# WIFI

## Softap wpa\_cli的使用

在平台开发初期阶段，对于WIFI相关问题，上层应用如果还无法使用，或者需要定位问题的层次，这时可以借助wpa\_cli，下面介绍一些wpa\_cli 调试WIFI的基础用法。

借助下面命令可以排除：

Wifi扫描、Wifi连接、Wifi配置等问题。

在串口中执行下面命令：

root@k200:/ # wpa\_cli -i wlan0 -p wlan0

wpa\_cli v2.1-devel-4.3

Copyright (c) 2004-2013, Jouni Malinen <j@w1.fi> and contributors

This software may be distributed under the terms of the BSD license.

See README for more details.

Interactive mode

>

此时进入与wpa\_supplicant 的交换模式。输入h能查看所有wpa\_cli的支持的命令，由于命令太多，此处不贴出来。下面以表格形式介绍wpa\_cli基本命令以及用法：

|  |  |  |  |
| --- | --- | --- | --- |
| **命令** | **命令缩写** | **描述** | **测试** |
| status | stat | 显示当前连接的状态信息 | > stat  bssid=c8:3a:35:16:89:88  ssid=Tenda\_168988  id=1  mode=station  pairwise\_cipher=CCMP  group\_cipher=CCMP  key\_mgmt=WPA-PSK  wpa\_state=COMPLETED  ip\_address=192.168.0.142  address=00:50:43:02:ff:01  > |
| ping |  | 测试指令，看service端是否有响应 | > ping  PONG  > |
| interface |  | 显示当前可用的interface，wpa\_supplicant 支持多interface | > interface  Available interfaces:  wlan0  > |
| set |  | 设置环境变量，如果不带参数，显示当前环境变量 | > set  set variables:  EAPOL::heldPeriod (EAPOL state machine held period, in seconds)  EAPOL::authPeriod (EAPOL state machine authentication period, in seconds)  EAPOL::startPeriod (EAPOL state machine start period, in seconds)  EAPOL::maxStart (EAPOL state machine maximum start attempts)  dot11RSNAConfigPMKLifetime (WPA/WPA2 PMK lifetime in seconds)  dot11RSNAConfigPMKReauthThreshold (WPA/WPA2 reauthentication threshold  percentage)  dot11RSNAConfigSATimeout (WPA/WPA2 timeout for completing security  association in seconds)  > |
| reassociate | reas | 设置连接标签，开启扫描，查找可用的AP进行连接，如果当前是连接状态，只会扫描一次。 | <3>CTRL-EVENT-SCAN-RESULTS  <3>WPS-AP-AVAILABLE  <3>Trying to associate with 94:ba:56:00:32:14 (SSID='yl\_B19W4' freq=2462 MHz)  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=5 BSSID=94:ba:56:00:32:14  <3>CTRL-EVENT-STATE-CHANGE id=0 state=6 BSSID=94:ba:56:00:32:14  <3>Associated with 94:ba:56:00:32:14  <3>CTRL-EVENT-CONNECTED - Connection to 94:ba:56:00:32:14 completed (reauth) [id=0 id\_str=]  <3>CTRL-EVENT-STATE-CHANGE id=0 state=9 BSSID=00:00:00:00:00:00  <3>CTRL-EVENT-STATE-CHANGE id=0 state=0 BSSID=00:00:00:00:00:00  <3>CTRL-EVENT-DISCONNECTED bssid=00:00:00:00:00:00 reason=0  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=3 BSSID=00:00:00:00:00:00 |
| preauthenticate | pr | 针对一个AP进行预认证 | > pr c8:3a:35:16:89:88  OK  <3>RSN: failed to get master session key from pre-auth EAPOL state machines  <3>RSN: pre-authentication with c8:3a:35:16:89:88 failed |
| identity | id | 设置identity | > id 0 xxxx  OK  > save\_config  OK  >  cat wpa\_supplicant.conf  network={  ssid="yl\_B19W4"  key\_mgmt=NONE  identity="xxxx"  password="123455678"  disabled=1  } |
| password |  | 设置密码 | password 0<network id> 11111111  network={  ssid="yl\_B19W4"  key\_mgmt=NONE  identity="xxxx"  password="11111111111"  disabled=1  } |
| disconnect | disc | 断开连接，并且会告知wpa\_supplicant 不在连接其他AP | > disc  OK  <3>CTRL-EVENT-STATE-CHANGE id=1 state=0 BSSID=00:00:00:00:00:00  <3>CTRL-EVENT-DISCONNECTED bssid=00:00:00:00:00:00 reason=0 |
| reconnect | reconn | 重新连接，在运行上面的过程后，运行此命令 | > reconn  OK  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=3 BSSID=00:00:00:00:00:00  <3>CTRL-EVENT-SCAN-RESULTS  <3>WPS-AP-AVAILABLE  <3>Trying to associate with a4:a8:0f:fc:18:3a (SSID='XXXXXXX' freq=2462 MHz)  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=5 BSSID=a4:a8:0f:fc:18:3a  <3>CTRL-EVENT-STATE-CHANGE id=1 state=6 BSSID=a4:a8:0f:fc:18:3a  <3>Associated with a4:a8:0f:fc:18:3a  <3>CTRL-EVENT-CONNECTED - Connection to a4:a8:0f:fc:18:3a completed (reauth) [id=1 id\_str=]  <3>CTRL-EVENT-STATE-CHANGE id=1 state=9 BSSID=00:00:00:00:00:00 |
| quit | q | 退出wpa\_cli |  |
| terminate | term | 杀掉后台wpa\_supplicant进程 |  |
| reconfigure | recon | 重新导入配置文件，可以在调试时，修改配置文件后运行此命令，使配置文件生效 |  |
| scan | scan | 扫描 | scan  > OK  <3>CTRL-EVENT-SCAN-RESULTS  <3>WPS-AP-AVAILABLE |
| scan\_result | scan\_r | 显示扫描结果 | scan\_r  > bssid / frequency / signal level / flags / ssid  a4:a8:0f:fc:18:3a 2462 -59 [ESS] XXXXXXX  d4:ee:07:03:ee:0c 2427 -68 [WPA-PSK-CCMP][WPA2-PSK-CCMP][ESS] HiWiFi\_03EE0C  d8:5d:4c:25:d0:f2 2412 -72 [WPA-PSK-CCMP][WPA2-PSK-CCMP-preauth][ESS] OTG  c8:3a:35:16:89:88 2462 -83 [WPA-PSK-CCMP][ESS] Tenda\_168988 |
| bss |  | 获取扫描结果 某一个热点的具体信息 | bss <<idx> | <bssid>>  bss 1  > id=371  bssid=d4:ee:07:03:ee:0c  freq=2427  beacon\_int=100  capabilities=0x0431  qual=0  noise=0  level=-72  tsf=0000016060803119  ie=000d4869576946695f303345453043010882848b960c1218240301042a010032043048606c2d1a6e101bff000000000000000000000000000000000000000000003d16040d000000000000000000000000000000000000000030140100000fac040100000fac040100000fac020000dd160050f20101000050f20401000050f20401000050f202dd180050f2020101000003a4000027a4000042435e0062322f00dd06d4ee07010100  flags=[WPA-PSK-CCMP][WPA2-PSK-CCMP][ESS]  ssid=HiWiFi\_03EE0C  > |
| list\_networks | list\_n | 已经保存配置文件中的AP | > list  network id / ssid / bssid / flags  0 yl\_B19W4 c8:3a:35:16:89:88  1 XXXXXXX any  > |
| bssid |  | 配置ssid的bssid | bssid 0 c8:3a:35:16:89:88  结果下面可以看到 |
| add\_network | add\_n | 添加一个AP配置，在framework还没调通之前，可以用此命令进行配置 | > add\_n  7  > save\_config  OK  > list  network id / ssid / bssid / flags  0 yl\_B19W4 c8:3a:35:16:89:88 [DISABLED]  2 客厅里的飞看\_B186M any [DISABLED]  3 客厅里的飞看\_B1PKO any [DISABLED]  4 XXXXXXX any [CURRENT]  5 Tenda\_168988 any [DISABLED]  6 any [DISABLED]  7 any [DISABLED] --🡪添加的  >save\_config --🡪如果想保存到配置文件中 |
| set\_network | set\_n | 设置ap的属性，用set\_network 不接参数，可以看到所有可用信息。 | > set\_n  set\_network variables:  ssid (network name, SSID)  psk (WPA passphrase or pre-shared key)  key\_mgmt (key management protocol)  identity (EAP identity)  password (EAP password)  ...  ------------------------------------------------------  > set\_n 7 ssid "B2C2.5"  OK  > list  network id / ssid / bssid / flags  0 yl\_B19W4 c8:3a:35:16:89:88 [DISABLED]  2 客厅里的飞看\_B186M any [DISABLED]  3 客厅里的飞看\_B1PKO any [DISABLED]  4 XXXXXXX any [CURRENT]  5 Tenda\_168988 any [DISABLED]  6 any [DISABLED]  7 B2C2.5 any [DISABLED]  > set\_n 7 psk 22225555  FAIL  > set\_n 7 psk "22225555"  OK  > list  network id / ssid / bssid / flags  0 yl\_B19W4 c8:3a:35:16:89:88 [DISABLED]  2 客厅里的飞看\_B186M any [DISABLED]  3 客厅里的飞看\_B1PKO any [DISABLED]  4 XXXXXXX any [CURRENT]  5 Tenda\_168988 any [DISABLED]  6 any [DISABLED]  7 B2C2.5 any [DISABLED]  > save  OK  配置成功 |
| select\_network | select\_n | 选择一个已经配置的AP进行连接，这个命令用的比较多。上面set\_n 命令进行配置后，可以用这命令进行连接 | > sel 7  OK 这样supplicant会自动连接B2C2.5 这个热点  --------------  > stat  bssid=c8:3a:35:16:89:88  ssid=Tenda\_168988  id=5  mode=station  pairwise\_cipher=CCMP  group\_cipher=CCMP  key\_mgmt=WPA-PSK  wpa\_state=COMPLETED  ip\_address=192.168.0.142  address=00:50:43:02:ff:01  ---------------------------------------  查看当前状态  ---------------------------------------  > list  network id / ssid / bssid / flags  0 yl\_B19W4 c8:3a:35:16:89:88 [DISABLED]  2 客厅里的飞看\_B186M any [DISABLED]  3 客厅里的飞看\_B1PKO any [DISABLED]  4 XXXXXXX any [DISABLED]  5 Tenda\_168988 any [CURRENT]  ---------- 查看当前可选的AP  ----------  > sel 4  OK  <3>CTRL-EVENT-STATE-CHANGE id=5 state=0 BSSID=00:00:00:00:00:00  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=3 BSSID=00:00:00:00:00:00  <3>CTRL-EVENT-DISCONNECTED bssid=00:00:00:00:00:00 reason=0  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=0 BSSID=00:00:00:00:00:00  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=3 BSSID=00:00:00:00:00:00  <4>Failed to initiate AP scan  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=0 BSSID=00:00:00:00:00:00  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=3 BSSID=00:00:00:00:00:00  <4>Failed to initiate AP scan  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=0 BSSID=00:00:00:00:00:00  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=3 BSSID=00:00:00:00:00:00  <4>Failed to initiate AP scan  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=0 BSSID=00:00:00:00:00:00  <3>CTRL-EVENT-SCAN-RESULTS  <3>WPS-AP-AVAILABLE  <3>Trying to associate with a4:a8:0f:fc:18:3a (SSID='XXXXXXX' freq=2462 MHz)  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=5 BSSID=a4:a8:0f:fc:18:3a  <3>CTRL-EVENT-STATE-CHANGE id=4 state=6 BSSID=a4:a8:0f:fc:18:3a  <3>Associated with a4:a8:0f:fc:18:3a  <3>CTRL-EVENT-CONNECTED - Connection to a4:a8:0f:fc:18:3a completed (reauth) [id=4 id\_str=]  <3>CTRL-EVENT-STATE-CHANGE id=4 state=9 BSSID=00:00:00:00:00:00  ------- 选择进行连接 -------  stat  > bssid=a4:a8:0f:fc:18:3a  ssid=XXXXXXX  id=4  mode=station  pairwise\_cipher=NONE  group\_cipher=NONE  key\_mgmt=NONE  wpa\_state=COMPLETED  ip\_address=192.168.88.101  address=00:50:43:02:ff:01  >  查看当前状态，连接ok |
| enable\_network | enable\_n | 将network 的标志位  disable 置0，该位为1时，wifi在断开连接状态，不会去主动连接该热点。如果wifi不主动连接任何热点，可以查看配置文件。 | network={  ssid="客厅里的飞看\_B186M"  key\_mgmt=NONE  disabled=1  }  network={  ssid="客厅里的飞看\_B1PKO"  key\_mgmt=NONE  disabled=1  }  network={  ssid="XXXXXXX"  key\_mgmt=NONE  }  network={  ssid="Tenda\_168988"  psk="12345678"  key\_mgmt=WPA-PSK  disabled=1  } |
| disable\_network | disable\_n | 对应上面  disable\_network network\_id |  |
| remove\_network | remove\_n | 忘记网络  remove\_network id  会删除对应network配置 |  |
| get\_network | get\_n | 获取network的属性  对应之前的set\_network | set\_network variables:  ssid (network name, SSID)  psk (WPA passphrase or pre-shared key)  key\_mgmt (key management protocol)  identity (EAP identity)  password (EAP password)  ...  > get\_network 0 ssid  "yl\_B19W4"  > list  network id / ssid / bssid / flags  0 yl\_B19W4 c8:3a:35:16:89:88 [DISABLED]  2 客厅里的飞看\_B186M any [DISABLED]  3 客厅里的飞看\_B1PKO any [DISABLED]  4 XXXXXXX any [DISABLED]  5 Tenda\_168988 any [DISABLED]  6 any [DISABLED]  7 B2C2.5 any [DISABLED]  > |
| wps\_pbc |  | wps push button功能 | 前提:路由开启wps push button功能  下面我已经打开Tenda\_168988 wps push button功能，然后在盒子上运行wps\_pbc  wps\_pbc  > OK  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=3 BSSID=00:00:00:00:00:00  <3>CTRL-EVENT-SCAN-RESULTS  <3>WPS-AP-AVAILABLE  <3>CTRL-EVENT-SCAN-RESULTS  <3>WPS-AP-AVAILABLE  <3>CTRL-EVENT-SCAN-RESULTS  <3>WPS-AP-AVAILABLE  <3>CTRL-EVENT-SCAN-RESULTS  <3>WPS-AP-AVAILABLE-PBC  <3>Trying to associate with c8:3a:35:16:89:88 (SSID='Tenda\_168988' freq=2412 MHz)  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=5 BSSID=c8:3a:35:16:89:88  <3>CTRL-EVENT-STATE-CHANGE id=8 state=6 BSSID=c8:3a:35:16:89:88  <3>Associated with c8:3a:35:16:89:88  <3>CTRL-EVENT-EAP-STARTED EAP authentication started |
| wps\_pin |  | Wps pin 功能 | 前提:打开路由热点wps功能，并设置pin值 如12345678，用scan\_r查看你想要连接的ssid的bssid，然后用下面命令进行连接  > wps\_pin c8:3a:35:16:89:88 12345678  12345678  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=3 BSSID=00:00:00:00:00:00  <3>CTRL-EVENT-SCAN-RESULTS  <3>WPS-AP-AVAILABLE-AUTH  <3>Trying to associate with c8:3a:35:16:89:88 (SSID='Tenda\_168988' freq=2412 MHz)  <3>CTRL-EVENT-STATE-CHANGE id=-1 state=5 BSSID=c8:3a:35:16:89:88  <3>CTRL-EVENT-STATE-CHANGE id=8 state=6 BSSID=c8:3a:35:16:89:88  <3>Associated with c8:3a:35:16:89:88  <3>CTRL-EVENT-EAP-STARTED EAP authentication started |
| save\_config | save\_c | 保存信息到配置文件中，每次修改配置后记得用 |  |
|  |  |  |  |
|  |  |  |  |

## Softap hostapd\_cli的使用

hostapd\_cli相对wpa\_cli来说比较简单，能使用的命令也非常少。

借助下面命令可以解决：

wifi热点配置、查看设备连接时长等问题。

hostapd\_cli –h

Options:

-h help (show this usage text)

-v shown version information

-p<path> path to find control sockets (default: /var/run/hostapd)

-a<file> run in daemon mode executing the action file based on events

from hostapd

-B run a daemon in the background

-i<ifname> Interface to listen on (default: first interface found in the

socket path)

hostapd\_cli 运行:

hostapd\_cli -i uap0 -p /data/misc/wifi/hostapd

下面列表列出了hostapd\_cli能使用的指令，以及使用方法：

|  |  |  |  |
| --- | --- | --- | --- |
| 命令 | 命令缩写 | 描述 | 测试 |
| all\_sta | al | 显示当前连入的STA,并记录连上的时间长度 | > all\_sta  40:f3:08:39:b6:74  connected\_time=579  00:90:4c:78:5d:5c  connected\_time=3359  > all  00:90:4c:78:5d:5c  connected\_time=3458 |
| deauthenticate <addr> | dea | 解除验证 | > all  40:f3:08:39:b6:74 ---🡪我的设备  connected\_time=59  00:90:4c:78:5d:5c  connected\_time=4008  > dea 40:f3:08:39:b6:74 -🡪可以看到设备断开，又启动连接  OK |
| disassociate <addr> |  | 断开连接 | 过程与上面差不多 |
| wps\_pin |  | AP端的wps功能 |  |
| wps\_pbc |  | Ap端的wps功能 |  |
| wps\_config <SSID> <auth> <encr> <key> |  | 配置Ap的属性 |  |

-s snaplen ] [ -T type ] [ -w file ]  
 [ -W filecount ]  
 [ -E spi@ipaddr algo:secret,... ]  
 [ -y datalinktype ] [ -Z user ]  
 [ expression ]

# tcpdump

普通情况下，直接启动tcpdump将监视第一个网络接口上所有流过的数据包。

监视指定网络接口的数据包

tcpdump -i eth1

如果不指定网卡，默认tcpdump只会监视第一个网络接口，一般是eth0，下面的例子都没有指定网络接口。

## 监视指定主机和端口的数据包

如果想要获取主机210.27.48.1接收或发出的telnet包，使用如下命令

tcpdump tcp port 23 host 210.27.48.1

对本机的udp 123 端口进行监视 123 为ntp的服务端口

tcpdump udp port 123

## tcpdump 与wireshark联合使用

Wireshark(以前是ethereal)是Windows下非常简单易用的抓包工具。但在Linux下很难找到一个好用的图形化抓包工具。  
还好有Tcpdump。我们可以用Tcpdump + Wireshark 的完美组合实现：在 Linux 里抓包，然后在Windows 里分析包。

tcpdump tcp -i eth1 -t -s 0 -c 100 and dst port ! 22 and src net 192.168.1.0/24 -w ./target.cap

(1)tcp: ip icmp arp rarp 和 tcp、udp、icmp这些选项等都要放到第一个参数的位置，用来过滤数据报的类型  
(2)-i eth1 : 只抓经过接口eth1的包  
(3)-t : 不显示时间戳  
(4)-s 0 : 抓取数据包时默认抓取长度为68字节。加上-S 0 后可以抓到完整的数据包  
(5)-c 100 : 只抓取100个数据包  
(6)dst port ! 22 : 不抓取目标端口是22的数据包  
(7)src net 192.168.1.0/24 : 数据包的源网络地址为192.168.1.0/24  
(8)-w ./target.cap : 保存成cap文件，方便用ethereal(即wireshark)分析

# 3.性能分析

## Top

root@zs600b:/ # top -m 10

-t表示查看线程

CTRL+C结束统计，