XR829 Android/Linux WLAN Software Debug Guide

Revision 1.0

July 17, 2018

Declaration

THE INFORMATION FURNISHED BY XRADIO IS BELIEVED TO BE ACCURATE AND RELIABLE. XRADIO RESERVES THE RIGHT TO MAKE CHANGES IN CIRCUIT DESIGN AND/OR SPECIFICATIONS AT ANY TIME WITHOUT NOTICE. XRADIO DOES NOT ASSUME ANY RESPONSIBILITY AND LIABILITY FOR ITS USE. NOR FOR ANY INFRINGEMENTS OF PATENTS OR OTHER RIGHTS OF THE THIRD PARTIES WHICH MAY RESULT FROM ITS USE. NO LICENSE IS GRANTED BY IMPLICATION OR OTHERWISE UNDER ANY PATENT OR PATENT RIGHTS OF XRADIO. THIS DATASHEET NEITHER STATES NOR IMPLIES WARRANTY OF ANY KIND, INCLUDING FITNESS FOR ANY PARTICULAR APPLICATION.

THIRD PARTY LICENCES MAY BE REQUIRED TO IMPLEMENT THE SOLUTION/PRODUCT. CUSTOMERS SHALL BE SOLELY RESPONSIBLE TO OBTAIN ALL APPROPRIATELY REQUIRED THIRD PARTY LICENCES. XRADIO SHALL NOT BE LIABLE FOR ANY LICENCE FEE OR ROYALTY DUE IN RESPECT OF ANY REQUIRED THIRD PARTY LICENCE. XRADIO SHALL HAVE NO WARRANTY, INDEMNITY OR OTHER OBLIGATIONS WITH RESPECT TO MATTERS COVERED UNDER ANY REQUIRED THIRD PARTY LICENCE.

Revision History

Version	Data	Summary of Changes
1.0	2018-7-17	Initial Version

表 0-1 Revision History

目 录

表

图

1 基本流程

1.1 STA 开启连接流程

STA 模式				
模块	软件流程	打印	无线网卡抓包	用户感知
Android	用户层开启 WLAN	logcat：setWifiEnabled	No Packets	正在打开 wifi
	加载 wlan 驱动	kernel：XRADIO WIFI OPEN		
Driver	上电，reset 拉高	kernel：sunxi-wlan 相关		
	SDIO 卡检测	kernel：Detect SDIO card 1		
	SDIO 卡识别成功	kernel ： XRadio Device:sdio clk=50000000		
	bootloader 下载完成	kernel：Bootloader complete		
	firmware 下载完成	kernel：Firmware completed.		
	firmware 启动完成	kernel：Firmware Startup Done.		
Android	启动 supplicant	logcat：supplicant 相关打印		
Android /Driver	创建网络接口 wlan0	kernel:xradio_vif_setup: id=0, type=2, p2p=0		
Android /Driver	第一次扫描	logcat：扫描相关打印 kernel：vif0 Scan request（驱动默认不打印）	遍历信道发送 ProbeReq 接收 ProbeRsp	扫描列表
以下流程只有在点击连接或者自动连接时才有				
Android /Driver	认证关联	kernel：（驱动默认不打印） if0-TX-auth if0-RX-auth if0-TX-assoc_req if0-RX-assoc_resp	Auth 交互 Assoc 交互	正在连接...
Android /Driver	802.11X(WPA 保护 AP only)	kernel：（驱动默认不打印） if0-RX--8021X if0-TX--8021X if0-RX--8021X if0-TX--8021X	EAPOL 交互(因认证方式而异)	正在进行身份验证...
Android /Driver	启动 DHCP	kernel：（驱动默认不打印） if0-TX--DHCP,Opt=53,MsgType=1 if0-RX--DHCP,Opt=53,MsgType=2 if0-TX--DHCP,Opt=53,MsgType=3 if0-RX--DHCP,Opt=53,MsgType=5	DHCP 包(已加密)	正在获取 IP 地址... /已连接
Driver	建立 TX/RX BAA	kernel：（驱动默认不打印）	ADDBA Req	已连接

/FW	(11n only)	if0-RX-action(ADDBA_REQ if0-TX-action(ADDBA_RESP-0)	ADDBA Rsp	

表 1-1 STA 模式打开连接流程

1.2 SoftAP 开启连接流程

SoftAP 模式				
模块	软件流程	打印	无线网卡抓包	用户感知
Android	用户层开启热点	无	No Packets	正在打开热点
	加载 wlan 驱动	kernel：XRADIO WIFI OPEN		
Driver	上电，reset 拉高	kernel：sunxi-wlan 相关		
	SDIO 卡检测	kernel：Detect SDIO card 1		
	SDIO 卡识别成功	kernel ： XRadio Device:sdio clk=50000000		
	bootloader 下载完成	kernel：Bootloader complete		
	firmware 下载完成	kernel：Firmware completed.		
	firmware 启动完成	kernel：Firmware Startup Done.		
Android	启动 hostapd	logcat：SoftAP started logcat：hostapd 相关打印		
Android /Driver	创建网络接口 wlan0	kernel：vif0, AP/GO mode	发送 beacon 帧	热点已启用
Android /Driver	启动 DHCPD	logcat:DHCP, IP range 192.168		
以下流程只有在被 STA 扫描连接时才有				
FW	扫描响应	无	发送 ProbeRsp	在对端扫描列表显示
Android /Driver	认证关联	kernel：（驱动默认不打印） if0-RX-auth if0-TX-auth if0-RX-assoc_req if0-TX-assoc_resp	Auth 交互 Assoc 交互	对端正在连接
Android /Driver	802.11X(WPA 保护 AP only)	kernel：（驱动默认不打印） if0-TX--8021X if0-RX--8021X if0-TX--8021X if0-RX--8021X	EAPOL 交互(因认证方式而异)	对端显示身份验证...
Android /Driver	DHCP 分配 IP	kernel：（驱动默认不打印） if0-RX--DHCP,Opt=53,MsgType=1 if0-TX--DHCP,Opt=53,MsgType=2 if0-RX--DHCP,Opt=53,MsgType=3	DHCP 包(已加密)	对端正在获取 IP 地址... /已连接

		if0-TX--DHCP,Opt=53,MsgType=5 logcat: DHCPDISCOVER(wlan0) DHCPOFFER(wlan0) DHCPREQUEST(wlan0) DHCPACK(wlan0)		
Driver /FW	建立 TX/RX BAA (11n only)	kernel: （驱动默认不打印） if0-RX-action(ADDBA_REQ if0-TX-action(ADDBA_RESP-0)	ADDBA Req ADDBA Rsp	已连接

表 1-2 SoftAP 模式打开连接流程

1.3 P2P 开启连接流程

P2P 模式				
模块	软件流程	打印	无线网卡抓包	用户感知
P2P 模式和 STA 模式共存，因此扫描连接之前的打开流程和 STA 一致。 当进入 P2P 的扫描界面后触发以下流程				
Android /Driver	P2P 扫描	kernel: vif2 Scan request（驱动默认不打印）	1，6，11信道 收发 ProbeReq 收发 ProbeRsp	P2P 扫描列表
以下流程只有在点击连接或者自动连接时才有				
Android /Driver	P2P	kernel: （驱动默认不打印） if0-TX-auth if0-RX-auth if0-TX-assoc_req if0-RX-assoc_resp	Auth 交互 Assoc 交互	正在连接...
Android /Driver	802.11X(WPA 保护 AP only)	kernel: （驱动默认不打印） if0-RX--8021X if0-TX--8021X if0-RX--8021X if0-TX--8021X	EAPOL 交互(因认证方式而异)	正在进行身份验证...
Android /Driver	启动 DHCP	kernel: （驱动默认不打印） if0-TX--DHCP,Opt=53,MsgType=1 if0-RX--DHCP,Opt=53,MsgType=2 if0-TX--DHCP,Opt=53,MsgType=3 if0-RX--DHCP,Opt=53,MsgType=5	DHCP 包(已加密)	正在获取 IP 地址... /已连接
Driver /FW	建立 TX/RX BAA (11n only)	kernel: （驱动默认不打印） if0-RX-action(ADDBA_REQ if0-TX-action(ADDBA_RESP-0)	ADDBA Req ADDBA Rsp	已连接

表 1-3 P2P 模式连接流程

2 基本思路

在分析问题的过程中，有几个比较常见的分析方法，分别是逆向分析，正向分析，排除分析，对比分析。一般对于单线或局部的问题，逆向或正向分析法就较快能找到问题的原因；但对于系统性的，问题范围较大，未知因素较多的情况下，更适合使用排除分析法和对比分析法，这样

2.1 逆向分析(从问题出发)

对于一般问题来说，优先考虑这种分析方法，因为一般情况下这种方法是顺藤摸瓜，能够较快且有条不紊的找到问题关键和根源，而且还可以防止思维过于发散引起的效率低下的问题。相对而言，应尽量避免无逻辑，大范围的乱尝试。

2.2 排除分析(缩小问题范围)

很多问题都可能涉及的系统的方方面面，因此需要对问题整体进行分层或者分模块，通过一些实验逐步的验证排除，然后达到缩小问题范围的目的，在问题范围缩小到一定程度的情况下，可以再结合逆向或者正向分析，找到问题的根因。这种方法的优点是，在很多情况下，比如对系统不熟悉，无切入点的情况下，比正向/逆向分析更有效率。

2.3 对比分析(缩小问题范围)

这种方法和排除分析法的目的很像，都是为了问题的定界和缩小范围。与排除法不同在于，对比分析法一般都是拿没有问题和有问题的场景进行对比，然后对比这场景的差异点，逐步限定对比的条件，可以快速的定位到问题点，然后再结合正向/逆向，分析问题根因。很多情况下，有着无可替代的作用。

2.4 正向分析(逻辑梳理)

当问题范围较小，并且对该模块比较熟悉时，可以使用该方法进行分析和梳理，把问题触发的整个逻辑链理清，然后找到问题的根因。

2.5 问题分类思路

2.5.1 功能问题

这类是指某个功能不能正常使用运行，或者出现概率性较高的问题。这类问题相对来说比较容易解决，解决的时间也比较可控。对于白盒的模块可以优先使用逆向分析；对于范围较大的黑盒问题，优先使用排除分析和对比分析，对问题的范围缩小，然后再进行逆向分析或者正向分析。具体可以参考“常见问题”。

2.5.2 性能问题

这类是指 WiFi 的性能达不到需求，比如屏蔽房吞吐低，干扰环境的吞吐低，视频传输卡顿，网络丢包严重，ping 延迟等等。由于性能问题可能涉及到系统各个方面影响，相对功能问题，性能问题的解决难度相对大。

一般来说，首先要确认硬件 RF 性能是 OK 的，该部分可以通过 ETF 测试或者信令测试等得到 RF 的测试指标报告。这个步骤是以下步骤的前提。

对于屏蔽房的性能问题，可以首先路由器兼容问题，通过几个路由器进行对比；其次，可以排查平台性能问题，比如主控性能，系统性能，可以把主控性能调整到最大进行对比测试。如果是小系统平台，可以使用其它平台的进行对比测试。

对于干扰环境的性能问题，由于干扰环境的干扰强度很难量化，没有绝对的标准，即没有确切的标准指明什么环境下吞吐应该是多少，因此，只能通过对比的方式判断性能好或不好，并且通过此方式拟定优化的目标。并且，由于干扰环境实时变化，因此，对比测试需要交替多次测试才具有较高可信度。

2.5.3 稳定性问题

这类问题是指需要长时间测试才能出现的问题，这种问题较难复现，一般解决的时间都不好确定。为了更快的解决问题，需要保存较完整的 log，或者添加足够的 log，争取问题复现一两次就可以快速的定位。

在测试的强度上，增加测试的机器，增加测试的时间，尝试分析容易复现的场景。

2.6 反馈方式

如果简单的问题，或者是系统性问题，可以依照本文进行初步的排查和分析。

如果确定为 WLAN 问题，或者与 WLAN 相关性较大时，可以找到相关接口人反馈相关问题。

2.6.1 接口人员

1.项目启动时有指定的相关负责人，则优先找该负责人。

2.没有指定负责人，则先找 FAE 团队进行支持，不清楚具体人员可咨询项目负责人或中心/部门上层。

2.6.2 背景信息

在反馈问题时，需提供 WLAN 驱动和固件版本，使用的平台和问题场景，以及紧急程度。

2.6.3 问题信息

尽可能提供多的信息，例如：

1）问题出现现象、概率，完整的 log，最好保留问题现场；

2）如果有初步排查，提供初步分析的结果。

3）提供优化或解决的目标，包括时间期限，交付的标准。

3 常用接口/工具

3.1 wpa_cli

通过命令行，可以直接打开 supplicant，从而运行 wpa_cli，可以解决客户没有显示屏而无法操作 WIFI 的问题，还可以避免界面的问题带到 driver。一般来说，可以用在很多没有键盘输入和 LCD 输出的安卓终端产品的操作上。

wpa_supplicant 包含两个主要的可执行工具：wpa_supplicant 和 wpa_cli。wpa_supplicant 是核心程序，它和 wpa_cli 的关系就是服务和客户端的关系：后台运行 wpa_supplicant，使用 wpa_cli 来搜索、设置、和连接网络。以下介绍简单的使用命令，更多的使用命令可以使用 wpa_cli --help.

3.1.1 启动和退出

wpa_cli 的启动命令，以及启动输出如下图 3-1，注意-p 指定了 wpa_cli 连接的 socket，对于非 android 的平台可能位置不一样，需要确认。

```
启动命令：wpa_cli -i wlan0 -p /data/misc/wifi/sockets
退出命令：exit 或 q
```

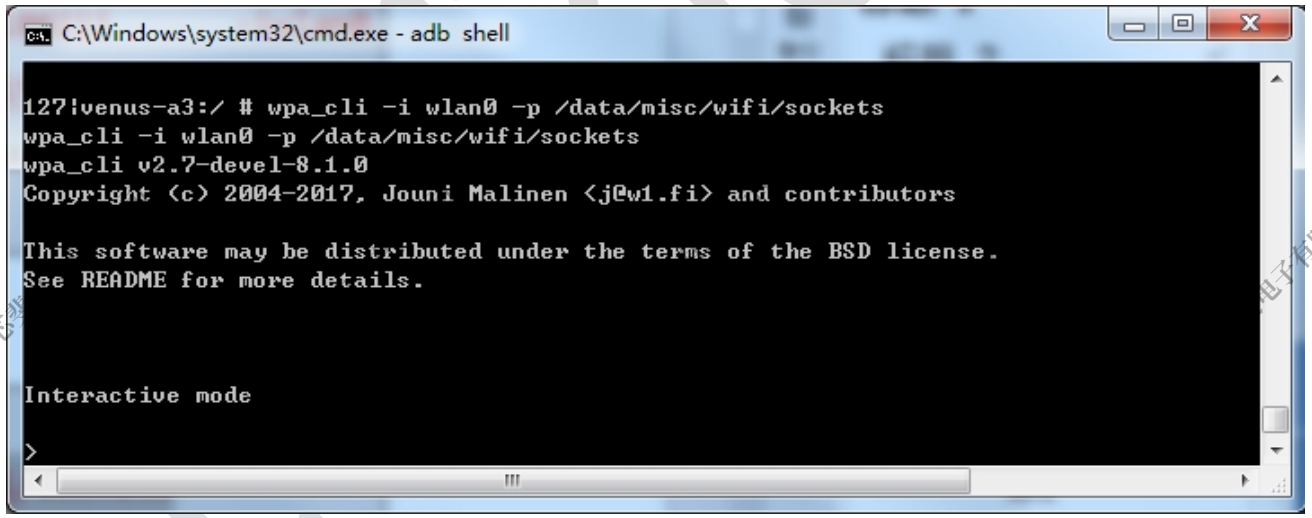

图 3-1 wpa_cli 启动

3.1.2 扫描 AP

启动扫描：scan

获取扫描结果：scan_results

```
> scan
scan
OK
<3>CTRL-EVENT-STATE-CHANGE id=-1 state=3 BSSID=00:00:00:00:00:00 SSID=
<3>CTRL-EVENT-SCAN-RESULTS
<3>WPS-AP-AVAILABLE
<3>CTRL-EVENT-STATE-CHANGE id=-1 state=2 BSSID=00:00:00:00:00:00 SSID=
```

图 3-2 wpa_cli 扫描

```
bssid / frequency / signal level / flags / ssid
00:87:36:00:5a:2c       2462    -50     [WPA-PSK-CCMP][WPA2-PSK-CCMP][ESS]
360-ZS5A2C
c8:3a:35:32:9e:a8       2412    -56     [WPA2-PSK-CCMP][ESS]    Tenda_329EA8
a8:57:4e:84:6e:94       2412    -58     [WPA-PSK-CCMP][WPA2-PSK-CCMP][WPS][ESS]
TP-LINK_CONCOX
70:62:b8:27:e3:4f       2457    -69     [WPA2-PSK-CCMP][ESS]    MagicAP-7JVD
e0:05:c5:e2:5e:b2       2452    -83     [WPA-PSK-CCMP][WPA2-PSK-CCMP][ESS]
Chinanet-6nHX
00:25:12:2a:c7:a9       2417    -88     [WPA-PSK-TKIP][WPS][ESS]        ChinaNet
-concox
00:25:5e:1c:fb:d2       2432    -89     [WPA2-PSK-CCMP][ESS]    OpenWrt
8c:21:0a:42:42:40       2437    -91     [WPA-PSK-CCMP][WPA2-PSK-CCMP][ESS]
TEST
00:0e:e8:b4:c2:10       2462    -63     [WEP][ESS]      KKS_PM
00:0e:e8:b4:c2:11       2462    -64     [WEP][ESS]      Ruler
86:97:77:d8:62:2c       2457    -71     [WEP][IBSS]     Connectify-me
00:00:00:00:00:00       2412    0       [ESS]   NVRAM WARNING: Err = 0x10
```

图 3-3 wpa_cli 扫描结果

3.1.3 连接 AP

1）连接不加密 AP

```
add_network
set_network 0 ssid "TES_TPLINK_WR847N"  //0 为 add_network 返回值
set_network 0 key_mgmt NONE
select_network 0
```

2）连接 WEP 加密 AP


```
add_network
set_network 1 ssid "ASUS"   //1 为 add_network 返回值
set_network 1 key_mgmt NONE
set_network 1 wep_key0 "12345678"
set_network 1 wep_tx_keyidx 0
select_network 1
```

3）连接 WPA/WPA2 加密 AP

```
add_network
set_network 2 ssid "ASUS"   //2 为 add_network 返回值
set_network 2 psk "22222222"
set_network 2 key_mgmt WPA-PSK
select_network 2
```

4）保存网络配置

```
save  //save 可以把连接的 AP 信息写入 wpa_supplicant 的网络配置
```

3.2 iw

iw 是一个用于对无线设备进行配置与操作的命令行工具，它基于 nl80211 实现，是基于 Wireless Extension 的 iwconfig 工具的替代品。本文档描述的 iw 功能实现与否的验证平台为 A31+Linux3.3+Android4.2+iw3.14 。iw 能做的事情有很多（要配合驱动与硬件支持），表 1 列出了其中常用的一些命令，通过此表格也可快速浏览其功能有哪些，相应命令的执行结果举例可在 2.2 部分找到。

命令	作用
iw list	列出所有无线设备的能力，如频谱，速率，11n 等
iw event	监听内核事件
iw dev wlan0 scan	扫描周围无线网络
iw dev wlan0 link	查看有无连接到 AP/连接 AP 的状态
iw dev wlan0 connect foo	连接 SSID 为 foo 的 AP（仅限 open 或 wep 加密）
iw dev wlan0 station	获取 station 的收发包等统计数据

dump	
iw dev wlan0 station get <peer-MAC>	获取对端 station 的收发包等统计数据，对于 managed 模式的 Sta 来说，peer 即它连接的 AP
iw dev wlan0 set bitrates ht-mcs-5 4	设置发送速，不加最后的参数可清除设置
iw phy phy0 set txpower fixed 10	设置无线设备的发射功率
iw dev wlan0 set power_save on	使能动态省电模式
iw dev wlan0 get power_save	查看当前省电模式
iw phy phy0 interface add mon0 type monitor	增加网络接口，monitor 可替换为 station, wds, mesh,ibss 类型，mon0 换为相应名字
iw dev mon0 del	删除网络接口
iw reg set alpha2	更新 regulatory domain 信息，alpha2 是 ISO/IEC 3166-1 alpha2 国家码

3.2.1 扫描 AP

```
iw dev wlan0 scan //触发一次扫描并将扫描结果 dump 出来，可指定频率，ssid 等
```

3.2.2 连接 AP

```
iw dev wlan0 connect TES#07_NETGEAR
//连接到指定的 SSID 的网络，只支持 open 或 wep 加密的
```

3.2.3 连接状态

```
iw dev wlan0 link  //SSID，频率，收发数，DTIM，Beacon 周期
iw dev wlan0 station dump //关联的 AP 信息，包括已收发包数据，信息强度，速率等
```


3.2.4 增加/删除接口

```
iw phy phy0 interface add mon0 type monitor //增加 monitor 接口 mon0
iw dev mon0 del //删除 monitor 接口 mon0
```

3.3 tcpdump

tcpdump 主要通过监测网络接口，抓取 TCP/IP 网络层的数据包，包括 tcp、ip 和 ICMP 数据包等，也能抓取 wpa_supplicant 通过 netdevice 与 UMAC 的交互包。使用 tcpdump 抓包指令之后可通过 omnipeek,wireshark 等软件来查看和分析数据包的。抓包命令如下：

```
tcpdump -i wlan0 -s 0 -w data/a.pcap
```

其中，-i wlan0 表示接口，-s 0 表示数据包报文截取的长度的默认值 65535，-w data/a.pcap 表示数据包保存的文件，可以通过 wireshark 来查看。

如果更多的参数配置，可以通过 tcpdump --help 查看。

```
Usage: tcpdump [-aAdDeflLnNOpqRStuUvxX] [-c count] [ -C file_size ]
              [ -E algo:secret ] [ -F file ] [ -i interface ] [ -M secret ]
              [ -r file ] [ -s snaplen ] [ -T type ] [ -w file ]
              [ -W filecount ] [ -y datalinktype ] [ -Z user ]
              [ expression ]
```

3.4 Onimpeek

Onimpeek 常用于无线抓包分析，Onimpeek 软件需要一个支持该软件的无线网卡才能实现抓包。具体使用这里不做详细介绍。

3.5 iperf

常用的网络性能测试工具，为开源工具。

3.5.1 UDP 测试

```
Server: iperf -s -u -w 20m -i -1
Client: iperf -c 192.168.52.106 -u -b 100M -i 1 -t 30
```


3.5.2 TCP 测试

```
Server: iperf -s -p 5002 -i 1
Client: iperf -c 192.168.51.6 -p 5002 -w 1m -i 1 -t 30
```

3.6 Ixchariot

较权威的网络性能测试工具，功能较为强大，具体不做详细介绍。

3.7 驱动 debugfs 调试接口

Debug 接口类型	接口名称	作用描述	用途
状态和统计	version	驱动和固件版本信息	确认驱动固件版本
	counters	收发帧信息的计数统计	确认是否有收发帧
	ratemap	收发帧的 rate 分布统计	分析吞吐性能问题
	dbgstats	平均发送聚合长度、发送 retry 率、11n 发送速率分布等汇总信息	分析吞吐性能问题
	bh_stat	驱动 bh 相关信息的统计（包含中断数）	分析吞吐性能问题
	vif_x/status	接口 x 的连接状态、连接模式参数	确认连接状态和模式
配置控制	set_ampdu_len	发送聚合帧最大长度控制	调试性能，控制聚合长度
	ps_disable	关闭 80211 协议的休眠模式	调试性能，关闭休眠模式
	set_sdio_clk	调整 SDIO 的时钟（cmd53 数据通信	调试 SDIO 的稳定性
	xradio_host_dbg/*	动态调整驱动的打印等级	控制驱动打印等级
	parse_flags	显示驱动收发帧的信息	调试帧交互过程

3.7.1 驱动打印等级控制（xradio_host_dbg）

一般用于驱动功能流程等调试，便于抓取更多的 log。打印等级是互相独立的，各个等级是或的关系。因此，可以单独控制那个等级的输出。如打印层级为 0x3，就是输出 ERROR 和 AWLY 信息。具体定义如下表：

打印等级	值	说明
XRADIO_DBG_ALWY	0x01	输出基本打印信息
XRADIO_DBG_ERROR	0x02	输出出错信息
XRADIO_DBG_WARN	0x04	输出警告信息
XRADIO_DBG_NIY	0x08	输出值得注意信息（develop）
XRADIO_DBG_MSG	0x10	输出调试信息（develop）
XRADIO_DBG_TRC	0x20	输出函数调用路径

节点路径为：/sys/kernel/debug/xradio_host_dbg/，操作方法：

操作	含义
echo debug_level > dbg_common	驱动公共流程的打印等级，包括初始化，上电，下载固件，调试接口等。默认为 0x7
echo debug_level > dbg_sbus	驱动 SDIO 接口操作的打印等级。默认为 0x7
echo debug_level > dbg_ap	驱动 BSS 相关信息的打印等级。默认为 0x7
echo debug_level > dbg_sta	驱动 BSS 中 STA 模式相关信息的打印等级。默认为 0x7
echo debug_level > dbg_scan	驱动扫描相关信息的打印等级。默认为 0x7
echo debug_level > dbg_bh	驱动 bh 相关信息的打印等级，包括中断。默认为 0x7
echo debug_level > dbg_txrx	驱动收发通路信息的打印等级，包括 queue，速率配置等。默认为 0x7
echo debug_level > dbg_pm	驱动休眠唤醒的打印等级。默认为 0x7
echo debug_level > dbg_etf	驱动 ETF 模式的打印等级。默认为 0x7

3.7.2 驱动收发帧打印控制（parse_flags）

一般用于帧交互流程相关调试。比如扫描、连接等。节点路径为：/sys/kernel/debug/ieee80211/phy*/xradio/，操作方法如下：

操作	含义
echo tx, rx> parse_flags	设定解释输出的收发帧，tx 为发送帧解释参数，rx 为接收帧解释参数。参数为 0 就是不解释。参数具体定义如下表：
cat parse_flags	查看当前设定

tx/rx 参数（下列值的或）	含义
0x1	显示控制帧
0x2	显示管理帧（扫描相关帧除外）
0x4	显示数据帧
0x8	显示扫描相关帧
0x10	显示 TCP 协议帧
0x20	显示 UDP 协议帧
0x40	显示 DHCP 协议帧
0x80	显示 ICMP 协议帧（包含 ping 协议
0x100	显示 PF_8021X 协议帧
0x200	在信息中显示 MAC 层的序列号
0x400	在信息中显示自身 MAC 地址
0x800	在信息中显示源 MAC 地址和目标 MAC 地址
0x1000	在信息中显示无线层对端 MAC 地址
0x2000	在信息中显示 IP 地址
0x4000	显示未知协议的帧

示例：echo 0x0142,0x5142 > parse_flags

1）认证过程的打印


```
[XRADIO] if0-TX-auth-SN=0(0)-08:bd:43:ff:88:77--    //发起认证
[WSM] Issue join command.
[STA] Join DTIM: 1, interval: 100
[XRADIO] if0-RX-auth-SN=2270(0)-08:bd:43:ff:88:77--  //收到认证应答
```

2）关联过程的打印

```
[XRADIO] if0-TX-assoc_req-SN=40(0)-08:bd:43:ff:88:77--      //发起关联
[XRADIO] if0-RX-assoc_resp-SN=3276(0)-08:bd:43:ff:88:77--   //收到关联应答
```

3）802.1x 交互过程的打印

```
[XRADIO] if0-RX-QoSdata(TDFD=01,R=0,P=0)-SN=0(0)-08:bd:43:ff:88:77--8021X
[XRADIO] if0-RX-back_req-08:bd:43:ff:88:77--
[AP] [STA]arp ip filter enable: 0
[AP] [STA] ndp ip filter enable: 0
[AP] CHANGED_BEACON_INT
[AP] BSS_CHANGED_ASSOC.
[XRADIO] if0-RX-beacon-SN=2273(0)-08:bd:43:ff:88:77--
[AP_WRN] [STA] ASSOC HTCAP 11N 58
[AP] [STA] Non-GF STA present
[AP] STA has ERP rates
[AP] BTCOEX_INFOMODE 2, internalTxRate : 6,nonErpInternalTxRate: 6
[AP] [CQM] RSSI threshold subscribe: 0(+-0)
[AP] [CQM] Beacon loss subscribe: 0
[AP] [CQM] TX failure subscribe: 0
[XRADIO] if0-TX-action-SN=2(0)-08:bd:43:ff:88:77--
[XRADIO] if0-TX-QoSdata(TDFD=10,R=0,P=0)-SN=0(0)-08:bd:43:ff:88:77--8021X
[XRADIO] if0-RX-QoSdata(TDFD=01,R=0,P=0)-SN=1(0)-08:bd:43:ff:88:77--8021X
[XRADIO] if0-TX-QoSdata(TDFD=10,R=0,P=0)-SN=1(0)-08:bd:43:ff:88:77--8021X
```

4）DHCP 交互过程的打印

```
[XRADIO]   if0-TX-QoSdata(TDFD=10,R=0,P=1)-SN=2(0)-08:bd:43:ff:88:78--DHCP,  Opt=53,
MsgType=1-255.255.255.255
```



```
[XRADIO]  if0-RX-QoSdata(TDFD=01,R=1,P=1)-SN=2(0)-08:bd:43:ff:88:78--DHCP,  Opt=53,
MsgType=2-192.168.1.1

[XRADIO] if0-RX-data(TDFD=01,R=0,P=1)-SN=857(0)-08:bd:43:ff:88:78--unknown

[XRADIO]  if0-TX-QoSdata(TDFD=10,R=0,P=1)-SN=3(0)-08:bd:43:ff:88:78--DHCP,  Opt=53,
MsgType=3-255.255.255.255

[XRADIO]  if0-RX-QoSdata(TDFD=01,R=1,P=1)-SN=3(0)-08:bd:43:ff:88:78--DHCP,  Opt=53,
MsgType=5-192.168.1.1
```


4 常见问题

4.1 开启 WLAN

4.1.1 SDIO 无法识别

在默认的打印等级下，如果出现以下黄色打印信息则表示 SDIO 无法识别。

```
[XRADIO] Driver Label:V1.0  Jul 27 2015 14:03:07
[XRADIO] Allocated hw_priv @ ed1ed980
[XRADIO] Scan SDIO card 1.  //1 表示卡座为卡 1
[SBUS_ERR] sdio probe timeout!
```

对于 SDIO 无法识别，可能存在以下的原因，需要逐个进行排查。

编号	可能原因
1	检查各路电源电压是否正确。
2	检测模组的各个 reset 是否有被正确拉高。
3	检查 32K 时钟是否正常
4	检查 SDIO 各个 IO 是否有上拉电阻。
5	更换芯片或者样机进行测试。
6	检查 SDIO 是否进行了扫卡（一般会有打印）。

4.1.2 SDIO 读写失败

在默认的打印等级下，如果出现类似以下黄色打印信息，其中带有 can't read，can't write 等关键字时，则表示 SDIO 读或写失败。

```
……
[XRADIO_ERR] xradio_load_firmware: can't read config register, err=-110.
[SBUS_ERR] xradio_data_read, error :[-110]
……
```


如果 SDIO 设备已经成功识别，但无法读写寄存器或者 memory，或者不稳，可能存在以下的原因，需要逐个进行排查。

编号	可能原因
1	SDIO 的 data 线存在短地或断路、互相短接等。
2	SDIO 存在 timing 问题，可以降低 SDIO 的频率进行。
3	检查系统平台是否支持非 2 的指数长度传输，如果不支持需要去掉内核的 non-power-of-two SDIO 选项。
4	芯片或者样机本身可能存在问题，可以更换进行测试。
5	对于非 Linux 平台，需要考虑 SDIO 传输长度不能是 512 字节（硬件特性）。

4.1.3 模组无法 wakeup

如果之前的步骤正常，但模组无法 wakeup，则可能是由于 24M 时钟没有正常工作导致。具体的错误打印如下：

```
……
[XRADIO_ERR] xradio_load_firmware: Wait_for_wakeup: device is not responding.
……
```

如果 24M 时钟是有源的，则可以通过示波器进行测量。如果是无源的，则需要硬件部门进行协助分析。一般来说，可能是负载电容过大，或者晶振电路不正确导致。

4.1.4 无法下载 bootloader

在默认的打印等级且之前步骤不出错的情况下，如果没有出现以下黄色打印信息则表示 bootloader 下载失败。可能存在以下的原因，需要逐个进行排查

```
……
[XRADIO] Bootloader complete
……
```

编号	可能原因
1	系统中没有 bootloader 文件，或者文件名错误。
2	26M 时钟不稳定，导致 Memory 读写不稳定。

3	芯片本身可能存在问题，更换芯片尝试。

4.1.5 无法下载 firmware

在默认的打印等级且之前步骤不出错的情况下，如果**没有出现**以下黄色打印信息则表示 firmware 下载失败。可能存在以下的原因，需要逐个进行排查。

```
……

[XRADIO] Firmware completed.

……
```

编号	可能原因
1	系统中没有 firmware 文件，或者文件名错误。
2	26M 时钟不稳定，导致 Memory 读写和 CPU 工作不稳定。
3	电源供电能力不足或不稳，导致 CPU 工作不稳定。
4	芯片本身可能存在问题，更换芯片尝试。
5	固件版本不对。

4.1.6 固件无法 Startup 或 Cmd timeout

在默认的打印等级且之前步骤不出错的情况下，如果出现以下黄色打印信息则表示 firmware 下载失败或者是命令超时，可能存在以下的原因。

```
……
[XRADIO_ERR] Firmware Startup Timeout!
……
```

```
……
[WSM_ERR] ***CMD timeout!>>>
……
```

编号	可能原因
1	中断线没有连接好，或者没有配置好。
2	时钟或者电压的不稳，导致 CPU 工作不稳定。
3	固件版本不对。

4.2 扫描连接

4.2.1 扫描不到 AP 或 AP 很少

wifi 能被正常打开，但是扫描列表中没有显示 AP 信息，可能存在以下的原因。

编号	可能原因
1	通过 iw，wpa_cli 等工具手动扫描分析
2	提高驱动的扫描打印等级为 0xf，查看是否有异常，参考 3.7 章节。
3	通过 driver 的 parse flag 分析，参考“常用工具”章节。
4	通过 Onimpeek 抓包分析扫描过程。
5	RF tx/rx 性能不佳导致，可以进行 ETF 测试进行验证。
6	电源供电能力不足或不稳。

4.2.2 无法连接

编号	可能原因
1	通过 iw，wpa_cli 等工具手动进行连接
2	通过 driver 的 parse flag 分析，参考 3.7.2 章节，查看各个交互过程是否正常。
3	通过 Onimpeek 抓包分析连接交互过程。
4	RF tx/rx 性能不佳导致，可以进行 ETF 测试进行验证。

4.3 通信断开

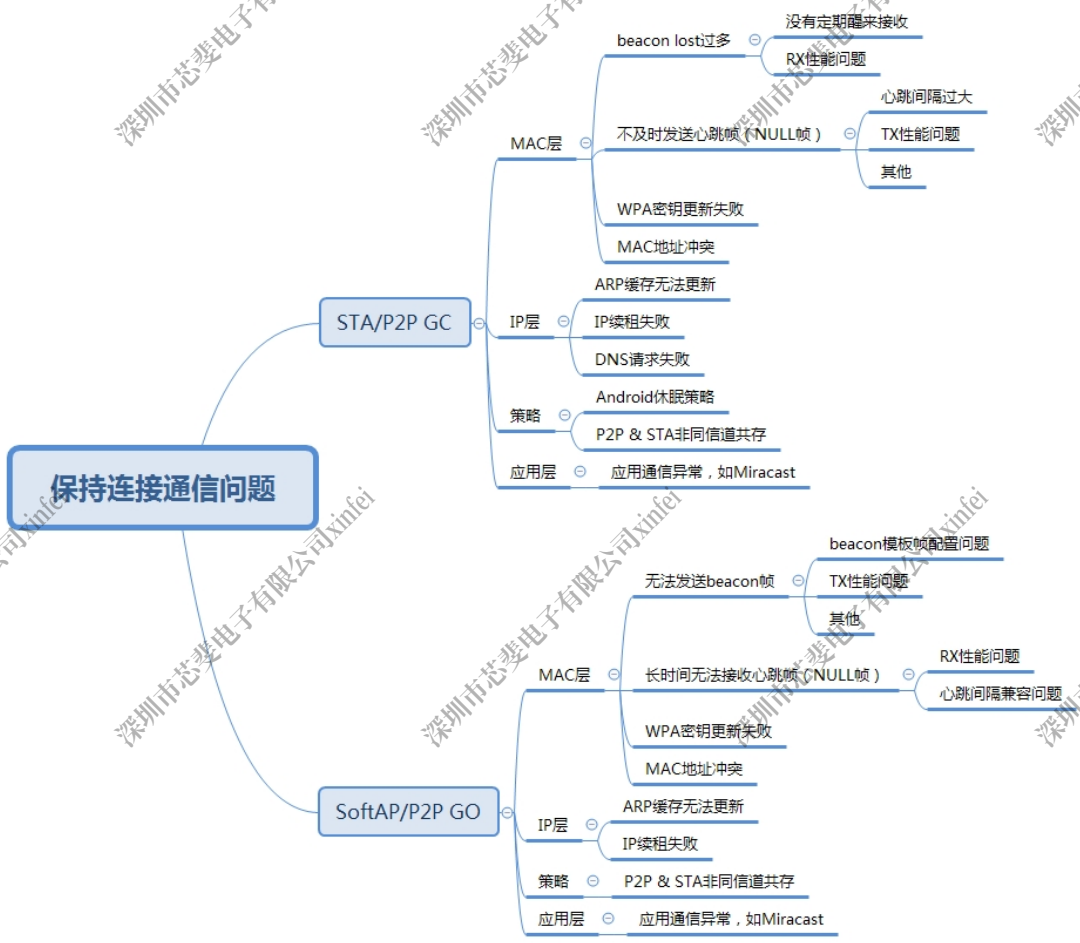

图 4-1 通信断开问题

1）STA/P2P GC 模式的通信失败原因分析：

序号	分类	原因	确认手段和步骤

S1	MAC 层	beacon 帧 lost	1.驱动层 beacon lost 或 bss lost 打印 2.空中抓包确认 AP 是否正常发出 beacon
S2		不及时发送心跳帧	1.空中抓包确认是否长时间无帧交互 2.空中抓包确认心跳帧发送间隔的大小
S3		WPA 密钥更新失败	1.wpa_supplicant 层相关异常打印 2.驱动层 8021x 帧收发打印(parse_flags) 3.空中抓包确认 EAPOL 交互过程
S4	IP 层	ARP 缓存更新失败	1.MAC 没断开，但 ping 超时。 2.查看系统的 ARP 缓存信息。 3.驱动层 ARP 帧收发打印(parse_flags) 4.空中抓包确认 ARP 帧交互过程
S5		IP 续租失败	1.MAC 没断开，但 ping 无法达到目标。 2.上层 DHCP 相关异常打印。 3.驱动层 DHCP 帧收发打印(parse_flags) 4.空中抓包确认 DHCP 帧交互过程
S6		DNS 请求失败	1.MAC 没断开且可以 ping 通 ip，但无法 ping 通域名。 2.TCP dump 抓包查看 DNS 交互过程
S7	策略	Android 休眠策略	3.查看系统休眠策略配置 4.通过系统 logcat 查看相关打印 5.在休眠相关通路添加打印
S8		P2P&STA 共存策略	1.驱动层打印“combo with different channels”。 2.通过查看驱动信息或者抓包确认 P2P 和 STA 是否处于相同信道。
S9	应用层	Miracast	1.通过 logcat 查看是否存在 RTSP 同步控制、RTP 数据流等异常 2.通过 logcat 查看是否编解码或者内存不足等异常

2）Softap/P2P GO 的通信失败原因分析：

序号	分类	原因	确认手段
A1	MAC 层	无法发送 beacon 帧	1.空中抓包确认发送 beacon 帧是否正常
A2		没有收到心跳帧	1.驱动层是否“Inactivity Event”打印 2.空中抓包确认是否长时间无帧交互 3.空中抓包确认心跳帧发送间隔的大小
A3		WPA 密钥更新失败	1.wpa_supplicant 层相关异常打印 2.驱动层 8021x 帧收发打印(parse_flags) 3.空中抓包确认 EAPOL 交互过程
A4	IP 层	ARP 缓存更新失败	1.若 MAC 没断开，尝试 ping 对方的 IP。 2.查看系统的 ARP 缓存信息 3.驱动层 ARP 帧收发打印(parse_flags) 4.空中抓包确认 ARP 帧交互过程
A5		IP 续租失败	1.若 MAC 没断开，尝试 ping 对方的 IP。 2.上层 DHCP 相关异常打印。 3.驱动层 DHCP 帧收发打印(parse_flags) 4.空中抓包确认 DHCP 帧交互过程
A6		P2P&STA 共存策略	1.驱动层打印“combo with different channels”。 2.通过查看驱动信息或者抓包确认 P2P 和 STA 是否处于相同信道。
A7	应用层	Miracast	3.通过 logcat 查看是否存在 RTSP 同步控制、RTP 数据流等异常 4.通过 logcat 查看是否编解码或者内存不足等异常

4.4 吞吐问题

排查问题时需要确认硬件性能是 OK 的，优先使用 UDP Tx/Rx 测试，UDP 没有问题的情况下再进行 TCP 的测试。

问题	说明	方法

屏蔽房吞吐较低，不稳	可能 RF 性能问题	1.确认 TXRX 速率分布，重传率 2.确认 ETF 射频测试指标
	可能主控性能不足	1.通过 dbgstats 确认 AMPDU 长度是否过小。（参考 3.7） 2.通过 status 确认 buf_used 是否过小(参考 3.7） 3.通过 bh_stat 确认 irq/rx 是否过小。 4.提高主控频率进行测试。
	打印过多会影响吞吐.若打印正常则可将打印关掉	通过 cat /proc/kmsg 或串口
	是否有建立块确认会话	需要抓包分析 ADDBA 的收发情况
	其他问题	路由器兼容性问题，更换路由器测试 确认 iperf 版本以及参数配置
干扰吞吐比较低	可能 RF 性能问题	确认 ETF 射频测试指标
	受 PS 很大影响	关闭 PS 尝试，参考 3.7 章节
	Retry 次数不够	debugfs 查看 policy info

