

密级级别：
生效时间：2019年5月6日
保密期限：2年

HIKVISION



网络失联问题梳理及排查思路

机器人业务中心 陈文聪

2019年5月6日

科技呵护未来

— First Choice for Security Professionals —

一、失联问题分类解读

二、排查步骤

三、工具介绍

一、失联问题分类解读

哪些因素会引起失联?

下面提到的每个因素都在实际项目中真实出现过

经过2年多时间的持续改进，从V2.0到V2.6，大多数AGV自身的wifi缺陷已经修复。

在不做新功能迭代或者重构的情况下，网络模块具有较高的鲁棒性！

目前大部分问题与环境 and AP有关系

■ 从技术角度可分为2大类

1. 漫游期间的问题 20%

- 扫描，目标AP的选择问题
- 漫游协议交互，（auth，assoc，4way-handshake）

2. 漫游完成以后的问题。80%

- 被迫下线
- 数据不通（网关，RCS）
- 批量失联

■ 出现概率分类：

1. 必现，呈区域性 80%
2. 偶现，个别AGV零星出现 20%

漫游过程/状态迁移

- 扫描, scan
- 认证/关联, association
- 4次握手, 4-way-handshake (视情况而定)
- 完成, complete

Wifi日志: /mnt/WPA_年_月_日_时_分_秒.log
导出日志, 搜索wlan0: State, 正常的漫游日志

最常见:

```
wlan0: State: ASSOCIATING -> ASSOCIATED  
wlan0: State: ASSOCIATED -> 4WAY_HANDSHAKE  
wlan0: State: 4WAY_HANDSHAKE -> 4WAY_HANDSHAKE  
wlan0: State: 4WAY_HANDSHAKE -> GROUP_HANDSHAKE  
wlan0: State: GROUP_HANDSHAKE -> COMPLETED
```

```
wlan0: State: DISCONNECTED -> SCANNING  
wlan0: State: SCANNING -> ASSOCIATING  
wlan0: State: ASSOCIATING -> ASSOCIATED  
wlan0: State: ASSOCIATED -> 4WAY_HANDSHAKE  
wlan0: State: 4WAY_HANDSHAKE -> 4WAY_HANDSHAKE  
wlan0: State: 4WAY_HANDSHAKE -> GROUP_HANDSHAKE  
wlan0: State: GROUP_HANDSHAKE -> COMPLETED
```

较特殊:

```
wlan0: State: COMPLETED -> ASSOCIATING  
wlan0: State: ASSOCIATING -> ASSOCIATED  
wlan0: State: ASSOCIATED -> COMPLETED
```

扫描 scan（AP选择问题）

HIKVISION

信号覆盖问题，找不到符合要求的信号 60%

漫游阈值： -68dbm

如果扫描到的AP都低于这个阈值，或者该区域经常性低于这个阈值
那就会容易出现失联

确认方式：

wpa_cli scan

wpa_cli scan_r

2.5版本的重要修改

单（多）信道扫描 -> 全信道扫描

根据实际部署，用户可选择扫描哪些信道。

选择**2.4G** 或者 **5G** 。尽量不要使用**auto**模式， **auto**模式是为了兼容性设计。
现场的部署也尽量选择其中一种，对于给**AGV**使用的网络，不建议**2.4**和**5G**混用。

典型的关联失败 30%

- 情况1: wlan0: State: ASSOCIATING -> DISCONNECTED
- 情况2: wlan0: State: COMPLETE -> DISCONNECTED

原因:

1. 信号覆盖或者干扰问题, 超出重传限制, 导致管理帧丢失。
2. AP策略, 检测低信号, 检测到无业务数, 将sta踢下线
3. AP工作异常, 响应慢导致关联超时, 容易出现漫游成功率低。
4. 安全性限制, 比如AGV 网卡的mac地址未在后台登记等, 防火墙

4次握手问题

HIKVISION

四次握手过程断开
10%

```
wlan0: State: COMPLETED -> ASSOCIATING
wlan0: State: ASSOCIATING -> ASSOCIATED
wlan0: State: ASSOCIATED -> 4WAY_HANDSHAKE
wlan0: State: 4WAY_HANDSHAKE -> 4WAY_HANDSHAKE
wlan0: State: 4WAY_HANDSHAKE -> 4WAY_HANDSHAKE
wlan0: State: 4WAY_HANDSHAKE -> 4WAY_HANDSHAKE
wlan0: State: 4WAY_HANDSHAKE -> DISCONNECTED
```

1. 检查密钥

wpa_cli list_network 可以查看ssid和密钥

2. 四次握手时间长，需要升级AP，并勘探现场干扰情况

```
: [19:32:19:936961]: wlan0: State: COMPLETED -> ASSOCIATING
: [19:32:20:810089]: wlan0: State: ASSOCIATING -> ASSOCIATED
: [19:32:21:030882]: wlan0: State: ASSOCIATED -> 4WAY_HANDSHAKE
: [19:32:21:383869]: wlan0: State: 4WAY_HANDSHAKE -> 4WAY_HANDSHAKE
: [19:32:21:666821]: wlan0: State: 4WAY_HANDSHAKE -> 4WAY_HANDSHAKE
: [19:32:26:861728]: wlan0: State: 4WAY_HANDSHAKE -> 4WAY_HANDSHAKE
: [19:32:27:064095]: wlan0: State: 4WAY_HANDSHAKE -> 4WAY_HANDSHAKE
: [19:32:27:128122]: wlan0: State: 4WAY_HANDSHAKE -> GROUP_HANDSHAKE
: [19:32:27:147802]: wlan0: State: GROUP_HANDSHAKE -> COMPLETED
```

3. 某些AP的密钥更新，存在缺陷

AGV长时间处于静止状态

比如H3C，需要升级AC版本到R5226

用undo ptk-rekey enable 命令关闭密钥更新

■ 从技术角度可分为2大类

1. 漫游期间的问题 20%

- 扫描，目标AP的选择问题
- 漫游协议交互，（auth，assoc，4way-handshake，complete）

2. 漫游完成以后的问题。80%

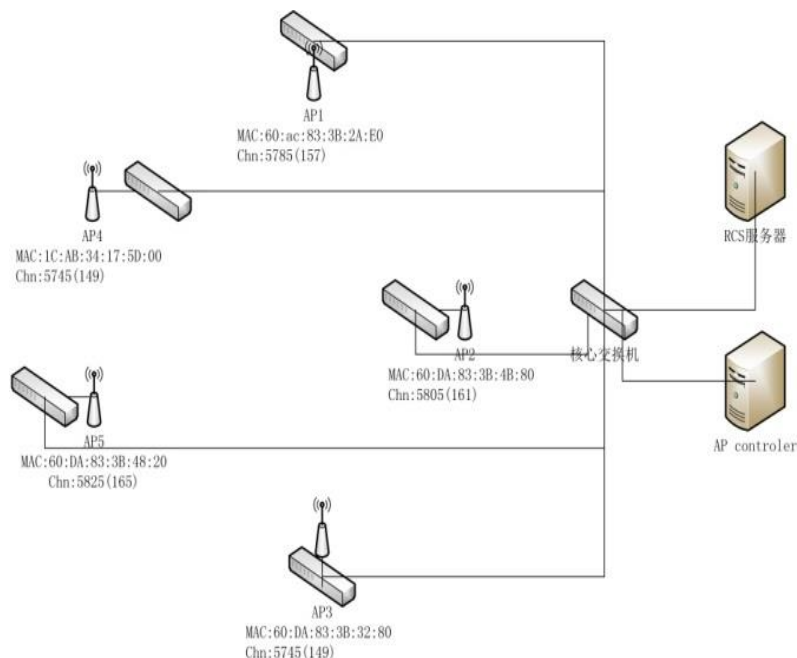
- 被迫下线
- 数据不通（网关，RCS）
- 批量失联

导致AGV网络不稳定因素：

- 信号覆盖弱，无法满足AGV运行要求； 50%
- 与办公网络混用，大流量影响稳定性 30%
- 项目中存在多个SSID，2.4G，5G混用
- 非法的AP介入，相同SSID不同网络。
- AP的开启了智能天线，节能选项；
- 密集终端场景，同一个AP接入STA过多，导致AP负载过高，表现为拒绝关联
- 区域AP信道分布不合理，重合信道的AP过多，导致信道利用率过高；
- 5G模式下带宽设置 $\geq 20\text{Mhz}$ ， 导致邻频干扰加剧
- 部署过于密集，导致信道利用率过高；

网络部署相关（2）

- 网段分配问题，Ip地址冲突
- 有线网络与无线处于同一个网段
- 获取不到ip地址，dhcp服务器异常，自己配置一个ip即可确认。
- 防火墙未关闭，导致私有报文无法穿透
- AGV的mac地址未在后台登记
- 交换机异常重启
- AP异常
- AC异常
- AP/AC存在缺陷，新项目中要确保更新固件



- 交换机Arp更新问题

系统视图下开启: *mac-address update arp*

- 密钥更新问题，会导致失联2分钟左右，建议关闭密钥更新

升级AC版本到R5226

关闭密钥更新命令: *undo ptk-rekey enable*

- 关闭FT功能（快速漫游）

非标准三层漫游网络

■ 跨网段问题，漫游后要重新申请ip地址

跨楼层漫游，早期桐庐项目，华为项目

ifconfig，确认当前ip地址（A）

arp -a，获取arp表项

udhcpc，获取到ip地址（B）

ifconfig wlan0 B，配置wlan0的IP, ping网关，查看联通性。

AP兼容性相关

■ 申通项目，sadb搜索不到设备

原因：组密钥协商失败。

华为AP，在WPA2 CCMP配置下，GTK协商没有用标准的实现方案，（GTK协商不在四次握手完成，而是单独有GTK的协商），导致GTK协商出现问题，组播/广播出现异常，Sadb就是依赖于二层广播帧，这就影响了上层业务

项目中遇到单播正常，组播不通情况，可以考虑从这个方向着手（特别是其他厂家的AP）

■ 现场AP开启FT 功能会存在兼容性问题，建议关闭

其他因素触发失联

HIKVISION

个体失联：

- 系统崩溃，导致AGV重启
- 小车由于地码视频丢失导致重启了 重启后不在码上导致的失联
- 电池原因，导致AGV反复重启
- AGV系统占用高，影响到通信业务，导致失联，（日日顺物流）

批量失联

- RCS服务器崩溃重启

说了这么多因素，那么如何快速分类判定呢？
有没有一个基本的操作流程

二、排查步骤

■ 观察现象

失联区域，时间

区域信号强度，干扰， 某个AP问题等因素

批量性 or 个体

批量：后台网络，RCS等因素较大

失联前夕AGV的运动状态

静止

漫游过程出问题概率较低

运动

■ 信号强度勘测

在易失联区域，用笔记本/手机接入网络，
做对比。

工具：wifi魔盒， 可看强度，可测漫游

■ 不同AGV之间做对比

设置的wifi参数是否一致？

wpa_cli roam_info

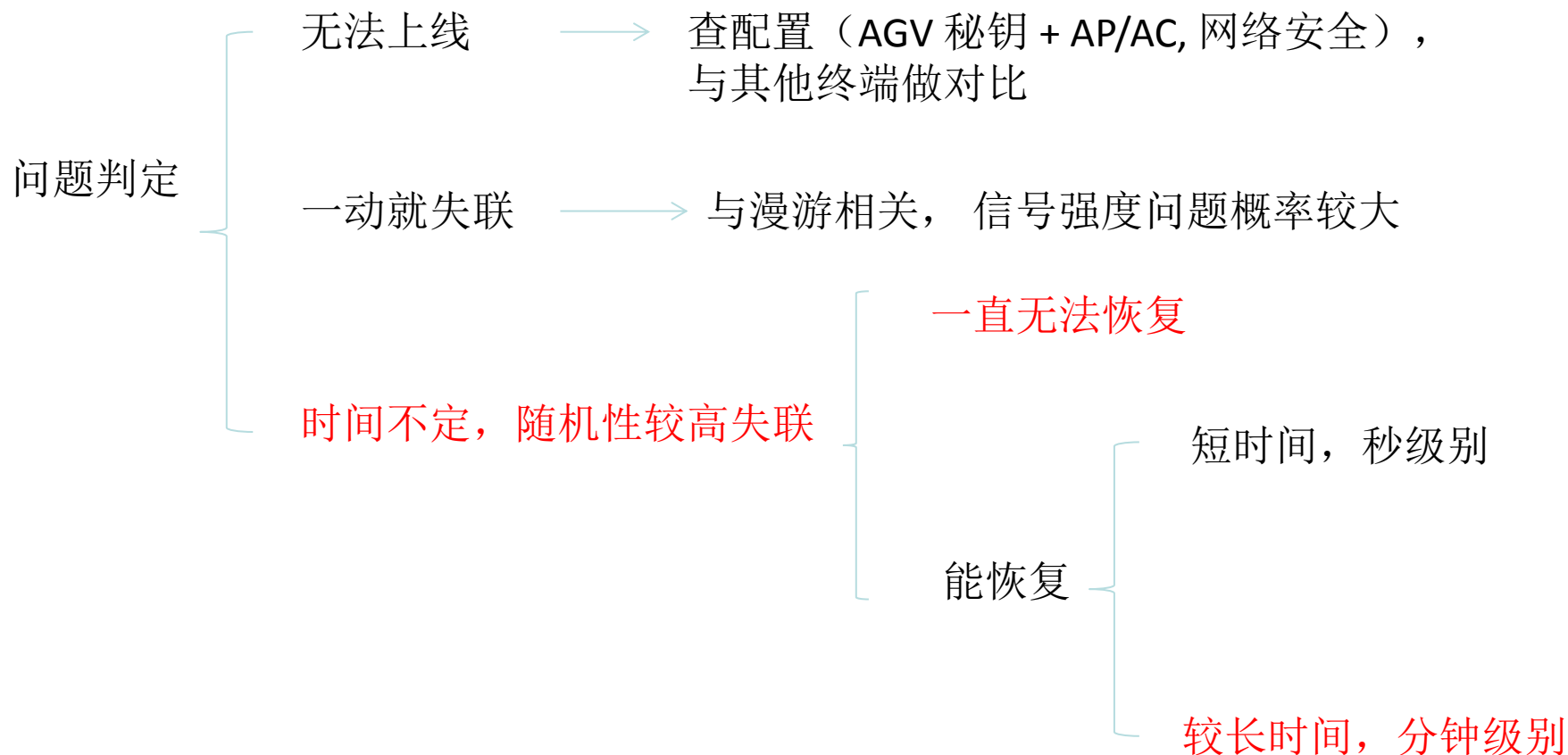
版本一致性

wpa_cli status

```
/root # wpa_cli roam_info  
Selected interface 'wlan0'  
on_off 1  
trigger -68  
delta 5  
indoor 0  
scan_period 1 s  
ccode CN  
band 2G  
freq_list  
/root #
```

```
/root # wpa_cli status  
Selected interface 'wlan0'  
bssid=48:7a:da:ae:88:b1  
freq=2412  
ssid=express-wifi  
id=0  
mode=station  
pairwise_cipher=CCMP  
group_cipher=CCMP  
key_mgmt=WPA2-PSK  
wpa_state=COMPLETED  
ip_address=10.64.27.98  
address=28:ed:e0:6f:92:5a  
wifi_roam_svn-208773
```

- 做对比测试，如果手机或电脑也无法上线，那必然是后台网络问题
- 手动配置AGV的ip地址，如果能ping通，怀疑是dhcp问题
- 运动or静止状态下失联，判断是否和漫游切换有关
- 观察失联是否批量性，是否和区域有关，搜索该区域最近的AP，用手机/PC进行对比测试



wpa_supplicant 进程在不在 ps命令

```
235 root      0 SW      [kworker/0:2]
264 root      0 SWN     [jffs2_gcd_mtd6]
268 root      0 SW      [kworker/u8:2]
272 root     24244 S        /home/centaurus
277 root     4736 S        /home/log_tool
278 root     2232 S        /usr/sbin/inetd -f
290 root      0 SW      [jbd2/mmcblk2p3-]
291 root      0 SW<     [ext4-rsv-conver]
349 root      0 SW      [wl_event_handle]
350 root      0 SW      [usb-thread]
351 root      0 SW      [usb-tx-thread]
368 root     7640 S        /home/wpa_supplicant -Dnl80211 -iwlan0 -c/etc/wpa_supplicant.conf -B
396 root     2332 S        /bin/sh
397 root     2468 S        /sbin/dropbear
398 root     2332 S        -sh
```

框架程序是否正常， Wpa_cli status

确定当前状态及wifi版本号

```
491 root     2332 R        ps
/root # wpa_cli status
Selected interface 'wlan0'
bssid=48:7a:da:ae:88:b1
freq=2412
ssid=express-wifi
id=0
mode=station
pairwise_cipher=CCMP
group_cipher=CCMP
key_mgmt=WPA2-PSK
wpa_state=COMPLETED
ip_address=10.64.27.98
address=28:ed:e0:6f:92:5a
wifi_roam_svn=208773
/root #
```

驱动是否正常 lsmod

```
391 root     2332 R        ps
/root # lsmod
bcmhdhd 494503 0 - Live 0x7f000000 (o)
/root #
```

■ 判定漫游过程 or 漫游完成后

漫游过程
继续分析WPA日志

关注扫描结果: scan_result

关注是否存在超时 timeout

关注disconnect, deauth

漫游完成
wpa_cli status
Complete状态

Ifconfig 看下wlan0 的 ip 在不在， 不在？ dhcpc看下能否获取ip

Ping 一下网关， 能通吗？ 笔记本也ping AGV试一下

tcpdump抓个包看看

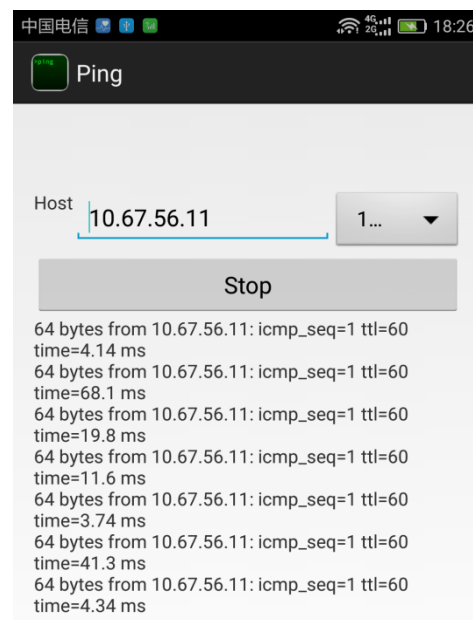
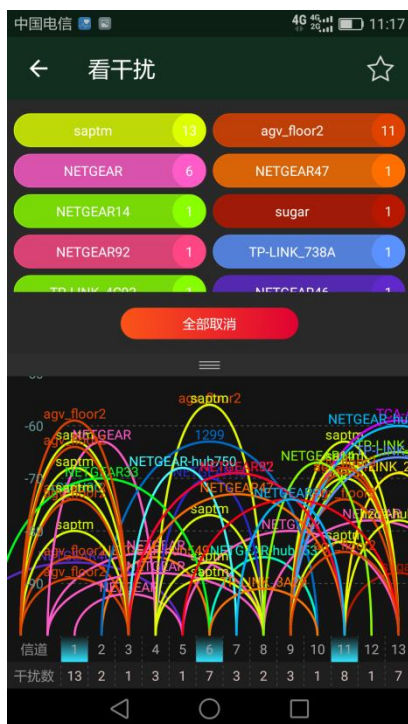
omnipeek抓个包看看

现场勘测工具

HIKVISION

■ Wifi魔盒

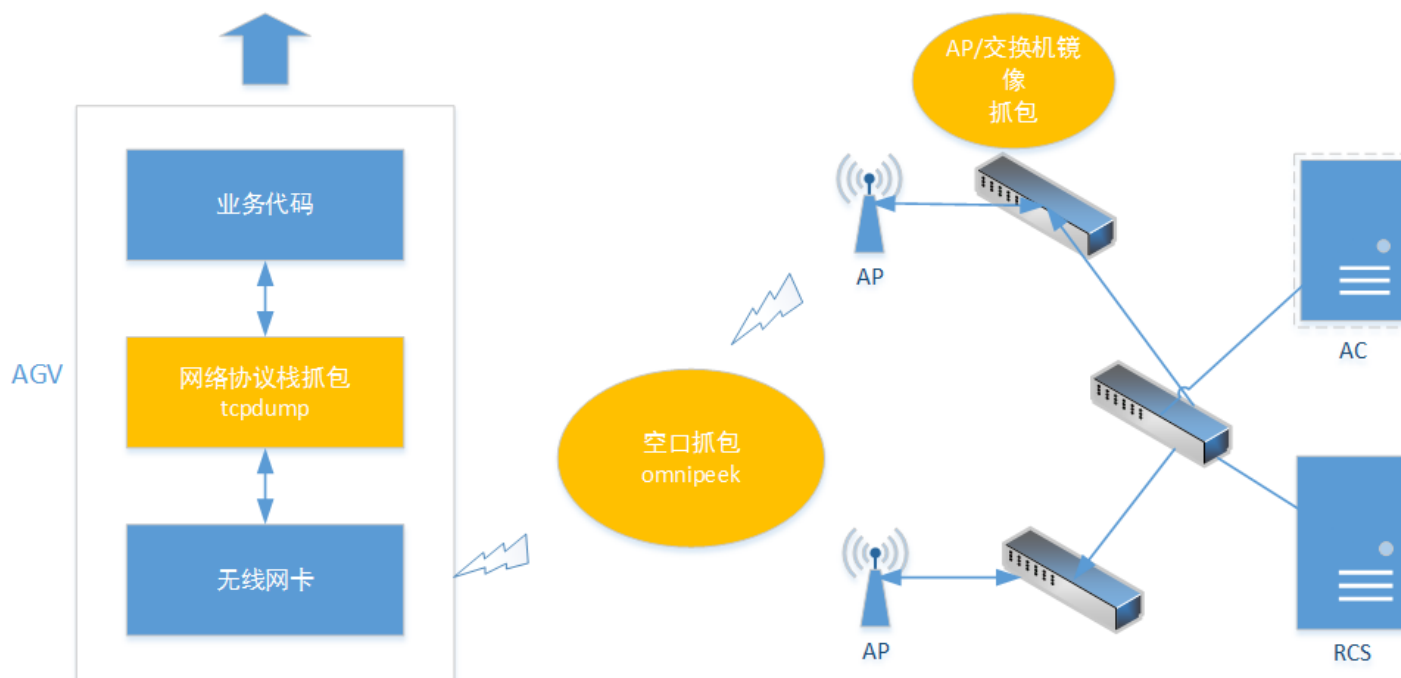
功能：初步勘探现场wifi环境，测试不同AP的信号强度，集成了ping等工具可测试联通性。



抓包定位问题

- tcpdump , 协议栈抓包
- 空口抓包 , wifi抓包

适用场景：漫游完成情况下，仍长时间处于失联情况下。
需要证明AGV是否有报文发出



tcpdump的使用



HIKVISION

出现失联现象时，不要重启AGV。

1. 使用有线的方式ssh登录到agv
2. `cd /mnt`
3. 将附件中的工具（tcpdump, arping）导入到agv，ssh敲rz，选择window下要导入的文件
4. 导入后agv后，要修改将工具修改为可执行权限
`chmod +x tcpdump`
5. 查看当前的ip地址
`ifconfig`
6. 开始抓包
`./tcpdump -i wlan0 -C 100M -w arp.cap`
7. 在失联状态下差不多抓2分钟，按ctrl+c 结束抓包
8. 将当前目录下arp.cap 以及抓包期间的WPA日志导出来，发给我

- 确定当前关联的信道， `wpa_cli status`
- 在AGV测输入`ifconfig` 可以获取wlan0的mac地址

■ 漫游问题分类

- 漫游前，目标选择问题(scan)
- 漫游期间，报文交互及处理逻辑问题（auth，assoc，4way-handshake）
- 漫游后，数据不通
- 与业务层交互问题
- 兼容性问题

综合运用才能找到问题的直接原因，如果一些现象无法解释，需要将现象清晰的反馈到研发。

Q & A

HIKVISION