

# Wireless LAN - Grundlagen, Design und 802.11n



**professional IT-Service**

André Beck  
IBH IT-Service GmbH  
Gostritzer Str. 67a  
01217 Dresden  
support@ibh.de

[www.ibh.de](http://www.ibh.de)

## Wireless LAN

- ◆ Rekapitulation der Technologie
- ◆ Wireless Network Design
- ◆ Neuigkeiten mit 802.11n

# Evolution der WLANs 1

## Pre-Standard

- ◆ Beginn ca. 1995
- ◆ Digital Networks RoamAbout
- ◆ Typisch 500kbps bis 2Mbps
- ◆ Spread Spectrum als Grundlage
  - Frequency Hopping Spread Spectrum
  - Direct Sequence Spread Spectrum
- ◆ Weitere Hersteller → viele untereinander inkompatible Systeme

# Evolution der WLANs 2

## Spread Spectrum 1

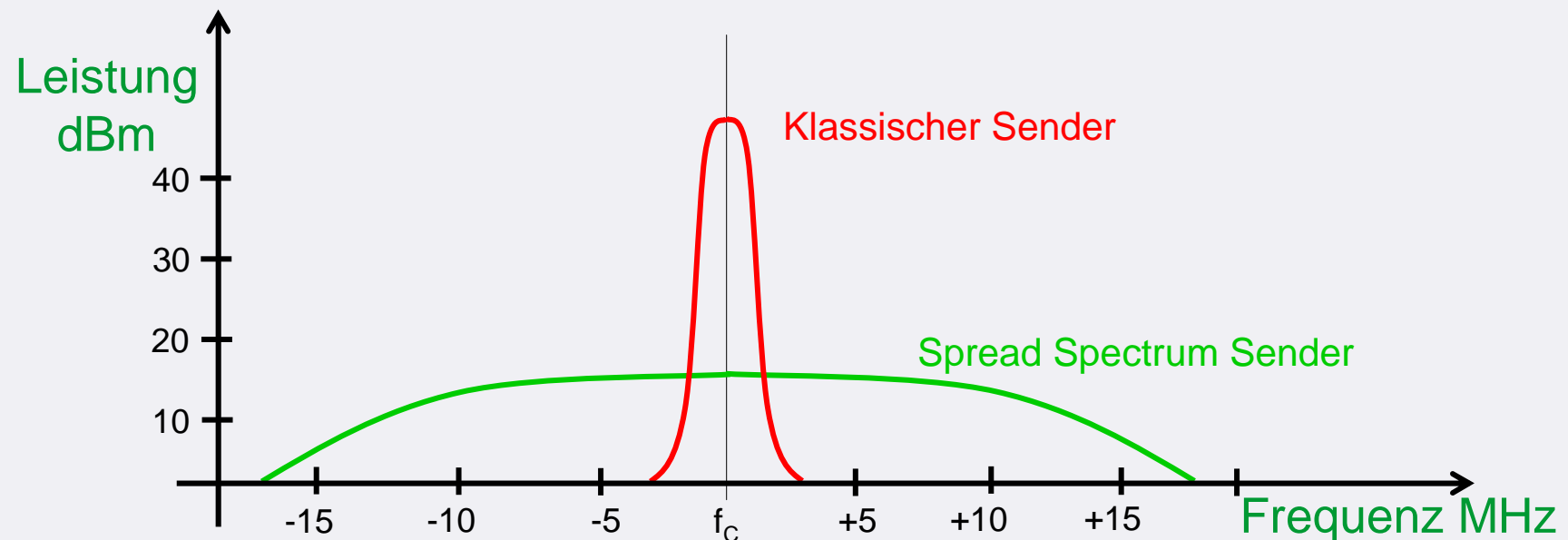
- ◆ Freigegebene Frequenzbänder
  - CB-Funk (*Citizen Band*)
  - 433MHz (Fernbedienungen, Wetterstationen...)
  - 2.4GHz (Industrial, Science & Medical)
  - 5GHz (UNI-1 – UNI-3)
- ◆ Probleme gegenüber dediziertem Datenfunk
  - Nur sehr niedrige Sendeleistungen zulässig
  - Viele Konkurrenten
  - Hohe Störungsrate
    - 2.4GHz ISM → Mikrowellenherd

# Evolution der WLANs 3

## Spread Spectrum 2

### ◆ Militärische Forschung

- Dedizierter Funk nutzt Frequenzspektrum schmalbandig mit hoher Leistung
- Spread Spectrum nutzt *breitbandig* mit *niedriger* Leistung



# Evolution der WLANs 4

## Spread Spectrum 3

### ◆ Militärische Forschung

- Verschmieren des Signals als Abhörschutz
  - Klassischer Sender kann einfach gefunden und demoduliert werden
  - Spread Spectrum ist weniger auffällig und ohne Kenntnis des Spreading-Verfahrens praktisch nicht mitzuhören
- Schutz vor schmalbandigen Störungen
  - Ein großer Teil der Information bleibt erhalten
  - ECC und zeitliches Multiplex
- Frequency Hopping Spread Spectrum
- Direct Sequence Spread Spectrum
- Orthogonal Frequency Division Multiplex

# Evolution der WLANs 5

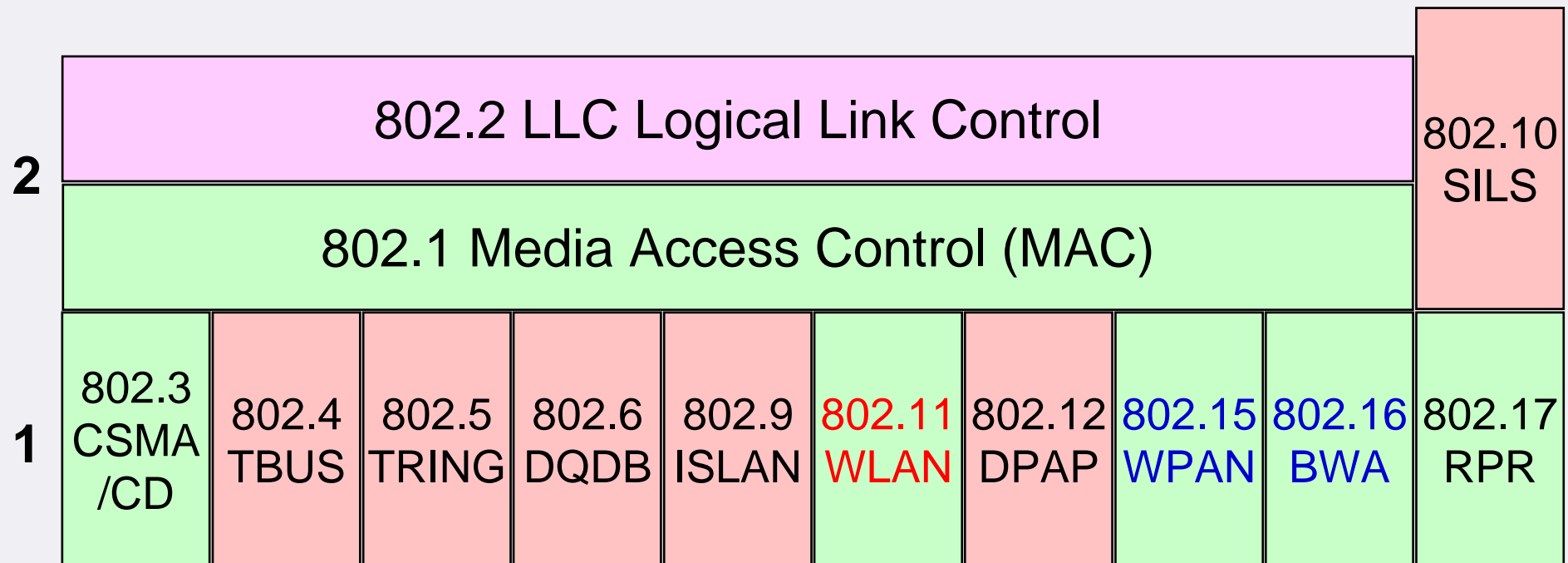
## Spread Spectrum 4

### ◆ WLAN im ISM-Band

- Spread Spectrum war Voraussetzung für die Machbarkeit
- Niedrige Sendeleistung ausreichend
- Wenig anfällig gegen (klassische) Störer
- Stört selbst nur geringfügig
- Erlaubt hohe Bitraten auf kurze Entfernungen

# Evolution der WLANs 6

## IEEE Standardisierung



- eingefroren (eventuell Anpassung an aktuelle Entwicklungen)
- in aktiver Weiterentwicklung
- Standardisierung im wesentlichen abgeschlossen

# Evolution der WLANs 7

## IEEE 802.11

- ◆ Erster Standard des IEEE zur Vereinheitlichung
  - *Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications (1999)*
  - Allgemeine Beschreibung des Gesamtsystems
  - MAC Service Definition
  - Frame-Formate
  - Authentisierung und Verschlüsselung
  - Clause 14: FHSS 2.4GHz PHY (1Mbps und 2Mbps)
  - Clause 15: DSSS 2.4GHz PHY (1Mbps und 2Mbps)
  - Clause 16: Infrared PHY (1Mbps und 2Mbps)

# Evolution der WLANs 8

## IEEE 802.11 Gesamtsystem 1

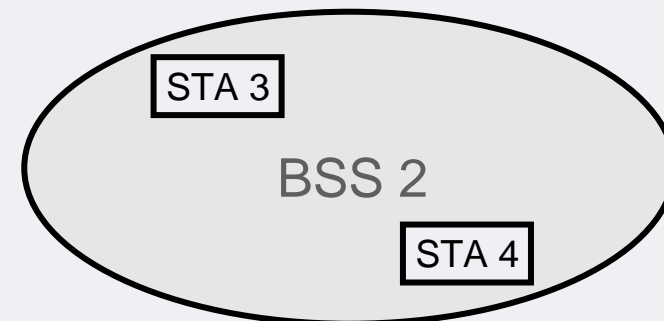
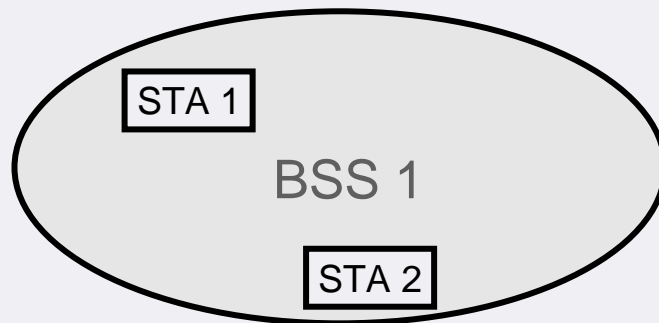
- ◆ Erster Wireless-Standard – neue Paradigmen
  - Neue Begriffswelt (STA, AP, DS, BSS...)
  - Adresse beschreibt keinen festen Ort mehr
  - Das Medium ist fundamental anders
    - Keine absoluten oder einfach feststellbaren Grenzen
    - Ungeschützt gegen externe Signale
    - Wesentlich unzuverlässiger als jeder wired PHY
    - Dynamische Topologie
    - Verletzt transitive Regel (jeder hört jeden) wegen Abschattung
    - Zeitlich und räumlich wechselnde Ausbreitungseigenschaften
  - Portable vs. Mobile Stationen
  - Ziel: Gegenüber LLC wie jeder andere 802 aussehen
    - MAC wird deutlich komplexer

# Evolution der WLANs 9

## IEEE 802.11 Gesamtsystem 2

### ◆ Begrifflichkeiten des neuen Systems

- STA – Station (Radio MAC & PHY)
- BSS – Basic Service Set

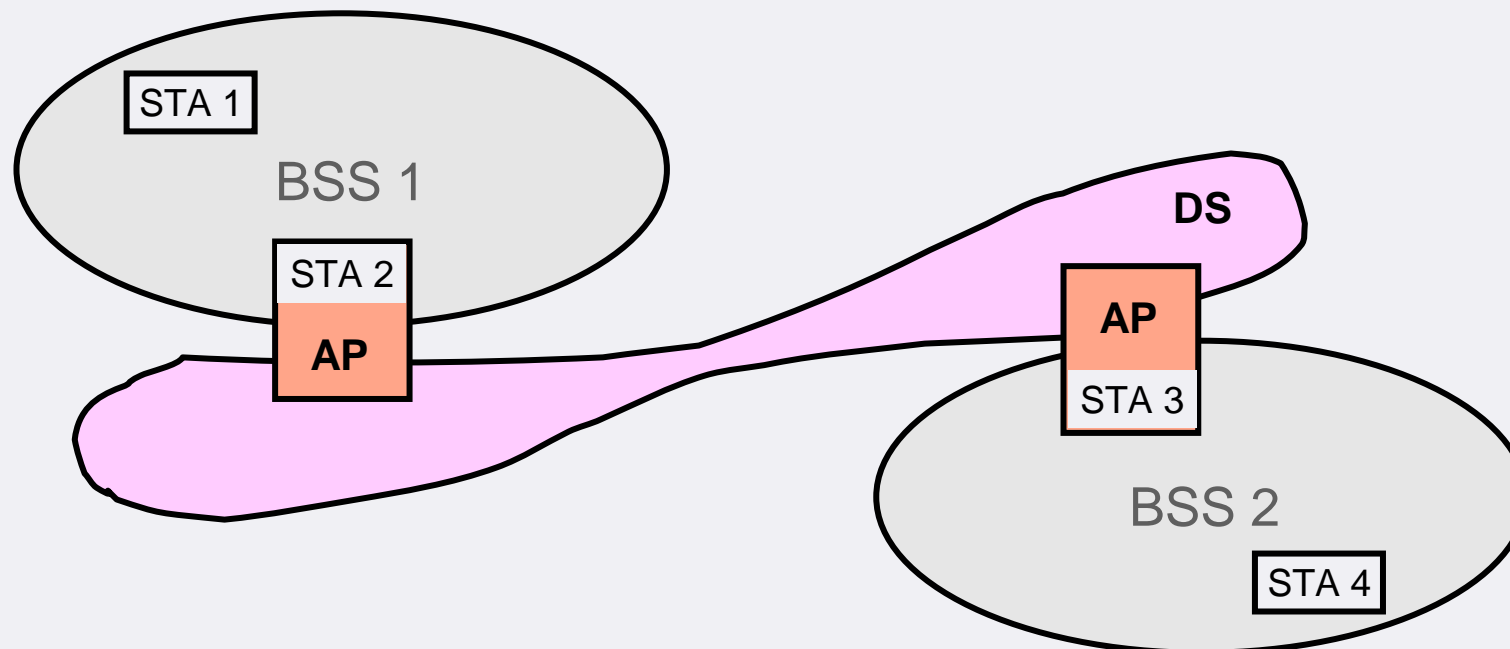


# Evolution der WLANs 10

## IEEE 802.11 Gesamtsystem 3

### ◆ Distribution System

- Optional (Infrastructure vs. Ad-Hoc)
- AP: Access Point – Vermittler zwischen WM und DSM

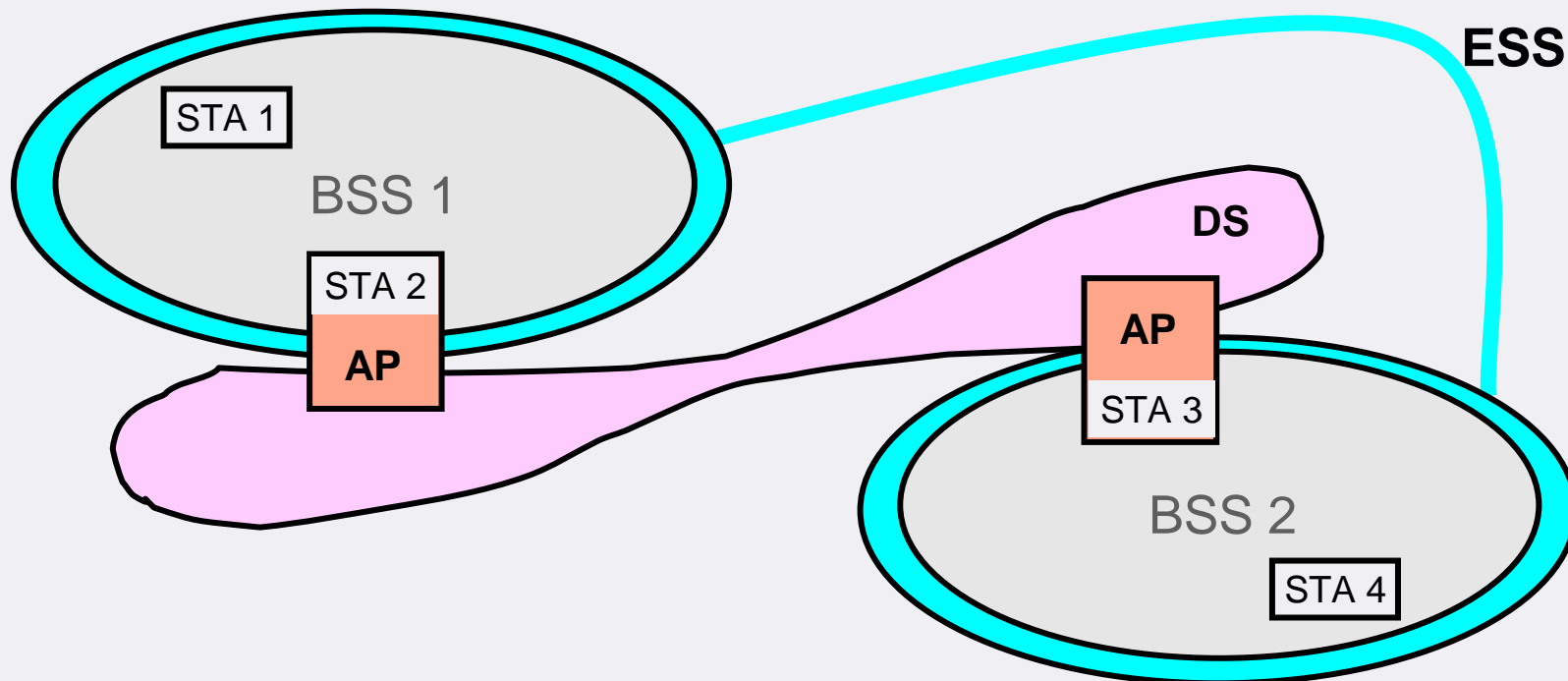


# Evolution der WLANs 11

## IEEE 802.11 Gesamtsystem 4

### ◆ ESS & Roaming

- Extended Service Set
- Überlappende BSS eines ESS erlauben Roaming

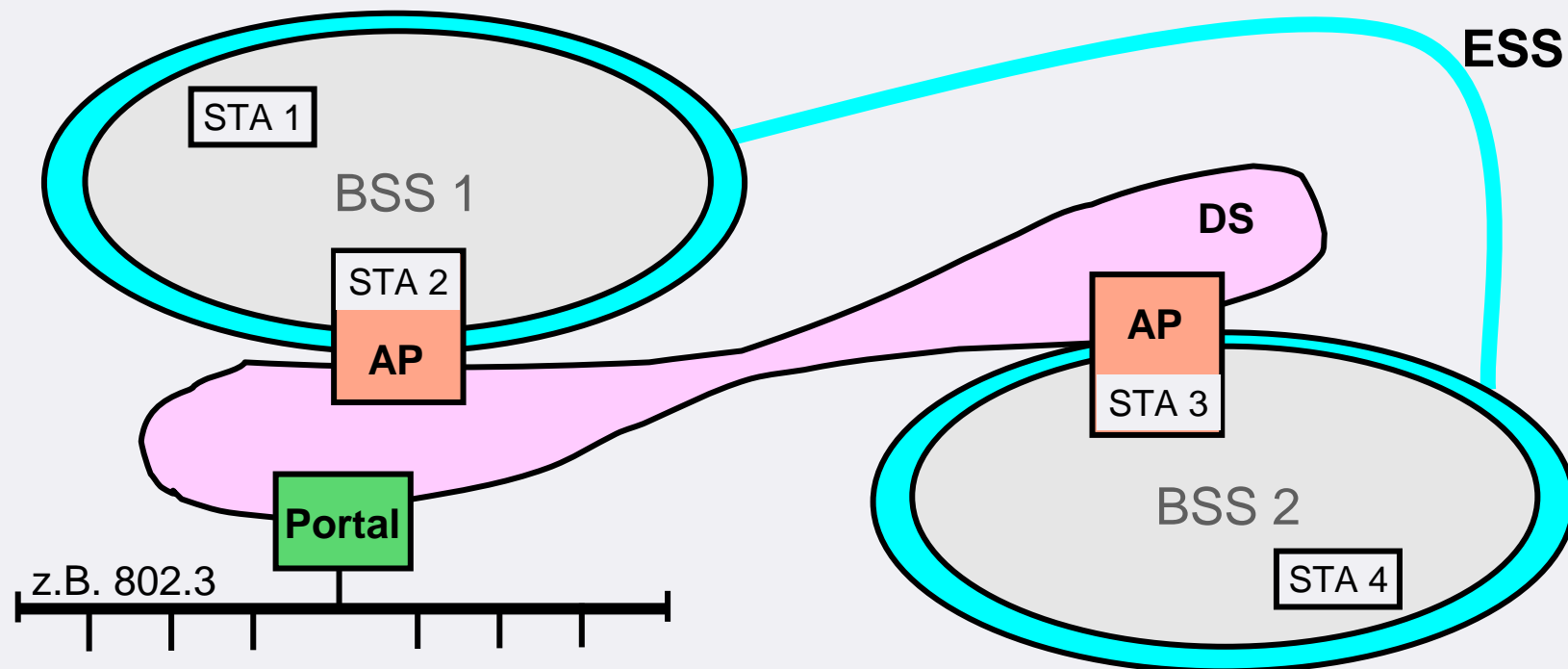


# Evolution der WLANs 12

## IEEE 802.11 Gesamtsystem 5

### ◆ Portals

- Verbindung zwischen DS und anderen 802.x-LANs
- Integration mit wired LANs

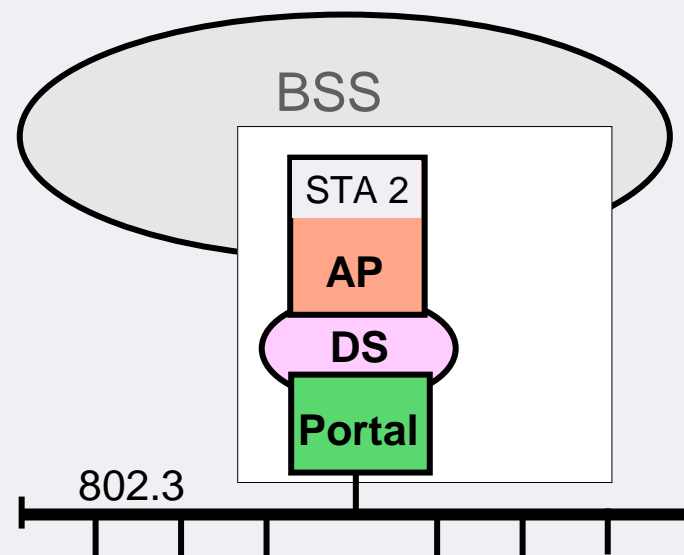


# Evolution der WLANs 13

## IEEE 802.11 Gesamtsystem 6

### ◆ Klassische (autonome) Access Points

- Meist kein AP-überspannendes DS
  - Ausnahme WDS
  - Minimale Hilfsprotokolle für Roaming (IAPP, 802.11F)
- Integration mit 802.3 durch Ethernet-Interface



# Evolution der WLANs 14

## IEEE 802.11 Service System

### ◆ Station Services

- Authentication & Deauthentication
- Privacy
- Auslieferung von Datenframes

### ◆ Distribution System Services

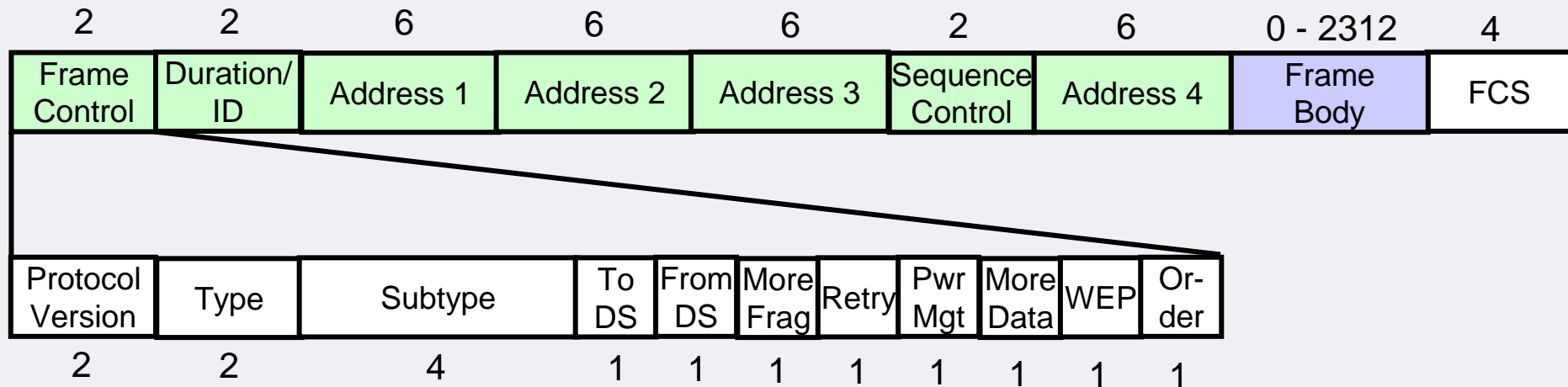
- Association & Disassociation
  - Etabliert die aktuelle Zuordnung STA zu AP
- Reassociation
  - Roaming innerhalb der ESS
- Distribution
- Integration

# Evolution der WLANs 15

## IEEE 802.11 Frame Format

### ◆ Einheitlicher Frameaufbau

- Control Frames
- Management Frames
- Data Frames



# Evolution der WLANs 16

## IEEE 802.11 Frame Format

- ◆ Type 00: Management, z.B.:
  - Beacon
  - Probe Request/Response
  - Association Request/Response
- ◆ Type 01: Control, z.B.:
  - RTS/CTS
  - ACK
- ◆ Type 10: Data, z.B.:
  - Data, Data+CF-Ack
  - CF-Ack without Data

# Evolution der WLANs 17

## IEEE 802.11 Authentication

### ◆ Open System

- Null-Authentisierung seitens 802.11
  - Die STA kann Open System mit anderen Verfahren, die außerhalb 802.11 liegen, hinterlegen, z.B. MAC-Auth
  - Open System & WEP Data

### ◆ Shared Key

- Challenge Handshake mit WEP
  - Requester schickt Responder Authentication Request
  - Responder schickt Requester 128 Byte Zufallsdaten
  - Requester schickt Responder diese Daten über WEP zurück
  - Responder vergleicht und schickt Success/Failure

# Evolution der WLANs 18

## IEEE 802.11 Wired Equivalent Privacy

- ◆ Ziel: Vertraulichkeitsniveau von wired LANs
  - Basiert auf Stream Cipher mit RC4 als PRNG
  - Keys von 40Bit bzw. 104Bit Länge (Export)
  - Sequenziell erzeugter 24Bit Initialization Vector (IV)
  - Verkettung von IV und Key als Seed für RC4 PRNG
  - Für Plaintext wird Integrity Check Value (ICV) ermittelt
  - Plaintext und ICV werden verkettet und mit Bitstrom aus dem PRNG XORed
  - IV (im Klartext) und Ciphertext bilden neuen Frame Body

# Evolution der WLANs 19

## IEEE 802.11 WEP Key Management

### ◆ Statisches Key-Management

- 4 Key-Slots
- Festlegen des Transmit Key
- Empfangene Frames können mit jedem der vier Schlüssel verschlüsselt worden sein
- Bei Übermittlung des IV werden 4Byte verwendet
  - 24Bit IV
  - 2Bit Key-ID
- Verschiedene Anwendungsszenarien
  - Semi-individuelle Keys
  - N+1-Rotation

# Evolution der WLANs 20

## IEEE 802.11 Zugriffsverfahren

### ◆ CSMA/CA

- Collision Avoidance durch Zeitfenster
  - IFS & Random Exponential Backoff
  - Network Allocation Vector (NAV)
- Erweiterte Avoidance durch Coordination Functions
  - Distributed Coordination Function
  - Point Coordination Function (optional, praktisch unbenutzt)
- Interframe Spacing
  - SIFS (Short IFS) bei ACK, CTS etc
  - PIFS (PCF IFS) für Priority Access (QoS) unter PCF
  - DIFS (DCF IFS) für normalen DCF-Betrieb
  - EIFS (Extended IFS) bei Fehlern

# Evolution der WLANs 21

## IEEE 802.11 Supplements

### ◆ 802.11a

- High-Speed PHY in the 5GHz Band (1999)
- Clause 17: OFDM PHY Specification for the 5GHz Band
- Datenraten in Mbps: 6, 9, 12, 18, 24, 36, 48, 54
- Modulationen: BPSK, QPSK, 16-QAM, 64-QAM
- Trennt in verschiedene Frequenzbereiche für Indoor und Outdoor

# Evolution der WLANs 22

## IEEE 802.11 Supplements

### ◆ 802.11b

- Higher-Speed PHY Extension in the 2.4GHz Band (1999)
- Clause 18: High Rate DSSS PHY Specification
- Datenraten: 5.5Mbps und 11Mbps
- Modulation: 8-chip CCK und optional PBCC
- Short Preamble Feature
- Channel Agility Feature (FHSS-Kompatibilität)
- Der Wegbereiter für den WLAN-Markt

# Evolution der WLANs 23

## IEEE 802.11 Supplements

### ◆ 802.11g

- Further Higher Data Rate Extension in the 2.4GHz Band (2003)
- Clause 19: Extended Rate PHY Specification
- Datenraten in Mbps: 6, 9, 12, 18, 24, 36, 48, 54 (ERP-OFDM, DSSS-OFDM), zus. 22 und 33 ERP-PBCC
- Modulationen: Analog 802.11a plus CCK
- Leicht reduzierte Sendeleistung bei OFDM
- DSSS-OFDM Feature
  - Frame beginnt als DSSS mit 802.11b B/QPSK Header
  - Nach dem Header wird auf OFDM umgeschaltet
- Die z.Z. verbreitetste WLAN-Technologie

# Evolution der WLANs 24

## IEEE 802.11 Supplements

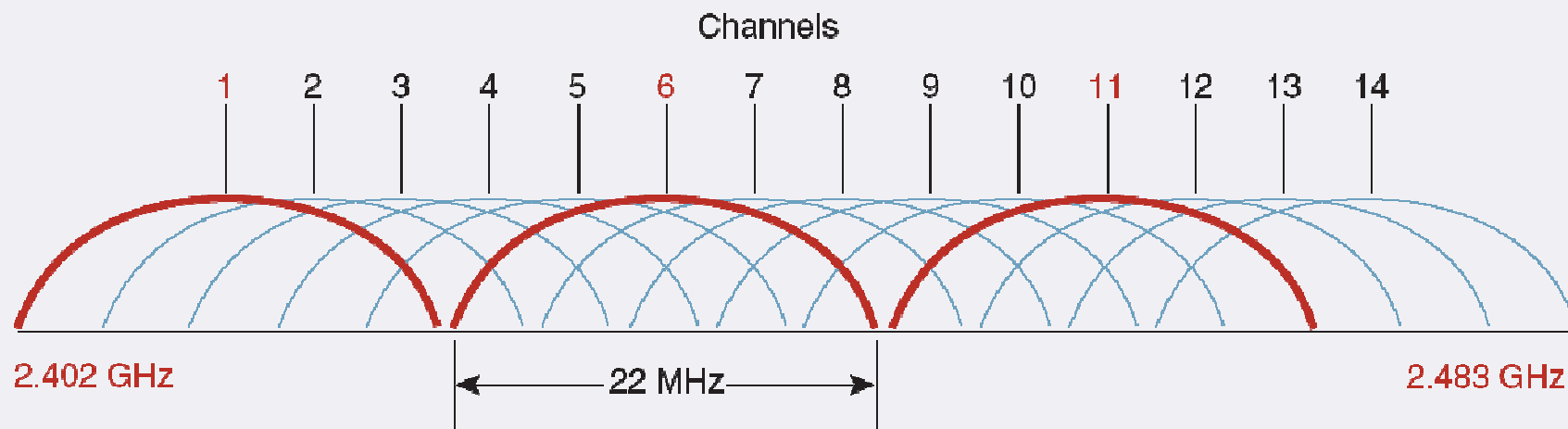
### ◆ 802.11i

- Amendment 6: Medium Access Control (MAC) Security Enhancements (2004+)
- Dringend benötigte Aufarbeitung der WEP-Probleme
  - 802.1x Integration für dynamisches Keying
  - TKIP gegen WEP-Schwächen
  - AES-CCMP als Ablösung für RC4
  - Aka WPA(2)

# WLAN Frequenznutzung 1

## Regulatory Domains & 2.4GHz ISM 1

- ◆ 14 Kanäle im Abstand von 5MHz
- ◆ 802.11b/g belegt ca. 22MHz Bandbreite
- ◆ Mindestabstand von 5 Kanälen bei überlappenden BSS
  - Z.B. 1,6,11



# WLAN Frequenznutzung 2

## Regulatory Domains & 2.4GHz ISM 2

◆ Nicht überall sind alle Kanäle verfügbar

Channel#	f <sub>c</sub> (MHz)	FCC (USA)	ETSI	TELEC (Japan)	MOC (Israel)
1	2412	✓	✓	✓	
2	2417	✓	✓	✓	
3	2422	✓	✓	✓	
4	2427	✓	✓	✓	
5	2432	✓	✓	✓	
6	2437	✓	✓	✓	
7	2442	✓	✓	✓	✓
8	2447	✓	✓	✓	✓
9	2452	✓	✓	✓	✓
10	2457	✓	✓	✓	✓
11	2462	✓	✓	✓	✓
12	2467		✓	✓	✓
13	2472		✓	✓	
14	2484			✓	

# WLAN Frequenznutzung 3

## Nutzungsmöglichkeiten der Kanäle

- ◆ In DE Kanäle 1-13 nutzbar
  - Für peripher überlappende BSS (Roaming)
  - Für stark überlappende BSS
    - Des gleichen ESS: Load Distribution
    - Verschiedener ESS: Entkopplung (Störungsminderung)
  - Problem: Der Frequenzraum ist stark begrenzt
  - Lösungsmöglichkeiten:
    - Kanalkoordination, sofern möglich
    - Sendeleistung stark verringern
    - Anzahl APs deutlich erhöhen
    - BSS physikalisch abgrenzen
    - Picozellen – ein AP pro Raum

# WLAN Frequenznutzung 4

## Antennen

- ◆ In DE maximal 100mW (20dBm) EIRP
  - *Effective Isotropic Radiated Power*
- ◆ Es gibt keine isotrop strahlenden Antennen
  - Klassischer Dipol hat typischen Gewinn von 2.2dBi (2.2dB gegenüber isotropem Strahler)
  - Antennen mit höherer Richtwirkung haben höheren Gewinn (z.B. 5dBi Patch und 18dBi Yagi)
  - Antennengewinn geht in die ETSI-Vorgabe ein!
  - Daher haben APs typisch 50mW oder weniger Ausgangsleistung
    - 50mW AP + 5dBi Patch → 17dBm + 5dBi → illegal
- ◆ Antenna Diversity oft hilfreich

# WLAN & Netzwerkdesign 1

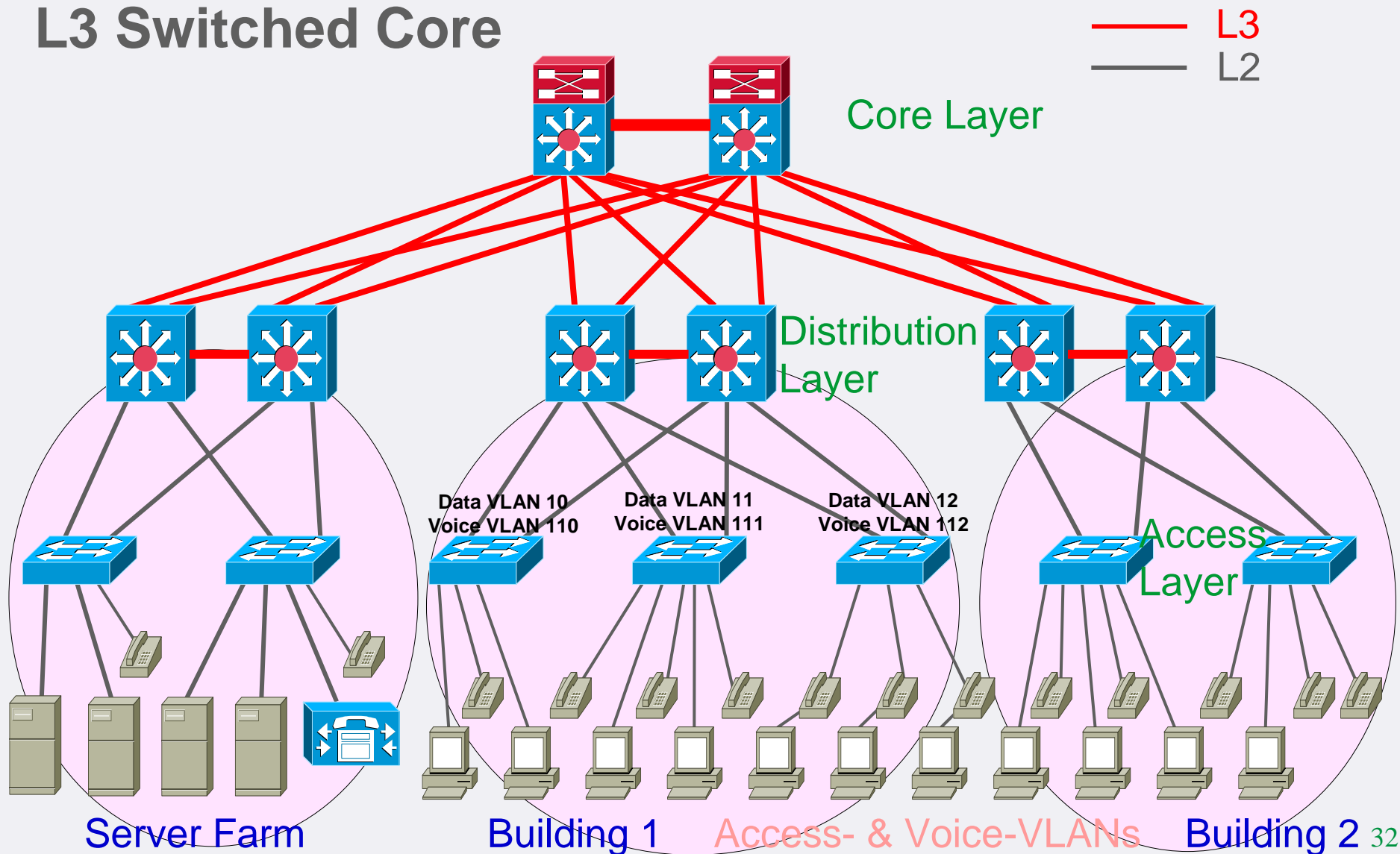
## Moderne LAN-Designs

### ◆ L3 Switched Core & Distribution

- L3-Switches mit *Routed Ports*
- Konsolidierung zu IP wird als abgeschlossen betrachtet
- Durchgängig dynamisches Routing
- L3-Switches in Core und Distribution redundant
- Default Gateway Redundanz in Distribution
- L2 nur noch im Access Layer
  - Keine Schleifen → STP unnötig
  - STP bleibt aus Sicherheitsgründen aktiviert
- Praktisch freie Skalierbarkeit

# WLAN & Netzwerkdesign 2

## L3 Switched Core



# WLAN & Netzwerkdesign 3

## L3 Switched Core

### ◆ Designaspekte

- Alle Verbindungen in Core und Distribution sind *Routed Ports*
- Ausfälle werden unmittelbar durch *Link Loss* bemerkt
- Redundante Topologie ist immer *dreiecksförmig*
- Dynamisches Routing etabliert dadurch immer *äquidistante Routen* (Core → Access)
- Normalbetrieb ist dadurch automatisch *Load Balancing*
- Bei Ausfällen bleibt einer der *etablierten Pfade* übrig  
→ keine Ausfallzeit (Core → Access)
- Verschiedene Access-Switches sind in *verschiedenen VLANs*
- Interswitch-Redundanz vs. Intraswitch-Redundanz
  - Core & Distribution: *Keine* redundanten Supervisorengines
  - Access: Redundante Supervisorengines hilfreich

# WLAN & Netzwerkdesign 4

## L3 Switched Core

### ◆ Folgen

- Broadcastdomains werden sehr klein
- Jeder signifikante Traffic wird geroutet
  - Access erreicht Server Farm nur über mehrere Routing Hops
  - Ansatzpunkt für Network *Security*
- Ausfall eines Core oder Distribution Switch wird praktisch transparent umgangen
- Ausfall eines Access Switch hat nur lokale Folgen
- Letzter denkbarer Schritt: L3 Access (Security → ISP)

### ◆ Und WLAN?

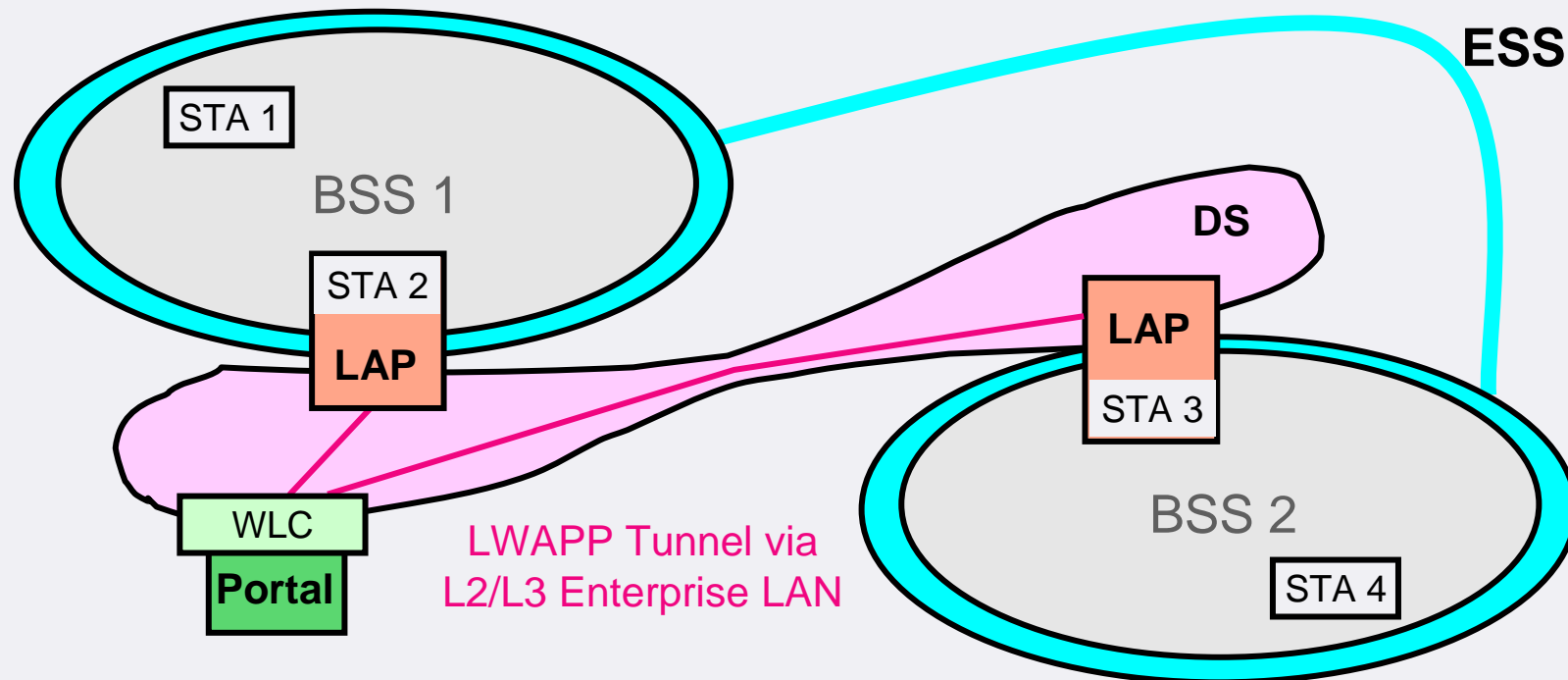
- Keine Campus-Spanning Broadcast Domains mehr
- 802.11 Roaming **erfordert** eine gemeinsame Broadcast Domain
- L3 Roaming Support ist ein Hack
- Autonome APs liefern keine saubere Lösung

# WLAN & Netzwerkdesign 5

## IEEE 802.11 Gesamtsystem voll implementiert

### ◆ Wireless LAN Controller

- Architektur für größere DS mit zentraler Steuerung
- DS als Tunnel über LAN (LWAPP/CAPWAP)
- Tunnel durch L3-LANs erlauben **emulierte Broadcast Domains**



## Einsatz von WLCs

### ◆ Skalierung

- Bis zu 250 LAP je WLC (Modell- und Lizenzabhängig)
- WLC-Clustering darüber hinaus (bis 6250 LAP)
- Meta-Management mit WCS

### ◆ Radio Resource Management

- Optimale Kanalverteilung
- Optimale Sendeleistungen (Feedback von STAs)
- Eingebauter Site Survey

### ◆ Weitere Features

- zentralere Kontrolle über Roaming
- zentraler Ansatzpunkt für Security (IDS/IPS)

# WLAN & Netzwerkdesign 7

## Darreichungsform von WLCs

### ◆ Standalone

- Anschluss per Gigabit-Aggregat an Switches, z.B.:
  - Cisco WLC 4402/4404 (2 bzw. 4 GE, bis 100 LAPs)
  - Cisco WLC 5508 (8 GE, bis 250 LAPs)

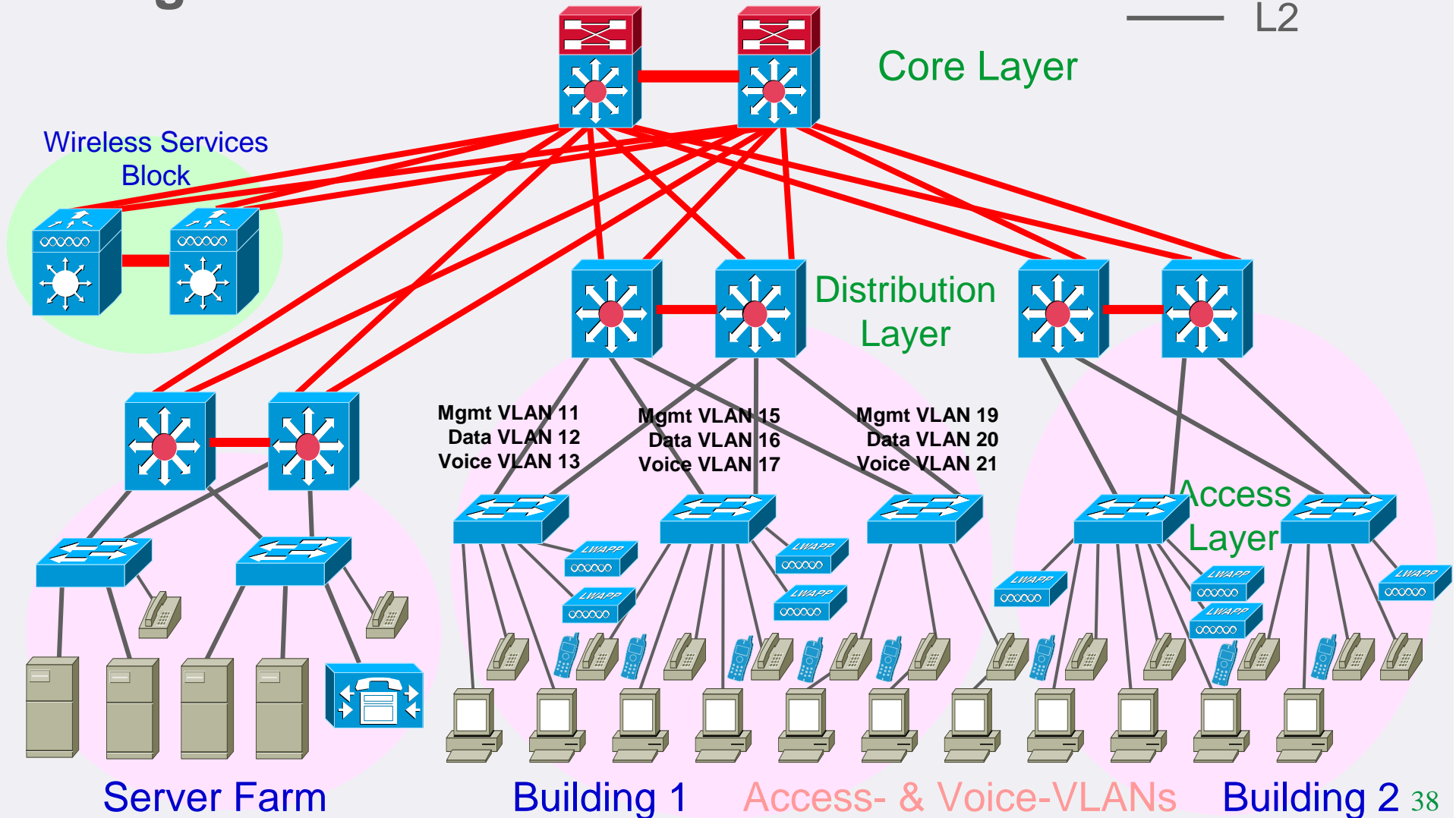
### ◆ Integriert

- Modul für ISRs (bis 12 LAPs)
- Catalyst 3750G-24 PoE mit angeflanschem WLC
  - bis 25/50 LAP je Switch
  - 3750 StackWISE!
- Catalyst 6500/7600 Series WiSM
  - Zwei WLC 4404 + CFC-Backend auf einem Cat6k-Modul
  - Benötigt Sup720-Generation
  - Ein WiSM bedient 300 LAPs (150 je WLC)

# WLAN & Netzwerkdesign 8

## Integration mit L3 Switched Core

— L3  
— L2



# WLAN & Netzwerkdesign 9

## QoS und WLCs

### ◆ Wireless QoS

- Wireless Downstream vs. Upstream
- Klassische DCF mit WLC bedingt QoS-fähig
- 802.11e (WMM) QoS heute im Ausrollen begriffen
- 802.11n hat 802.11i (WPA2), 802.11e und U-APSD im Schlepptau

### ◆ Wired QoS

- LWAPP Tunnel (zwischen WLCs und LAPs)
- Eigentlicher Traffic (zwischen WLCs und LAN)
- 802.11D (802.11p)/802.11e CoS vs. Cisco QoS Baseline

### ◆ VoWLAN 4.1 Design Guide ([www.cisco.com/go/srnd](http://www.cisco.com/go/srnd))

# Stand der Technologie 1

## Security & QoS

- ◆ 802.11i RSN ist verfügbar
  - WEP ist auch der breiten Öffentlichkeit als unsicher bekannt
  - WPA2 löst WPA gerade ab
  - Aktuelle Hardware beherrscht AES-CCMP
  - Erste Angriffe auf WPA TKIP veröffentlicht
    - Chopping-Attack (Injection) mit Ausnutzung von 802.11e Queues
  - Zunehmende Unterstützung der neueren 802.1X-Methoden
    - PEAP, EAP-TLS, EAP-TTLS...
- ◆ Management Frame Protection kommt
- ◆ 802.11e ist verfügbar
  - WMM in immer mehr APs und Treibern
  - Enge Verbindung mit Power Saving (It's green!)
  - In der Praxis häufig noch eher wacklig (besonders Multivendor)

# Stand der Technologie 2

## 802.11a

- ◆ 802.11a auch in Deutschland angekommen
  - 2.4GHz ISM ist völlig überfüllt
  - 5GHz in DE verfügbar
    - Vfg 8/2006 der BNA löste Regelung von 2002 ab
    - 5150 – 5250MHz: Indoor, 23dBm EIRP, 0.25mW/25kHz
    - 5250 – 5350MHz: Indoor, 23dBm EIRP, 10mW/MHz, DFS+DPC
    - 5470 – 5725MHz: 30dBm EIRP, 50mW/MHz, DFS+DPC
    - 4+4+11 → 19 Kanäle ohne Überlappung
    - Radar!
  - Hohe AP-Dichte nötig, aber auch machbar
    - VoWLAN
    - AP HA & Load Balancing

# Stand der Technologie 3

## TGn

### ◆ IEEE Task Group n

- Tagt seit 2003
  - 2004: 32 Vorschläge
  - 2005: 3 Vorschläge übrig: TGnSync, WWiSE, MITMOT, aber Wahl eines Gewinners liefert keine 75% Mehrheit
  - 2006: Die drei Gruppen präsentieren einen vereinigten Draft
  - 2007: Draft 2.0 angenommen
  - ...
  - 2009: Draft 8.0 angenommen
- Überraschende Verabschiedung im September 2009

### ◆ Wi-Fi Alliance

- 2007: Baseline auf Basis von Draft 2.0 als **Pre-N**
- Zahlreiche Produkte auf dieser Grundlage am Markt

# Stand der Technologie 4

## 802.11n

### ◆ Multiple Input Multiple Output (MIMO)

#### ● Mehr als eine Antenne

- Multipath positiv nutzen (Diversity)

- Mehr als eine *HF-Kette*

  - ◆ Individuelle Sender, Empfänger und A/D bzw. D/A

  - ◆ Ideal: Eine Kette je Antenne

  - ◆ Ermöglicht Spatial Division Multiplex

  - ◆ Ermöglicht Spatial Beamforming

- Typische Angabe: *TxAnt X RxAnt: SpatialStreams*

  - ◆ 2 X 3: 2 (2 Transmit, 3 RX [Diversity], 2 Spatial Streams – z.B. Cisco 1140)

  - ◆ 4 X 4: 4 (802.11n Maximum)

  - ◆ Typisch: 2X2:2, 2X3:2, 3X3:2 (d.h. max. 300Mbps)

  - ◆ Neuerdings: 3X3:3 (450Mbps)

# Stand der Technologie 5

## 802.11n MIMO MCS Raten

### ◆ 8 Stufen je Spatial Stream

MCS Index	Spatial Streams	Modulation	Coding Rate	Rate @20MHz (GI=400ns)	Rate @40MHz (GI=400ns)
0	1	BPSK	$\frac{1}{2}$	7 $\frac{2}{9}$	15
1	1	QPSK	$\frac{1}{2}$	14 $\frac{4}{9}$	30
2	1	QPSK	$\frac{3}{4}$	21 $\frac{2}{3}$	45
3	1	16-QAM	$\frac{1}{2}$	28 $\frac{8}{9}$	60
4	1	16-QAM	$\frac{3}{4}$	43 $\frac{1}{3}$	90
5	1	64-QAM	$\frac{2}{3}$	57 $\frac{7}{9}$	120
6	1	64-QAM	$\frac{3}{4}$	65	135
7	1	64-QAM	$\frac{5}{6}$	72 $\frac{2}{9}$	157.5
8	2	BPSK	$\frac{1}{2}$	14 $\frac{4}{9}$	30
9	2	QPSK	$\frac{1}{2}$	28 $\frac{8}{9}$	60
10	2	QPSK	$\frac{3}{4}$	43 $\frac{1}{3}$	90
11	2	16-QAM	$\frac{1}{2}$	57 $\frac{7}{9}$	120
12	2	16-QAM	$\frac{3}{4}$	86 $\frac{2}{3}$	180
13	2	64-QAM	$\frac{2}{3}$	115 $\frac{5}{9}$	240
14	2	64-QAM	$\frac{3}{4}$	130	270
15	2	64-QAM	$\frac{5}{6}$	144 $\frac{4}{9}$	300

## 802.11n

### ◆ Channel Bonding (40MHz)

- Zusammenfassung von zwei 20MHz-Kanälen
- Standardisiert das Verfahren (Ablösung proprietären Bondings)
- Definiert für 2.4GHz und 5GHz Radios
  - Im 2.4GHz ISM nicht sinnvoll (auch im SOHO fragwürdig)
  - Im 5GHz unproblematisch 9 Kanäle mit 40MHz verfügbar

### ◆ Frame Aggregation

- Reduzieren des CSMA/CA-Overheads
- A-MSDU (MAC Top) und A-MPDU (MAC Bottom)

## 802.11n

### ◆ Rückwärtskompatibilität

- Koexistenz mit Vorgängerstandards
- Ohne: Greenfield Preamble
- Mixed Mode (L-SIG TXOP)
  - 802.11n eingebettet in 802.11a oder 802.11g (20MHz)
- CTS
  - Bei 40MHz immer notwendig (auf beiden 20MHz-Unterkanälen)
  - Bei Mixed Mode zusätzlich CTS für 802.11b notwendig
- Kostet Performance

# Stand der Technologie 8

## 802.11n - Designaspekte

### ◆ Stromverbrauch

- Dual Band 802.11n APs der ersten Generation
  - Leistungsbedarf > 15.4W (802.3af)
  - Cisco Aironet 1250
- Aktuelle Generation (1140) wieder innerhalb 802.3af

### ◆ LAN-Bandbreite

- Durchsatz eines Radios ca. 150Mbps
  - Dual Radio APs theoretisch 300Mbps
  - Gigabit mit PoE am Access Layer (oder Bottleneck)
  - QoS-Aspekte für LAN beachten (verschärft sich)

### ◆ WLC-Durchsatz

- Bisherige Skalierung ging von ca. 30Mbps je AP aus
- WiSM erreicht maximal 8Gbps zum LAN (inhärent Duplex)
  - 300 Dual Radio LAPs aggregieren das Zehnfache!  
→ Überbuchung beachten oder reduzieren
- 5508 erhöht die Skalierbarkeit bei Standalone-WLCs

# Stand der Technologie 9

## 802.11n - Designaspekte

- ◆ Lohnt erst wirklich mit 5GHz
  - 40MHz nur in 5GHz verwendbar
  - Keine Koexistenz mit 802.11b nötig
  - Zellgröße sinkt → Mehr APs (Faktor ca. 2 bis 2.5 gegen 802.11b)
- ◆ Anderes Ausbreitungsverhalten
  - Updates für Survey-Hard- & Software notwendig
  - Reagiert stärker auf Umgebung (Türen, Menschen)

# Fehlersuche im WLAN 1

## Problemfelder

### ◆ Dämpfung

- Bausubstanz wie Stahlbeton, Klinker
- Höhere Frequenzen stärker gedämpft
- Dämpfung ist nicht uniform

### ◆ Reflexion

- Metallflächen, Stahlbeton
- Führen zu Mehrwegeausbreitung
  - Eintreffen eines Signalstroms zu leicht versetzten Zeitpunkten
  - Destruktive Selbstinterferenz möglich
  - 802.11 a/b/g ohne Diversity-Antennen: Unvermittelter Packet Loss

### ◆ Beugung

- Beim Durchdringen von Bausubstanz mit schwankender Dichte
- Gittereffekte (Stahlbeton)

# Fehlersuche im WLAN 2

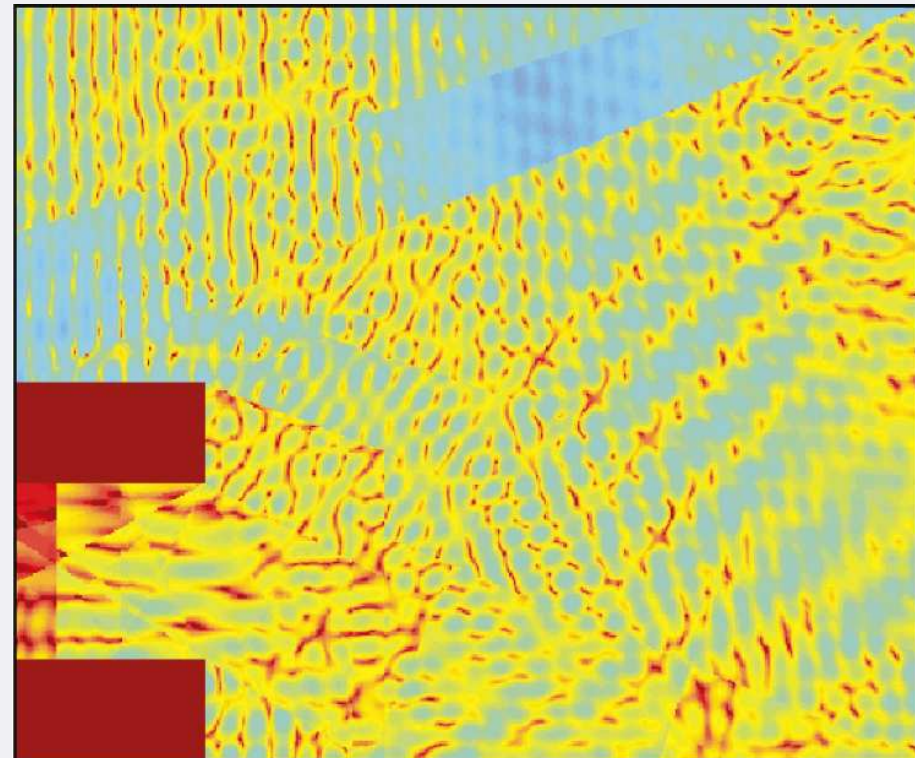
## Folgen

- ◆ Spatial zerklüftetes Funkfeld
  - Beugung, Reflexion
  - Nicht-uniforme Dämpfung (Gang vs. Wand, Schattenwurf)
- ◆ Temporal veränderliches Funkfeld
  - Die spatiale Struktur ist nicht statisch!

## Zitat aus IEEE 802.11:

*For wireless PHYs, well-defined coverage areas simply do not exist. Propagation characteristics are dynamic and unpredictable. Small changes in position or direction may result in dramatic differences in signal strength. Similar effects occur whether a STA is stationary or mobile (as moving objects may impact station-to-station propagation).*

## Statisches Funkfeld in einem Büro (Quelle: IEEE 802.11)



# Fehlersuche im WLAN 3

## Interferenz

### ◆ Co-Channel Interferenz

- Andere APs auf der selben Frequenz
  - Eigene APs oder fremde APs
  - Ab einer gewissen AP-Dichte unvermeidbar
  - Bei 5GHz wegen 20MHz-Kanälen leichte Randinterferenz
  - Nahfeld: Interferenz selbst bei „nichtüberlappenden“ Kanälen

### ◆ Fremdinterferenz

- Nicht-802.11-Quellen
  - Mikrowelle, Wireless Videolinks
  - Bluetooth
  - Radar
  - Jammer

### ◆ Tools

- Wireless STA sieht nur die Folgen (Defekte Frame-CRC → Loss)
- Einziges Messmittel ist ein Spectrum Analyzer
  - Analyzer für allgemeine HF-Anwendungen (hoher Aufwand)
  - Cisco Spectrum Expert (dedizierter Analyzer für WLAN)

# Fehlersuche im WLAN 4

## Wireless Sniffing 1

- ◆ Analyse von Problemen auf L2 oder höher
  - Analyse auf L1 (PHY) mit STAs nicht möglich
- ◆ Hoher Aufwand
  - Geeignete Hardware (RFMON Support)
    - z.B. Intel 3945, Atheros 5k/9k
  - Geeignete Software (RFMON-fähiger Treiber)
    - Windows WLANIC-Treiber beherrschen kein RFMON (nur NDIS5)
    - Zunehmend guter Support unter Linux
  - Eine WLANIC pro Kanal
    - Explodierender Aufwand in Roaming-Umgebungen
    - Cardbus-Knappheit, räumliche Verteilung: Mehrere Rechner
  - Unzuverlässig
    - Der Sniffer sieht nicht alle Frames
    - Definitive Aussagen sind schwer (ACKs/Seq# helfen manchmal)

# Fehlersuche im WLAN 5

## Wireless Sniffing 2

### ◆ Hoher Aufwand

- Geeignete Analysesoftware
  - Muss Wireless Sniffing beherrschen (802.11, RadioTap)
  - Sollte für VoWLAN VoIP-Support haben (RTP Streams)
  - Wireshark unter Linux (aktuellste Entwicklerreleases)
- Decryption
  - Generelles Problem, wenn Keys nicht verfügbar
  - Typisch nur für WEP und WPA(2)-PSK implementiert
  - Mitschnitt der Crypto-Aushandlung essenziell (EAPOL 4-way)
    - ◆ Kollidiert mit Unzuverlässigkeit
- Auswertung!
  - Wer analysiert hunderte MByte Mitschnitt mit hunderttausenden Frames?
  - Wie lange dauert das, bis ein Problem eingekreist ist?

**Vielen Dank für Ihre Aufmerksamkeit!**



**professional IT-Service**

**Fragen Sie!  
Wir antworten.**

**[www.ibh.de](http://www.ibh.de)**