Grundlagen WLAN

René Pfeiffer <pfeiffer@luchs.at>

CaT

18. Juni 2007

Inhaltsübersicht - Wovon reden wir?

Inhaltsübersicht - Wovon reden wir?

- Physik (ganz kurz)
- WLAN Technologien und Standards
- Terminologie
- Verschlüsselung
- Absicherung

Aussprache (Umgangssprache)

Aussprache (Umgangssprache)

- Wireless Local Area Network (WLAN)
- Wireless Fidelity (WiFi)
- Wireless
- IEEE 802.11

Physik

Frequenzbereiche

Frequenzbereiche

- 2,4-2,5 Gigahertz (GHz)
  - typischerweise Mikrowellen, drahtlose Telefone, Babyfone
- 5 GHz
- 5,15-5,25 GHz
- 5,25-5,35 GHz
- 5,725-5,875 GHz

Frequenzbereiche

- 2,4-2,5 Gigahertz (GHz)
  - typischerweise Mikrowellen, drahtlose Telefone, Babyfone
- 5 GHz
- 5,15-5,25 GHz
- 5,25-5,35 GHz
- 5,725-5,875 GHz
- Reichweiten variieren zwischen 10 und 200 Metern
- Kilometerreichweite mit speziellen Antennen
- „Line of sight”

Frequenzmodulation

Frequenzmodulation

- Direct-sequence spread spectrum (DSSS)
- Orthogonal Frequency-Division Multiplexing (OFDM)

Frequenzmodulation

- Direct-sequence spread spectrum (DSSS)
- Orthogonal Frequency-Division Multiplexing (OFDM)
- Methoden modulieren Informationen auf Trägerfrequenz
- Methoden beugen Interferenzen vor

Frequenzkanäle

Frequenzkanäle

- 1 bis 11 (USA)
- 1 bis 13 (Europa)
- 1 bis 14 (Japan)

Frequenzkanäle

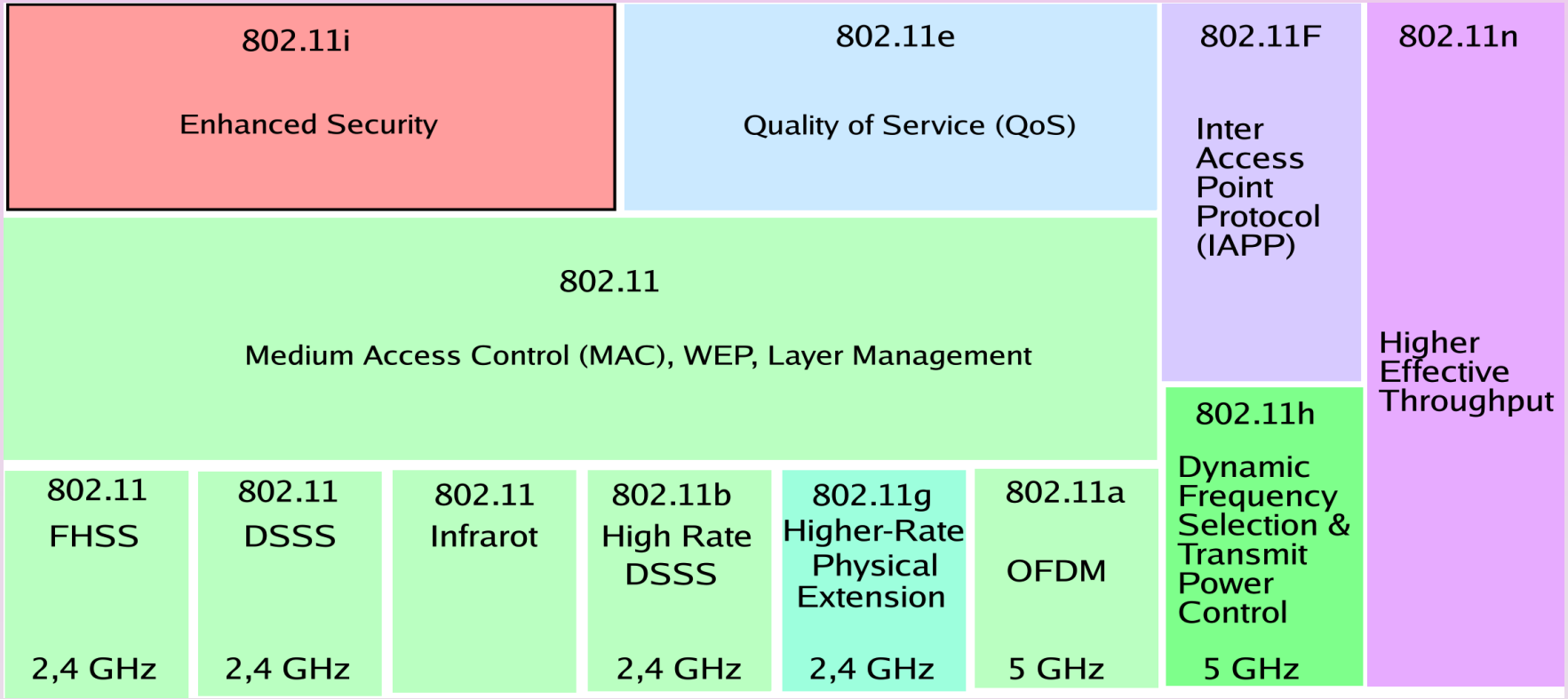
- 1 bis 11 (USA)
- 1 bis 13 (Europa)
- 1 bis 14 (Japan)
- Kanäle überlappen frequenztechnisch
  - „Abstände einhalten”, wenn viele Sender zusammen
  - Faustregel für Verteilungen: 1, 6, 11

Protokolle und Standards

IEEE 802.11 Familie

- Wireless LAN Standards beginnen 1991 mit 802.11
  - 802.11 (veraltet), 1997, 2 Mbit/s
  - 802.11a, 1999, 54 Mbit/s
  - 802.11b, 1999, 11 Mbit/s
  - 802.11g, 2003, 54 Mbit/s
  - 802.11n, 2008, 248 Mbit/s
- 802.11b und 802.11g derzeit verbreitet

IEEE 802.11 Familie - Übersicht



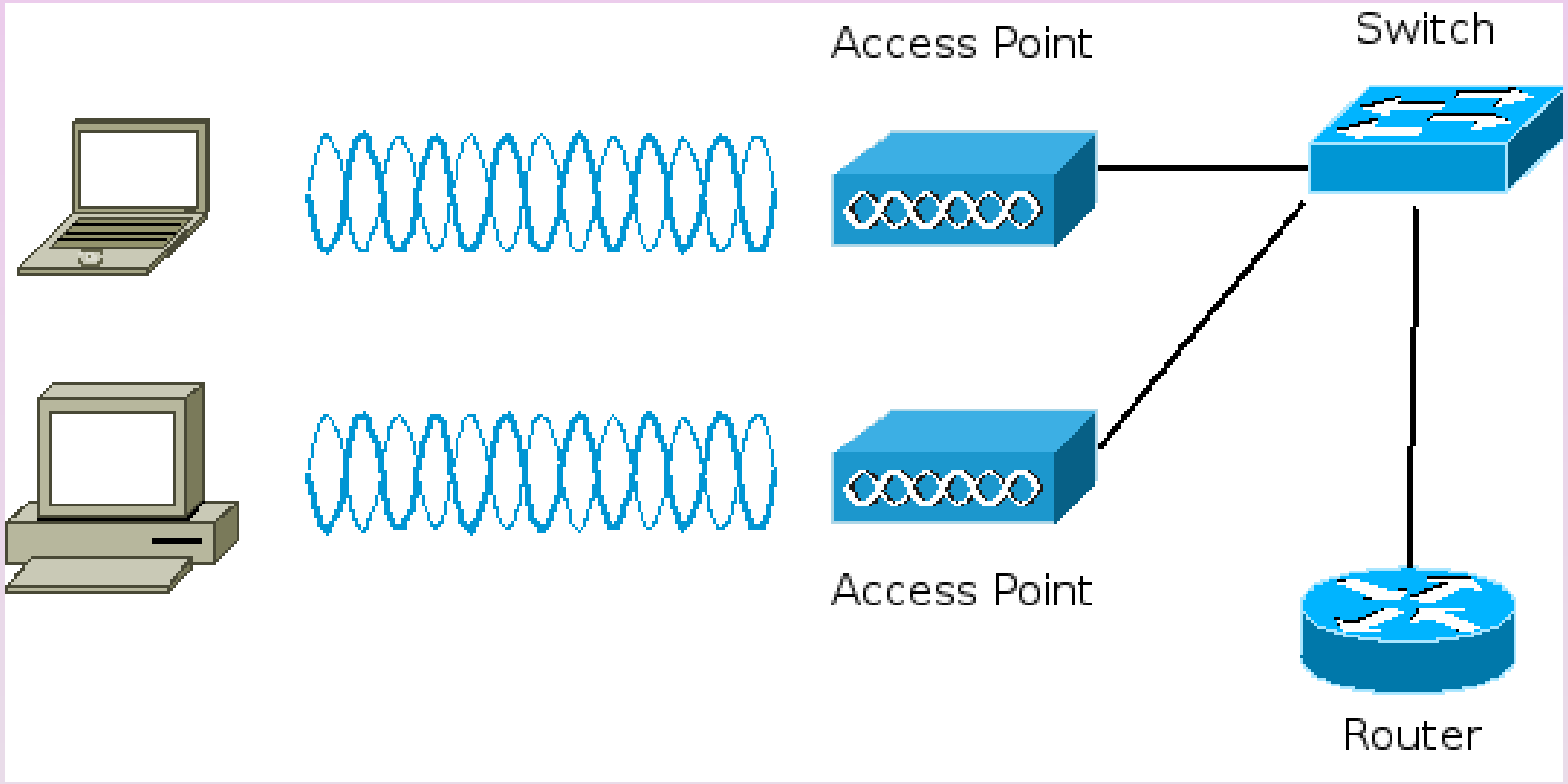
Terminologie

WLAN Bestandteile

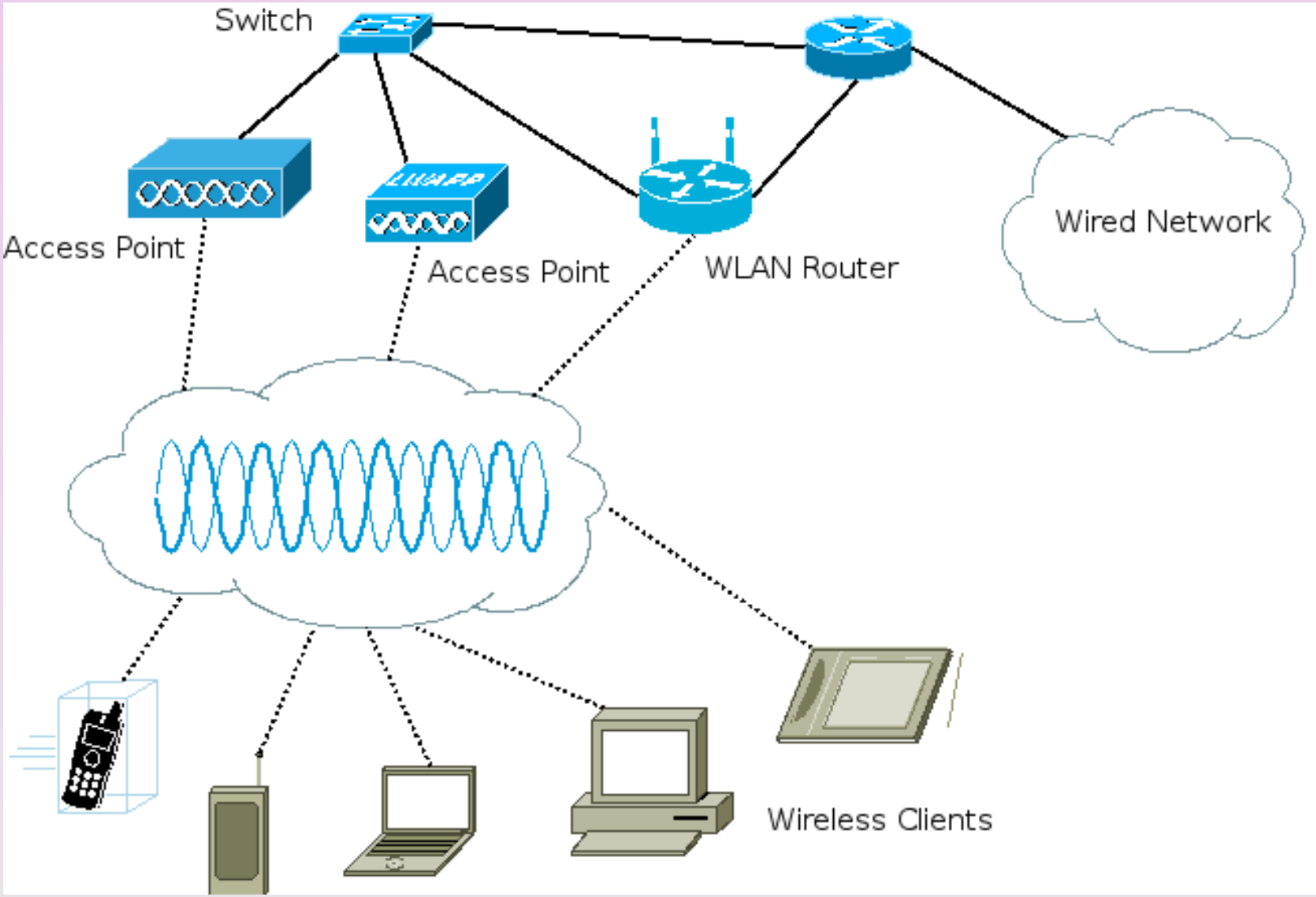
WLAN Bestandteile

- Antennen in allen Formen und Farben
- Access Point
  - zum Verbinden auf der Luftschnittstelle
- WLAN Client
- WLAN Router

WLAN Trennung Layer2/3



WLAN Beispielnetzwerk mit allen Komponenten



Verschlüsselungsmethoden

Wired Equivalent Privacy (WEP)

Wired Equivalent Privacy (WEP)

- *Wired Equivalent Privacy* / *Wireless Encryption Protocol*
- WEP benutzt
  - 40 Bit Schlüssel + 24 Bit *Initialisierungvektor* (IV) oder
  - 104 Bit Schlüssel + 24 Bit *Initialisierungvektor* (IV)
- WEP verwendet Stromchiffre RC4
- WEP kann durch Mitlauschen kompromittiert werden
  - 17 verschiedene Attacken bekannt
  - WEP Sicherheit „hält” Minuten bis Tage

Wi-Fi Protected Access (WPA)

Wi-Fi Protected Access (WPA)

- WPA benutzt ebenfalls RC4
- WPA verwendet 128 Schlüssel + 48 Bit IV
- Einführung *Temporal Key Integrity Protocol* (TKIP)
  - WEP Schlüssel werden pro Paket „gemischt”
  - TKIP prüft Paketintegrität
  - TKIP ändert periodisch die Schlüssel
- WPA prüft Checksummen von Paketen
- *Michael* Algorithmus gegen Replay Attacken

802.11i (WPA2)

802.11i (WPA2)

- WPA2 = WPA + 802.11i
- WPA2 hat zusätzlich
  - Counter Mode with Cipher Block Chaining Message Authentication Code Protocol (CCMP)
  - CCMP verwendet *Advanced Encryption Standard* (AES)
- bis zu 256 Bit Schlüssellänge
- SSID geht in Schlüsselgenerierung ein

Enterprise Mode (802.11X)

Enterprise Mode (802.11X)

- Pre-Shared Key (PSK) Modus nur für kleine Netze machbar
- Enterprise Mode führt *802.11X authentication server* ein
  - Verwendung von Zertifikaten
  - Einführung von TLS (SSL)
  - Verwenden von SIM-Karten
- Wesentlich sicherer
- Erfordert mehr Aufwand für Infrastruktur

OpenVPN und IPsec

OpenVPN und IPsec

- Betreiben von Wi-Fi ohne WiFi-Security
  - DHCP unverschlüsselt
  - Verwenden von OpenVPN/IPsec mit Gateway
- Funktioniert mit alter Hardware
- Verschlüsselung unabhängig von Wi-Fi Schicht
- Verwenden von PSKs und Zertifikaten
- Funktioniert zusätzlich zu WEP/WEP2/WPA/WPA2

Absicherung von Wi-Fi Netzwerken

Absicherung von Wi-Fi Netzwerken

Grundlegendes

Grundlegendes

- „beste” Firmware und Treiber
- keine öffentlichen Managementzugänge (Web Interfaces, Telnet, SSH, . . .)
- kein SSID Broadcast (*hidden SSID*)
- MAC-Adreßfilter
- Hotspot exklusiv oder Wi-FI Zugang?
  - Hotspot muß mit *allen* Clients zusammenarbeiten
  - Wi-Fi Zugang muß mit *ausgewählten* Clients zusammenarbeiten

  Beides schließt sich aus!
- Einsatz von Paketfiltern

Hidden SSID und MAC-Adreßfilter bringt nichts, hält aber auf. ☺

Wireless Tools

Wireless Tools

- Kismet
- Linux® WPA/WPA2/IEEE 802.1X Supplicant
- Wavemon
- Wellenreiter
- WiFi Radar
- Wireless Tools for Linux®

Wireless Tools für Linux®

Wireless Tools für Linux®

```
iwconfig eth0
iwlist eth0 scan
```

Über dieses Dokument

- Autor: René Pfeiffer
- Erstellt mit LaTeX und LaTeX Beamer Class
- Dokumentensammlung unter

  http://web.luchs.at/information/docs.php