工具使用篇：wpa_supplicant和wireless-tool

不懂内核的小潘
软件开发行业 研发工程师

关注他

本篇文章讲述下最常用的连接配置无线网络的工具:wireless-tools 或wpa_supplicant。下面说下这两个工具的使用方法

wpa_supplicant

1. wpa_supplicant是一个开源项目，已经被移植到Linux，Windows以及很多嵌入式系统上。它是WPA的应用层认证客户端，负责完成认证相关的登录、加密等工作。
2. wpa_supplicant是一个 独立运行的 守护进程，其核心是一个消息循环，在消息循环中处理WPA状态机、控制命令、驱动事件、配置信息等。

wpa_supplicant依赖于openssl库，所以在编译wpa_supplicant前要先编译安装下openssl 3.0库。经过编译后的wpa_supplicant源程序可以看到两个主要的可执行工具：wpa_supplicant和wpa_cli。wpa_supplicant是核心服务程序，它和wpa_cli的关系就是服务端和客户端的关系：后台运行wpa_supplicant。wpa_cli通过wpa_request里的send向wpa_supplicant进程发出搜索，设置，连接网络命令并得到结果

如何用wpa_supplicant连接一个WiFi热点?

当加载完wlan驱动后，首先起的就是wpa_supplicant服务端的守护进程

其运行wpa_supplicant 命令如下：

```
/usr/bin/wpa_supplicant -d -Dnl80211 -iwlan0 -c/etc/wpa_supplicant.conf -B

/usr/bin/wpa_supplicant : wpa_supplicant可执行程序path

-d : debug  增加调试信息

-D : driver 可选指定的驱动程序，nl80211是当前的标准，但并非所有无线芯片的模块都支持它；wext

-i : interface 网络接口名称 wlan0

-c : ilename  -c是读取配置文件/etc/wpa_supplicant.conf

-B: 后台运行
```

```
wpa_supplicant.conf是配置文件内容，如果用wpa_cli配置网络的话，至少要保证以下两行在配置文件
# 指定socket路径方便和hostapd_cli通信
ctrl_interface=/var/run/wpa_supplicant
# 使用wpa_supplicant来扫描和选择AP
ap_scan=1
```

```
# 存储已连接的SSID密码(非必须写入，但一般也要写入)，不然使用不了wpa_cli save_config
update_config=1
```

连接不加密的SSID的配置文件

```
ctrl_interface=/var/run/wpa_supplicant
update_config=1
ap_scan=1

network={
     ssid="NONE_TEST"
     key_mgmt=NONE
 }
```

连接WPA2-PSK/WPA-PSK的SSID的配置文件

```
ctrl_interface=/var/run/wpa_supplicant
update_config=1
ap_scan=1

network={
    ssid="WPA2_PSK_TEST"
     key_mgmt=WPA-PSK
     psk="11111111"
 }
```

连接WPA3-PSE的SSID的配置文件

```
ctrl_interface=/var/run/wpa_supplicant
update_config=1
ap_scan=1

network={
     ssid="WPA3_PSE_TEST"
     key_mgmt=SAE
     psk="11111111"
     ieee80211w=2
 }
```

上述方法将指定的SSID的配置信息写进wpa_supplicant.conf配置文件里，每次启机不需要在配置无线网络直接起DHCP进程即可获取网络，不过该方法不够灵活，下面的方法可以随意指定连入任何加密方式的热点

wpa_cli配置连接不加密的SSID

```
wpa_cli -i wlan0 add_network
wpa_cli -i wlan0 set_network 0 ssid '"NONE_TEST"'
wpa_cli -i wlan0 set_network 0 key_mgmt NONE
wpa_cli -i wlan0 enable_network 0
```

wpa_cli配置连接WPA2-PSK的SSID

```
wpa_cli -i wlan0 add_network
wpa_cli -i wlan0 set_network 0 ssid '"WPA2_PSK_TEST"'
wpa_cli -i wlan0 set_network 0 key_mgmt WPA2-PSK
wpa_cli -i wlan0 set_network 0 psk '"11111111"'
wpa_cli -i wlan0 enable_network 0
```

wpa_cli配置连接WPA3-PSE的SSID

```
wpa_cli -i wlan0 add_network
wpa_cli -i wlan0 set_network 0 ssid '"WPA3_PSE_TEST"'
wpa_cli -i wlan0 set_network 0 key_mgmt SAE
wpa_cli -i wlan0 set_network 0 psk '"11111111"'
wpa_cli -i wlan0 set_network 0 ieee80211w 2
wpa_cli -i wlan0 enable_network 0
```

其他常用的wpa_cli的命令

```
# wpa_cli status                //查看网络状态
Selected interface 'wlan0'
bssid=00:0b:82:a4:2d:f2
freq=5745
ssid=WPA2_PSK_TEST
id=1
mode=station
wifi_generation=5
pairwise_cipher=CCMP
group_cipher=CCMP
key_mgmt=WPA2-PSK
wpa_state=COMPLETED
ip_address=192.168.132.136
address=c0:74:ad:e8:5e:60
ieee80211ac=1

# wpa_cli scan          //打开搜索周围WiFi热点扫描信息
Selected interface 'wlan0'
OK

# wpa_cli scan_results  //列出热点扫描结果
c2:74:ad:79:f1:0d       2412    -61     [WPA2-PSK-CCMP][ESS]    8888
c2:74:ad:69:f1:0d       2412    -62     [WPA2-PSK-CCMP][ESS]    7777
c2:74:ad:49:f0:85       2462    -63     [WPA2-PSK-CCMP][ESS]    5555
c2:74:ad:9e:a0:b9       2437    -64     [WPA2-PSK-CCMP][ESS]    ygz1111

# wpa_cli list_network           //查看当前设备下当前记住几个SSID
Selected interface 'wlan0'
network id / ssid / bssid / flags
0       wp_master       any
1       WPA2_TEST any     [CURRENT]
2       WPA3_TEST   any

# wpa_cli enable_network $NET_ID //使能哪个net_id
# wpa_cli select_network $NET_ID //切换使用哪个net_id
# wpa_cli remove_network $NET_ID  //忘记某个net_id，也就是忘记哪个SSID

# wpa_cli disconnect //断开网络连接
# wpa_cli reconfigure //wpa_supplicant进程起来的时候再次重新加载配置文件/etc/wpa_supp
# wpa_cli save_config //保存已连过的状态及优先级
# wpa_cli reconnect // 重新连接

一接入USB无线网卡，就自动执行wpa_supplicant等
可以用热插拔mdev机制

一连接WIFI AP，就自动执行dhclient，可以写脚本后台监测
# wpa_cli -a/sbin/wpa_action.sh -B //后台监测脚本wpa_action.sh
```

wireless-tool也是比较常用的工具

WirelessTools (WT)就是用来操作对无线网卡进行配置的工具集，编译时依赖于libnl库，wpa_cli几乎可以配置连接所有无线网卡,但是WirelessTools不一定可以操作所有无线网卡，它包括以下工具：

iwconfig：设置基本无线参数，是无线标准ioctl用户态工具

iwlist：扫描、列出频率，比特率，密钥等

iwspy：获取每个节点链接的质量

iwpriv：iwpriv是iwconfig的辅助工具，无线私有ioctl用户态工具

ifrename： 基于各种静态标准命名接口

通过以上工具实现对无线网络的监控、分析、以及测试WIFI网络。

常用的工具命令有以下这些：

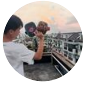
```
iwlist 相关的
# iwlist
Usage: iwlist [interface] scanning [essid NNN] [last]
              [interface] frequency
              [interface] channel
              [interface] bitrate
              [interface] rate
              [interface] encryption
              [interface] keys
              [interface] power
              [interface] txpower
              [interface] retry
              [interface] ap
              [interface] accesspoints
              [interface] peers
              [interface] event
              [interface] auth
              [interface] wpakeys
              [interface] genie
              [interface] modulation

# iwlist wlan0 scan  //列出区域内的无线网络
          Cell 01 - Address: C2:74:AD:49:F0:85
                    ESSID:"5555"
                    Mode:Managed
                    Frequency:2.462 GHz (Channel 11)
                    Quality:2/5  Signal level:-72 dBm  Noise level:0 dBm
                    IE: IEEE 802.11i/WPA2 Version 1
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : PSK
                    Encryption key:on
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s
                              11 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s; 36 Mb/s
                              48 Mb/s; 54 Mb/s
          Cell 02 - Address: C2:74:AD:42:F7:9A
                    ESSID:"7777"
                    Mode:Managed
                    Frequency:5.765 GHz
                    Quality:2/5  Signal level:-76 dBm  Noise level:0 dBm
                    IE: IEEE 802.11i/WPA2 Version 1
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : PSK
                    Encryption key:on
                    Bit Rates:6 Mb/s; 9 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s
                              36 Mb/s; 48 Mb/s; 54 Mb/s
          Cell 03 - Address: C2:74:AD:9E:A0:B9
                    ESSID:"ygz1111"
                    Mode:Managed
                    Frequency:2.437 GHz (Channel 6)
                    Quality:4/5  Signal level:-62 dBm  Noise level:0 dBm
                    IE: IEEE 802.11i/WPA2 Version 1
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : PSK
                    Encryption key:on
                    Bit Rates:1 Mb/s; 2 Mb/s; 5.5 Mb/s; 6 Mb/s; 9 Mb/s
                              11 Mb/s; 12 Mb/s; 18 Mb/s; 24 Mb/s; 36 Mb/s
                              48 Mb/s; 54 Mb/s
# iwlist wlan0 rate //看协商速率
# iw wlan0 link 查看

iw相关的
# iw list  # 查看本机支持的无线特性, such as band information (2.4 GHz, and 5 GHz),
iphy phy0
        wiphy index: 0
        max # scan SSIDs: 10
        max scan IEs length: 2048 bytes
        max # sched scan SSIDs: 0
        max # match sets: 0
        max # scan plans: 1
        max scan plan interval: -1

GSPHONE: read event: 16
        max scan plan iterations: 0

        Retry short limit: 7
GSPHONE: the changed link device index: 3, name is: wlan0 state: 1

        Retry long limit: 4
        Coverage class: 0 (up to 0m)
        Device supports roaming.
        Device supports T-DLS.
        Supported Ciphers:
                * WEP40 (00-0f-ac:1)
                * WEP104 (00-0f-ac:5)
                * TKIP (00-0f-ac:2)
                * CCMP-128 (00-0f-ac:4)
                * CMAC (00-0f-ac:6)
                * GMAC-256 (00-0f-ac:12)
                * GMAC-128 (00-0f-ac:11)
                * CMAC-256 (00-0f-ac:13)
                * 00-90-4c:0
                * GCMP-128 (00-0f-ac:8)
                * GCMP-256 (00-0f-ac:9)
                * GMAC-128 (00-0f-ac:11)
                * GMAC-256 (00-0f-ac:12)
        Available Antennas: TX 0 RX 0
        Supported interface modes:
                 * IBSS
                 * managed
                 * AP
                 * P2P-client
                 * P2P-GO
                 * P2P-device
        Band 1:
                Capabilities: 0x1020
                        HT20
                        Static SM Power Save
                        RX HT20 SGI
                        No RX STBC
                        Max AMSDU length: 3839 bytes
                        DSSS/CCK HT40
                Maximum RX AMPDU length 65535 bytes (exponent: 0x003)
                Minimum RX AMPDU time spacing: 16 usec (0x07)
                HT RX MCS rate indexes supported: 0-7
                HT TX MCS rate indexes are undefined
                Bitrates (non-HT):
                        * 1.0 Mbps
                        * 2.0 Mbps (short preamble supported)
                        * 5.5 Mbps (short preamble supported)
                        * 11.0 Mbps (short preamble supported)
                        * 6.0 Mbps
                        * 9.0 Mbps
                        * 12.0 Mbps
                        * 18.0 Mbps
                        * 24.0 Mbps
                        * 36.0 Mbps
                        * 48.0 Mbps
                        * 54.0 Mbps
                Frequencies:
                        * 2412 MHz [1] (20.0 dBm)
                        * 2417 MHz [2] (20.0 dBm)
                        * 2422 MHz [3] (20.0 dBm)
                        * 2427 MHz [4] (20.0 dBm)
                        * 2432 MHz [5] (20.0 dBm)
                        * 2437 MHz [6] (20.0 dBm)
                        * 2442 MHz [7] (20.0 dBm)
                        * 2447 MHz [8] (20.0 dBm)
                        * 2452 MHz [9] (20.0 dBm)
                        * 2457 MHz [10] (20.0 dBm)
                        * 2462 MHz [11] (20.0 dBm)
                        * 2467 MHz [12] (disabled)
                        * 2472 MHz [13] (disabled)
                        * 2484 MHz [14] (disabled)
        Band 2:
                Capabilities: 0x1020
                        HT20
                        Static SM Power Save
                        RX HT20 SGI
                        No RX STBC
                        Max AMSDU length: 3839 bytes
                        DSSS/CCK HT40
                Maximum RX AMPDU length 65535 bytes (exponent: 0x003)
                Minimum RX AMPDU time spacing: 16 usec (0x07)
                HT RX MCS rate indexes supported: 0-7
                HT TX MCS rate indexes are undefined
                VHT Capabilities (0x0f805132):
                        Max MPDU length: 11454
                        Supported Channel Width: neither 160 nor 80+80
                        RX LDPC
                        short GI (80 MHz)
                        SU Beamformee
                VHT RX MCS set:
                        1 streams: MCS 0-9
                        2 streams: not supported
                        3 streams: not supported
                        4 streams: not supported
                        5 streams: not supported
                        6 streams: not supported
                        7 streams: not supported
                        8 streams: not supported
                VHT RX highest supported: 0 Mbps
                VHT TX MCS set:
                        1 streams: MCS 0-9
                        2 streams: not supported
                        3 streams: not supported
                        4 streams: not supported
                        5 streams: not supported
                        6 streams: not supported
                        7 streams: not supported
                        8 streams: not supported
                VHT TX highest supported: 0 Mbps
                Bitrates (non-HT):
                        * 6.0 Mbps
                        * 9.0 Mbps
                        * 12.0 Mbps
                        * 18.0 Mbps
                        * 24.0 Mbps
                        * 36.0 Mbps
                        * 48.0 Mbps
                        * 54.0 Mbps
                Frequencies:
                        * 5170 MHz [34] (disabled)
                        * 5180 MHz [36] (30.0 dBm)
                        * 5190 MHz [38] (disabled)
                        * 5200 MHz [40] (30.0 dBm)
                        * 5210 MHz [42] (disabled)
                        * 5220 MHz [44] (30.0 dBm)
                        * 5230 MHz [46] (disabled)
                        * 5240 MHz [48] (30.0 dBm)
                        * 5260 MHz [52] (30.0 dBm) (no IR, radar detection)
                        * 5280 MHz [56] (30.0 dBm) (no IR, radar detection)
                        * 5300 MHz [60] (30.0 dBm) (no IR, radar detection)
                        * 5320 MHz [64] (30.0 dBm) (no IR, radar detection)
                        * 5500 MHz [100] (30.0 dBm) (no IR, radar detection)
                        * 5520 MHz [104] (30.0 dBm) (no IR, radar detection)
                        * 5540 MHz [108] (30.0 dBm) (no IR, radar detection)
                        * 5560 MHz [112] (30.0 dBm) (no IR, radar detection)
                        * 5580 MHz [116] (30.0 dBm) (no IR, radar detection)
                        * 5600 MHz [120] (30.0 dBm) (no IR, radar detection)
                        * 5620 MHz [124] (30.0 dBm) (no IR, radar detection)
                        * 5640 MHz [128] (30.0 dBm) (no IR, radar detection)
                        * 5660 MHz [132] (30.0 dBm) (no IR, radar detection)
                        * 5680 MHz [136] (30.0 dBm) (no IR, radar detection)
                        * 5700 MHz [140] (30.0 dBm) (no IR, radar detection)
                        * 5720 MHz [144] (30.0 dBm) (no IR, radar detection)
                        * 5745 MHz [149] (30.0 dBm)
                        * 5765 MHz [153] (30.0 dBm)
                        * 5785 MHz [157] (30.0 dBm)
                        * 5805 MHz [161] (30.0 dBm)
                        * 5825 MHz [165] (30.0 dBm)
        Supported commands:
                 * new_interface
                 * set_interface
                 * new_key
                 * start_ap
                 * set_bss
                 * join_ibss
                 * set_pmksa
                 * del_pmksa
                 * flush_pmksa
                 * remain_on_channel
                 * frame
                 * frame_wait_cancel
                 * set_wiphy_netns
                 * set_channel
                 * tdls_mgmt
                 * tdls_oper
                 * start_p2p_device
                 * channel_switch
                 * connect
                 * disconnect
        Supported TX frame types:
                 * IBSS: 0x00 0x10 0x20 0x30 0x40 0x50 0x60 0x70 0x80 0x90 0xa
                 * managed: 0x00 0x10 0x20 0x30 0x40 0x50 0x60 0x70 0x80 0x90
                 * AP: 0x00 0x10 0x20 0x30 0x40 0x50 0x60 0x70 0x80 0x90 0xa0
                 * AP/VLAN: 0x00 0x10 0x20 0x30 0x40 0x50 0x60 0x70 0x80 0x90
                 * P2P-client: 0x00 0x10 0x20 0x30 0x40 0x50 0x60 0x70 0x80 0x
                 * P2P-GO: 0x00 0x10 0x20 0x30 0x40 0x50 0x60 0x70 0x80 0x90 0x
                 * P2P-device: 0x00 0x10 0x20 0x30 0x40 0x50 0x60 0x70 0x80 0x
        Supported RX frame types:
                 * IBSS: 0xd0
                 * managed: 0x40 0xb0 0xd0
                 * AP: 0x00 0x20 0x40 0xa0 0xb0 0xc0 0xd0
                 * AP/VLAN: 0x00 0x20 0x40 0xa0 0xb0 0xc0 0xd0
                 * P2P-client: 0x40 0xd0
                 * P2P-GO: 0x00 0x20 0x40 0xa0 0xb0 0xc0 0xd0
```

```
                * P2P-device: 0x40 0xd0
        WoWLAN support:
                * wake up on anything (device continues operating normally)
                * wake up on pattern match, up to 8 patterns of 1-255 bytes,
                  maximum packet offset 255 bytes
        software interface modes (can always be added):
        valid interface combinations:
                * #{ AP } <= 2, #{ managed } <= 4, #{ P2P-client, P2P-GO } <=
                  total <= 5, #channels <= 2
        Device supports SAE with AUTHENTICATE command
        Device supports scan flush.
        Supported extended features:

# iw dev wlan0 link # 获取设备连接状态信息（实测不包含IP地址）
Connected to 00:0b:82:a4:2d:f2 (on wlan0)
        SSID: WPA2_TEST
        freq: 5745
        RX: 4389770 bytes (23010 packets)
        TX: 918614 bytes (4140 packets)
        signal: -31 dBm
        rx bitrate: 200.0 MBit/s
        tx bitrate: 200.0 MBit/s

# iw wlan0 info # 获取设备工作状态信息
Interface wlan0
        ifindex 3
        wdev 0x1
        addr c0:74:ad:e8:5e:60
        ssid WP805_ROAM_TEST
        type managed
        wiphy 0
        txpower 31.00 dBm
# iw dev wlan0 set freq 2437 #修改wlan0频率
iw是替换iwconfig

iwconfig相关的
1、配置ssid
# iwconfig wlan0 essid liangym
2、配置mode
# iwconfig wlan0 mode Managed
# iwconfig wlan0 mode monitor
3、配置工作频率
iwconfig wlan0 freq 2422000000
iwconfig wlan0 freq 2.422G
iwconfig wlan0 channel 3
iwconfig wlan0 channel auto
3、配置网络
iwconfig wlan0 key xxxx      //输入验证密码
iwconfig wlan0 key open     //密码验证功能打开
iwconfig wlan0 essid  "test" //设置ESSID
iwconfig wlan0 ap auto       //加入无线网络
```

参考文章：wpa_supplicant - 建筑维基 (archlinux.org)

如果本篇对大家有用的话，记得点赞 + 关注，后续持续更新

对嵌入式相关问题有疑问可以付费咨询



不懂内核的小潘

10 次咨询 ★★★★★ 5.0

软件开发行业 研发工程师

1396 次赞同 去咨询 >

参考链接：

linux 无线网络配置工具wpa_supplicant与wireless-tools .
blog.csdn.net/acs713/article/details/8218…

linux WIFI命令iwlist、iwconfig、iwpriv_panamera12的博客-CSDN博客
blog.csdn.net/wteruiycbqqvwt/article/details/89678177

编辑于 2023-08-27 22:00・IP 属地浙江

「真诚赞赏，手留余香」

赞赏

还没有人赞赏，快来当第一个赞赏的人吧!

开发工具 Wi-Fi

发布一条带图评论吧

还没有评论，发表第一个评论吧

文章被以下专栏收录

WiFi学习专栏
记录下WiFi学习过程

推荐阅读

【无线网络技术专题（十一）】无线网络常用软件与工具大全
网络工程师大彭

浅谈无线VLAN的设置
首先我们来看一个常见的错误配置方式 拓扑 需求1.网络拓扑如上图所示，AC是无线控制器，其E1/0/1口连接着AP的LAN1口 2.按照 表1-1 完成无线网络的配置.使用户连接WLAN使能够获取对应VLAN的I…
一路有你

苹果手机怎么用usb共享网络 搞了一天终于搞定
如果设备管理器是这种情况，下 ccleaner清除注册表搞定。 如果 显示苹果设备，显示的是其他设 然后点开有黄色感叹号 1.打开设 管理器” 2.查看 “通用串行总线 制器”，看看有没有apple…
坤哥2020