Kommunikationsnetz Franken e.V.

WLAN Neuerungen

WPA, WMM, WDS und noch einiges mehr

Max Riegel

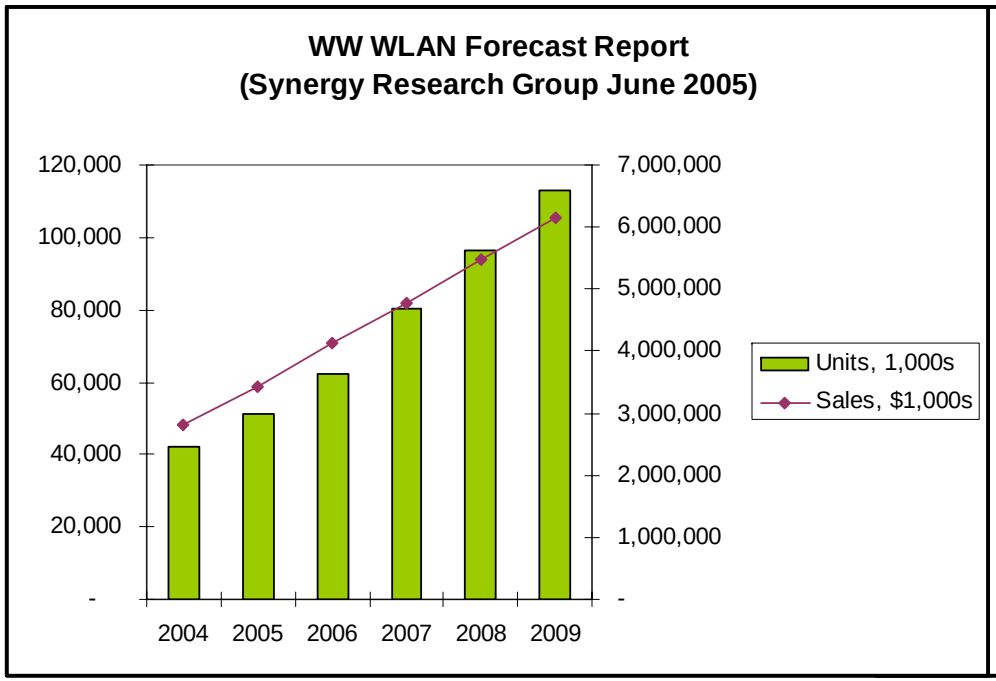
<riegel@max.franken.de>

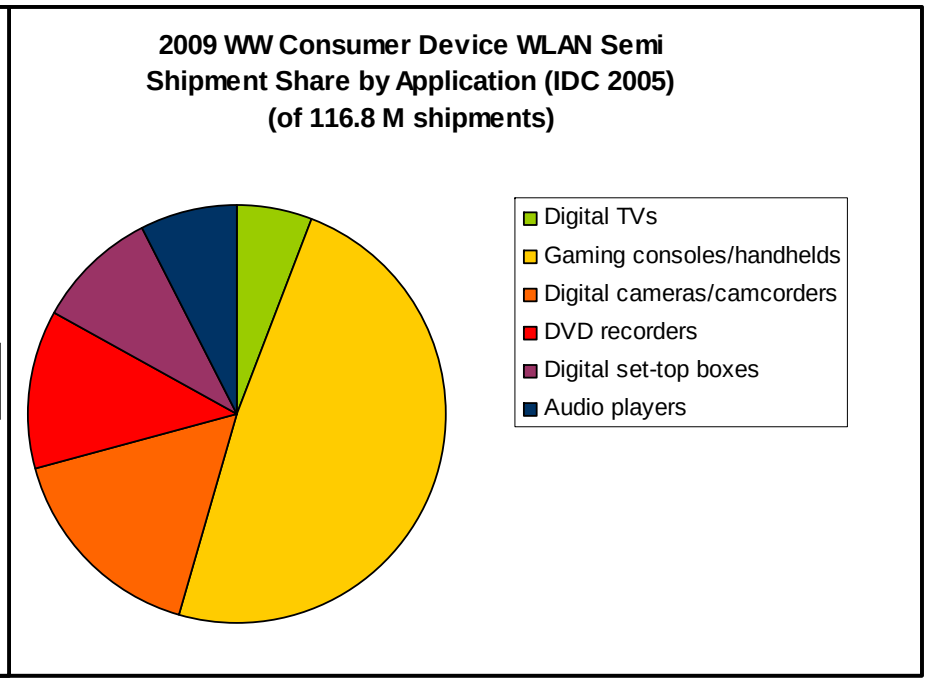
KNF Kongress ’05, 2005-11-20

Übersicht

- **Marktvorhersagen**
- **Erweiterungen des IEEE802.11 Standards**
- **Zertifizierung durch die WiFi Alliance**
  - WPA, WPA2
  - WMM
- **Firmenspezifische Erweiterungen**
  - WDS
  - CCX

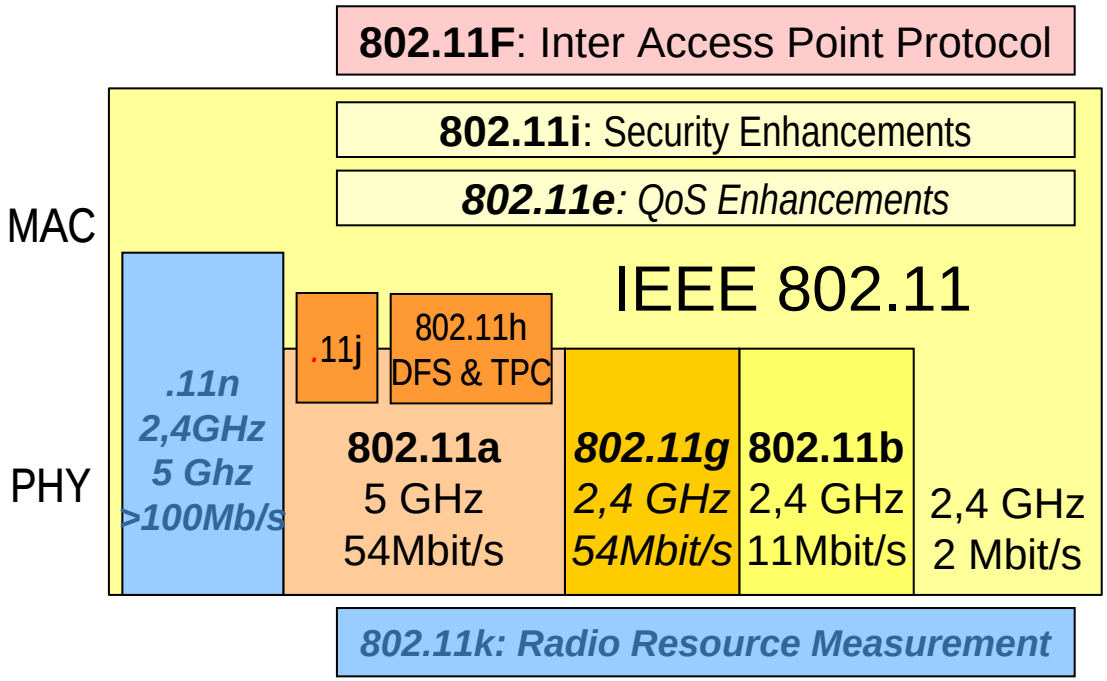
Der WLAN Markt wächst weiter...





- **Über 70% der Laptops inzwischen mit integriertem WLAN**
- **Weltweit mehr als 65 000 WLAN Hot-Spots**

IEEE 802.11 Wireless LAN Standards und Standardisierung



- m 802.11 Standard Maintenance
- p Wireless Access for Vehicular Environment
- r Fast Roaming
- s ESS Mesh Networking
- T Wireless Performance Prediction
- u Wireless Interworking with External Networks
- v Wireless Network Management
- w Protected Management Frames

IEEE802.11 Standard Amendments

Kürzel	Titel	Start	Abschluss
802.11a	Higher Speed PHY Extension in the 5 GHz Band	Sept. 1997	Sept. 1999
802.11b	Higher Speed PHY Extension in the 2.4 GHz Band	Dez. 1997	Sept. 1999
802.11c	MAC Bridges - Supplement for Support by IEEE802.11	Dez. 1997	Sept. 1998
802.11d	Operation in Additional Regulatory Domains	Juni 1999	Juni 2001
802.11e	MAC Enhancements for QoS (and Security => i)	März 2000	Sept. 2005
802.11F	Inter Access Point Protocol across Distribution Systems	März 2000	Juni 2003
802.11g	Further Higher Data-rate Extension in the 2.4 GHz Band	Sept. 2000	Juni 2003
802.11h	Spectrum and Transmit Power Management in the 5 GHz Band	Dez. 2000	Sept. 2003
802.11i	MAC Security Enhancements	Mai 2001	Juni 2004

IEEE802.11 Standard Amendments, Forts.

Kürzel	Titel	Start	Abschluss
802.11j	4.9GHz – 5GHz Operation in Japan	Dez. 2002	Sept. 2004
P802.11k	Radio Resource Measurement	Dez. 2002	
P802.11n	High Throughput	Sept. 2003	
P802.11p	Wireless Access for Vehicular Environment	Sept. 2004	
P802.11r	Fast Roaming	Mai 2004	
P802.11s	ESS Mesh Networking	Mai 2004	
P802.11u	InterWorking with External Networks	Dez. 2004	
P802.11v	Wireless Network Management	Dez. 2004	
P802.11w	Protected Management Frames	März 2005	

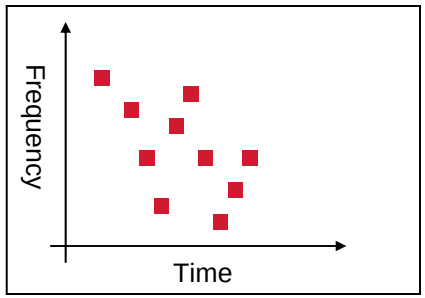
Der Wireless LAN IEEE802.11 Standard

Verabschiedet: Juni 1997

- **Betrieb im 2.4GHz ISM Band, gemäß:**
  - North America: FCC part 15.247-15.249
  - Europe: ETS 300 - 328
  - Japan: RCR - STD-33A
- **Enthält drei verschiedene PHYs: DSSS, FHSS, Infrared**
- **Ein gemeinsamer MAC Layer**
- **Robust gegen Interferenzen**
- **Auch in schwierigen Umgebungen zuverlässige Datenübertragung**
- **Zwei Konfigurationen: Ad-hoc und Infrastruktur**

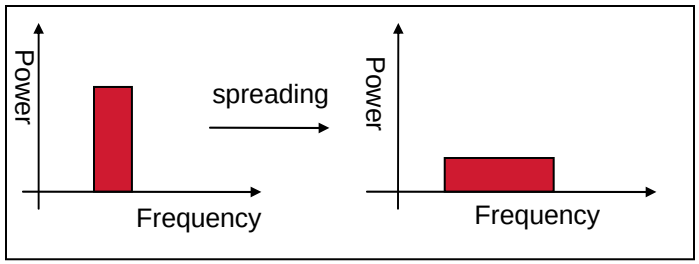
IEEE802.11 (a & b)
2.4 GHz & 5 GHz Physical Layers

- ***Baseband IR, 1 and 2Mbps, 16-PPM and 4-PPM***



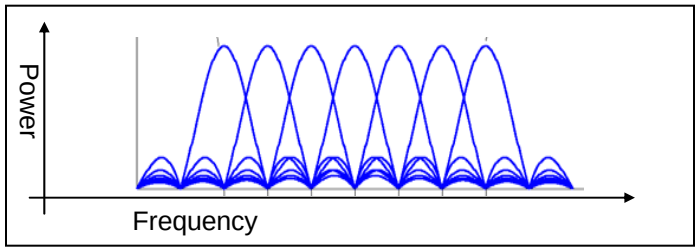
- **2.4 GHz *Frequency Hopping Spread Spectrum***
  - 2/4 FSK mit 1/2 Mbps
  - 79 überlappungsfreie Kanäle mit jeweils 1 MHz Breite (US)

- **2.4 GHz *Direct Sequence Spread Spectrum***
  - DBPSK/DQPSK mit 1/2 Mbps
  - Spreizung mit einem 11 Bit Barker Code
  - 11/13 Arbeitsfrequenzen im 2.4 GHz Band



- **2.4 GHz High Rate DSSS Ext. (802.11b)**
  - CCK/DQPSK mit 5.5/11 Mbps

- **5 GHz *OFDM* PHY (802.11a)**
  - Spezifikation identisch mit HiperLAN2 PHY
  - Regulatorische Anforderungen in Europa



IEEE802.11e:
MAC Enhancements for Quality of Service

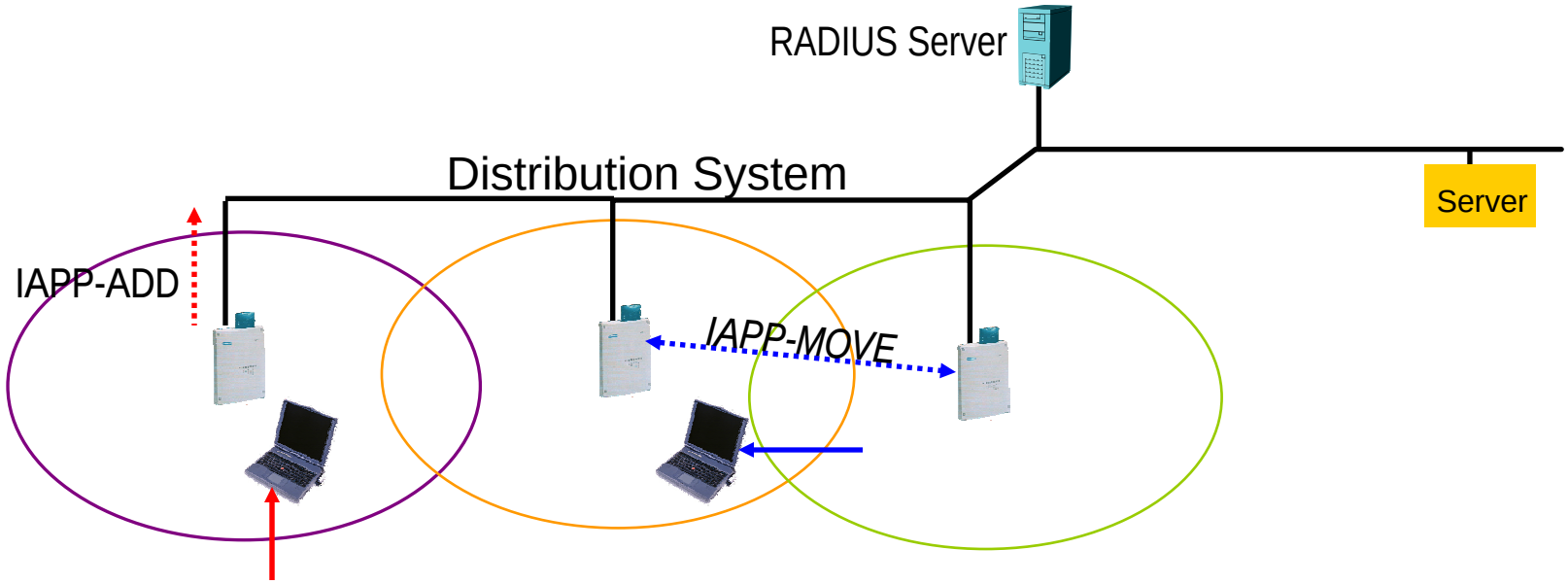
- **Unterstütz sowohl ‘harte’ (IntServ) als auch ‘weiche’ (DiffServ) QoS**
- **Rückwärtskompatibel mit bisherigem DCF und PCF**
- **EDCF (Enhanced DCF)**
  - 8 unterschiedliche Verkehrspriorisierungen durch gestufte Priorisierung beim Zugriff auf das Übertragungmedium
- **HCF (Hybrid Coordination Function)**
  - einsetzbar sowohl während PCF und DCF Periode
  - basiert auf einer zentralen Steuerung des Zugriffs („hybrid coordinator“)
  - kann vorgegebene Datenrate, Verzögerungszeit und Jitter für einzelne Datenflüsse strikt einhalten

Optional:

- **Direct Link Protocol (DLP)**
  - Terminal-zu-Terminal Übertragung im Infrastruktur Mode
  - DLP regelt dabei auftretende Probleme, z.B. im PowerDown Mode
- **Block ACK**
  - Eine ganze Gruppe von Übertragungsrahmen wird zusammen bestätigt.

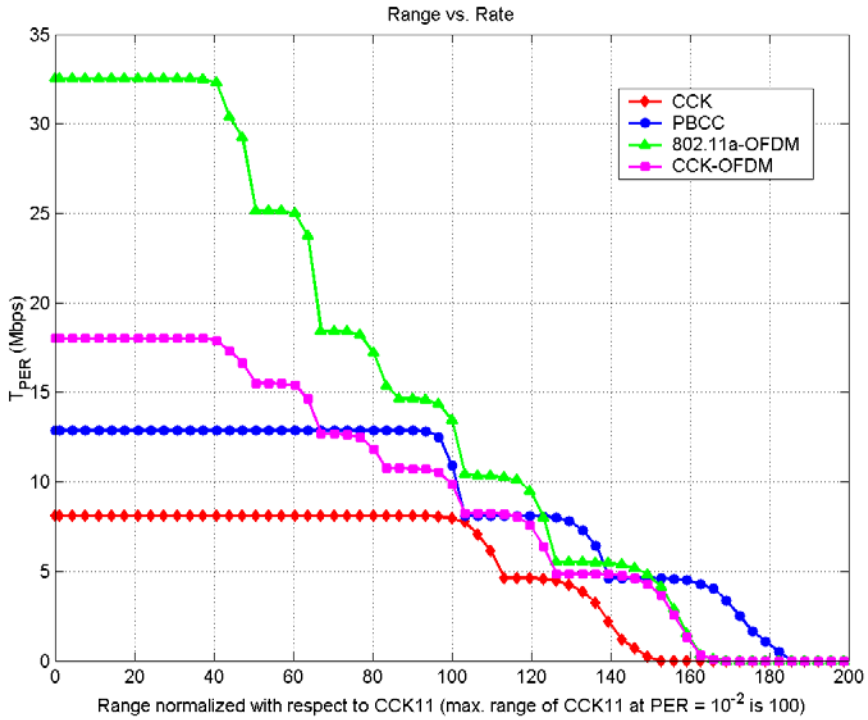
IEEE802.11F:
Inter-Access Point Protocol (IAPP)

- **Das IAPP definiert Prozeduren für**
  - die Lokalisierung des alten Access Point
  - die Übergabe des Contexts an den neuen Access Point



IEEE802.11g: Höhere Geschwindigkeiten im 2.4GHz Band

- **Basis:** CCK mit kurzer Preample (802.11b) und OFDM wie 802.11a, aber auf 2,4 GHz.
- **Optional:** PBCC Vorschlag für 22 Mbit/s von Texas Instruments
- **Optional:** CCK-OFDM Vorschlag für bis zu 54 Mbit/s von Intersil



Range vs. throughput rate comparison of

- CCK (802.11b),
- OFDM(*"802.11a"*),
- PBCC,
- CCK-OFDM

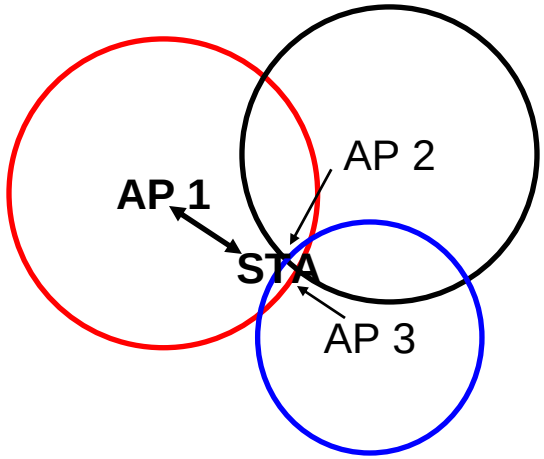
(Batra, Shoemake; Texas Instruments; Doc: 11-01-286r2)

IEEE802.11h: Erfüllung der Zulassungsbedingungen in Europa

Die Europäische Regulierung schreibt zwei spezielle Funktionen für die Nutzung des 5 GHz Bereiches für Radio-LAN Systeme vor. Notwendig für den Einsatz von IEEE802.11a in Europa.

- **TPC (Transmission Power Control - Steuerung der Sendeleistung)**
  - unterstützt die Verringerung von Interferenzen durch Anpassung der Sendeleistung an die räumlichen Bedingungen
  - hilft auch zur Verbesserung der Übertragungsgüte und zur Reduktion des Stromverbrauchs

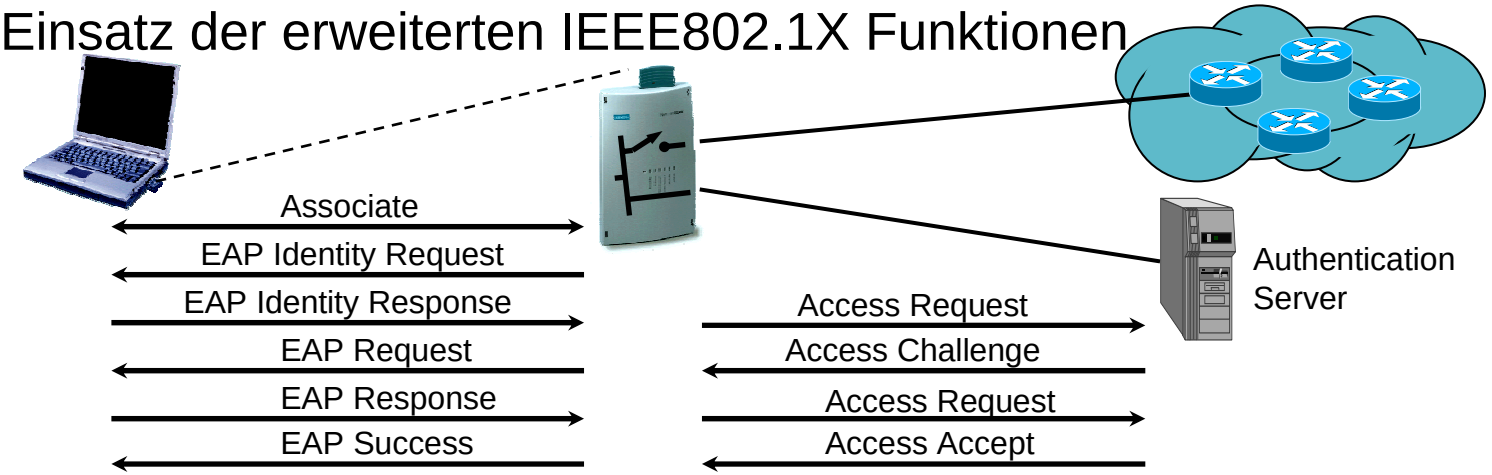
- **DFS (Dynamic Frequency Selection)**
  - Access Point sucht sich selber ein ‚freies' Frequenzband für den Betrieb
  - Dazu müssen die Endgeräte Informationen über andere Nutzer des Spektrums bereitstellen.



IEEE802.11i:
Robust Security Network (RSN)

Zusätzliche Verbesserungen zu den existierenden IEEE802.11 Funktionen:

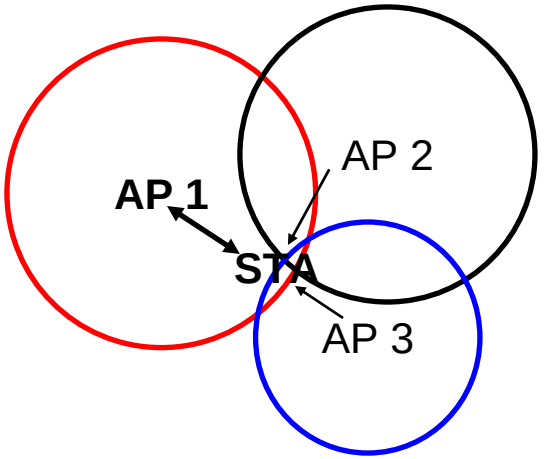
- **Data privacy mechanism:**
  - TKIP (Temporal Key Integrity Protocol) um RC4-basierte Hardware für höhere Anforderungen tauglich zu machen, oder
  - WRAP (Wireless Robust Authenticated Protocol), das auf AES (Advanced Encryption Standard) und OCB (Offset Codebook) basiert.
- **Security Association Management:**
  - Verhandlungsprozeduren um den Kontext aufzubauen
  - Einsatz der erweiterten IEEE802.1X Funktionen



IEEE802.11k:
Radio Resource Measurement

Upcoming

- **Für echtes QoS werden nicht nur verbesserte Steuerungsalgorithmen im MAC sondern auch eine Verwaltung der Radio Resource benötigt**
- **IEEE802.11k stellt Funktionen für die Verwaltung der Radio Resource zur Verfügung:**
  - TPC (Transmission Power Control)
    - auch Bestandteil von IEEE802.11h
  - DFS (Dynamic Frequency Selection)
    - auch Bestandteil von IEEE802.11h
  - Radio Measurement Prozeduren
    - Beacon Report
    - Frame Report
    - Channel Load Report
    - Noise Histogram Report
    - Medium Sensing Time Histogram Report
    - STA Statistics Report



IEEE P802.11n: mehr als 100 Mbit/s Nutzdatenrate

- **PHY und MAC Funktionserweiterungen zur Steigerung der Nutzdatenrate auf > 100 Mbit/s im 2.4 GHz Band und im 5 GHz Band**
- **Vorschläge basieren auf**
  - doppelter Kanalbandbreite
    - 40 MHz anstelle 20 MHz
  - Anwendung von MIMO (Multiple Input Multiple Output)
    - unabhängiger Parallelbetrieb von mehreren Sende- und Empfangsantennen
- **Zwei nahezu gleich stark unterstütze Vorschläge haben den Fortschritt in der Standardisierung das letzte Jahr blockiert.**
  - Vereinheitlichter Vorschlag für Januar angekündigt.

IEEE P802.11p: Drahtlose Kommunikation im Fahrzeugumfeld

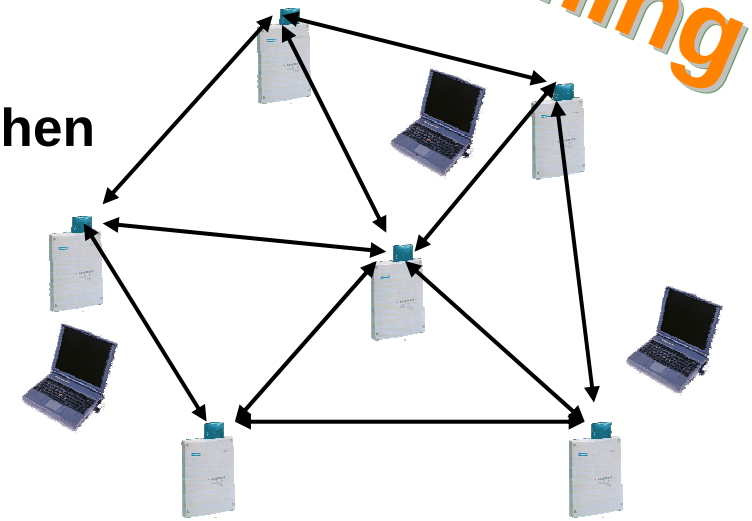
- **Speziell für den 5.85-5.95 GHz Bereich in Nordamerika**
- **Erweiterungen des MAC um die Anforderungen der Fahrzeug zu Fahrzeug oder Fahrzeug zu Bodenstation Kommunikation zu erfüllen.**
  - Spezielles Problem: sehr kurze Übertragungsfenster von 4-50ms für den Austausch der Daten
- **Für Fahrzeuggeschwindigkeiten von mindestens 200 km/h und Reichweiten bis 1000m**
- **Zeitrahmen:**
  - Beginn: Sept. 2004
  - voraussichtlicher Abschluss: Juni 2007

IEEE P802.11r: Schnellerer Hand-Over

- **Beim Einsatz von 802.11i werden umfangreiche Prozeduren für die Weitergabe/Neuaufbau der Sicherheit über die Luft benötigt**
  - Erneute Authentisierung, erneute Schlüsselgenerierung
  - Besonders schädlich für VoIP
- **Spezielle Protokollerweiterungen sollten den beschleunigten Aufbau und die Weitergabe der Sicherheitsbeziehung zum nächsten Access Point erlauben.**
- **Zeitrahmen:**
  - Beginn: Mai 2004
  - voraussichtlicher Abschluss: März 2007

IEEE P802.11s: Meshed Networking

Upcoming



- **Selbstkonfigurierende, drahtlose Netze**
- **Protokollerweiterungen zum automatischen Verbindungsaufbau zwischen den Netzknoten (Access Points)**
  - Lösung unterstützt sowohl Broadcast/Multicast Verkehr als auch Unicast Verkehr zwischen einzelnen Terminals
  - Nutzt alle 4 Adressfelder im MAC Protocol aus
  - Standardisierung des bisher nicht offiziell spezifizierten WDS (Wireless Distribution Systems)

- **Zeitrahmen:**
  - Beginn: Mai 2004
  - voraussichtlicher Abschluss: 2008

IEEE P802.11u: Interworking mit öffentlichen Netzen

- **IEEE802.11 wurde für den privaten und geschäftlichen Einsatz entworfen**
- **Der Standard weist einige Schwächen für den Einsatz im öffentlichen Umfeld auf, z.B.:**
  - Netzerkennung und Netzauswahl
    - welche Dienste, welcher Betreiber
  - Parallelbetrieb von offener und gesicherter Kommunikation
  - Nahtloser Wechsel zu anderen Netzen
  - Fehlende Einflussmöglichkeiten des Access Point auf das Terminal, z.B. um Hand-over auszulösen
- **Erweiterungen speziell für das Zusammenwirken mit Mobilfunksystemen**
- **Zeitrahmen**
  - Beginn: Dez. 2004
  - Voraussichtliches Ende: 2008

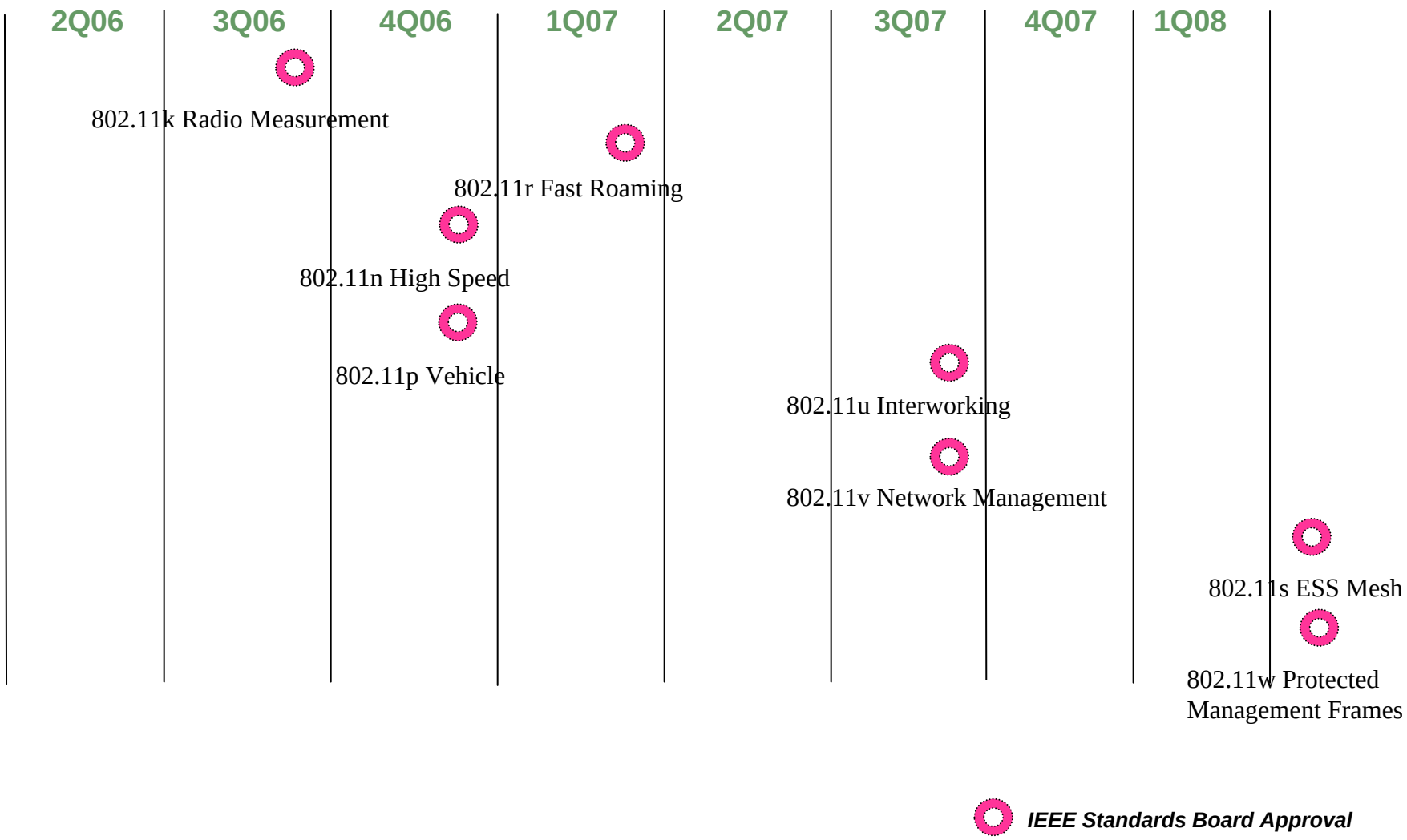
IEEE P802.11v:
WLAN Netz Management

- **Ergänzung zur 802.11k (Radio Resource Measurement)**
  - 802.11k ermöglicht nur Messungen
- **Definition von Schnittstellen zum Management eines WLAN Netzes von einer übergeordneten Management-Zentrale**
- **Erweiterung um Prozeduren zum Monitoring, zur Konfiguration und zum Update der WLAN Terminals**
- **Unterstützung einer zentralen Architektur als auch dezentrale Architectur**
- **Zeitrahmen:**
  - Beginn: Dez. 2004
  - Voraussichtlicher Abschluss: 2008

P802.11w: Protected Management Frames

- **802.11i schützt nur die Benutzerdaten zwischen Terminal und Access Point**
- **802.11w führt Sicherheitsmechanismen für Management Frames ein für:**
  - Datenintegrität
  - Authentisierung
  - Einmaligkeit
  - Vertraulichkeit
- **z.B. für Scanning, Authentication, Association, Deassociation Frames**
- **Zeitrahmen:**
  - Beginn: März 2005
  - voraussichtlicher Abschluss: 2008

Voraussichtliche Fertigstellung der offenen 802.11 Erweiterungen



http://www.ieee802.org/11/802.11_Timelines.htm

Wi-Fi Alliance (http://www.wi-fi.org)

- **Zielsetzung:**
  - Zertifizierung der Interoperabilität von IEEE802.11 Produkten
    - Vergabe des Wi-Fi Zeichens
  - Verbreitung des Wi-Fi Zeichens als marktübergreifendes Merkmal aller IEEE802.11 konformen Lösungen
- **Derzeitige Aktivitäten:**
  - Bekanntmachung und Umsetzung der Gütesiegel-Strategie
    - einheitliches Wi-Fi Logo für alle IEEE 802.11 Zertifizierungen
    - produktspezifisch ergänzt durch die Kennzeichnung der getesteten Funktionalitäten
  - Beginn der 802.11a/b/g Wi-Fi Zertifikation inklusive Dual-Mode/Dual-Band Funktion
  - Bekanntmachung der Wi-Fi Protected Access (WPA) Initiative, verpflichtend für alle neuen Produkte
  - Weitere Vorbereitung des Wi-Fi Zone Programms

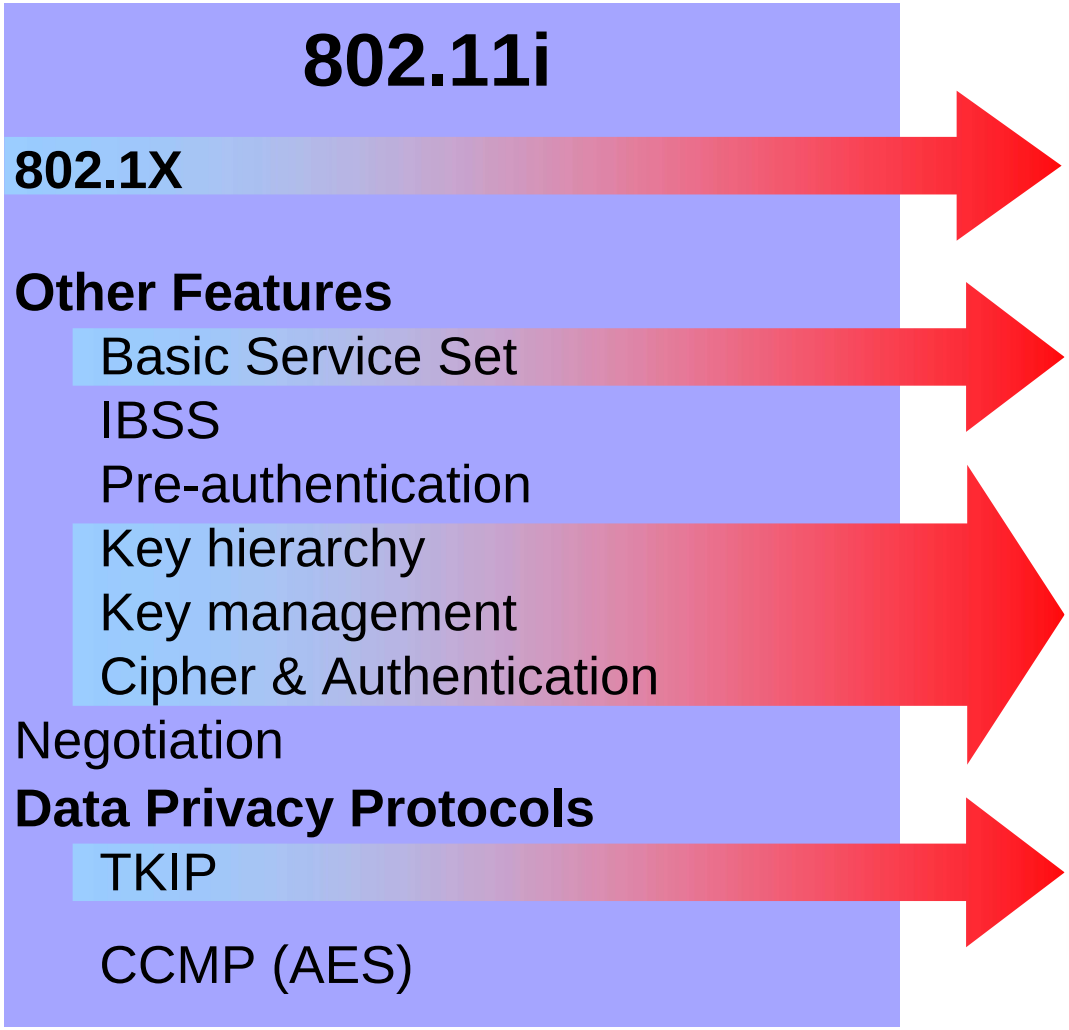
Logo

Gütesiegel

Reaktion auf die WEP Unsicherheit

- **Nachdem sich die Verabschiedung des neuen Sicherheitsstandards 802.11i verzögerte, wurde durch die Wi-Fi Alliance eine Untermenge unter dem Begriff WPA (Wi-Fi Protected Access) als Pseudostandard etabliert und dafür verpflichtend die Zertifizierung eingeführt.**
- **WPA basiert grundsätzlich auf WEP, bietet jedoch zusätzlichen Schutz durch dynamische Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren, und bietet zur Authentifizierung von Nutzern PSK (Pre-Shared-Keys) oder Extensible Authentication Protocol (EAP) an.**
  - WPA Personal
    - In kleineren/privaten Netzwerken wird meist PSK eingesetzt.
  - WPA Enterprise
    - Die Authentifizierung über EAP wird meist in großen Firmennetzen genutzt, da hierfür ein RADIUS-Server benötigt wird

Wi-Fi Protected Access (WPA)



- **Der Markt hat nach einer schnellen Lösung des WEP Problems verlangt.**

Wi-Fi Protected Access

- **WPA implementiert, was von 802.11i stabil war.**
- **WPA2 beschreibt den gesamten 802.11i Standard**

WPA2 – die Erweiterung von WPA

- **WPA2 umfasst den vollständigen 802.11i-Standard**
  - Verschlüsselungsalgorithmus AES (Advanced Encryption Standard) anstelle von TKIP.
    - WPA-fähige Geräte, die AES beherrschen, sind nicht unbeding WPA2 konform.
- **WPA2 Mixed Mode unterstützt WPA- und WPA2-fähige Geräte**
- **WPA2 umfasst wie WPA zwei Betriebsvarianten:**
  - WPA2 Personal
    - PSK
  - WPA2 Enterprise
    - EAP (EAP-TLS als Testmethode)
- **Unterstützung von ‘PMK Caching’ und ‘Preauthentication’ für Fast Roaming**

WPA/WPA2 Extended EAP

- **Zertifizierung von WPA und WPA2 erfolgt mit EAP-TLS**
- **EAP-TLS eignet sich nur wenig für den Einsatz in großen Netzen**
  - Verwaltung der Zertifikate
- **Zur Unterstützung des Einsatzes von WPA Enterprise werden weitere EAP-Methoden unterstützt:**
  - EAP-TTLS/MSCHAPv2
  - PEAPv0/EAP-MSCHAPv2
  - PEAPv1/EAP-GTC
  - EAP-SIM

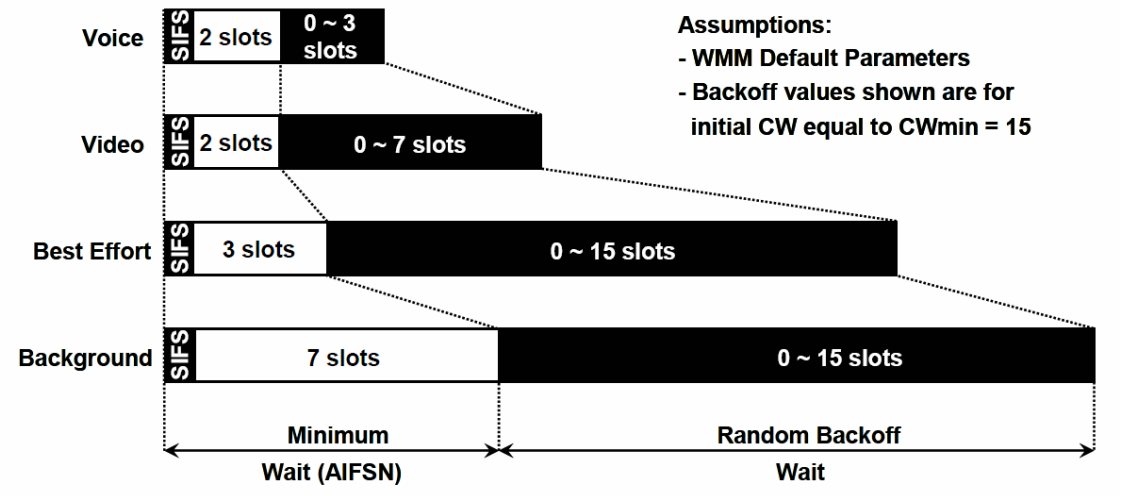
WMM – Wi-Fi Multimedia

- **Unterstützung von QoS in WLAN Netzen**
- **Im Prinzip Zertifizierung von IEEE802.11e**
  - Aufgeteilt in mehrere Unter-Profile
    - nicht alle Anwendungen benötigen alle in 802.11e beschriebenen Funktionalitäten
  - WMM™
    - EDCF
  - WMM™ - Scheduled Access
    - HCF
  - WMM™ - Power Save
    - Low power support
- **WMM Zertifizierung ist seit ca. 1 Jahr verfügbar**
  - wird von den meisten Clients und den besseren Access Points (Cisco, Proxim, etc.) unterstützt
  - Scheduled Access und Power Save noch in der Vorbereitung

WMM Funktionalität

- **Bietet 4 verschiedene Access Categories (AC)**
  - entspricht IEEE802.1D Tags:
  - WMM Voice Priority 7, 6
  - WMM Video Priority 5, 4
  - WMM Best Effort Priority 0, 3
  - WMM Background Priority 2, 1

- **Kategorien werden über Zugriff-Timer realisiert:**



WMM Leistungsfähigkeit

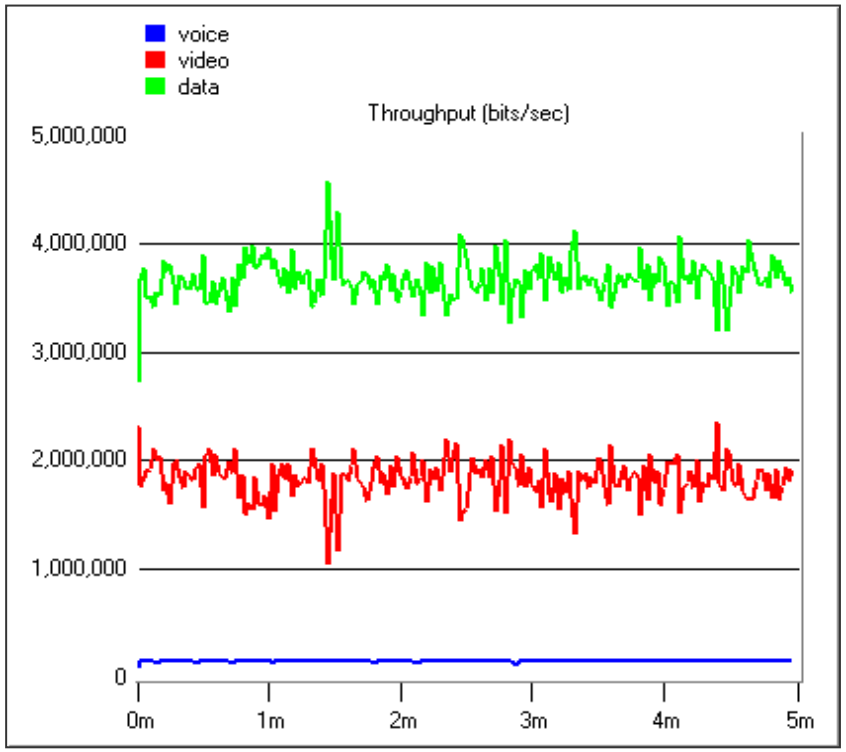
- **Testumgebung IEEE802.11b mit 11 Mbps**
- **2 Video, 4 Voice, and 4 Data Terminals**
- **Puffergröße**
  - 20,000 bits for voice, 1Mbit for video, infinite for data
- **Traffic pattern and default EDCF parameters:**

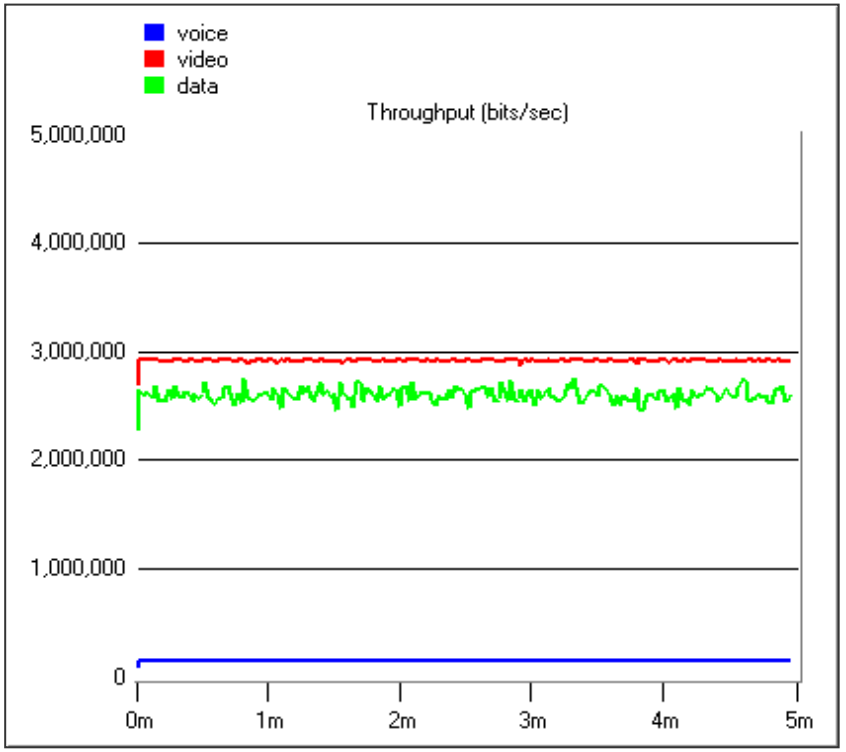
Type	Inter-arrival Time (Avg. in sec)	Frame Size (bytes)	Data Rate (Mbps)
Voice	Constant (0.02)	92	0.0368
Video	Constant (0.001)	1464	1.4
Data	Exponential (0.012)	1500	1.0

Type	Prior.	AC	AIFS	CWmin	CWmax	TXOP limit (msec)
Voice	**7**	3	PIFS	7	15	3
Video	**5**	2	PIFS	15	31	6
Data	**0**	0	DIFS	31	1023	0

DCF vs. EDCF

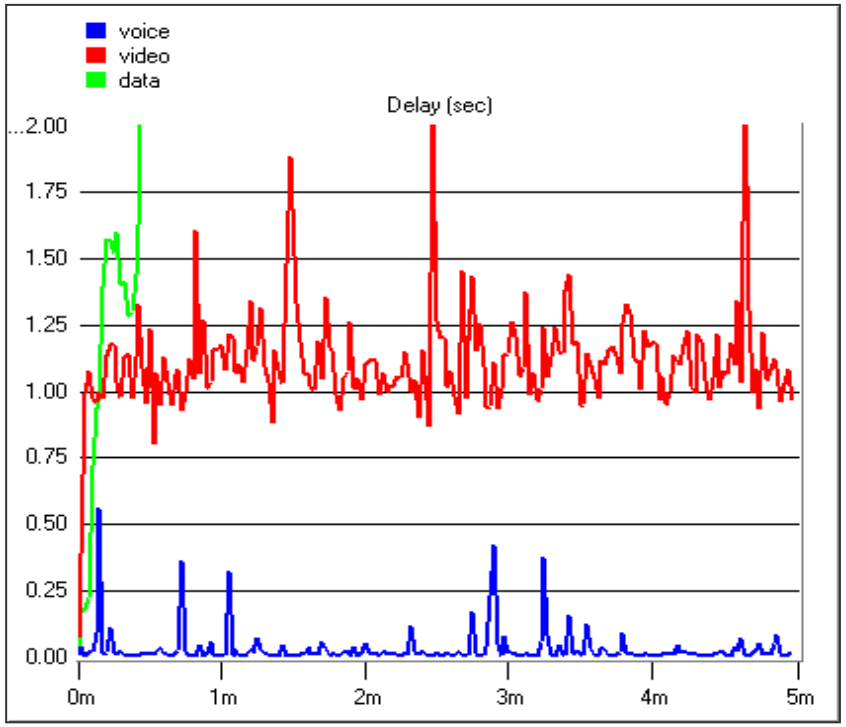
- Vergleich von Durchsatz
- Höherer Video-Durchsatz mit EDCF

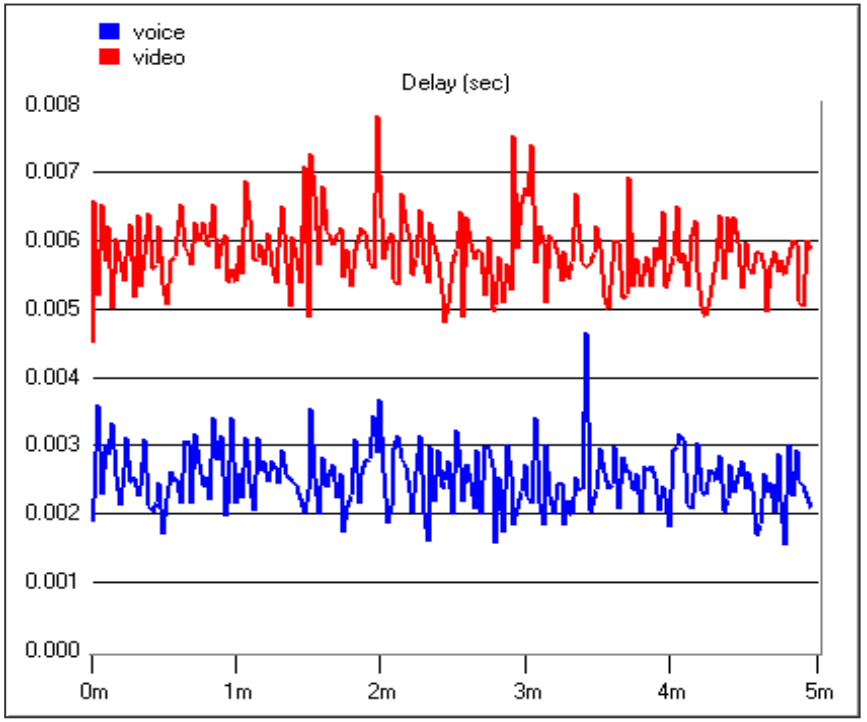




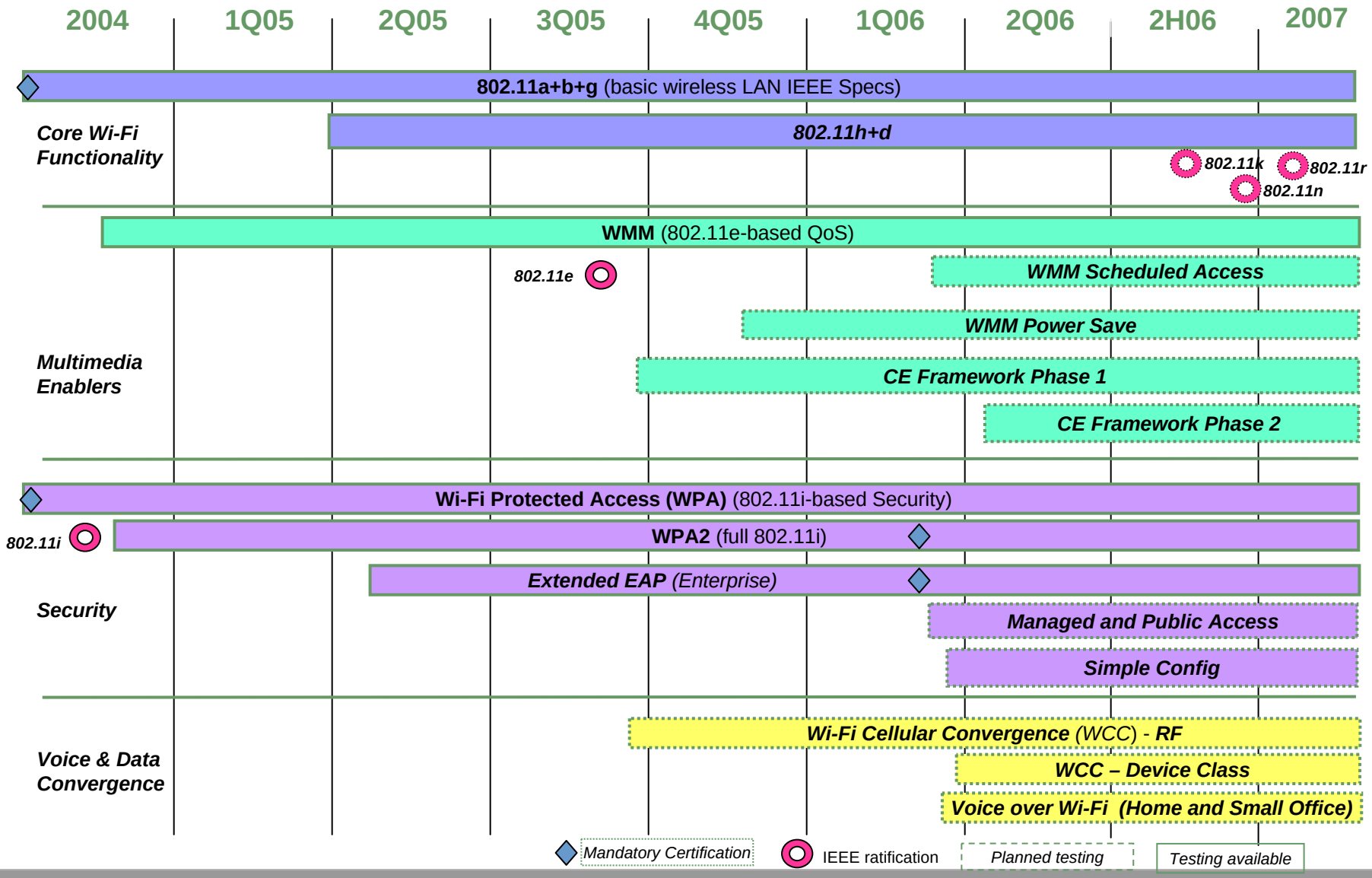
DCF vs. EDCF

- Vergleich der Verzögerungszeiten
- Verzögerung von Voice und Video deutlich reduziert





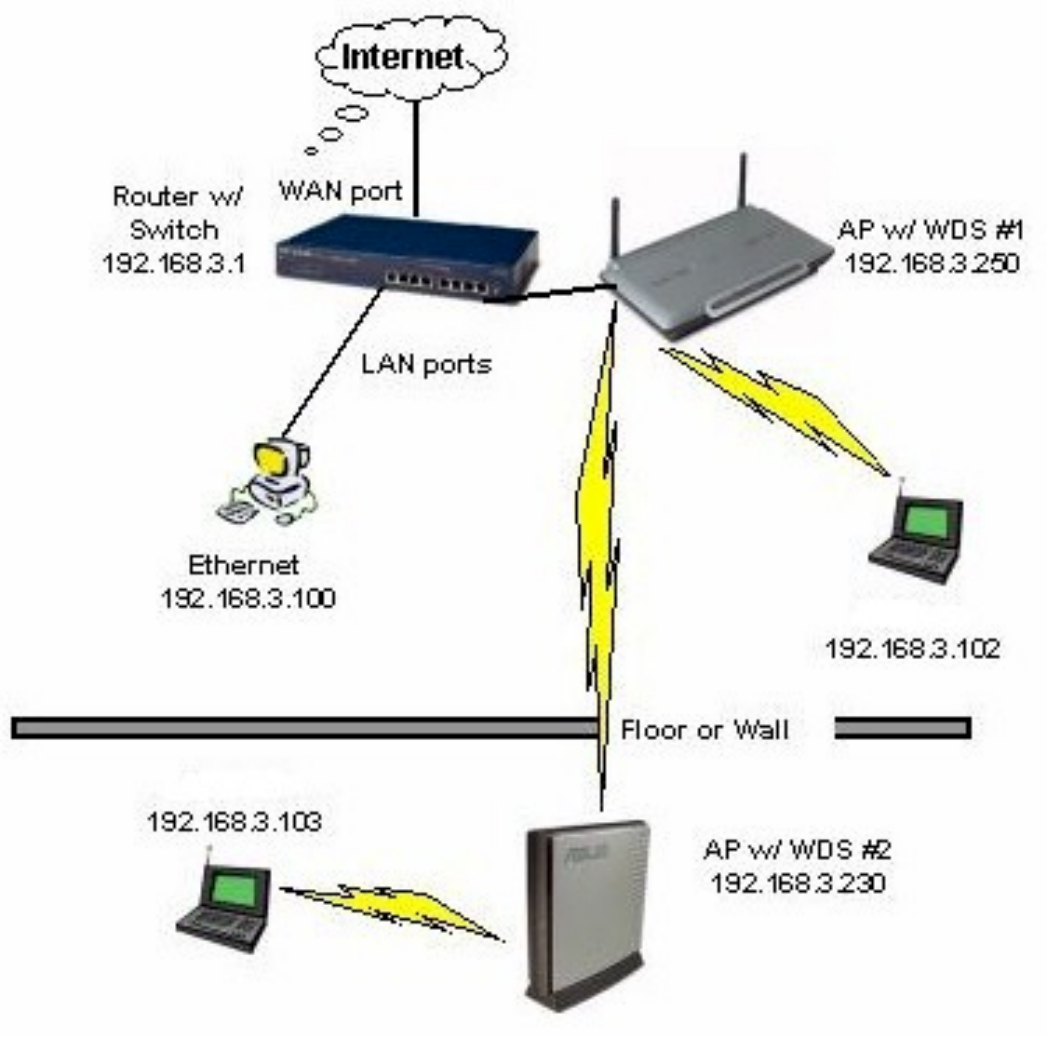
Zeitplan für weitere Wi-Fi Zertifizierungen

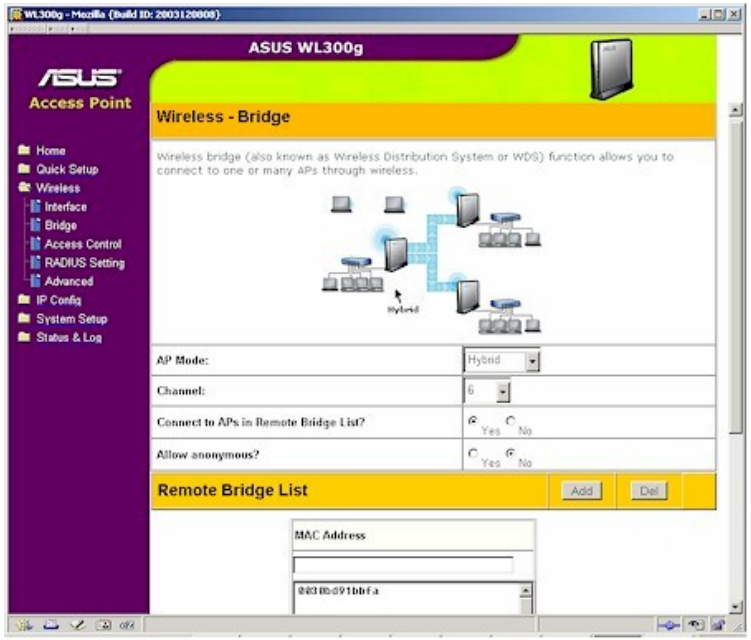


WDS – Wireless Distribution System

- **Drahtlose Verbindung zwischen mehreren Access Points untereinander.**
  - erspart die Daten-Verkabelung von Folge-Access-Points. Einzig die Stromversorgung jedes einzelnen Access Points ist erforderlich.
- **Funktioniert über ein oder mehrere Radio-Interfaces.**
  - Single-Radio-WDS benutzt das WLAN-Interface sowohl für die Verbindung zum vorhergehenden und/oder nächsten Access Point als auch für die Versorgung der Clients.
    - Nutzbandbreite halbiert sich mit jedem zusätzlichen Access Point in Reihe
  - Bei Dual-Radio Accesspoints wird ein Radio-Interface zur Anbindung des nächsten Access Points verwendet, ein zweites für die Clients.
    - Optimal sind Radios in unterschiedlichen Frequenzbändern, e.g. 802.11a & 802.11g

Beispiel für WDS





CCX – Cisco Compatible Extensions

- **Programm zur Sicherung der Kompatibilität zwischen Cisco APs "Access Points" und Hardware von anderen Anbietern.**
  - Cisco Compatible Extensions "CCX" definieren das Vorhandensein von zusätzliche Funktionen im Bereich Sicherheit und Reichweite.
  - Die Funktionen an sich sind bekannte Standards
- **CCX kompatible Chips gibt es von allen namhaften Herstellern.**
- **CCX garantiert, dass die volle Funktionalität der Cisco APs in realen Netzen genutzt werden können.**

THE END

- **Danke für Eure Aufmerksamkeit.**

- **Fragen und Anmerkungen?**