Hostapd sebagai Authentikator (AP) dan dukungan Authentikasi & Accounting dengan freeRadius sebagai Server Authentikasi

By

Josua M Sinambela

josh at gadjahmada edu

NOVEMBER 2004

HostAPd

- Merupakan daemon autentikator untuk driver HostAP pada sistem Operasi Linux yang bekerja khusus pada Adapter Wireless PCI/PLX/PCMCIA ber-chipset Prism2/2.5/3.

- Download dari : http://hostap.epitest.fi/releases

- Dukungan HostAPd :

  Full IEEE 802.1x

  Dynamic WEP Keying

  Radius Accounting

  Full IEEE 802.11i/RSN (WPA/WPA2) Dynamic TKIP/CCMP keying

Persiapan Instalasi

- Pastikan Sistem Operasi sudah mendukung hostap driver.

- Agar hostap mendukung WPA/WPA2, upgrade firmware adapter prism ke versi 1.7.x atau yang terbaru

- Gunakan tools hostap-utils (under linux) untuk melakukan upgrade firmware, atau menggunakan program winupdate (under windows)

- Dalam melakukan upgrade firmware, hati hati .. Karena bisa sangat fatal yang menyebabkan adapter tidak berfungsi sama sekali so " Use your own risk :p "

Instalasi

- tar –zxvf hostapd-0.2.4.tar.gz
- cd hostapd-0.2.4
- make
- cp hostapd /usr/sbin
- cp hostapd.conf /etc/
- vi /etc/hostapd.conf

Session Edit View Bookmarks Settings Help

```
##### hostapd configuration file ###########################################
interface=wlan0
logger_syslog=1
logger_syslog_level=0
logger_stdout=1
logger_stdout_level=0
debug=2
dump_file=/tmp/hostapd.dump
daemonize=1

##### IEEE 802.11 related configuration ####################################
ssid=DellC400
macaddr_acl=0
auth_algs=1

##### IEEE 802.1X (and IEEE 802.1aa/D4) related configuration ###############
ieee8021x=1
minimal_eap=0
eap_message=NetworkProtected

wep_key_len_broadcast=13
wep_key_len_unicast=13
wep_rekey_period=300
eapol_key_index_workaround=0

##### RADIUS configuration #################################################
own_ip_addr=172.16.1.1
nas_identifier=localhost
# RADIUS authentication server
auth_server_addr=127.0.0.1
auth_server_port=1812
auth_server_shared_secret=rahasia
# RADIUS accounting server
acct_server_addr=127.0.0.1
acct_server_port=1813
acct_server_shared_secret=rahasia
radius_acct_interim_interval=120
-- INSERT --                                                    36,34           Top
```

Shell

Keterangan

interface=wlan0

Interface wireless yang menggunakan driver hostap.

logger_syslog=1
logger_syslog_level=0
logger_stdout=1
logger_stdout_level=0
debug=2

Tingkatan atau level logging dan mode debugging, baca hostapd.conf default

daemonize=1

Agar hostapd dapat bekerja sebagai daemon.. Atau berjalan secara background

Keterangan

ssid=DellC400

SSID Access Point

macaddr_acl=0

Authentikasi berdasar MAC address (0=Off)

auth_algs=1

Algoritma Authentikasi (0=Open 1=Shared)

Keterangan

ieee8021x=1
Menggunakan authentikasi 802.1x

minimal_eap=0
Untuk testing = 1

eap_message=NetworkProtected
Pesan pada EAP-Request

wep_key_len_broadcast=13
wep_key_len_unicast=13
WEP 104 bit (sering di sebut 128 bit WEP dengan 104 secret bits)

wep_rekey_period=300
Periode pergantian kunci dalam satuan detik (300detik=5menit), sehingga kunci encrypsi setiap 5 menit akan berganti.

own_ip_addr=172.16.1.1

nas_identifier=localhost

Kita set sebagai IP dari wlan0 (NAS-IP-Address), localhost sebagai shortname NAS. Harus sesuai dengan clients.conf pada konfigurasi radius.
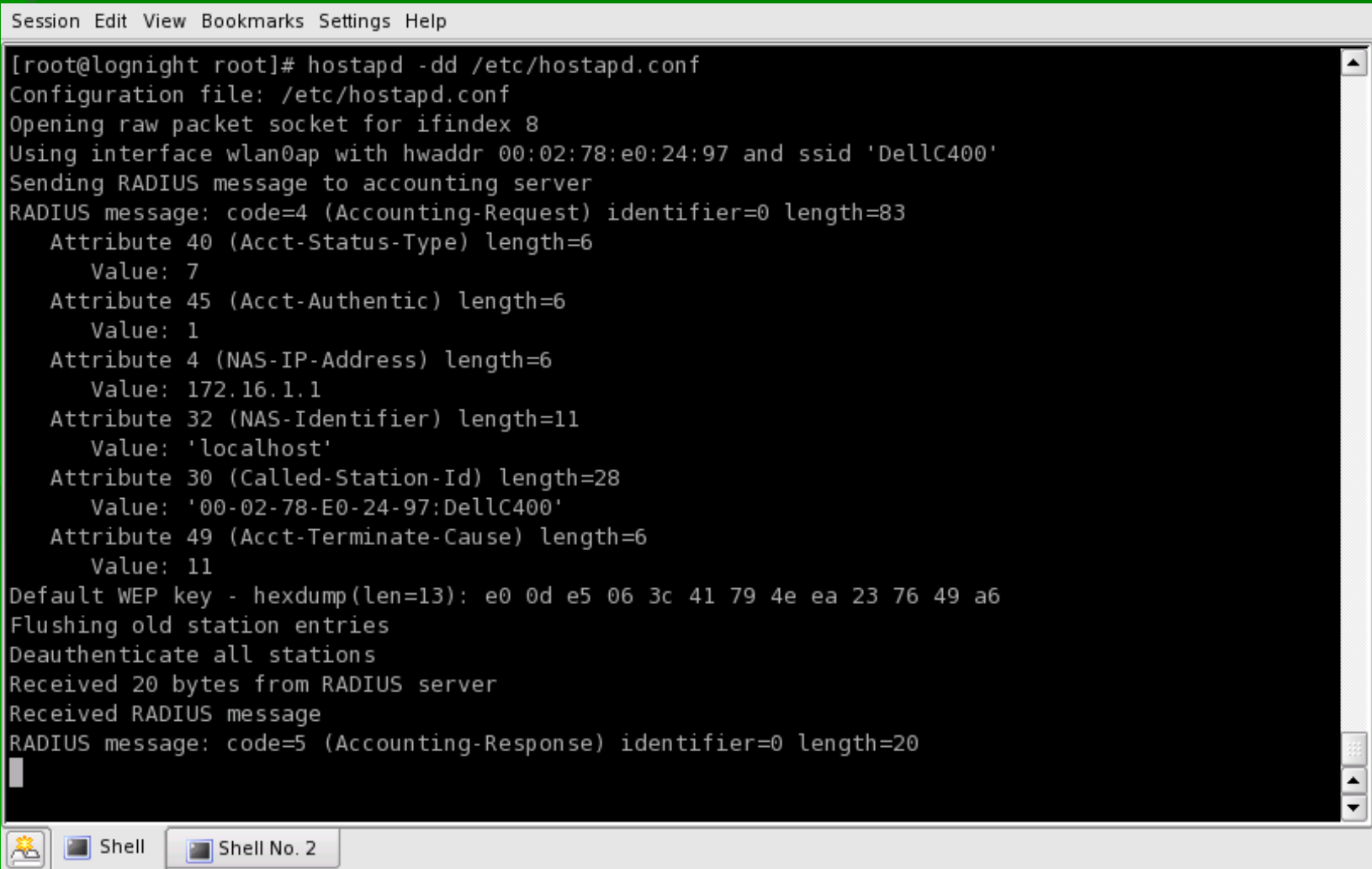
auth_server_addr=127.0.0.1

auth_server_port=1812

auth_server_shared_secret=rahasia

Sesuai dengan konfigurasi clients.conf pada konfigurasi radius

acct_server_addr=127.0.0.1

acct_server_port=1813

acct_server_shared_secret=rahasia
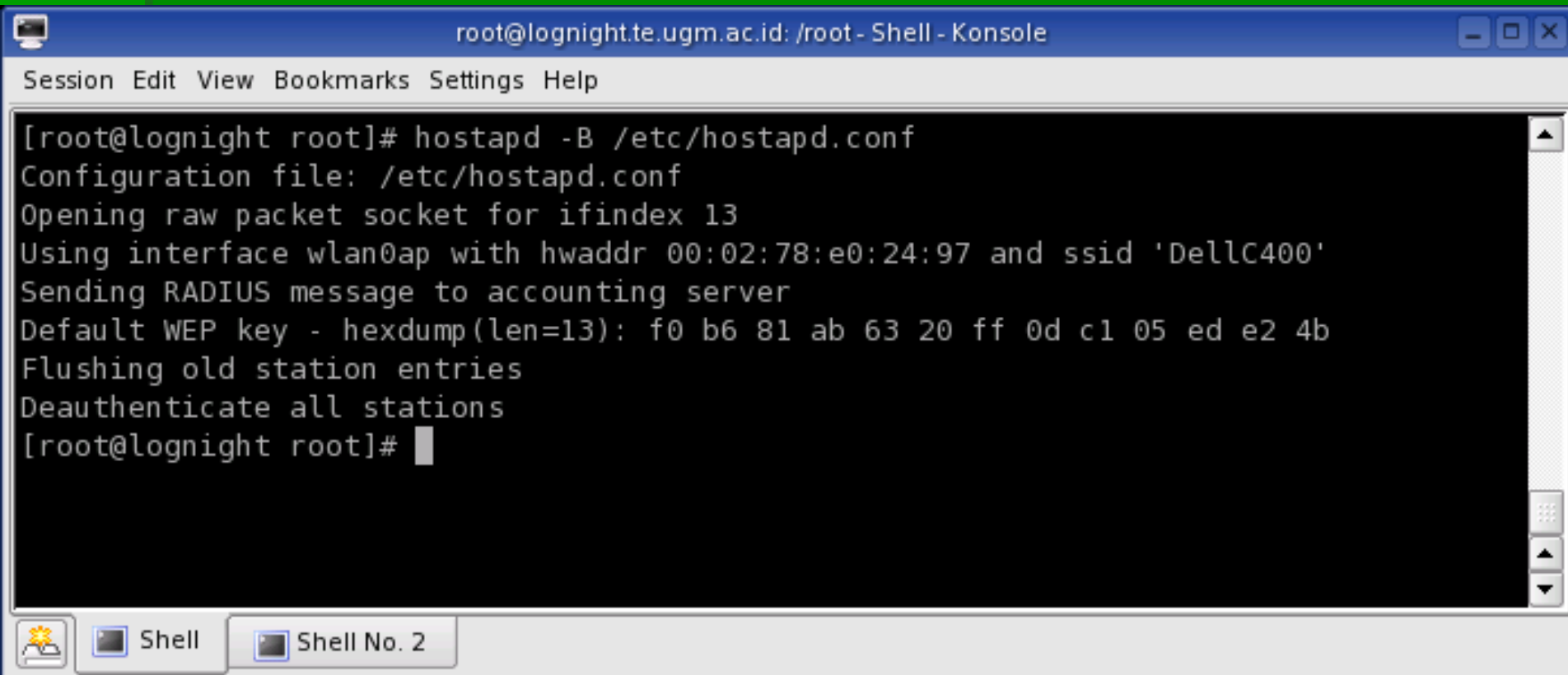
Running hostapd

- Menjalankan hostapd mode debugging

```
Session  Edit  View  Bookmarks  Settings  Help

[root@lognight root]# hostapd -dd /etc/hostapd.conf
Configuration file: /etc/hostapd.conf
Opening raw packet socket for ifindex 8
Using interface wlan0ap with hwaddr 00:02:78:e0:24:97 and ssid 'DellC400'
Sending RADIUS message to accounting server
RADIUS message: code=4 (Accounting-Request) identifier=0 length=83
   Attribute 40 (Acct-Status-Type) length=6
      Value: 7
   Attribute 45 (Acct-Authentic) length=6
      Value: 1
   Attribute 4 (NAS-IP-Address) length=6
      Value: 172.16.1.1
   Attribute 32 (NAS-Identifier) length=11
      Value: 'localhost'
   Attribute 30 (Called-Station-Id) length=28
      Value: '00-02-78-E0-24-97:DellC400'
   Attribute 49 (Acct-Terminate-Cause) length=6
      Value: 11
Default WEP key - hexdump(len=13): e0 0d e5 06 3c 41 79 4e ea 23 76 49 a6
Flushing old station entries
Deauthenticate all stations
Received 20 bytes from RADIUS server
Received RADIUS message
RADIUS message: code=5 (Accounting-Response) identifier=0 length=20
```

Shell   Shell No. 2

Running hostapd

- Menjalankan hostapd mode background

```
[root@lognight root]# hostapd -B /etc/hostapd.conf
Configuration file: /etc/hostapd.conf
Opening raw packet socket for ifindex 13
Using interface wlan0ap with hwaddr 00:02:78:e0:24:97 and ssid 'DellC400'
Sending RADIUS message to accounting server
Default WEP key - hexdump(len=13): f0 b6 81 ab 63 20 ff 0d c1 05 ed e2 4b
Flushing old station entries
Deauthenticate all stations
[root@lognight root]#
```

iwconfig

Session Edit View Bookmarks Settings Help

```
sit0      no wireless extensions.

wifi0     IEEE 802.11b  ESSID:"DellC400"  Nickname:"lognight.te.ugm.ac.id"
          Mode:Master  Frequency:2.422GHz  Access Point: 00:02:78:E0:24:97
          Bit Rate:11Mb/s   Sensitivity=1/9
          Retry min limit:8   RTS thr:off   Fragment thr:off
          Encryption key:22E8-E99B-1B7A-41D6-5101-676B-6E [4]   Security mode:open
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:27   Missed beacon:0

wlan0     IEEE 802.11b  ESSID:"DellC400"  Nickname:"lognight.te.ugm.ac.id"
          Mode:Master  Frequency:2.422GHz  Access Point: 00:02:78:E0:
          Bit Rate:11Mb/s   Sensitivity=1/9
          Retry min limit:8   RTS thr:off   Fragment thr:off
          Encryption key:22E8-E99B-1B7A-41D6-5101-676B-6E [4]
          Power Management:off
          Link Quality:0  Signal level:0  Noise level:0
          Rx invalid nwid:0  Rx invalid crypt:0  Rx invalid frag:0
          Tx excessive retries:0  Invalid misc:27   Missed beacon:0

wlan0ap   IEEE 802.11b  ESSID:"DellC400"  Nickname:"lognight.te.     ac.id"
          Mode:Master  Frequency:2.422GHz  Access Point: 00:0     E0:24:97
          Bit Rate:11Mb/s   Sensitivity=1/9
          Retry min limit:8   RTS thr:off   Fragment thr off
          Encryption key:22E8-E99B-1B7A-41D6-5101-676B-6E [4]   Security mode:open
          Power Management:off

[root@lognight root]#
```
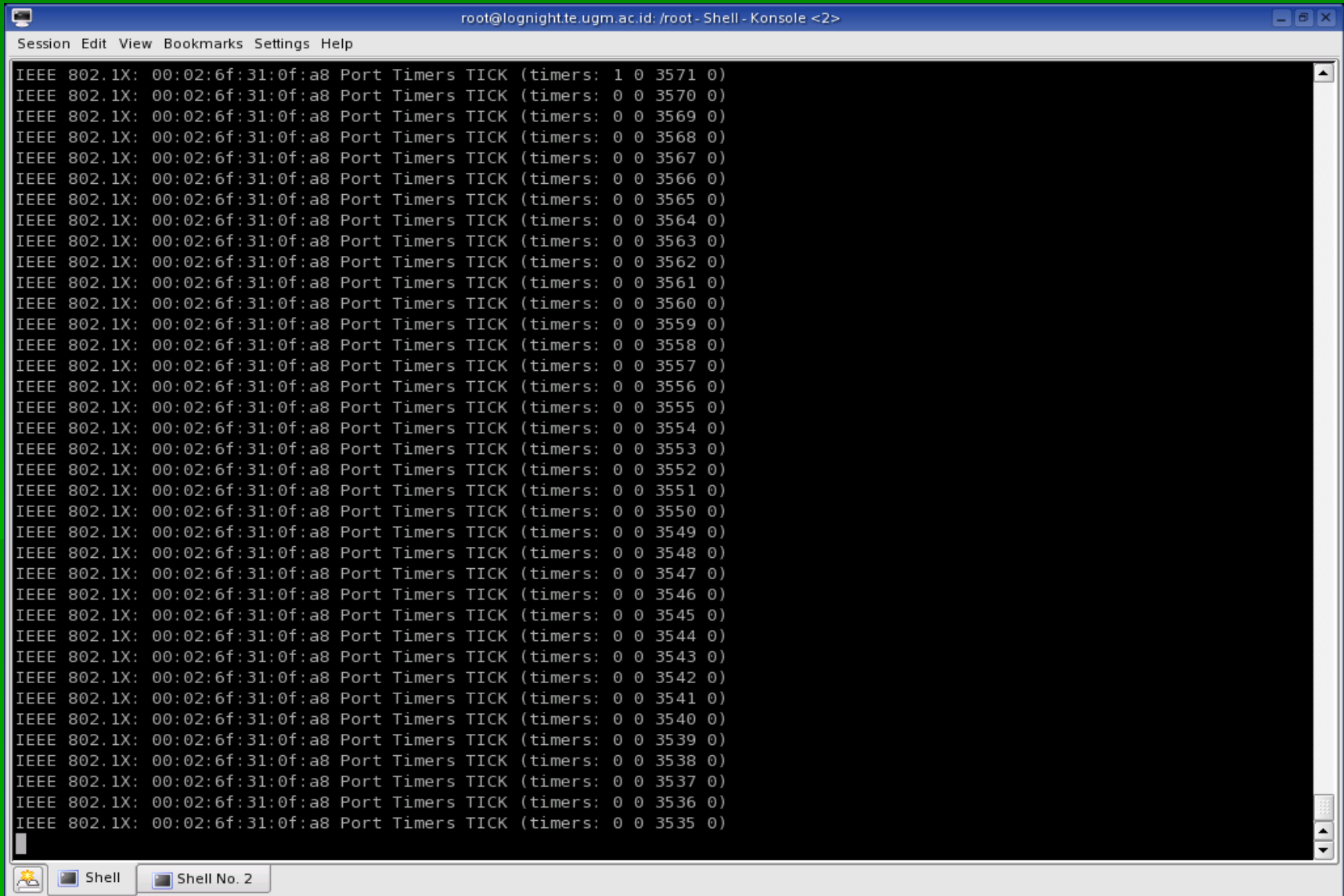
> WEP 104bit Key setiap 5 menit akan berubah

Shell | Shell No. 2

Debugging hostapd using EAP-TLS

```
  Copied RADIUS State Attribute
Sending RADIUS message to authentication server
RADIUS message: code=1 (Access-Request) identifier=6 length=182
   Attribute 1 (User-Name) length=12
      Value: 'nightlogin'
   Attribute 4 (NAS-IP-Address) length=6
      Value: 172.16.1.1
   Attribute 32 (NAS-Identifier) length=11
      Value: 'localhost'
   Attribute 5 (NAS-Port) length=6
      Value: 1
   Attribute 30 (Called-Station-Id) length=28
      Value: '00-02-78-E0-24-97:DellC400'
   Attribute 31 (Calling-Station-Id) length=19
      Value: '00-02-6F-31-0F-A8'
   Attribute 12 (Framed-MTU) length=6
      Value: 1400
   Attribute 61 (NAS-Port-Type) length=6
      Value: 19
   Attribute 77 (Connect-Info) length=24
      Value: 'CONNECT 11Mbps 802.11b'
   Attribute 79 (EAP-Message) length=8
   Attribute 24 (State) length=18
   Attribute 80 (Message-Authenticator) length=18
IEEE 802.1X: 00:02:6f:31:0f:a8 REAUTH_TIMER entering state INITIALIZE
IEEE 802.1X: 00:02:6f:31:0f:a8 REAUTH_TIMER entering state INITIALIZE
Received 133 bytes from RADIUS server
Received RADIUS message
RADIUS message: code=11 (Access-Challenge) identifier=6 length=133
   Attribute 79 (EAP-Message) length=77
   Attribute 80 (Message-Authenticator) length=18
   Attribute 24 (State) length=18
RADIUS packet matching with station 00:02:6f:31:0f:a8
IEEE 802.1X: 00:02:6f:31:0f:a8 BE_AUTH entering state REQUEST
IEEE 802.1X: Sending EAP Packet to 00:02:6f:31:0f:a8 (identifier 7)
IEEE 802.1X: 00:02:6f:31:0f:a8 REAUTH_TIMER entering state INITIALIZE
IEEE 802.1X: 00:02:6f:31:0f:a8 REAUTH_TIMER entering state INITIALIZE
Received 111 bytes management frame
```

Debugging hostapd using EAP-TLS

```
root@lognight.te.ugm.ac.id: /root - Shell - Konsole <2>

Session  Edit  View  Bookmarks  Settings  Help

IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 27 0 3599 22)
IEEE 802.1X: 00:02:6f:31:0f:a8 REAUTH_TIMER entering state INITIALIZE
Received 42 bytes management frame
RX frame - hexdump(len=42): 08 01 02 01 00 02 78 e0 24 97 00 02 6f 31 0f a8 00 02 78 e0 24 97 a0 40 aa aa 03 00 00 00 88 8e
 01 00 00 06 02 08 00 06 0d 00
DATA
IEEE 802.1X: 10 bytes from 00:02:6f:31:0f:a8
   IEEE 802.1X: version=1 type=0 length=6
   EAP: code=2 identifier=8 length=6 (response)
IEEE 802.1X: 00:02:6f:31:0f:a8 BE_AUTH entering state RESPONSE
Encapsulating EAP message into a RADIUS packet
  Copied RADIUS State Attribute
Sending RADIUS message to authentication server
RADIUS message: code=1 (Access-Request) identifier=8 length=182
   Attribute 1 (User-Name) length=12
      Value: 'nightlogin'
   Attribute 4 (NAS-IP-Address) length=6
      Value: 172.16.1.1
   Attribute 32 (NAS-Identifier) length=11
      Value: 'localhost'
   Attribute 5 (NAS-Port) length=6
      Value: 1
   Attribute 30 (Called-Station-Id) length=28
      Value: '00-02-78-E0-24-97:DellC400'
   Attribute 31 (Calling-Station-Id) length=19
      Value: '00-02-6F-31-0F-A8'
   Attribute 12 (Framed-MTU) length=6
      Value: 1400
   Attribute 61 (NAS-Port-Type) length=6
      Value: 19
   Attribute 77 (Connect-Info) length=24
      Value: 'CONNECT 11Mbps 802.11b'
   Attribute 79 (EAP-Message) length=8
   Attribute 24 (State) length=18
   Attribute 80 (Message-Authenticator) length=18
IEEE 802.1X: 00:02:6f:31:0f:a8 REAUTH_TIMER entering state INITIALIZE
IEEE 802.1X: 00:02:6f:31:0f:a8 REAUTH_TIMER entering state INITIALIZE
Received 172 bytes from RADIUS server

 Shell      Shell No. 2
```

Timer debugging hostapd


```
root@lognight.te.ugm.ac.id: /root - Shell - Konsole <2>

Session  Edit  View  Bookmarks  Settings  Help

IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 1 0 3571 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3570 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3569 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3568 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3567 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3566 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3565 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3564 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3563 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3562 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3561 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3560 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3559 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3558 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3557 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3556 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3555 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3554 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3553 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3552 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3551 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3550 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3549 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3548 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3547 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3546 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3545 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3544 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3543 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3542 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3541 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3540 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3539 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3538 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3537 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3536 0)
IEEE 802.1X: 00:02:6f:31:0f:a8 Port Timers TICK (timers: 0 0 3535 0)

Shell      Shell No. 2
```