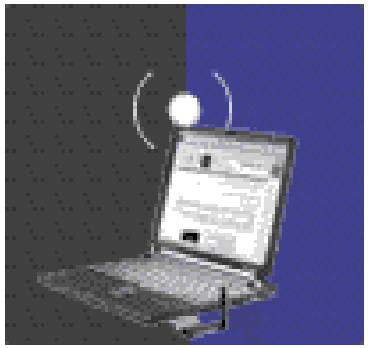
Wireless Networking For Beginners

Dennis Rex

SCALE 3X - 2005

Agenda

- Wireless Choices – 802.11A, B, G
- Devices - USB, PCI, PCMCIA, “bridges”
- Wireless chipsets - the good, the bad, the ugly
- Finding and installing the right driver
- Wireless settings and utilities
- Basic security tips
- Resources and links
- Q & A



Wireless Modes

- 802.11B & G
  - Same 2.4GHz band
  - 11mbps and 54mbps speeds
  - Best range (B mode)
- 802.11A
  - 5.2GHz band
  - Shorter range, less crowded, more common in business settings

Device Types

- USB
- PCMCIA/Cardbus
- PCI
- Mini-PCI
- Wireless Ethernet adapters

USB

- Flexible to position
- Easy to install
- Hotplug capable
- Inexpensive
- CPU consumption
- Speed
- No External antenna

PCMCIA/Cardbus

- Nearly universal for laptops
- Good driver support
- Hotplug capable
- Many with external antenna connections
- High-power options
- Can be fragile

PCI

- Good desktop choice
- Most have detachable antennae
- Location can be a problem
- IRQ conflicts, especially on older boxes

Mini-PCI

- Notebook-only
- Great range with internal case antenna
- No external antenna options
- No hotswap
- Difficult to upgrade

Wireless Ethernet Adapters

- No drivers needed
- Plugs into Ethernet port
- Great position flexibility
- Usually routeable
- Limited external antenna options
- Relatively expensive: 2x-3x PCMCIA

Wireless Chipsets

- Good: Native drivers, simple setup
  - ORiNOCO (classic), Cisco, Prism (2, 2.5, 3),
- OK: Manufacturer or open source drivers
  - Intel Centrino, Atheros, ACX100
- Usable with a wrapper:
  - Broadcom, RealTek
- Good luck:
  - ORiNOCO World Gold (Hermes II), RaLink RT2400/2500 (driver is available)

Wireless Drivers (a short list)

- orinoco_cs: Works with most ORiNOCO and Prism cards
- wlan-ng: Prism and Prism USB devices
- Prism54: 802.11G Prism cards
- HostAP: Prism 2-3
- MadWiFi: Atheros
- Ndiswrapper: Broadcom, RealTek via Windows drivers
- Linuxant: A commercial wrapper

Getting Connected Settings & Utilities

- Wireless success is a two-step process:
  - Finding and associating with an access point
  - Establishing a network connection
- Managing the wireless connection can be by GUI or command line
  - Network name, mode, channel, rate, key settings
- Network interface settings and status
  - GUI, CLI or distro scripts

Command line options

- Wireless Tools – iwconfig
  - Used for setting wireless parameters, scanning for available networks or displaying status.
  - Usually the data source for UI's.
  - Nearly universal across distros and configurations.
    - Most drivers use wireless tools
  - Settings are not persistent
    - Frequently-used values can be stored in distro-specific script files.

Terminal

File Edit View Terminal Tabs Help

Terminal | Terminal

```
IWCONFIG(8)          Linux Programmer's Manual          IWCONFIG(8)

NAME
       iwconfig - configure a wireless network interface

SYNOPSIS
       iwconfig [interface]
       iwconfig interface [essid X] [nwid N] [freq F] [channel C]
                          [sens S] [mode M] [ap A] [nick NN]
                          [rate R] [rts RT] [frag FT] [txpower T]
                          [enc E] [key K] [power P] [retry R]
                          [commit]
       iwconfig --help
       iwconfig --version

DESCRIPTION
       Iwconfig  is  similar  to ifconfig(8), but is dedicated to
       the wireless interfaces. It is used to set the  parameters
       of  the  network interface which are specific to the wire-
       less operation (for example :  the  frequency).   Iwconfig
       may  also  be  used  to  display those parameters, and the
       wireless statistics (extracted from /proc/net/wireless).

Lines 1-25
```

GUI Wireless Options

- KWiFiManager
  - An ORiNOCO utility look-alike
  - Originally a stand-alone, now integrated into KDE
  - Allows 4 profiles to be stored
- Gnome wireless applet
  - Signal strength
- XFCE4 wavelan plugin
  - Signal strength, SSID

Interface eth1 - KWiFi-Verwaltung

File Settings Help

Connection speed [MBit/s]:

0 1 2 5.5 11

OUT OF RANGE

Signal strength: 0

Scan for Networks...

Status of Active Connection

Searching for network:

Access point: 44:44:44:44:44:44

Local IP: unavailable

Frequency [channel]: 2.412 [1]

AccessPoint: UNKNOWN

Interface wlan0 - KWiFi-Verwaltung

File Settings Help

Connection speed [MBit/s]:

0 11 22 54 108

GOOD

Signal strength: 23

Scan for Networks...

Status of Active Connection

Connected to network: uni-exp

Access point: 00:07:85:92:5B:13

Local IP: 158.64.11.38

Frequency [channel]: 2.442 [7]

AccessPoint: LU, Luxembourg, rue Richard Coudenhove-Calergi, Fondation RESTENA

Statistics - KWiFiManager

Noise/Signal Level Statistics

38

5

BLUE = signal level, RED = noise level

-240 s

now

Information - k

Available networks:

uni-exp

OK

2 3 4

Interface eth1 - KWiFi

Statistics - KWiFiMan

Interface wlan0 - K

23

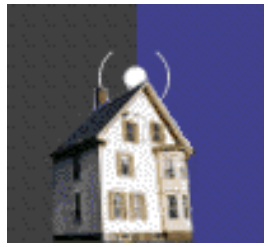
11:02

Interface tools

- CLI – ifconfig, route, dhclient or dhcpcd
  - Activate and configure the interface
  - Obtain or assign an IP address and gateway
  - Usually scripted. Again, distro-specific locations
- UIs – NEAT, NetDrake, YaST, Netconfig
  - Almost universally, these tools simply overwrite a configuration file. Sometimes, knowing the location and syntax of the files makes changes quicker.

Wireless Security

- Worthy of its own topic. We'll touch on the basics
- Two primary wireless security objectives:
  - Control access to the wireless LAN
  - Protect the data



Wireless Security - Encryption

- WEP – Wired Equivalent Privacy
  - Encrypts data packets only
  - Uses a 10 or 26 digit hex key on each client matching the access point
  - Several published vulnerabilities
  - Attack tools are easily obtained

Wireless Security - Access

- ESSID Broadcast Disable - Security through obscurity
  - Extended Service Set Identifier, the “network name”
  - Needed for clients to associate
  - Default setting is to beacon – announce the name to prospective client devices
  - Access point is still visible
  - SSID is broadcast in response to a probe
  - Broadcast disable can cause connection problems

Wireless Security - Access

- MAC address filtering – access control
  - Media access control address. A unique hexadecimal address assigned by the manufacturer to each network device. ex: A0:12:3E:00:00
  - Routers can be set to deny or accept specific addresses

Wireless Security - Access

- MAC addresses are easily cloned, or "spoofed."
- MAC addresses are sent in **every** 802.11 frame
- MAC addresses are **never** encrypted

[Terminal] | Terminal | ethereal_capture | [xterm] | [The GIMP] | [Brushes] | [Tools] | [Tool Options]

ethereal_capture_probe - Ethereal

File Edit View Capture Analyze Help

No.	Time	Source	Destination	Protocol	Info
14	12.389883	GemtekTe_31:79:a6	Broadcast	IEEE 802	Beacon frame
15	12.680482	LinksysG_83:b7:8a	LinksysG_12:7e:b0	IEEE 802	Probe Response
16	12.682237	LinksysG_83:b7:8a	LinksysG_12:7e:b0	IEEE 802	Probe Response

```
▷ Prism Monitoring Header
▽ IEEE 802.11
    Type/Subtype: Probe Response (5)
  ▽ Frame Control: 0x0850 (Normal)
      Version: 0
      Type: Management frame (0)
      Subtype: 5
    ▽ Flags: 0x8
        DS status: Not leaving DS or network is operating in AD-HOC mode (To DS: 0  From DS: 0) (0x00)
        .... .0.. = More Fragments: This is the last fragment
        .... 1... = Retry: Frame is being retransmitted
        ...0 .... = PWR MGT: STA will stay up
        ..0. .... = More Data: No data buffered
        .0.. .... = WEP flag: WEP is disabled
        0... .... = Order flag: Not strictly ordered
    Duration: 314
    Destination address: 00:06:25:12:7e:b0 (LinksysG_12:7e:b0)
    Source address: 00:0c:41:83:b7:8a (LinksysG_83:b7:8a)
    BSS Id: 00:0c:41:83:b7:8a (LinksysG_83:b7:8a)
    Fragment number: 0
    Sequence number: 2672
▷ IEEE 802.11 wireless LAN management frame
```

```
0090  50 08 3a 01 00 06 25 12  7e b0 00 0c 41 83 b7 8a   P:....%. ~...A...
00a0  00 0c 41 83 b7 8a 00 a7  95 6d 8d 46 8e 01 00 00   ..A..... .m.F....
00b0  64 00 05 00 00 07 6c 69  6e 6b 73 79 73 01 04 82   d.....li nksys...
00c0  84 0b 16 03 01 06 04 06  00 02 00 00 00 00         ........ ......
```

Filter: | Clear | Apply | Basic Service Set ID (wlan.bssid), 6 bytes

Wireless Security - Access

- Isolation via LAN configurations
  - Turn off DHCP and use non-standard IP range
    - Makes it a little harder for a hacker to get onto your LAN
    - Sniffers often reveal IP range and manual setting is simple

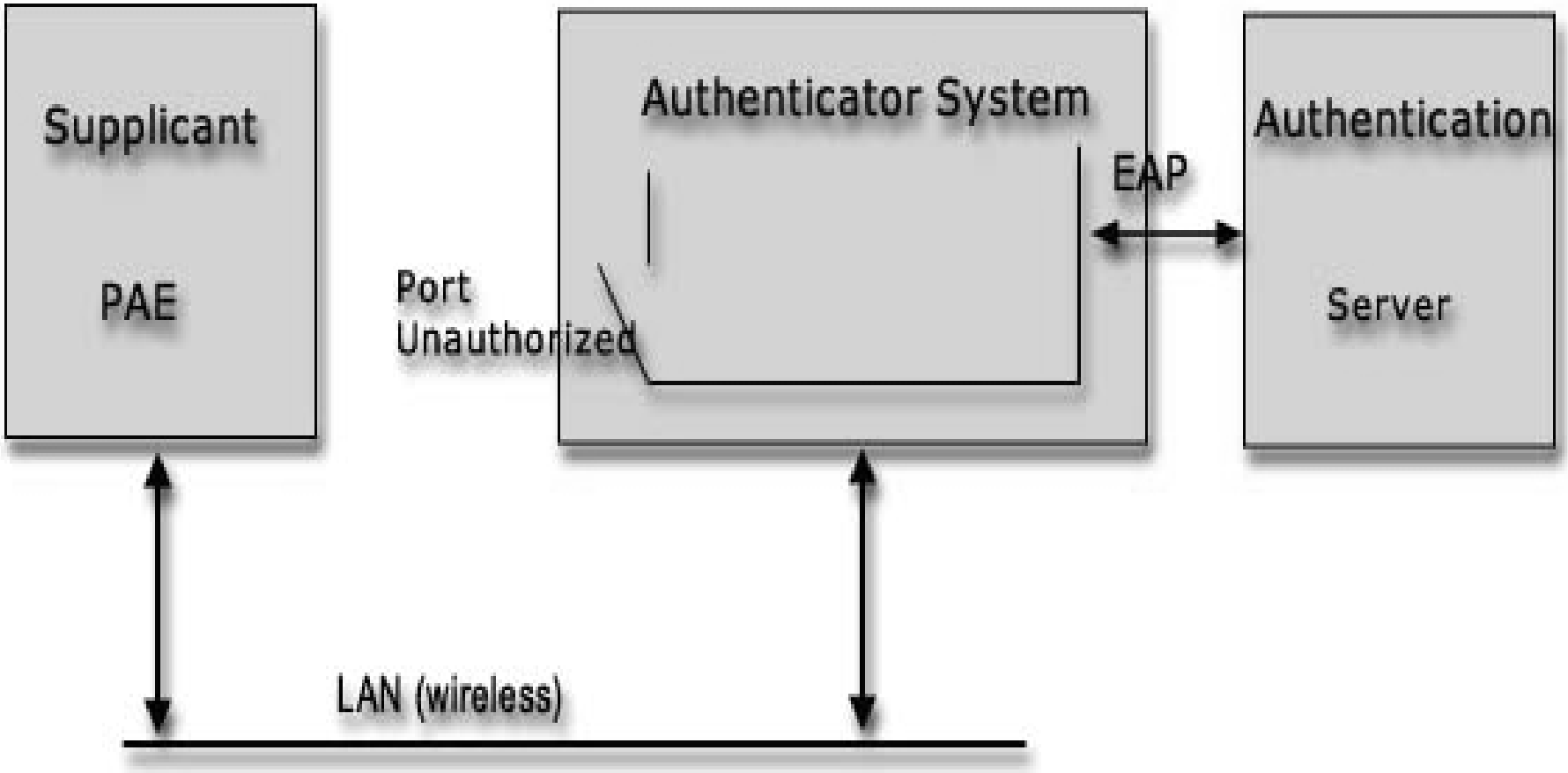
Wireless Security - Access

- DMZ, subnet or VLAN
  - Fences off the wireless portion from the wired LAN
  - Complex and often expensive
- Netbios or firewall options
  - Some routers allow the blocking of file sharing or ports/protocols between wireless and wired

Wireless Security - Access

- 802.1x – effectively, a wireless gate
  - Authenticates users based on various credentials
  - Requires hardware support and/or external server
  - Requires a client (supplicant)
    - Xsupplicant (OSS), Meetinghouse (Commercial)
  - No data encryption
  - A basis for WPA

802.1x example



Wireless Security - WPA

- WiFi Protected Access
- Combines 802.1x (access control) with WEP (encryption) and adds frequent key changes to dodge hacks that depend on large numbers of packets.
- Other than dictionary attacks against WPA-PSK, no known vulnerabilities.
- wpa_supplicant needed (XSupplicant soon)

Recap, by steps

- Load the driver
- Activate the interface
- Set wireless parameters
- Association
- 802.1x (if appropriate)
- DHCP
- Surf

Resources and Links

- Linux & Wireless LANs
- Open1X.org
- Unofficial 802.11 Security Web Page
- AbsoluteValue Systems Adapter List
- SourceForge
- DSLReports Wireless Networking Forum
- FreeRADIUS mailing list

Resources and Links - 2

- irc.freenode.net
  - #ATU, #ndiswrapper, #hostap
- WiFi Networking News
- Manufacturer sites
  - Meetinghouse Data Systems
  - Funk Software
  - Cisco, Linksys, ZyXEL
- LUGs