

# Wireless Network Setup for Linux Clients

This guide has the purpose to help Linux users (any distro) to setup the connection to Sissa Wi-Fi. The user must have a basic knowledge of the Linux system and must know the fundamental commands and procedures of this environment.

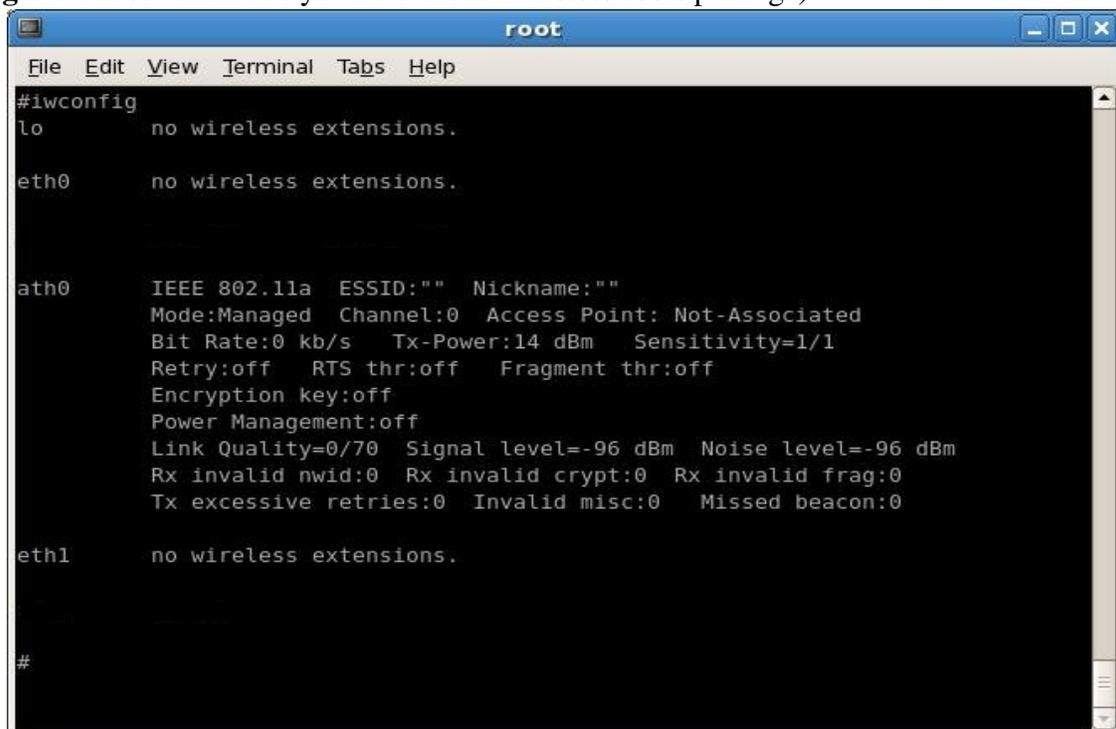
Available Sissa wireless networks (SSID)are:

- **SISSA-WiFi** (scientific and general pupose network: students, faculty, and long-term visitors)
- **SISSA-AMM** (staff network: administrative and techincal persomel)

**Important:** in order to successfully log into one of the Sissa wireless networks **your password must have been updated after december 31, 2007!!**

**Before you can setup a wireless connection you must verify that your *wireless network interface card* (WNIC) is properly installed.**

1. To identify the WNIC, as 'root' user, open a terminal window and type the command **iwconfig** (to use **iwconfig** and **iwlist** commands you must install **wireless-tools** package):



```
root
File Edit View Terminal Tabs Help
#iwconfig
lo      no wireless extensions.

eth0    no wireless extensions.

ath0    IEEE 802.11a  ESSID:""  Nickname:""
Mode:Managed Channel:0 Access Point: Not-Associated
Bit Rate:0 kb/s Tx-Power:14 dBm Sensitivity=1/1
Retry:off RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality=0/70 Signal level=-96 dBm Noise level=-96 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:0 Missed beacon:0

eth1    no wireless extensions.

#
```

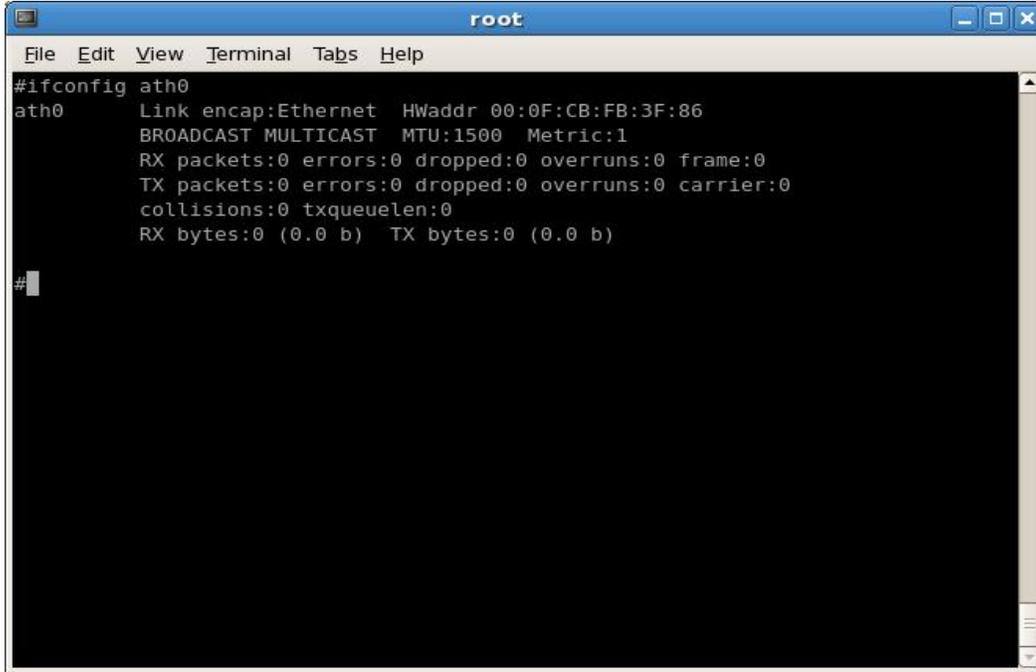
We see that **ath0** is the WNIC device, since i have an *atheros* chipset in my laptop.

On your computer, with a different WNIC chipset, you could see **eth1**, **wifi0**, or other device names that **ath0**.

**If you don't see any network device with wireless extensions in the command output, the WNIC is not properly configured on your system!**

Check the documentation of your WNIC and its drivers for Linux.

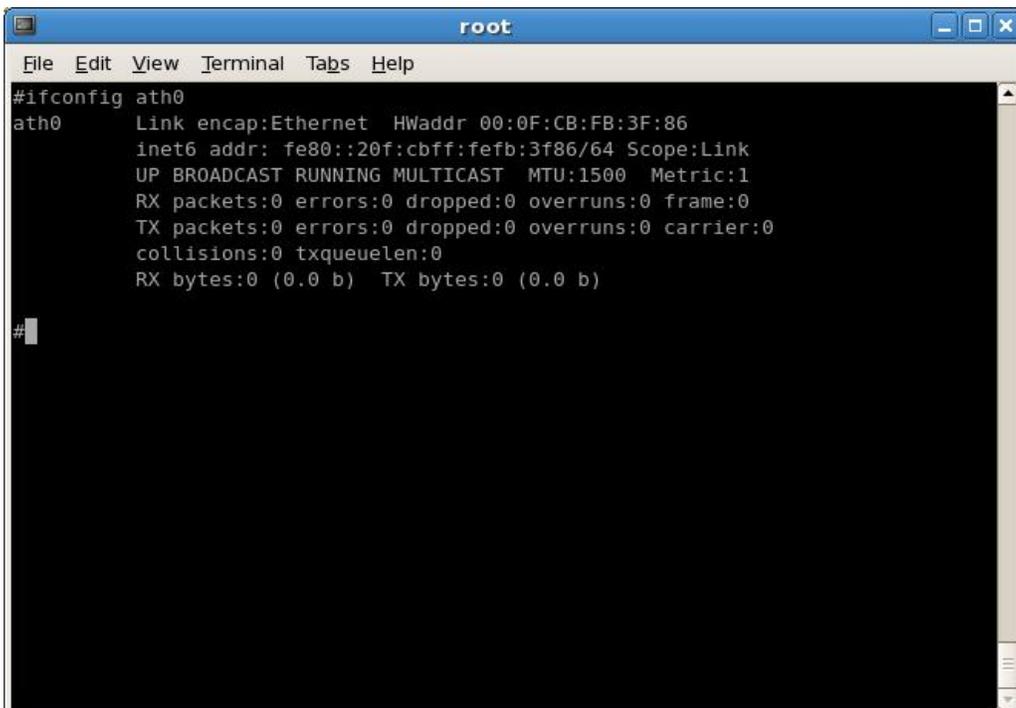
2. To verify and switch on the WNIC, now type the command **ifconfig ath0**



```
root
File Edit View Terminal Tabs Help
#ifconfig ath0
ath0  Link encap:Ethernet  HWaddr 00:0F:CB:FB:3F:86
      BROADCAST MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

#
```

3. Here the WNIC is switched off. To turn it on, type the command **ifconfig ath0 up**, and to verify again **ifconfig ath0**

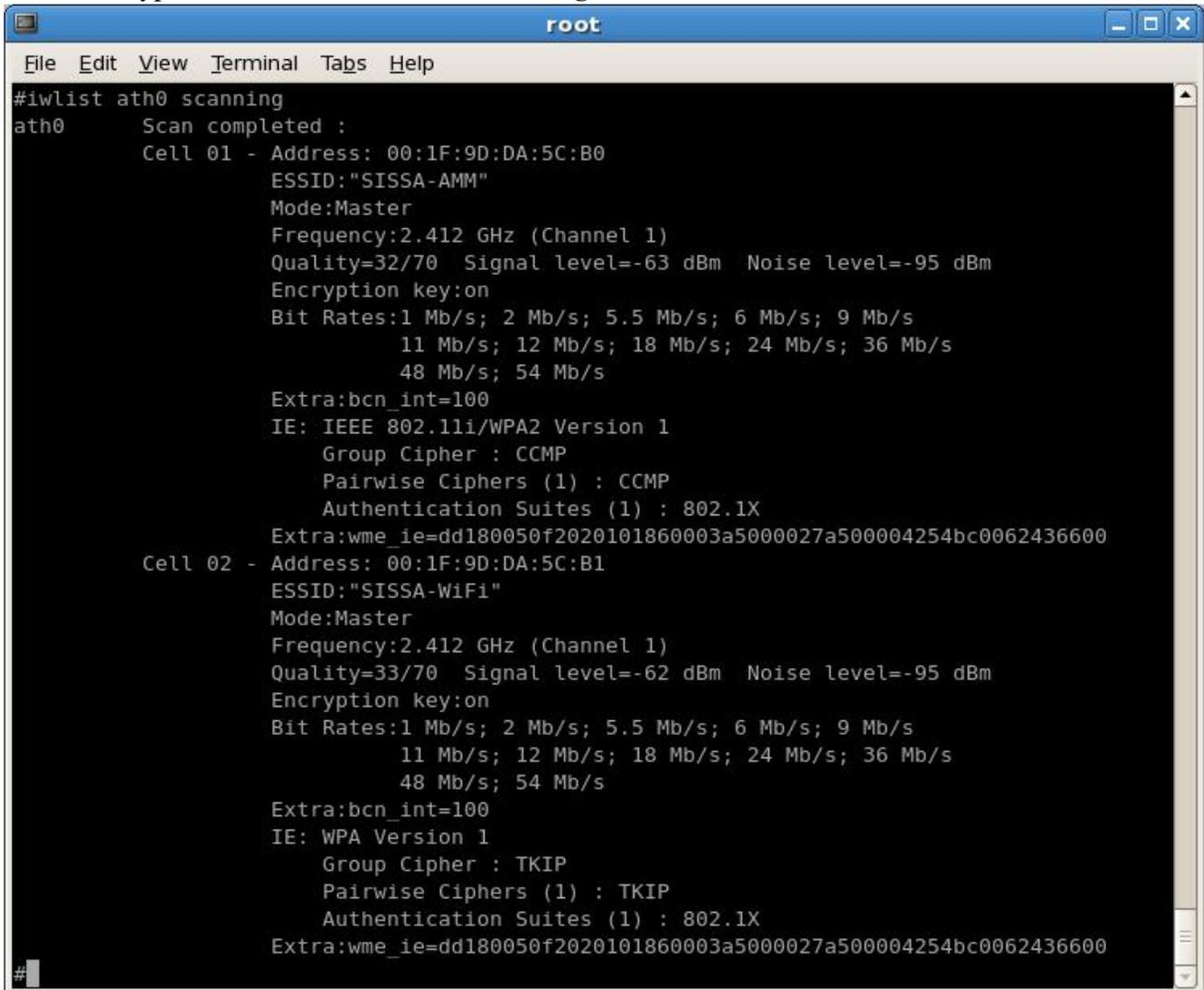


```
root
File Edit View Terminal Tabs Help
#ifconfig ath0
ath0  Link encap:Ethernet  HWaddr 00:0F:CB:FB:3F:86
      inet6 addr: fe80::20f:cbff:febf:3f86/64 Scope:Link
      UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
      RX packets:0 errors:0 dropped:0 overruns:0 frame:0
      TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
      collisions:0 txqueuelen:0
      RX bytes:0 (0.0 b)  TX bytes:0 (0.0 b)

#
```

You should see 'UP', in the second line output, before 'BROADCAST'.

4. Last step: verify that the WNIC works and verify that we are in range of one of the Sissa wireless networks. Type the command **iwlist ath0 scanning**



```
root
File Edit View Terminal Tabs Help
#iwlist ath0 scanning
ath0      Scan completed :
          Cell 01 - Address: 00:1F:9D:DA:5C:B0
                    ESSID:"SISSA-AMM"
                    Mode:Master
                    Frequency:2.412 GHz (Channel 1)
                    Quality=32/70  Signal level=-63 dBm  Noise level=-95 dBm
                    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
                    Extra:bcn_int=100
                    IE: IEEE 802.11i/WPA2 Version 1
                        Group Cipher : CCMP
                        Pairwise Ciphers (1) : CCMP
                        Authentication Suites (1) : 802.1X
                    Extra:wme_ie=dd180050f2020101860003a5000027a500004254bc0062436600
          Cell 02 - Address: 00:1F:9D:DA:5C:B1
                    ESSID:"SISSA-WiFi"
                    Mode:Master
                    Frequency:2.412 GHz (Channel 1)
                    Quality=33/70  Signal level=-62 dBm  Noise level=-95 dBm
                    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
                    Extra:bcn_int=100
                    IE: WPA Version 1
                        Group Cipher : TKIP
                        Pairwise Ciphers (1) : TKIP
                        Authentication Suites (1) : 802.1X
                    Extra:wme_ie=dd180050f2020101860003a5000027a500004254bc0062436600
#
```

We see two networks (SSID): SISSA-AMM and SISSA-WiFi.

5. Once you have verify that your WNIC works, there are several tools you can use to setup a wireless connections on a Linux system. Here we explain how to configure the one of the most widely used: **wpa\_supplicant**

## wpa\_supplicant

**wpa\_supplicant** is an implementation of the WPA Supplicant component, i.e. , the part that runs in the client stations. It implements WPA key negotiation with a WPA Authenticator (i.e. Access Point) and EAP authentication with Authentication Server (read RADIUS). In addition, it controls the roaming and IEEE 802.11 authentication/association of the wireless LAN driver.

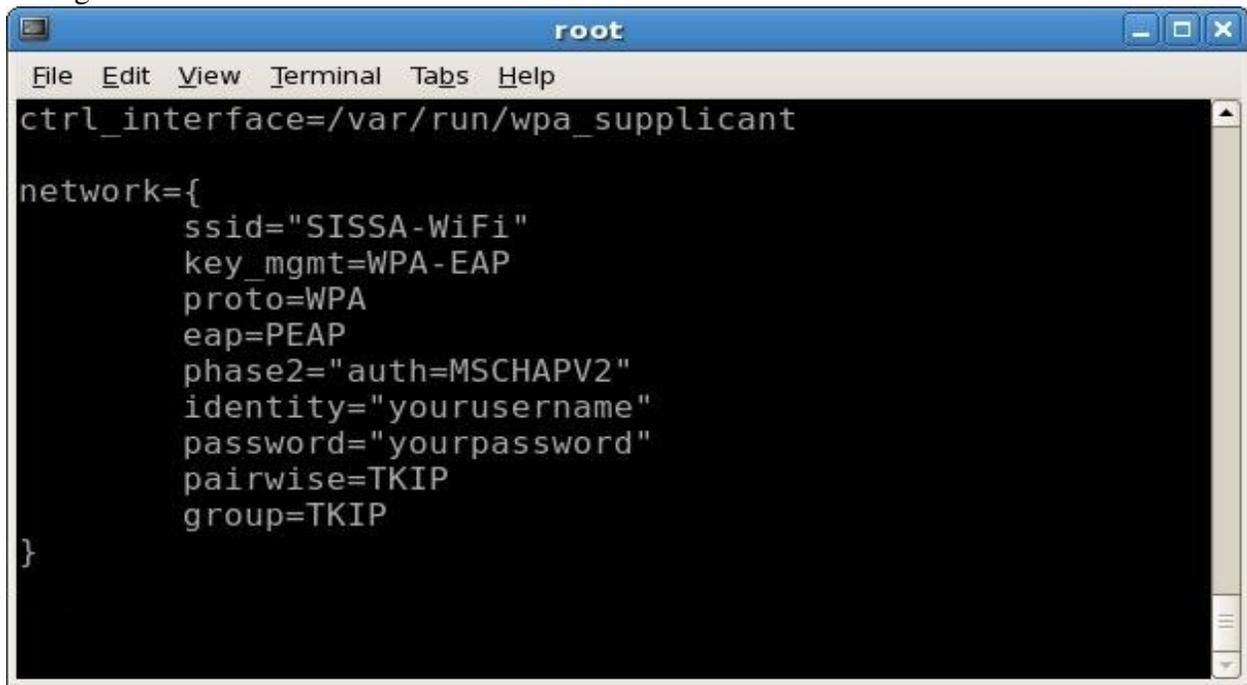
wpa\_supplicant is configured using a text file that lists all accepted networks and security policies, by default this file is /etc/wpa\_supplicant.conf.

To connect to **SISSA-WiFi** network , the configuration parameters are:

- SSID: **SISSA-WiFi**
- Authentication: **PEAP**
- Inner Authentication: **MSCHAP v2**
- Key management: **WPA Enterprise**
- Encryption: **TKIP** or **AES-CCMP**

1.You need to insert this parameters and your credentials (valid username and password) in the wpa\_supplicant configuration file.

Edit the wpa\_supplicant configuration file, say **SISSA-WiFi.wpa\_supplicant.txt**, and insert the following lines:

A screenshot of a terminal window titled "root" with a menu bar containing "File", "Edit", "View", "Terminal", "Tabs", and "Help". The terminal displays the following configuration for wpa\_supplicant:

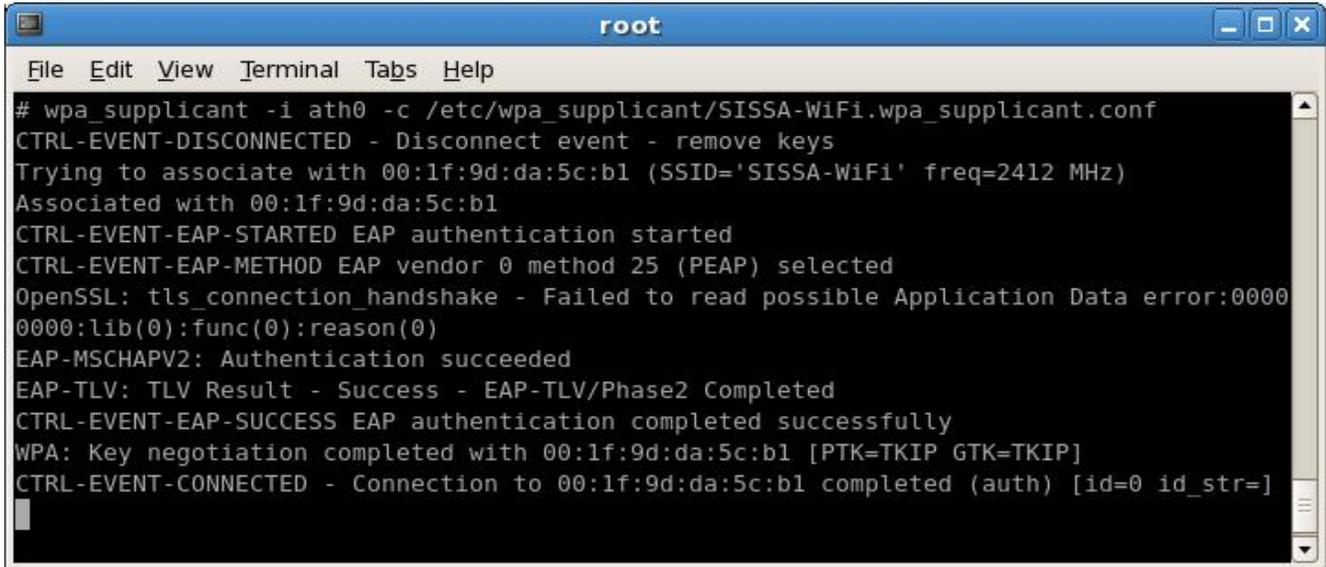
```
ctrl_interface=/var/run/wpa_supplicant

network={
    ssid="SISSA-WiFi"
    key_mgmt=WPA-EAP
    proto=WPA
    eap=PEAP
    phase2="auth=MSCHAPV2"
    identity="yourusername"
    password="yourpassword"
    pairwise=TKIP
    group=TKIP
}
```

Of course, use your own credentials in place of “yourusername” and “yourpassword”

2. Switch on the wireless network interface card with **ifconfig ath0 up**, and start wpa\_supplicant on the foreground with the command:

**wpa\_supplicant -i ath0 -c /etc/wpa\_supplicant/SISSA-WiFi.wpa\_supplicant.conf**

A terminal window titled 'root' with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal displays the output of the wpa\_supplicant command. The output shows the process starting, associating with the wireless interface, and successfully completing EAP authentication and key negotiation. The final line indicates the connection is completed.

```
# wpa_supplicant -i ath0 -c /etc/wpa_supplicant/SISSA-WiFi.wpa_supplicant.conf
CTRL-EVENT-DISCONNECTED - Disconnect event - remove keys
Trying to associate with 00:1f:9d:da:5c:b1 (SSID='SISSA-WiFi' freq=2412 MHz)
Associated with 00:1f:9d:da:5c:b1
CTRL-EVENT-EAP-STARTED EAP authentication started
CTRL-EVENT-EAP-METHOD EAP vendor 0 method 25 (PEAP) selected
OpenSSL: tls_connection_handshake - Failed to read possible Application Data error:0000
0000:lib(0):func(0):reason(0)
EAP-MSCHAPV2: Authentication succeeded
EAP-TLV: TLV Result - Success - EAP-TLV/Phase2 Completed
CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully
WPA: Key negotiation completed with 00:1f:9d:da:5c:b1 [PTK=TKIP GTK=TKIP]
CTRL-EVENT-CONNECTED - Connection to 00:1f:9d:da:5c:b1 completed (auth) [id=0 id_str=]
```

If login succeeded you should see at the end of the command output some lines like:

**CTRL-EVENT-EAP-SUCCESS EAP authentication completed successfully**

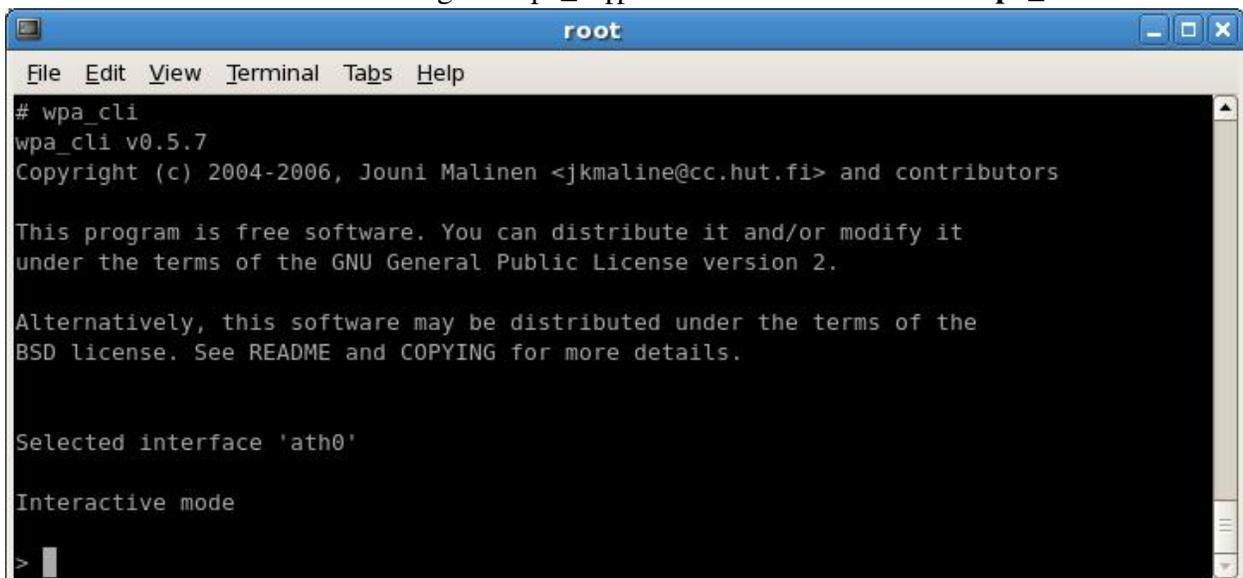
**WPA: Key negotiation completed with ... [PTK=TKIP GTK=TKIP]**

**CTRL-EVENT-CONNECTED - Connection to ... completed (auth) [id=0 id\_str=]**

3. Now that you know wpa\_supplicant works with this configuration, kill the process and launch it in the background as a daemon (notice the trial -B option):

**wpa\_supplicant -i ath0 -c /etc/wpa\_supplicant/SISSA-WiFi.wpa\_supplicant.conf -B**

4. Check the wireless connection using the wpa\_supplicant command line client **wpa\_cli**:

A terminal window titled 'root' with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal displays the output of the wpa\_cli command. The output shows the version, copyright information, license details, and the selected interface 'ath0'. The terminal is in interactive mode.

```
# wpa_cli
wpa_cli v0.5.7
Copyright (c) 2004-2006, Jouni Malinen <jkmaline@cc.hut.fi> and contributors

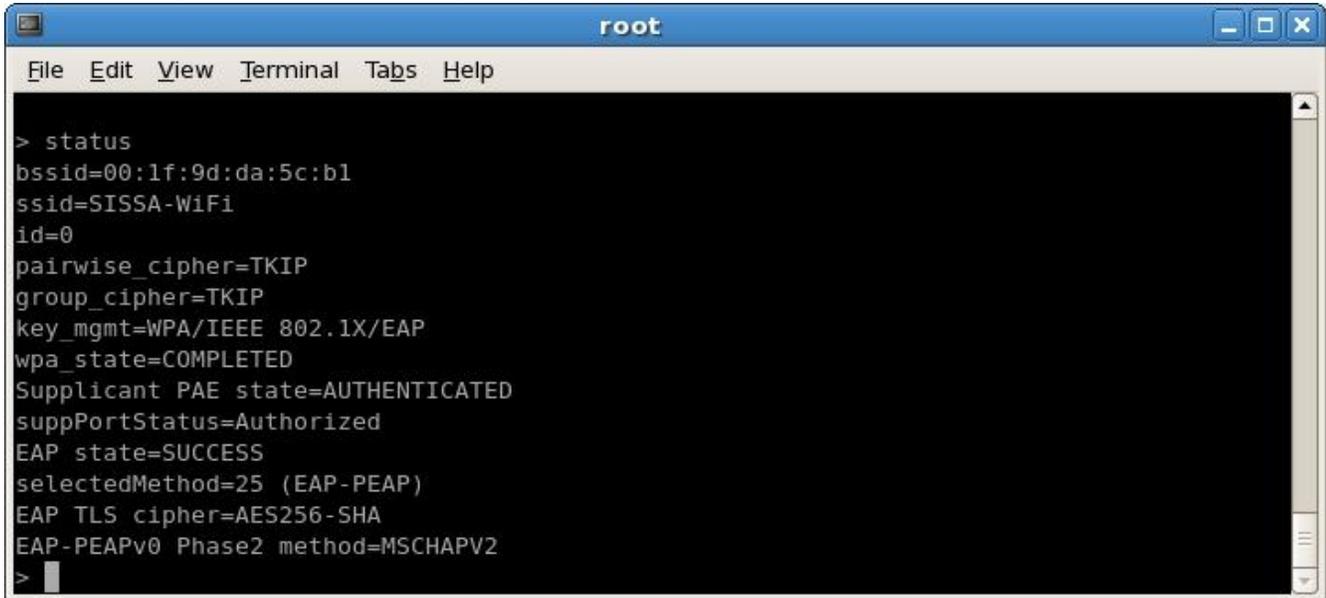
This program is free software. You can distribute it and/or modify it
under the terms of the GNU General Public License version 2.

Alternatively, this software may be distributed under the terms of the
BSD license. See README and COPYING for more details.

Selected interface 'ath0'

Interactive mode
>
```

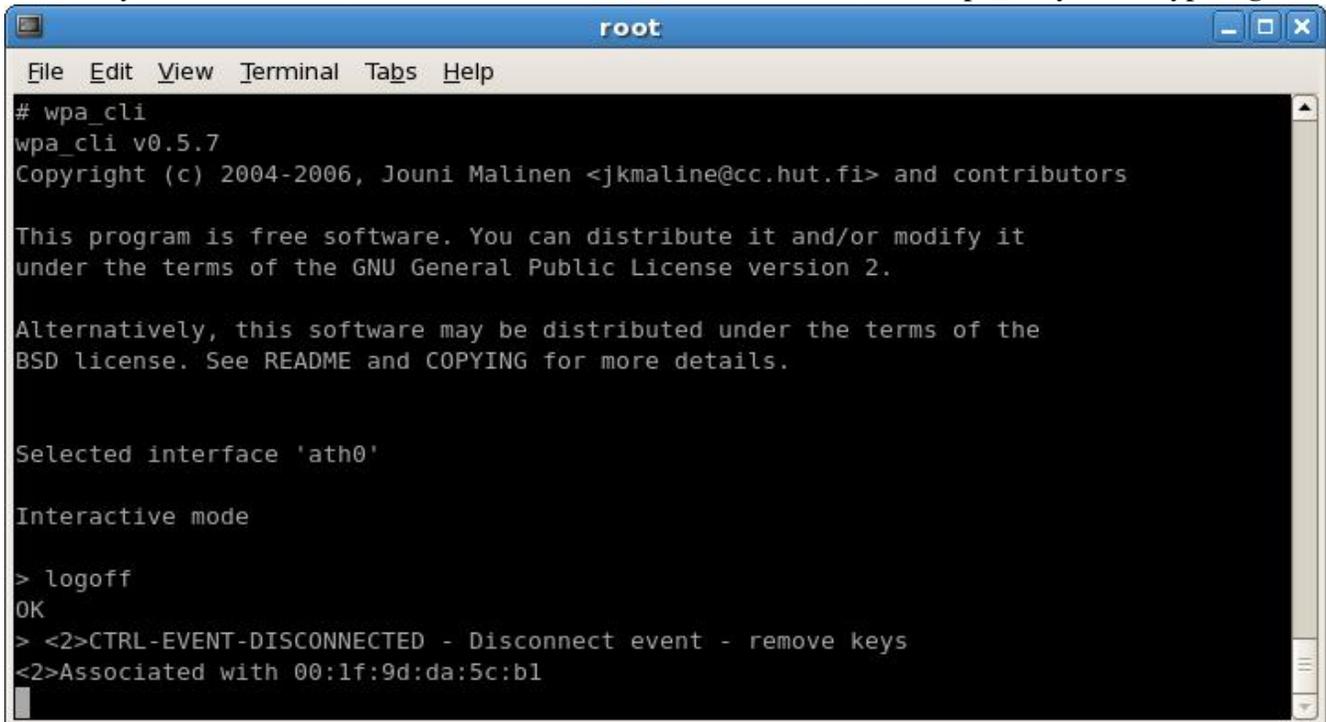
5. from the wpa\_cli command prompt, type **status**. If you're connected you should see something like:

A terminal window titled "root" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the output of the 'status' command in wpa\_cli. The output lists various connection parameters including bssid, ssid, pairwise\_cipher, group\_cipher, key\_mgmt, wpa\_state, Supplicant PAE state, suppPortStatus, EAP state, selectedMethod, EAP TLS cipher, and EAP-PEAPv0 Phase2 method.

```
> status
bssid=00:1f:9d:da:5c:b1
ssid=SISSA-WiFi
id=0
pairwise_cipher=TKIP
group_cipher=TKIP
key_mgmt=WPA/IEEE 802.1X/EAP
wpa_state=COMPLETED
Supplicant PAE state=AUTHENTICATED
suppPortStatus=Authorized
EAP state=SUCCESS
selectedMethod=25 (EAP-PEAP)
EAP TLS cipher=AES256-SHA
EAP-PEAPv0 Phase2 method=MSCHAPV2
>
```

You're in! Configure, if necessary, upper layer TCP/IP protocol DHCP to lease a dynamic IP address.

6. When you have finished, to disconnect from the wireless network, from wpa\_cli, you can type **logoff**

A terminal window titled "root" with a menu bar (File, Edit, View, Terminal, Tabs, Help). The terminal shows the output of the 'logoff' command in wpa\_cli. It displays the wpa\_cli version, copyright information, license details, the selected interface 'ath0', and the 'logoff' command output, including a disconnect event and the removal of keys.

```
# wpa_cli
wpa_cli v0.5.7
Copyright (c) 2004-2006, Jouni Malinen <jkmaline@cc.hut.fi> and contributors

This program is free software. You can distribute it and/or modify it
under the terms of the GNU General Public License version 2.

Alternatively, this software may be distributed under the terms of the
BSD license. See README and COPYING for more details.

Selected interface 'ath0'

Interactive mode

> logoff
OK
> <2>CTRL-EVENT-DISCONNECTED - Disconnect event - remove keys
<2>Associated with 00:1f:9d:da:5c:b1
```

