Wireless LAN Security

- Setup & Optimizing Wireless Client in Linux
- Hacking and Cracking Wireless LAN
- Setup Host Based AP (hostap) in Linux & freeBSD
- Securing & Managing Wireless LAN : Implementing 802.1x EAP-TLS EAP-PEAP-MSCHAPv2 , FreeRADIUS + dialupadmin + MySQL with Windows XP SP2 & Linux Client using wpa_supplicant (DEMO ☺)
- Make Deep Security (99%) with WPA2

  Wifi Protected Access = 802.1x + (TKIP or

How to Setup & Optimizing Wireless Client in Linux

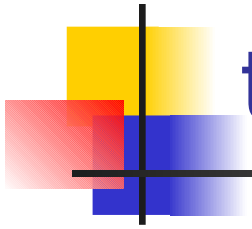
- Wireless Client Adapter Recommended for Linux User

http://www.seattlewireless.net/index.cgi/HardwareComparison

http://www.seattlewireless.net/index.cgi/Client_5fAdapters_5f802_5f11

- Recommended to use latest kernel
- Tips & Tricks using wlan-ng driver
- Tips & Tricks using Orinoco compatible
- Tips & Tricks using hostap

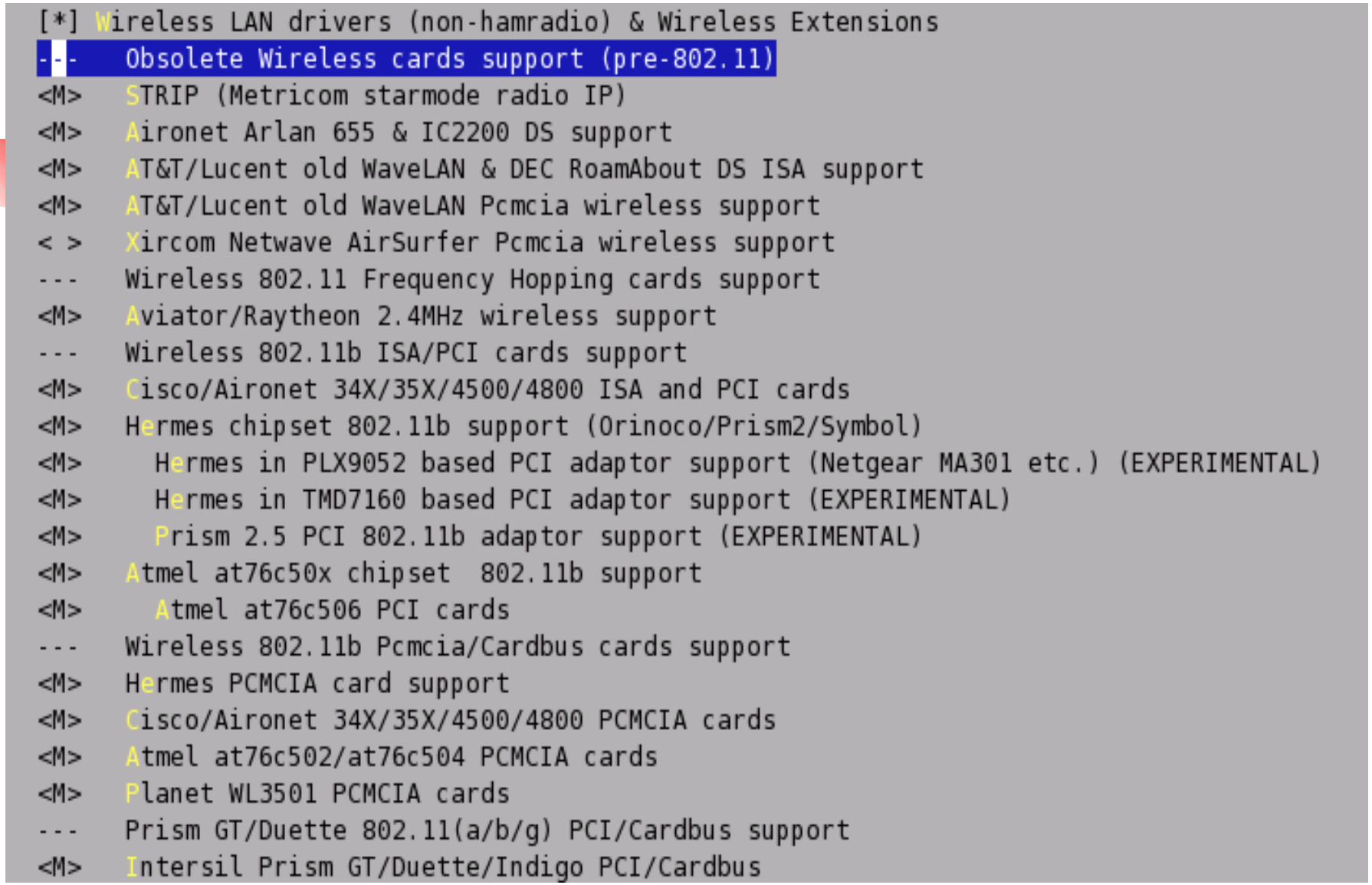
Use latest kernel and configure to support your hardware



- Get a latest Kernel & unpack

  Get from http://www.kernel.org
- Configure your kernel source to support wireless lan drivers (non-harmradio) & wireless extensions and your adapter

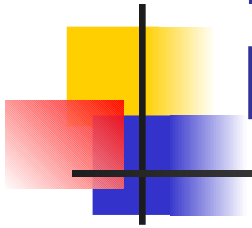
  (pcmcia/PCI/USB).
- make menuconfig (I’m love in it :p)


[*] Wireless LAN drivers (non-hamradio) & Wireless Extensions
-*-   Obsolete Wireless cards support (pre-802.11)
<M>   STRIP (Metricom starmode radio IP)
<M>   Aironet Arlan 655 & IC2200 DS support
<M>   AT&T/Lucent old WaveLAN & DEC RoamAbout DS ISA support
<M>   AT&T/Lucent old WaveLAN Pcmcia wireless support
< >   Xircom Netwave AirSurfer Pcmcia wireless support
---   Wireless 802.11 Frequency Hopping cards support
<M>   Aviator/Raytheon 2.4MHz wireless support
---   Wireless 802.11b ISA/PCI cards support
<M>   Cisco/Aironet 34X/35X/4500/4800 ISA and PCI cards
<M>   Hermes chipset 802.11b support (Orinoco/Prism2/Symbol)
<M>   Hermes in PLX9052 based PCI adaptor support (Netgear MA301 etc.) (EXPERIMENTAL)
<M>   Hermes in TMD7160 based PCI adaptor support (EXPERIMENTAL)
<M>   Prism 2.5 PCI 802.11b adaptor support (EXPERIMENTAL)
<M>   Atmel at76c50x chipset 802.11b support
<M>   Atmel at76c506 PCI cards
---   Wireless 802.11b Pcmcia/Cardbus cards support
<M>   Hermes PCMCIA card support
<M>   Cisco/Aironet 34X/35X/4500/4800 PCMCIA cards
<M>   Atmel at76c502/at76c504 PCMCIA cards
<M>   Planet WL3501 PCMCIA cards
---   Prism GT/Duette 802.11(a/b/g) PCI/Cardbus support
<M>   Intersil Prism GT/Duette/Indigo PCI/Cardbus

For PCMCIA cards

```
<*> PCMCIA/CardBus support
[*]   Enable PCMCIA debugging
<M>   CardBus yenta-compatible bridge support
<*>   Cirrus PD6729 compatible bridge support
<*>   i82092 compatible bridge support
<*>   i82365 compatible bridge support
<*>   Databook TCIC host bridge support
```

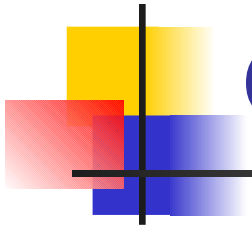
Make fun with your kernel



- make
- make modules_install
- copy yourbzimage and System Map to /boot
- Configure your boot loader ;

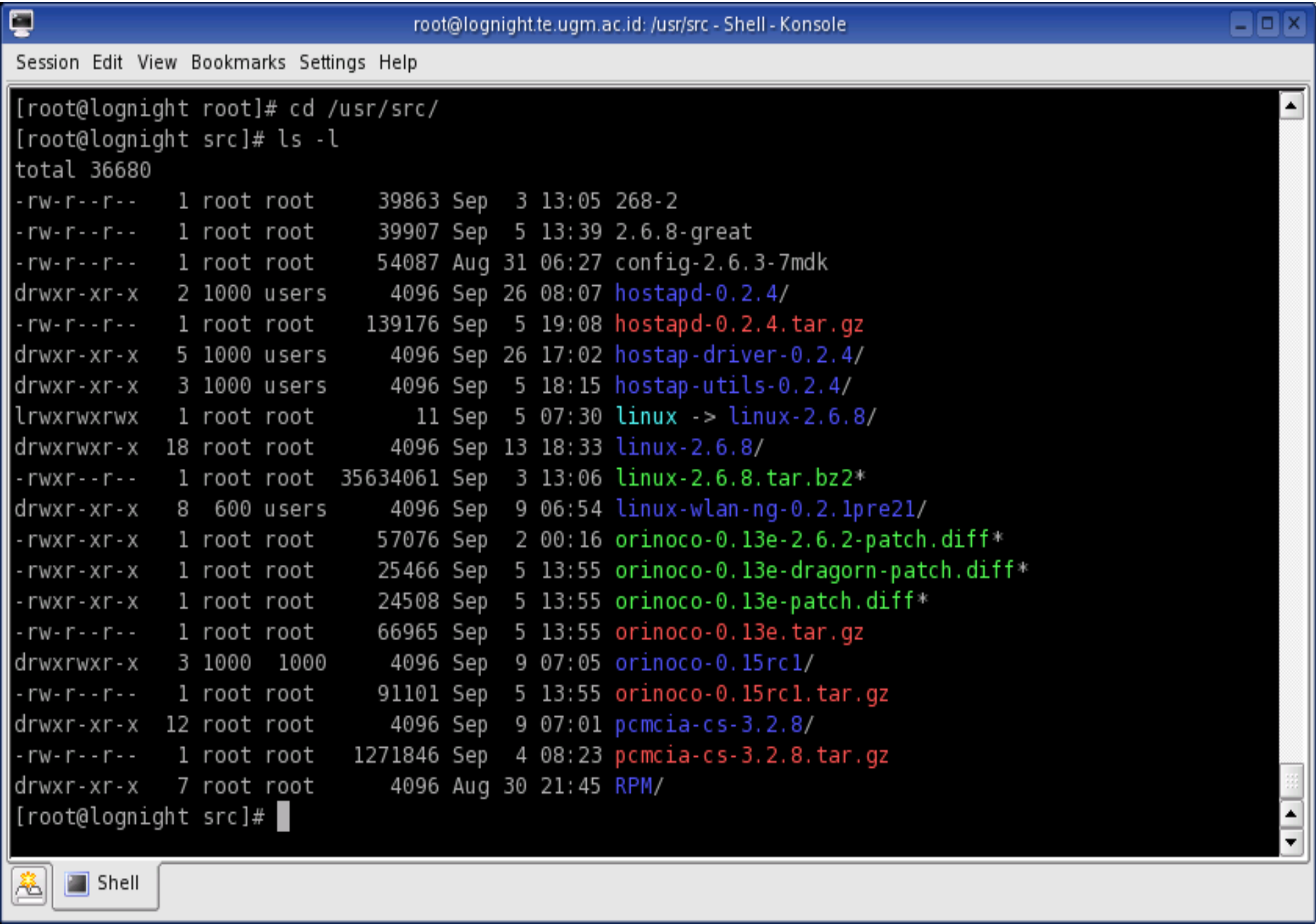
For LILOman ☺ , don’t forget to type lilo –v and reboot your computer to use your new kernel

Tips & Trick using wlan-ng driver

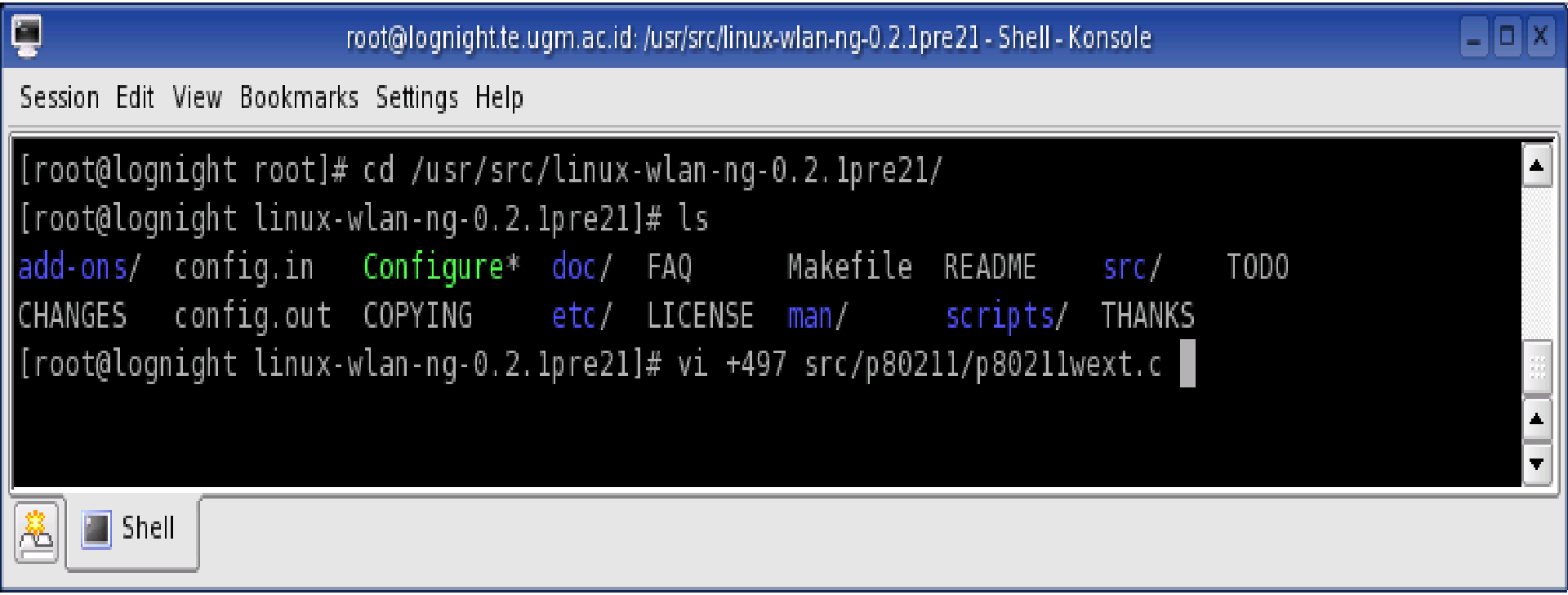


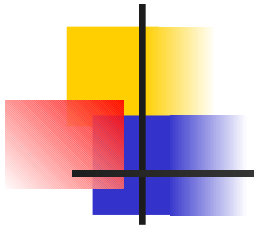
- Works only for prism2/2.5/3 cards
- Get latest wlan-ng package from the net

  http://www.linux-wlan.com/download.htr
- Unpack, hack the source , configure to your kernel, compile and install


root@lognight.te.ugm.ac.id: /usr/src - Shell - Konsole
Session Edit View Bookmarks Settings Help
[root@lognight root]# cd /usr/src/
[root@lognight src]# ls -l
total 36680
-rw-r--r-- 1 root root   39863 Sep 3 13:05 268-2
-rw-r--r-- 1 root root   39907 Sep 5 13:39 2.6.8-great
-rw-r--r-- 1 root root   54087 Aug 31 06:27 config-2.6.3-7mdk
drwxr-xr-x 2 1000 users   4096 Sep 26 08:07 hostapd-0.2.4/
-rw-r--r-- 1 root root   139176 Sep 5 19:08 hostapd-0.2.4.tar.gz
drwxr-xr-x 5 1000 users   4096 Sep 26 17:02 hostap-driver-0.2.4/
drwxr-xr-x 3 1000 users   4096 Sep 5 18:15 hostap-utils-0.2.4/
lrwxrwxrwx 1 root root   11 Sep 5 07:30 linux -> linux-2.6.8/
drwxrwxr-x 18 root root   4096 Sep 13 18:33 linux-2.6.8/
-rwxr--r-- 1 root root 35634061 Sep 3 13:06 linux-2.6.8.tar.bz2*
drwxr-xr-x 8 600 users   4096 Sep 9 06:54 linux-wlan-ng-0.2.1pre21/
-rwxr-xr-x 1 root root   57076 Sep 2 00:16 orinoco-0.13e-2.6.2-patch.diff*
-rwxr-xr-x 1 root root   25466 Sep 5 13:55 orinoco-0.13e-dragorn-patch.diff*
-rwxr-xr-x 1 root root   24508 Sep 5 13:55 orinoco-0.13e-patch.diff*
-rw-r--r-- 1 root root   66965 Sep 5 13:55 orinoco-0.13e.tar.gz
drwxrwxr-x 3 1000 1000   4096 Sep 9 07:05 orinoco-0.15rc1/
-rw-r--r-- 1 root root   91101 Sep 5 13:55 orinoco-0.15rc1.tar.gz
drwxr-xr-x 12 root root   4096 Sep 9 07:01 pcmcia-cs-3.2.8/
-rw-r--r-- 1 root root   1271846 Sep 4 08:23 pcmcia-cs-3.2.8.tar.gz
drwxr-xr-x 7 root root   4096 Aug 30 21:45 RPM/
[root@lognight src]#
Shell

Find words “sens” (sensitivity) in source code using mc or grep tools ;



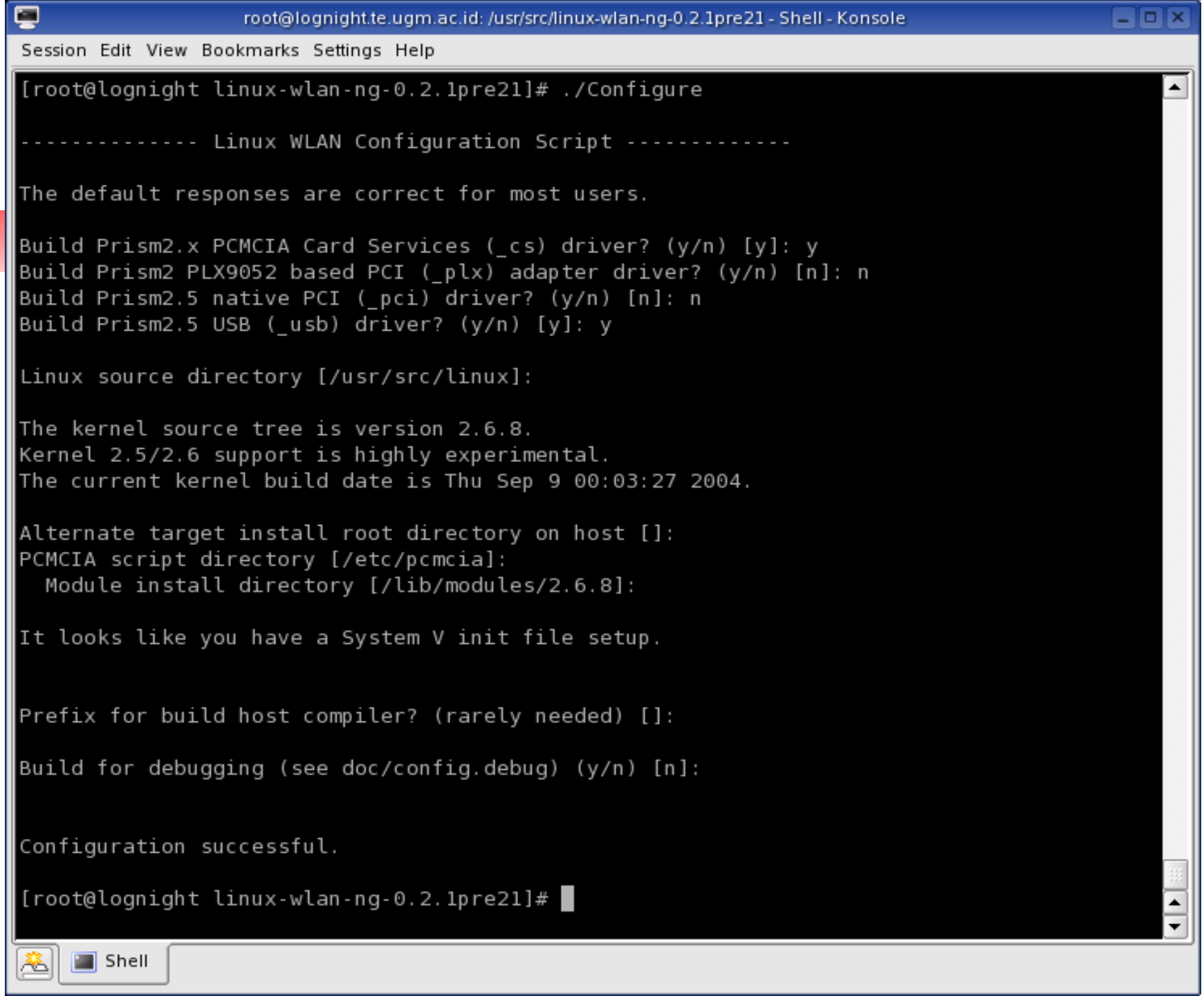


root@lognight.te.ugm.ac.id: /usr/src/linux-wlan-ng-0.2.1pre21 - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
        range->max_qual.level = 154;
        range->max_qual.noise = 154;
        range->sensitivity = 9;// dapat diubah untuk meningkatkan sensitivitas 3 >> 9
        // XXX these need to be nsd-specific!

        range->min_rts = 0;
-- INSERT --                                                    497,79-86     32%
```

Shell


root@lognight.te.ugm.ac.id: /usr/src/linux-wlan-ng-0.2.1pre21 - Shell - Konsole
Session Edit View Bookmarks Settings Help
[root@lognight linux-wlan-ng-0.2.1pre21]# ./Configure
-------------- Linux WLAN Configuration Script ------------
The default responses are correct for most users.
Build Prism2.x PCMCIA Card Services (_cs) driver? (y/n) [y]: y
Build Prism2 PLX9052 based PCI (_plx) adapter driver? (y/n) [n]: n
Build Prism2.5 native PCI (_pci) driver? (y/n) [n]: n
Build Prism2.5 USB (_usb) driver? (y/n) [y]: y
Linux source directory [/usr/src/linux]:
The kernel source tree is version 2.6.8.
Kernel 2.5/2.6 support is highly experimental.
The current kernel build date is Thu Sep 9 00:03:27 2004.
Alternate target install root directory on host []:
PCMCIA script directory [/etc/pcmcia]:
Module install directory [/lib/modules/2.6.8]:
It looks like you have a System V init file setup.
Prefix for build host compiler? (rarely needed) []:
Build for debugging (see doc/config.debug) (y/n) [n]:
Configuration successful.
[root@lognight linux-wlan-ng-0.2.1pre21]#
Shell

Compile and install wlan-ng module

- [root@lognight root]# cd /usr/src/linux-wlan-ng-0.2.1pre21/
- [root@lognight linux-wlan-ng-0.2.1pre21]# make all; make install;

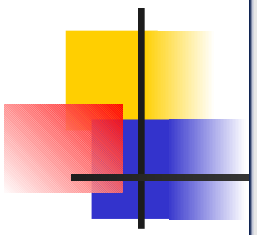
For Pcmcia Card Adapter, install pcmcia-cs first.

The latest package is recommended.

Get from http://pcmcia-cs.sourceforge.net/

I use pcmcia-cs-3.2.8.

- [root@lognight src]# tar -zxvf pcmcia-cs-3.2.8.tar.gz
- [root@lognight src]# cd pcmcia-cs-3.2.8
- [root@lognight pcmcia-cs-3.2.8]#

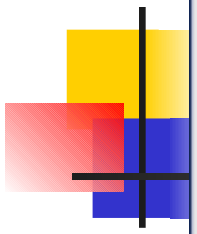


root@lognight.te.ugm.ac.id: /usr/src/pcmcia-cs-3.2.8 - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
[root@lognight pcmcia-cs-3.2.8]# ./Configure

    -------- Linux PCMCIA Configuration Script --------

The default responses for each question are correct for most users.
Consult the PCMCIA-HOWTO for additional info about each option.

Linux kernel source directory [/usr/src/linux]:

The kernel source tree is version 2.6.8.
The current kernel build date is Thu Sep 9 00:03:27 2004.

Build 'trusting' versions of card utilities (y/n) [n]: y
Include 32-bit (CardBus) card support (y/n) [y]:
Include PnP BIOS resource checking (y/n) [n]:

The PCMCIA drivers need to be compiled to match the kernel they
will be used with, or some or all of the modules may fail to load.
If you are not sure what to do, please consult the PCMCIA-HOWTO.

How would you like to set kernel-specific options?
    1 - Read from the currently running kernel
    2 - Read from the Linux source tree
Enter option (1-2) [3]: 2

Module install directory [/lib/modules/2.6.8]:

Kernel configuration options:
    Kernel-tree PCMCIA support is enabled.
    Symmetric multiprocessing support is disabled.
    Preemptive kernel support is enabled.
    Realtime Hardware Abstraction Layer is disabled.
    High memory support is disabled.
```

Shell



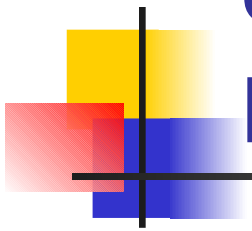
root@lognight.te.ugm.ac.id: /usr/src/pcmcia-cs-3.2.8 - Shell - Konsole

Session Edit View Bookmarks Settings Help

```
Module install directory [/lib/modules/2.6.8]:

Kernel configuration options:
    Kernel-tree PCMCIA support is enabled.
    Symmetric multiprocessing support is disabled.
    Preemptive kernel support is enabled.
    Realtime Hardware Abstraction Layer is disabled.
    High memory support is disabled.
    PCI BIOS support is enabled.
    Power management (APM) support is enabled.
    SCSI support is enabled.
    IEEE 1394 (FireWire) support is disabled.
    Networking support is enabled.
     Radio network interface support is enabled.
     Token Ring device support is disabled.
     Fast switching is disabled.
     Frame Diverter is disabled.
    Module version checking is enabled.
    Kernel debugging support is disabled.
    /proc filesystem support is enabled.
    PAE support is disabled.


Configuration successful.

** Your kernel is configured with PCMCIA driver support.  Therefore,
** 'make all' will compile the PCMCIA utilities but not the drivers.
** See README-2.4 if this is not what you intended!

[root@lognight pcmcia-cs-3.2.8]#
```

Shell

Compiling and installing, setting configuration pcmcia-cs and starting pcmcia daemon



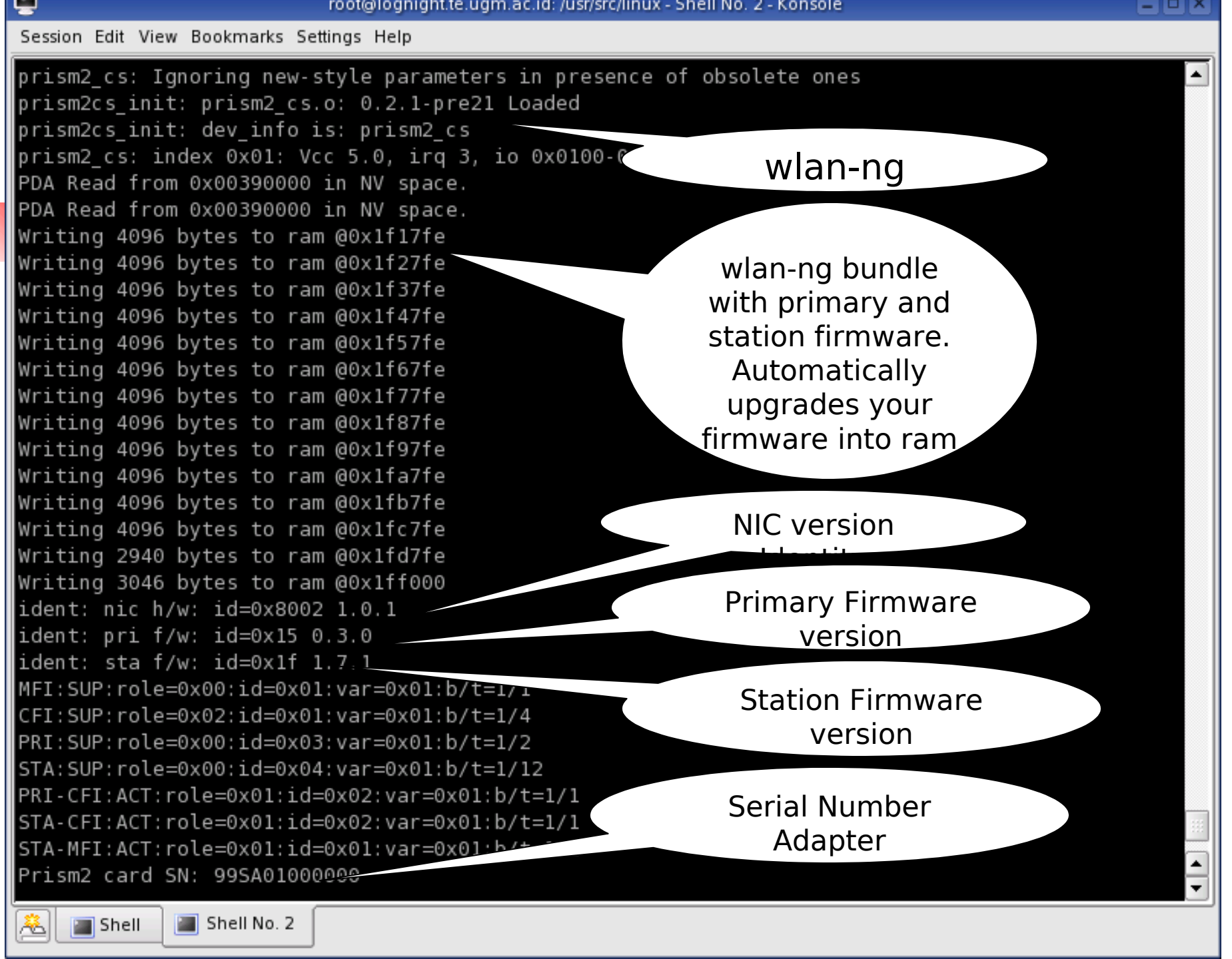
- make all
- make install

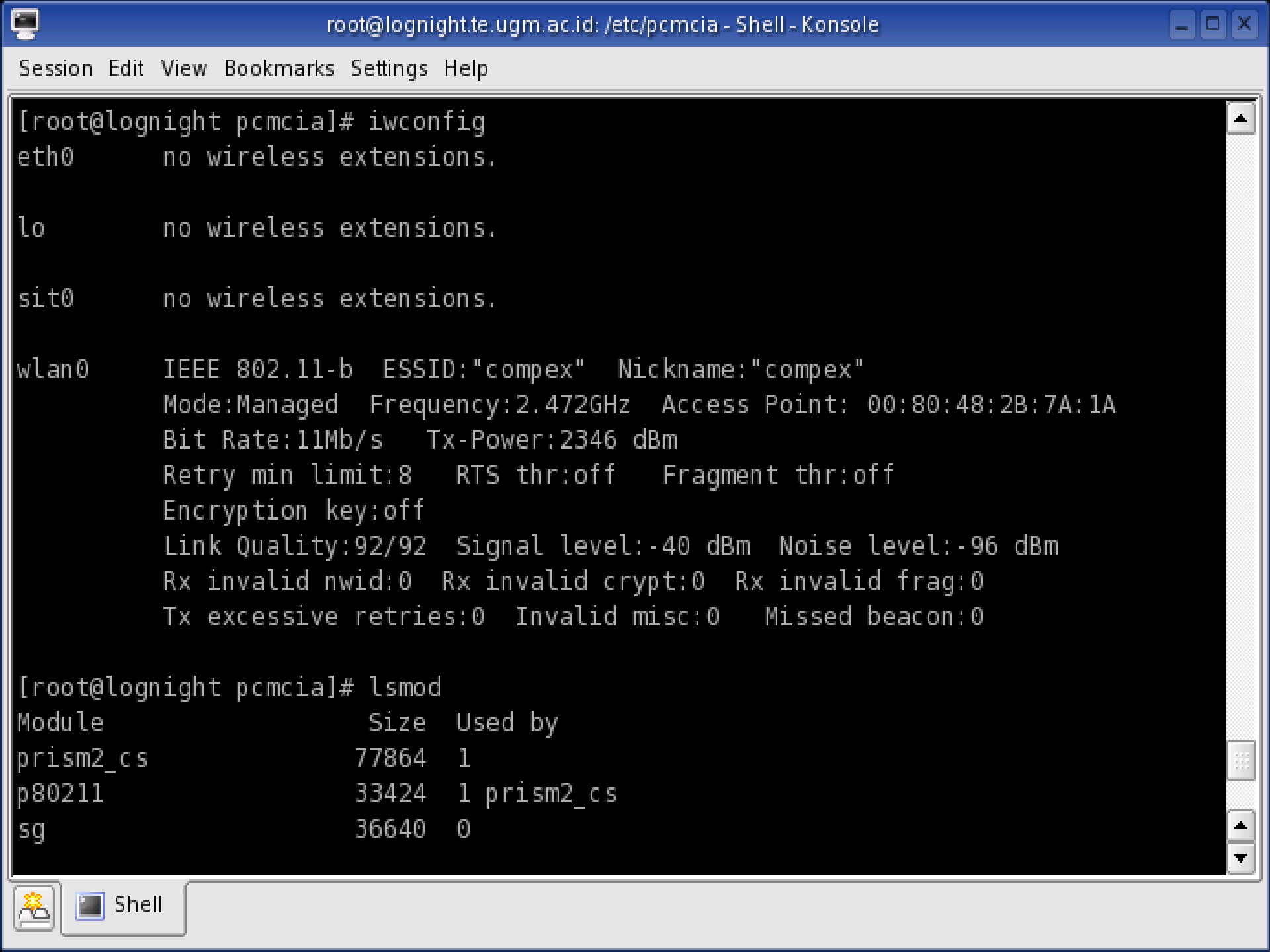
Now go to /etc/pcmcia and edit *.conf and *.opts

- /etc/init.d/pcmcia start

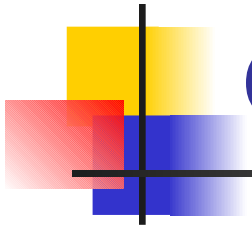
Starting PCMCIA services: cardmgr[23313]: watching 1 socket

done.


root@loghight.te.ugm.ac.id: /usr/src/linux - Shell No. 2 - Konsole
Session Edit View Bookmarks Settings Help
prism2_cs: Ignoring new-style parameters in presence of obsolete ones
prism2cs_init: prism2_cs.o: 0.2.1-pre21 Loaded
prism2cs_init: dev_info is: prism2_cs
prism2_cs: index 0x01: Vcc 5.0, irq 3, io 0x0100-0
PDA Read from 0x00390000 in NV space.
PDA Read from 0x00390000 in NV space.
Writing 4096 bytes to ram @0x1f17fe
Writing 4096 bytes to ram @0x1f27fe
Writing 4096 bytes to ram @0x1f37fe
Writing 4096 bytes to ram @0x1f47fe
Writing 4096 bytes to ram @0x1f57fe
Writing 4096 bytes to ram @0x1f67fe
Writing 4096 bytes to ram @0x1f77fe
Writing 4096 bytes to ram @0x1f87fe
Writing 4096 bytes to ram @0x1f97fe
Writing 4096 bytes to ram @0x1fa7fe
Writing 4096 bytes to ram @0x1fb7fe
Writing 4096 bytes to ram @0x1fc7fe
Writing 2940 bytes to ram @0x1fd7fe
Writing 3046 bytes to ram @0x1ff000
ident: nic h/w: id=0x8002 1.0.1
ident: pri f/w: id=0x15 0.3.0
ident: sta f/w: id=0x1f 1.7.1
MFI:SUP:role=0x00:id=0x01:var=0x01:b/t=1/1
CFI:SUP:role=0x02:id=0x01:var=0x01:b/t=1/4
PRI:SUP:role=0x00:id=0x03:var=0x01:b/t=1/2
STA:SUP:role=0x00:id=0x04:var=0x01:b/t=1/12
PRI-CFI:ACT:role=0x01:id=0x02:var=0x01:b/t=1/1
STA-CFI:ACT:role=0x01:id=0x02:var=0x01:b/t=1/1
STA-MFI:ACT:role=0x01:id=0x01:var=0x01:b/t=
Prism2 card SN: 99SA01000000
wlan-ng
wlan-ng bundle with primary and station firmware. Automatically upgrades your firmware into ram
NIC version
Primary Firmware version
Station Firmware version
Serial Number Adapter
Shell
Shell No. 2


root@lognight.te.ugm.ac.id: /etc/pcmcia - Shell - Konsole
Session Edit View Bookmarks Settings Help
[root@lognight pcmcia]# iwconfig
eth0 no wireless extensions.
lo no wireless extensions.
sit0 no wireless extensions.
wlan0 IEEE 802.11-b ESSID:"compex" Nickname:"compex"
Mode:Managed Frequency:2.472GHz Access Point: 00:80:48:2B:7A:1A
Bit Rate:11Mb/s Tx-Power:2346 dBm
Retry min limit:8 RTS thr:off Fragment thr:off
Encryption key:off
Link Quality:92/92 Signal level:-40 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
[root@lognight pcmcia]# lsmod
Module Size Used by
prism2_cs 77864 1
p80211 33424 1 prism2_cs
sg 36640 0
Shell

Tips & Trick using Orinoco driver



- Only for Orinoco compatible cards (Lucent/Cabletron, Hermes, Orinoco, Prism2)
- Get latest orinoco package from net

http://savannah.nongnu.org/cvs/?group=orinoco

http://ozlabs.org/people/dgibson/dldwd/

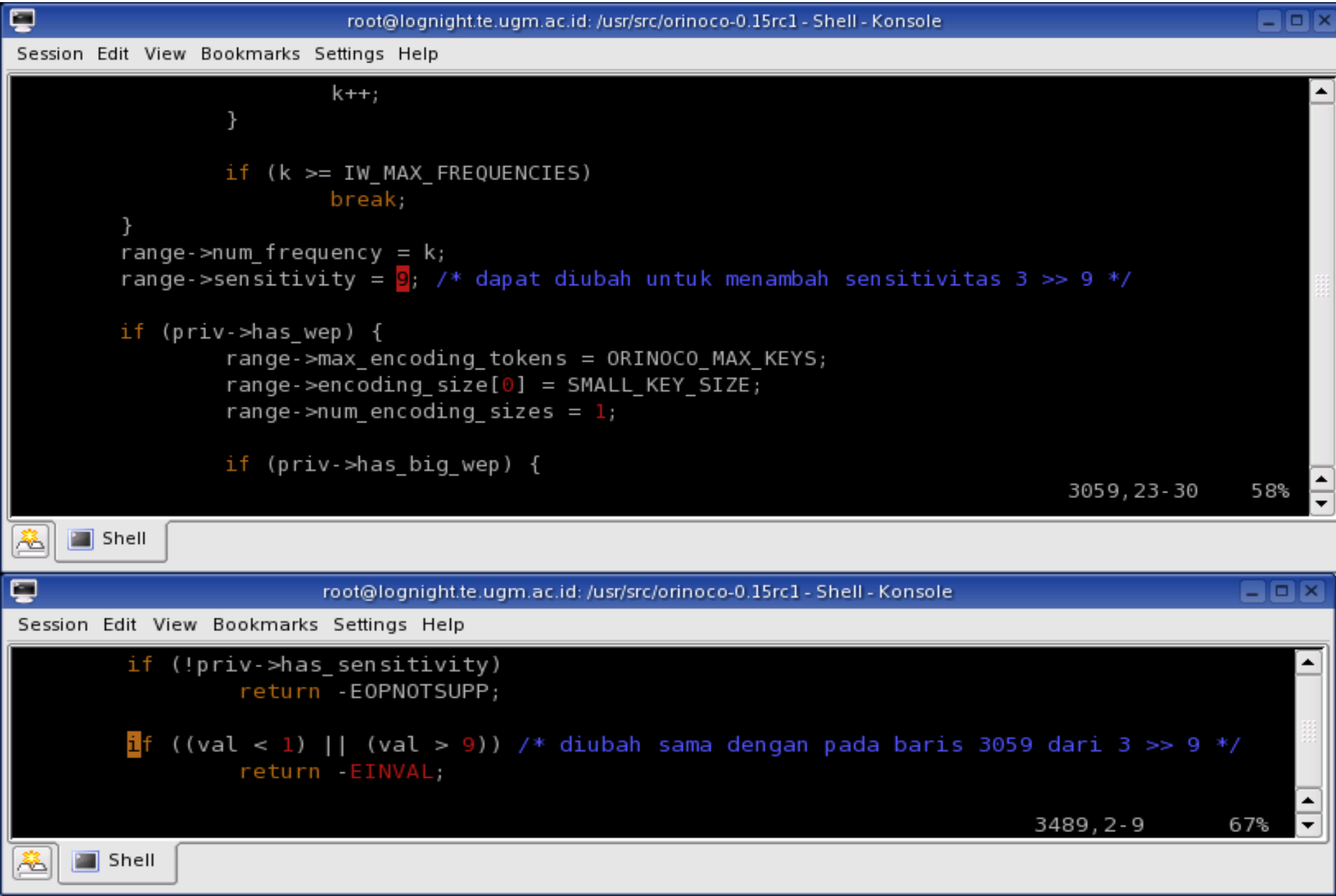
http://airsnort.shmoo.com/

- Unpack, compile and install to your kernel

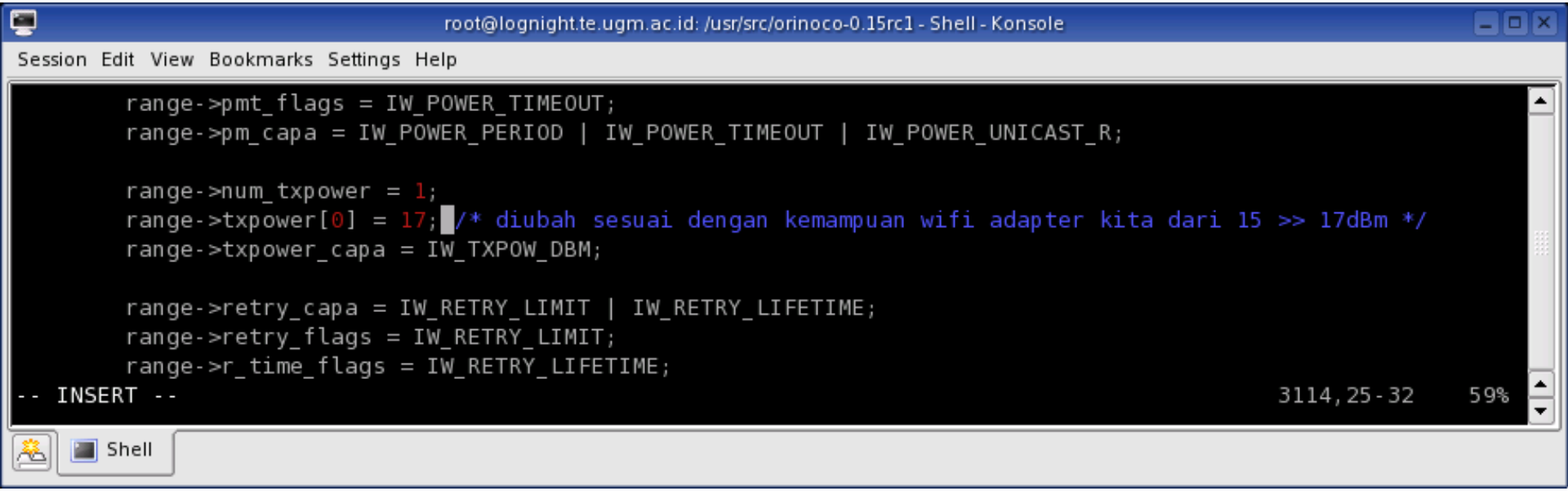
[root@lognight root]# cd /usr/src/orinoco-0.15rc1

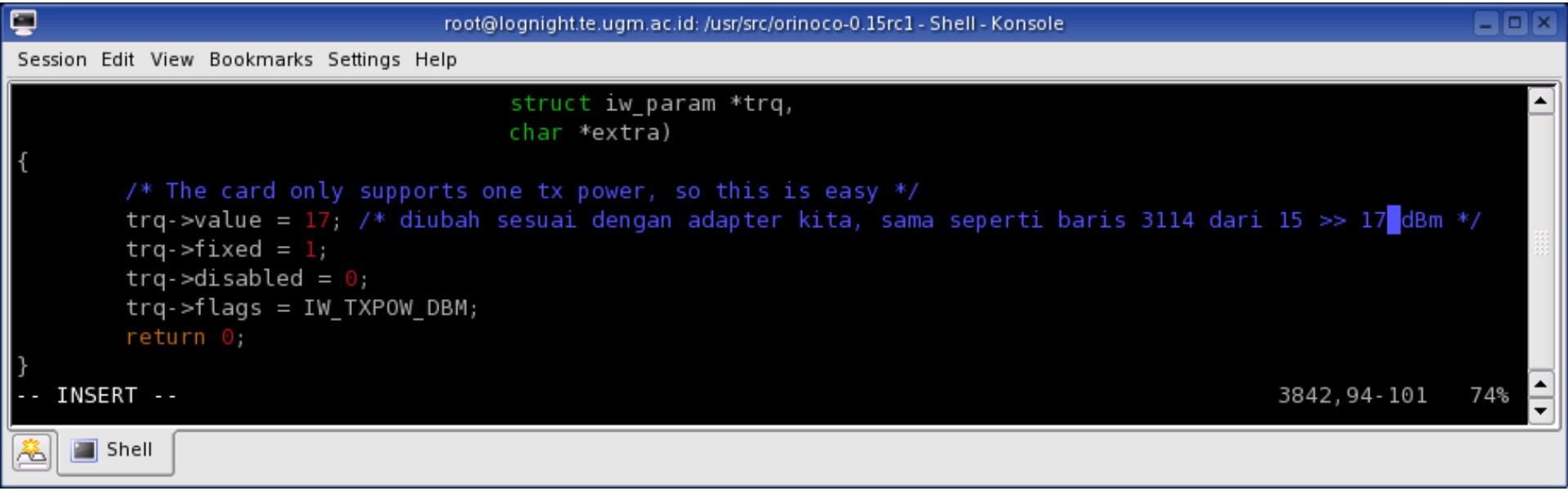
[root@lognight orinoco-0.15rc1]# vi orinoco.c

Find words “sens” (sensitivity) in source code using mc or grep tools ; Edit them

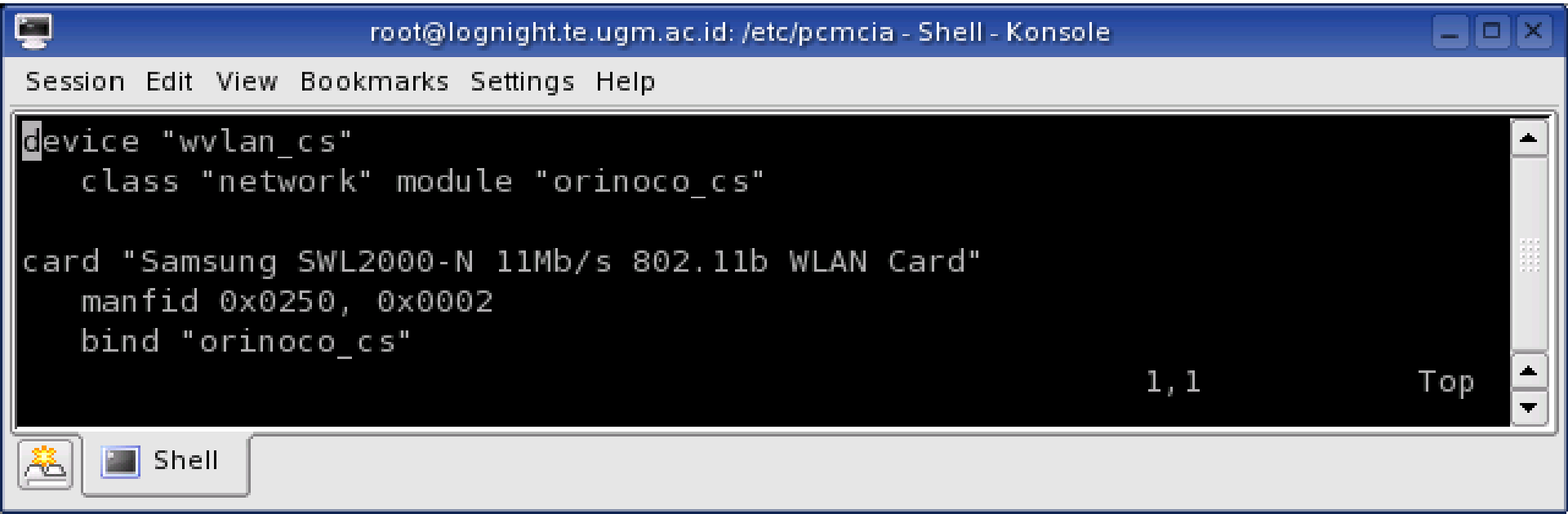


We can also tune the txpower. It's only used for prior to 0.15rc1 version. Txpower in the new version orinoco no longer reported 'cause unreliable

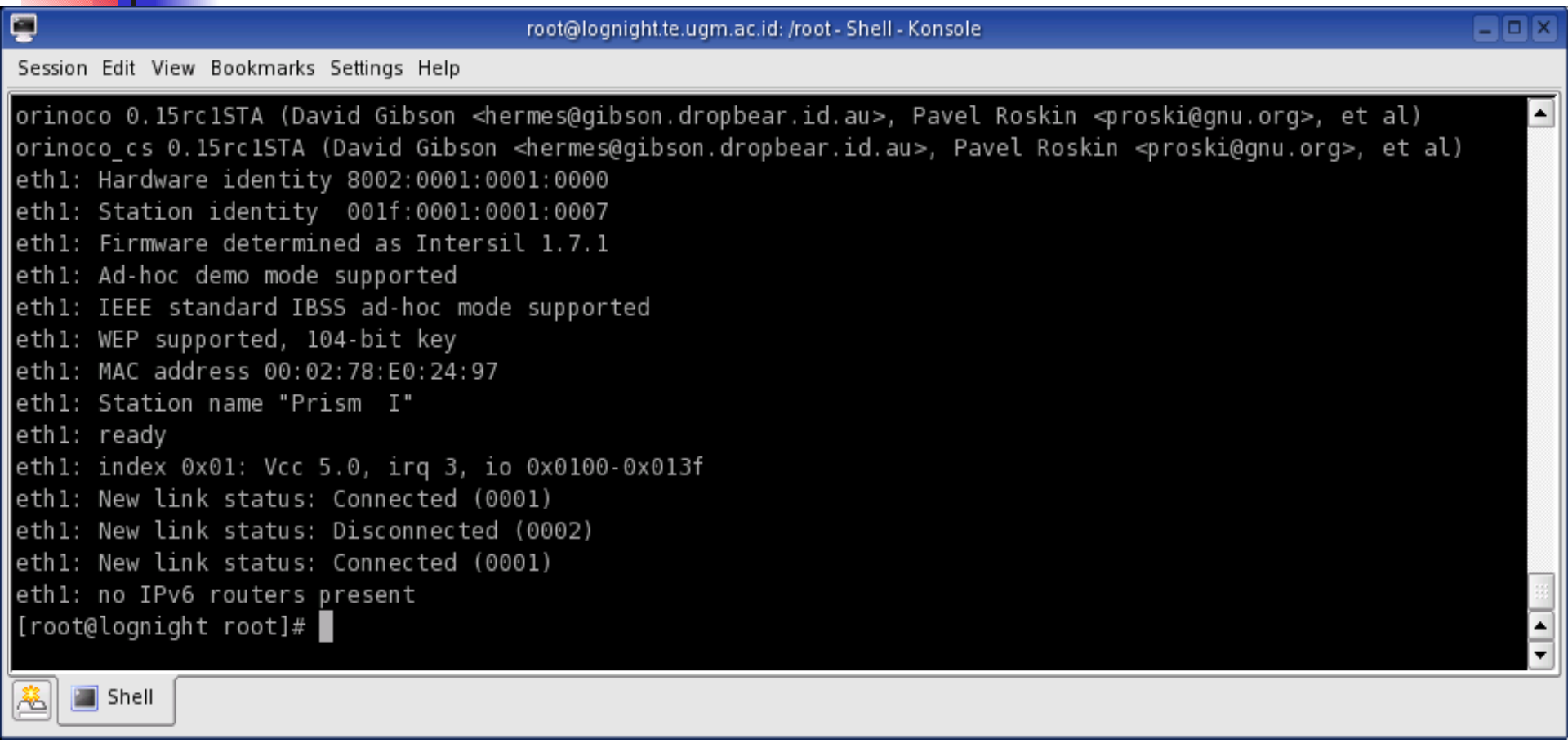




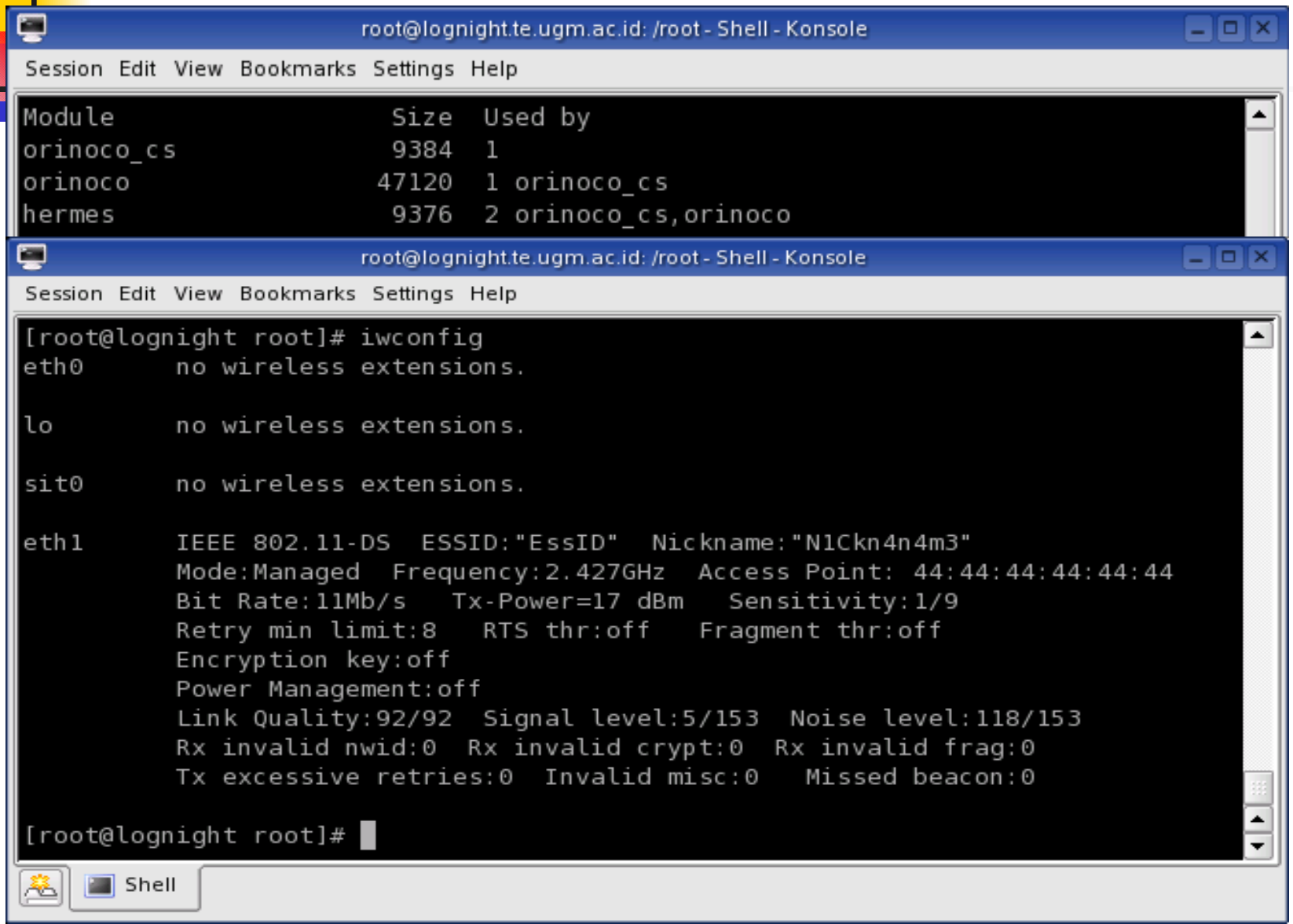
- make
- make install
- Go to /etc/pcmcia ; edit pcmcia.conf ; restart pcmcia daemon



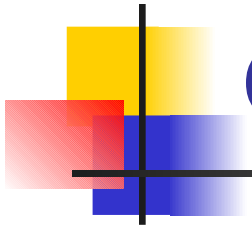
dmesg


root@lognight.te.ugm.ac.id: /root - Shell - Konsole
Session Edit View Bookmarks Settings Help
orinoco 0.15rc1STA (David Gibson <hermes@gibson.dropbear.id.au>, Pavel Roskin <proski@gnu.org>, et al)
orinoco_cs 0.15rc1STA (David Gibson <hermes@gibson.dropbear.id.au>, Pavel Roskin <proski@gnu.org>, et al)
eth1: Hardware identity 8002:0001:0001:0000
eth1: Station identity 001f:0001:0001:0007
eth1: Firmware determined as Intersil 1.7.1
eth1: Ad-hoc demo mode supported
eth1: IEEE standard IBSS ad-hoc mode supported
eth1: WEP supported, 104-bit key
eth1: MAC address 00:02:78:E0:24:97
eth1: Station name "Prism I"
eth1: ready
eth1: index 0x01: Vcc 5.0, irq 3, io 0x0100-0x013f
eth1: New link status: Connected (0001)
eth1: New link status: Disconnected (0002)
eth1: New link status: Connected (0001)
eth1: no IPv6 routers present
[root@lognight root]#
Shell

lsmod & iwconfig



Tips & Tricks using hostap driver



- Only for Prism2/2.5/3 Cards
- Get latest stable hostap-driver package from net

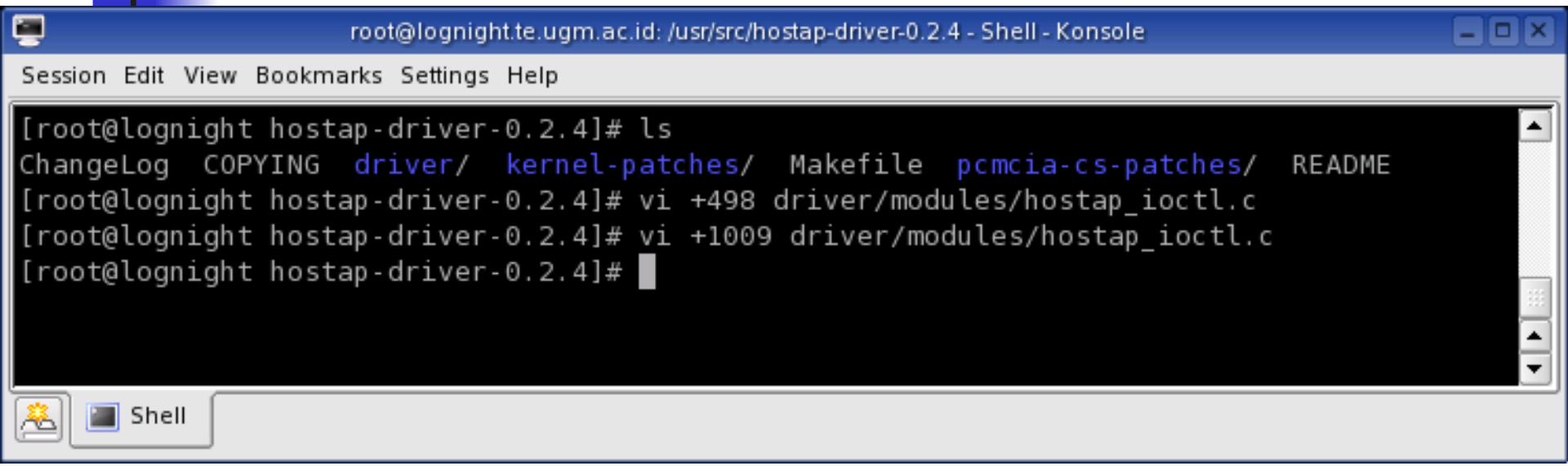
  http://hostap.epitest.fi/releases/

Unpack, hack the source, compile and install to your kernel

[root@lognight src]# cd hostap-driver-0.2.4/

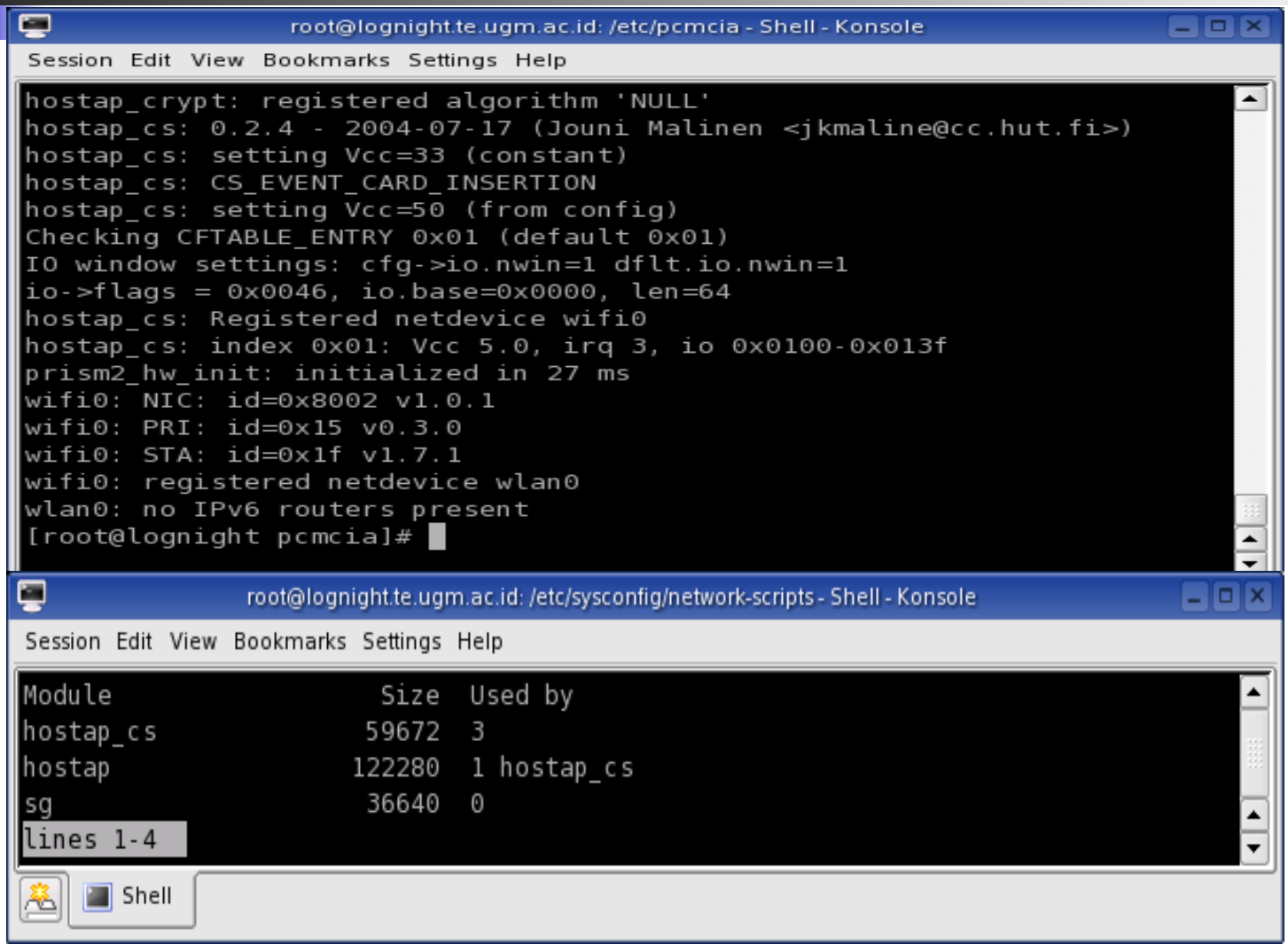
[root@lognight hostap-driver-0.2.4]#

Find words “sens” (sensitivity) in source code using mc or grep tools ; Edit them

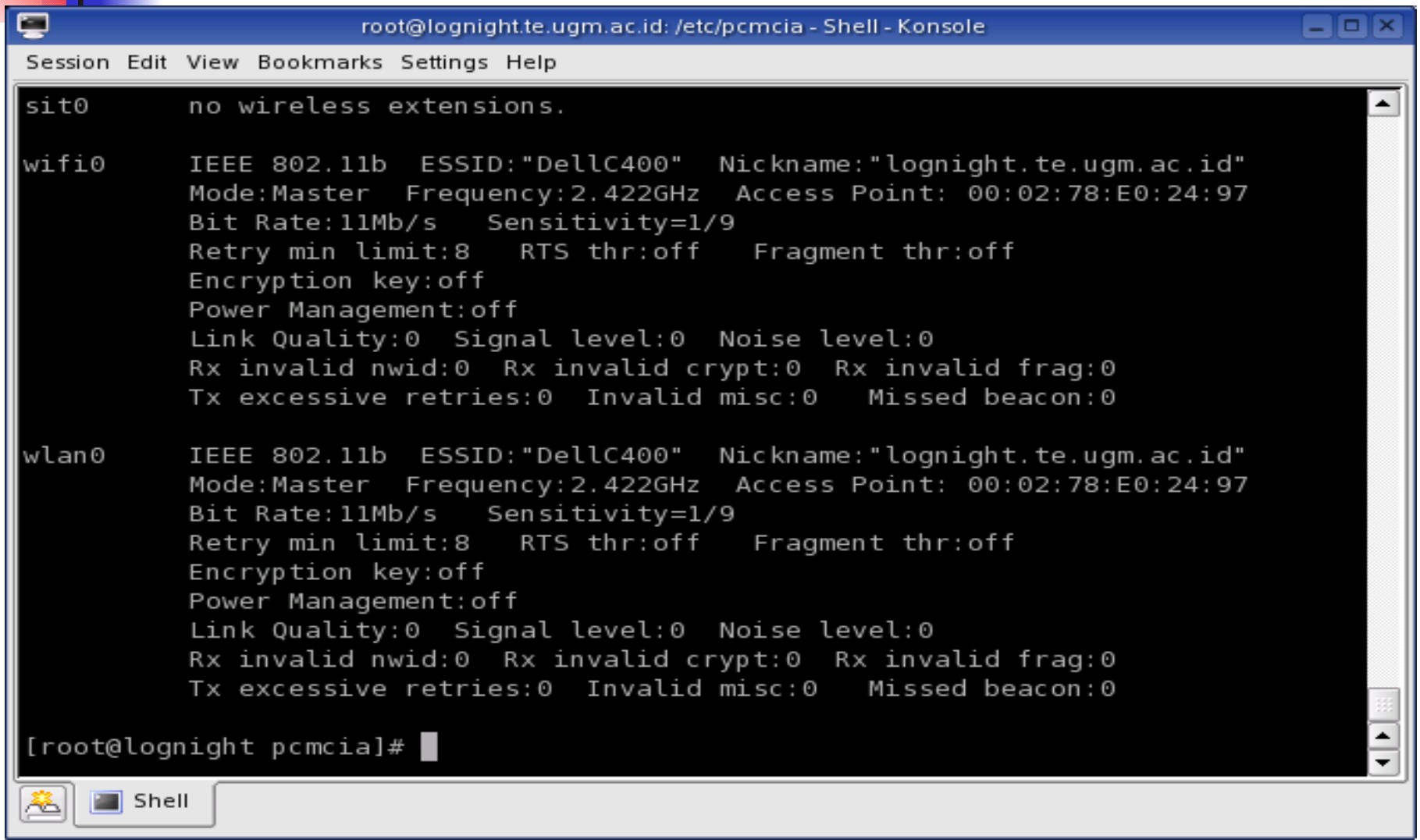


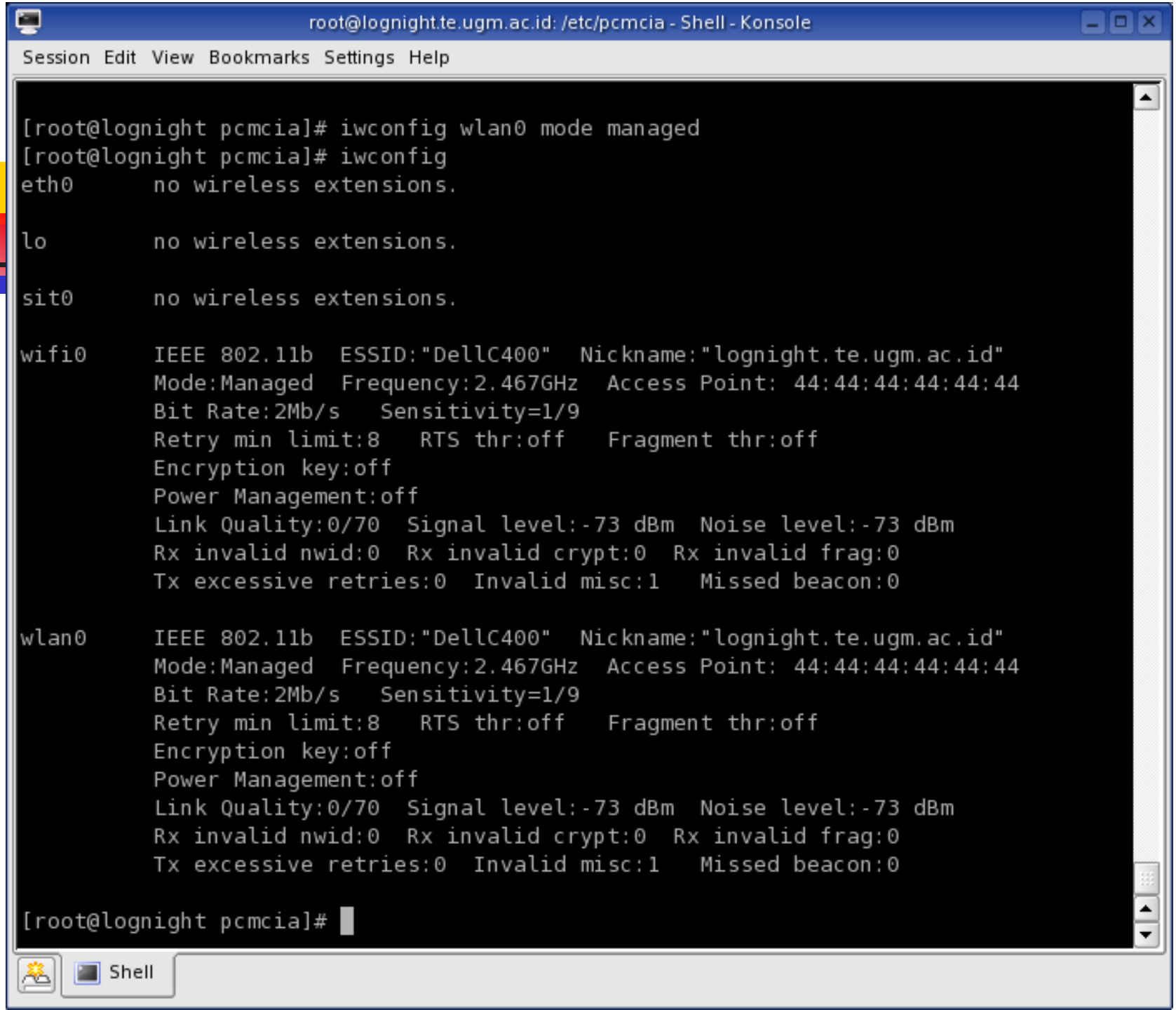
- make
- cd /etc/pcmcia
- mv hostap_cs.conf pcmcia.conf
- restart pcmcia daemon /etc/init.d/pcmcia restart

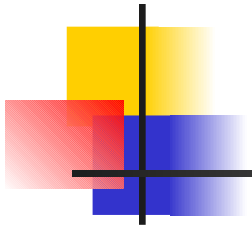
dmesg & lsmod


root@lognight.te.ugm.ac.id: /etc/pcmcia - Shell - Konsole
Session Edit View Bookmarks Settings Help
hostap_crypt: registered algorithm 'NULL'
hostap_cs: 0.2.4 - 2004-07-17 (Jouni Malinen <jkmaline@cc.hut.fi>)
hostap_cs: setting Vcc=33 (constant)
hostap_cs: CS_EVENT_CARD_INSERTION
hostap_cs: setting Vcc=50 (from config)
Checking CFTABLE_ENTRY 0x01 (default 0x01)
IO window settings: cfg->io.nwin=1 dflt.io.nwin=1
io->flags = 0x0046, io.base=0x0000, len=64
hostap_cs: Registered netdevice wifi0
hostap_cs: index 0x01: Vcc 5.0, irq 3, io 0x0100-0x013f
prism2_hw_init: initialized in 27 ms
wifi0: NIC: id=0x8002 v1.0.1
wifi0: PRI: id=0x15 v0.3.0
wifi0: STA: id=0x1f v1.7.1
wifi0: registered netdevice wlan0
wlan0: no IPv6 routers present
[root@lognight pcmcia]#
root@lognight.te.ugm.ac.id: /etc/sysconfig/network-scripts - Shell - Konsole
Session Edit View Bookmarks Settings Help
Module Size Used by
hostap_cs 59672 3
hostap 122280 1 hostap_cs
sg 36640 0
lines 1-4
Shell

iwconfig


root@lognight.te.ugm.ac.id: /etc/pcmcia - Shell - Konsole
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:off
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:0 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:E0:24:97
Bit Rate:11Mb/s Sensitivity=1/9
Retry min limit:8 RTS thr:off Fragment thr:off
Encryption key:off
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:0 Missed beacon:0
[root@lognight pcmcia]#
Shell


root@lognight.te.ugm.ac.id: /etc/pcmcia - Shell - Konsole
Session Edit View Bookmarks Settings Help
[root@lognight pcmcia]# iwconfig wlan0 mode managed
[root@lognight pcmcia]# iwconfig
eth0 no wireless extensions.
lo no wireless extensions.
sit0 no wireless extensions.
wifi0 IEEE 802.11b ESSID:"DellC400" Nickname:"lognight.te.ugm.ac.id"
Mode:Managed Frequency:2.467GHz Access Point: 44:44:44:44:44:44
Bit Rate:2Mb/s Sensitivity=1/9
Retry min limit:8 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality:0/70 Signal level:-73 dBm Noise level:-73 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:1 Missed beacon:0
wlan0 IEEE 802.11b ESSID:"DellC400" Nickname:"lognight.te.ugm.ac.id"
Mode:Managed Frequency:2.467GHz Access Point: 44:44:44:44:44:44
Bit Rate:2Mb/s Sensitivity=1/9
Retry min limit:8 RTS thr:off Fragment thr:off
Encryption key:off
Power Management:off
Link Quality:0/70 Signal level:-73 dBm Noise level:-73 dBm
Rx invalid nwid:0 Rx invalid crypt:0 Rx invalid frag:0
Tx excessive retries:0 Invalid misc:1 Missed beacon:0
[root@lognight pcmcia]#
Shell



THANKS

Setup and Optimizing
Wireless Client in Linux OS

by

Josua M Sinambela

Pengguna OpenSource

email : josh@ugm.ac.id

jogja-wireless@yahoogroups.com