户身份的合法性进行认证，对密钥的生成、更新进行动态管理，并且采用 TKIP（Temporal Key Integrity Protocol，临时密钥完整性协议）和 CCMP（Counter mode with CBC-MAC Protocol，[计数器模式]搭配[区块密码锁链－信息真实性检查码]协议）加密机制对报文进行加密。

AKM 分为 802.1X、Private-PSK 和 PSK 和三种模式：

- 802.1X：采用 802.1X 认证对用户进行身份认证，并在认证过程中生成 PMK（Pairwise Master Key，成对主密钥），客户端和 AP 使用该 PMK 生成 PTK（Pairwise Transient Key，成对临时密钥）。
- Private-PSK：采用 PSK（Pre-Shared Key，预共享密钥）认证进行身份认证，使用客户端的 MAC 地址作为 PSK 密钥生成 PMK，客户端和 AP 使用该 PMK 生成 PTK。
- PSK：采用 PSK 认证进行身份认证，并通过 PSK 密钥生成 PMK，客户端和 AP 使用该 PMK 生成 PTK。

(1) 密钥种类

802.11i 协议中密钥主要包括 PTK 和 GTK（Group Temporal Key，群组临时密钥）两种：

- PTK 用于保护单播数据。
- GTK 用于保护组播和广播数据。

(2) WPA 安全模式密钥协商

WPA 是一种比 WEP 加密性能更强的安全机制。在 802.11i 协议完善前，采用 WPA 为用户提供一个临时性的 WLAN 安全增强解决方案。在 WPA 安全网络中，客户端和 AP 通过使用 EAPOL-Key 报文进行四次握手协商出 PTK，通过使用 EAPOL-Key 报文进行二次组播握手协商出 GTK。

(3) RSN 安全模式密钥协商

RSN 是按照 802.11i 协议为用户提供的一种 WLAN 安全解决方案。在 RSN 网络中，客户端和 AP 通过使用 EAPOL-Key 类型报文进行四次握手协商出 PTK 和 GTK。

(4) 密钥更新

如果客户端长时间使用一个密钥，或携带当前网络正在使用的组播密钥离线，此时网络被破坏的可能性很大，安全性就会大大降低。WLAN 网络通过身份认证与密钥管理中的密钥更新机制来提高 WLAN 网络安全性。密钥更新包括 PTK 更新和 GTK 更新。

- PTK 更新：PTK 更新是对单播数据报文的加密密钥进行更新的一种安全手段，采用重新进行四次握手协商出新的 PTK 密钥的更新机制，来提高安全性。
- GTK 更新：GTK 更新是对组播数据报文的加密密钥进行更新的一种安全手段，采用重新进行两次组播握手协商出新的 GTK 密钥的更新机制，来提高安全性。

(5) 忽略授权信息

授权信息包括 VLAN、ACL 和 User Profile，分为 RADIUS 服务器下发的授权信息和设备本地下发的授权信息。若用户不想使用授权信息，则可以配置忽略授权信息。

(6) 入侵检测

当设备检测到一个未通过认证的用户试图访问网络时，如果开启入侵检测功能，设备将对其所在的 BSS 采取相应的安全策略。

入侵检测所采取的安全模式，包括以下几种：

- 将用户 MAC 地址加入到阻止 MAC 地址列表：缺省模式。如果设备检测到未通过认证用户的关联请求报文，临时将该报文的源 MAC 地址加入阻塞 MAC 地址列表中，在一段时间内，源 MAC 地址为此非法 MAC 地址的无线客户端将不能和 AP 建立连接，在这段时间过后恢复正常。该 MAC 地址的阻塞时间由阻塞非法入侵用户时长决定。
- 关闭收到非法报文的无线服务：关闭收到未通过认证用户的关联请求报文的 BSS 一段时间，该时间由临时关闭服务时长决定。
- 关闭所有无线服务：直接关闭收到未通过认证用户的关联请求报文的 BSS 所提供的服务，直到用户在 Radio 口上重新生成该 BSS。

(7) 加密套件

由于 WEP 加密易破解，一旦攻击者收集到足够多的有效数据帧进行统计分析，那么将会造成数据泄露，无线网络将不再安全。802.11i 增加了 TKIP 和 CCMP 两种加密套件来保护用户数据安全，以下分别介绍。

a. TKIP

TKIP 加密机制依然使用 RC4 算法，所以不需要升级原来无线设备的硬件，只需通过软件升级的方式就可以提高无线网络的安全性。相比 WEP 加密机制，TKIP 有如下改进：

- 通过增长了算法的 IV（Initialization Vector，初始化向量）长度提高了加密的安全性。相比 WEP 算法，TKIP 直接使用 128 位密钥的 RC4 加密算法，而且将初始化向量的长度由 24 位加长到 48 位；
- 采用和 WEP 一样的 RC4 加密算法，但其动态密钥的特性很难被攻破，并且 TKIP 支持密钥更新机制，能够及时提供新的加密密钥，防止由于密钥重用带来的安全隐患；
- 支持 TKIP 反制功能。当 TKIP 报文发生 MIC 错误时，数据可能已经被篡改，也就是无线网络很可能正在受到攻击。当在一段时间内连续接收到两个 MIC 错误的报文，AP 将会启动 TKIP 反制功能，此时，AP 将通过关闭一段时间无线服务的方式，实现对无线网络攻击的防御。

b. CCMP

CCMP 加密机制使用 AES（Advanced Encryption Standard，高级加密标准）加密算法的 CCM（Counter-Mode/CBC-MAC，区块密码锁链－信息真实性检查码）方法，CCMP 使得无线网络安全有了极大的提高。CCMP 包含了一套动态密钥协商和管理方法，每一个无线用户都会动态的协商一套密钥，而且密钥可以定时进行更新，进一步提供了 CCMP 加密机制的安全性。在加密处理过程中，CCMP 也会使用 48 位的 PN（Packet Number）机制，保证每一个加密报文都会使用不同的 PN，在一定程度上提高安全性。

1.1.3 认证模式

1. 静态PSK密钥

PSK 认证方式需要在 AP 侧预先输入预共享密钥，在客户端关联过程中，手动输入该密钥，AP 和客户端通过四次握手密钥协商来验证客户端的预共享密钥的合法性，若 PTK 协商成功，则证明该用户合法，以此来达到认证的目的。

2. 802.1X认证

设备端支持采用 EAP 中继方式或 EAP 终结方式与远端 RADIUS 服务器交互。若用户认证位置在 AP 上，则 AP 为认证设备，由 AP 处理认证过程，若用户认证位置在 AC 上，则 AC 为认证设备，由 AC 处理认证过程。

- 握手功能：使能 802.1X 握手功能之后，设备将定期向通过 802.1X 认证的在线用户发送握手报文，即单播 EAP-Request/Identity 报文，来检测用户的在线状态。
- 安全握手功能：802.1X 安全握手是指在握手报文中加入验证信息，以防止非法用户仿冒正常用户的在线的 802.1X 的客户端与设备进行握手报文的交互。使能 802.1X 安全握手功能后，支持安全握手的客户端需要在每次向设备发送的握手应答报文中携带验证信息，设备将其与认证服务器下发的验证信息进行对比，如果不一致，则强制用户下线。
- 在无线服务下启动了 802.1X 的周期性重认证功能后，设备会根据周期性重认证定时器设定的时间间隔定期向在线 802.1X 用户发起重认证，以检测用户连接状态的变化、确保用户的正常在线，并及时更新服务器下发的授权属性（例如 ACL、VLAN、User Profile）。

3. 静态WEP密钥

在 Pre-RSNA 安全机制的 WEP 加密机制中，由于连接同一 BSS 下的所有客户端都使用同一加密密钥和 AP 进行通信，一旦某个用户的密钥泄露，那么所有用户的数据都可能被窃听或篡改，因此 802.11 提供了动态 WEP 加密机制。在动态 WEP 加密机制中，加密单播数据帧的 WEP 密钥是由客户端和认证服务器通过 802.1X 认证协商产生，保证了每个客户端使用不同的 WEP 单播密钥，从而提高了单播数据帧传输的安全性。组播密钥是 WEP 密钥，若未配置 WEP 密钥，则 AP 使用随机算法产生组播密钥。

当客户端通过 802.1X 认证后，AP 通过发送 RC4 EAPOL-Key 报文将组播密钥及密钥 ID 以及单播密钥的密钥 ID（固定为 4）分发给客户端。

1.2 AP管理

随着无线网络的大规模发展，当大量部署 AP（Access Point，接入点）时，AP 升级软件、射频参数的配置和调整等管理工作将给用户带来高昂的管理成本。为解决这一问题，WLAN 采用 AC+Fit AP 架构，即通过 AC（Access Controller，接入控制器）对下属的 AP 进行集中控制和管理，AP 不需

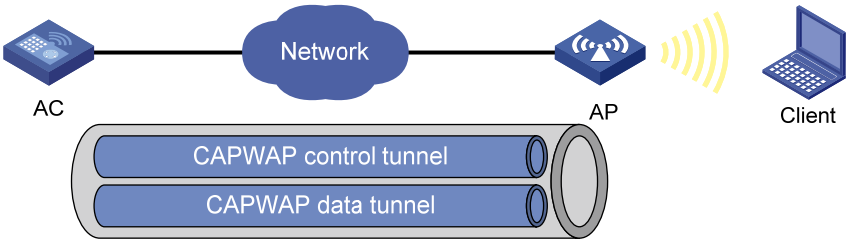
要任何配置，所有的配置都保存在 AC 上并由 AC 下发，同时由 AC 对 AP 进行统一的管理和维护，AP 和 AC 间采用 CAPWAP（Controlling and Provisioning of Wireless Access Point，无线接入点控制与供应）隧道进行通讯，用于传递数据报文和控制报文。

1.2.1 CAPWAP隧道

CAPWAP 隧道为 AP 和 AC 之间的通信提供了通用的封装和传输机制，CAPWAP 隧道使用 UDP 协议作为传输协议，并支持 IPv4 和 IPv6 协议。

如 图 1-1 所示，AC通过CAPWAP协议与AP建立控制隧道和数据隧道，AC通过控制隧道对AP进行管理和监控，通过数据隧道转发客户端的数据报文。

图1-1 CAPWAP 隧道典型组网图



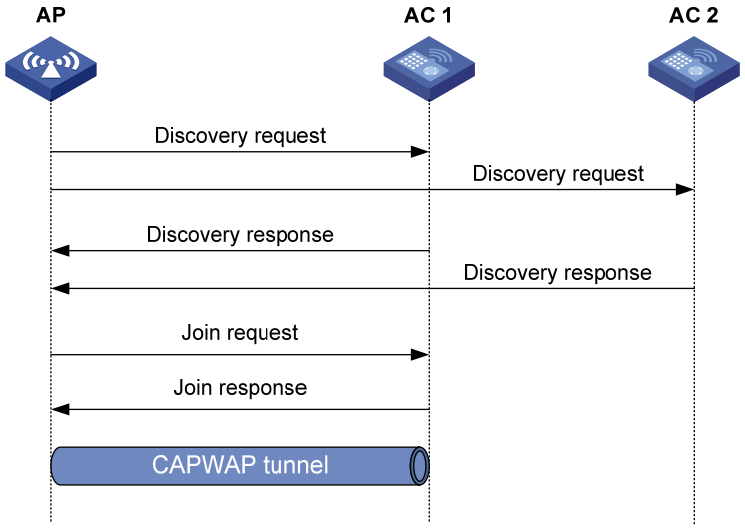
2. 获取AC地址

AP 零配置启动后，AP 会自动创建 VLAN-interface 1，并在该接口上默认开启 DHCP 客户端、DHCPv6 客户端和 DNS 客户端功能，完成上述操作后，AP 将使用获取的 AC 地址发现 AC 并建立 CAPWAP 隧道。AP 获取 AC 地址的方式如下：

- 静态配置：通过预配置为 AP 手工指定 AC 的 IP 地址。
- DHCP 选项：通过 DHCP 服务器返回的 Option 138 或 Option 43 选项获取 AC 地址。若通过两个选项都获取了 AC 地址，则 AP 选择从 Option 138 获取的地址作为 AC 地址，并向 AC 地址发送单播 Discovery request 报文来发现、选择 AC 并建立 CAPWAP 隧道。有关 Option 选项的详细介绍请参见“系统功能介绍”中的 DHCP 及 DNS。
- DNS：AP 通过 DHCP 服务器获取 AC 的域名后缀及 DNS server 的 IP 地址，再将从自身获取的主机名与域名后缀形成 AC 的完整域名进行 DNS 解析，获取 AC 地址，AP 向获取的所有 AC 地址发送单播 Discovery request 报文来发现、选择 AC 并建立 CAPWAP 隧道。
- 广播：AP 通过向 IPv4 广播地址 255.255.255.255 发送 Discovery request 广播报文来发现、选择 AC 并建立隧道。
- IPv4 组播：AP 通过向 IPv4 组播地址 224.0.1.140 发送 Discovery request 组播报文来发现、选择 AC 并建立隧道。
- IPv6 组播：AP 通过向 IPv6 组播地址 FF0E::18C 发送 Discovery request 组播报文来发现、选择 AC 并建立隧道。

3. CAPWAP建立隧道过程

图1-2 CAPWAP 隧道建立过程



AP 发现 AC 并建立 CAPWAP 隧道过程如下：

(1) AP 向 AC 地址发送 Discovery request 报文。

(2) AC 收到 Discovery request 报文后，根据本地策略和报文内容决定是否对 AP 进行回复 Discovery response 报文，Discovery response 报文中会携带优先级值、AC 上是否存在该 AP 的信息和 AC 上的负载信息等，以此实现 AC 选择 AP。

(3) AP 收到各个 AC 的 Discovery response 报文后，根据报文中携带的内容，选择最优 AC。

(4) AP 向选择的最优 AC 发送 Join request 报文。

(5) AC 根据报文内容，检查是否为该 AP 提供服务，并回复 Join response 报文。

(6) AP 若收到 Result Code 为失败的 Join response 报文，则不建立隧道；若 AP 收到 Result Code 为成功的 Join response 报文，则 AP 和 AC 成功建立隧道。

AP 依次使用静态配置、DHCP 选项、DNS、广播、IPv4 组播和 IPv6 组播获取的 AC 地址进行发现 AC 并建立隧道过程，若某一种方式成功建立 CAPWAP 隧道，则停止发现 AC 的过程。

1.2.2 AP组

AP 组用来实现对批量 AP 的配置管理，通过使 AP 继承其所属组的配置来达到对大量 AP 的配置的目的。AP 组配置，全局配置及 AP 配置共同构成了分级继承的 AP 运行配置。在大规模无线网络中，同一 AC 管理的 AP 数量可达几万台，对每一台 AP 逐一配置将导致网络管理难度极大提高。AP 组用来降低逐个配置 AP 的操作成本，用户可以创建多个组，对不同的组用户可以根据需要配置不同的 AP 配置。

所有 AP 缺省情况下均属于默认组，默认组组名为 default-group，默认组不需创建、不可删除。

AP 组可以指定多个 AP 名称、AP 序列号、AP MAC 地址和 AP IP 地址四种入组规则，AP 的入组匹配顺序为：优先根据 AP 名字入组规则匹配入组，其次是 AP 序列号入组规则，然后是 AP MAC 地址入组规则，最后是 AP IP 地址入组规则，若未匹配到任何入组规则，则 AP 将被加入到默认组。

需要注意的是：

- AP 必须属于一个 AP 组，且只能属于一个 AP 组。
- 同一入组规则不能重复出现在不同的 AP 组中，若将同一入组规则配置在新 AP 组中，将导致原 AP 组中对应的入组规则自动删除（相当于迁移组）。
- 默认组不能配置 AP 名字、AP 序列号、AP MAC 和 AP IP 地址四种入组规则。
- 删除 AP 入组规则，AP 会根据 AP 的入组规则匹配顺序重新匹配 AP 组。比如，删除某一 AP 组下的一个 AP 名字入组规则，该 AP 会优先进入指定了该 AP 序列号的 AP 组，如果匹配不到 AP 序列号，则该 AP 会优先进入指定了该 AP MAC 地址入组规则的 AP 组，如果匹配不到 AP MAC 地址，则该 AP 会优先进入指定了该 AP IP 地址入组规则的 AP 组，如果仍然匹配不到，则该 AP 会进入默认组。
- AP 组下有 AP 已经入组（手工 AP 或自动 AP），则该 AP 组不允许删除；配置了入组规则，但是没有 AP 入组的 AP 组可以被删除。
- AP 的生效配置取决于 AP、AP 组及 AP 全局配置中优先级最高的配置，优先级从高到低为 AP 配置、AP 组配置、全局配置。若优先级高的配置不存在，则 AP 使用优先级低的配置。若都不存在 AP 的配置，则使用缺省值。

1.2.3 全局配置

全局配置作用于所有 AP 组下的 AP，由于全局配置的优先级最低，所以仅当 AP 和 AP 组下无配置时，才会继承全局配置。AP、AP 组及全局配置的优先级从高到低为 AP 视图配置、AP 组视图配置、全局视图配置。若优先级高的配置不存在，则 AP 使用优先级低的配置；若都不存在 AP 的配置，则使用优先级最低的视图下的缺省配置。

1.2.4 预配置

通常情况下，可以通过终端连接到 AP 之后，对 AP 进行配置，但这种逐台配置 AP 的操作方式不利于大规模的 AP 部署以及集中化管理。AP 预配置提供了一种在 AC 上对 AP 的基本网络参数进行配置，并将预配置信息下发至 AP 的方法。下发到 AP 的配置会保存为 AP 私有预配置文件 wlan_ap_prvs.xml，当 AP 重启时，该私有预配置文件才会生效。

需要注意的是：

- AC 只能将预配置信息发送给与它建立 CAPWAP 隧道的 AP，同时只有主 AC 才能对已经与它建立 CAPWAP 隧道的 AP 进行预配置。
- 一些预配置可以在 AP 预配置下和 AP 组预配置下都进行配置，则优先使用 AP 预配置下的配置。

预配置提供的配置包括：

- 配置 AP 与指定的 AC 建立 CAPWAP 隧道。
- 配置 AP 的 IP 地址。
- 配置 AP 的网关地址。
- 配置 AP 发现 AC 时使用的域名服务器的域名后缀。
- 配置 AP 发现 AC 时使用的域名服务器的 IP 地址。
- 配置 802.1X Client。

1.2.5 区域码

区域码决定了射频可以使用的工作频段、信道、发射功率级别等。在配置 WLAN 设备时，必须正确地设置区域码，以确保不违反当地的管制规定。为了防止区域码的修改导致射频的工作频段、信道等与所在国家或地区的管制要求冲突，可以开启区域码锁定功能。

1.2.6 自动AP

在无线网络中部署的 AP 数量较多时，开启自动 AP 功能可以简化配置。开启自动 AP 功能后，无需配置手工 AP 配置，AP 和 AC 就可以建立 CAPWAP 连接，AC 将以 AP 的 MAC 地址来命名上线的自动 AP。在 AP 发现 AC 过程中，AP 优先选择存在手工 AP 的 AC 建立 CAPWAP 隧道连接，若不存在手工 AP 配置，则 AP 会从开启自动 AP 功能的 AC 中，选择最优 AC 进行 CAPWAP 隧道连接。自动 AP 功能生成的 AP，没有提供 AP 视图进行相关参数配置，自动 AP 需要固化为手工 AP 或者通过 AP 组进行配置。

出于网络安全因素考虑，自动 AP 应配合固化功能或 AP 认证功能共同使用。若配置固化功能时，用户应在自动 AP 第一次接入后，将所有自动 AP 固化为手工 AP 并关闭自动 AP 功能。

1.2.7 AC备份

在集中式转发模式下，AC 在汇聚层上承担了大量 AP 的状态维护和数据转发工作。AC 设备的故障将导致无线网络的服务中断。

通过 AC 备份功能，可以将两台 AC 相连，构建一个备份组，备份组中的两台 AC 分别为主 AC 和备 AC，主备 AC 通过 WHA（WLAN High Availability，无线局域网高可靠性）数据备份通道进行 AP 数据的同步，当主 AC 发生故障时，备 AC 能够立即接管当前所有在线 AP，使业务流量不中断。

1.2.8 配置准备

CAPWAP 隧道的建立需要 DHCP 和 DNS 的配合。因此，首先需要完成以下配置任务：

- AP 需要获取到自身的 IP 地址，因此需要在 DHCP server 上配置地址池为 AP 分配 IP 地址。
- 若获取 AC 地址的方式为 DHCP 选项方式，则需要在 DHCP server 上将对应地址池的 Option 138 或 Option 43 配置为 AC 的 IPv4 地址，或使用 Option 52 配置 AC 的 IPv6 地址。
- 若获取 AC 地址的方式为 DNS 方式，则需要在 DHCP server 对应的地址池上配置 DNS server 的 IP 地址和 AC 的域名后缀。并在 DNS server 上创建区域，添加 AC 的 IP 地址和域名的映射。
- 保证 AC 和 AP 之间的路由可达。

有关 DHCP 和域名解析的详细介绍和相关配置，请参见“系统功能介绍”中的 DHCP 及 DNS。

1.3 客户端限速

每个 AP 提供的带宽由接入的所有客户端共享，如果部分客户端占用过多带宽，将导致其它客户端受到影响。通过配置客户端限速功能，可以限制单个客户端对带宽的过多消耗，保证所有接入客户端均能正常使用网络业务。

1.3.1 客户端限速模式

客户端限速功能有两种工作模式：

- 动态模式：配置所有客户端使用的速率总值，每个客户端的限制速率是速率总值/客户端数量。例如，配置所有客户端可用速率的总和为 10Mbps，当有 5 个用户上线时，每个客户端的可用带宽限制为 2Mbps。
- 静态模式：为所有客户端配置相同的限速速率，该配置对所有客户端生效。当接入客户端增加至一定数量时，如果所有接入客户端限制速率的总和超出 AP 可提供的有效带宽，那么每个客户端将不能保证获得配置的带宽。

动态模式与静态模式仅用于配置基于无线服务模板或基于射频方式的客户端限速功能。

1.3.2 客户端限速方式

客户端限速功能有三种配置方式：

- 基于客户端类型：该方式配置的客户端限速对所有客户端生效，每种类型的客户端的速率都不能超过配置的限速值。
- 基于无线服务模板：该方式配置的客户端限速对使用同一个无线服务接入的所有客户端生效。
- 基于射频：该方式配置的客户端限速对使用同一个射频接入的所有客户端生效。

如果同时配置多种方式或不同模式的客户端限速，则多个配置将同时生效，每个客户端的限速值为多种方式及不同模式中的限速速率最小值。

1.4 智能带宽保障

在实际应用中，网络中的流量不会一直处于某个稳定的状态。当某个 BSS 的流量非常大时，会挤占其它 BSS 的可用带宽。如果直接对单个 BSS 的报文进行限速，在总体流量较小时，又会导致闲置带宽被浪费。

智能带宽保障功能提供了更灵活的流量控制机制，当网络未拥塞时，所有 BSS 的报文都可以通过；在网络发生拥塞时，每个 BSS 都可以获取最低的保障带宽。通过这种方式，既确保了网络带宽的充分利用，又兼顾了不同无线服务之间带宽占用的公平原则。例如，配置 SSID 1、SSID 2 及 SSID 3 的保障带宽占总带宽的比例分别为 25%、25%及 50%。当网络空闲时，SSID 1 可以超过保障带宽，任意占用网络剩余带宽；当网络繁忙、没有剩余带宽时，SSID 1 至少可以占有自己的保障带宽部分（25%）。

智能带宽保障功能只能对由 AP 发送至客户端的流量（即出方向流量）进行控制。

1.5 无线多媒体

802.11 网络提供了基于竞争的无线接入服务，但是不同的应用对于网络的要求是不同的，而无线网络不能为不同的应用提供不同质量的接入服务，所以已经不能满足实际应用的需要。

IEEE 802.11e 为基于 802.11 协议的 WLAN 体系添加了 QoS 功能，Wi-Fi 组织为了满足不同 WLAN 厂商对 QoS 的需求，定义了 WMM（Wi-Fi Multimedia，Wi-Fi 多媒体）协议。WMM 协议用于保证优先发送高优先级的报文，从而保证语音、视频等应用在无线网络中有更好的服务质量。

1.5.1 WMM状态

在 WMM 状态页面中可以查看 AC 连接的各 AP 是否开启 WMM 功能。

1.5.2 WMM配置

在 WMM 配置页面中，可以配置每个 AP 的 SVP 映射、连接准入控制策略以及允许接入的客户端最大数等信息。

SVP 映射是指将 IP 头中 Protocol ID 为 119 的 SVP 报文放入指定的 AC-VI 或 AC-VO 队列中，保证 SVP 报文比其他数据报文具有更高的优先级。没有进行 SVP 映射时，SVP 报文将进入 AC-BE 队列。

CAC（Connect Admission Control，连接准入控制）用来限制能使用高优先级队列（AC-VO 和 AC-VI 队列）的客户端个数，从而保证已经使用高优先级队列的客户端能够有足够的带宽。如果客户端需要使用高优先级的 AC，则需要进行请求，AP 按照基于信道利用率的准入策略或基于用户数量的准入策略算法，计算是否允许客户端使用高优先级 AC，并将结果回应给客户端。当单独或同时开启 AC-VO、AC-VI 队列的 CAC 功能时，如果客户端申请 AC 失败，设备会对其进行降级至 AC-BE 处理。

1.5.3 EDCA参数

在 EDCA 参数页面中，可以查看和修改 EDCA 参数和 ACK 策略。

EDCA（Enhanced Distributed Channel Access，增强的分布式信道访问）是 WMM 定义的一套信道竞争机制，有利于高优先级的报文享有优先发送的权利和更多的带宽。

WMM 协议为 AC 定义了以下 EDCA 参数：

- AIFSN（Arbitration Inter Frame Spacing Number，仲裁帧间隙数）：在 802.11 协议中，空闲等待时长（DIFS）为固定值，而 WMM 针对不同 AC 配置退避前需要等待的时隙，AIFSN 数值越小，用户的空闲等待时间越短。
- ECWmin（Exponent form of CWmin，最小竞争窗口指数形式）和 ECWmax（Exponent form of CWmax，最大竞争窗口指数形式）：决定了平均退避时间值。这两个数值越大，该 AC 中报文的平均退避时间越长。
- TXOP Limit（Transmission Opportunity Limit，传输机会限制）：AC 中的报文每次竞争成功后，可占用信道的最大时长。这个数值越大，用户一次能占用信道的时长越大。如果是 0，则每次占用信道后只能发送一个报文。

ACK 策略有两种：Normal ACK 和 No ACK。

- Normal ACK 策略：接收者在接收到每个单播报文后，都要回复 ACK 进行确认。
- No ACK（No Acknowledgment）策略：在无线报文交互过程中，不使用 ACK 报文进行接收确认。在通信质量较好、干扰较小的情况下，No ACK 策略能有效提高报文传输效率。但是，在通信质量较差的情况下，如果使用 No ACK 策略，则会造成丢包率增大的问题。

1.5.4 射频与客户端协商参数

在射频与客户端协商参数页面中，用户除了可以查看和修改 EDCA 参数，还可以开启或关闭连接准入控制策略功能。

1.5.5 客户端的WMM统计信息

在客户端的 WMM 统计信息页面中，用户除了可以查看 SSID 等设备的基本信息和数据流量统计信息，还可以查看到客户端接入时指定的 AC 的 APSD 属性。

U-APSD 是对传统节能模式的改进。在这种机制下，客户端不再定期监听 Beacon 帧，而是由客户端决定何时到 AP 上获取缓存报文。对于客户端的一次请求，AP 可以发送多个缓存报文给客户端，该机制显著改善了客户端的节能效果。开启 WMM 功能的同时将自动开启 U-APSD 节能模式。

1.5.6 传输流信息

在传输流信息页面中，用户可以查看包括来自有线网络报文的用户优先级、传输流标识、流方向、允许富余带宽等传输流信息。

1.6 WIPS

WIPS（Wireless Intrusion Prevention System，无线入侵防御系统）是针对 802.11 协议开发的二层协议检测和防护功能。WIPS 通过 AC 与 Sensor（开启 WIPS 功能的 AP）对信道进行监听及分析处理，从中检测出威胁网络安全、干扰网络服务、影响网络性能的无线行为或设备，并提供对入侵的无线设备的反制，为无线网络提供一套完整的安全解决方案。

WIPS 由 Sensor、AC 以及网管软件组成。Sensor 负责收集无线信道上的原始数据，经过简单加工后，上传至 AC 进行综合分析。AC 会分析攻击源并对其实施反制，同时向网管软件输出日志信息。网管软件提供丰富的图形界面，提供系统控制、报表输出、告警日志管理功能。

WIPS 支持以下功能：

- 攻击检测：提供多种攻击方式的攻击检测功能。
- 设备分类：通过侦听无线信道的 802.11 报文来识别无线设备，并对其进行分类。
- 反制：对非法设备进行攻击，使其它设备无法关联到非法设备，从而保护用户网络的安全。

1.6.1 开启WIPS

开启 WIPS 功能前，需要将 AP 加入到指定 VSD（Virtual Security Domain，虚拟安全域）中。该 AP 也称为 Sensor。

1.6.2 配置虚拟安全域

通过在虚拟安全域上应用分类策略、攻击检测策略、Signature 策略或反制策略，使已配置的分类策略、攻击检测策略、Signature 策略或反制策略在虚拟安全域内的 Radio 上生效。

1.6.3 配置分类策略

1. 分类策略

可以通过两种配置方式实现设备分类，其中手工分类的优先级高于自动分类。

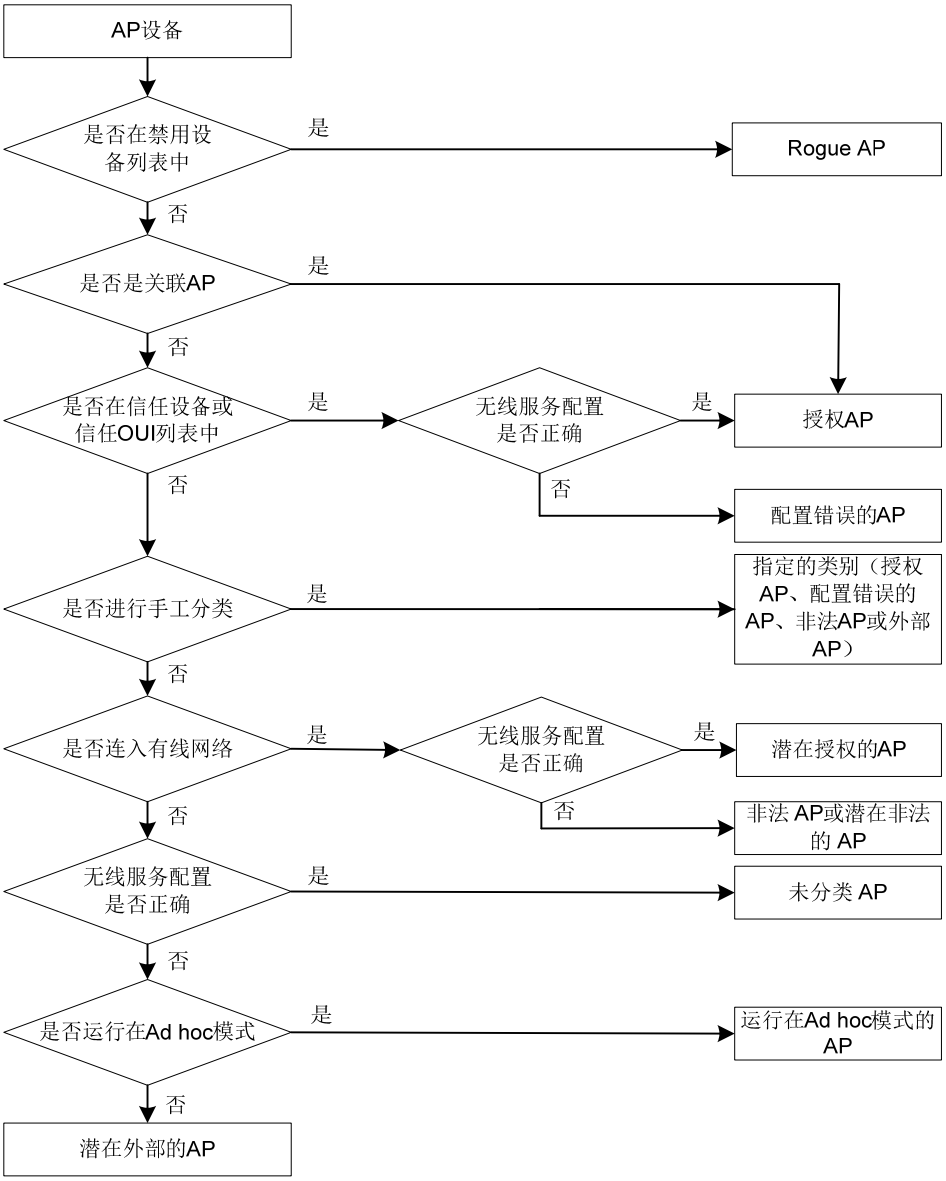
- 自动分类：通过信任设备列表、信任 OUI 列表和静态禁用设备列表对所有设备进行分类；或通过自定义的 AP 分类规则对 AP 设备进行分类。
- 手工分类：通过手动指定 AP 的类型对设备进行分类。

2. AP的分类类别

WIPS 将检测到的 AP 分为以下几类：

- 授权 AP（Authorized AP）：允许在无线网络中使用的 AP。包括已经关联到 AC 上且不在禁用列表中的 AP 和手动指定的授权 AP。
- 非法 AP（Rouge AP）：不允许在无线网络中使用的 AP。包括禁用设备列表中的 AP、不在 OUI 配置文件中的 AP 和手动指定的非法 AP。
- 配置错误的 AP（Misconfigured AP）：无线服务配置错误，但是允许在无线网络中使用的 AP。例如，在信任设备列表中，但使用了非法 SSID 的 AP；在 OUI 配置文件中，但不在禁用设备列表的 AP；在信任 OUI 或是信任设备列表中，但是未与 AC 关联的 AP。
- 外部 AP（External AP）：其他无线网络中的 AP。WIPS 可能会检测到邻近网络中的 AP，例如邻近公司或个人住宅中的 AP。
- Ad hoc：运行在 Ad hoc 模式的 AP。WIPS 通过检测 Beacon 帧将其分类为 Ad hoc。
- 潜在授权的 AP（Potential-authorized AP）：无法确定但可能是授权的 AP。如果 AP 既不在信任设备或信任 OUI 列表中也不在禁用设备列表中，那么该 AP 很可能是授权的 AP，如 Remote AP。
- 潜在非法的 AP（Potential-rogue AP）：无法确定但可能是非法的 AP。如果 AP 既不在信任设备或信任 OUI 列表中也不在禁用设备列表中，而且它的无线服务配置也不正确，那么，如果检测到它的有线端口可能连接到网络中，则认为其为潜在非法的 AP；如果能确定其有线端口连接到网络中，则认为其为非法 AP，如恶意入侵者私自接入网络的 AP。
- 潜在外部的 AP（Potential-external AP）：无法确定但可能是外部的 AP。如果 AP 既不在信任设备或信任 OUI 列表中也不在禁用设备列表中，而且它的无线服务配置也不正确，同时也没有检测到它的有线端口连接到网络中，则该 AP 很可能是外部的 AP。
- 未分类 AP（Uncategorized AP）：无法确定归属类别的 AP。
- WIPS对检测到的AP的分类处理流程如 图 1-3 所示：

图1-3 WIPS 对检测到的 AP 设备的分类处理流程示意图



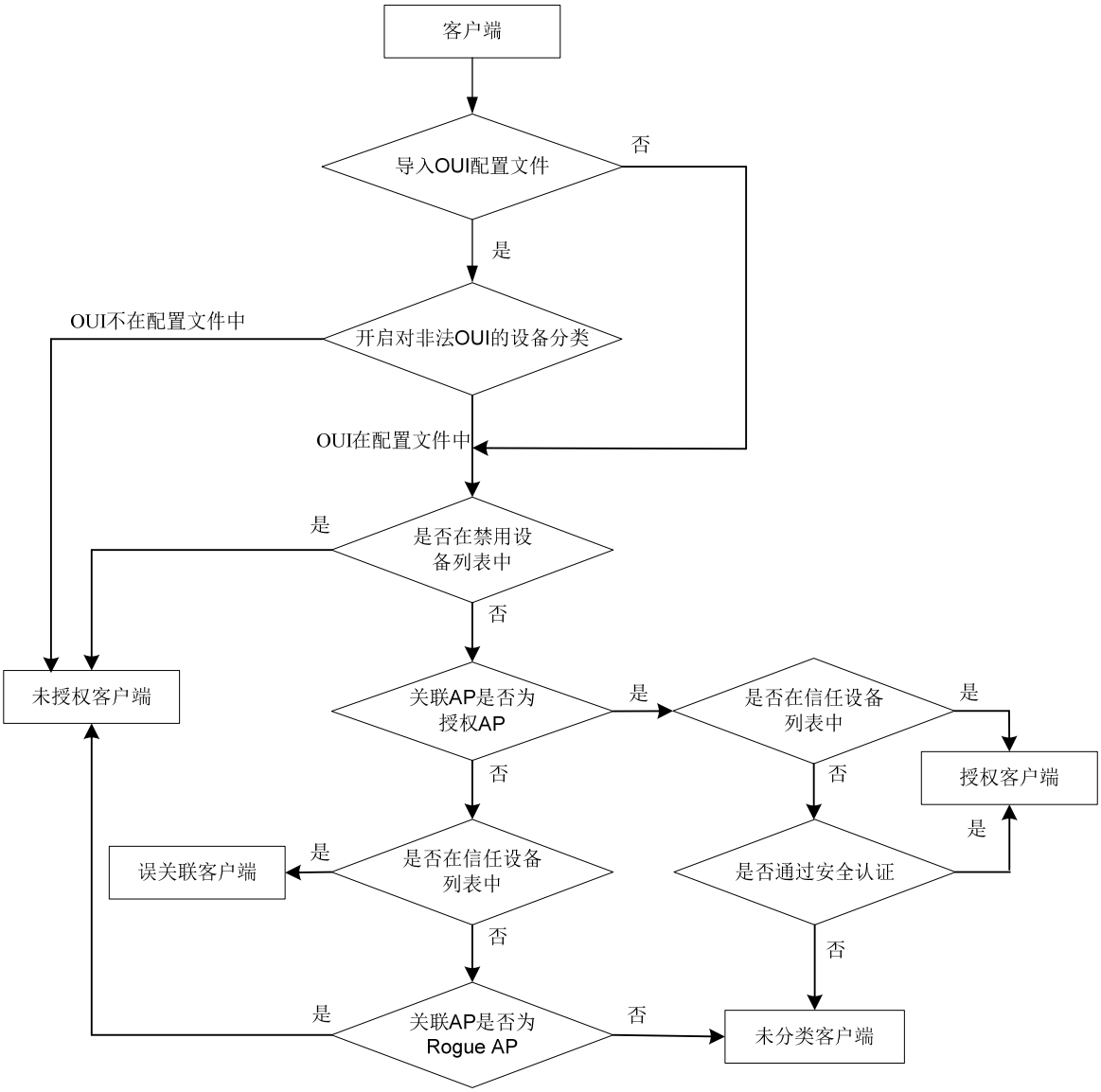
3. 客户端的分类类别

WIPS 将检测到的客户端分为以下几类：

- 授权客户端（Authorized Client）：允许使用的客户端，如关联到授权 AP 上的受信任的客户端或通过加密认证方式关联到授权 AP 上的客户端都是授权的客户端。
- 未授权客户端（Unauthorized Client）：不允许使用的客户端。如在禁用设备列表中的客户端、连接到 Rogue AP 上的客户端以及不在 OUI 配置文件中的客户端都是未授权客户端。
- 错误关联客户端（Misassociation Client）：信任设备列表中的客户端关联到非授权 AP 上。错误关联的客户端可能会对网络信息安全带来隐患。
- 未分类客户端（Uncategorized Client）：无法确定归属类别的客户端。

WIPS对检测到的客户端的分类处理流程如 图 1-4 所示：

图1-4 WIPS 对检测到的客户端的分类处理流程示意图



1.6.4 配置攻击检测策略

WIPS 通过分析侦听到的 802.11 报文，来检测针对 WLAN 网络的无意或者恶意的攻击，并以告警的方式通知网络管理员。

1. 表项学习速率和表项时间参数

如果攻击者通过发送大量报文来增加 WIPS 的处理开销等。通过检测周期内学习到设备的表项来判断是否需要对表项学习进行限速处理。设备在统计周期内学习到的 AP 或客户端表项达到触发告警阈值，设备会发送告警信息，并停止学习 AP 表项和客户端表项。

2. 泛洪攻击检测

泛洪攻击是指通过向无线设备发送大量同类型的报文，使无线设备会被泛洪攻击报文淹没而无法处理合法报文。WIPS 通过持续地监控 AP 或客户端的流量来检测泛洪攻击。当大量同类型的报文超出上限时，认为无线网络正受到泛洪攻击。

目前 WIPS 能够防范的泛洪攻击包括：

- Probe-request/Association-request/Reassociation-request 帧泛洪攻击

攻击者通过模拟大量的客户端向 AP 发送 Probe-request/Association-request/Reassociation-request 帧，AP 收到大量攻击报文后无法处理合法客户端的 Probe-request /Association-request/Reassociation-request 帧。

- Authentication 帧泛洪攻击

攻击者通过模拟大量的客户端向 AP 发送 Authentication 帧，AP 收到大量攻击报文后无法处理合法客户端的 Authentication 帧。

- Beacon 帧泛洪攻击

该攻击是通过发送大量的 Beacon 帧使客户端检测到多个虚假 AP，导致客户端选择正常的 AP 进行连接时受阻。

- Block ACK 泛洪攻击

该攻击通过仿冒客户端发送伪造的 Block ACK 帧来影响 Block ACK 机制的正常运行，导致通信双方丢包。

- RTS/CTS 泛洪攻击

在无线网络中，通信双方需要遵循虚拟载波侦听机制，通过 RTS（Request to Send，发送请求）/CTS（Clear to Send，清除发送请求）交互过程来预留无线媒介，通信范围内的其它无线设备在收到 RTS 和（或）CTS 后，将根据其中携带的信息来延迟发送数据帧。RTS/CTS 泛洪攻击利用了虚拟载波侦听机制的漏洞，攻击者能通过泛洪发送 RTS 和（或）CTS 来阻塞 WLAN 网络中合法无线设备的通信。

- Deauthentication 帧泛洪攻击

攻击者通过仿冒 AP 向与其关联的客户端发送 Deauthentication 帧，使得被攻击的客户端与 AP 的关联断开。这种攻击非常突然且难以防范。单播 Deauthentication 帧攻击是针对某一个客户端，而广播 Deauthentication 帧攻击是针对与该 AP 关联的所有客户端。

- Disassociation 帧泛洪攻击

攻击原理同 Disassociation 帧泛洪攻击。攻击者是通过仿冒 AP 向与其关联的客户端发送 Disassociation 帧，使得被攻击的客户端与 AP 的关联断开。这种攻击同样非常突然且难以防范。

- EAPOL-Start 泛洪攻击

IEEE 802.1X 标准定义了一种基于 EAPOL（EAP over LAN，局域网上的可扩展认证协议）的认证协议，该协议通过客户端发送 EAPOL-Start 帧开始一次认证流程。AP 接收到 EAPOL-Start 后会回复一个 EAP-Identity-Request，并为该客户端分配一些内部资源来记录认证状态。攻击者可以通过模拟大量的客户端向 AP 发送 EAPOL-Start 来耗尽该 AP 的资源，使 AP 无法处理合法客户端的认证请求。

- Null-data 泛洪攻击

该攻击通过仿冒合法客户端向与其关联的 AP 发送 Null-data 帧，使得 AP 误认为合法的客户端进入省电模式，将发往该客户端的数据帧进行暂存。如果攻击者持续发送 Null-data 帧，当暂存帧的存储时间超过 AP 暂存帧老化时间后，AP 会将暂存帧丢弃，妨害了合法客户端的正常通信。

- EAPOL-Logoff 泛洪攻击

在 EAPOL 认证环境中，当通过认证的客户端需要断开连接时，会发送一个 EAPOL-Logoff 帧来关闭与 AP 间的会话。但 AP 对接收到的 EAPOL-Logoff 帧不会进行认证，因此攻击者通过仿冒合法客户端向 AP 发送 EAPOL-Logoff 帧，可以使 AP 关闭与该客户端的连接。如果攻击者持续发送仿冒的 EAPOL-Logoff 帧，将使被攻击的客户端无法保持同 AP 间的连接。

- EAP-Success/Failure 泛洪攻击

在使用 802.1X 认证的 WLAN 环境中，当客户端认证成功时，AP 会向客户端发送一个 EAP-Success 帧（code 字段为 success 的 EAP 帧）；当客户端认证失败时，AP 会向客户端发送一个 EAP-Failure 帧（code 字段为 failure 的 EAP 帧）。攻击者通过仿冒 AP 向请求认证的客户端发送 EAP-Failure 帧或 EAP-Success 帧来破坏该客户端的认证过程，通过持续发送仿冒的 EAP-Failure 帧或 EAP-Success 帧，可以阻止被攻击的客户端与 AP 间的认证。

3. 畸形报文检测

畸形报文攻击是指攻击者向受害客户端发送有缺陷的报文，使得客户端在处理这样的报文时会出现崩溃。WIPS 利用 Sensor 监听无线信道来获取无线报文，通过报文解析检测出具有某些畸形类型特征的畸形报文，并发送告警。

目前支持的畸形报文检测包括：

- IE 重复的畸形报文

该检测是针对所有管理帧的检测。当解析某报文时，该报文所包含的某 IE 重复出现时，则判断该报文为重复 IE 畸形报文。因为厂商自定义 IE 是允许重复的，所以检测 IE 重复时，不检测厂商自定义 IE。

- Fata-Jack 畸形报文

该检测是针对 Authentication 帧的检测。Fata-jack 畸形类型规定，当身份认证算法编号即 Authentication algorithm number 的值等于 2 时，则判定该帧为 Fata-jack 畸形报文。

- IBSS 和 ESS 置位异常的畸形报文

该检测是针对 Beacon 帧和探查响应帧进行的检测。当报文中的 IBSS 和 ESS 都置位为 1 时，由于此种情况在协议中没有定义，所以该报文被判定为 IBSS 和 ESS 置位异常的畸形报文。

- 源地址为广播或者组播的认证和关联畸形报文

该检测是针对所有管理帧的检测。当检测到该帧的 TO DS 等于 1 时，表明该帧为客户端发给 AP 的，如果同时又检测到该帧的源 MAC 地址为广播或组播，则该帧被判定为 Invalid-source-address 畸形报文。

- 畸形 Association-request 报文

该检测是针对认证请求帧的检测。当收到认证请求帧中的 SSID 的长度等于 0 时，判定该报文为畸形关联请求报文。

- 畸形 Authentication 报文

该检测是针对认证帧的检测。当检测到以下情况时请求认证过程失败，会被判断为认证畸形报文。

  - 当对认证帧的身份认证算法编号（Authentication algorithm number）的值不符合协议规定，并且其值大于 3 时；

- 当标记客户端和 AP 之间的身份认证的进度的 Authentication Transaction Sequence Number 的值等于 1，且状态代码 status code 不为 0 时；
- 当标记客户端和 AP 之间的身份认证的进度的 Authentication Transaction Sequence Number 的值大于 4 时。

- 含有无效原因值的解除认证畸形报文

该检测是针对解除认证畸形帧的检测。当解除认证畸形帧携带的 Reason code 的值属于集合[0，67～65535]时，则属于协议中的保留值，此时判定该帧为含有无效原因值的解除认证畸形报文。

- 含有无效原因值的解除关联畸形报文

该检测是针对解除关联帧的检测。当解除关联帧携带的 Reason code 的值属于集合[0，67～65535]时，则属于协议中的保留值，此时判定该帧为含有无效原因值的解除关联畸形报文。

- 畸形 HT IE 报文

该检测是针对 Beacon、探查响应帧、关联响应帧、重关联请求帧的检测。当检测到以下情况时，判定为 HT IE 的畸形报文，发出告警，在静默时间内不再告警。

- 解析出 HT Capabilities IE 的 SM Power Save 值为 2 时；
- 解析出 HT Operation IE 的 Secondary Channel Offset 值等于 2 时。

- IE 长度非法的畸形报文

该检测是针对所有管理帧的检测。信息元素（Information Element，简称 IE）是管理帧的组成元件，每种类型的管理帧包含特定的几种 IE。报文解析过程中，当检测到该报文包含的某个 IE 的长度为非法时，该报文被判定为 IE 长度非法的畸形报文。

- 报文长度非法的畸形报文

该检测是针对所有管理帧的检测。当解析完报文主体后，IE 的剩余长度不等于 0 时，则该报文被判定为报文长度非法的畸形报文。

- 无效探查响应报文

该检测是针对探查响应报文。当检测到该帧为非 Mesh 帧，但同时该帧的 SSID Length 等于 0，这种情况不符合协议（协议规定 SSID Length 等于 0 的情况是 Mesh 帧），则判定为无效探查响应报文。

- Key 长度超长的 EAPOL 报文

该检测是针对 EAPOL-Key 帧的检测。当检测到该帧的 TO DS 等于 1 且其 Key Length 大于 0 时，则判定该帧为 Key 长度超长的 EAPOL 报文。Key length 长度异常的恶意的 EAPOL-Key 帧可能会导致 DOS 攻击。

- SSID 长度超长的畸形报文

该检测是针对 Beacon、探查请求、探查响应、关联请求帧的检测。当解析报文的 SSID length 大于 32 字节时，不符合协议规定的 0～32 字节的范围，则判定该帧为 SSID 超长的畸形报文。

- 多余 IE 畸形报文

该检测是针对所有管理帧的检测。报文解析过程中，当检测到既不属于报文应包含的 IE，也不属于 reserved IE 时，判断该 IE 为多余 IE，则该报文被判定为多余 IE 的畸形报文。

- Duration 字段超大的畸形报文

该检测是针对单播管理帧、单播数据帧以及 RTS、CTS、ACK 帧的检测。如果报文解析结果中该报文的 Duration 值大于指定的门限值，则为 Duration 超大的畸形报文。

4. 攻击检测

- Spoofing

Spoofing 攻击是指攻击者仿冒其他设备，从而威胁无线网络的安全。例如：无线网络中的客户端已经和 AP 关联，并处于正常工作状态，此时如果有攻击者仿冒 AP 的名义给客户端发送解除认证/解除关联报文就可能导致客户端下线，从而达到破坏无线网络正常工作的目的；又或者攻击者仿冒成合法的 AP 来诱使合法的客户端关联，攻击者仿冒成合法的客户端与 AP 关联等，从而可能导致用户账户信息泄露。

目前支持的 Spoofing 检测包括：AP 地址仿冒和客户端地址仿冒

- Weak IV

WEP 安全协议使用的 RC4 加密算法存在一定程度的缺陷，当其所用的 IV 值不安全时会大大增加其密钥被破解的可能性，该类 IV 值即被称为 Weak IV。WIPS 特性通过检测每个 WEP 报文的 IV 值来预防这种攻击。

- Windows 网桥

当一个连接到有线网络的无线客户端使用有线网卡建立了 Windows 网桥时，该无线客户端就可以通过连接外部 AP 将外部 AP 与内部有线网络进行桥接。此组网方式会使外部 AP 对内部的有线网络造成威胁。WIPS 会对已关联的无线客户端发出的数据帧进行分析，来判断其是否存在于 Windows 网桥中。

- 设备禁用 802.11n 40MHz

支持 802.11n 标准无线设备可以支持 20MHz 和 40MHz 两种带宽模式。在无线环境中，如果与 AP 关联的某个无线客户端禁用了 40MHz 带宽模式，会导致 AP 与该 AP 关联的其它无线客户端也降低无线通信带宽到 20MHz，从而影响到整个网络的通信能力。WIPS 通过检测无线客户端发送的探测请求帧来发现禁用 40MHz 带宽模式的无线客户端。

- Omerta

Omerta 是一个基于 802.11 协议的 DoS 攻击工具，它通过向信道上所有发送数据帧的客户端回应解除关联帧，使客户端中断与 AP 的关联。Omerta 发送的解除关联帧中的原因代码字段为 0x01，表示未指定。由于正常情况下不会出现此类解除关联帧，因此 WIPS 可以通过检测每个解除关联帧的原因代码字段来检测这种攻击。

- 未加密授权 AP/未加密信任客户端

在无线网络中，如果有授权 AP 或信任的无线客户端使用的配置是未加密的，网络攻击者很容易通过监听来获取无线网络中的数据，从而导致网络信息泄露。WIPS 会对信任的无线客户端或授权 AP 发出的管理帧或数据帧进行分析，来判断其是否使用了加密配置。

- 热点攻击

热点攻击指恶意 AP 使用热点 SSID 来吸引周围的无线客户端来关联自己。攻击者通过伪装成公共热点来引诱这些无线客户端关联自己。一旦无线客户端与恶意 AP 关联上，攻击者就会发起一系列的安全攻击，获取用户的信息。用户通过在 WIPS 中配置热点文件，来指定 WIPS 对使用这些热点的 AP 和信任的无线客户端进行热点攻击检测。

- 绿野模式

当无线设备使用 802.11n 绿野模式时，不可以和其他 802.11a/b/g 设备共享同一个信道。通常当一台设备侦听到有其他设备占用信道发送和接收报文的时候，会延迟报文的发送直到信道空闲时再发

送。但是 802.11a/b/g 设备不能和绿野模式的 AP 进行通信，无法被告知绿野模式的 AP 当前信道是否空闲，会立刻发送自己的报文。这可能会导致报文发送冲突、差错和重传。

- 关联/重关联 DoS 攻击

关联/重关联 DoS 攻击通过模拟大量的客户端向 AP 发送关联请求/重关联请求帧，使 AP 的关联列表中存在大量虚假的客户端，达到拒绝合法客户端接入的目的。

- 中间人

在中间人攻击中，攻击者在合法 AP 和合法客户端的数据通路中间架设自己的设备，并引诱合法客户端下线并关联到攻击者的设备上，此时攻击者就可以劫持合法客户端和合法 AP 之间的会话。在这种情况下，攻击者可以删除，添加或者修改数据包内的信息，获取验证密钥、用户密码等机密信息。中间人攻击是一种组合攻击，客户端在关联到蜜罐 AP 后攻击者才会发起中间人攻击，所以在配置中间人攻击检测之前需要开启蜜罐 AP 检测。

- 无线网桥

攻击者可以通过接入无线网桥侵入公司网络的内部，对网络安全造成隐患。WIPS 通过检测无线网络环境中是否存在无线网桥数据以确定周围环境中是否存在无线网桥。当检测到无线网桥时，WIPS 系统即产生告警，提示当前无线网络环境存在安全隐患。如果该无线网桥是 Mesh 网络时，则记录该 Mesh 链路。

- AP 信道变化

AP 设备在完成部署后通常是固定不动的，正常情况下 WIPS 通过检测发现网络环境的中 AP 设备的信道是否发生变化。

- 广播解除关联帧/解除认证帧

当攻击者仿冒成合法的 AP，发送目的 MAC 地址为广播地址的解除关联帧或者解除认证帧时，会使合法 AP 下关联的客户端下线，对无线网络造成攻击。

- AP 扮演者攻击

在 AP 扮演者攻击中，攻击者会安装一台恶意 AP 设备，该 AP 设备的 BSSID 和 ESSID 与真实 AP 一样。当该恶意 AP 设备在无线环境中成功扮演了真实 AP 的身份后，就可以发起热点攻击，或欺骗检测系统。WIPS 通过检测收到 Beacon 帧的间隔小于 Beacon 帧中携带的间隔值次数达到阈值来判断其是否为攻击者扮演的恶意 AP。

- AP 泛洪

AP 设备在完成部署后通常是固定不动的，正常情况下 WIPS 通过检测发现网络环境的中 AP 设备的数目达到稳定后不会大量增加。当检测到 AP 的数目超出预期的数量时， WIPS 系统即产生告警，提示当前无线网络环境存在安全隐患。

- 蜜罐 AP

攻击者在合法 AP 附近搭建一个蜜罐 AP，通过该 AP 发送与合法 AP SSID 相似的 Beacon 帧或 Probe Response 帧，蜜罐 AP 的发送信号可能被调得很大以诱使某些授权客户端与之关联。当有客户端连接到蜜罐 AP，蜜罐 AP 便可以向客户端发起某些安全攻击，如端口扫描或推送虚假的认证页面来骗取客户端的用户名及密码信息等。因此，需要检测无线环境中对合法设备构成威胁的蜜罐 AP。WIPS 系统通过对外部 AP 使用的 SSID 进行分析，若与合法 SSID 的相似度值达到一定阈值就发送蜜罐 AP 告警。

- 节电攻击

对于处于非节电模式下的无线客户端，攻击者可以通过发送节电模式开启报文（Null 帧），诱使 AP 相信与其关联的无线客户端始终处于睡眠状态，并为该无线客户端暂存帧。被攻击的无线客户端因为处于非节电模式而无法获取这些暂存帧，在一定的时间之后暂存帧会被自动丢弃。WIPS 通过检测节电模式开启/关闭报文的比例判断是否存在节电攻击。

- 软 AP

软 AP 是指客户端上的无线网卡在应用软件的控制下对外提供 AP 的功能。攻击者可以利用这些软 AP 所在的客户端接入公司网络，并发起网络攻击。WIPS 通过检测某个 MAC 地址在无线客户端和 AP 这两个角色上的持续活跃时长来判断其是否是软 AP，不对游离的客户端进行软 AP 检测。

- 非法信道

用户可以设置合法信道集合，并开启非法信道检测，如果 WIPS 在合法信道集合之外的其它信道上监听到无线通信，则认为在监听到无线通信的信道上存在入侵行为。

1.6.5 Signature检测

Signature 检测是指用户可以根据实际的网络状况来配置 Signature 规则，并通过该规则来实现自定义攻击行为的检测。WIPS 利用 Sensor 监听无线信道来获取无线报文，通过报文解析，检测出具有某些自定义类型特征的报文，并将分析检测的结果进行归类处理。

每个 Signature 检测规则中最多支持配置 6 条子规则，分别对报文的 6 种特征进行定义和匹配。当 AC 解析报文时，如果发现报文的特征能够与已配置的子规则全部匹配，则认为该报文匹配该自定义检测规则，AC 将发送告警信息或记录日志。

可以通过子规则定义的 6 种报文特征包括：

- 帧类型
- MAC 地址
- 序列号
- SSID
- SSID 长度
- 自定义报文位置

1.6.6 反制

在无线网络中设备分为两种类型：非法设备和合法设备。非法设备可能存在安全漏洞或被攻击者操纵，因此会对用户网络的安全造成严重威胁或危害。反制功能可以对这些设备进行攻击使其他无线终端无法关联到非法设备。

1.6.7 配置忽略告警信息的MAC地址列表

对于可以忽略 WIPS 告警信息的设备列表中的无线设备，WIPS 仍然会对其做正常的监测，但是不会产生与该设备相关的任何 WIPS 告警信息。

1.7 黑白名单

1.7.1 黑白名单简介

无线网络很容易受到各种网络威胁的影响，非法设备对于无线网络来说是一个很严重的威胁，因此需要对客户端的接入进行控制。通过黑名单和白名单功能来过滤客户端，对客户端进行控制，防止非法客户端接入无线网络，可以有效的保护企业网络不被非法设备访问，从而保证无线网络的安全。

1. 白名单

白名单定义了允许接入无线网络的客户端 MAC 地址表项，不在白名单中的客户端不允许接入。白名单表项只能手工添加和删除。

2. 黑名单

黑名单定义了禁止接入无线网络的客户端 MAC 地址表项，在黑名单中的客户端不允许接入。黑名单分为静态黑名单和动态黑名单，以下分别介绍。

(1) 静态黑名单

用户手工添加、删除的黑名单称为静态黑名单，当无线网络明确拒绝某些客户端接入时，可以将这些客户端加入静态黑名单。

(2) 动态黑名单

设备通过检测而自动生成和删除的黑名单称为动态黑名单，当 AP 检测到来自某一客户端的攻击报文时，会将该客户端的 MAC 地址动态加入到动态黑名单中，在动态黑名单表项老化时间内拒绝该客户端接入无线网络。

1.7.2 黑白名单过滤机制

当收到客户端关联请求报文或 AP 发送的 Add mobile 报文时，AC 将使用白名单和黑名单对客户端的 MAC 地址进行过滤。静态黑名单和白名单对所有与 AC 相连的 AP 生效，而动态黑名单只会对接收到攻击报文的 AP 生效。具体的过滤机制如下：

- 当 AC 上存在白名单时，将判断客户端的 MAC 地址是否在白名单中，如果在白名单中，则允许客户端通过任意 AP 接入无线网络，否则将拒绝该客户端接入。
- 当 AC 上不存在白名单时，则首先判断客户端的 MAC 地址是否在静态黑名单中，如果客户端在静态黑名单中，则拒绝该客户端通过任何 AP 接入无线网络。如果该客户端不在静态黑名单中，则继续判断其是否在动态黑名单中。如果在动态黑名单中，则不允许该客户端通过动态黑名单中指定的 AP 接入无线网络，但可以通过其它 AP 接入；如果不在动态黑名单中，则允许客户端通过任意 AP 接入。

1.8 射频管理

射频是一种高频交流变化电磁波，表示具有远距离传输能力、可以辐射到空间的电磁频率。WLAN 是利用射频作为传输媒介，进行数据传输无线通信技术之一。

射频的频率介于 300KHz 和约 300GHz 之间，WLAN 使用的射频频率范围为 2.4GHz 频段（2.4GHz～2.4835GHz）和 5GHz 频段（5.150GHz～5.350GHz 和 5.725GHz～5.850GHz）。

1.8.1 射频模式

按 IEEE 定义的 802.11 无线网络通信标准划分，射频模式主要有 802.11a、802.11b、802.11g、802.11n 和 802.11ac：

- 802.11a：工作频率为 5GHz，由于选择了 OFDM（Orthogonal Frequency Division Multiplexing，正交频分复用）技术，能有效降低多路径衰减的影响和提高频谱的利用率，使 802.11a 的物理层速率可达 54Mbps。但是在传输距离上存在劣势。
- 802.11b：工作频率为 2.4GHz，相比 5GHz 能够提供更大的传输距离，数据传输速率最高达 11Mbps。由于早期的无线通信更加追求传输距离，所以 802.11b 比 802.11a 更早被投入使用。
- 802.11g：工作频率为 2.4GHz，可以兼容 802.11b。802.11g 借用了 802.11a 的成果，在 2.4GHz 频段采用了 OFDM 技术，最高速率可以达到 54Mbps。
- 802.11n：工作于双频模式（2.4GHz 和 5GHz 两个工作频段），能够与 802.11a/g 标准兼容。802.11n 的数据传输速率达 100Mbps 以上，理论最高可达 600Mbps，使无线局域网平滑地和有线网络结合，全面提升了网络吞吐量。
- 802.11ac：是 802.11n 的继承者，理论最高速率可达 6900Mbps，全面提升了网络吞吐量。

表1-1 WLAN 的几种主要射频模式比较

协议	频段	最大速度	范围（室内）	范围（室外）
802.11a	5GHz	54Mbps	约50米	约100米
802.11b	2.4GHz	11Mbps	约300米	约600米
802.11g	2.4GHz	54Mbps	约300米	约600米
802.11n	2.4GHz/5GHz	600Mbps	约300米	约600米
802.11ac	5GHz	6900Mbps	约30米	约60米

不同的射频模式所支持的信道、功率有所不同，所以射频模式修改时，如果新的射频模式不支持原来配置的的信道、功率，则 AP 会根据新射频模式自动调整这些参数。

注意

修改射频模式时，会导致当前在线客户端下线。

在指定了射频模式以后，可以进行射频功能配置，具体情况如下：

- 如果指定的射频模式为 **802.11a**、**802.11b**或 **802.11g**，则可以配置射频基础功能，有关射频基础功能配置的详细介绍，请参见“射频基础功能”
- 如果指定的射频模式为 **802.11n**，则可以配置射频基础功能和 802.11n功能，有关 802.11n功能配置的详细介绍，请参见“802.11n功能”。
- 如果指定的射频模式为 **802.11ac**，则可以配置射频基础功能、802.11n功能和 802.11ac功能，有关 802.11ac功能配置的详细介绍，请参见“802.11ac功能”。

1.8.2 信道

信道是具有一定频宽的射频。在 WLAN 标准协议里，2.4GHz 频段被划分为 13 个相互交叠的信道，每个信道的频宽是 20MHz，信道间隔为 5MHz。这 13 个信道里有 3 个独立信道，即没有相互交叠的信道，目前普遍使用的三个互不交叠的独立信道号为 1、6、11。

5GHz 频段拥有更高的频率和频宽，可以提供更高的速率和更小的信道干扰。WLAN 标准协议将 5GHz 频段分为 24 个频宽为 20MHz 的信道，且每个信道都为独立信道。各个国家开放的信道不一样，目前中国 5GHz 频段开放使用的信道号是 36、40、44、48、52、56、60、64、149、153、157、161 和 165。

1.8.3 功率

射频功率是指天线在无线介质中所辐射的功率，反映的是 WLAN 设备辐射信号的强度。射频功率越大，射频覆盖的范围越广，客户端在同一位置收到的信号强度越强，也就越容易干扰邻近的网络。随着传输距离的增大，信号强度随之衰减。

1.8.4 速率

射频速率是客户端与 WLAN 设备之间的数据传输速度。不同的射频模式，根据所使用扩频、编码和调制技术，对应不同的传输速率。802.11a、802.11b、802.11g、802.11n 和 802.11ac 的速率支持情况如下：

- 802.11a：6Mbps、9Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、54Mbps。
- 802.11b：1Mbps、2Mbps、5.5Mbps、11Mbps。
- 802.11g：1Mbps、2Mbps、5.5Mbps、6Mbps、9Mbps、11Mbps、12Mbps、18Mbps、24Mbps、36Mbps、48Mbps、54Mbps。
- 802.11n：根据不同信道带宽可支持不同的速率组合，具体请参见“MCS”
- 802.11ac：根据不同信道带宽和空间流数量可支持不同的速率组合，具体请参见“VHT-MCS”。

1.8.5 MCS

IEEE 802.11n 除了向前兼容 IEEE 802.11a/b/g 的速率外，还定义了新的速率调制与编码策略，即 MCS（Modulation and Coding Scheme，调制与编码策略）。

无线数据传输的物理速率受到编码方式、调制方式、载波比特率、空间流数量、数据子信道数等多种因素的影响，不同的因素组合将产生不同的物理速率。MCS 使用索引的方式将每种组合以及由该组合产生的物理速率进行排列，形成索引值与速率的对应表，称为 MCS 表。802.11n 的 MCS 表共有两个子表，分别用于保存信道带宽为 20MHz 和 40MHz 时的物理速率。索引值的取值范围为 0～76，能够描述 77 种物理速率，两个 MCS 子表中的索引值相互独立。

802.11n规定，当带宽为 20MHz时，MCS0～15 为AP必须支持的MCS索引，MCS0～7 是客户端必须支持的MCS索引，其余MCS索引均为可选速率。表 1-2 和 表 1-3 分别列举了带宽为 20MHz和带宽为 40MHz的MCS速率表。

说明

完整的 MCS 对应速率表可参见 IEEE 802.11n-2009 标准协议。

表1-2 MCS 对应速率表（20MHz）

MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	1	BPSK	6.5	7.2
1	1	QPSK	13.0	14.4
2	1	QPSK	19.5	21.7
3	1	16-QAM	26.0	28.9
4	1	16-QAM	39.0	43.3
5	1	64-QAM	52.0	57.8
6	1	64-QAM	58.5	65.0
7	1	64-QAM	65.0	72.2
8	2	BPSK	13.0	14.4
9	2	QPSK	26.0	28.9
10	2	QPSK	39.0	43.3
11	2	16-QAM	52.0	57.8
12	2	16-QAM	78.0	86.7
13	2	64-QAM	104.0	115.6
14	2	64-QAM	117.0	130.0
15	2	64-QAM	130.0	144.4

表1-3 MCS 对应速率表（40MHz）

MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	1	BPSK	13.5	15.0
1	1	QPSK	27.0	30.0
2	1	QPSK	40.5	45.0
3	1	16-QAM	54.0	60.0
4	1	16-QAM	81.0	90.0
5	1	64-QAM	108.0	120.0
6	1	64-QAM	121.5	135.0
7	1	64-QAM	135.0	150.0

MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
8	2	BPSK	27.0	30.0
9	2	QPSK	54.0	60.0
10	2	QPSK	81.0	90.0
11	2	16-QAM	108.0	120.0
12	2	16-QAM	162.0	180.0
13	2	64-QAM	216.0	240.0
14	2	64-QAM	243.0	270.0
15	2	64-QAM	270.0	300.0

从表中可以得到结论：

- 当 MSC 索引取值为 0～7 时，空间流数量为 1，且当 MCS＝7 时，速率值最大；
- 当 MSC 索引取值为 8～15 时，空间流数量为 2，且当 MCS＝15 时，速率值最大。

MCS 分为三类：

- 基本 MCS 集：客户端必须支持的基本 MCS 集，才能够与 AP 以 802.11n 模式进行连接。
- 支持 MCS 集：AP 所能够支持的更高的 MCS 集合，用户可以配置支持 MCS 集让客户端在支持基本 MCS 的前提下选择更高的速率与 AP 进行数据传输。
- 组播 MCS 集：AP 以组播方式对其 BSS 内的客户端发送消息所使用的速率。

1.8.6 VHT-MCS

802.11ac中定义的VHT-MCS表在表项内容上与 802.11n的MCS表完全相同，只是在子表划分方式上存在区别，VHT-MCS根据信道带宽和空间流数量的组合来划分子表。802.11ac支持 20MHz、40MHz、80MHz和 160MHz（80+80MHz）四种带宽，最多支持 8 条空间流，因此VHT-MCS表共划分为 32 个子表。每个子表中的MCS索引独立编号，目前编号范围为 0～9。AP支持的VHT-MCS表仅有 12 套，具体如 表 1-4～表 1-15 所示。

说明

完整的 VHT-MCS 对应速率表可参见 IEEE 802.11ac-2013 标准协议。

表1-4 VHT-MCS 对应速率表（20MHz，1NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	1	BPSK	6.5	7.2
1	1	QPSK	13.0	14.4
2	1	QPSK	19.5	21.7
3	1	16-QAM	26.0	28.9

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
4	1	16-QAM	39.0	43.3
5	1	64-QAM	52.0	57.8
6	1	64-QAM	58.5	65.0
7	1	64-QAM	65.0	72.2
8	1	256-QAM	78.0	86.7
9	Not valid			

表1-5 VHT-MCS 对应速率表（20MHz，2NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	2	BPSK	13.0	14.4
1	2	QPSK	26.0	28.9
2	2	QPSK	39.0	43.3
3	2	16-QAM	52.0	57.8
4	2	16-QAM	78.0	86.7
5	2	64-QAM	104.0	115.6
6	2	64-QAM	117.0	130.0
7	2	64-QAM	130.0	144.4
8	2	256-QAM	156.0	173.3
9	Not valid			

表1-6 VHT-MCS 对应速率表（20MHz，3NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	3	BPSK	19.5	21.7
1	3	QPSK	39.0	43.3
2	3	QPSK	58.5	65.0
3	3	16-QAM	78.0	86.7
4	3	16-QAM	117.0	130.0
5	3	64-QAM	156.0	173.3
6	3	64-QAM	175.5	195.0
7	3	64-QAM	195.0	216.7
8	3	256-QAM	234.0	260.0

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
9	3	256-QAM	260.0	288.9

表1-7 VHT-MCS 对应速率表（20MHz，4NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	4	BPSK	26.0	28.9
1	4	QPSK	52.0	57.8
2	4	QPSK	78.0	86.7
3	4	16-QAM	104.0	115.6
4	4	16-QAM	156.0	173.3
5	4	64-QAM	208.0	231.1
6	4	64-QAM	234.0	260.0
7	4	64-QAM	260.0	288.9
8	4	256-QAM	312.0	346.7
9	Not valid			

表1-8 VHT-MCS 对应速率表（40MHz，1NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	1	BPSK	13.5	15.0
1	1	QPSK	27.0	30.0
2	1	QPSK	40.5	45.0
3	1	16-QAM	54.0	60.0
4	1	16-QAM	81.0	90.0
5	1	64-QAM	108.0	120.0
6	1	64-QAM	121.5	135.0
7	1	64-QAM	135.0	150.0
8	1	256-QAM	162.0	180.0
9	1	256-QAM	180.0	200.0

表1-9 VHT-MCS 对应速率表（40MHz，2NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	2	BPSK	27.0	30.0
1	2	QPSK	54.0	60.0
2	2	QPSK	81.0	90.0
3	2	16-QAM	108.0	120.0
4	2	16-QAM	162.0	180.0
5	2	64-QAM	216.0	240.0
6	2	64-QAM	243.0	270.0
7	2	64-QAM	270.0	300.0
8	2	256-QAM	324.0	360.0
9	2	256-QAM	360.0	400.0

表1-10 VHT-MCS 对应速率表（40MHz，3NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	3	BPSK	40.5	45.0
1	3	QPSK	81.0	90.0
2	3	QPSK	121.5	135.0
3	3	16-QAM	162.0	180.0
4	3	16-QAM	243.0	270.0
5	3	64-QAM	324.0	360.0
6	3	64-QAM	364.5	405.0
7	3	64-QAM	405.0	450.0
8	3	256-QAM	486.0	540.0
9	3	256-QAM	540.0	600.0

表1-11 VHT-MCS 对应速率表（40MHz，4NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	4	BPSK	54.0	60.0
1	4	QPSK	108.0	120.0
2	4	QPSK	162.0	180.0
3	4	16-QAM	216.0	240.0

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
4	4	16-QAM	324.0	360.0
5	4	64-QAM	432.0	480.0
6	4	64-QAM	486.0	540.0
7	4	64-QAM	540.0	600.0
8	4	256-QAM	648.0	720.0
9	4	256-QAM	720.0	800.0

表1-12 VHT-MCS 对应速率表（80MHz，1NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	1	BPSK	29.3	32.5
1	1	QPSK	58.5	65.0
2	1	QPSK	87.8	97.5
3	1	16-QAM	117.0	130.0
4	1	16-QAM	175.5	195.0
5	1	64-QAM	234.0	260.0
6	1	64-QAM	263.0	292.5
7	1	64-QAM	292.5	325.0
8	1	256-QAM	351.0	390.0
9	1	256-QAM	390.0	433.3

表1-13 VHT-MCS 对应速率表（80MHz，2NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	2	BPSK	58.5	65.0
1	2	QPSK	117.0	130.0
2	2	QPSK	175.5	195.0
3	2	16-QAM	234.0	260.0
4	2	16-QAM	351.0	390.0
5	2	64-QAM	468.0	520.0
6	2	64-QAM	526.5	585.0
7	2	64-QAM	585.0	650.0
8	2	256-QAM	702.0	780.0

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
9	2	256-QAM	780.0	866.7

表1-14 VHT-MCS 对应速率表（80MHz，3NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	3	BPSK	87.8	97.5
1	3	QPSK	175.5	195.0
2	3	QPSK	263.3	292.5
3	3	16-QAM	351.0	390.0
4	3	16-QAM	526.5	585.0
5	3	64-QAM	702.0	780.0
6	Not valid			
7	3	64-QAM	877.5	975.0
8	3	256-QAM	1053.0	1170.0
9	3	256-QAM	1170.0	1300.0

表1-15 VHT-MCS 对应速率表（80MHz，4NSS）

VHT-MCS 索引	空间流数量	调制方式	速率(Mb/s)	
			800ns GI	400ns GI
0	4	BPSK	117.0	130.0
1	4	QPSK	234.0	260.0
2	4	QPSK	351.0	390.0
3	4	16-QAM	468.0	520.0
4	4	16-QAM	702.0	780.0
5	4	64-QAM	936.0	1040.0
6	4	64-QAM	1053.0	1170.0
7	4	64-QAM	1170.0	1300.0
8	4	256-QAM	1404.0	1560.0
9	4	256-QAM	1560.0	1733.3

和 MCS 一样，VHT-MCS 也分为三类：基本 VHT-MCS 集、支持 VHT-MCS 集和组播 VHT-MCS 集，每类的意义也和 MCS 相同。

1.8.7 射频基础功能

1. 射频工作信道

配置射频工作信道的目的是尽量减少和避免射频的干扰。干扰主要来自两方面：一种是 WLAN 设备间的干扰，比如相邻 WLAN 设备使用相同信道，会造成相互干扰；另一种是 WLAN 设备和其他无线射频之间的干扰，比如 WLAN 设备使用的信道上有雷达信号则必须立即让出该信道。

射频工作的信道可以手工配置或者由系统自动选择。

- 如果用户配置了手工信道，所配置的信道将一直被使用而不能自动更改，除非发现雷达信号。如果因为发现雷达信号而进行信道切换，AP 会在 30 分钟后将信道切换回手工指定的信道，并静默一段时间，如果在静默时间内没有发现雷达信号，则开始使用该信道；如果发现雷达信号，则再次切换信道。
- AP 默认采用自动信道模式，随机选择工作信道。

2. 射频最大传输功率

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。

3. 功率锁定

如果先开启功率调整，再配置功率锁定，AC 会自动将当前传输功率设置并锁定为自动功率调整后的功率值，在 AC 重启后，AP 能继续使用锁定的功率调整值。

如果先配置功率锁定命令，后开启功率调整功能，由于功率已经被锁定，功率调整功能不会运行，所以在开启功率调整功能前，请确保功率没有被锁定。

功率锁定后，如果信道发生调整，并且锁定的功率值大于调整后使用信道支持的最大功率，设备会将功率值调整为信道支持的最大功率。

有关自动功率调整相关配置的详细介绍请参见“网络 > 无线配置 > 射频资源 > 射频优化”页面。

4. 射频速率

射频速率可以分为以下四种：

- 禁用速率：AP 禁用的速率。
- 强制速率：客户端关联 AP 时，AP 要求客户端必须支持的速率。
- 支持速率：AP 所支持的速率。客户端关联 AP 后，可以在 AP 支持的“支持速率集”中选用更高的速率发送报文。当受干扰、重传、丢包等影响较大时，AP 会自动降低对客户端的发送速率；当受影响较小时，AP 会自动升高对客户端的发送速率。
- 组播速率：AP 向客户端发送组播和广播报文的速率。组播速率必须在强制速率中选取，且只能配置一个速率值或由 AP 自动选择合适的速率。

5. 前导码类型


说明

只有 2.4GHz 射频，才支持配置前导码类型。

前导码是数据报文头部的一组 Bit 位，用于同步发送端与接收端的传输信号。前导码的类型有两种，长前导码和短前导码。短前导码能使网络性能更好，默认使用短前导码。如果需要兼容网络中一些较老的客户端时可以使用长前导码保持兼容。

6. 射频覆盖范围

天线发出的电磁波在介质中传播的时候，随着距离的增加以及周围环境因素的影响，信号强度逐渐降低。电磁波的覆盖范围主要与环境的开放程度、障碍物的材质类型有关。设备在不加外接天线的情况下，传输距离约 300 米，若空间中有隔离物，传输大约在 35～50 米左右。

如果借助于外接天线，覆盖范围则可以达到 30～50 公里甚至更远，这要视天线本身的增益而定。

7. 发送Beacon帧的时间间隔

在 WLAN 环境中，AP 通过不断广播 Beacon 帧来让客户端发现自己。AP 发送 Becaon 帧时间间隔越小，AP 越容易被客户端发现，但 AP 的功耗越大。

8. 禁止 802.11b客户端接入

当射频模式为 802.11g 或 802.11gn 时，为了提高传输速率，可以通过开启禁止 802.11b 客户端接入功能来隔离低速率的 802.11b 客户端的影响；当开启禁止 802.11b 客户端接入功能后，不允许客户端以 802.11b 模式接入。

9. RTS门限

在无线环境中，为了避免冲突的产生，无线设备在发送数据前会执行冲突避免，即使用 RTS/CTS（Request to Send/Clear to Send，请求发送/允许发送）帧或 CTS-to-self（反身 CTS）帧来清空传送区域，取得信道使用权。但是如果每次发送数据前都执行冲突避免，则会降低过多的传输量，浪费了无线资源。因此，802.11 协议规定仅当发送帧长超过 RTS 门限的帧时，需要执行冲突避免；帧长小于 RTS 门限的帧，则可以直接发送。

当网络中设备较少时，产生干扰的概率较低，可以适当增大 RTS 门限以减少冲突避免的执行次数，提高吞吐量。当网络中设备较多时，可以通过降低 RTS 门限，增加冲突避免的执行次数来减少干扰。

10. 802.11g保护功能

说明

只有当射频**模式**为 802.11g 或 802.11n（2.4GHz）时，才支持配置 802.11g 保护功能。

当网络中同时存在 802.11b 和 802.11g 的客户端，由于调制方式不同，802.11b 客户端无法解析 802.11g 信号，会导致 802.11b 与 802.11g 网络之间彼此造成干扰。802.11g 保护功能用于避免干扰情况的发生，通过使 802.11g 和 802.11n 设备发送 RTS/CTS 报文或 CTS-to-self 报文来取得信道使用权，确保 802.11b 客户端能够检测到 802.11g 和 802.11n 客户端正在进行数据传输，实现冲突避免。

开启 802.11g 保护功能后，当 AP 在其工作信道上扫描到 802.11b 信号，则会在传输数据前通过发送 RTS/CTS 报文或 CTS-to-self 报文进行冲突避免，并通知客户端开始执行 802.11g 保护功能；如果未检测到 802.11b 信号，则不会采取上述动作。

当 802.11b 客户端在开启了 802.11g 或 802.11n（2.4GHz）的 AP 上接入时，AP 上的 802.11g 保护功能将自动开启并生效。

11. 帧的分片门限

帧的分片是将一个较大的帧分成更小的分片，每个分片独立进行传输和确认。当帧的实际大小超过指定的分片门限值时，该帧将被分片传输。

在干扰较大的无线环境，建议适当降低帧的分片门限值，增加帧的分片数量，则当传输受到干扰时，仅需要重传未成功发送的分片，从而提高吞吐量。

12. 帧的最大重传次数

在无线网络中传输的单播数据，必须得到接收端的应答，否则便认为传送失败。设备会对传送失败的帧进行重传，如果在达到最大重传次数时，仍然没有传送成功，则丢弃该帧，并将此状况告知上层协议。

每个帧或帧片段都分别对应一个重传计数器。无线设备上具有两个重传计数器：短帧重传计数器与长帧重传计数器。长度小于 RTS 门限值的帧视为短帧；长度超过 RTS 门限值的帧则为长帧。当帧传送失败，对应的重传计数器累加，然后重新传送帧，直至达到最大重传次数。

区分短帧和长帧的主要目的是为了让网络管理人员利用不同长度的帧来调整重传策略。由于发送长帧前需要执行冲突避免，因此长帧比短帧占用了更多的缓存空间和传输时间。在配置帧的最大重传次数时，适当减少长帧的最大重传次数，可以减少所需要的缓存空间和传输时间。

1.8.8 802.11n功能

说明

如果多个用户登录到 AC 设备上对某台 AP 配置 802.11n 功能，同一时间只有一个用户可以配置成功。

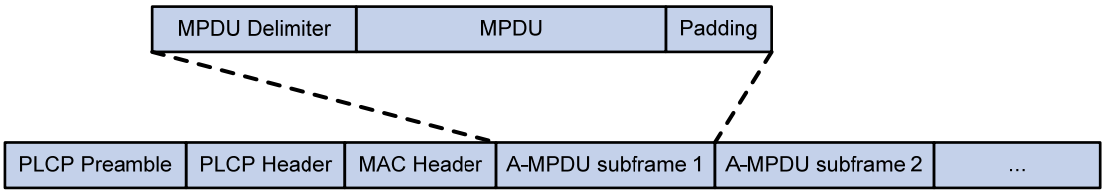
IEEE 802.11n 协议的制定，旨在提供高带宽、高质量的 WLAN 服务，使无线局域网达到以太网的性能水平。802.11n 通过物理层和 MAC（Media Access Control，媒体访问控制）层的优化来提高 WLAN 的吞吐能力，从而提高传输速率。

802.11n 的物理层建立在 OFDM 系统之上，采用 MIMO（Multiple Input,Multiple Output，多输入多输出）、40MHz 传输带宽、Short GI（Short Guard Interval，短保护间隔）、STBC（Space-Time Block Coding，空时块编码）、LDPC（Low-Density Parity Check，低密度奇偶校验）等技术使物理层达到高吞吐（High Throughput）的效果，并采用 A-MPDU（Aggregate MAC Protocol Data Unit，聚合 MAC 协议数据单元）、A-MSDU（Aggregate MAC Service Data Unit，聚合 MAC 服务数据单元）、BA（Block Acknowledgment，块确认）等技术，提高 MAC 层的传输效率。

1. A-MPDU功能

802.11n 标准中采用 A-MPDU 聚合帧格式，减少了每个传输帧中的附加信息，同时也减少了所需要的 ACK 帧的数目，从而降低了协议的负荷，有效的提高了网络吞吐量。A-MPDU 是将多个 MPDU（MAC Protocol Data Unit，MAC 协议数据单元）聚合为一个 A-MPDU，这里的 MPDU 为经过 802.11 封装的数据报文。A-MPDU 抢占一次信道并使用一个 PLCP（Physical Layer Convergence Procedure，物理层汇聚协议）头来提升信道利用率。一个 A-MPDU 中的所有 MPDU 必须拥有相同的 QoS 优先级，由同一设备发送，并被唯一的一个设备接收。

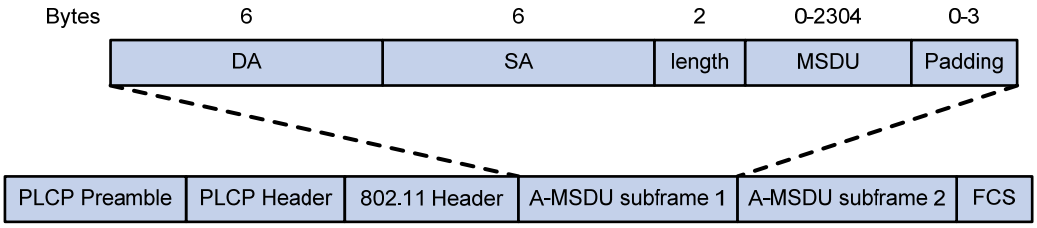
图1-5 A-MPDU 报文格式图



2. A-MSDU功能

A-MSDU 技术是指把多个 MSDU（MAC Service Data Unit，MAC 服务数据单元）聚合成一个较大的载荷。目前，MSDU 仅指 Ethernet 报文。通常，当 AP 或客户端从协议栈收到 MSDU 报文时，会封装 Ethernet 报文头，封装之后称之为 A-MSDU Subframe；而在通过射频发送出去前，需要一一将其转换成 802.11 报文格式。而 A-MSDU 技术旨在将若干个 A-MSDU Subframe 聚合到一起，并封装为一个 802.11 报文进行发送。从而减少了发送每一个 802.11 报文所需的 PLCP Preamble、PLCP Header 和 802.11MAC Header 的开销，提高了报文发送的效率。

图1-6 A-MSDU 报文格式图



A-MSDU 是将多个 MSDU 组合在一起发送，这些 MSDU 必须拥有相同的 QoS 优先级，而且必须由同一设备发送，并被唯一的一个设备接收。当一个设备接收到一个 A-MSDU 时，需要将这个 A-MSDU 分解成多个 MSDU 后分别处理。

3. Short-GI功能

Short GI 是 802.11n 针对 802.11a/g 所做的改进。射频在使用 OFDM 调制方式发送数据时，整个帧是被划分成不同的数据块进行发送的，为了数据传输的可靠性，数据块之间会有 GI（Guard Interval，保护间隔），用以保证接收侧能够正确的解析出各个数据块。无线信号的空间传输会因多径等因素在接收侧形成时延，如果后面的数据块发送的过快，会和前一个数据块形成干扰，GI 就是用来规避这个干扰的。802.11a/g 的 GI 时长为 800ns，在多径效应不严重时，可以使用 Short GI，Short GI 时长为 400ns，在使用 Short GI 的情况下，可提高 10%的传输速率。另外，Short GI 与带宽无关，支持 20MHz、40MHz 带宽。

4. LDPC功能

802.11n 引入了 LDPC（Low-Density Parity Check，低密度奇偶校验）机制，该机制通过校验矩阵定义了一类线性码，并在码长较长时需要校验矩阵满足“稀疏性”，即校验矩阵中 1 的个数远小于 0。在 802.11n 出现以前，所有以 OFDM 为调制方式的设备都使用卷积作为前向纠错码。802.11n 引入了 LDPC 校验码，将传输的信噪比增加到了 1.5 到 3dB 之间，使传输质量得到提升。对 LDPC 的支持需要设备间的协商，以保证设备双方都支持 LDPC 校验。

5. STBC功能

802.11n 引入了 STBC（Space-Time Block Coding，空时块编码）机制，该机制可以将空间流编码成时空流，是 802.11n 中使用的一个简单的可选的发送分集机制。该机制的优点是不要求客户端具有高的数据传输速率，就可以得到强健的链路性能。STBC 是完全开环的，不要求任何反馈或额外的系统复杂度，但是会降低效率。

6. MCS索引

当非 802.11n 客户端上线时，将使用基础速率传输单播数据。当 802.11n 客户端上线时，将使用 MCS 索引所代表的调制与编码策略传输单播数据。

当未配置组播 MCS 索引时，802.11n 客户端和 AP 之间将使用组播速率发送组播数据；当配置了组播 MCS 索引且客户端都是 802.11n 客户端时，AP 和客户端将使用组播 MCS 索引所代表的调制与编码策略传输组播数据。当配置了组播索引且存在非 802.11n 客户端时，AP 和客户端将使用基础模式的组播速率传输组播数据，即 802.11a/b/g 的组播速率。

需要注意的是：

- 组播 MCS 索引需要小于或等于最大基本 MCS 索引，最大基本 MCS 需要小于或等于最大支持 MCS 索引。
- 配置的 802.11n 基本 MCS 最大索引值 index 表示射频的 802.11n 基本 MCS 的最大索引值，即该射频的 802.11n 基本 MCS 集是 0～index。
- 配置的 802.11n 支持 MCS 最大索引值 index 表示射频的 802.11n 支持 MCS 的最大索引值，即该射频的 802.11n 支持 MCS 集是 0～index。
- 配置的 802.11n 组播 MCS 索引值 index 表示射频发送 802.11n 组播报文使用的 MCS 索引。

7. 仅允许 802.11n及 802.11ac客户端接入功能

开启仅允许 802.11n 及 802.11ac 客户端接入功能后，仅允许 802.11n 及 802.11ac 客户端接入，不允许 802.11a/b/g 客户端接入，可以隔离低速率的客户端的影响，提高 802.11n 设备的传输速率。

8. 802.11n信道带宽

802.11n 沿用了 802.11a/b/g 的信道结构。20MHz 信道划分为 64 个子信道，为了防止相邻信道干扰，在 802.11a/g 中，需预留 12 个子信道，同时，需用 4 个子信道充当导频（pilot carrier）以监控路径偏移，因此 20MHz 带宽的信道在 802.11a/g 中用于传输数据的子信道数为 48 个；而在 802.11n 中，只需预留 8 个子信道，加上充当导频的 4 个子信道，20MHz 带宽的信道在 802.11n 中用于传输数据的子信道数为 52 个，提高了传输速率。

802.11n 将两个相邻的 20MHz 带宽绑定在一起，组成一个 40MHz 通讯带宽（其中一个为主信道，另一个为辅信道）来提高传输速率。

射频的带宽配置及芯片的支持能力决定了射频工作在 20MHz 的带宽还是工作在 20/40MHz 的带宽。

9. MIMO模式

MIMO 是指一个天线采用多条流进行无线信号的发送和接收。MIMO 能够在不增加带宽的情况下成倍的提高信息吞吐量和频谱利用率。MIMO 模式包括以下四种：

- **1x1**：采用一条流进行无线信号的发送和接收。
- **2x2**：采用两条流进行无线信号的发送和接收。
- **3x3**：采用三条流进行无线信号的发送和接收。
- **4x4**：采用四条流进行无线信号的发送和接收。

支持流的数量与 AP 型号有关，请以设备的实际情况为准。

10. AP绿色节能功能

开启绿色节能功能后，在没有用户与 Radio 关联时，Radio 将工作在 1x1 模式（仅采用一条流进行无线信号的发送和接收），节省用电量。

11. 802.11n保护功能

说明

本功能所指的 802.11n 包括 802.11n 和 802.11ac。

当网络中同时存在 802.11n 和非 802.11n 的客户端，由于调制方式不同，非 802.11n 客户端无法解析 802.11n 信号，会导致非 802.11n 与 802.11n 网络之间彼此造成干扰。802.11n 保护功能用于避免干扰情况的发生，通过使 802.11n 设备发送 RTS/CTS 报文或 CTS-to-self 报文来取得信道使用权，确保非 802.11n 客户端能够检测到 802.11n 客户端正在进行数据传输，实现冲突避免。

开启 802.11n 保护功能后，当 AP 在其工作信道上扫描到非 802.11n 信号，则会在传输数据前通过发送 RTS/CTS 报文或 CTS-to-self 报文进行冲突避免，并通知客户端开始执行 802.11n 保护功能；如果未检测到非 802.11n 信号，则不会采取上述动作。

当非 802.11n 客户端在开启了 802.11n 或 802.11ac 的 AP 上接入时，AP 上的 802.11n 保护功能将自动开启并生效。

12. 智能天线功能

开启智能天线功能之后，AP 能够根据客户端的当前位置和信道信息，自动调整信号的发送参数，使射频能够集中发送至接收方所处的位置，从而提高客户端的信号质量和稳定性。

针对不同使用环境，本设备提供以下几种智能天线策略：

- 自适应策略：对语音视频等报文使用高可靠性策略，对其它报文使用高吞吐量策略。
- 高可靠性策略：优化噪声影响，抵抗局部干扰源，保证客户端带宽，降低客户端下线几率。本策略适用于对于带宽稳定要求较高的环境。
- 高吞吐量策略：提高收发信号强度，增加吞吐量。本策略适用于对于性能要求较高的环境。

1.8.9 802.11ac功能

说明

如果多个用户登录到 AC 设备上对某台 AP 配置 802.11ac 功能，同一时间只有一个用户可以配置成功。

802.11ac 是 802.11n 的继承者，它采用并扩展了源自 802.11n 的众多概念，包括更宽的射频带宽（提升至 160MHz）、更多的 MIMO 空间流（增加到 8）、多用户的 MIMO、以及更高阶的调制方式（达到 256QAM），从而进一步提高了 WLAN 的传输速率。

1. NSS

当802.11ac客户端上线时，将使用NSS（Number of Spatial Streams，空间流数）所对应的VHT-MCS索引所代表的调制与编码策略传输单播数据。

当非 802.11ac 客户端上线时，将使用基础速率或 MCS 所代表的调制与编码策略传输单播数据。

当未配置组播 NSS 时，802.11ac 客户端和 AP 之间将使用组播速率或组播 MCS 所代表的调制与编码策略发送组播数据。

当配置了组播 NSS 且客户端都是 802.11ac 客户端时，AP 和客户端将使用 VHT-MCS 索引所代表的调制与编码策略传输组播数据。

当配置了组播 NSS 且存在非 802.11ac 客户端时，AP 和客户端将使用基础模式的组播速率或 MCS 所代表的调制与编码策略传输组播数据，即 802.11a/b/g/n 的组播速率。

需要注意的是：

- 组播 NSS 需要小于或等于最大基本 NSS，最大基本 NSS 需要小于或等于最大支持 NSS。
- 配置的 802.11ac 基本 NSS 最大数值 number 表示射频的 802.11ac 最大基本 NSS，即该射频的 802.11ac 基本 NSS 是 1～number。
- 配置的 802.11ac 支持 NSS 最大数值 number 表示射频的 802.11ac 最大支持 NSS，即该射频的 802.11ac 支持 NSS 是 1～number。
- 配置的 802.11ac 组播 NSS 数值 number 表示射频发送 802.11ac 组播报文使用的 NSS。配置的 VHT-MCS 索引值 index 表示射频发送 802.11ac 组播报文使用的对应 NSS 的 VHT-MCS 索引。

2. 仅允许 802.11ac客户端接入功能

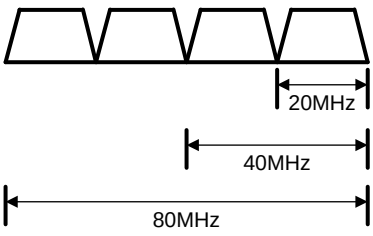
开启仅允许 802.11ac 客户端接入功能后，仅允许 802.11ac 客户端接入，不允许 802.11a/b/g/n 客户端接入，可以隔离低速率的客户端的影响，提高 802.11ac 设备的传输速率。

3. 802.11ac信道带宽

802.11ac 将信道带宽从 802.11n 的 20MHz/40MHz 提升到了 80MHz。带宽的提升带来了可用数据子载波的增加。

802.11ac 沿用了 802.11n 的信道带宽划定方式，通过将相邻的信道合并得到更大带宽的信道。在 802.11ac 中，可以将相邻的两个 20Mhz 信道合并得到带宽为 40Mhz 的信道，也可以将两个 40Mhz 带宽的信道合并，得到带宽为 80Mhz 的信道。

图1-7 802.11ac 信道带宽划定方式示意图



1.9 射频优化

WLAN RRM（Radio Resource Management，射频资源管理）是一种可升级的射频管理解决方案，通过“采集（AP 实时收集射频环境信息）—>分析（AC 对 AP 收集的数据进行分析评估）—>决策（根据分析结果，AC 统筹分配信道和发送功率）—>执行（AP 执行 AC 设置的配置，进行射频资源调优）”的方法，提供一套系统化的实时智能射频管理方案，使无线网络能够快速适应无线环境变化，保持最优的射频资源状态。WLAN RRM 主要通过信道调整和功率调整的方式来优化射频的服务质量。

1.9.1 信道调整

信道调整是指 AC 在调整周期到达时，通过计算信道质量，挑选出质量最优的信道应用到 Radio 上。影响信道质量的因素包括：

- 误码率：包括无线报文传输过程中物理层的误码率和 CRC 错误。
- 干扰：802.11 信号或非 802.11 信号对无线接入服务产生的影响。
- 重传：由于 AP 没有收到 ACK 报文造成的数据重传。
- 雷达信号：在工作信道上检测到雷达信号。在这种情况下，AC 会立即通知 AP 切换工作信道。

信道调整的工作流程如下：

(1) AC 检测当前工作信道，如果信道质量变差达到任意一个调整门限，则 AC 通过计算信道质量，挑选出质量最优的新信道。调整门限包括 CRC 错误门限、信道干扰门限和重传门限。

(2) AC 比较新旧信道的信道质量，只有在新旧信道的信道质量差超过容限系数时，AP 才会应用新信道。

1.9.2 功率调整

功率调整就是在整个无线网络的运行过程中，AC 能够根据实时的无线环境情况，动态地调整 Radio 的发送功率，使 Radio 的发送功率在能够覆盖足够范围的情况下减少对其他 Radio 的干扰。Radio 的发送功率增加或减少取决于以下因素：

- 邻居 Radio 数（邻居 Radio 指的是一个 Radio 能探测到的、由同一 AC 管理的其他 Radio）；
- 在邻居 Radio 的功率排名中指定 Radio；
- 指定邻居 Radio 接收到本 Radio 的功率值和设置的功率调整门限值的比较情况。

增加邻居 Radio 或某个邻居 Radio 发生故障或离线时，AP 会根据由邻居 Radio 的功率排名中指定 Radio 探测到本 AP 的 Radio 功率值和功率调整门限值的比较结果调整自身的发送功率。如果 AP 上某个 Radio 的邻居数达到触发功率调整的最大邻居数，AP 会根据以下原则来调整功率：

- 如果指定的邻居 Radio 接收到该 AP 上某 Radio 的功率大于配置的门限值，且差值超过 6，那么本 AP 会减小该 Radio 的功率。
- 如果指定的邻居 Radio 接收到该 AP 上某 Radio 的功率小于配置的门限值，且差值超过 3，那么本 AP 会增大该 Radio 的功率。

如果 Radio 的邻居 Radio 数小于触发功率调整的最大邻居数，AP 会将该 Radio 的功率调整到最大值。

AP 支持三种功率调整模式，它们分别适用于不同的无线环境：

- 自定义模式：缺省的功率调整模式，当覆盖模式与高密模式均无法达到理想效果时，可以通过手动配置功率调整参数来进行功率调整。
- 覆盖模式：该模式下功率调整方式偏向于扩大 AP 信号的覆盖范围，适用于 AP 数量较少的无线环境。
- 高密模式：该模式下的功率调整方式偏向于避免 AP 之间的信号干扰，适用于 AP 数量较多，存在大量信号重叠区域的无线环境。

高密模式和覆盖模式为系统预定义的功率调整模式，在这两种模式下，功率调整的相关参数为系统预设，不能修改。只有在自定义模式下，用户才能设置功率调整参数。

1.9.3 射频扫描

自动信道调整、自动功率调整功能处于关闭状态时，如果希望信道利用率与干扰率依旧能够实时显示，需要开启射频扫描功能。

开启射频扫描功能后，AP 将对无线环境进行扫描与数据采集工作，周期性的将数据上报给 AC，由 AC 生成信道报告和邻居报告，二者用于信道利用率、干扰率的统计。

1.9.4 RRM保持调整组

启用信道或功率调整功能后，每隔一定时间 AC 就会重新计算 Radio 的信道质量或功率大小，如果计算结果满足设定的调整条件，则会进行信道或功率的调整。但在某些干扰严重的环境，频繁调整信道或功率很可能会影响用户的正常使用。在这种情况下，可以通过配置 RRM 保持调整组，保证在一定时间内稳定 RRM 保持调整组内 Radio 的信道和功率。对于没有加入到 RRM 保持调整组的 Radio，其信道和功率将正常调整。

1.9.5 Baseline

Baseline（射频工作参数基线）保存了 Radio 的即时工作信道和传输功率，以及对应的射频参数信息。如果当前 Radio 的工作信道与功率值合适，则可以将 Radio 的信道、功率值存储为射频工作参数基线，在需要的时候重新应用这些保存的值。

射频工作参数基线保存、应用范围有三种：某 AP 下的一个 Radio、某 AP 组下同一型号 AP 的同一类型 Radio、同一 AC 下的所有 AP 的 Radio。

如果某个 Radio 满足下列条件之一，则射频工作参数基线中保存的工作信道与功率值均不会应用到对应的 Radio。

- 射频不存在；
- 射频状态为 Down；
- 射频工作参数基线中保存的射频类型与实际射频类型不匹配；
- 射频工作参数基线中保存的 AP 的区域码与实际情况不匹配；
- 无线服务未生效；
- 射频工作参数基线中保存的射频工作信道不合法；
- 射频工作参数基线中保存的射频带宽与实际射频带宽不匹配；
- 射频工作信道已手动配置为固定值；
- 工作信道被锁定；

- 当前工作信道处于信道保持调整期；
- 射频功率被锁定；
- 当前射频功率处于功率保持调整期；
- 射频工作参数基线中保存的射频功率小于配置的最小传输功率；
- 射频工作参数基线中保存的射频功率大于配置的最大传输功率。

1.10 负载均衡

1.10.1 负载均衡简介

WLAN 负载均衡用于在高密度无线网络环境中平衡 Radio 的负载，充分地保证每个 AP 的性能和无线客户端的带宽。

启动负载均衡的 WLAN 环境要求为：相互进行负载均衡的 AP 必须要连到同一 AC 上，并且客户端能扫描到相互进行负载均衡的 Radio，客户端接入的 SSID 快速关联功能处于关闭状态。

1.10.2 负载均衡类型

目前，AC 支持两种类型的负载均衡：基于 Radio 的负载均衡和基于负载均衡组的负载均衡。

- 基于 Radio 的负载均衡是针对 AC 上的所有 Radio 进行的负载均衡。
- 基于负载均衡组的负载均衡可以限制负载均衡的范围，在跨 AP 的多个 Radio 之间进行负载均衡。创建负载均衡组后，AC 将以负载均衡组为单位，在各个组内的 Radio 间进行会话模式、流量模式或带宽模式的负载均衡，没有加入到任何负载均衡组的 Radio 不会参与负载均衡。

1.10.3 负载均衡模式

- 会话模式：当 Radio 上的在线客户端数量达到或超过会话门限值并且与同一 AC 内其他 Radio 上的在线客户端数量最小者的差值达到或超过会话差值门限值，Radio 才会开始运行负载均衡。
- 流量模式：当 Radio 上的流量达到或超过流量门限值并且与同一 AC 内其他 Radio 上的流量最小者的差值达到或超过流量差值门限值，Radio 才会开始运行负载均衡。
- 带宽模式：当 Radio 上的带宽达到或超过带宽门限值并且与同一 AC 内其他 Radio 上的带宽最小者的差值达到或超过带宽差值门限值，Radio 才会开始运行负载均衡。

1.10.4 负载均衡参数

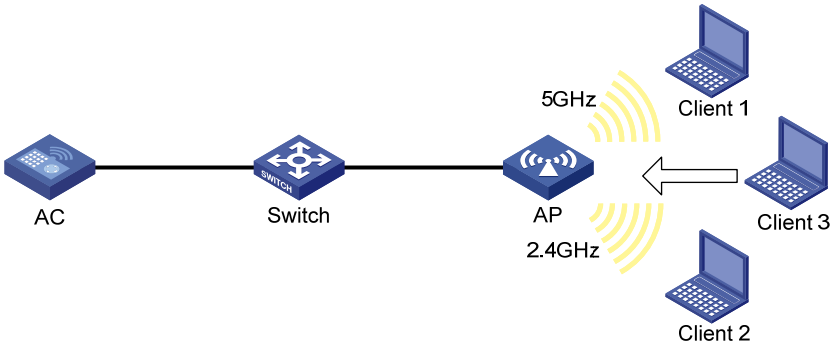
- 负载均衡 RSSI 门限：在进行负载均衡计算时，一个客户端可能会被多个 Radio 检测到，如果某个 Radio 检测到该客户端的 RSSI 值低于设定值，则该 Radio 将判定该客户端没有被检测到。如果只有过载的 Radio 可以检测到某客户端，其他 Radio 由于检测到该客户端的 RSSI 值低于设定值，将判定该客户端没有被检测到，则 AC 会通过让过载的 Radio 减少拒绝该客户端关联请求的最大次数，增大该客户端接入的概率。
- 设备拒绝客户端关联请求的最大次数：如果客户端反复向某个 Radio 发起关联请求，且 Radio 拒绝客户端关联请求次数达到设定的最大拒绝关联请求次数，那么该 Radio 会认为此时该客户端不能连接到其它任何的 Radio，在这种情况下， Radio 会接受该客户端的关联请求。

1.11 频谱导航

在实际无线网络环境中，有些客户端只能工作在 2.4GHz 频段上，有些客户端可以工作在 2.4GHz 频段或者 5GHz 频段，这有可能导致 2.4GHz 射频过载，5GHz 射频相对空余。在这种情况下，可以使用频谱导航功能，将支持双频工作的客户端优先接入 5GHz 射频，使得两个频段上的客户端数量相对均衡，从而提高整网性能。

如 图 1-8 所示，无线网络中存在三个客户端，AP上开启 5GHz射频和 2.4GHz射频，Client1 关联到AP的 5GHz射频，Client2 关联到AP的 2.4GHz射频。AC上开启频谱导航功能后，当Client3 准备接入无线网络时，如果对 5GHz射频进行关联，将直接关联成功，如果对 2.4GHz射频进行关联，将被AC拒绝。

图1-8 启动频谱导航的 WLAN 环境



1.12 探针

在 AP 的 Radio 接口上开启探针功能后，AP 通过对信道进行扫描，收集客户端信息并生成客户端表项，实现对客户端的监测。开启探针功能后，可以在“网络 > 监控 > 探针”页面中查看监测到的信息。

AP 的 Radio 接口不能同时开启 WIPS 功能和探针功能。

1.13 无线定位

无线定位技术是利用基于 WiFi 技术的 RFID（Radio Frequency Identification，射频识别）和支持 Wi-Fi 标准的设备发送的无线报文，实现对无线设备的定位、追踪和监测。目前，设备支持 AeroScout 定位、蓝牙定位、CUPID 定位和指纹定位四种定位方式。

1.13.1 无线定位系统的组成

无线定位系统由以下三类设备组成：

- 被定位的设备：可以向周围发送无线报文的设备，对于 AeroScout 定位来说，分为 Tag（AeroScout 公司生产的一种定位设备）和 MU（除 Tag 外的其他设备）两种类型。
- 定位信息接收设备：符合 802.11 标准要求的 AP 或其它接收设备。
- 定位服务器：运行定位软件的服务器。

定位信息接收设备将搜集到的定位信息发送到定位服务器，定位服务器通过软件计算出被定位设备的位置信息。

1.13.2 无线定位的工作过程简介

无线定位的工作过程为：

(1) AP 发现定位服务器

- 对于 AeroScout 定位，定位服务器在发起定位信息搜集时，首先向 AP 发起协商，通知 AP 需要搜集的设备类型，Tag 设备使用的组播地址等。AP 在收到定位服务器发送的报文后，会将报文中的 IP 地址和端口号保存，用来向定位服务器发送搜集到的定位信息。随后，AP 将开始搜集定位信息。
- 对于其他定位方式，AP 会根据配置的定位服务器地址发送收集到的定位信息。

(2) AP 搜集定位信息

AP 在收到由被定位设备发出的无线报文后，会将报文与搜集到的定位信息一起封装为定位协议的协议报文（下文中简称为定位报文）发送给定位服务器。

(3) 定位服务器进行定位计算

定位服务器收到定位报文后，提取报文中的定位信息并按照定位算法进行计算，得到被定位设备的位置信息。

1.13.3 接收报文相关处理

1. 信道匹配

在无线网络中，AP 可能收到非工作信道上的无线报文，由于 AP 接收到此类报文的 RSSI 要比报文所在信道的真实 RSSI 值低，不适合定位服务器进行定位计算。因此，AeroScout 定位方式中提供了信道匹配功能，AP 在接收到无线报文后，将按以下方法对 Tag 设备和 MU 设备进行信道匹配处理：

- Tag 设备会将每个无线报文在多个信道上进行发送，并且携带信道信息，以适应周围接收无线报文的不同 AP。AP 在收到无线报文后，将报文中携带的信道信息与当前工作信道进行比较，如果信道一致，则将该报文封装后发送给定位服务器，如果信道不一致，直接丢弃该报文。
- MU 设备发送的无线报文中不携带信道信息，由 AP 完成信道匹配难度较大，所以 AP 在收到 MU 设备发送的无线报文后，直接封装发送给定位服务器，由定位服务器完成信道匹配工作。

2. 报文稀释

由于 AP 需要将与自己关联和非关联的客户端定位报文都发送给定位服务器，报文数量可能非常庞大。通过报文稀释功能，可以有效减少 AP 向定位服务器发送的报文数量。报文稀释功能是指 AP 每收到一定数量的报文后，才会向定位服务器发送一个报文。例如，将稀释因子配置为 100，则 AP 在收到 100 个来自同一客户端的无线报文（不包括管理报文和广播报文）后，才会将其封装成定位报文并向定位服务器发送。

此外，在稀释超时时间内，若 AP 收到的报文数量没有达到稀释因子数，则将最近接收到的无线报文发送给定位服务器，避免报文搜集周期过长，影响定位的准确性。

2 网络安全

2.1 QoS策略

QoS 即服务质量。对于网络业务，影响服务质量的因素包括传输的带宽、传送的时延、数据的丢包率等。在网络中可以通过保证传输的带宽、降低传送的时延、降低数据的丢包率以及时延抖动等措施来提高服务质量。

QoS 策略包含了三个要素：类、流行为、策略。用户可以通过 QoS 策略将指定的类和流行为绑定起来，灵活地进行 QoS 配置。

2.1.1 类

类用来定义一系列的规则来对报文进行分类。

2.1.2 流行为

流行为用来定义针对报文所做的 QoS 动作。

2.1.3 策略

策略用来将指定的类和流行为绑定起来，对符合分类条件的报文执行流行为中定义的动作。

2.1.4 应用策略

QoS 策略支持以下应用方式：

- 基于接口应用 QoS 策略：QoS 策略对通过接口接收或发送的流量生效。接口的每个方向（出和入两个方向）只能应用一个策略。如果 QoS 策略应用在接口的出方向，则 QoS 策略对本地协议报文不起作用。一些常见的本地协议报文如下：链路维护报文等。
- 基于全局应用 QoS 策略：QoS 策略对所有流量生效。

2.2 优先级映射

报文在进入设备以后，设备会根据映射规则分配或修改报文的各种优先级的值，为队列调度和拥塞控制服务。

优先级映射功能通过报文所携带的优先级字段来映射其他优先级字段值，就可以获得决定报文调度能力的各种优先级字段，从而为全面有效的控制报文的转发调度等级提供依据。

2.2.1 端口优先级

如果配置了优先级信任模式，即表示设备信任所接收报文的优先级，会自动解析报文的优先级或者标志位，然后按照映射表映射到报文的优先级参数。

如果没有配置优先级信任模式，并且配置了端口优先级值，则表明设备不信任所接收报文的优先级，而是使用端口优先级，按照映射表映射到报文的优先级参数。

1. 配置端口优先级

按照接收端口的端口优先级，设备通过一一映射为报文分配优先级。

2. 配置优先级信任模式

根据报文自身的优先级，查找优先级映射表，为报文分配优先级参数，可以通过配置优先级信任模式的方式来实现。

在配置接口上的优先级模式时，用户可以选择下列信任模式：

- Untrust：不信任任何优先级。
- Dot1p：信任报文自带的 802.1p 优先级，以此优先级进行优先级映射。
- DSCP：信任 IP 报文自带的 DSCP 优先级，以此优先级进行优先级映射。

2.2.2 优先级映射表

报文在进入设备以后，设备会根据映射规则分配或修改报文的各种优先级的值，为队列调度和拥塞控制服务。

优先级映射功能通过报文所携带的优先级字段来映射其他优先级字段值，就可以获得决定报文调度能力的各种优先级字段，从而为全面有效的控制报文的转发调度等级提供依据。

设备中提供了三张优先级映射表，分别 802.1p 优先级到本地优先级映射表、DSCP 到 802.1p 优先级映射表和 DSCP 到 DSCP 映射表。如果缺省优先级映射表无法满足用户需求，可以根据实际情况对映射表进行修改。

2.3 802.1X

802.1X 协议是一种基于端口的网络接入控制协议，即在局域网接入设备的端口上对所接入的用户和设备进行认证，以便控制用户设备对网络资源的访问。

2.3.1 802.1X的体系结构

802.1X 系统中包括三个实体：

- 客户端：请求接入局域网的用户终端，由局域网中的设备端对其进行认证。客户端上必须安装支持 802.1X 认证的客户端软件。
- 设备端：局域网中控制客户端接入的网络设备，位于客户端和认证服务器之间，为客户端提供接入局域网的端口，并通过与认证服务器的交互来对所连接的客户端进行认证。
- 认证服务器端：用于对客户端进行认证、授权和计费，通常为 RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）服务器。认证服务器根据设备端发送来的客户端认证信息来验证客户端的合法性，并将验证结果通知给设备端，由设备端决定是否允许客户端接入。

2.3.2 802.1X的认证方法

在接入设备上，802.1X 认证方法有三种方式：

- CHAP 或 PAP 认证方法。在这种方式下，设备对 EAP 认证过程进行终结，将收到的 EAP 报文中的客户端认证信息封装在标准的 RADIUS 报文中，与服务器之间采用 PAP 或 CHAP 方法进行认证。CHAP 以密文的方式传送密码，而 PAP 是以明文的方式传送密码。

- EAP 认证方法。在这种方式下，设备端对收到的 EAP 报文进行中继，使用 EAPOR（EAP over RADIUS）封装格式将其承载于 RADIUS 报文中发送给 RADIUS 服务器。

2.3.3 接入控制方式

端口支持以下两种接入控制方式：

- 基于端口认证：只要该端口下的第一个用户认证成功后，其它接入用户无须认证就可使用网络资源，但是当第一个用户下线后，其它用户也会被拒绝使用网络。
- 基于 MAC 认证：该端口下的所有接入用户均需要单独认证，当某个用户下线后，也只有该用户无法使用网络。

2.3.4 授权状态

端口支持以下三种授权状态：

- 强制授权：表示端口始终处于授权状态，允许用户不经认证即可访问网络资源。
- 强制非授权：表示端口始终处于非授权状态。设备端不为通过该端口接入的客户端提供认证服务。
- 自动识别：表示端口初始状态为非授权状态，仅允许 EAPOL 报文收发，不允许用户访问网络资源；如果用户通过认证，则端口切换到授权状态，允许用户访问网络资源。

2.3.5 周期性重认证

该功能开启后，设备会根据周期性重认证时间间隔定期向该端口在线 802.1X 用户发起重认证，以检测用户连接状态的变化、确保用户的正常在线，并及时更新服务器下发的授权属性（例如 ACL、VLAN、User Profile）。

2.3.6 在线用户握手

该功能开启后，设备会根据周期发送握手请求报文时间间隔定期向通过 802.1X 认证的在线用户发送握手报文，以定期检测用户的在线情况。如果设备连续多次没有收到客户端的响应报文，则会将用户置为下线状态。

2.3.7 安全握手

在线用户握手功能处于开启状态的前提下，还可以通过开启在线用户握手安全功能，来防止在线的 802.1X 认证用户使用非法的客户端与设备进行握手报文的交互，而逃过代理检测、双网卡检测等 iNode 客户端的安全检查功能。

2.3.8 认证触发

设备端主动触发方式用于支持不能主动发送 EAPOL-Start 报文的客户端，例如 Windows XP 自带的 802.1X 客户端。设备主动触发认证的方式分为以下两种：

- 单播触发：当设备收到源 MAC 地址未知的报文时，主动向该 MAC 地址单播发送 Identity 类型的 EAP-Request 帧来触发认证。若设备端在设置的时长内没有收到客户端的响应，则重发该报文。

- 组播触发：设备每隔一定时间（缺省为 30 秒）主动向客户端组播发送 Identity 类型的 EAP-Request 帧来触发认证。

2.3.9 Auth-Fail VLAN

802.1X Auth-Fail VLAN 功能允许用户在认证失败的情况下访问某一特定 VLAN 中的资源。需要注意的是，这里的认证失败是认证服务器因某种原因明确拒绝用户认证通过，比如用户密码错误，而不是认证超时或网络连接等原因造成的认证失败。

1. 基于端口认证

在接入控制方式为基于端口认证的端口上配置 Auth-Fail VLAN 后，若该端口上有用户认证失败，则该端口会离开当前的 VLAN 被加入到 Auth-Fail VLAN，所有在该端口接入的用户将被授权访问 Auth-Fail VLAN 里的资源。

当加入 Auth-Fail VLAN 的端口上有用户发起认证并失败，则该端口将会仍然处于 Auth-Fail VLAN 内；如果认证成功，则该端口会离开 Auth-Fail VLAN，之后端口加入 VLAN 情况与认证服务器是否下发授权 VLAN 有关，具体如下：

若认证服务器下发了授权 VLAN，则端口加入下发的授权 VLAN 中。用户下线后，端口会离开下发的授权 VLAN，若端口上配置了 Guest VLAN，则加入 Guest VLAN，否则加入缺省 VLAN。

若认证服务器未下发授权 VLAN，则端口回到缺省 VLAN 中。用户下线后，端口仍在缺省 VLAN 中。

2. 基于MAC认证

在接入控制方式为基于 MAC 认证的端口上配置 Auth-Fail VLAN 后，该端口上认证失败的用户将被授权访问 Auth-Fail VLAN 里的资源。

当 Auth-Fail VLAN 中的用户再次发起认证时，如果认证成功，则设备会根据认证服务器是否下发 VLAN 决定将该用户加入到下发的授权 VLAN 中，或使其回到端口的缺省 VLAN 中；如果认证失败，则该用户仍然留在该 Auth-Fail VLAN 中。

2.3.10 Guest VLAN

802.1X Guest VLAN 功能允许用户在未认证的情况下，访问某一特定 VLAN 中的资源。

当端口上处于 Guest VLAN 中的用户发起认证且失败时：如果端口配置了 Auth-Fail VLAN，则该端口会被加入 Auth-Fail VLAN；如果端口未配置 Auth-Fail VLAN，则该端口仍然处于 Guest VLAN 内。

当端口上处于 Guest VLAN 中的用户发起认证且成功时，端口会离开 Guest VLAN，之后端口加入 VLAN 情况与认证服务器是否下发 VLAN 有关，具体如下：

若认证服务器下发 VLAN，则端口加入下发的 VLAN 中。用户下线后，端口离开下发的 VLAN 回到初始 VLAN 中，该初始 VLAN 为端口加入 Guest VLAN 之前所在的 VLAN。

若认证服务器未下发 VLAN，则端口回到初始 VLAN 中。用户下线后，端口仍在该初始 VLAN 中。

根据端口的接入控制方式不同，Guest VLAN 的生效情况有所不同。

1. 基于端口认证

在接入控制方式为基于端口认证的端口上配置 Guest VLAN 后，若全局和端口上都使能了 802.1X，端口授权状态为 auto，且端口处于激活状态，则该端口就被立即加入 Guest VLAN，所有在该端口接入的用户将被授权访问 Guest VLAN 里的资源。

2. 基于MAC认证

在接入控制方式为基于 MAC 认证的端口上配置 Guest VLAN 后，端口上未认证的用户将被授权访问 Guest VLAN 里的资源。

2.3.11 Critical VLAN

802.1X Critical VLAN 功能允许用户在认证时，当所有认证服务器都不可达的情况下访问某一特定 VLAN 中的资源。目前，只采用 RADIUS 认证方式的情况下，在所有 RADIUS 认证服务器都不可达后，端口才会加入 Critical VLAN。若采用了其它认证方式，则端口不会加入 Critical VLAN。

根据端口的接入控制方式不同，Critical VLAN 的生效情况有所不同。

1. 基于端口认证

在接入控制方式为基于端口认证的端口上配置 Critical VLAN 后，若该端口上有用户认证时，所有认证服务器都不可达，则该端口会被加入到 Critical VLAN，之后所有在该端口接入的用户将被授权访问 Critical VLAN 里的资源。在用户进行重认证时，若所有认证服务器都不可达，且端口指定在此情况下强制用户下线，则该端口也会被加入到 Critical VLAN。

已经加入 Critical VLAN 的端口上有用户发起认证时，如果所有认证服务器不可达，则端口仍然在 Critical VLAN 内；如果服务器可达且认证失败，且端口配置了 Auth-Fail VLAN，则该端口将会加入 Auth-Fail VLAN，否则回到端口的缺省 VLAN 中；如果服务器可达且认证成功，则该端口加入 VLAN 的情况与认证服务器是否下发 VLAN 有关，具体如下：

若认证服务器下发了授权 VLAN，则端口加入下发的授权 VLAN 中。用户下线后，端口会离开下发的授权 VLAN，若端口上配置了 Guest VLAN，则加入 Guest VLAN，否则加入缺省 VLAN。

若认证服务器未下发授权 VLAN，则端口回缺省 VLAN 中。用户下线后，端口仍在缺省 VLAN 中。

2. 基于MAC认证

在接入控制方式为基于 MAC 认证的端口上配置 Critical VLAN 后，若该端口上有用户认证时，所有认证服务器都不可达，则端口将允许 Critical VLAN 通过，用户将被授权访问 Critical VLAN 里的资源。

当 Critical VLAN 中的用户再次发起认证时，如果所有认证服务器不可达，则用户仍然在 Critical VLAN 中；如果服务器可达且认证失败，且端口配置了 Auth-Fail VLAN，则该用户将会加入 Auth-Fail VLAN，否则回到端口的缺省 VLAN 中；如果服务器可达且认证成功，则设备会根据认证服务器是否下发授权 VLAN 决定将该用户加入下发的授权 VLAN 中，或使其回到端口的缺省 VLAN 中。

2.3.12 端口的强制认证ISP域

在端口上指定强制认证域为 802.1X 接入提供了一种安全控制策略。所有从该端口接入的 802.1X 用户将被强制使用指定的认证域来进行认证、授权和计费，从而防止用户通过恶意假冒其它域账号从本端口接入网络。另外，管理员也可以通过配置强制认证域对不同端口接入的用户指定不同的认证域，从而增加了管理员部署 802.1X 接入策略的灵活性。

2.3.13 EAD快速部署

EAD（Endpoint Admission Defense，端点准入防御）作为一个网络端点接入控制方案，它通过安全客户端、安全策略服务器、接入设备以及第三方服务器的联动，加强了对用户的集中管理，提升

了网络的整体防御能力。但是在实际的应用过程中 EAD 客户端的部署工作量很大，例如，需要网络管理员手动为每一个 EAD 客户端下载、升级客户端软件，这在 EAD 客户端数目较多的情况下给管理员带来了操作上的不便。

802.1X 认证支持的 EAD 快速部署功能就可以解决以上问题，它允许未通过认证的 802.1X 用户访问一个指定的 IP 地址段（称为 Free IP），并可以将用户发起的 HTTP 访问请求重定向到该 IP 地址段中的一个指定的 URL，实现用户自动下载并安装 EAD 客户端的目的。

2.3.14 配置 802.1X SmartOn功能

开启了 SmartOn 功能的端口上收到 802.1X 客户端发送的 EAPOL-Start 报文后，将向其回复单播的 EAP-Request/Notification 报文，并开启 SmartOn 通知请求超时定时器定时器等待客户端响应的 EAP-Response/Notification 报文。若 SmartOn 通知请求超时定时器超时后客户端仍未回复，则设备会重发 EAP-Request/Notification 报文，并重新启动该定时器。当重发次数达到规定的最大次数后，会停止对该客户端的 802.1X 认证；若在重发次数达到最大次数之前收到了该 Notification 报文的回复报文，则获取该报文中携带的 Switch ID 和 SmartOn 密码的 MD5 摘要，并与设备本地配置的 SmartOn 的 Switch ID 以及 SmartOn 密码的 MD5 摘要值比较，若相同，则继续客户端的 802.1X 认证，否则中止客户端的 802.1X 认证。

802.1X SmartOn 功能与在线用户握手功能互斥，建议两个功能不要同时开启。

2.4 ISP域

设备对用户的管理是基于 ISP（Internet Service Provider，互联网服务提供者）域的，一个 ISP 域对应着一套实现 AAA（Authentication、Authorization、Accounting，认证、授权、计费）的配置策略，它们是管理员针对该域用户制定的一套认证、授权、计费方法，可根据用户的接入特征以及不同的安全需求组合使用。

设备支持的认证方法包括：

- 不认证：对用户非常信任，不对其进行合法性检查，一般情况下不采用这种方法。
- 本地认证：认证过程在接入设备上完成，用户信息（包括用户名、密码和各种属性）配置在接入设备上。优点是速度快，可以降低运营成本；缺点是存储信息量受设备硬件条件限制。
- 远端认证（RADIUS）：认证过程在接入设备和远端的服务器之间完成，接入设备和远端服务器之间通过 RADIUS 协议通信。优点是用户信息集中在服务器上统一管理，可实现大容量、高可靠性、支持多设备的集中式统一认证。当远端服务器无效时，可配置备选认证方式完成认证。

设备支持的授权方法包括：

- 不授权：接入设备不请求授权信息，不对用户可以使用的操作以及用户允许使用的网络服务进行授权。此时，认证通过的 login 用户只有系统所给予的缺省用户角色，其中 FTP/SFTP/SCP 用户的工作目录是设备的根目录，但并无访问权限；认证通过的非 login 用户，可直接访问网络。
- 本地授权：授权过程在接入设备上进行，根据接入设备上为本地用户配置的相关属性进行授权。
- 远端授权（RADIUS）：授权过程在接入设备和远端服务器之间完成。RADIUS 协议的认证和授权是绑定在一起的，不能单独使用 RADIUS 进行授权。RADIUS 认证成功后，才能进行授

权，RADIUS 授权信息携带在认证回应报文中下发给用户。当远端服务器无效时，可配置备选授权方式完成授权。

设备支持的计费方法包括：

- 不计费：不对用户计费。
- 本地计费：计费过程在接入设备上完成，实现了本地用户连接数的统计和限制，并没有实际的费用统计功能。
- 远端计费（RADIUS）：计费过程在接入设备和远端的服务器之间完成。当远端服务器无效时，可配置备选计费方式完成计费。

每个用户都属于一个 ISP 域。为便于对不同接入方式的用户进行区分管理，提供更为精细且有差异化的认证、授权、计费服务，设备将用户划分为以下几个类型：

- LAN 接入用户：例如 802.1X 认证用户。
- 登录用户：例如 Telnet、FTP、终端接入用户（即从 Console、AUX 等接口登录的用户）。
- Portal 用户。

在多 ISP 的应用环境中，不同 ISP 域的用户有可能接入同一台设备，因此系统中可以存在多个 ISP 域，其中包括一个缺省存在的名称为 system 的 ISP 域。如果某个用户在登录时没有提供 ISP 域名，系统将把它归于缺省的 ISP 域。系统缺省的 ISP 域可以手工修改为一个指定的 ISP 域。

用户认证时，设备将按照如下先后顺序为其选择认证域：接入模块指定的认证域-->用户名中指定的 ISP 域-->系统缺省的 ISP 域。其中，仅部分接入模块支持指定认证域，例如 802.1X 认证。

2.5 RADIUS

2.5.1 RADIUS协议简介

RADIUS（Remote Authentication Dial-In User Service，远程认证拨号用户服务）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。

- RADIUS 客户端：一般位于接入设备上，可以遍布整个网络，负责将用户信息传输到指定的 RADIUS 服务器，然后根据服务器返回的信息进行相应处理（如接受/拒绝用户接入）。
- RADIUS 服务器：一般运行在中心计算机或工作站上，维护用户的身份信息和与其相关的网络服务信息，负责接收接入设备发送的认证、授权、计费请求并进行相应的处理，然后给接入设备返回处理结果（如接受/拒绝认证请求）。

RADIUS 协议使用 UDP 作为封装 RADIUS 报文的传输层协议，通过使用共享密钥机制来保证客户端和 RADIUS 服务器之间消息交互的安全性。

当接入设备对用户提供 AAA（Authentication、Authorization、Accounting，认证、授权、计费）服务时，若要对用户采用 RADIUS 服务器进行认证、授权、计费，则作为 RADIUS 客户端的接入设备上需要配置相应的 RADIUS 服务器参数。

2.5.2 RADIUS增强功能

1. Accounting-on功能

设备重启后，重启前的原在线用户可能会被 RADIUS 服务器认为仍然在线而短时间内无法再次登录。为了解决这个问题，需要开启 Accounting-on 功能。

开启了 Accounting-on 功能后，设备会在重启后主动向 RADIUS 服务器发送 Accounting-on 报文来告知自己已经重启，并要求 RADIUS 服务器停止计费且强制通过本设备上线的用户下线。若设备发送 Accounting-on 报文后 RADIUS 服务器无响应，则会在按照一定的时间间隔尝试重发几次。分布式设备单板重启时，Accounting-on 功能的实现需要和 H3C IMC 网管系统配合使用。

2. Session control功能

H3C 的 IMC RADIUS 服务器使用 session control 报文向设备发送授权信息的动态修改请求以及断开连接请求。设备上开启接收 session control 报文的开关后，会打开知名 UDP 端口 1812 来监听并接收 RADIUS 服务器发送的 session control 报文。

需要注意的是，该功能仅能和 H3C 的 IMC RADIUS 服务器配合使用。

2.6 BYOD

BYOD（Bring Your Own Device）指携带自己的设备办公，这些设备主要是指个人电脑、手机、平板电脑等终端设备。BYOD 解决方案可以为企业和用户提供基于用户身份信息、终端信息、接入场景的认证、授权服务。

2.6.1 BYOD规则

BYOD 规则是用户终端特征与用户终端类型的一种映射关系。在用户认证的过程中，接入设备获取到用户终端的相关特征（例如 DHCP Option 55 指纹信息）后，可根据 BYOD 规则识别出用户所使用的终端类型。

目前 BYOD 支持的用户终端特征包括：DHCP Option 55、HTTP User Agent 和 MAC 地址。

- DHCP Option55：DHCP 请求参数列表选项，终端利用该选项指明需要从服务器获取哪些网络配置参数。
- HTTP UserAgent：属于 HTTP 请求报文头域的一部分，用于携带终端访问 Web 页面时所使用的操作系统（包括版本号）、浏览器（包括版本号）等信息。
- MAC 地址：终端的 MAC OUI 信息或终端所属的 MAC 地址范围。

同一个特征只能对应一种终端类型，但一种终端类型可以对应多个特征。不同终端特征的识别优先级由高到低为：DHCP Option 55 指纹->HTTP User Agent 指纹->MAC 地址指纹。

系统中已经预定义了一系列常用的 BYOD 规则，用户也可以根据实际组网需求通过命令行添加规则。

2.6.2 BYOD授权

BYOD 授权是指，用户通过本地认证之后，设备通过匹配该用户的终端特征来给用户授予相关的网络访问权限。BYOD 授权是通过用户组实现的。每一个用户都属于一个用户组，用户组中定义了基于终端类型的授权属性。用户在认证过程中，接入设备通过 BYOD 规则来识别用户的终端类型，并根据识别出的终端类型为其授权相应的授权属性。

2.7 本地认证

本地认证泛指由接入设备对用户进行认证、授权和计费，进行本地认证的用户的信息（包括用户名、密码和各种属性）配置在接入设备上。

为使某个请求网络服务的用户可以通过本地认证，需要在设备上添加相应的用户条目。所谓用户，是指在设备上设置的一组用户属性的集合，该集合以用户名唯一标识。

为了简化用户的配置，增强用户的可管理性，引入了用户组的概念。用户组是一系列公共用户属性的集合，某些需要集中管理的公共属性可在用户组中统一配置和管理，属于该用户组的所有用户都可以继承这些属性。

2.8 来宾管理

随着无线智能终端的快速发展，对于来公司参观的访客，公司需要提供一些网络服务。这些访客成员通常为供应商、贵宾、听众或者是其他合作伙伴等。当访客用自己的手机、笔记本、IPAD 等终端接入公司网络时，涉及到用户账号注册，以及访问权限控制的问题。为了简化访客的注册和审批流程，以及对访客权限的管理控制，提供了来宾用户管理功能，具体包括：

- 手工添加来宾用户：手工创建来宾用户，并配置相应的来宾用户属性。
- 导入来宾用户：将指定路径 CSV 文件的来宾帐户信息导入到设备上，并生成相应的来宾用户。
- 批量创建来宾用户：批量生成一系列来宾用户，相应的用户名和密码按照指定规律生成。
- 导出来宾用户：将设备上的来宾帐户信息导出到指定路径 CSV 文件中供其它设备使用。
- 来宾用户的注册与审批，具体过程如下：

(1) 来宾用户通过设备推出的 Portal Web 页面填写注册信息，主要包括用户名、密码和电子邮箱地址，并提交该信息。

(2) 设备收到来宾用户的注册信息后，记录该注册信息，并向来宾管理员发送一个注册申请通知邮件。

(3) 来宾管理员收到注册申请通知邮件之后，在 Web 页面上对注册用户进行编辑和审批。

(4) 如果该注册用户在等待审批时间超时前被来宾管理员审批通过，则设备将自动创建一个来宾用户，并生成该用户的相关属性。若该注册用户在等待审批时间超时后还未被审批通过，则设备将会删除本地记录的该用户注册信息。

(5) 来宾用户创建之后，设备将自动发送邮件通知来宾用户或来宾接待人用户注册成功，向他们告知来宾用户的密码及有效期信息。

(6) 来宾用户收到注册成功通知后，将可以使用注册的帐户访问网络。

- 来宾用户过期自动删除功能：设备定时检查本地来宾用户是否过期并自动删除过期的用户。
- 邮件通知功能：向来宾、来宾接待人、来宾管理员发送帐户审批、密码信息的邮件。

2.9 接入管理

2.9.1 端口安全

端口安全是一种基于 MAC 地址对网络接入进行控制的安全机制，是对已有的 802.1X 认证和 MAC 地址认证的扩充。这种机制通过检测端口收到的数据帧中的源 MAC 地址来控制非授权设备或主机对网络的访问，通过检测从端口发出的数据帧中的目的 MAC 地址来控制对非授权设备的访问。

端口安全的主要功能是通过定义各种端口安全模式，让设备学习到合法的源 MAC 地址，以达到相应的网络管理效果。启动了端口安全功能之后，当发现非法报文时，系统将触发相应特性，并按照预先指定的方式进行处理，既方便用户的管理又提高了系统的安全性。这里的非法报文是指：

- MAC 地址未被端口学习到的用户报文；

- 未通过认证的用户报文。

2.9.2 Portal

Portal 在英语中是入口的意思。Portal 认证通常也称为 Web 认证，即通过 Web 页面接受用户输入的用户名和密码，对用户进行身份认证，以达到对用户访问进行控制的目的。在采用了 Portal 认证的组网环境中，未认证用户上网时，接入设备强制用户登录到特定站点，用户可以免费访问其中的服务；当用户需要使用互联网中的其它信息时，必须在 Portal Web 服务器提供的网站上进行 Portal 认证，只有认证通过后才可以使用这些互联网中的设备或资源。

根据是否为用户主动发起认证，可以将 Portal 认证分为主动认证和强制认证两种类型：用户可以主动访问已知的 Portal Web 服务器网站，输入用户名和密码进行认证，这种开始 Portal 认证的方式称作主动认证；用户访问任意非 Portal Web 服务器网站时，被强制访问 Portal Web 服务器网站，继而开始 Portal 认证的过程称作强制认证。

Portal 认证是一种灵活的访问控制技术，可以在接入层以及需要保护的关键数据入口处实施访问控制，具有如下优势：

- 可以不安装客户端软件，直接使用 Web 页面认证，使用方便。
- 可以为运营商提供方便的管理功能和业务拓展功能，例如运营商可以在认证页面上开展广告、社区服务、信息发布等个性化的业务。
- 支持多种组网型态，例如二次地址分配认证方式可以实现灵活的地址分配策略且能节省公网 IP 地址，可跨三层认证方式可以跨网段对用户作认证。

3 工具

3.1 无线报文捕获

无线报文捕获是一种报文捕获及分析特性，该特性能够捕获设备接口的入方向报文并对报文进行解析处理，便于用户分析接口接收到的报文；还可以将报文数据存储为 pcap 格式的文件，方便用户后续查看。

目前支持以下两种报文捕获的方式：

- 本地报文捕获

本地报文捕获方式下，设备将捕获的报文自动上传到 FTP 服务器。

- 远程报文捕获

远程报文捕获方式下，设备与第三方报文捕获软件 Wireshark 客户端建立连接，并将捕获的报文发送给 Wireshark 客户端，供用户在 Wireshark 客户端上查看。Wireshark 客户端连接到 AP 的 RPCAP 服务端口，就可以获取到指定的 Radio 口捕获的从客户端发往 AP 的报文。

3.1.1 无线报文捕获过滤规则

无线报文捕获可以使用捕获过滤表达式指定捕获过滤规则，对进入指定物理接口的报文进行过滤，满足捕获过滤规则的报文则被捕获。捕获过滤规则由关键字、逻辑操作符、运算操作符和比较操作符等组合而成。有关无线报文捕获更多规则的详细介绍，请参见网址：http://wiki.wireshark.org/CaptureFilters。

3.1.2 关键字

捕获过滤规则使用的关键字分为常量关键字和变量关键字。

1. 常量关键字

常量关键字是固定的字符串，可以分为以下几类：协议类型、传输方向和传输方向的类型等。

表3-1 常量关键字

常量关键字类型	描述	关键字
协议	捕获指定的协议报文。如果没有指明协议类型，默认捕获所有Packet Capture支持的协议	支持的协议有：ip，ip6，arp，tcp，udp，icmp等
报文传输方向	捕获指定传输方向的报文。如果没有指定本关键字，默认报文传输方向为源或目的方向	• src：表示源方向 • dst：表示目的方向 • src or dst：表示源或目的方向
报文传输方向类型	捕获指定的报文传输方向类型的报文。如果没有指定本类关键字，默认报文传输方向类型为主机	• host：表示主机 • net：表示网段 • port：表示端口号

常量关键字类型	描述	关键字
		• portrange：表示端口号范围
特殊关键字	-	• broadcast：表示捕获广播报文 • multicast：表示捕获组播报文、广播报文 • less：表示小于等于 • greater：表示大于等于 • len：表示报文长度 • vlan：表示捕获 VLAN 报文

2. 变量关键字

变量关键字形式固定，但内容可变。捕获过滤规则的变量关键字不可以单独使用，其前需要使用常量关键字对其进行修饰。

需要注意的是，所有的协议类型常量关键字、broadcast 和 multicast 关键字不能对变量关键字进行修饰。其它的常量关键字不可单独使用，其后需要使用变量关键字。

表3-2 变量关键字

变量关键字类型	举例
整型	将整型用二进制、八进制、十进制或十六进制形式表示。例如：port 23，表示端口号为23
整型范围	将整型范围用二进制、八进制、十进制、十六进制形式和“-”表示。例如：portrange 100-200，表示端口号范围为100到200
IPv4地址	使用点分十进制格式表示。例如：src 1.1.1.1，表示源主机IPv4地址是1.1.1.1（在没有指定报文传输方向类型时，报文传输方向类型默认为host）
IPv6地址	使用冒号分十六进制格式表示。例如：dst host 1::1，表示报文的目的主机IPv6地址是1::1
IPv4网段	使用IPv4地址和掩码或者IPv4网络号表示。以下两种表达式等价： • src 1.1.1，表示源主机的 IPv4 网段为 1.1.1 • src net 1.1.1.0/24，表示源主机的 IPv4 网段为 1.1.1.0/24
IPv6网段	使用IPv6地址和网络前缀表示。例如：dst net 1::/64，表示目的IPv6网段为1::/64 • 需要注意的是，指定 IPv6 网段变量关键字时，必须指定 net 常量关键字

3.1.3 捕获过滤操作符

1. 逻辑操作符

逻辑操作符的逻辑运算顺序为从左到右，下表为逻辑操作符的分类举例。

表3-3 逻辑操作符

逻辑操作符	描述
!或者not	非操作符。表示对捕获过滤规则取反操作

逻辑操作符	描述
&&或者and	与操作符。表示连接多个捕获过滤规则。当此操作符连接多个过滤规则时，报文若符合此操作符连接的全部过滤规则，才会过滤成功，否则，过滤失败。
||或者or	或操作符。表示对多个捕获过滤规则进行选择。当此操作符连接多个过滤规则时，报文若不符合此操作符连接的全部过滤规则，才会过滤失败，否则，过滤成功。

其中非操作符优先级最高，与操作符和或操作符的优先级相同。

2. 运算操作符

表3-4 运算操作符

运算操作符	描述
+	加法运算符，用来将其两侧的值加到一起
-	减法运算符，用来将它前面的数值中减去它后面的数值
*	乘法运算符，用来将其两侧的值相乘
/	除法运算符，用来将其左边的值被右边的值除
&	按位与，用来将其两侧的数值逐位进行比较产生一个新值。对于每一位，只有两个操作数的对应位都为1时结果才为1
|	按位或，用来将其两侧的操作数逐位进行比较产生一个新值。对于每一位，如果其中任意操作数中对应的位为1，那么结果位就为1
<<	按位左移，用来将其左侧操作数的每位向左移动，移动的位数由其右侧操作数指定
>>	按位右移，用来将其左侧操作数的每位向右移动，移动的位数由其右侧操作数指定
[ ]	取位运算符，与协议类型关键字结合使用。例如：ip[6]，表示IP报文偏移6个字节后，取得的一个字节的值

3. 比较操作符

下表为比较操作符的分类举例。

表3-5 比较操作符分类

比较操作符	描述
=	相等，判断两侧操作数是否相等。例如：ip[6]=0x1c，表示捕获IPv4报文数据域偏移6字节，取得的一个字节值为0x1c的报文
!=	不等，判断两侧操作数是否不等。例如：len!=60，表示捕获报文长度不等于60字节的报文
>	大于，判断左侧操作数大于右侧操作数。例如：len>100，表示捕获报文长度大于100字节的报文
<	小于，判断左侧操作数小于右侧操作数。例如：len<100，表示捕获报文长度小于100字节的报文
>=	大于等于，判断左侧操作数大于等于右侧操作数；与常量关键字greater等价。例如：len>=100，表示捕获报文长度大于等于100字节的报文
<=	小于等于，判断左侧操作数小于等于右侧操作数；与常量关键字less等价。例如：len<=100，表示捕获报文长度小于等于100字节的报文

3.1.4 捕获过滤表达式

捕获过滤表达式由关键字、逻辑操作符、运算操作符和比较操作符之间的多种组合而成。以下为典型捕获过滤表达式：

1. 逻辑操作符表达式

由关键字和逻辑运算符组合的捕获过滤表达式。例如：not port 23 and not port 22，表示捕获端口号既不是 23，又不是 22 的报文；port 23 or icmp，表示捕获端口号是 23 或 icmp 协议的报文。

由逻辑操作符连接的多个变量关键字，可以使用同一个常量关键字进行修饰（就近原则），例如：src 192.168.56.1 or 192.168.27，表示捕获的源 IPv4 地址为 192.168.56.1 或者源 IPv4 网段为 192.168.27 的报文。上述表达式与“src 192.168.56.1 or src 192.168.27”等价。

2. *expr relop expr*表达式

由关键字、运算操作符和比较操作符组合的捕获过滤表达式。其中，*expr* 是算术表达式；*relop* 为比较操作符。例如：len+100>=200，表示捕获长度大于等于 100 字节的报文。

3. *proto* [*expr*:*size*]表达式

由协议类型关键字和运算操作符“[ ]”组合的捕获过滤表达式。其中，*proto* 表示协议类型，*expr* 为算术表达式，表示偏移量，*size* 为整数，表示字节个数，缺省值为 1。*proto* [*expr*:*size*]的返回值为从 *proto* 协议报文数据区域起始位置，偏移 *expr* 个字节开始，取 *size* 个字节的数据。例如：ip[0]&0xf != 5，表示捕获第一个字节与 0x0f 按位相与得到的值不是 5 的 IP 报文。

expr:*size* 也可以使用名字表示。例如：icmptype 表示 ICMP 报文的类型域，则表达式：icmp[icmptype]=0x08，表示捕获 icmp 的 type 字段的值为 0x08 的报文。

4. vlan *vlan_id*表达式

由关键字 vlan，逻辑操作符等组合的捕获过滤表达式。其中，*vlan_id* 为整型，表示 VLAN 编号。例如，vlan 1 and ip6，表示捕获 VLAN 编号为 1 的 IPv6 报文。

需要注意的是：

- 如果用户需要对带 VLAN 的报文进行捕获过滤，必须使用此类捕获过滤表达式且关键字 vlan 要在其它捕获过滤条件之前指定，否则不能正常过滤。例如：icmp，表示捕获不带 vlan 的 icmp 报文。
- 如果捕获过滤规则之前没有指定 vlan，则认为这些捕获过滤规则只对不带 vlan 的报文进行捕获过滤，即对带 vlan 的报文不捕获。例如：
  - !tcp and vlan 1：表示捕获不带 vlan 标记的 tcp 报文以外的且属于 vlan 1 的报文。
  - icmp and vlan 1：icmp 表示捕获不带 vlan 标记的 icmp 协议报文，而 vlan 1 表示捕获 vlan 标记为 1 的报文，所以该捕获过滤表达式前后矛盾，因此不会收到任何报文，对于此类捕获过滤规则，只要没有语法错误，命令行均会下发成功，用户需要自己保证逻辑的正确性。
  - RF Ping
  - RF Ping 即无线链路质量检测。该检测过程中，AP 根据客户端上线时协商的速率集，以每个速率发送 5 个空数据报文进行链路质量检测。AP 根据客户端的响应报文可以获取 AP 与客户端之间的无线链路质量信息，如信号强度、报文重传次数、RTT（Round-trip Time，往返时间）等。