DECUS
HP-User Society
Symposium
Bonn, April 2004

Peter Schürholt
HPS – NSG
Senior Consultant

Wireless LANs 1H04

Implementierung und Anwendung

Wireless LAN ?
Ja, aber mit Sicherheit !

Agenda

Wireless LAN

- **Technologie**
- **Topologien**
- **Site Survey**
- **Sicherheit**
- **Betrieb**

page 2

WLAN Planung

Grundsatzentscheidungen

- Wofür ? (Anwendung, Einsatzbereich, Skalierung)
- Welchen WLAN-Standard, welche Technologie ?
- Welche Komponenten, welche Topologie ?
- Aktive und passive Sicherheit ?
- Operation & Monitoring, Management
- $ $ $ $ $ (ROI ?)

page 3

Wireless LAN

Back to the roots „Äther-Net“

einige Synonyme (nicht immer richtig bzw. eindeutig):

- WLAN
- WaveLan
- Funk-Lan/ -Netz
- Wireless Ethernet
- Wi-Fi-LAN

usw.

page 4

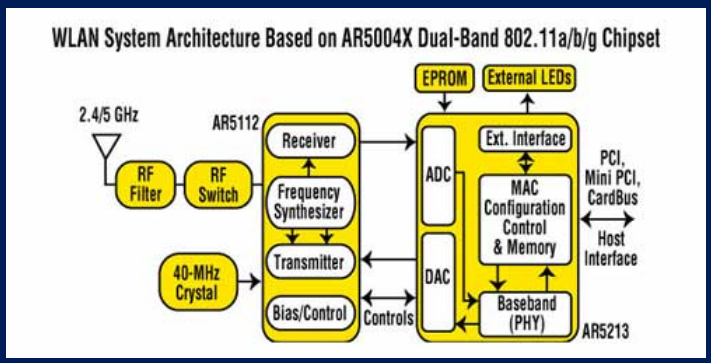
IEEE 802.11 (Wi-Fi) im Wettbewerb

IEEE 802.11 b,g,a

- ETSI HiperLAN/HiperLink (Datenrate 20-155Mbps)
- Bluetooth (Datenrate 57-750kbps)
- IEEE 802.15 (MAC-WPAN)
- Corporate GSM (14,5 Kbps – 384Kbps)
- Corporate UMTS (2Mbps)
- WBFH (HomeRF (2.0))
- IEEE802.16a,c,e (MAN, 2 – 60 GHz)
- .....

page 5

WLAN – Chip-Sets



ca. 40 verschiedene Chip-Hersteller

Agere, Atheros, Broadcom, Intel, Intersil,Texas Instruments

..... usw.

Agere MIMO-Chip bis zu 162Mbps

page 6

WLAN – Karten

- **PCMCIA (PC-Card)**
- **PCI**
- **ISA**
- **USB-Adapter**
- **Compact Flash Adapter**

Adapter *können* einen Anschluß für eine externe Antenne haben

page 7

Reichweiten (Wi-Fi)

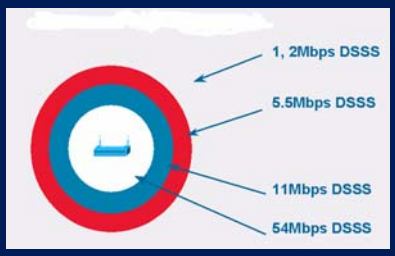
Die Reichweite wird bestimmt durch das Zusammenspiel von Abstrahlleistung, Antennen-Technik und Örtlichkeiten

Die Abstrahlung ist in der EU auf 100/200mW EIRP begrenzt (USA → 1000mW)

- ca. 30m in Gebäuden (2-3 massive Wände)
- ca. 300m außerhalb von Gebäuden
- Reichweiten bei 5Ghz etwa 1/3
- die Reichweite kann durch externe Antennen erheblich gesteigert werden (bis zu 60 Km mit Parabol-Antennen)

page 8

Bandbreite / Entfernung



IEEE802.11b,g

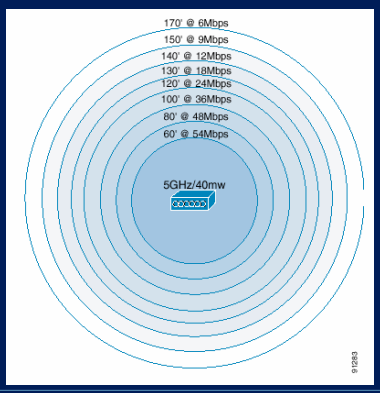
1 Mbps → 350/2000 ft.

11Mbps → 140/800 ft

IEEE802.11a

6 Mbps → 170/1000 ft.

54 Mbps → 60/100 ft

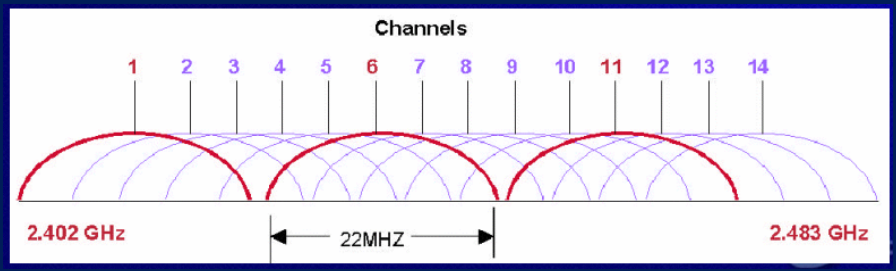


page 9

IEEE 802.11b Channels

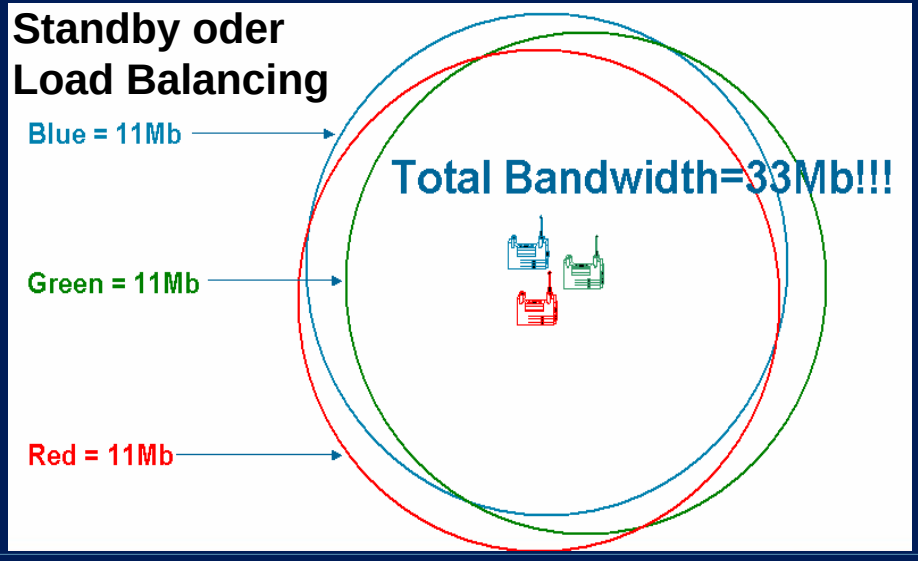
- IEEE 802.11b definiert 14 Kanäle im 2.4 Ghz-Band
- in Deutschland 13 definiert und nutzbar
- davon drei nicht-überlappende Kanäle (→802.11a bis zu 19)

Kanalverteilung (US)



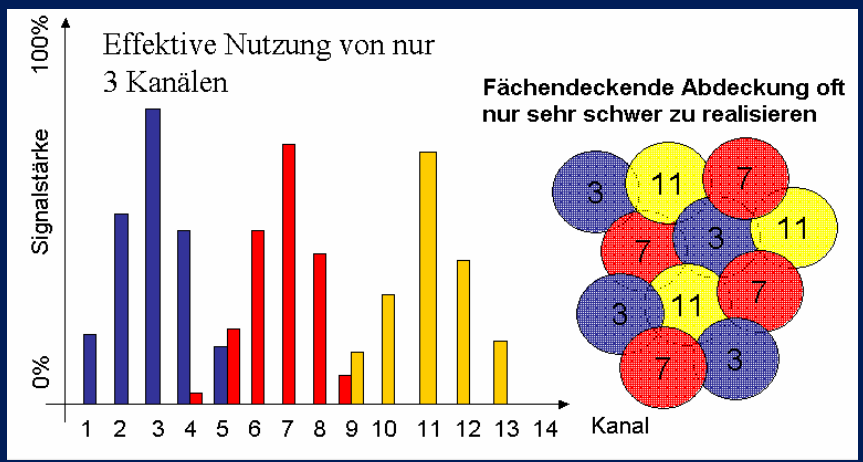
page 10

Bandbreite / Abdeckung / Redundanz



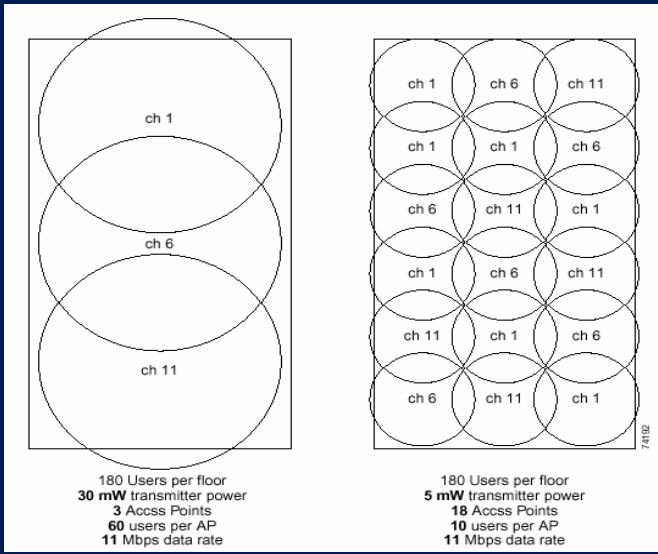
page 11

IEEE 802.11b Channels



page 12

Ausleuchtung und Bandbreite



page 13

Multimedia über WLAN

IP-Telefony, Stream Audio, Stream Video

- Bandbreitenreservierung ?
- Traffic-Priorization ?
- Slot-Reservierung und Polling

Priority	Access Category	Designation
1	0	Best Effort
2	0	Best Effort
0	0	Best Effort
3	1	Video Probe
4	2	Video
5	2	Video
6	3	Voice
7	3	Voice

- 802.11e ständig verschoben (Ende 2004)
- Interim WME (Wi-Fi Multimedia Extensions)

page 14

Berechnungsbeispiel – Outdoor (1)

- Max. EIRP nach FCC ist 36dB (4 Watt)
  - PC Card +15dB
  - Antenne +14dB
  - 50‘ Kabel - 3.6dB
  - Pigtail & Connector - 0.9dB

zusammen 24.5dB

Differenz 11.5dB

Es darf also eine Antenne mit zusätzlichen 11.5dB Gewinn eingesetzt werden (Parabol, max. 40Km Reichweite)

page 15

Berechnungsbeispiel – Outdoor (2)

- Max. EIRP nach ETSI ist 20dB (100mW)
  - PC Card + 8dB
  - Antenne + 14dB
  - 50‘ Kabel - 3.6dB
  - Pigtail & Connector - 0.9dB

zusammen 17.5dB

Differenz 2.5dB

Es darf also eine Antenne mit zusätzlichen 2.5dB Gewinn eingesetzt werden (Stab-Antenne, max. 4-5 Km Reichweite)

page 16

Antennen

- **Omni-Antenne**
  2.5 bis 10db Gewinn, 360º
- **Yagi-Antenne**
  >10db Gewinn, 30-50º
- **Patch-Antenne**
  5 bis 10db Gewinn, 60-90º
- **Dish-Antenne**
  >20db Gewinn, 3-12º

page 17

IEEE 802.11a

- **RegTP-Einschränkungen (definiert im 802.11h)**
  - im europ. Standard bereits vorhanden (HiperLAN II)
  - DFS (Dynamic Frequency Selection)
  - TPC (Transmission Power Control)
- **Sendeleistung**
  - 30mW bei IEEE802.11a
  - 200mW bei IEEE802.11h
- Frequenzbereiche: 5150 bis 5350 und 5470 bis 5725 MHz
- Outdoor von 5470 bis 5725 MHz ??

page 18

IEEE 802.11g

- Rückwärtskompatibel zu 802.11b
  - oft nur bei gleichem Chipsatz (Wi-Fi-Zertifikat beachten)
- 802.11g nur solange, bis ein b-Gerät in der gleichen Zelle auftaucht
- 2,4 GHz-Frequenzband aber andere Modulationstechnik
- Bis zu 54Mbps (Brutto)
- Sendeleistung 100mW (indoor, outdoor)
- 3 nicht überlappende Kanäle

page 19

Fazit Technologien – es kommt drauf an

- 802.11a/b/g-Standards sind in Deutschland zugelassen (Einschränkungen beachten)
- 802.11a ca. 30% teurer als 802.11b
- 802.11a-Ausleuchtung geringer (1/3), dafür aber mehr Kanäle verfügbar
- 2,4 GHz ist überfüllt, 5,x GHz noch nicht
- proprietäre Lösungen vermeiden (xx Mbps)
- Multi-Band-Lösungen (b,g,a) bevorzugen

page 20

WLAN – Topologien (1)

- **Ad-hoc-Mode (oder peer-to-peer)**

  Endgeräte kommunizieren direkt miteinander

  gleicher Kanal, gleicher Netzwerkname, fertig

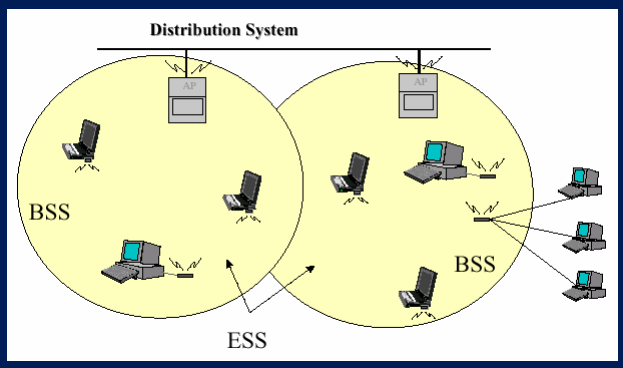
Combi-Karten

Multi-Band !

page 21

WLAN – Topologien (2)

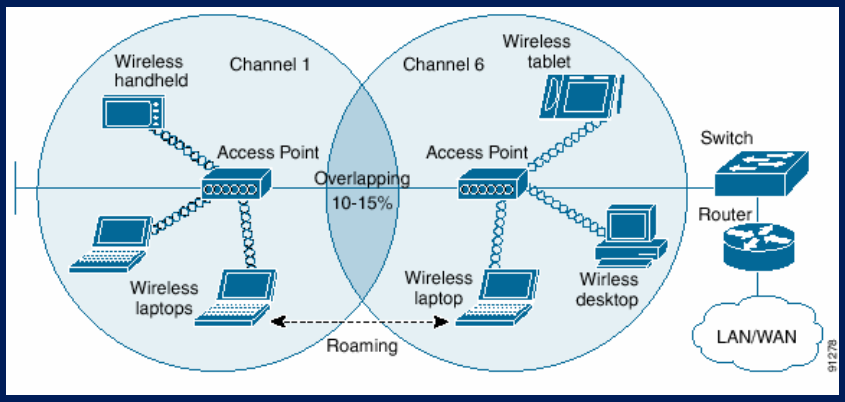
- **Access-Points**
- **Root Unit**
- **Repeater Unit**



- **BSS (Basic Service Set)**
- **ESS (Extended Service Set)**

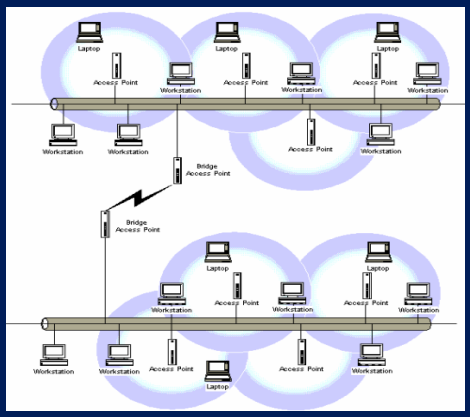
page 22

WLAN – Topologien (3)



page 23

WLAN – Topologien (4)



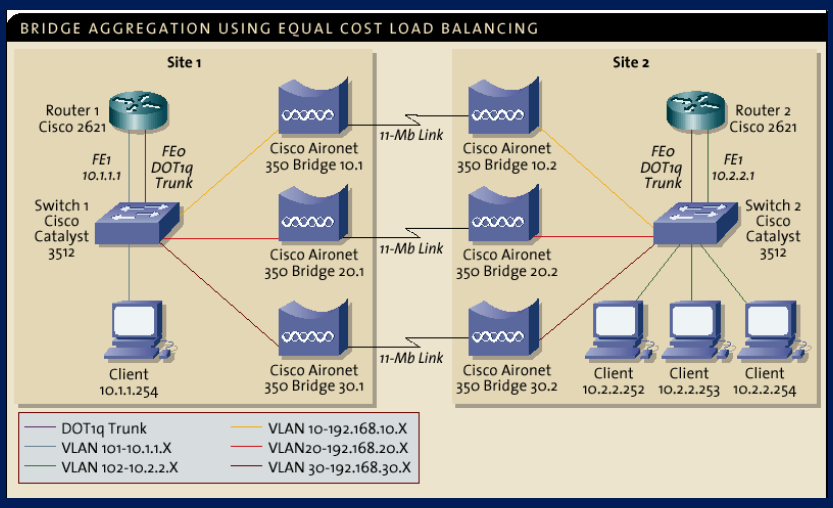
Bridges

Point-to-Point

Point-to-Multipoint

page 24

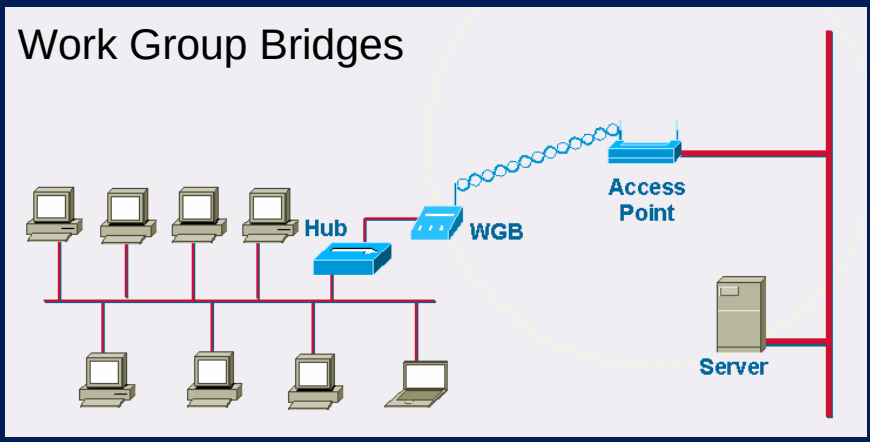
WLAN – Topologien (5)



WLAN-Packet max. 1540 Bytes (1518 für Ethernet) !

page 25

WLAN – Topologien (6)



page 26

WLAN – Topologien (7)

ISDN

Analog

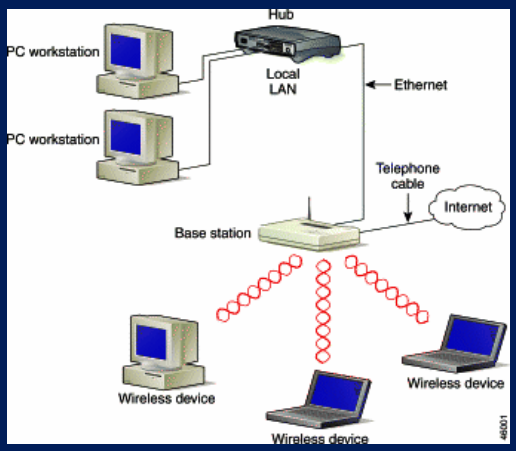
DSL

Cable Modem

LAN

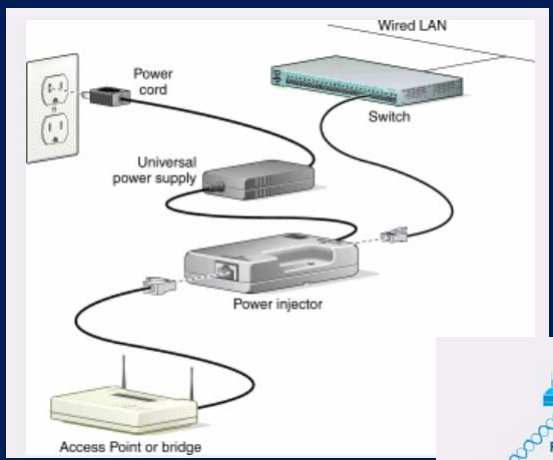
Wireless

Base Stations



page 27

Spannungsversorgung

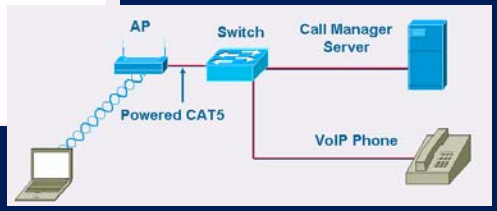


Cat5-Power

Pin 4&5 (neg.)

Pin 7&8 (pos.)

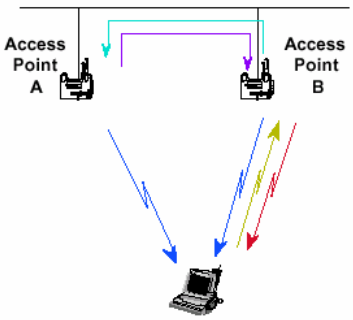
Standard IEEE 802.3af



page 28

Roaming (intra-subnet)

Roaming ist noch Vendor-spezifisch (IAPP – IEEE802.11F)



Roaming von Access Point A zu Access Point B

Schritte beim Wechsel:

1. Adapter hört die "beacon's" der APs.
2. Adapter wertet AP-beacons aus, nutzt den besten AP
3. Client sendet Verbindungsanfrage zum ausgesuchten AP (B).
4. AP (B) bestätigt Verbindungsanfrage und registriert Client
5. AP (B) informiert AP (A), dass der Client zu AP (B) gewechselt hat
6. AP (A) sendet die zwischengespeicherten Pakete zu AP (B) und löscht Client-Registrierung

page 29

Roaming (inter-subnet)

- **DHCP (im Zusammenspiel mit IEEE 802.1X)**
- **LAM** (Local-Area Mobility → CISCO)
- **Mobile IP** (RFC 2002, 2003, 2006)
  - Client bekommt Home-Address und Care-of-Address
  - AP ist Home Agent
  - Tunnel zwischen Care-Of-Agent und Home-Agent
- IEEE 802.1X mit TKIP

page 30

Roaming (inter-WISP)

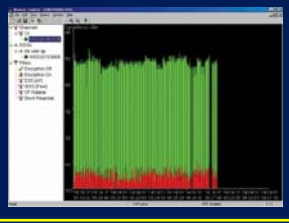
- Clearing-Stelle (z.B. eco-Verband, Greenspot)
  - regelt Beziehungen zwischen WISPs
  - SSG (Service-Selection Gateway)
  - WEB-Registration, Authentication, Billing
- technische Herausforderungen
  (gleiche IP; feste IP; QoS; Security .....)

page 31

Site Survey (Task-List)

- Bandbreite pro Client / Clients pro Zelle ?
- Roaming ja/nein, inter/intra-subnet
- Redundanz/Load Balancing ja/nein ?
- QoS ja/nein ?
- Ausleuchtung / Signalstärke (SNR)
- Störquellen vorhanden ?
- Sicherheit / Verfügbarkeit
- Meßgeräte / Software / Tools

Simulation Tool ?



TOOLS

Sniffer Wireless

Fluke Waverunner

Fluke Optiview INA

NetStumbler

.....

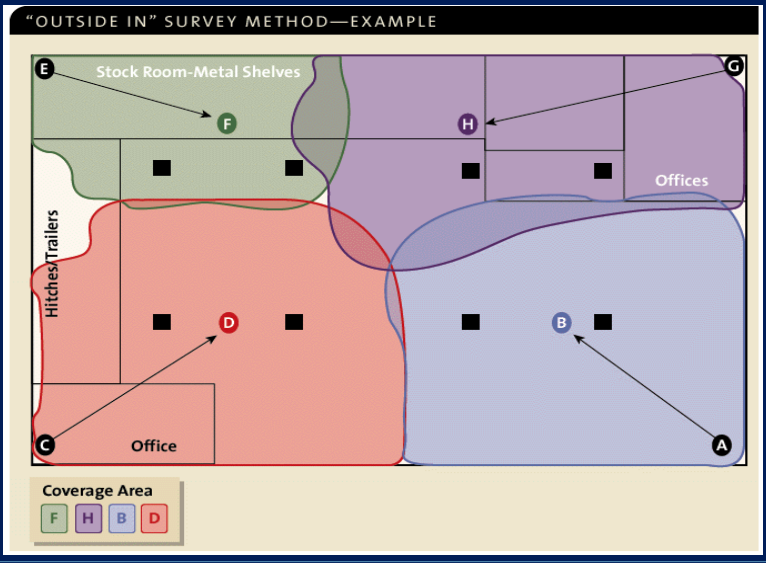
page 32

Site Survey Report

- Lokation der Geräte
- Spannungsversorgung
- Anbindung an das LAN
- Ausleuchtungsskizze
- Beschreibung der Geräte und Antennen
- Vorschlag für die Konfiguration der Geräte
- Fotos bei besonders kritischen Stellen
- Meßprotokolle (Screenshots)
  - Signalstärke
  - Signalqualität (retransmits)

page 33

Site Survey



page 34

Site Survey Report

page 35

Site Survey (Audit)

- WLAN-Analyzer
  - Observer 8.3 (Network Instruments)
  - Airopeek NX 2.01 (Wildpackets)
  - Wireless Sniffer 4.75 (Network Associates)
  - u.v.a.
- Durchsatzmessungen
  - Netio 1.21 (TCP und UDP), 1-32Kbyte-Pakete
  - Chariot von Netiq (Traffic Simulation, Agents, Con-Matrix)
  - u.v.a.

WLAN-Hersteller liefern Tools of mit

page 36

Site Survey (Tipps und Tricks)

- Am besten mit einer Pilot-Installation anfangen
- Langer Stab und Stativ (erspart oft die Leiter)
- Kabeltrommel mitbringen
- lange Kabelbinder und Tape für temporäre Befestigungen
- PDA oder Laptop als Empfänger benutzen –
  Spectrum Analyzer sind viel zu empfindlich und kompliziert
- Baupläne besorgen – selbst zeichnen sehr zeitaufwendig
- Person mit allen Zugangsberechtigungen bereitstellen
- wenn notwendig das Cat5-Kabel verlängern, nicht das RF-Kabel
- nicht wundern – HF geht oft merkwürdige Wege

page 37

No Wireless Policy

Scanner

- „wilde“ APs und WLAN-Bridges
- „wilde“ WLAN Clients (Router ??)
- softAPs (teilweise mit VPN-Gateway)
- Freund/Feind-Erkennung

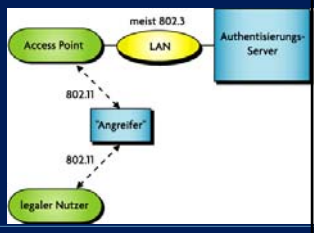
- History
- Alert und Notification
- Capturing

z.B. NetChem

page 38

WLAN Security Attacks

- Aktives Stören des RF-Signals (Störsender) !!!
- Tausende AP simulieren
- Angriffe auf die „weak keys“ im WEP
- bekannten Klartext schicken
- Brute Force auf IVs und MAC-Adressen (benötigt ca. 15 GB Speicherplatz auf der Platte)
- Man-in-the middle attack (MITM)
- Fantasie ohne Grenzen



page 39

WLAN Sicherheit

- WEP-Keys (fixed, key-rotation, dynamic)
- IEEE 802.1X und RADIUS (EAP, LEAP, PEAP ...)
- SmartCards (besser als Digital-Badge)
- EAP-TLS (SSL), PKI erforderlich
- EAP-MD5, verwendet CHAP
- IEEE 802.1i (AES, dynamic key management) → WPA2
  - keys 128 bis 256 bits, RADIUS und EAP-TLS
- VPN mit IPsec (3DES), VPN-Client erforderlich

page 40

WLAN Sicherheit ... it depends

- Gürtel
  - VPN, IPsec (168bit 3DES)
- Gürtel und Hosenträger
  - plus WEP, dynamic key, EAP-TLS, PEAP, LEAP
- Gürtel mit Doppelschnalle und Hosenträger
  - plus Certification (SmartCard, Ergometric ...)

page 41

WLAN Betrieb

- „wilde“ WLAN-Geräte
- große Installationen brauchen WLAN-Management Tools
  - HP ProCurve 700-series
  - CISCO BBSM, Cisco-Works Wireless ...
- RADIUS
- Key Management
- Filter (MAC, User, Port usw.)
- Einbindung in NW-Management
  - Monitoring, Alarming, Logging ...

page 42

CISCO Wireless LAN Products

- CISCO Aironet 350-Series
- CISCO Aironet 1100-Series
- CISCO Aironet 1200-Series
- CISCO Aironet 1400-Series
- CISCO 7900 Wireless Phone
- CISCO Wireless Network Management
- CISCO Wireless Antennas, Cable, Accessories
- CISCO BBSM
- ..... → http://www.cisco.com/en/US/products/hw/wireless/index.html

page 43

HP ProCurve Wireless LAN Products

***HP* ProCurve AP420**

- 802.1X support includes MD5, TLS, TTLS, and PEAP
- IEEE 802.11 b/g
- 64 VLANs (RADIUS-supported), WPA Support
- IEEE 802.3af Power over Ethernet support

***HP* ProCurve AP520wl**

- Dual PCMCIA Slot AP
- WPA, Bridge Function
- externe Antennen

page 44

HP ProCurve Wireless LAN Products

HP ProCurve Access Controller 720wl

HP ProCurve Access Control Server 740wl

HP ProCurve Integrated Access Manager 760wl

http://h18000.www1.hp.com/products/wireless/wlan/ap.html

page 45

	802.11a	802.11h	802.11g	802.11b
Status	Standard	Draft (Std Q4/03?)	Standard (seit 12.6.03)	Standard
Frequenzband (MHz)	5150-5350, 5725-5825	5150-5350, 5725-5825	2400,0-2483,5	2400,0-2483,5
Datenrate brutto (Mbit/s)	54	54	54	11
Datenrate netto (Mbit/s)	32	28	32	5
Sendeleistung [RegTP] (mW)	30	200	100	100
Reichweite (ca., m)	10 bis 15	30 bis 50	30 bis 50	30 bis 50
Einsatz [RegTP]	indoor	indoor	indoor, outdoor	indoor, outdoor
Spektrum	300 MHz	300 MHz	83,5 MHz	83,5 MHz
Kanäle [RegTP]	8	8	3	3
Zugriffsverfahren	CSMA/CA	CSMA/CA RTS/CTS	CSMA/CA RTS/CTS	CSMA/CA
Multicasting	ja	ja	ja	ja
QoS	zukünftig	zukünftig	zukünftig	nein
PHY	OFDM	OFDM mit DFS	CCK/OFDM CCK/DSSS	CCK/DSSS
Link-Kontrolle	nein	TPC	nein	nein