

目录

第 1 章 RFPing	1-1
1.1 RFPing介绍	1-1
1.2 RFPing基本配置.....	1-1
1.3 RFPing配置举例.....	1-1
1.4 RFPing排错帮助.....	1-2
第 2 章 空口抓包.....	2-1
2.1 空口抓包介绍	2-1
2.2 空口抓包配置	2-2
2.3 空口抓包举例	2-3
2.4 空口抓包排错帮助	2-5
第 3 章 频谱分析.....	3-1
3.1 频谱分析介绍	3-1
3.2 频谱分析配置	3-1
3.3 频谱分析举例	3-2
3.4 频谱分析排错帮助	3-3
第 4 章 smtp	4-1
4.1 smtp介绍	4-1
4.2 smtp基本配置.....	4-1
4.3 smtp配置举例.....	4-2
4.4 smtp排错帮助.....	4-4

第1章 RFPing

1.1 RFPing 介绍

为了监测 AP 和关联的客户端之间的无线链路通信质量，系统管理员可能需要获取 AP 和该客户端之间的无线链路连接信息，如信号强度，报文重传次数，RTT(Round-trip Time, 往返时延)等。为此，我司开发主动侦测无线终端的链路质量功能：RFPing。该功能是在 AC 上下发命令链路监测命令给 AP，使 AP 以指定客户端所支持的所有速率向该客户端发送空数据帧，然后 AP 收集回应报文信号强度及平均时延等信息并发送给 AC 回显。

1.2 RFPing 基本配置

1) 开启 RFPing 功能

命令	解释
特权模式	
wireless link-test <client-MAC> (count <1-100>) (timeout <1000-5000>)	开启 RFPing 功能 <client-MAC>: 需要测试 client 的 mac 地址，仅允许测试已关联的无线客户端 count <1-100>: radio 接口以每种速率发送 ping 包的个数 timeout <1000-5000>: radio 接口等待 ping 包响应的最大超时时间，单位为 ms

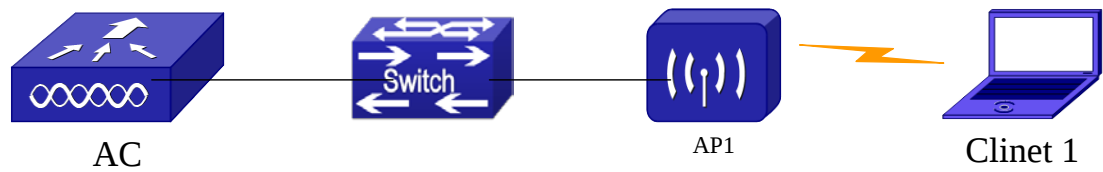
2) 停止 RFPing 功能

命令	解释
特权模式	
ctrl+c	关闭 RFPing 功能，停止链路测试

3) RFPing 功能的 debug 调试

命令	解释
特权模式	
debug wireless link-test msg no debug wireless link-test msg	打开/关闭 RFPing 功能 debug 调试，可以看到 ac 和 ap 之间的消息交互，包括：命令下发、信息上报、停止测试消息

1.3 RFPing 配置举例



搭建环境，AC 通过 switch 或 poe 和 ap 相连，ap 被成功管理；client1 关联 ap1。

1、AC 基本配置：

AC#wireless link-test e0-46-9a-b1-fa-ef count 5 timeout 3000

Client 关联 ap1，在 ac 可以看到 client 关联成功。配置 Client 每种速率的发包次数为 5，配置超时时间为 3000ms，点击“回车”开始测试。测试效果如下：

AC#wireless link-test e0-46-9a-b1-fa-ef count 5 timeout 3000

Testing link to client e0-46-9a-b1-fa-ef, press CTRL_C to break.....

link Status

RTT:Round trip time

Client MAC Address:e0-46-9a-b1-fa-ef

No./MCS	Rate(Mbps)	Txcnt	RxCnt	RSSI	Retries	RTT(ms)
6	12	5	5	54	0	0
7	18	5	5	53	0	0
8	24	5	5	53	0	0
9	36	5	5	53	0	0
10	48	5	5	53	0	0
11	54	5	5	52	0	0
MCS-0	6.5	5	5	52	0	0
MCS-1	13	5	5	53	0	0
MCS-2	19.5	5	5	53	0	0
MCS-3	26	5	5	53	0	0
MCS-4	39	5	5	53	0	0
MCS-5	52	5	5	53	0	0
MCS-6	58.5	5	5	53	0	0
MCS-7	65	5	5	53	0	0
MCS-8	13	5	5	53	0	0
MCS-9	26	5	5	53	0	0
MCS-10	39	5	5	52	0	0
MCS-11	52	5	5	52	0	0

MCS-12	78	5	5	52	0	0
MCS-13	104	5	5	52	0	0
MCS-14	117	5	5	52	0	0
MCS-15	130	5	5	52	0	0

No more Rate, link-test complete!

AC#

1.4 RFPing 排错帮助

- ☞ 测试中可能出现配置的 radio 模式是带宽 40M、GI=400，但是测试速率中显示带宽 20M、GI=800 的协商速率，这个原因是 client 和 ap 在协商的过程中，由于链路质量等问题，高速率向低速率兼容，协商为低速率；
- ☞ 测试中可能出现 client 突然掉电后，链路测试依然进行，这个原因是 ap 上的 client 还没有删除，测试仍在继续。

第2章 空口抓包

2.1 空口抓包介绍

在实际的无线组网中，经常出现信号干扰或者报文冲突的问题，而这一类的问题通常很难通过无线设备上的调试信息或显示信息进行定位。为了便于管理员能够在远程快速定位此类问题，可以将某个 AP 作为抓包工具，用于侦听、捕获和记录无线报文。捕获到的无线报文信息会保存在文件类型为“.pcap”的记录文件中，供管理员参考及定位问题使用。如下图所示，通过开启 Capture AP 上的无线抓包功能，可以捕获空口中的无线报文，包括无线环境中的其他 AP、Rogue AP、Client 等；同时，通过配置 Capture AP 上的无线捕获有线端口，也可以捕获经过 Capture AP 的有线报文。

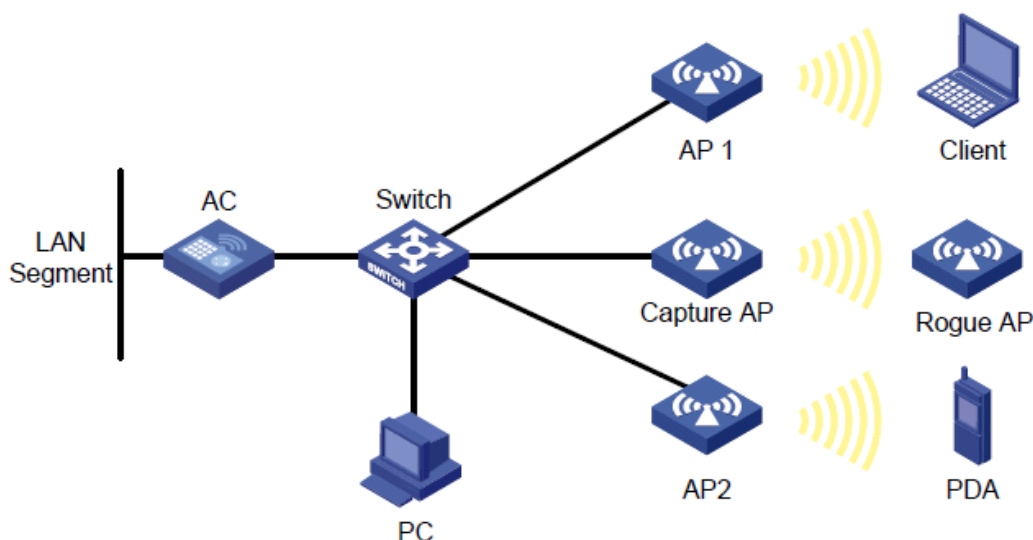


图 2-1 无线捕获组网图

无线捕获的过程分为命令开启、报文截获、报文传送、报文处理四个部分。无线捕获工作在两种模式下：文件捕获模式和远程捕获模式。

在文件捕获模式下，管理员在 AC 上配置无线捕获模块的相关参数，AC 把命令和参数以消息的形式发送给 Capture AP，开启无线抓包功能。被捕获的报文存储在 Capture AP 的一个文件中，Capture AP 抓包结束后，以 pcap 格式的文件形式发送给 AC。管理员将抓包得到的文件下载到本地，能够使用一些工具对报文进行进一步分析，如 Wireshark 和 OmniPeek。

在远程捕获模式下，被捕获的报文被实时重定向到一个正在运行 Wireshark 工具的外部 PC 上，远程无线捕获适用于与 Windows 的 WireShark 网络分析工具共同工作。一个无

线捕获服务器运行在 AP 上，并且通过 TCP 连接发送捕获报文到 Wireshark 工具。当使用远程捕获模式时，Capture AP 不存储任何捕获数据到本地的文件系统。Capture AP 使用配置消息中 AC 下发的参数，开始进行报文捕获，实时将捕获到的数据远程到监控软件中，常用的监控软件是 Wireshark；Capture AP 上不会保存捕获到的数据。在 PC 机上开启监控软件，以 Wireshark 为例（版本为 1.6.0.37592），打开软件，选择“Capture -> Option”，弹出对话框如下图所示：

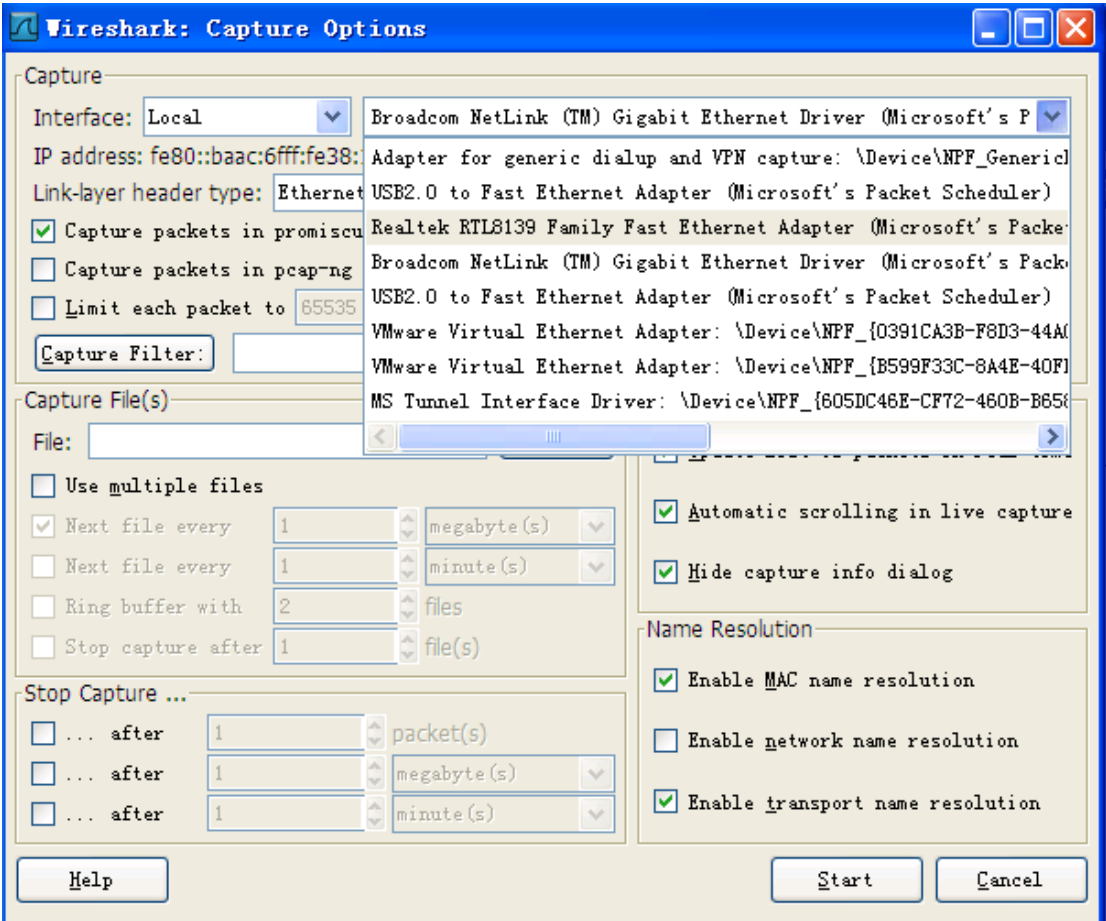


图 2-2 option 选择界面

选择 interface 为 remote 之后出现对话框如下图所示：

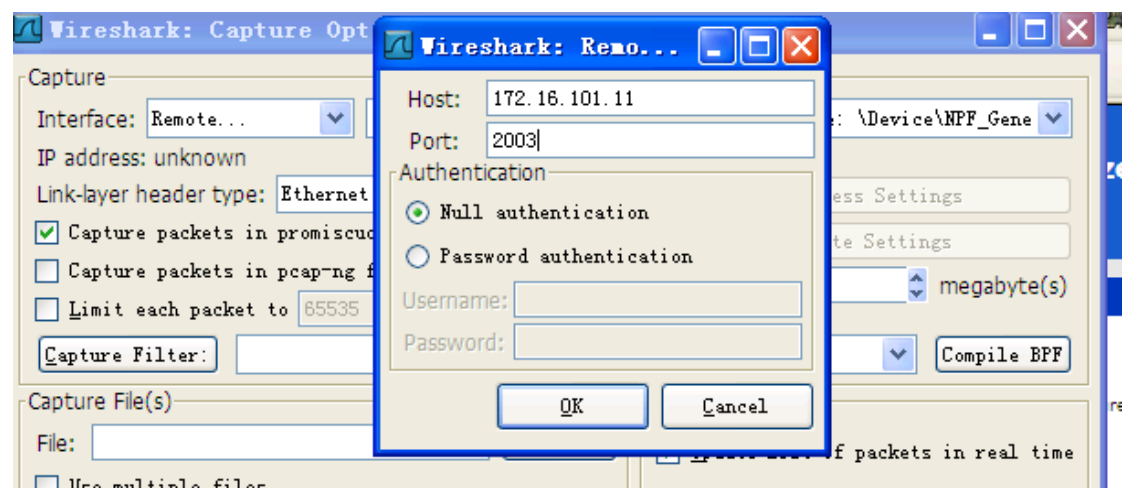


图 2-3 选择 remote 后弹出的界面

Capture AP 直接将捕获到的数据发送到 Wireshark 上，对于 Wireshark 而言，Host 中应该填的是 Capture AP 的 IP 地址，并且保证两者可以互相通信；因为在 AC 上配置的远程无线捕获的端口为 2003，所以 Port 中填的是 2003，默认值为 2002。设置完以上的参数后，点击 OK 回到 option 选择界面的对话框，在 interface 的右侧下拉列表中选择无线捕获的类型，然后点击 Start 按钮，就会在 Wireshark 看到实时显示的抓包结果。

2.2 空口抓包配置

空口抓包的配置序列如下：

- 1. 配置空口抓包的报文捕获模式
- 2. 配置空口抓包相关参数
 - 1)配置混杂模式抓包
 - 2)配置 file 模式抓包时间限制
 - 3)配置 file 模式抓包数量限制
 - 4)配置 mac 地址过滤条件
- 3. 配置控制某个 AP 开启空口抓包

1. 配置空口抓包的报文捕获模式

命令	解释
特权模式	
wireless capture mode {file remote [<2002-2006>]}	配置 AP 无线抓包捕获模式，文件捕获或远程捕获。
no wireless capture mode	

2. 配置空口抓包相关参数

1) 配置混杂模式抓包

命令	解释
特权模式	
wireless capture promiscuous-mode no wireless capture promiscuous-mode	配置开启混杂模式抓包。

2) 配置 file 模式抓包时间限制

命令	解释
特权模式	
wireless capture duration <60-3600> no wireless capture duration	file 模式下，可以配置捕获报文的限制时间。

3) 配置 file 模式抓包数量限制

命令	解释
特权模式	
wireless capture packet-num <1-10000> no wireless capture packet-num	file 模式下，可以配置捕获报文的最大个数限制。

4) 配置 mac 地址过滤条件

命令	解释
特权模式	
wireless capture filter-mac <macaddr> no wireless capture filter-mac	可以配置报文捕获的 mac 地址过滤条件。

3. 配置控制某个 AP 开启空口抓包

命令	解释
特权模式	
wireless capture start ap <macaddr> interface {radio <1 2> ethernet }	配置完上述参数后，管理员可以选择 AP 和抓包接口，下发开始抓包的命令。

2.3 空口抓包举例

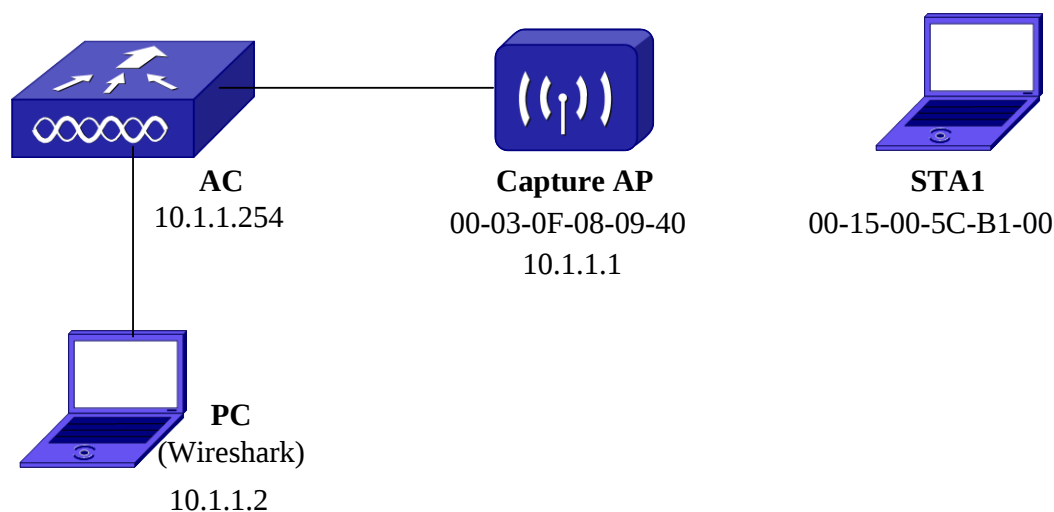


图 2-4 空口抓包案例应用拓扑

拓扑简介：

上图中，Capture AP 被 AC 管理，同时与地址为 10.1.1.2 的 PC 同一网段；STA1 关联到 Capture AP 上，可以通过 AC 控制 Capture AP 空口抓包。

应用 1：采用文件捕获模式，控制 Capture AP 捕获 Radio1 频段包含有 STA1 mac 地址的所有空口报文，设置捕获时长为 2min，捕获报文数量为默认值。

配置文件捕获模式。

```
AC#wireless capture mode file
```

配置开启混杂模式抓包。

```
AC#wireless capture promiscuous-mode
```

配置抓包时长为 120s。

```
AC#wireless capture duration 120
```

配置过滤 STA1 mac 地址条件。

```
AC#wireless capture filter-mac 00-15-00-5c-b1-00
```

配置 Capture AP 在 radio1 抓包。

```
AC#wireless capture start ap 00-03-0f-08-09-40 interface radio 1
```

抓包开始后，查看抓包状态。

```
AC#show wireless capture status
```

```
wireless capture status..... Enable
```

```
Capture ap MAC..... 00-03-0f-08-09-40
```

```
wireless capture running status..... wireless capture in progress
```

```
wireless download status..... ----  
wireless capture mode..... file  
wireless capture interface..... radio 1  
wireless capture duration..... 120  
wireless capture packet number..... 10000  
wireless capture filter mac..... 00-15-00-5c-b1-00  
wireless capture promiscuous mode..... Enable
```

可以手动停止抓包，也可以等到 120s 后 AP 自动停止，也可能是抓包数量达到了 10000 个 AP 自动停止，停止后 AP 会上传抓包文件至 AC，文件名为“file_capture.pcap”，可以将文件再传到 PC 上，用 Wireshark 或 Omnipcap 分析。

应用 2：采用远程捕获模式，控制 Capture AP 捕获通过自己有线口的报文。

```
AC#wireless capture mode remote 2003
```

In remote mode, the capture duration and packet numbers parameters will be ignored by Capture AP.

```
AC#wireless capture start ap 00-03-0f-09-51-30 interface ethernet
```

```
AC#show wireless capture status
```

```
wireless capture status..... Enable  
Capture ap MAC..... 00-03-0f-08-09-40  
wireless capture running status..... wireless capture in progress  
wireless download status..... ----  
wireless capture mode..... remote  
Remote port..... 2003  
wireless capture interface..... ethernet  
wireless capture duration..... 3600  
wireless capture packet number..... 10000  
wireless capture filter mac..... ----  
wireless capture promiscuous mode..... Enable
```

抓包开启后，在 PC 上 Wireshark 打开远程端口 10.1.1.1:2003，可以直接显示出 Capture AP 抓到的报文。

2.4 空口抓包排错帮助

当在使用 AP 空口抓包过程中遇到问题时，请检查是否是如下原因：

- ☞ 抓取其它 AP 或客户端交互的报文时，确定混杂模式是否打开。
- ☞ 抓取其它 AP 或客户端交互的报文时，要确保 Capture AP 与它们同一 channel。

- ☞ 文件模式抓包时，AC 上是否有足够的 flash 空间存储抓包文件(AP 会根据这个空间限定抓包的多少，如果空间太小，能抓到的报文就相应很少)。
- ☞ 抓无线报文时，没有抓到需要的报文，需确定抓包的过程中 Capture AP 相应的 radio 没有被 down 掉。

第3章 频谱分析

3.1 频谱分析介绍

AP 为无线用户提供 WLAN 服务，为了保障服务的质量，进行射频管理是必须的。射频管理是指对 AP 的射频参数进行设置，包括信道、速率、发射功率等，降低信道间的干扰，平衡客户端负载，实现信道资源的公平分配，尽可能为无线用户提供优质服务。在开放的无线环境中，各类应用程序和设备共享频谱资源。频谱分析作为射频管理的一部分，能够实时地了解无线频谱的使用情况，逐渐被提上日程，以便于管理射频干扰并防止意外停机。

无线信号的传播受周围环境影响，无线环境是在不断变化的，移动的障碍物、正在工作的微波炉、蓝牙设备、游戏手柄等带来的干扰都可能对无线信号的传播造成影响，所以实时了解无线环境中频谱资源的使用情况，能够帮助无线网络管理员作出决策，调整 AP 的信道、发射功率等射频参数，来保证无线服务的质量。

频谱分析对非 802.11 射频干扰源及其对 WLAN 性能的影响提供一层重要的可视能力。从实现原理上来说，频谱分析就是对搜集到的信号进行傅里叶变换，把原本随时间变化的信号表示方式，变换为随频率变化的信号表示方式，从而能够清晰地了解无线频谱的使用情况，并可以检测出、识别并且帮助定位单个射频干扰源，包括蓝牙、无绳电话、微波设备等多种设备。

从实现方法上来讲，AC 将频谱分析所需的参数（频谱分析开关和频谱分析结果上报间隔等参数）通过消息的方式下发给 AP，AP 解析消息，根据下发的配置进行频谱扫描，将扫描到的信号做快速傅里叶变换及分类等处理后，以消息的方式将频谱分析结果间歇性地上报给 AC，AC 收到消息后进行解析，并存储频谱分析结果，到达清空记录时间时做一次清空结果。

3.2 频谱分析配置

频谱分析的配置序列如下：

- 1. 开启频谱分析功能
- 2. 配置频谱分析相关参数
 - 1)配置频谱分析结果上报时间间隔
 - 2)配置频谱分析结果老化时间
- 3. 查看频谱分析结果
- 1. 使能/关闭频谱分析功能

命令	解释
Radio 配置模式	
spectral-scan	打开/关闭某 profile 下所有 AP 的频谱分析功
no spectral-scan	能

2. 使能/关闭 AP 向网管上报频谱分析数据功能

命令	解释
Radio 配置模式	
spectral-scan gui-report no spectral-scan gui-report	打开/关闭某 profile 下所有 AP 向网管上报频谱分析数据功能

3. 配置频谱分析相关参数

1) 配置频谱分析结果上报间隔

命令	解释
Profile 配置模式	
spectral-scan-report-interval <1, 300> no spectral-scan-report-interval	spectral-scan-report-interval <1, 300>:配置 ap 上报频谱分析结果的时间间隔; no spectral-scan-report-interval: 将频谱分析结果上报时间间隔恢复为默认值, 默认 5s。

2) 配置频谱分析结果老化时间

命令	解释
Wireless 配置模式	
agetime spectral-scan <0, 300> no agetime spectral-scan	agetime spectral-scan <0, 300>: 配置 AC 上频谱分析结果老化时间, 0 为不老化 no agetime spectral-scan: 将 AC 上频谱分析结果老化时间恢复默认值, 默认 15 分钟

4. 查看频谱分析结果

1) 显示频谱分析功能状态

命令	解释
特权模式	
show wireless ap profile <1-1024> radio <1-2>	查看某 profile 下的 AP 的频谱分析功能是否打开

2) 查看参与频谱分析的 AP 列表

命令	解释
特权模式	
show wireless ap spectrum monitors	查看当前添加到频谱分析任务中的 AP 列表

3) 查看 AP 进行频谱扫描的信道信息

命令	解释
特权模式	
show wireless ap <macaddr> radio <1-2> spectral-scan channel status	查看 ap 进行频谱分析的信道概要, 包括扫描信道、信道中心频率、该信道的信道质量

4) 查看 AP 频谱分析的结果

命令	解释
特权模式	
show wireless ap <macaddr> radio <1-2> spectral-scan interference status	查看 AP 频谱分析结果, 包括干扰设备类型、中心频点、干扰信号的最大、最小频率、影响的信道

5) 清除 AP 频谱分析的结果

命令	解释
特权模式	
clear wireless ap [<macaddr> [radio <1-2>]] spectral-scan list	使用该命令清除指定 AP 或所有 AP 的频谱分析结果

3.3 频谱分析举例

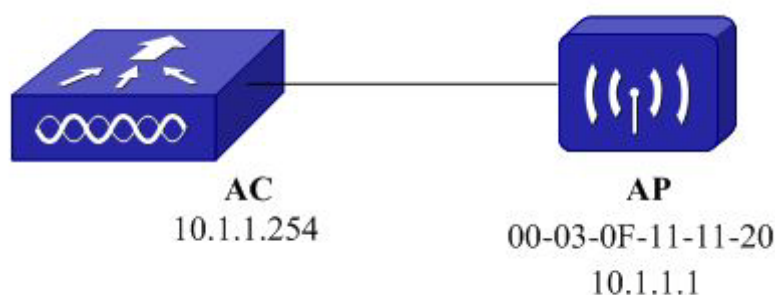


图 3-1 频谱分析应用拓扑

拓扑说明: AP 被 AC 管理, 并通过 profile 22 下发配置。该环境中存在微波干扰设备。

应用: AP 被 AC 管理上后, 通过 AC 开启频谱分析功能:

1) 在 radio1 下开启频谱分析功能

```
AC(config-wireless)#ap profile 22
```

```
AC(config-ap-profile)#radio 1
```

```
AC(config-ap-profile-radio)#spectral-scan
```

```
AC(config-ap-profile-radio)#exit
```

2) 设置频谱分析结果上报时间间隔为 10s (可选)

```
AC(config-ap-profile)# spectral-scan-report-interval 10
```

```
AC(config-ap-profile)#exit
```

3) 设置频谱分析结果老化时间为 20 分钟（可选）

```
AC(config-wireless)#agetime spectral-scan 20
```

```
AC(config-wireless)#end
```

4) 下发配置

```
AC#wireless ap profile apply 22
```

All configurations will be send to the aps associated to this profile and associated clients on these aps will be disconnected. Are you sure you want to apply the profile configuration?
[Y/N]Y

5) 等待 10s 以上的时间，通过命令查看频谱分析结果

```
AC#show wireless ap 00-03-0f-11-11-20 radio 1 spectral-scan interference status
```

```
MAC address..... 00-03-0f-11-11-20
```

```
Location.....
```

```
Radio..... 1 - 802.11b/g/n
```

```
Device Type 1: Microwave
```

```
Device Type 2: Bluetooth
```

```
Device Type 3: Cordless Phone
```

```
Device Type 4: Tone
```

```
Device Type 5: Other
```

Device Type	centerFreq	Affected Channel	Age
1	2.484GHz	14	0d:00:00:02

3.4 频谱分析排错帮助

当在使用频谱分析过程中遇到问题时，请检查是否是如下原因：

- ☞ AC 上已配置频谱分析功能，但 AP 未进行频谱分析：通过 `show wireless ap spectrum monitor` 查看 AP 是否添加到频谱分析任务中；
- ☞ 开启频谱分析功能后，无法扫描到干扰设备：确认 `radio1` 状态是否是 up，同时确认 `radio1` 下只有 `vap0` 状态为 up；
- ☞ 若经过多个上报周期仍没有扫描到干扰设备，需要使用 `debug` 调试工具确认 AP 是否周期性的向 AC 发送频谱分析结果。

第4章 smtp

4.1 smtp 介绍

随着技术的深入发展，目前出现了很多手机邮箱终端，越来越多的人可以很方便的通过手机邮箱终端来收发邮件。

鉴于上述技术的出现，我们可以将设备的 **syslog** 同时以邮件的方式发送给网络管理员，这样就可以让网管人员随时随地查看到设备的运行情况，对于设备的异常情况可以及时发现、及时解决，减少设备异常带来的损失。所以 **AC** 的邮件功能对网络维护有很重的意义。

除 **syslog** 信息外，其它重要的信息也可以通过邮件的方式发送的网络管理人员，**smtp** 功能主要提供在 **AC** 上发邮件的通用接口，任何信息都可以通过此接口以邮件的形式通知给网络管理人员。

4.2 smtp 基本配置

AC 上 **smtp** 功能的基本配置序列：

1. 开启 **smtp** 功能
2. 创建收件人规则并对收件人规则进行各项配置
3. 配置 **smtp server** 相关参数
4. 显示 **smtp** 功能的相关配置
5. 对 **smtp** 相关配置进行测试

1. 开启/关闭 **smtp** 功能

命令	解释
全局配置模式	
smtp no smtp	进入 smtp 配置模式，同时开启 smtp 功能全局开关； no 命令关闭 smtp 功能全局开关，不再提供投递邮件的功能。

2. 创建/删除收件人规则并对收件人规则进行各项配置

命令	解释
smtp 配置模式	
receiver rule <rule-id> no receiver rule <rule-id>	创建 smtp 收件人规则并且进入 smtp 收件人规则配置模式； no 命令删除某个 smtp 收件人规则。
smtp 收件人规则配置模式	

receiver description <desc> no receiver description	为当前收件人规则配置描述信息；no 命令可恢复该描述信息为默认配置，默认配置为空。
receiver address <email-addr> no receiver address <email-addr>	在当前收件人规则中添加收件人；no 命令用于删除已经配置的收件人。
receiver severity [critical warnings informational debugging] no receiver severity	配置 smtp 收件人规则的严重级别，只有邮件的严重级别不低于（高于或者等于）该规则中配置的严重级别才需要给该规则中配置的收件人投递邮件；no 命令会恢复该项配置的默认值，默认值为 critical。
receiver time-range from <start-time> to <end-time> [monday tuesday wednesday thursday friday saturday sunday weekend weekday everyday] no receiver time-range [monday tuesday wednesday thursday friday saturday sunday weekend weekday everyday]	为当前规则中的收件人配置接收邮件的时段，在配置时段以外时间，AC 不会向该规则中的收件人投递邮件；no 命令恢复该项配置的默认值。

3. 配置 smtp server 相关参数

命令	解释
smtp 配置模式	
smtp server ipv4 <ipaddr> [port <port-num>] no smtp server	配置或者更新 smtp 服务器的地址和端口；no 命令用于删除 smtp 服务器配置
smtp sender address <email-addr> no smtp sender address	指定发件人，如果当前已经存在发件人，则会覆盖掉当前配置，下次投递邮件的时候，用新配置的发件人来发送邮件；no 命令可以删除当前配置的发件人地址。
smtp server authentication username <username> password <password> no smtp server authentication	给 smtp server 配置认证的用户名和密码；no 命令会恢复默认的用户名和密码，默认为空。
smtp server source-ipv4 <ipaddr> no smtp server source-ipv4	给 AC 指定一个源 ip 地址，该源地址需要是一个有效的 interface 的 ip 地址。AC 会采用该 ip 地址作为源 ip 与服务器建立 TCP 连接；no 命令可以删除该源 ip 地址。

4. 显示 smtp 功能的相关配置

命令	解释
----	----

特权模式	
show smtp status	显示 smtp 的相关配置信息，包括 smtp 开启状态，服务器地址、端口号，和服务器的连接状态，发送方邮件地址，发送邮件源 IP 地址，服务器认证用户名和密码。
show smtp receiver rule [<rule-id>] status	显示 smtp 收件人规则的相关配置信息。

5. 对 smtp 相关配置进行测试

命令	解释
特权模式	
smtp test-mail-send	尝试给当前配置的收件人投递一份 test 邮件，邮件标题和内容都是“test”，如果各项参数都配置正确，我们可以通过登陆收件人邮箱查看到该邮件；否则投递失败。在 console 口上可以看到投递邮件的整个过程。

4.3 smtp 配置举例

典型案例：

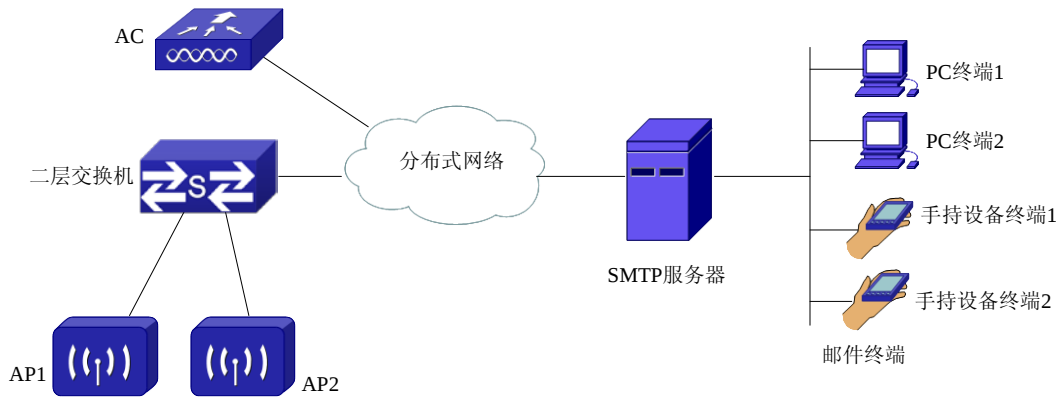


图 4-1 smtp 典型案例

AC 上的 smtp 功能应用场景如上图所示。AP1 和 AP2 通过二层交换机接入到网络，被 AC 管理，共同为客户提供接入服务器。网络中同时还存在一台邮件服务器，负责将网络中的邮件投递出去，对于本地的用户，邮件可以直接投递到用户，对于非本地用户，则需要中继到用户所在的邮件服务器（中继部分该图中并未画出，AC 是需要实现 smtp 客户端，不关心服务器及其中继服务器的细节），邮件终端可以通过 POP3、IMAP 等协议去查看邮件内容。

AC 作为 smtp client，如果发现一些网络中存在的异常事件，如 AP 掉线，可以立即通

过网络中 smtp 服务器给网络管理人员发送一封邮件，将网络中存在的异常通知到相应的 PC 或手持邮件终端，网络管理人员则可以通过邮件终端的提醒功能第一时间查看 AC 发过来的邮件，了解到网络中的异常，并第一时间处理这种异常，降低由于网络异常带来的损失。

具体的配置如下：

smtp 服务器相关参数：

smtp 服务器类型：Windows2003 自带的 smtp 服务器

smtp 服务器地址：192.168.1.200

smtp 服务器端口：25

支持的认证方式：LOGIN

认证用户名：admin@domain.com

认证密码：domain_123456

投递邮件要求：

A、邮件统一以发件人admin@domain.com的名义投递

B、普通的网络管理员zhangsan@domain.com需要全天监控网络的状态，需要关注 warnings 及以上严重级别的网络事件，对于非常严重的网络事件需要及时去处理

C、部门经理lisi@domain.com 只关注 critical 及以上严重级别的网络事件，而且每天在休息时间不想收到任何邮件，即只在早晨 8 点到晚上 11 点接受邮件

AC smtp 功能相关配置如下：

开启 smtp 功能，并进入 smtp 配置模式

AC(config)#smtp

配置 smtp 服务器地址和端口：192.168.1.200:25

AC(config-smtp)#smtp server ipv4 192.168.1.200 port 25

配置 smtp 服务器认证参数：用户名 admin@domain.com，密码 domain_123456

AC(config-smtp)#smtp server authentication username admin@domain.com password domain_123456

配置发件人地址

AC(config-smtp)#smtp sender address admin@domain.com

配置一个收件人规则，该规则中的收件人全天监控 warning 严重级别及以上的网络事件

AC(config-smtp)#receiver rule 1

配置该规则的描述信息：普通网管 – 任何时间都需要接收 warning 及以上的网络事件

AC(config-smtp-rule)#receiver description general staff - any time receive warning email

配置该规则中的收件人地址 zhangsan@domain.com

AC(config-smtp-rule)#receiver address zhangsan@domain.com

配置该规则中的收件人关注的事件严重级别

AC(config-smtp-rule)#receiver severity warnings

无需配置接收邮件时间段，默认全天接收

上述规则已经配置完毕，退出收件人规则配置模式

AC(config-smtp-rule)#exit

再配置一个收件人规则，收件人只关注 critical 及以上严重级别的网络事件，在休息时间不接受任何邮件

AC(config-smtp)#receiver rule 2

配置该规则的描述信息：部门经理 – 工作时间接收 critical 及以上的网络事件

AC(config-smtp-rule)#receiver description department manager - working time receive critical email

配置该规则中的收件人地址 lisi@domain.com

AC(config-smtp-rule)#receiver address lisi@domain.com

配置该规则中的收件人关注的事件严重级别

AC(config-smtp-rule)#receiver severity critical

配置该规则中的收件人接收邮件的时间

AC(config-smtp-rule)#receiver time-range from 8:00 to 23:00 everyday

配置完毕

4.4 smtp 排错帮助

在使用中，如果发现邮件投递不能生效，可以采用下面的检查步骤：

- ☞ 在特权模式输入命令 `smtp test-mail-send`，根据 console 控制台打印信息判断当前配置存在的问题。
- ☞ 检查 smtp 收件人邮箱配置是否正确。
- ☞ 检查 smtp 收件人时间配置是否正确。
- ☞ 检查 smtp 邮件发送等级配置是否正确。
- ☞ 检查 AC smtp 服务器的地址，端口配置是否跟服务器的配置一致。
- ☞ 若以上配置均正确，但邮件发送还是失败，则检查 AC 路由是否正确配置可达 smtp 服务器。