

目录

第 1 章 无线安全	1-1
第 2 章 AP威胁检测	2-1
2.1 AP威胁检测介绍	2-1
2.2 AP威胁检测配置	2-2
2.3 AP威胁检测举例	2-4
2.4 AP威胁检测排错帮助	2-4
第 3 章 Client威胁检测	3-1
3.1 Client威胁检测介绍	3-1
3.2 Client威胁检测配置	3-2
3.3 Client威胁检测举例	3-4
3.4 Client威胁检测排错帮助	3-4
第 4 章 反制功能	4-1
4.1 反制功能介绍	4-1
4.2 反制功能配置	4-1
4.3 反制功能举例	4-2
4.4 反制功能排错帮助	4-3
第 5 章 用户隔离	5-1
5.1 用户隔离介绍	5-1
5.2 用户隔离配置	5-2
5.3 用户隔离举例	5-3
5.4 用户隔离排错帮助	5-3
第 6 章 ARP抑制&ARP代理	6-1
6.1 ARP抑制&ARP代理介绍	6-1
6.2 ARP抑制&ARP代理配置	6-1
6.3 ARP抑制&ARP代理举例	6-1
6.4 ARP抑制&ARP代理排错帮助	6-2
第 7 章 动态黑名单	7-1
7.1 动态黑名单概述	7-1
7.2 动态黑名单配置	7-1
7.3 动态黑名单举例	7-2

7.4 动态黑名单排错帮助	7-2
第 8 章 无线SAVI	8-1
8.1 无线SAVI技术简介	8-1
8.2 无线SAVI配置	8-1
8.3 无线SAVI功能举例	8-2
8.4 无线SAVI排错帮助	8-5
第 9 章 DHCP抑制	9-1
9.1 DHCP抑制介绍	9-1
9.2 DHCP抑制配置	9-1
9.3 DHCP抑制举例	9-1
9.4 DHCP抑制排错帮助	9-2

第1章 无线安全

IEEE 802.11 网络很容易受到各种网络威胁的影响，如未经授权的 AP（Access point）用户、Ad-hoc 网络、泛洪攻击等。Rogue 设备对于企业网络安全来说是一个很严重的威胁。WIDS（Wireless Intrusion Detection System）用于对有恶意的用户攻击和无线网络入侵进行早期检测。WIPS（Wireless Intrusion Prevention System）可以保护企业网络 and 用户不被无线网络上未经授权的设备访问。无线安全功能不仅可以对恶意的用户攻击和无线网络入侵进行早期检测，而且可以采取反制措施进行主动防御，从而确保企业网络 and 用户不被无线网络上未经授权的设备访问。

如下是对无线安全消息的描述：

1. RF Scan Report Message

Managed AP 会周期性的向 AC Controller 发送 RF Scan Report Message，其中记录了周围的邻居 AP 和 Client 信息，根据这些邻居信息，WIDS 模块会做相应的威胁检测，以便确定周围是否存在非法设备。（unknown 即可，不用非得是 rogue）

2. Client-Threat-Deauthenticate Message

当“合法 Client 关联非法 AP”检测到威胁且被认定为 Rogue 设备后，如果开启了 known client 的保护功能，AC Controller 发送此消息给 Managed AP，由 AP 假冒此 Client 发送解认证消息给其关联的 AP，以解除 Known Client 和 Unknown AP 的连接。

3. WIDS-Configuration-Message

当相关配置改变或 Rogue AP 攻击表改变时，AC Controller 发送此消息给 AP，里面的字段除 AP MAC Address 外都是可选的。

表 1-1 WIDS-Configuration-Message 消息格式

Description	Element ID	Element Length	Content
AP MAC Address	0x0021	6 bytes	AP MAC Address
Enable Wired Network Detection	0x7001	1 byte	0—Disable Detection 1—Enable Detection
Minimum Wired Network Detection Interval	0x7002	2 bytes	0—Network detection is performed on every RF Scan sweep. 1–3600—Number of seconds between detection attempts.
AP Attack Interval	0x7003	2 bytes	Number of seconds between transmissions of de-authentication frames by operational mode radios.

Number of BSSIDs in the attack list.	0x7004	2 bytes	Number of BSSID for which the AP will execute a de-authentication attack. Set to 0 for an empty list.
BSSID Attack List	0x7005	7 to 112 bytes	6-byte BSSID followed by 1 byte channel number. The list size depends on number of entries.

第2章 AP 威胁检测

2.1 AP威胁检测介绍

AP 实时监测周边的射频环境，包括邻居 Client 和 AP 信息，并将监测到的信息周期性发给关联的 AC，如果 AC 不是整个集群中的 Controller，还要将 RF Scan Report Message 转发到 AC Controller，AC Controller 分析 RF Scan Report Message 中的邻居信息，通过制定的非法设备检测规则，对整个 WLAN 网络中的异常设备进行监视。

其中 AP 的工作状态分为下表所示的四种；AP 端射频扫描用的 Radio 可以配置为两种模式：Active 和 Sentry。处于 Active 模式的 Radio 正常处理用户流量，只是在设定的间隔时间内周期性的扫描，但它只能扫描自己的工作频段，例如 2.4G 或 5G；处于 Sentry 模式的 Radio 不处理任何用户流量，专用于扫描监测信息，它可以轮流监控 2.4G 和 5G 频段内的所有信道。由于 Sentry mode 的 Radio 专用于射频扫描工作，且同时监测 2.4G 和 5G 频段内的所有信道，因此它能够更加全面、准确、迅速的得到射频信息。因此，有些威胁必须是 sentry mode 上报的 RF Scan Report Message 才能检测出来，其中包括 ap 工作在非法信道，Unmanaged AP 接入有线网络。

表 2-1 AP 的四种工作状态

状态	解释
Managed	处于被 AC 管理（瘦 AP）状态。
Standalone	处于独立运作（胖 AP）状态，必须由管理员在 Valid AP 表中把此 AP 手动设为 standalone 状态。
Unknown	无法识别的状态，非 Managed 和 standalone，但没有被判定为非法 AP。
Rogue	非法 AP，被相关检测认定为威胁。

根据黑客常用的非法 AP 使用方法，本产品制订了 11 种检测来监视 WLAN 网络中的异常 AP：网管设置的非法 AP、非法 AP 假冒合法的 SSID、Beacon 帧中 Vendor 字段不合法、Beacon 帧中没有 SSID 字段、在错误信道接收到 managed AP 的 Beacon 帧、Managed AP 发送无效的 SSID、AP 工作在非法信道、合法的胖 AP 配置错误和 Unmanaged AP 接入有线网络、AP 使用了错误的安全认证方式，AP 工作在 WDS 模式。AC Controller 运行上述 11 种检测，如果检测到威胁，则把 AP 定性为 Rogue，并发送 Trap 通知网管。

同时，如果 AC Controller 开启了反制功能，会发送 WIDS-Configuration-Message，将 Rogue AP 列表发送给 Managed AP，然后由 Managed AP 对 Rogue AP 进行反制，同时发送"wsRFScanRogueAPDetected"Trap 通知网管。

下面将对 11 种防御规则进行介绍：

1. 网管设置的非法 AP

网管可以设置在本地或 Radius 服务器的 Valid-AP 数据库中的认证，在 Valid-AP 数据库中管理员可以手动配置 AP 的三种状态：Managed、Standalone、Rogue。网管设置的非

法 AP 就是本地或 Radius 服务器的 Valid-AP 数据库被网管配置为 Rogue 的 AP。

2. 非法 AP 假冒合法的 SSID

AC controller 中 SSID 查询系统的网络配置记录着合法性的 SSID，非法 AP 有时会假冒这些合法性的 SSID 来欺骗客户 Client 接入，从而窃取客户信息。

3. Beacon 帧中 Vendor 字段不合法

有些黑客会冒充 Managed AP 的 mac 并发送 Managed SSID 的情况，本产品约定 Managed AP 的 beacon 帧中必须携带 vendor 字段，这样通过检测 vendor 字段就可以检测出 Managed AP Mac 地址的 Rogue AP（如果没有 vendor 字段，RF Scan Report Message 中的 Neighbor AP Info 中的 AP MAC Address 为 00-00-00-xx-xx-xx）。

4. Beacon 帧中没有 SSID 字段

黑客为了避免被检测到，有可能会在 beacon 帧中不包含 SSID 字段，但它仍可以通过发送 probe response 帧给发送 probe request 的 Client，以欺骗 client 接入，骗取安全信息。

5. 在错误信道接收到 Managed AP 的 Beacon 帧

由于 Managed AP 的信道是由 AC 分配的，所以 AC 知道 Managed AP 应该工作的信道，而黑客会假冒 Managed AP 的 mac，但其发送 beacon 帧所使用的信道却可能在错误的信道。

6. AP 使用了错误的安全认证方式

AP 的 beacon 帧中会带有其安全认证方式 (open、WEP、WPA)，因此通过检测 beacon 帧中携带的安全认证方式是否和 AC Controller 中记录的 AP 配置一致，可以检测出此类 rogue AP。

7. Managed AP 发送无效的 SSID

如果 Managed AP 发送无效的 SSID，则检测到 Managed AP 的 AP 会将 RF Scan Report Message 发送给 AC controller，该信息中将包含此不合法的 SSID。

8. AP 工作在非法信道

不同国家对射频资源有不同的规定，有些信道在某些国家是合法的在另一些国家却是非法的，如果 AP 工作在非法信道，此步可以检测出来。因为要侦听全信道的 beacon 帧，所以只能由 sentry mode 的 Radio 发送的 RF Scan Report 信息才能检测出这种威胁。

9. 合法的胖 AP 配置错误

如果 AP 初始状态为 Standalone，且检查扫描到的配置和 AC Controller 保存的配置一致，则此 AP 为合法 AP。否则为 Rogue AP。注：要检查的配置有工作信道、SSID、安全认证方式、WDS 模式和是否接入有线网络。

10. AP 工作在 WDS 模式

WDS (Wireless Distribution System) 无线分布式系统，是使接入点 (AP) 通过无线进行连接的协议。运行在 WDS 模式的 AP 通过桥接或中继的方式互相连接，降低了对有线网络的依赖，提高了整个网络结构的灵活性和便捷性。

如果 AP 是通过 WDS 方式连接到 AC 上并且被 AC 管理，但同时又有假冒的 AP 被检测出未工作在 WDS 模式，则可被认为是威胁。

11. Unmanaged AP 接入有线网络

因为只有 Managed AP 才能接入有线网络，所以如果 AP 的状态是 Unknown 且被检测到连接在有线网络上，则检测为 Rogue AP。

2.2 AP 威胁检测配置

1. 网管设置的非法 AP 配置

命令	解释
无线全局配置模式	
wids-security admin-config-rogue	打开网管设置的非法 AP 检测。

2. 非法 AP 假冒合法的 SSID 配置

命令	解释
无线全局配置模式	
wids-security unknown-ap-managed-ssid no wids-security unknown-ap-managed-ssid	打开/关闭非法 AP 假冒合法的 SSID 检测。

3. Beacon 帧中 Vendor 字段不合法配置

命令	解释
无线全局配置模式	
wids-security fakeman-ap-managed-ssid no wids-security fakeman-ap-managed-ssid	打开/关闭 Beacon 帧中 Vendor 字段不合法检测。

4. Beacon 帧中没有 SSID 字段配置

命令	解释
无线全局配置模式	
wids-security managed-ap-ssid-invalid no wids-security managed-ap-ssid-invalid	打开/关闭 Beacon 帧中没有 SSID 字段检测。

5. 在错误信道接收到 managed AP 的 Beacon 帧配置

命令	解释
无线全局配置模式	
wids-security fakeman-ap-chan-invalid no wids-security fakeman-ap-chan-invalid	打开/关闭在错误信道接收到 managed AP 的 Beacon 帧检测。

6. AP 使用了错误的安全认证方式配置

命令	解释
无线全局配置模式	
wids-security managed-ssid-secu-bad no wids-security managed-ssid-secu-bad	打开/关闭 AP 使用了错误的安全认证方式检测。

7. Managed AP 发送无效的 SSID 配置

命令	解释
无线全局配置模式	
wids-security managed-ap-ssid-invalid no wids-security managed-ap-ssid-invalid	打开/关闭 Managed AP 发送无效的 SSID 检测。

8. AP 工作在非法信道配置

命令	解释
无线全局配置模式	
wids-security ap-chan-illegal no wids-security ap-chan-illegal	打开/关闭 AP 工作在非法信道检测。

9. 合法的胖 AP 配置错误配置

命令	解释
无线全局配置模式	
wids-security standalone-cfg-invalid no wids-security standalone-cfg-invalid	打开/关闭合法的胖 AP 配置错误检测。

10. AP 工作在 WDS 模式配置

命令	解释
无线全局配置模式	
wids-security wds-device-unexpected no wids-security wds-device-unexpected	打开/关闭 AP 工作在 WDS 模式检测。

11. Unmanaged AP 接入有线网络配置

1) 打开/关闭 Unmanaged AP 接入有线网络检测

命令	解释
无线全局配置模式	
wids-security unmanaged-ap-wired no wids-security unmanaged-ap-wired	打开/关闭 Unmanaged AP 接入有线网络检测。

wids-security wired-detection-interval <interval> no wids-security wired-detection-interval	设置每一轮检测的最短空闲等待时间；恢复每一轮检测的最短空闲等待时间到默认值。
--	--

2) 设置检测组播帧所带的 VLAN ID

命令	解释
AP Profile 配置模式	
wired-detection-vlan <0-4094> no wired-detection-vlan	设置检测组播帧所带的 VLAN ID；恢复检测组播帧所带的 VLAN ID 到默认值。

12. Debug 的相关配置

命令	解释
特权模式	
debug wireless wids internal-info no debug wireless wids internal-info	打开/关闭 WIDS 威胁检测过程中的 debug 信息。

2.3 AP威胁检测举例

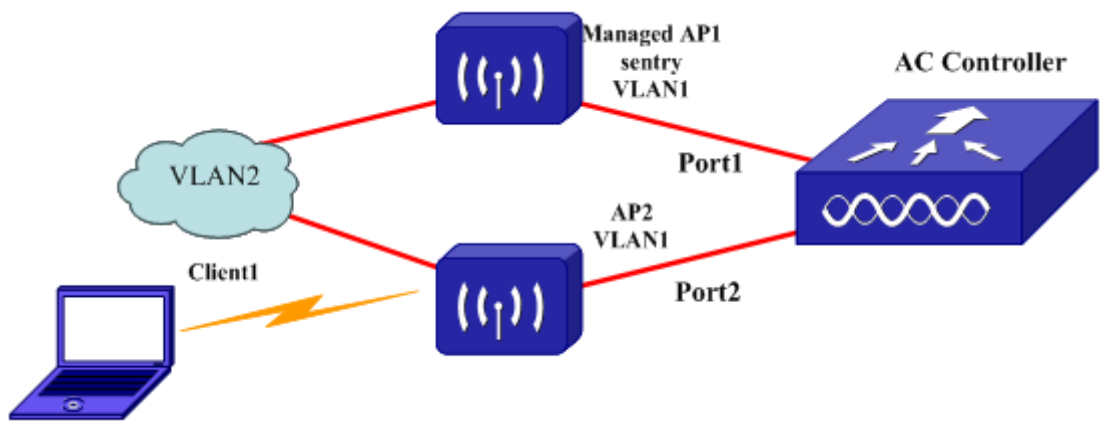


图 2-1 Unmanaged AP 接入有线网络案例

如上图所示为一台 AC 组成的网络，Managed AP1 经过 port1 与 AC controller 相连，定期发送 RF scan report message 给 AC controller 进行处理。AP1 的状态设置为 sentry 模式；AP2 为网络中的待检测设备。要想检测出该网络中，是否存在 Unmanaged AP 接入有线网络，需要分别对 AP1 和 AC controller 进行如下配置：

```
AC>enable
AC#config
```

```
AC(config)#wireless
AC(config-wireless)#wids-security unmanaged-ap-wired
AC(config-wireless)#wids-security wired-detection-interval 120
AC(config-wireless)#ap profile 1
AC(config- AP Profile)#vlan 2
```

2.4 AP威胁检测排错帮助

在配置、使用 AP 威胁检测时，如果出现 AP 威胁检测未能正常运行或检测结果错误。请检查是否是如下原因：

- ☞ 请查看物理连接是否正确。
- ☞ 请查看 AP 威胁检测是否已启动。
- ☞ AP 工作在非法信道和 Unmanaged AP 接入有线网络检测时，要确认扫描 AP 的工作模式为 sentry mode。
- ☞ 如果非法 AP 假冒合法的 SSID 威胁检测项出现检测结果错误，请查看 AP 检测到的不在此集群中的 AP 是否使用了相同的 SSID。如果存在，请修改不在此集群中的 AP 的 SSID。
- ☞ 如果 Beacon 帧中没有 SSID 字段检测项出现检测结果错误，请查看网络中是否有 VAP 配置了 Hidden SSID。如果存在，请关闭此检测。
- ☞ 如果 AP 使用了错误的安全认证方式检测项出现检测结果错误，请查看 AC Controller 是否与集群中 AP 的相关安全方式保持同步。
- ☞ 如果 Managed AP 发送无效的 SSID 检测项出现检测结果错误，请查看 AC Controller 是否与集群中的 AP 网络配置保持同步。

第3章 Client 威胁检测

3.1 Client威胁检测介绍

Client 的状态分为以下四种：

表 3-1 Client 的四种状态

状态	解释
Authenticated	通过认证的 Client
Detected	检测到的 Client，没有通过认证但也没有被认定为非法
Black-Listed	黑名单中的 Client
Rogue	非法 Client

根据非法 Client 的常用方法，本产品制订了 7 种检测规则来监视 WLAN 网络中的异常 Client 进行监视：OUI 不合法、Known Client Database 判定非法、认证请求帧泛洪攻击、探查请求帧泛洪攻击、解认证请求帧泛洪攻击、认证失败最大次数超过阈值、合法 Client 关联未知 AP。AC Controller 运行上述 7 种检测规则，如果检测到威胁，则把 Client 定性为 Rogue，并发送 Trap 通知网管。同时如果是合法 Client 关联未知 AP 发现的 Rogue Client，会执行 Known Client 保护机制。

AC Controller 支持的上述 Client 威胁检测，可以单独配置是否开启相应检测，检测算法只运行在 AC controller 上，从收到的射频扫描（RF Scan）报告中提取邻居 Client 信息，按下面顺序进行威胁检测。

1. OUI 不合法

网管可以设置在 AC controller 的 OUI 表中设置合法的 OUI，因此可以通过查询目标 Client Mac 地址的 OUI 字段（前三个字节）是否在 OUI 表中有符合项，来检测此类威胁。

2. Known Client Database 判定非法

网管可以设置 AC controller 从本地或 Radius 服务器读取 Known Client Database，如果是合法 Client，则 Known Client Database 中就会有相应的客户端条目。因此根据 Known Client Database 中的配置可以检测 Client 是否合法。

如果网管设置 AC controller 从本地服务器读取 Known Client Database，那么 AC 就会从本地的 Known Client Cache 中读取 Known Client Database。

如果设置为 Radius 服务器，则 AC 实际是从本地的 Known Client Cache 中读取 Client 表项，当 Client 表项中没有与此 Client 相关的项时，先将此 Client 放入 Detected Clients Database 中，则 AC 向 Radius 服务器发送请求，读取 Known Client Database 中的相应表项，等 Radius 服务器返回结果后，根据返回结果改整 Detected Clients Database 中 Client 的状态，同时将 Radius 服务器返回结果放入本地的 Known Client Cache。

3. 关联请求帧泛洪攻击

泛洪攻击（Flooding 攻击）是指 WLAN 设备会在短时间内接收了大量的同种类型的报

文。此时 WLAN 设备会被泛洪的攻击报文淹没而无法处理真正的无线终端的报文。

关联请求帧泛洪攻击是指 Rogue Client 在短时间内对某个 AP 设备发送大量的关联请求帧。此时 AP 设备会被泛洪的攻击报文淹没而无法处理真正的无线终端的报文。针对此项威胁，本产品通过判断关联请求帧是否超出了配置的该帧发送速率来检测，即如果在检测时间内发送 Association Frame 超过阈值，则检测为威胁。

4. 解关联请求帧泛洪攻击

解关联请求帧泛洪攻击是指 Rogue Client 在短时间内对某个 AP 设备发送大量的解关联请求帧。此时 AP 设备会被泛洪的攻击报文淹没而无法处理真正的无线终端的报文。针对此项威胁，本产品通过判断解关联请求帧是否超出了配置的该帧发送速率来检测，即如果在检测时间内发送 Dis-association Frame 超过阈值，则检测为威胁。

5. 认证请求帧泛洪攻击

泛洪攻击（Flooding 攻击）是指 WLAN 设备会在短时间内接收了大量的同种类型的报文。此时 WLAN 设备会被泛洪的攻击报文淹没而无法处理真正的无线终端的报文。

认证请求帧泛洪攻击是指 Rogue Client 在短时间内对某个 AP 设备发送大量的认证请求帧。此时 AP 设备会被泛洪的攻击报文淹没而无法处理真正的无线终端的报文。针对此项威胁，本产品通过判断认证请求帧是否超出了配置的该帧发送速率来检测，即如果在检测时间内发送 Authentication Frame 超过阈值，则检测为威胁。如果使能了动态黑名单，还应将其加入动态黑名单。

6. 探查请求帧泛洪攻击

探查请求帧泛洪攻击是指 Rogue Client 在短时间内对某个 AP 设备发送大量的探查请求帧。针对此项威胁，本产品通过判断探查请求帧是否超出了配置的该帧发送速率来检测，即如果在检测时间内发送 Probe Request Frame 超过阈值，则检测为威胁。

7. 解认证请求帧泛洪攻击

解认证请求帧泛洪攻击是指 Rogue Client 在短时间内对某个 AP 设备发送大量的认证请求帧。针对此项威胁，本产品通过判断解认证请求帧是否超出了配置的该帧发送速率来检测，即如果在检测时间内发送 De-Authentication Request Frame 超过阈值，则检测为威胁。

认证失败最大次数

8. Client 认证失败次数的阈值

有的未知 Client 为了接入受保护的无线网络，会一直尝试发送认证请求，直到认证请求被允许。针对此项威胁，本产品通过判断 Client 认证次数是否超出了配置阈值，即如果超出了配置的最大认证失败数，检测为威胁。

9. 合法 Client 关联未知 AP

合法 Client 可能会因为未知 AP 的引导而通过未知 AP 连入网络，这样合法 Client 的各种信息就会暴露在使用次未知 AP 的黑客面前。要检测此种威胁，需要检测 Client 关联的 AP 的合法性，如果 AC 检测到 AP 状态为 unknown，合法 Client 关联到此 AP 上则检测为威胁。

3.2 Client 威胁检测配置

1. OUI 不合法威胁检测配置

命令	解释
无线全局配置模式	
wids-security oui-database-mode {both local read-only}	设置 OUI 合法性检测时所用的 OUI 数据库类型。
wids-security client oui-database no wids-security client oui-database	打开/关闭 OUI 不合法检测。
oui database <oui> <oui> no oui database <oui>	添加/删除 OUI database。

2. Known Client Database 判定非法配置

命令	解释
无线全局配置模式	
wids-security client known-client-database no wids-security client known-client-database	打开/关闭 Known Client Database 判定非法检测。

3. 关联请求帧泛洪攻击

命令	解释
无线全局配置模式	
wids-security client configured-assoc-rate no wids-security client configured-assoc-rate	打开关联请求帧泛洪攻击检测。
wids-security client threshold-interval-assoc <1-3600> no wids-security client threshold-interval-assoc <1-3600>	设置 Client 发送 802.11 关联请求帧的检测时间。
wids-security client threshold-value-assoc <1-99999> no wids-security client threshold-value-assoc	设置 Client 发送 802.11 关联请求帧的阈值。

4. 解关联请求帧泛洪攻击

命令	解释
无线全局配置模式	
wids-security client configured-disassoc-rate no wids-security client configured-disassoc-rate	打开解关联请求帧泛洪攻击检测。

wids-security client threshold-interval-disassoc <1-3600> no wids-security client threshold-interval-disassoc	设置 Client 发送 802.11 解关联请求帧的检测时间。
wids-security client threshold-value-disassoc <1-99999> no wids-security client threshold-value-disassoc	设置 Client 发送 802.11 解关联请求帧的阈值。

5. 认证请求帧泛洪攻击配置

命令	解释
无线全局配置模式	
wids-security client configured-auth-rate no wids-security client configured-auth-rate	打开/关闭认证请求帧泛洪攻击检测。
wids-security client threshold-interval-auth <1-3600> no wids-security client threshold-interval-auth	设置认证请求帧的检测时间；恢复认证请求帧的检测时间为默认值(60)。
wids-security client threshold-value-auth <1-99999> no wids-security client threshold-value-auth	设置认证请求帧阈值；恢复认证请求帧阈值到默认值(120)。

6. 探查请求帧泛洪攻击配置

命令	解释
无线全局配置模式	
wids-security client configured-probe-rate no wids-security client configured-probe-rate	打开/关闭探查请求帧泛洪攻击检测。
wids-security client threshold-interval-probe <1-3600> no wids-security client threshold-interval-probe	设置探查请求帧的检测时间；恢复探查请求帧的检测时间为默认值(60)。
wids-security client threshold-value-probe <1-99999> no wids-security client threshold-value-probe	设置探查请求帧阈值；恢复探查请求帧阈值到默认值(120)。

7. 解认证请求帧泛洪攻击配置

命令	解释
无线全局配置模式	
wids-security client configured-deauth-rate no wids-security client configured-deauth-rate	打开/关闭解认证请求帧泛洪攻击检测。

wids-security client threshold-interval-deauth <1-3600>	设置解认证请求帧的检测时间；恢复解认证请求帧的检测时间为默认值(60)。
no wids-security client threshold-interval-deauth	
wids-security client threshold-value-deauth <1-99999>	设置解认证请求帧阈值；恢复解认证请求帧阈值到默认值(120)。
no wids-security client threshold-value-deauth	

8. 认证失败最大次数

命令	解释
无线全局配置模式	
wids-security client max-auth-failure no wids-security client max-auth-failure	打开/关闭认证失败最大次数检测。
wids-security client threshold-auth-failure <1-99999>	设置认证失败最大次数阈值；恢复认证失败最大次数阈值到默认值(5)。
no wids-security client threshold-auth-failure	

9. 合法 Client 关联未知 AP

命令	解释
无线全局配置模式	
wids-security client auth-with-unknown-ap no wids-security client auth-with-unknown-ap	打开/关闭合法 Client 关联未知 AP。

10. Debug 的相关配置

命令	解释
特权模式	
debug wireless wids known-client internal-info no debug wireless wids known-client internal-info	打开/关闭操作 Known client 数据库的 debug 信息。

3.3 Client威胁检测举例



图 3-1 认证请求帧泛洪攻击案例

如上图所示中，Client1 和 Client2 通过 AP1 连入无线网络。Client1 正常通信，Client2 为泛洪攻击中的认证请求帧泛洪攻击，其不断的向 AP1 发送认证请求。要想检测出该网络中 Client2 是认证请求帧泛洪攻击的 Rogue Client，需要对 AC controller 进行如下配置：

```
AC>enable
```

```
AC#config
```

```
AC(config)#wireless
```

```
AC(config-wireless)#no wids-security client threshold-interval-auth
```

```
AC(config-wireless)#wids-security client threshold-value-auth 6000
```

```
AC(config-wireless)#wids-security client configured-auth-rate
```

3.4 Client威胁检测排错帮助

在配置、使用 Client 威胁检测时，可能会由于物理连接、配置错误等原因导致本项检测未能正常运行或出现错误检测。请检查是否是如下原因：

- ☞ 保证物理连接的正确无误。
- ☞ 确认已启动 Client 威胁检测。
- ☞ 确认相应阈值（认证请求帧泛洪攻击、探查请求帧泛洪攻击、解认证请求帧泛洪攻击和认证失败最大次数）设置是否合适。

第4章 反制功能

4.1 反制功能介绍

在检测到Rogue AP后，如果开启了Rogue AP反制功能，AC Controller将攻击列表发送给Managed AP，由Managed AP对Rogue 设备采取措施。反制措施分为两种：Rogue AP反制功能和Known Client保护功能。启动反制措施后，Sentry Mode的Radio假冒Client发送解认证消息给Rogue AP，而Active Mode的Radio会发送解认证消息给关联到Rogue AP的Client，以解除Rogue AP和Client的连接。但下列情况不会加入攻击列表：

- AP 的 Mac 地址为 Managed AP Mac（不管是假冒的还是实际的）
- AP 工作在 ad-hoc 模式
- AP 工作在非法信道上
- AP 攻击列表满（最多 16 个 Rogue AP）

1、Rogue AP 反制功能

AC Controller 检测出 Rogue AP 后，如果开启了 Rogue AP 反制功能，会将其添加到 Rogue AP 攻击列表中，并将列表通过 WIDS-Configuration-Message 发送给所有 Managed AP。Sentry Mode 的 Radio 假冒 Client 发送解认证消息给 Rogue AP，而 Active Mode 的 Radio 会发送解认证消息给关联到 Rogue AP 的 Client。

2、Known Client 保护功能

如果 AC Controller 开启合法 Client 关联非法 AP 检测，并检测出了威胁，则当开启了此威胁的 Rogue 认定后，Client 被标志为 Rogue Client，同时将 Rogue Client 的信息（包括 mac，Channel，association AP mac，Association AP Radio 等）构造成消息发送给 client-security task，这个 task 的信息队列容量为 128.，因此最多接收 128 条消息，接收到 WIDS 模块发送的消息后 client-security task 会构造 Client-Threat-Deauthenticate Message 发送给 managed AP，Sentry mode 的 Radio 假冒此 Client 发送解认证消息给其关联的 AP，从而解除与非法 AP 的连接。

4.2 反制功能配置

1. Rogue AP 反制功能配置

1) 打开/关闭 Rogue AP 反制功能

命令	解释
无线全局配置模式	
wids-security ap-de-auth-attack no wids-security ap-de-auth-attack	打开/关闭 Rogue AP 反制功能。

2) 恢复 Rogue AP 到其先前状态

命令	解释
特权模式	
wireless acknowledge-rogue [<macaddr>]	如果指定 mac 地址的 Rogue AP 已经被网管清除了威胁，恢复其先前状态。
wireless acknowledge-rogue	改变所有 Rogue AP 到先前状态。

2. Known Client 保护功能配置

1) 打开/关闭 Known Client 保护功能

命令	解释
无线全局配置模式	
wids-security client threat-mitigation no wids-security client threat-mitigation	打开/关闭 Known Client 保护功能。

2) 将 Client 从 Detected Clients Database 中清除

命令	解释
特权模式	
clear wireless detected-client [<macaddr>] non-auth	将 mac 地址指定的非 Authenticated 状态的 Client 从 Detected Clients Database 中清除。
clear wireless detected-client non-auth	将 detected-client 数据库所有 Client 清除。

3) 改变 Rogue Client 的状态

命令	解释
特权模式	
wireless detected-client [<macaddr>] ack-rogue	改变 mac 地址指定 Rogue Client 的状态。
wireless detected-client ack-rogue	改变所有 Rogue Client 的状态。

注：如果 Client 在被认定为 Rogue 之前是 Authenticated，则状态变为 Authenticated；否则，状态变为 Detected。

3. Debug 的相关配置

命令	解释
特权模式	
debug wireless wids msg no debug wireless wids msg	打开/关闭 WIDS 发送消息的 debug 信息。

4.3 反制功能举例

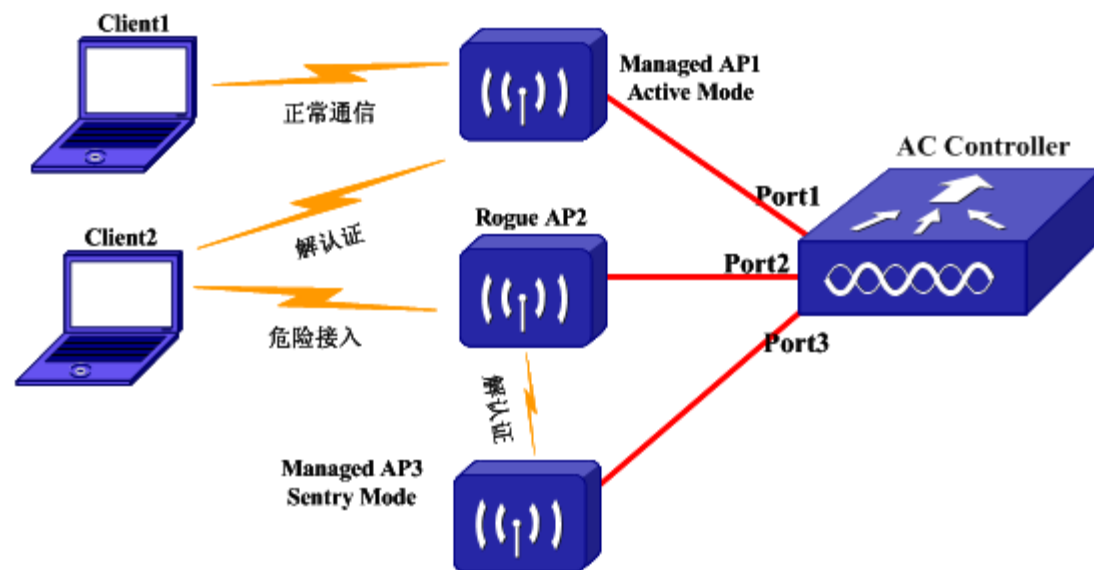


图 4-1 Rogue AP 反制功能案例

如上图所示，Client1 和 Client2 分别通过 AP1 和 AP2 连入无线网络。经检测发现：Client1 和 Client2 都是认证客户端；

- ☞ AP1 是 Managed 状态 Active 模式的合法 AP；
- ☞ AP2 为 Rogue AP；
- ☞ AP3 是 Managed 状态 Sentry 模式的合法 AP；
- ☞ Client2 正通过 Rogue AP2 接入网络。

针对这种情况，应该开启 Rogue AP 反制功能。AC controller 将 AP2 添加到 Rogue AP 攻击列表中，并将列表通过 WIDS-Configuration-Message 发送给所有 AP1 和 AP3。AP1 的 Radio 会发送解认证消息给 Client2；AP3 的 Radio 会假冒 Client2 发送解认证消息给 AP2。为了实现上面的反制过程，需要对 AC controller 进行如下配置：

```
AC>enable
```

```
AC#config
```

```
AC(config)#wireless
```

```
AC(config-wireless)#wids-security ap-de-auth-attack
```

当 AP 无威胁后，网管需要将其 Rogue 状态变更为先前状态：

```
AC(config-wireless)#wireless acknowledge-rogue 00-03-0f-01-02-03
```

```
AC(config-wireless)#no wids-security ap-de-auth-attack
```

4.4 反制功能排错帮助

在配置、使用反制功能时，可能会由于物理连接、配置错误等原因导致本项反制未能正常运行或出现错误反制。请检查是否是如下原因：

- ☞ 应保证物理连接的正确无误

- ☞ 确认已启动反制功能
- ☞ 确认已清除威胁的 Rogue AP 是否恢复了先前状态

第5章 用户隔离

5.1 用户隔离介绍

可运营的 WLAN 网络中，用户之间是互不信任的，所以必须采用用户隔离技术防止用户之间的互相攻击或窃听。同时，如果用户利用局域网互相访问和传递数据，也会占用网络资源，致使网络拥塞，因此在某些场合也必须采用用户隔离禁止用户间互相访问。具体策略如下：

- 1) AP 内部采用 MAC 互访控制原理隔离用户。确保同一 AP 下的用户不能二层相通，只能与上行口相通。
- 2) AP 之间采用 MAC 地址访问控制或组网汇聚设备二层隔离技术如 VLAN/PVLAN/PVC 进行隔离，保证不同 AP 下的用户不能直接相通。
- 3) AC 采用相同端口隔离方式隔离用户。当 AC 的同一端口既是报文入端口又是出端口时，AC 丢弃该报文。

根据AP不同的工作方式，可以将用户隔离分为两大类：集中式转发方式和分布式转发方式。

1、集中式转发方式

集中式转发方式中，AP驱动层不会对802.11数据包做任何处理，直接转成802.3格式封装隧道送往AC处理。因此，用户隔离全部都是在AC上实现。这里主要利用了控制器芯片的L2 Port Bridge功能。

正常情况下，控制器在二层查表时如果发现入端口和出端口一样，会丢弃该报文。但如果开启了Port的L2 Port Bridge功能，则允许二层转发时，从接收的端口再发送回去，每个Port可以单独配置L2 Port Bridge功能，典型的应用就是在WLAN网络中，如下图所示，同一AP下属于相同VLAN的Client要相互通信，必须要开启AC相应Port的L2 Port Bridge功能（如图中的P1）：

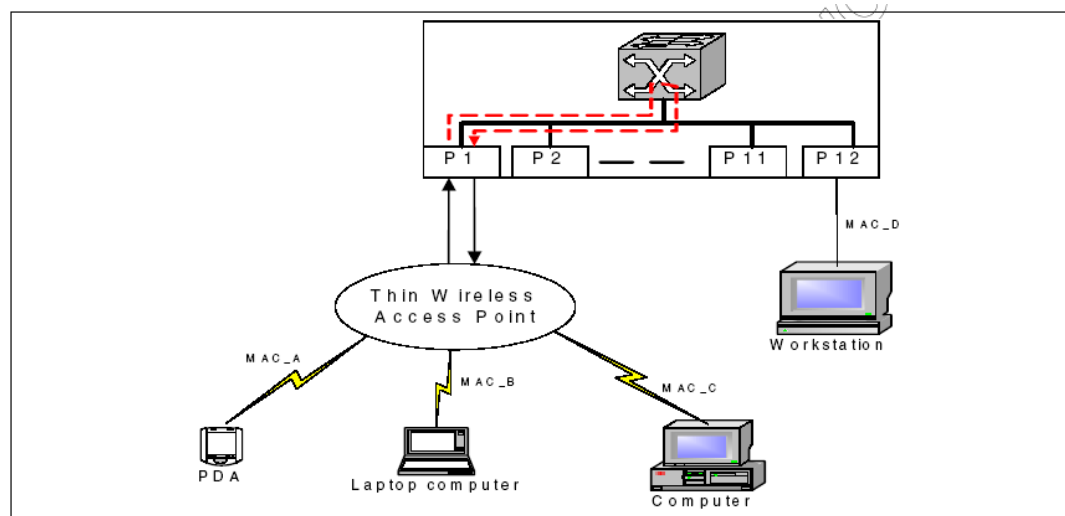


图 5-1 L2 Port Bridge 功能的应用

当然，如果关闭了L2 Port Bridge功能，则AP下相同VLAN的Client在二层就不能互通。同时，它不影响不同VLAN间的三层转发，即经过L3查表转发的报文可以从接收端口发送。

因此，利用L2 Port Bridge功能可以隔离相同VLAN下的无线用户，且不影响不同VLAN间的三层互通。

根据用户所处的不同情况，集中式转发方式时的用户隔离可分为下面四个情况：

- 1) 同一AP下不同SSID之间的用户二层网络的隔离：一般情况下，同一AP下不同SSID之间的用户所属的VLAN不同，他们之间通过VLAN隔离二层网络的互通。如果同一AP下不同SSID分配的VLAN相同，则情况等同于B。
- 2) 同一AP下相同SSID之间的用户二层网络的隔离：同一AP下相同SSID之间的用户所属的VLAN相同，正常情况下可以通过AC进行二层转发，但这时必须开启AC上对应物理Port的L2 Port Bridge功能；如果关闭了L2 Port Bridge，则同一AP下相同SSID之间的用户二层不能互通。
- 3) 不同AP下不同SSID之间的用户二层网络的隔离：一般情况下，不同AP下不同SSID之间的用户所属的VLAN不同，他们之间通过VLAN隔离二层网络，同A；如果不同AP下不同SSID分配相同的VLAN，则情况等同于D
- 4) 不同AP下相同SSID之间的用户二层网络的隔离：不同AP下相同SSID之间的用户有可能VLAN设置是不一样的，这种情况下通过VLAN隔离二层网络；但一般情况下VLAN设置是相同的，这样的话就不能利用VLAN来隔离二层网络了，但由于集中转发方式下AP必须把数据VP送到AC，由AC处理，不同AP和AC建立的VP有可能是通过同一物理端口接入，也可能是通过不同物理端口接入，因此不同AP下相同SSID之间的用户二层网络的隔离时必须考虑下面两种情况：
 - ◆ 如果不同AP和AC建立的VP通过同一物理端口接入，则关闭AC上对应端口的L2 port bridge功能；
 - ◆ 如果不同AP和AC建立的VP通过不同物理端口接入，则可以通过开启不同物理端口间的端口二层隔离来隔离不同物理端口间的二层网络。

2、分布式转发方式

分布式转发方式中，AP驱动层需要对802.11数据包解析，如果目的地址是相同BSSID下的Client，直接转发，否则转成802.3格式送往内部网桥做转发，之后送往有线网络，与传统的有线网络转发类似。因此，用户隔离需要AP和连接的有线网络共同完成。其中，同一AP下的用户隔离是AP控制的，不同AP下的用户隔离是AP连接的有线网络控制的。

根据用户所处的不同情况，分布式转发方式时的用户隔离可分为下面四个情况：

- 1) 同一AP下不同SSID之间的用户二层网络的隔离：一般情况下，同一AP下不同SSID之间的用户所属的VLAN不同，他们之间通过VLAN隔离二层网络的互通。如果同一AP下不同SSID分配的VLAN相同，暂时不做隔离处理。
- 2) 同一AP下相同SSID之间的用户二层网络的隔离：同一AP下相同SSID之间的用户二层网络的隔离通过内部网桥实现。
 - ◆ 没有开启用户隔离时，相同BSSID之间用户互相访问的二层报文在802.11驱动层转发；
 - ◆ 开启用户隔离，即关闭802.11驱动层的转发功能，相同BSSID之间用户互相访

问的二层报文转为802.3格式送往AP内部网桥处理，由内部网桥隔离相同VLAN间的二层报文。

- 3) 不同AP下不同SSID之间的用户二层网络的隔离：一般情况下，不同AP下不同SSID之间的用户所属的VLAN不同，他们之间通过VLAN隔离二层网络的互通。如果不同AP下不同SSID分配的VLAN相同，则情况等同于D。
- 4) 不同AP下相同SSID之间的用户二层网络的隔离：不同AP下相同SSID之间的用户有可能VLAN设置是不一样的，这种情况同C；但一般情况下，VLAN设置是相同的，这样的话就不能利用VLAN来隔离二层网络了，必须利用AP连接的AC的端口隔离进行二层网络的隔离。比较简单的方法是所有控制器的下联口均端口隔离，只能和上联口互通，但有可能不符合某些应用。

5.2 用户隔离配置

1. 开启/关闭 AC 指定端口的二层用户隔离

命令	解释
无线全局配置模式	
l2tunnel station-isolation allowed vlan {WORD add WORD except WORD remove WORD} no l2tunnel station-isolation allowed vlan	打开集中转发式模式下的用户隔离状态，本命令的 no 操作为关闭本隔离。

2. 配置同 VAP 下的用户隔离

命令	解释
Network 配置模式	
station-isolation no station-isolation	启动同 VAP 关联的无线用户隔离功能。 No 命令关闭隔离功能。

3. 配置 RADIO 下的所有 VAP 的用户隔离

命令	解释
Radio 配置模式	
station-isolation no station-isolation	启动 radio 下所有的 VAP 开启用户隔离功能。 No 命令关闭隔离功能。

4. 配置同 VLAN 下的不同 VAP 之间的用户隔离

命令	解释
Profile 配置模式	
station-isolation allowed vlan {[add 	设置 AP 下的属于相同 VLAN 的

<code>remove]] <vlan id>}</code> <code>no station-isolation allowed vlan</code>	VAP 之间的隔离。 No 命令删除隔离 VLAN，关闭隔离功能。
--	--------------------------------------

5.3 用户隔离举例

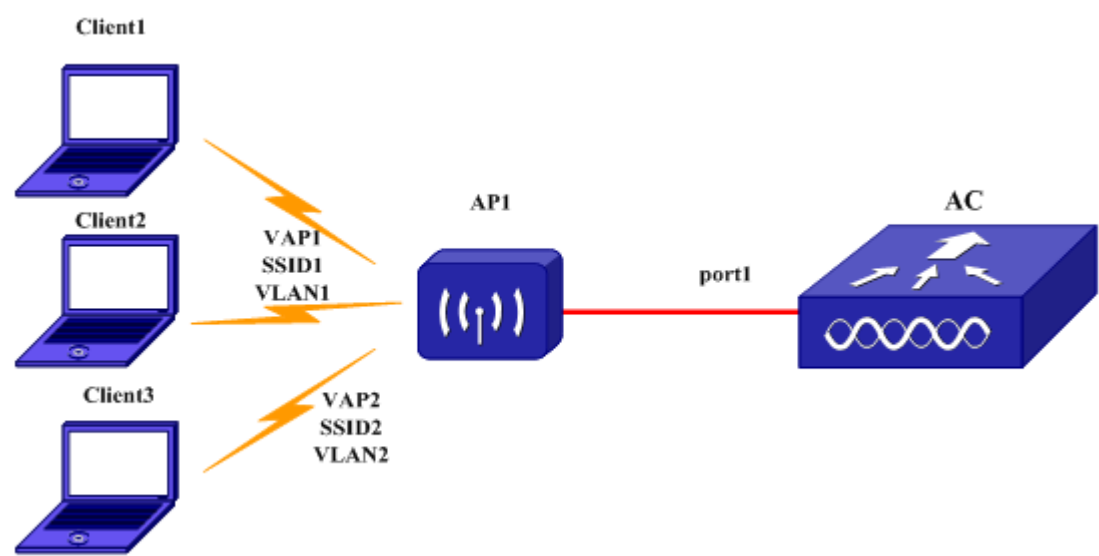


图 5-2 集中式转发方式用户隔离举例

如上图所示的网络中，Client1 和 Client2 接入 AP1，都属于 VLAN1；Client3 接入 AP1，但属于 VLAN2；AP1 工作在集中转发模式下。Client1 与 client3，client2 与 client3 属于不同的 vlan，相互是不通的。由于 Client1 和 Client2 同属于 VLAN1，二者二层是可以互通的。如果要隔离，就必须在 AC 上关闭 port1 的 L2 port bridge 功能，从 Port1 收到的包就不可再送回 Port1，从而隔离了通过 port1 接入 AC 下 AP 的所有 Client 的二层网络。为了达到这样的目的，需要使用控制器指定端口的二层用户隔离的功能并进行相应的配置：

```
AC>enable
AC#config
AC(config)#wireless
AC(config-wireless)#l2tunnel station-isolation allowed vlan 1
```

5.4 用户隔离排错帮助

在配置、使用用户隔离时，可能会由于物理连接、配置错误等原因导致本项隔离未能正常运行或出现错误过滤。请检查是否是如下原因：

- ☞ 首先应该保证物理连接的正确无误；
- ☞ 其次，确认是否属于同一个 VLAN。如果属于同一个 VLAN，在采用集中式转发的情况下，请确认控制器的指定端口是否开启了二层用户隔离；在采用分布式转发的情况下，

请确认是否开启了 AP 上的用户隔离。

第6章 ARP 抑制&ARP 代理

6.1 ARP抑制&ARP代理介绍

AP中的ARP抑制&ARP代理功能是通过检测DHCP报文，记录通过DHCP获取地址且非漫游客户端的MAC与IP的地址映射，通过ARP广播变单播或ARP代理的方式，减少空口的ARP广播报文，以节省Client的电力。

ARP抑制&ARP代理的流程如下：

1. DHCP

当打开ARP抑制功能时，为了及时更新Client的IP信息，需要在AP端检测服务器发往本地无线用户的DHCP报文，从而提取Client的IP信息，保存到本地关联Client的ARP表。

2. ARP 抑制

ARP 抑制（ARP 广播转单播）：AP 收到 ARP Request 报文后，用目的 IP 查询本地关联 Client 的 ARP 表，如果找到符合项，则把目的 mac 由 0xffffffff 改为目的 Client 的 mac 地址，把广播报文转为单播报文，发往目的 Client；如果没有找到，则不作处理。

3. ARP 代理

ARP 代理：DHCP 使 AP 维护了接入的 Client 的 MAC 和 IP 地址映射。在开启 ARP 代理后，收到 ARP-Request，AP 会将维护表中的 mac 地址返回 ARP-Reply（这里是真实的 Client 地址，不是传统代理中填充的 AP mac 地址），而不必将 ARP-Request 向 Client 转发。当 ARP 抑制和 ARP 代理同时开启时，AP 采用 ARP 代理方式处理 ARP 广播报文。

6.2 ARP抑制&ARP代理配置

1.ARP 抑制配置

命令	解释
Network 配置模式	
arp-suppression no arp-suppression	开启/关闭 AP 上的 ARP 抑制功能。

2.ARP 代理配置

命令	解释
Network 配置模式	
proxy-arp no proxy-arp	开启/关闭 AP 上的 ARP 代理功能。

6.3 ARP抑制&ARP代理举例

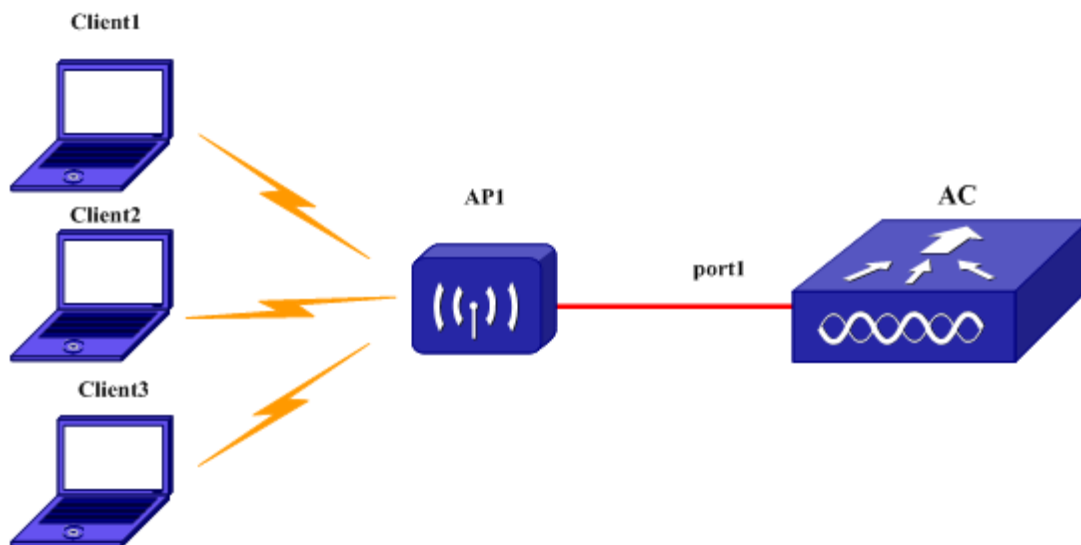


图 1-1 ARP 代理&ARP 抑制举例

如上图所示的网络中，Client1、Client2 和 Client3 都通过 AP1 连接网络。现假设 Client1 想与 Client3 连接，但不知道 Client 的 mac 地址。Client1 会发送 ARP request 信号以广播的形式给所有的客户，这样严重的影响了网络通信的效率。如果此时 AP1 开启了 ARP 抑制，相应的自动使能 ARP 广播转单播，DHCP 帧检测功能，这样 AP1 就记录着本地所有 Authenticated Clients 的 IP 和 Mac 映射表（Client1、2 和 3），则 AP1 接收到 Client1 的 ARP request 信号后，用目的 IP 查询本地关联 Client 的 ARP 表，把目的 mac 由 0xffffffff 改为目的 Client3 的 mac 地址，把广播报文转为单播报文，发往 Client3。为了达到这样的目的，需要使用 ARP 抑制功能并进行相应的配置：

```
AC>enable
AC#config
AC(config)# wireless
AC(config-wireless)#network 1
AC(config-network)# arp-suppression
```

假如此时开启的 ARP 抑制模式为 ARP 代理，则 AP1 接到 Client1 的 ARP request 信号后，AP 会将映射表中 Client3 的 mac 地址返回 ARP-Reply，而不必再将 ARP-Request 广播给所有的 Client。为了达到这样的目的，需要使用 ARP 代理功能并进行相应的配置：

```
AC>enable
AC#config
AC(config)# wireless
AC(config-wireless)#network 1
AC(config-network)# proxy-arp
```

6.4 ARP抑制&ARP代理排错帮助

在配置、使用 ARP 抑制&ARP 代理时，可能会由于物理连接、配置错误等原因导致本项功能运行错误。请检查是否是如下原因：

- ☞ 首先应保证物理连接的正确无误。
- ☞ 其次，确认 Client 获取到的地址是否属于 IPv4。
- ☞ 再次，AP 是否工作在 WDS 模式。
- ☞ 然后，确认是否开启 ARP 抑制或者 ARP 代理。

第7章 动态黑名单

7.1 动态黑名单概述

动态黑名单（Dynamic Blacklist）属于无线安全功能模块中防 DOS 攻击的部分。动态黑名单列表包含将被丢弃帧的终端设备的 MAC 地址。AP 使用该列表，丢弃该名单中的终端设备发送的数据帧。当检测到某个终端设备发送泛洪报文超过安全阈值，将该终端设备添加到黑名单列表。

在无线安全功能中，当新添加一个无线终端记录时，要检查是否符合添加到动态黑名单的条件。在动态黑名单功能开启时，如果符合，将无线终端的 MAC 地址和泛洪攻击的类型添加到动态黑名单。动态黑名单有新的记录添加成功后，查询该 MAC 地址的无线终端所属的 AP 的 IP 地址（如果查询成功，说明该无线终端已经上线），向该 IP 地址下发一条解除与该无线终端连接的命令；对于没有与 AP 连接的无线终端，当它请求连接时，认证模块将查询动态黑名单，检查该无线终端的 MAC 地址是否在黑名单中，如果查询成功，将拒接该无线终端的认证请求。

该名单包含将被丢弃的帧的终端设备的 MAC 的地址。当检测到某个终端设备发送泛洪报文而引起网络拥塞时，通过 WIDS 动态添加黑名单列表。

符合添加到动态黑名单的泛红攻击包括：

- (1) 认证请求帧泛洪攻击（Configured Authentication Rate Test）
- (2) 探查请求帧泛洪攻击（Configured Probe Request Rate Test）
- (3) 解认证请求帧泛洪攻击（Configured De-Authentication Requests Rate Test）
- (4) 认证失败最大次数（Maximum Authentication Failures Test）

开启动态黑名单功能以后，AC 将符合上述条件的 Rogue 设备的 MAC 地址添加到动态黑名单列表，设置表项的老化时间（这个时间可以配置），在老化时间到后，删除此表项。

动态黑名单的表项最多为 128 个，在没有空白表项时，不会添加到动态黑名单中。

7.2 动态黑名单配置

1. 动态黑名单配置

命令	解释
Wireless Config	
dynamic-blacklist no dynamic-blacklist	打开/关闭动态黑名单功能。

2. 动态黑名单老化时间配置

命令	解释
Wireless Config	

dynamic-blacklist lifetime <60-3600> no dynamic-blacklist lifetime	设置动态黑名单的老化时间，no 命令将动态黑名单的老化时间恢复到默认值（300s）
---	---

3. 手动清除动态黑名单中无线终端的配置

命令	解释
Privileged EXEC	
clear dynamic-blacklist (FF-FF-FF-FF-FF-FF)	在动态黑名单中手动删除无线终端的 MAC 地址记录，无指定 MAC 时将清除所有无线终端的 MAC 地址记录。

4. 相关显示配置

命令	解释
特权模式	
show wireless dynamic-blacklist	显示动态黑名单中的所有无线终端记录

7.3 动态黑名单举例

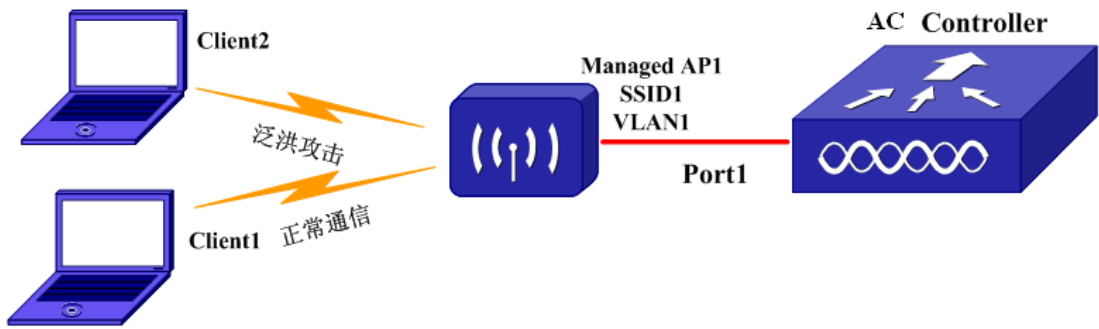


图 7-1 动态黑名单案例

如图所示，Client1 和 Client2 通过 AP1 连入无线网络。Client1 正常通信，Client2 为泛洪攻击中的认证请求帧泛洪攻击，其不断的向 AP1 发送认证请求。要想把发送泛洪攻击帧的 client 加入到动态黑名单中，需要对 AC controller 进行如下配置：

首先开启防泛洪攻击检测：

```
AC > enable
AC # config
AC (config)# wireless
AC (config-wireless)# no wids-security client threshold-interval-auth
AC (config-wireless)# wids-security client threshold-value-auth 6000
```

```
AC (config-wireless)# wids-security client configured-auth-rate
```

然后开启动态黑名单功能以及本地 MAC 认证功能

```
AC(config-wireless)#dynamic-blacklist
```

```
AC(config-wireless)#dynamic-blacklist lifetime 600
```

```
AC(config-wireless)#network 100
```

```
AC(config-network)#mac authentication local
```

7.4 动态黑名单排错帮助

在配置、使用动态黑名单时，可能会由于物理连接、配置错误等原因导致动态黑名单未能正常运行。下面将分别对 2 种错误情况的排错进行说明：

动态黑名单未能正常运行：

首先应该保证物理连接的正确无误；

其次，确认已配置启动符合动态黑名单条件威胁检测（详见上节相应检测的配置）。

再次，确认已配置启动动态黑名单和在 `network` 下配置启动 MAC 本地认证（详见上节相应动态黑名单和 MAC 认证的配置）。

出现错误动态黑名单记录：

认证请求帧泛洪攻击、探查请求帧泛洪攻击、解认证请求帧泛洪攻击和认证失败最大次数，确认相应阈值设置是否合适，相应的设备是否都检测为 `rogue`。

相应设备的动态黑名单记录是否超出保活时间。

第8章 无线 SAVI

8.1 无线SAVI技术简介

SAVI 全称 Source Address Validation Improvement，中文称为“源地址验证改进”。有线网络环境里实现的 SAVI 称为有线 SAVI，无线网络环境中实现的 SAVI 称为无线 SAVI，本手册描述的是后者。有线 SAVI 与无线 SAVI 的基本原理相同，都是在接入设备上建立 SAVI 表项，然后根据 SAVI 表项对终端 IP 报文进行过滤，只有符合条件的 IP 报文才被放行。

SAVI 的主要目的是验证终端（STA）IPv4/IPv6 报文的源 MAC、源 IP 真实有效性。为了达到这个目的，无线 SAVI 会让 AP（Access Point）监听终端使用 DHCP/DHCPv6 获取地址的过程以及终端发出的 IPv6 DAD NS/NA（地址冲突检测 NS/NA）报文，通过监听这些报文，在 AP、AC 上建立 MAC、IP（STA 的 MAC、IP）两元组表项，根据这个两元组对终端 IP 报文进行过滤，符合条件的被放行，不符合条件的被丢弃。

SAVI 的另外一个目的是防止终端私设 IP 地址。无线 SAVI 一直防止终端私设 IPv4 地址；无线 SAVI 可以选择性的防止终端私设 IPv6 地址。为了达到这个目的，无线 SAVI 会让 AP 选择是否需要监听终端发出的 IPv6 DAD NS/NA 建立 MAC、IP（STA 的 MAC、IP）两元组表项。

无线 SAVI 功能还允许网络管理员为长久占用某个 IP 地址的终端配置静态 SAVI 表项，这类终端可以使用静态配置的 IP 地址访问网络。

8.2 无线SAVI配置

无线 SAVI 的配置序列：

- 1. 配置 SLAAC 类型动态绑定的生存周期
- 2. 配置为同一个 STA 建立的最多 SAVI 动态绑定表项数量
- 3. 配置在一个 AP 上建立的最多 SAVI 动态绑定表项数量
- 4. 配置防止 STA 私设 IPv6 地址
- 5. 配置静态 SAVI 表项
- 6. 在 AP profile 模式下开启 SAVI 功能
- 7. 应用 AP profile，下发配置到相应的 AP

- 1. 配置 SLAAC 类型动态绑定的生存周期

命令	解释
无线全局配置模式	
savi ipv6-nd lifetime <1-31536000> no savi ipv6-nd lifetime	全局配置 SAVI SLAAC 类型动态绑定处于 BOUND 状态的生存周期，默认生存周期为 4 小时(14400 秒)，最大 31536000 秒（365 天）。

	no 命令恢复默认配置。
--	--------------

2. 配置为同一个 STA 建立的最多 SAVI 动态绑定表项数量

命令	解释
AP profile 配置模式	
savi dyn-mac-binding-limit<8-16> no savi dyn-mac-binding-limit	配置为同一个 STA 建立的最多 SAVI 动态绑定表项数量，默认最大数量为 8，范围是 8-16（静态表项不计算在内）。 no 命令恢复默认配置。

3. 配置在同一个 AP 建立的最多 SAVI 动态绑定表项数量

命令	解释
AP profile 配置模式	
savi binding-limit <0-320> no savi binding-limit	配置在同一个 AP 建立的最多 SAVI 动态绑定表项数量，默认值是 240 个，范围是 0-320（静态表项不计算在内）。 no 命令恢复默认配置。

4. 配置防止 STA 私设 IPv6 地址

命令	解释
AP profile 配置模式	
savi ipv6-slaac enable no savi ipv6-slaac enable	关闭防止 STA 私设 IPv6 地址。 no 命令开启防止 STA 私设 IPv6 地址。

5. 配置静态 SAVI 表项

命令	解释
无线全局配置模式	
savi binding <client-mac> <ipv4 ipv6> <client-ip> no savi binding <ipv4 ipv6> <client-ip>	全局创建 SAVI 静态绑定表项功能，创建的表项为静态表项，类型为 STATIC。参数 <client-mac>是 STA 的 MAC 地址，格式 XX-XX-XX-XX-XX-XX；参数<client-ip>是 STA 的 IP 地址。 no 命令是删除相应的静态绑定，删除时不必再指定 STA 的 MAC 地址。

6. 在 AP profile 模式下开启 SAVI 功能

命令	解释
AP profile 配置模式	
savi enable	在 AP profile 下管理的 AP 上开启 SAVI 功

no savi enable	能，对 STA IP 报文的源 MAC、IP 进行有效性验证。 no 命令在该 AP profile 下管理的 AP 上关闭 SAVI 功能。
-----------------------	--

7. 应用 AP profile，下发配置到相应的 AP

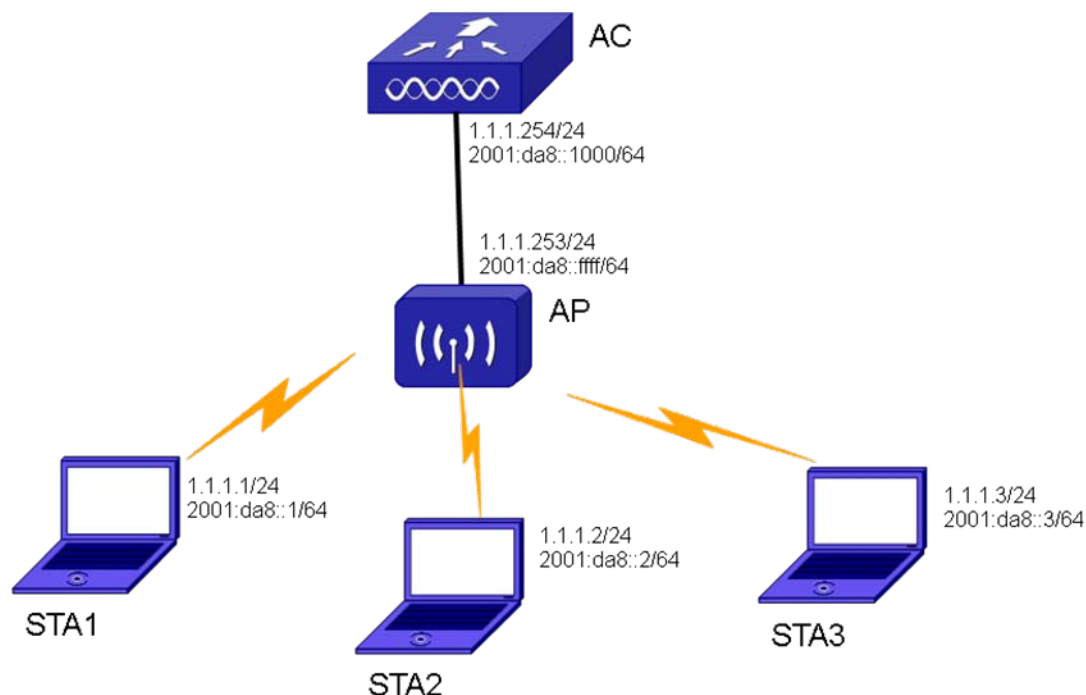
命令	解释
特权配置模式	
wireless ap profile apply	开启、关闭 SAVI 功能，都需要手动下发配置才能生效。 在 SAVI 功能开启时，修改 savi ipv6-nd lifetime <1-31536000>会自动下发配置到 AP；在 SAVI 功能关闭时，修改 savi ipv6-nd lifetime <1-31536000>不会自动下发配置到 AP。 不管是否开启 SAVI 功能，修改其它 SAVI 参数都会自动下发配置，不需要手工下发。

8.3 无线 SAVI 功能举例

案例 1:

对无线 STA 发出的 IP 报文做源地址有效性验证。

AC 使用 ap profile 1 管理 AP，在 profile 1 上开启 SAVI 功能，下发配置。



(1) AC 配置如下:

Wireless

Ap profile 1

Savi enable

Exit

Exit

Exit

Wireless ap profile apply 1

Sta1 关联到 AP, 获取 IPv4 地址 1.1.1.1, 获取 IPv6 地址 2001:da8::1。

Sta2 关联到 AP, 获取 IPv4 地址 1.1.1.2, 获取 IPv6 地址 2001:da8::2。

Sta3 关联到 AP, 获取 IPv4 地址 1.1.1.3, 获取 IPv6 地址 2001:da8::3。

Sta1 可以 ping 通 1.1.1.2、1.1.1.3、2001:da8::2、2001:da8::3。

sta1 使用发包软件发出源 mac 为 sta1-mac、源 IP 为 1.1.1.2, 目的 mac 为 sta3-mac、目的 IP 为 1.1.1.3 的 IP 数据流量, 在 sta3 上抓取不到这个流量。

Sta1 使用发包软件发出源 mac 为 sta1-mac、源 IP 为 2001:da8::2, 目的 mac 为 sta3-mac、目的 IP 为 2001:da8::3 的 IP 数据流量, 在 sta3 上抓取不到这个流量。

(2) 在 AC 关闭无线 SAVI 功能重试上面的操作。

AC 配置如下:

Wireless

Ap profile 1

No savi enable

Exit

Exit

Exit

Wireless ap profile apply 1

Sta1 关联到 AP，获取 IPv4 地址 1.1.1.1，获取 IPv6 地址 2001:da8::1。

Sta2 关联到 AP，获取 IPv4 地址 1.1.1.2，获取 IPv6 地址 2001:da8::2。

Sta3 关联到 AP，获取 IPv4 地址 1.1.1.3，获取 IPv6 地址 2001:da8::3。

Sta1 可以 ping 通 1.1.1.2、1.1.1.3、2001:da8::2、2001:da8::3。

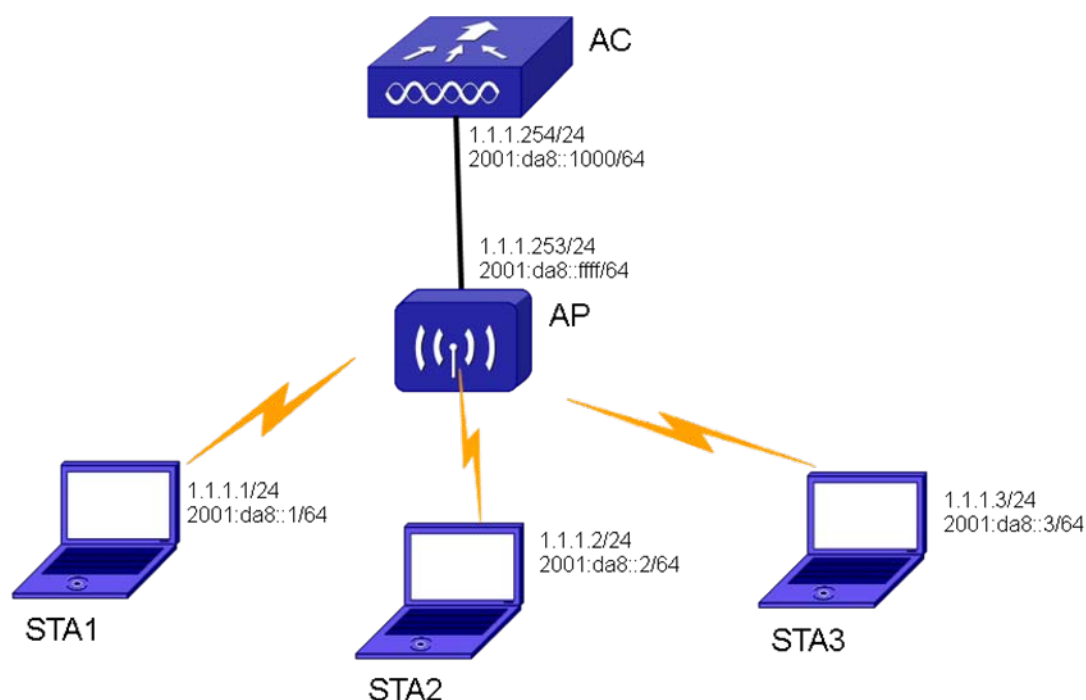
sta1 使用发包软件发出源 mac 为 sta1-mac、源 IP 为 1.1.1.2，目的 mac 为 sta3-mac、目的 IP 为 1.1.1.3 的 IP 数据流量，在 sta3 上可以抓取到这个流量。

Sta1 使用发包软件发出源 mac 为 sta1-mac、源 IP 为 2001:da8::2，目的 mac 为 sta3-mac、目的 IP 为 2001:da8::3 的 IP 数据流量，在 sta3 上可以抓取到这个流量。

案例 2:

防止 STA 私设 IP 地址。

AC 使用 ap profile 1 管理 AP，在 profile 1 上开启 SAVI 功能，下发配置。



(1) AC 配置如下:

Wireless

Ap profile 1

Savi enable

No savi ipv6-slaac enable

```
Exit
Exit
Exit
Wireless ap profile apply 1
```

Sta1 配置静态 IPv4 地址 1.1.1.1，配置静态 IPv6 地址 2001:da8::1，关联到 AP。

Sta2 关联到 AP，获取 IPv4 地址 1.1.1.2，获取 IPv6 地址 2001:da8::2。

Sta3 关联到 AP，获取 IPv4 地址 1.1.1.3，获取 IPv6 地址 2001:da8::3。

Sta1 不能 ping 通 1.1.1.2、1.1.1.3、2001:da8::2、2001:da8::3。

(2) 在 AC 上关闭防私设 IPv6 地址功能重试上面的操作。

```
Wireless
Ap profile 1
savi ipv6-slaac enable
exit
exit
exit
wireless ap profile apply 1
```

Sta1 配置静态 IPv4 地址 1.1.1.1，配置静态 IPv6 地址 2001:da8::1，关联到 AP。

Sta2 关联到 AP，获取 IPv4 地址 1.1.1.2，获取 IPv6 地址 2001:da8::2。

Sta3 关联到 AP，获取 IPv4 地址 1.1.1.3，获取 IPv6 地址 2001:da8::3。

Sta1 不能 ping 通 1.1.1.2、1.1.1.3，但可以 ping 通 2001:da8::2、2001:da8::3。

8.4 无线SAVI排错帮助

在使用无线 SAVI 过程遇到问题，请检查是否如下原因造成的：

- ☞ 因为无线 SAVI 是以 ap profile 为单位开启的，所以请先确定是否在正确的 ap profile 下开启的 SAVI。
- ☞ STA 关联进网络，不能使用 IPv6 地址访问网络，请确认是否关闭了防私设 IPv6 地址功能，关闭防私设 IPv6 地址功能的命令是 `savi ipv6-slaac enable`。
- ☞ STA 关联进网络，持续 4 小时后不能使用 IPv6 地址访问网络，请调整 SLAAC 类型 SAVI 绑定的生存周期，命令是 `savi ipv6-nd lifetime <1-31536000>`。
- ☞ STA 关联进网络，无法 dhcp 获取 ip 地址，请确认是否关联 AP 已经到达 SAVI 绑定表的表项容量上限。当达到 AP 上限的时候，无法创建新的动态绑定，可以使用命令 `savi binding-limit <0-320>` 配置更大数值以满足需求。

第9章 DHCP 抑制

9.1 DHCP抑制介绍

AP中的DHCP抑制功能是根据DHCP报文中的FLAGS字段将DHCP OFFER/ACK报文广播转单播的方式，减少空口的DHCP广播报文，以节省Client的电力。

DHCP抑制的流程如下：

1. DHCP

当打开DHCP抑制功能时，需要在AP端检测服务器发往本地无线用户的DHCP报文，从而提取DHCP报文中的FLAGS信息。

2. DHCP 抑制方式

DHCP 广播转单播：AP 收到 DHCP 发现/请求报文后，根据 DHCP 报文中的 FLAGS 字段，如果报文中 FLAGS 为 0，则把目的 mac 由 0xffffffff 改为目的 Client 的 mac 地址，把广播报文转为单播报文，发往目的 Client；报文中 FLAGS 为 1，则不作处理。

9.2 DHCP抑制配置

1.DHCP 抑制配置

命令	解释
Network 配置模式	
dhcp-suppression no dhcp-suppression	开启/关闭 AP 上的 DHCP 抑制功能。

9.3 DHCP抑制举例

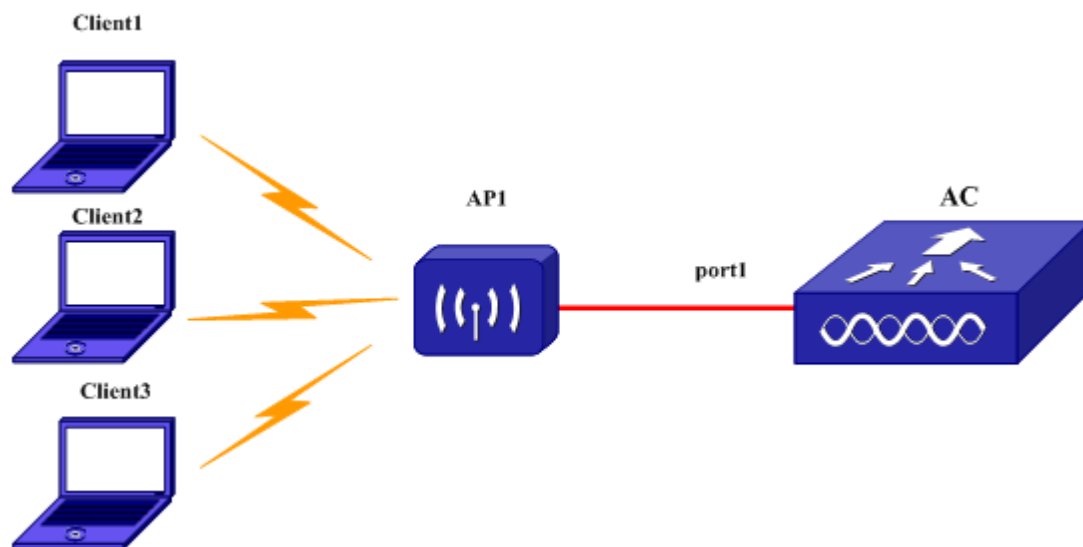


图 3-1 DHCP 代理举例

如上图所示的网络中，Client1、Client2 和 Client3 都通过 AP1 连接网络。现假设 Client1 通过 DHCP 获取地址，Client1 会将发送 DHCP 发现/请求报文以广播的形式给所有的设备，当 DHCP 服务器收到 DHCP 发现/请求报文后同样会将回复的报文以广播方式发往整个网络。如果此时 AP1 开启了 DHCP 抑制，会检查 DHCP 发现/请求报文中的 FLAGS，如果 FLAGS 为 0，AP1 将 DHCP OFFER/ACK 报文广播转单播后发往 Client1，而不必再将 DHCP 报文广播给所有的 Client。

为了达到这样的目的，需要使用 DHCP 代理功能并进行相应的配置：

```
AC>enable
AC#config
AC(config)# wireless
AC(config-wireless)#network 1
AC(config-network)# dhcp-suppression
```

9.4 DHCP抑制排错帮助

在配置、使用 DHCP 抑制时，可能会由于物理连接、配置错误等原因导致本项功能运行错误。请检查是否是如下原因：

- ☞ 首先应保证物理连接的正确无误。
 - ☞ 其次，确认 Client 是否是通过 IPV4 获取地址。
 - ☞ 再次，AP 是否为 WDS 模式。
- 然后，确认是否开启 DHCP 抑制。