

MADWIFI-WPA__SUPPLICANT(RSN/WPA-PSK/CCMP) Guide

André Pfeiler <andrep@translever.com>

version 1.0.0, 29. May 2006 - last revised 30. May 2006

madwifi-ng and wpa__supplicant with RSN/WPA-PSK/CCMP authentication in some configurations gives an error like: State: SCANNING -> ASSOCIATING, wpa_driver_madwifi_associate, ioctl[[unknown???]: Invalid argument, Association request to the driver failed. Here is a little description how it works for me with an Atheros Chipset, kernel-2.6.16.18 Debian GNU/Linux testing.

Contents

1	What you need	1
1.1	Getting this document	1
1.2	Download, compile and install the madwifi driver	2
1.3	Download, configure, compile and install wpa__supplicant	2
2	Configure your network device	3
2.1	Bringing up your network device	3
3	Configure wpa__supplicant for RSN/WPA-PSK/CCMP	3
4	Check loaded kernel modules	4
4.1	load kernel modules in needed	4
5	Starting wpa__supplicant	4

1 What you need

- wireless-tools
- kernel needs to be compiled with AES support. 'modprobe aes' or check in the kernel config if option CONFIG_CRYPT_AES=m or y
- madwifi
- wpa__supplicant

1.1 Getting this document

Download this document [PDF](#) , [PS](#) , [Text](#) , [TeX](#) , [sgml](#) version or all as [tar.bz2 package](#) including the configuration files.

1.2 Download, compile and install the madwifi driver

use the latest madwifi-ng subversion checkout

```
# cd /usr/src
# svn checkout http://svn.madwifi.org/trunk madwifi-ng
# cd madwifi-ng
# make
# make install
```

1.3 Download, configure, compile and install wpa_supplicant

use the latest wpa_supplicant version

```
# cd /usr/src
# wget http://hostap.epitest.fi/wpa_supplicant/wpa_supplicant-0.4.9.tar.gz
# tar xvfz wpa_supplicant-0.4.9.tar.gz
# cd wpa_supplicant-0.4.9
# touch .config
```

—————insert these lines into the newly created .config file —————

```
CONFIG_DRIVER_MADWIFI=y
# Change include directories to match with the local setup
CFLAGS += -I/usr/src/madwifi-ng
CONFIG_DRIVER_WEXT=y
CONFIG_IEEE8021X_EAPOL=y
# EAP-MD5 (automatically included if EAP-TTLS is enabled)
CONFIG_EAP_MD5=y
# EAP-MSCHAPv2 (automatically included if EAP-PEAP is enabled)
CONFIG_EAP_MSCHAPV2=y
# EAP-TLS
CONFIG_EAP_TLS=y
# EAP-PEAP
CONFIG_EAP_PEAP=y
# EAP-TTLS
CONFIG_EAP_TTLS=y
# EAP-GTC
CONFIG_EAP_GTC=y
# EAP-OTP
CONFIG_EAP_OTP=y
# LEAP
CONFIG_EAP_LEAP=y
# PKCS#12 (PFX) support (used to read private key and certificate file from
# a file that usually has extension .p12 or .pfx)
CONFIG_PKCS12=y
# Include control interface for external programs, e.g, wpa_cli
CONFIG_CTRL_IFACE=y
```

```
# make
# make install
```

2 Configure your network device

example configuration with static ip:

```
#####
# AtherosG AR5212 802.11abg NIC (rev 01) #
#####
auto ath0
iface ath0 inet static
address 192.168.1.112
netmask 255.255.255.0
network 192.168.1.0
broadcast 192.168.1.255
gateway 192.168.1.1
```

2.1 Bringing up your network device

if done, bring up your network device

```
# /etc/init.d/networking restart
```

or

```
# ifconfig ath up
```

3 Configure wpa_supplicant for RSN/WPA-PSK/CCMP

create this file

```
# touch /etc/wpa_supplicant.conf
```

insert the following lines

```
#####
```

```
ctrl_interface=/var/run/wpa_supplicant
ctrl_interface_group=0
eapol_version=1 # 2 works for me too
ap_scan=1
fast_reauth=1
network={
ssid="hacktheplanet" # this should be your ESSID
key_mgmt=WPA-PSK
proto=RSN
pairwise=CCMP TKIP
```

```
group=CCMP TKIP
scan_ssid=0
#psk="YourPassphrase" # use 'wpa_passphrase yourEssid' and enter your passphrase up to 64 chars
psk=*****
}
```

```
#####
```

4 Check loaded kernel modules

```
# lsmod
Module Size Used by
wlan_ccmp 6528 3
fglrx 376012 0
lp 7840 0
wlan_xauth 1536 0
wlan_tkip 10368 0
wlan_scan_sta 10496 1
ath_pci 74660 0
ath_rate_sample 9600 1 ath_pci
wlan 153820 7 wlan_ccmp,wlan_xauth,wlan_tkip,wlan_scan_sta,ath_pci,ath_rate_sample
ath_hal 189392 3 ath_pci,ath_rate_sample
```

4.1 load kernel modules in needed

if not all modules are loaded, especially wlan_xauth and wlan_tkip, try

```
# modprobe wlan_xauth
# modprobe wlan_tkip
```

5 Starting wpa_supplicant

Now you should be able to start wpa_supplicant and auth to your hotspot.

```
# wpa_supplicant -dd -D madwifi -i ath0 -c /etc/wpa_supplicant.conf
```

you should see something like this:

```
State: GROUP_HANDSHAKE -> COMPLETED
CTRL-EVENT-CONNECTED - Connection to 00:14:a5:8d:34:94 completed (auth)
EAPOL: External notification - portValid=1
EAPOL: External notification - EAP success=1
EAPOL: SUPP_PAE entering state AUTHENTICATING
EAPOL: SUPP_BE entering state SUCCESS
EAP: EAP entering state DISABLED
EAPOL: SUPP_PAE entering state AUTHENTICATED
EAPOL: SUPP_BE entering state IDLE
```

if everything works as expected, replace the -dd by -B to start wpa_supplicant in daemon mode.