SIEMENS
mobile

# Die Standardisierung für herstellerübergreifende Sicherheitslösungen in WLAN Hotspots

Maximilian Riegel

ICM Networks, Advanced Standardization

Berlin, 2002-12-03

# Inhalt

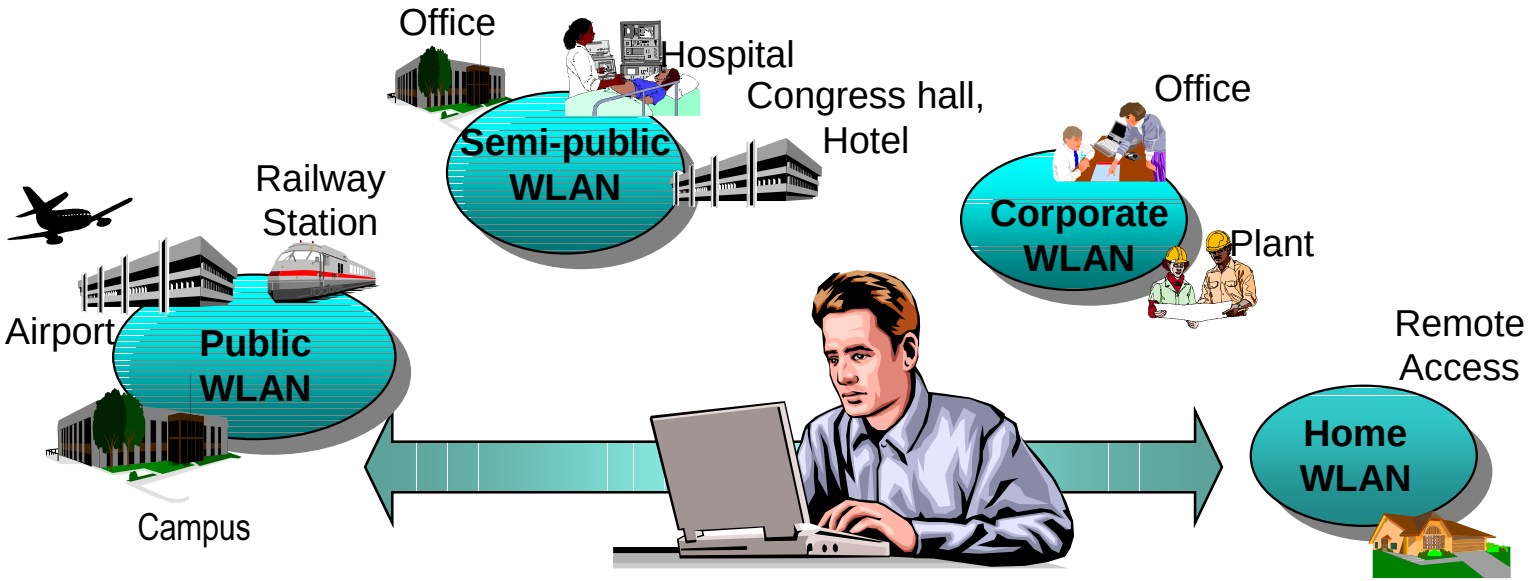
SIEMENS mobile

- **Die Bedeutung von Wireless LAN**
- **WLAN - ein neuer Baustein im Internet**
  - Sicherheit im Internet
- **Die Standardisierung im Rahmen der IEEE P802.11**
- **Die Rolle der Wi-Fi Alliance**
- **Der Betrieb von öffentlichen WLAN Hotspots**
- **Aus dem Blickwinkel des WLAN-Nutzers**
- **Die Verbindung von WLAN Hotspots mit dem Mobilfunk**

# Die Bedeutung von Wireless LAN

SIEMENS mobile

- **Notebook-Nutzer benötigen heute überall den Zugang zu ihren Daten über das Internet**
- **WLAN (Wireless LAN) ist mehr als nur der Ersatz eines Kabels; es ermöglicht den problemlosen breitbandigen Internet-Zugang**



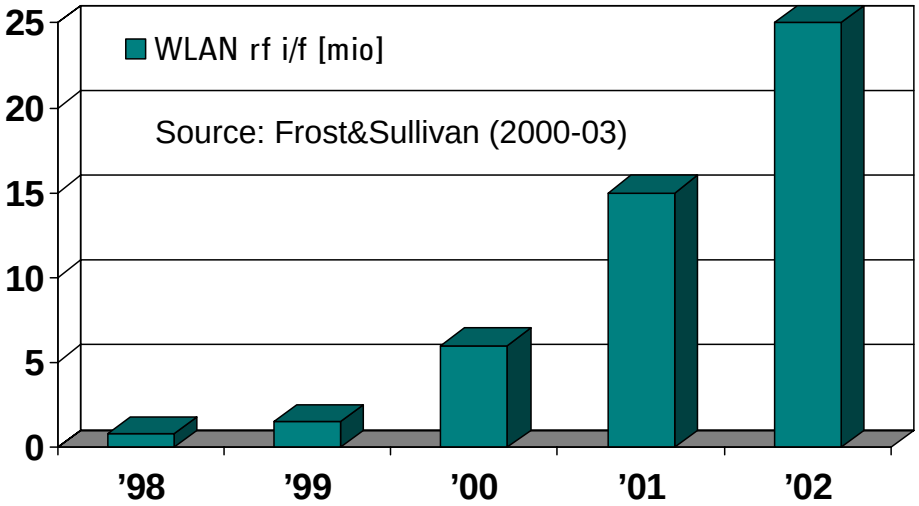

- **WLAN Versorgung in „Hotspots“ ist ausreichend.**
- **Geräte nach dem Standard IEEE802.11b (Wi-Fi) erfüllen die Anwenderwünsche hinsichtlich Bandbreite, Kosten und Einfachheit.**

# WLAN ist ein wachsender Markt

SIEMENS mobile

- **Wireless LAN hat die Nische verlassen**
  - Die großen Hersteller sind aktiv (Cisco, Intel, …)
  - Notebooks mit integriertem WLAN (Apple, IBM, ...)
- **Die Marktentwicklung hat die Vorhersagen übertroffen**
  **Zum Vergleich:**
  **Gesamter PC-Weltmarkt in ‘01: ~ 120 Mio Geräte; > 30 % portable.**

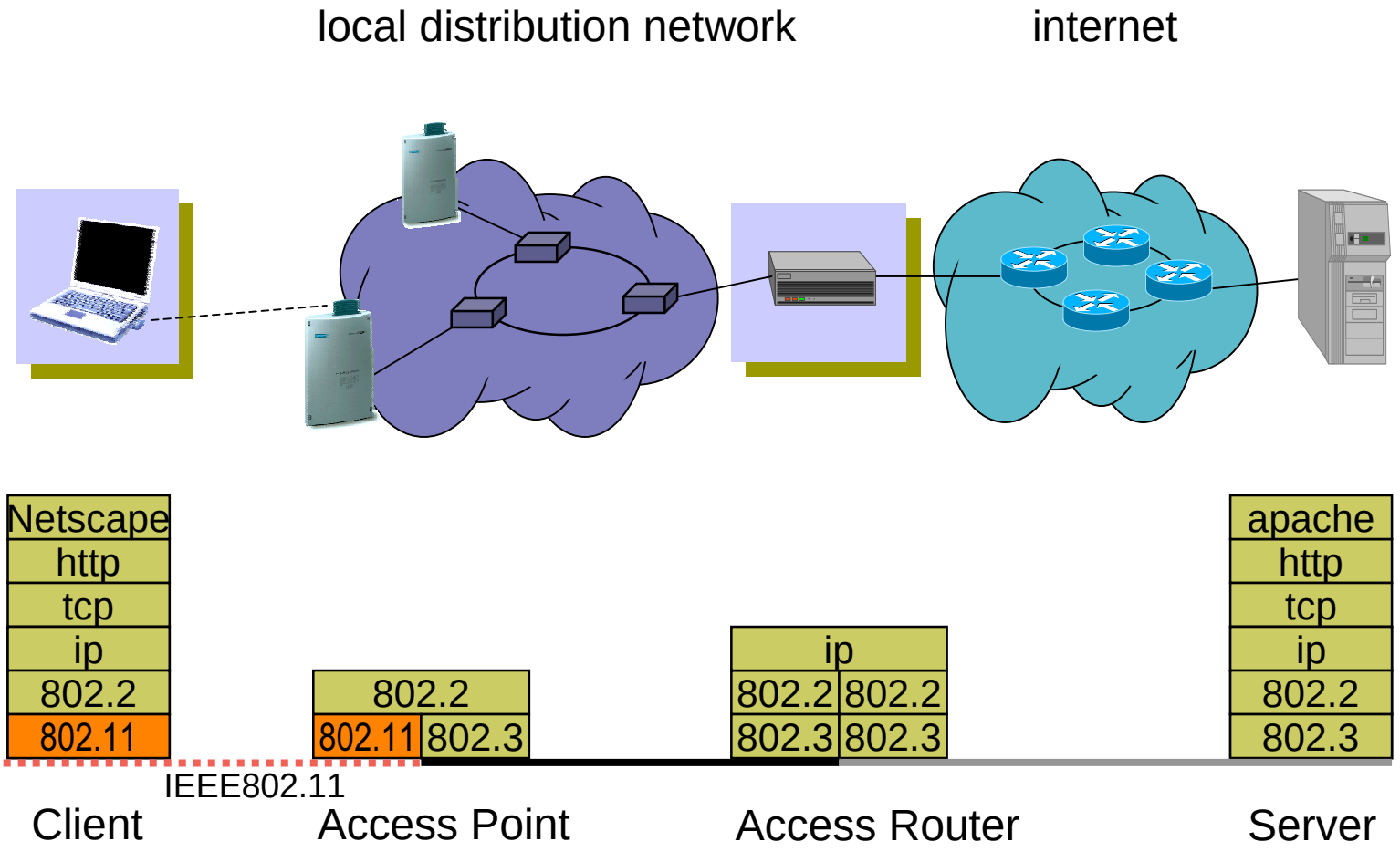



- **Die treibende Technologie ist IEEE802.11b (Wi-Fi) [11Mb/s, 2.4 GHz].**

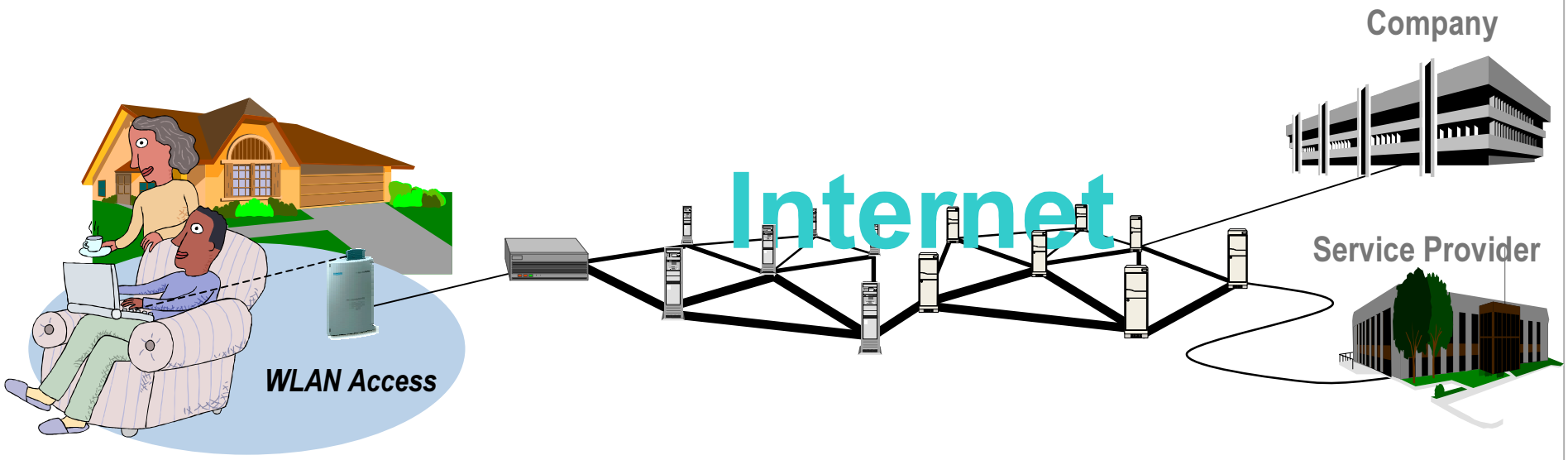
# Die Basisarchitektur von Wireless LAN IEEE802.11

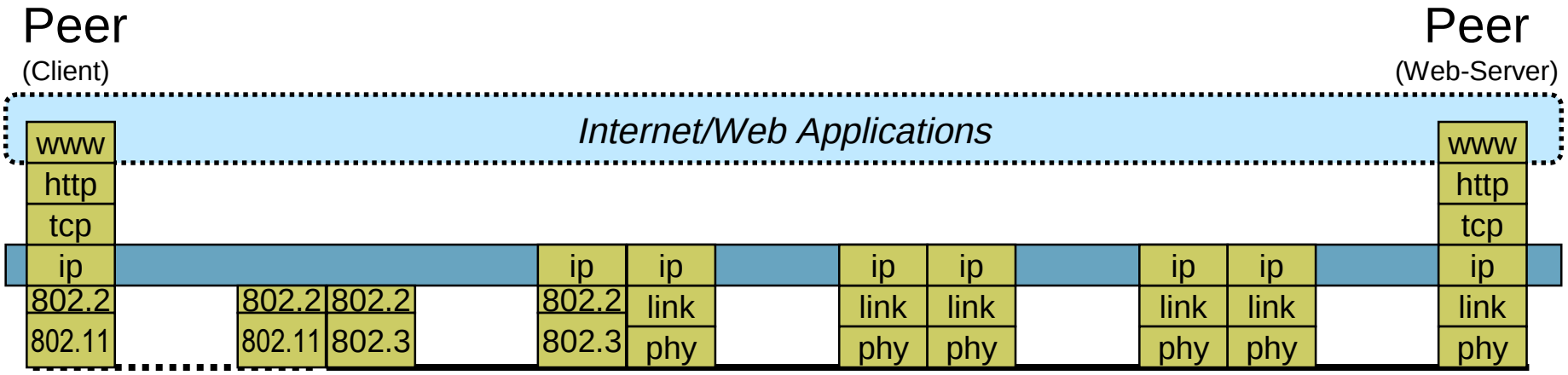
SIEMENS mobile



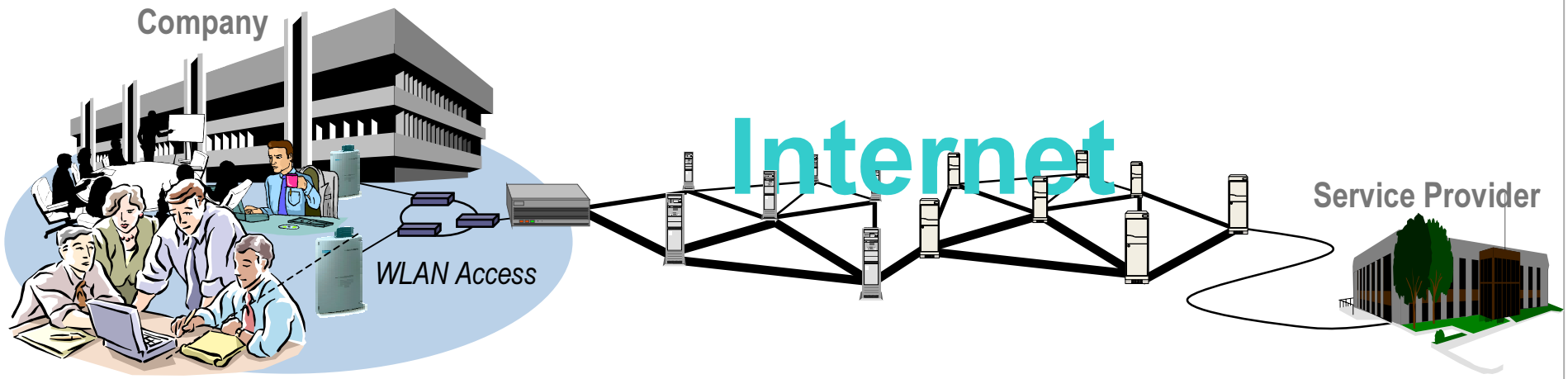
# Home WLAN Hotspot

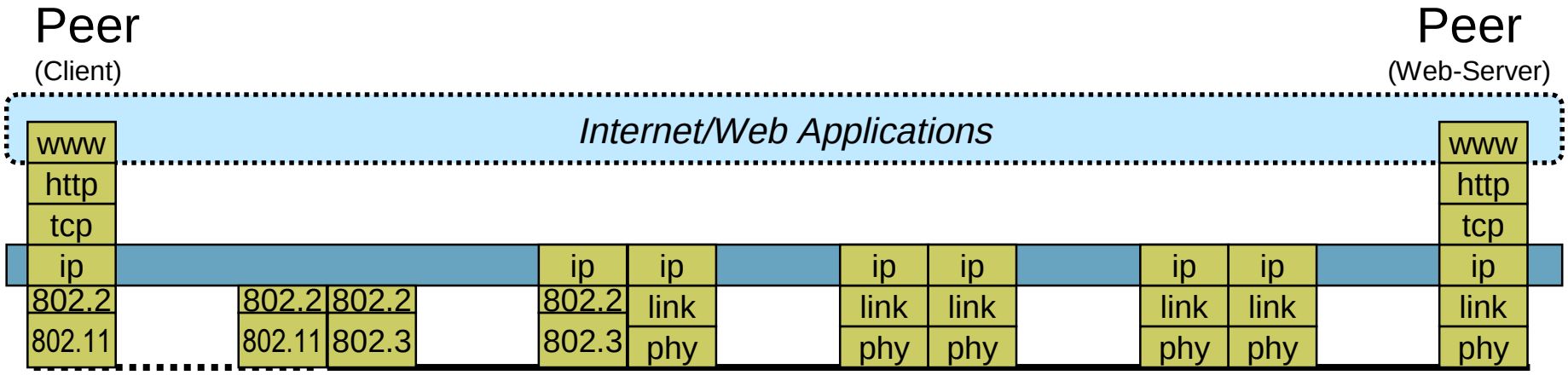


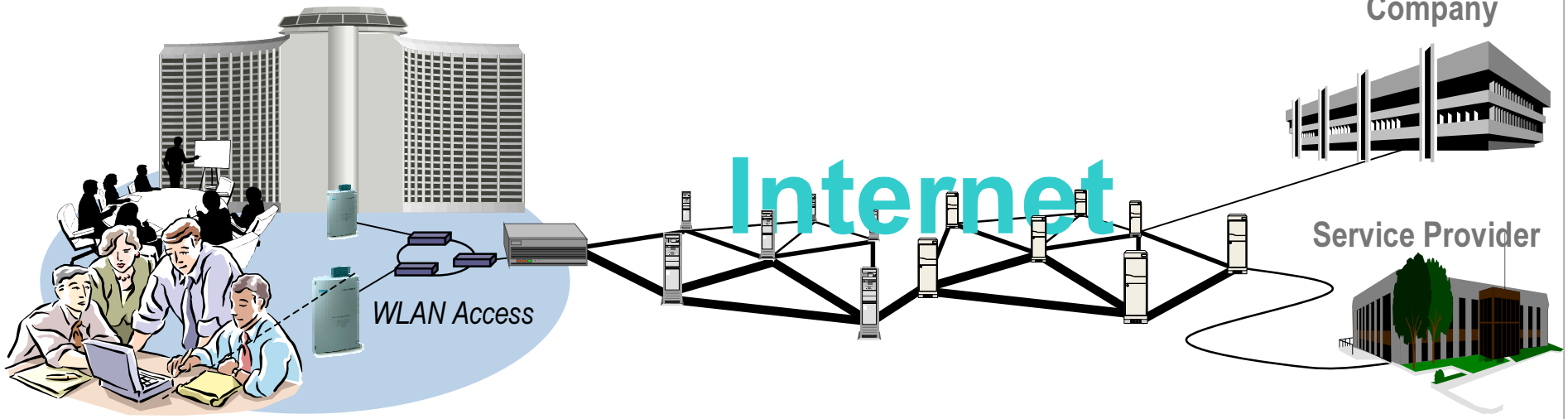
# Corporate WLAN Hotspot

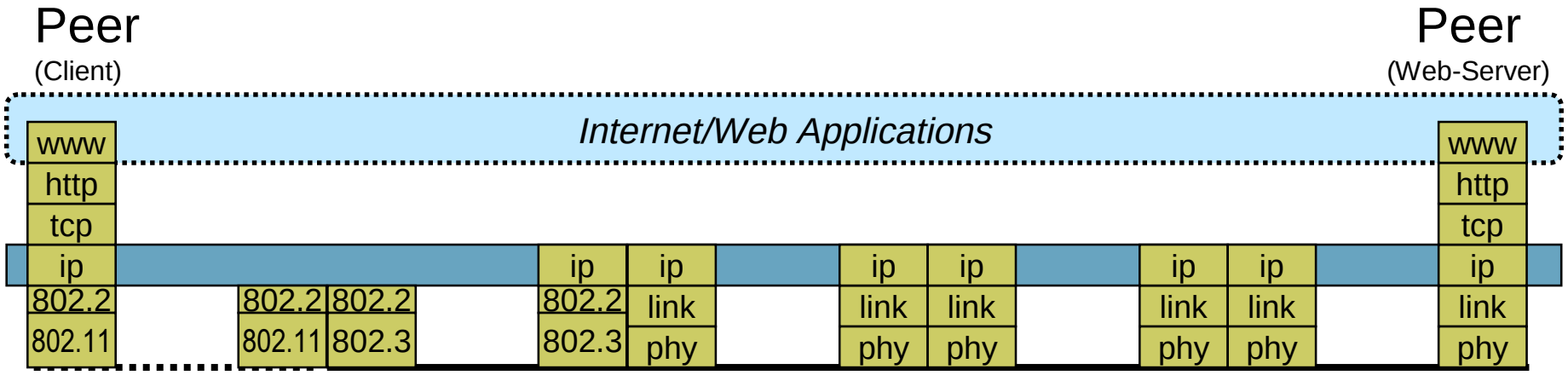


# Semi-Public WLAN Hotspot

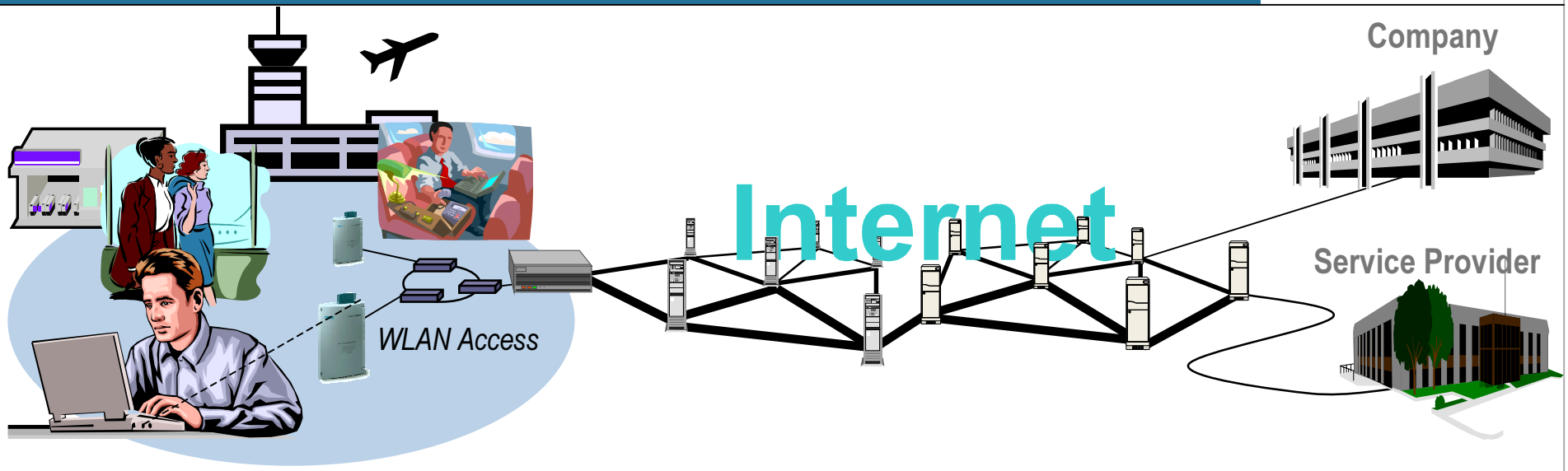


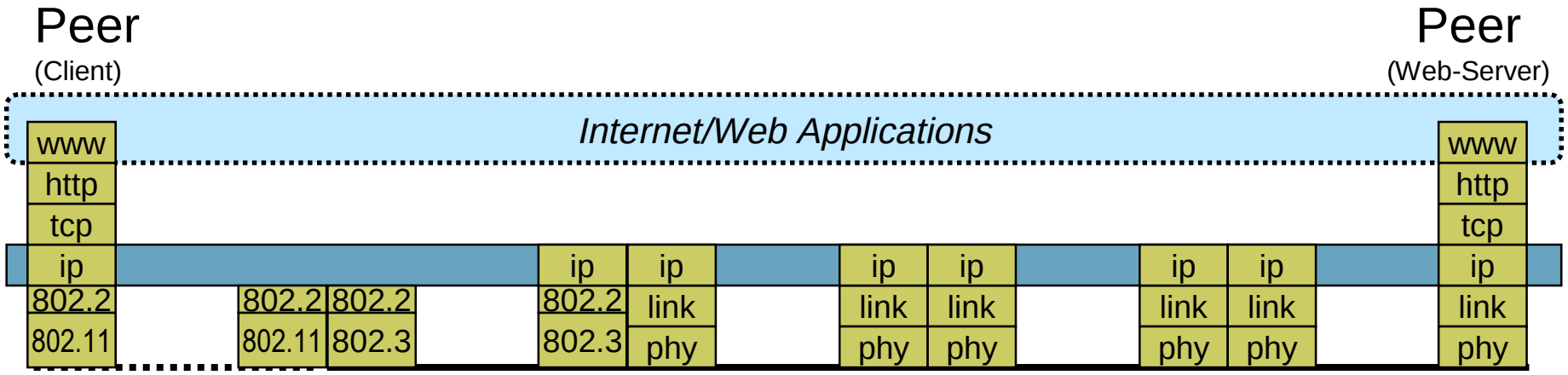



# Public WLAN Hotspot

SIEMENS mobile



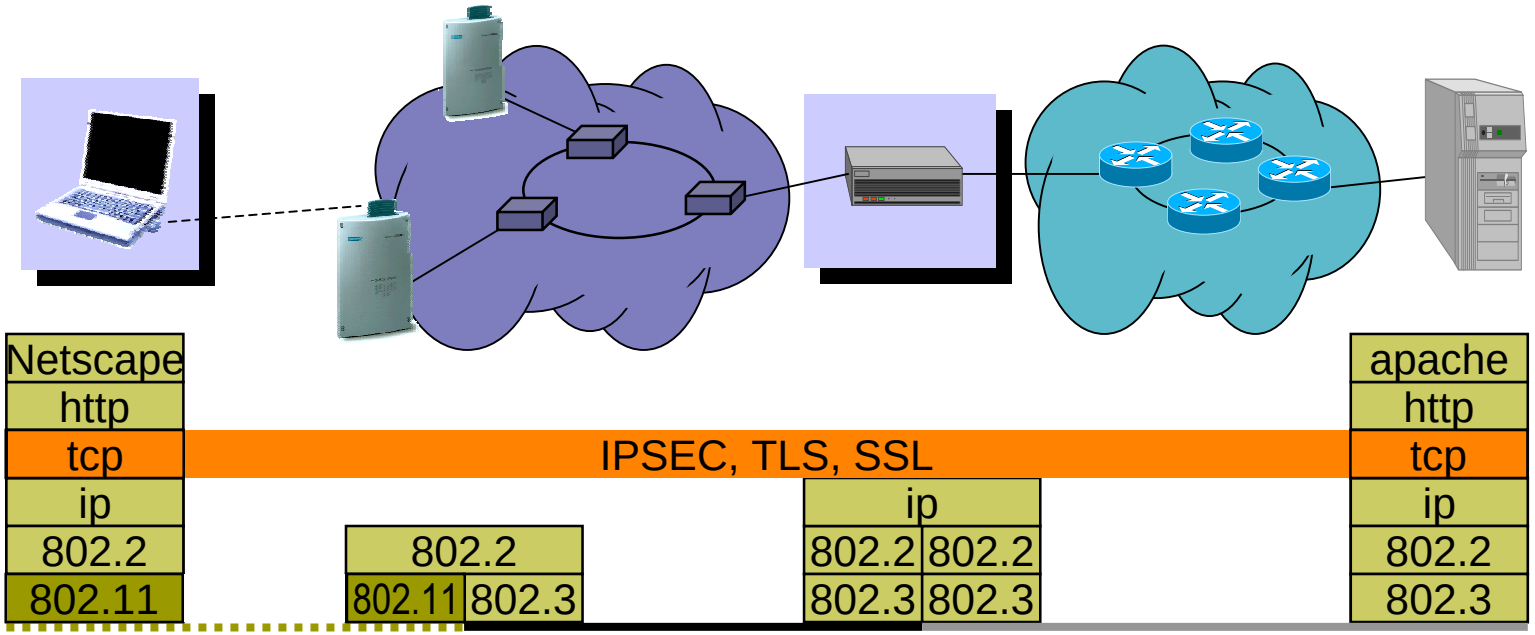



# Die Sicherheit von WLAN ist nur ein Teil des Problems

SIEMENS mobile

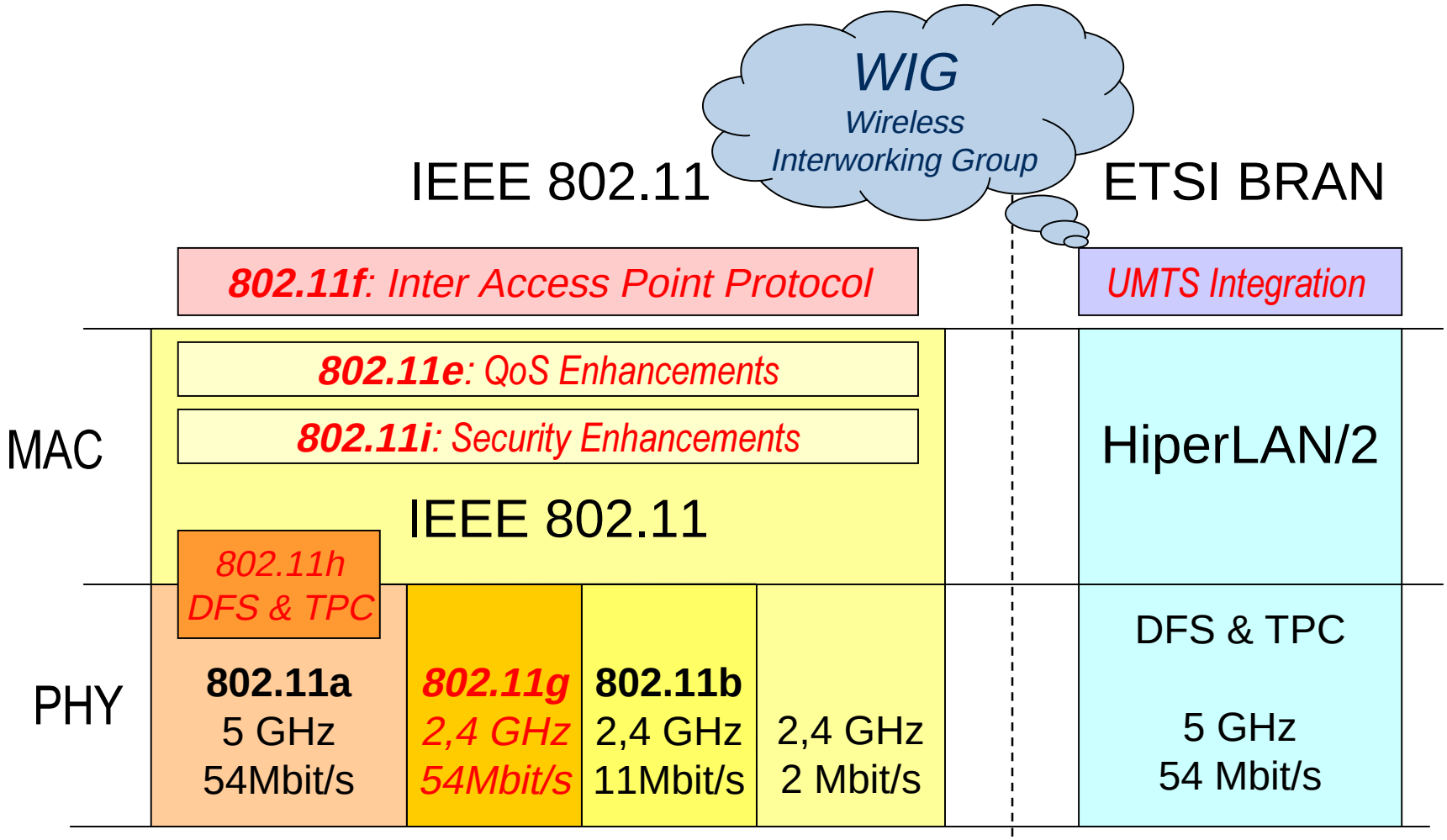
- **Auch ein verbesserter WLAN Standard löst das Problem nicht; der Schutz der Anwenderdaten kann nicht am Access Point enden.**




- **Nur Ende-zu-Ende Sicherheitstechniken (z.B. VPN, IPSEC, SSL, TLS) gewährleisten den Schutz der Anwenderdaten**
- **VPN Techniken können vorteilhaft auch beim WLAN Einsatz in Firmennetzen eingesetzt werden.**

# Wireless LAN Standardisierung




*Current standardization topics*

# Der Wireless LAN IEEE802.11 Standard


*Verabschiedet: Juni 1997*
*802.11b im September 1999*

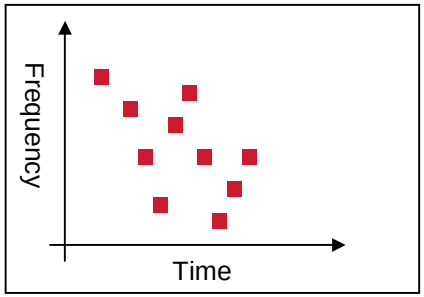
- **Betrieb im 2.4GHz ISM Band, gemäß:**
  - North America: FCC part 15.247-15.249
  - Europe: ETS 300 - 328
  - Japan: RCR - STD-33A
- **Enthält drei verschiedene PHYs: DSSS, FHSS, Infrared**
- **Ein gemeinsamer MAC Layer**
- **Robust gegen Interferenzen**
- **Auch in schwierigen Umgebungen zuverlässige Datenübertragung**
- **Zwei Konfigurationen: Ad-hoc und Infrastruktur**
- **Die Erweiterung IEEE802.11b bietet auf Basis des bisherigen MAC bis zu 11Mbit/s.**

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

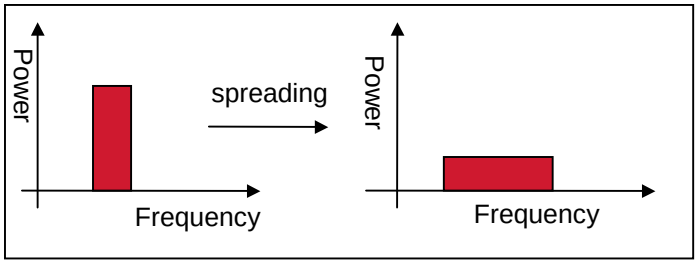
SIEMENS mobile

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



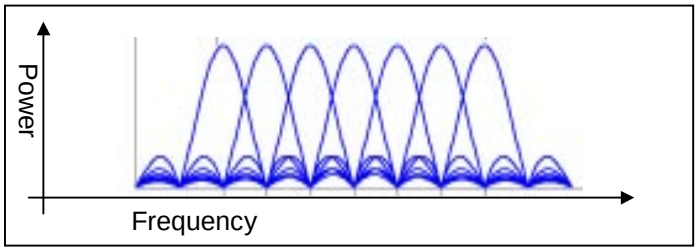

- **2.4 GHz *Frequency Hopping Spread Spectrum***
  - 2/4 FSK mit 1/2 Mbps
  - 79 überlappungsfreie Kanäle mit jeweils 1 MHz Breite (US)

- **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



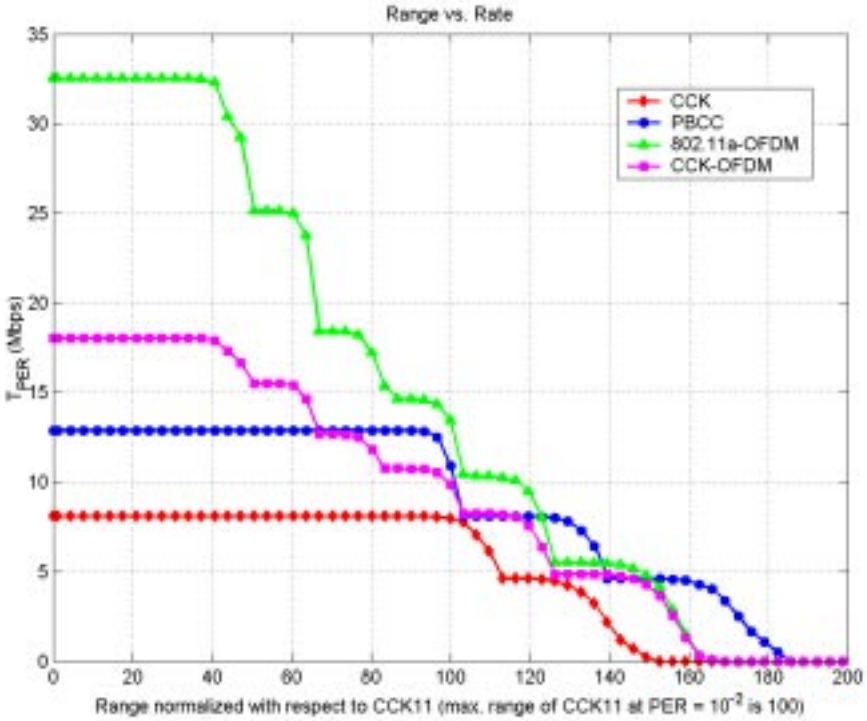

 

# IEEE802.11g: Höhere Geschwindig-keiten im 2.4GHz Band

Upcoming

SIEMENS mobile

- **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

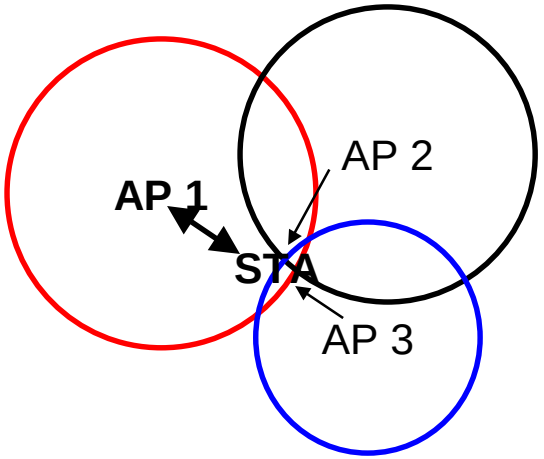
Upcoming

SIEMENS mobile

**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.



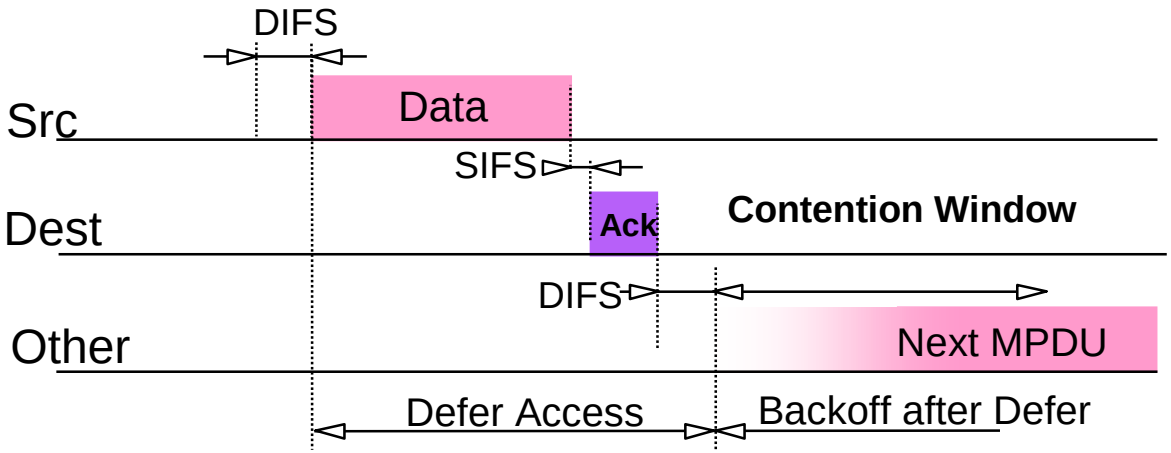

 

# Meinungen zum Einsatz von 5 GHz Systemen für WLAN Hotspots ...

SIEMENS mobile

- **IEEE802.11b (2.4 GHz) ist der dominierende Standard.**
- **Es gibt Bestrebungen, IEEE802.11b zu verbessern**
  - mehr Bandbreite (bis zu 54 Mbit/s)
  - QoS (die heutigen Anwendungen kommen gut ohne aus)
  - Netzfunktionen (Sicherheit und besserer Hand-over).
- **5 GHz Systeme werden wohl erst dann eingesetzt werden, wenn das 2.4 GHz ISM so überbelegt ist, dass kein vernünftiger Betrieb mehr möglich ist**
  - Anwendungen über TCP/IP sind sehr robust gegenüber fehlerbehafteten Übertragungswegen
- **Was es noch zu bedenken gibt:**
  - Kosten: 5 GHz ist teurer als 2.4 GHz
  - Leistungsverbrauch: Es wird für die gleiche Entfernung 7dB (5x) mehr Sendeleistung benötigt.
  - IEEE802.11 b/g wird weiterhin zusätzlich benötigt.

# Das CSMA/CA Zugriffsverfahren




DIFS: DCF InterFrame Space

SIFS: Short InterFrame Space

MPDU: MAC Protocol Data Unit

- **Reduzierte Wahrscheinlichkeit von Kollisionen**
  - alle Stationen verfolgen die aktuelle Belegung des Mediums
- **Zugriff wenn das Medium länger als DIFS frei ist,**
  - falls nicht, abwarten und Zugriff erst nach einer zusätzlichen Wartezeit
- **Empfänger quittiert korrekt empfangene Pakete sofort**
  - wenn der Sender kein ACK empfängt, wird angenommen, dass ein Fehler aufgetreten ist und die Übertragung wird wiederholt (unter Umständen mehrmals mit immer längeren Wartezeiten).

# IEEE802.11e: MAC Enhancements für Quality of Service (EDCF & HCF)

Upcoming

SIEMENS mobile

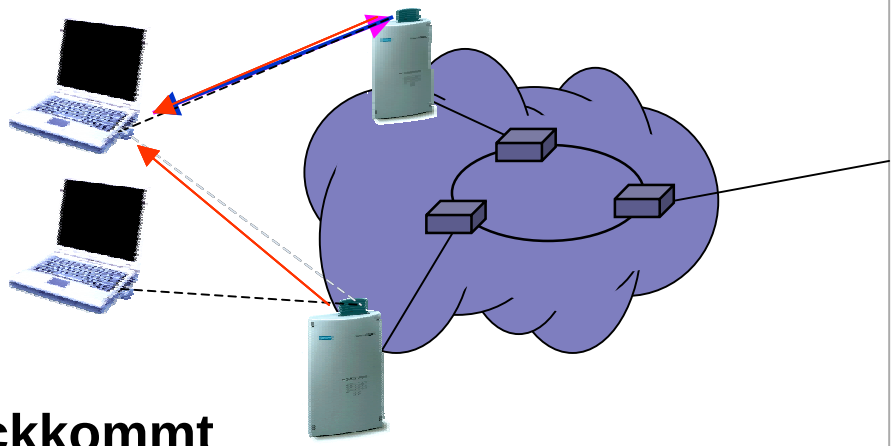
- **EDCF (Enhanced Distributed Coordination Function)**
  - priorisierter DCF Zugriff auf das Medium in Abhängig von der Traffic-Klasse (4 unterschiedliche Stufen)
  - es gibt mehrere Übertragungspuffer mit unterschiedlicher Zugriffspriorität auf das Medium wobei die Wartezeiten bei den niederprioren Traffic-Klassen länger sind.
- **HCF (Hybrid coordination function)**
  - nur im QoS-erweiterten Infrastruktur-Mode
  - wird zur Steuerung auch in der DCF Phase verwendet
  - basiert auf einem QoS-fähigen zentralen Koordinator
    - im Access Point (quality enhanced access point - QAP)
    - verwendet die höhere Priorität des PCF Mode
  - ist in der Lage, definierte Jitter-, Durchsatz- und Verzögerungszeiten zu realisieren.

**In der Standardisierung gibt es lang anhaltende Diskussionen über HCF.**

# Hand-over innerhalb eines WLAN Hotspots

SIEMENS mobile

- **Endgerät erkennt, dass die Übertragungsqualität zum Access Point (AP) nachlässt.**
- **Endgerät scannt das Band auf Suche nach einem anderen AP**
  - oder verwendet die Ergebnisse früherer Messungen
- **Endgerät schickt Reassociation Request an den neuen AP**




- **Wenn Reassociation Response zurückkommt**
  - dann ist das Endgerät zum neuen AP ‚geroamt'
  - andernfalls wird die Suche weitergeführt.
- **Wenn der AP den Reassociation Request annimmt,**
  - wird der alte AP normalerweise über das Verteilsystem informiert
  - zeigt der neue AP die Reassociaton dem Verteilsystem an

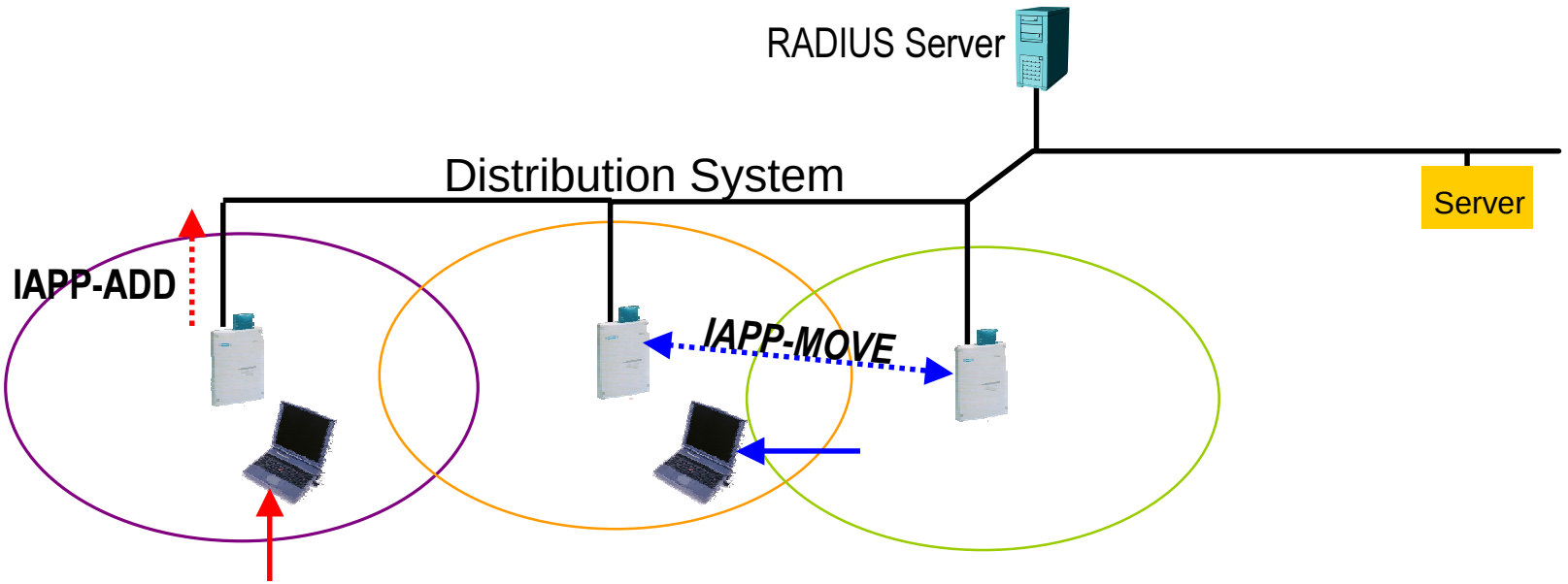
 

# IEEE802.11f: Inter-Access Point Protocol (IAPP)

Upcoming

SIEMENS mobile

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



# IEEE802.11
# Verschlüsselung und Zugangskontrolle

SIEMENS mobile

- **Das Ziel der P802.11 war eine dem Draht vergleichbare Sicherheit (Wired Equivalent Privacy - WEP) zu realisieren**
  - Weltweite Einsetzbarkeit
- **802.11 besitzt eine Authentisierungsfunktion**
  - Zugangskontrolle zum WLAN
  - Optionen für “OPEN”, “Shared Key” oder herstellerspezifische Lösungen
- **„Shared key“ Authentisierung basiert auf WEP**
  - Geräte, nicht Nutzer werden authentisiert
  - WEP setzt einen RC4 Algorithmus ein mit
    - einen 40 bit secret key
    - einen 24 bit Initialisierungs-Vector (IV)
    - und einen Integrity Check Vector (ICV) im Datenpaket.

# Die Schwächen der WEP Sicherheit

SIEMENS mobile

- **WEP ist unsicher bei jeder Schlüssellänge**
  - IV Raum zu klein, fehlende *Reply Protection*
  - *known plaintext* Angriffe
- **Keine Benutzer-Authentisierung**
  - Nur die Netzwerk-Interfaces werden authentisiert.
- **Keine beidseitige Authentisierung**
  - Nur Endgerät gegenüber Access Point
- **Fehlende Schlüsselverwaltung**
  - Keine standardisierte Methode zum Austausch der Schlüssel
  - Geringe Unterstützung von Teilnehmer-spezifischen Schlüsseln für größere Gruppen
- **WEP ist kein Mittel um einen sicheren WLAN Zugang zu gewähren,**
  - … aber es kann für einfachere Fälle durchaus ausreichend sein.

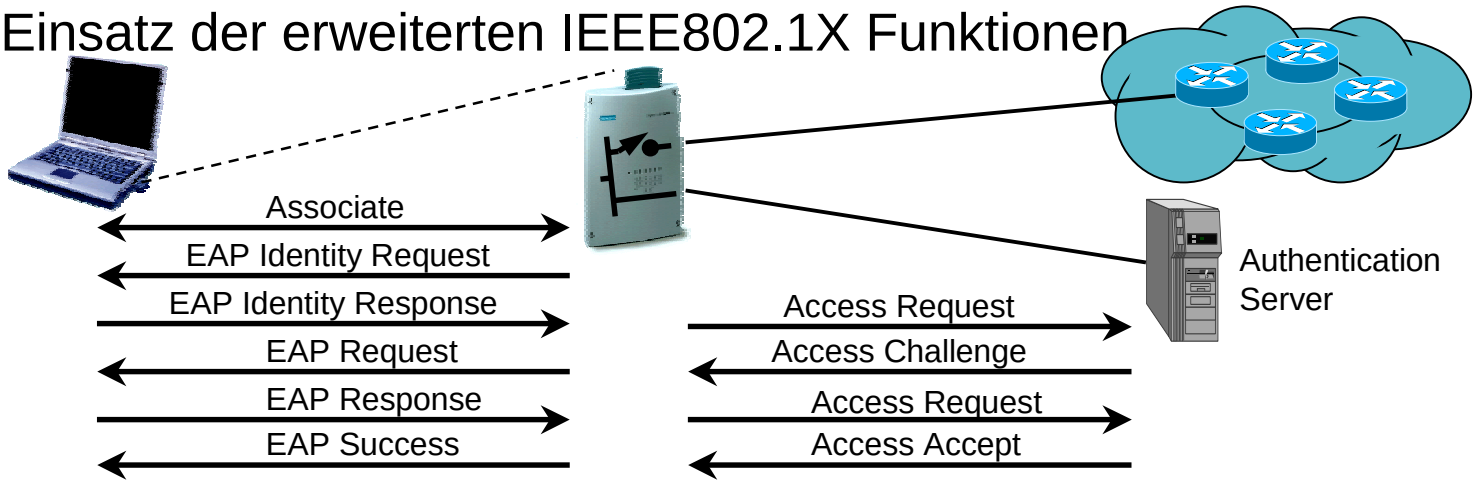
# IEEE802.11i: Robust Security Network (RSN)

Upcoming

SIEMENS mobile

**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:**
  - RSN Verhandlungsprozeduren um den Kontext aufzubauen
  - Einsatz der erweiterten IEEE802.1X Funktionen



# Eigenschaften des IEEE802.11 Standards

SIEMENS mobile

- **Ein gemeinsamer MAC, der verschiedene PHY bedient**
- **Zwei Konfigurationen:**
  - Ad-hoc (Peer-to-peer, independent) und Infrastruktur (mit Access Point)
- **Der Zugriff auf das Medium wird mit CSMA/CA (collision avoidance) geregelt und kann optional durch einen zentral gesteuert werden (Point coordinator)**
- **Datenübertragung mit dem**
  - Connectionless Service
    - Daten werde ohne vorhergehende Reservierung des Mediums übertragen
    - vor allem für burst-artige Anwendungen geeignet
    - Service entspricht dem Übertragungsverfahren des Internet
  - Isochronous Service
    - reserviert das Medium für einzelne Verbindungen auch wenn keine Daten übertragen werden
    - funktioniert nur wenn keine räumliche Überlappung der WLAN Zellen stattfindet
- **Robust gegen Rauschen and Interferenzen durch Überprüfung der erfolgreichen Datenübertragung im Link Layer (ACK)**
- **Mechanismus gegen Hidden Node Problem (RTS/CTS)**
- **Mobilität (Hand-over Mechanismus)**
- **Sicherheit (WEP)**
- **Funktionen zur Reduktion des Leistungsbedarfs der Endgeräte**

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

## früher: WECA (Wireless Ethernet Compliance Alliance)

SIEMENS mobile

- **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
- **Insgesamt 194 Mitgliedsfirmen**
- **505 zertifizierte Produkte seit Beginn**
  - bis jetzt ausschließlich IEEE 802.11b, derzeit ca. 20 neue Zertifizierungen pro Woche
- **Derzeitige Aktivitäten:**
  - Bekanntmachung und Umsetzung der neuen Gütesiegel-Strategie
    - einheitliches Wi-Fi Logo für alle IEEE 802.11 Zertifizierungen
    - produktspezifisch ergänzt durch die Kennzeichnung der getesteten Funktionalitäten
  - Beginn der 802.11a Wi-Fi Zertifikation inklusive Dual-Band Funktion
  - Bekanntmachung der *Wi-Fi Protected Access (WPA)* Initiative
  - Weitere Vorbereitung des *Wi-Fi Zone* Programms

# Wi-Fi Logo und produktspezifische Kennzeichnung

SIEMENS mobile


Logo der Wi-Fi Alliance


Gütesiegel


Produktkennzeichnung

# Wi-Fi Protected Access (WPA)

SIEMENS mobile

- **WPA ist eine technische Lösung um kurzfristig dem größtem Problem einer weiteren Verbreitung von Wi-Fi Produkten zu begegnen.**
- **Untermenge des kommenden Standards IEEE802.11i.**
- **Zertifizierung ab Februar 2003, verpflichtend ab Oktober 2003**
- **Funktionen:**
  - Sicherheit nur für den Infrastruktur Betrieb
  - Verwendung von 802.1X zusammen mit 802.11
  - Ersatz von WEP durch TKIP/Michael
  - Zentrale Authentisierung mittels RADIUS Server
  - Für den Heimbetrieb auch ohne RADIUS möglich
  - Optional gleichzeitiger Zugang für WPA-Clients und Nicht-WPA Clients
- **Nicht berücksichtigt:**
  - Sicherer Ad-hoc Mode
  - Fast handoff
  - Denial of Service Angriffe

# Der Betrieb von WLAN Hotspots...


- ✓ **Keine Installationen auf Kundenrechnern**
- ✓ **Angebot an alle potentiellen Nutzer**
- ✓ **Der Zugang ist selbsterklärend**

# WLAN-Betreiber zu werden ist recht einfach...

SIEMENS mobile

- **Rechtliche Gesichtspunkte:**
  - Lizenzfreie Nutzung des 2,4 GHz ISM Band
  - Keine Telekommunikationslizenz notwendig, solange
    - kein Telefoniedienst angeboten wird,
    - kein grundstücksübergreifende Übertragung angeboten wird.
- **Kosten:**
  - Die untere Grenze:
    Investment: WLAN Access Point mit DSL Router (~ 350 €)
    Operation: ~ 60 €/Monat für eine DSL Flat Rate
  - Die meisten kommerziellen Einrichtungen sind erheblich aufwendiger, vor allem wegen der Abrechnung von Nutzungskosten.
- **Es ist recht einfach und ziemlich billig, einen WLAN Hotspot aufzumachen, wenn man Kenntnis davon hat,**

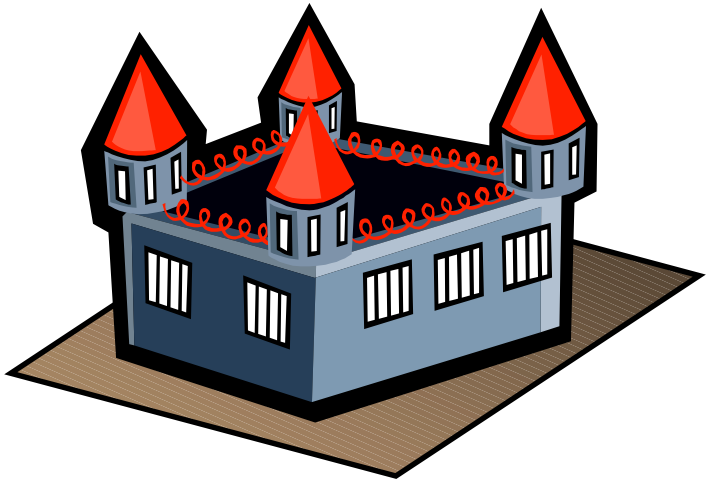
*... und die meisten werden das auch wissen,*
*sobald sie WLAN in ihrem Wohnzimmer installiert haben!*

# Beim Verkauf von WLAN Zugang gelten die selben Regeln wie sonst auch…

SIEMENS mobile

- **Welches Geschäft würden Sie bevorzugen?**

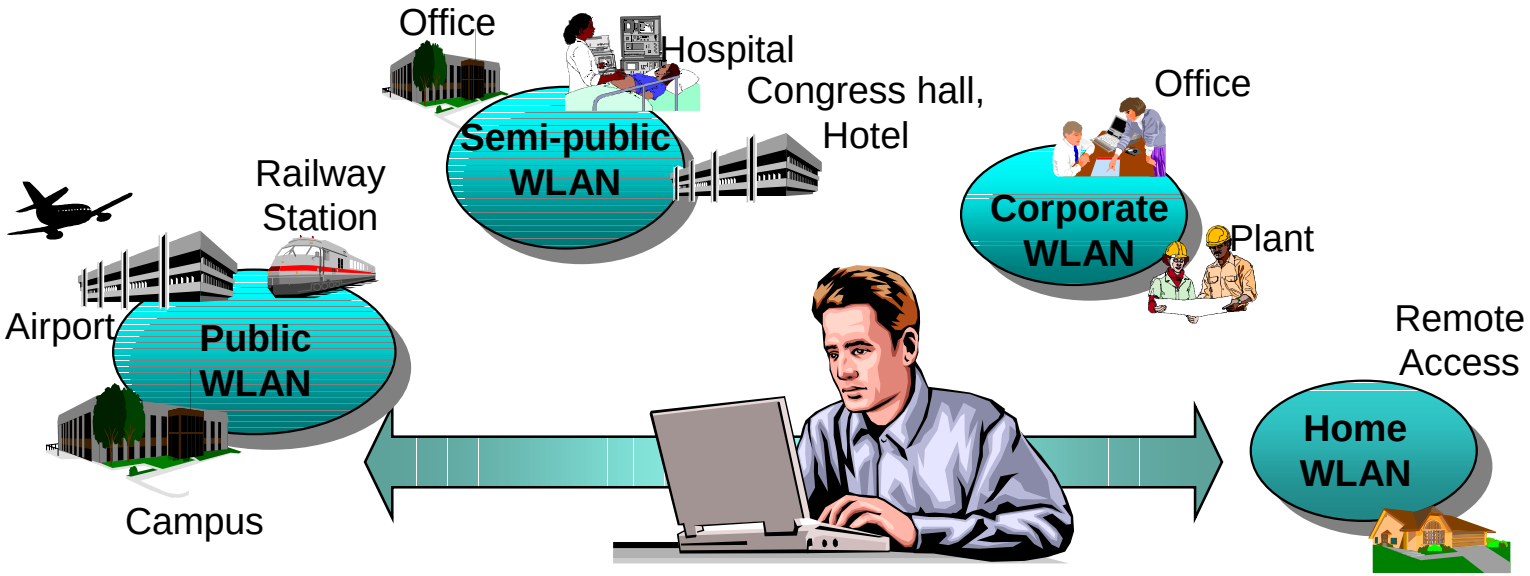


***Zu viel Sicherheit schadet dem Umsatz!***

# WLAN-Hotspots aus Nutzersicht: *„Eine Lösung für immer und überall“*

SIEMENS mobile

- **Die Nutzer kommen mit vielen verschiedenen Geräten, und jeder Nutzer hat auch noch seine eigene Konfiguration.**
- **Man sollte davon ausgehen, dass nur ganz wenige Voraussetzungen bei der Mehrzahl gegeben ist.**



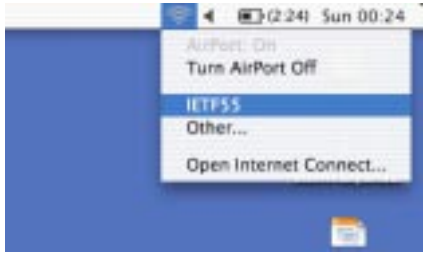

- **Die meisten WLAN-Notebooks erhalten ihre Netzwerk-Konfiguration mittels DHCP.**
- **Ein Web-Browser dürfte auf allen Notebooks vorhanden sein.**

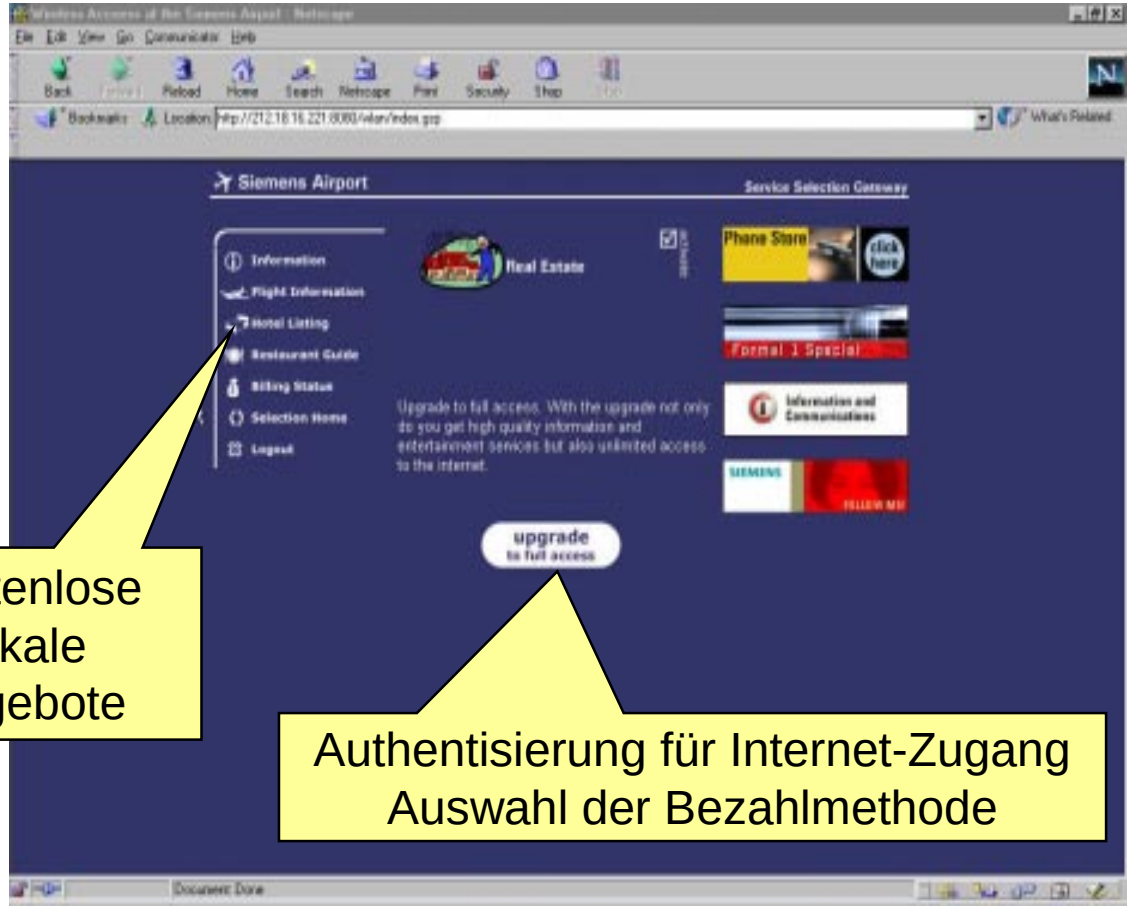
# Geübte WLAN Nutzer wissen: Jede Session beginnt mit einer Web-Seite

SIEMENS mobile

- **Nach dem Einbuchen ins WLAN...**




**...ein Check der Netzverbindung mit dem Web-Browser**



# Mobilfunk und Wireless LAN

SIEMENS mobile

## GSM/GPRS/UMTS

- immer und überall
- Telephonie, Messaging
- QoS
- kostbare Bandbreite
- wenige große Betreiber
- hochverfügbar
- große Kundenbasis
- große Umsätze

## WLAN IEEE802.11

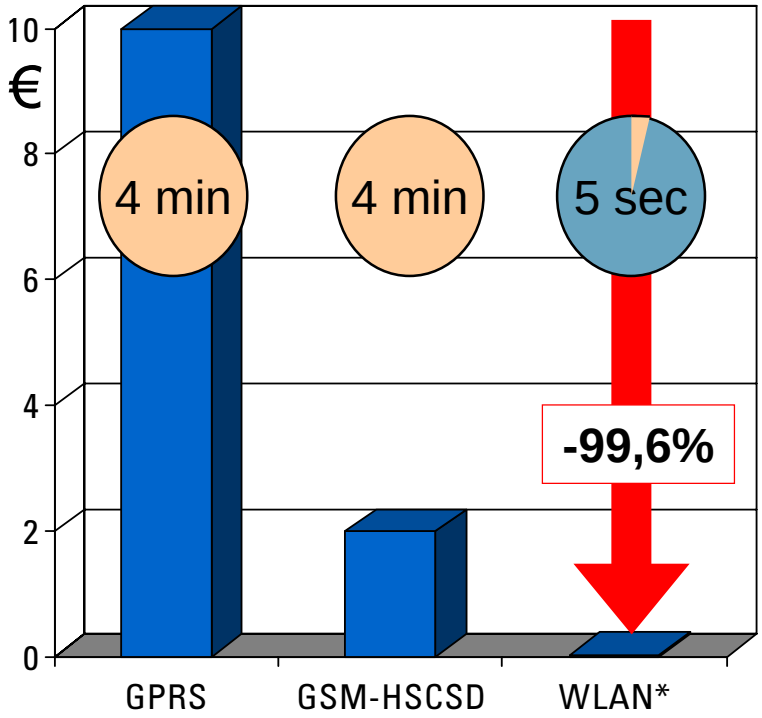
- gelegentlich an bestimmten Stellen
- email, Web
- ‚best effort'
- billige Bandbreite
- viele Betreiber, ISP Markt
- unspezifiziert
- Gelegenheitsnutzer
- kleine Umsätze

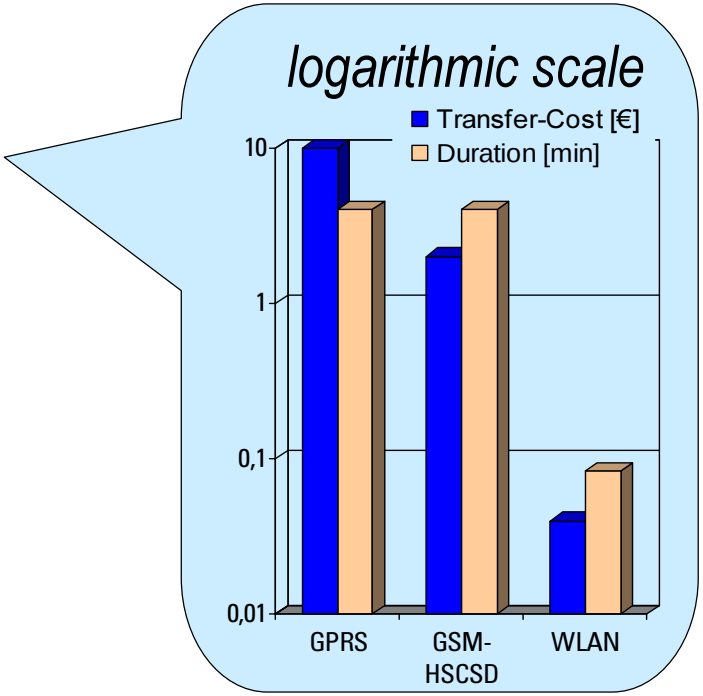
 

# WLAN ist viel billiger als 2G/3G

SIEMENS mobile

Übertragungskosten/-dauer eines 1 Mbyte .ppt/.doc/.xls Dokuments




* **based on current IP volume prices of 40€ /GByte.**
**Time based pricing results in similar costs,**
**e.g. MobileStar Pulsar pricing plan: $0,10/min**

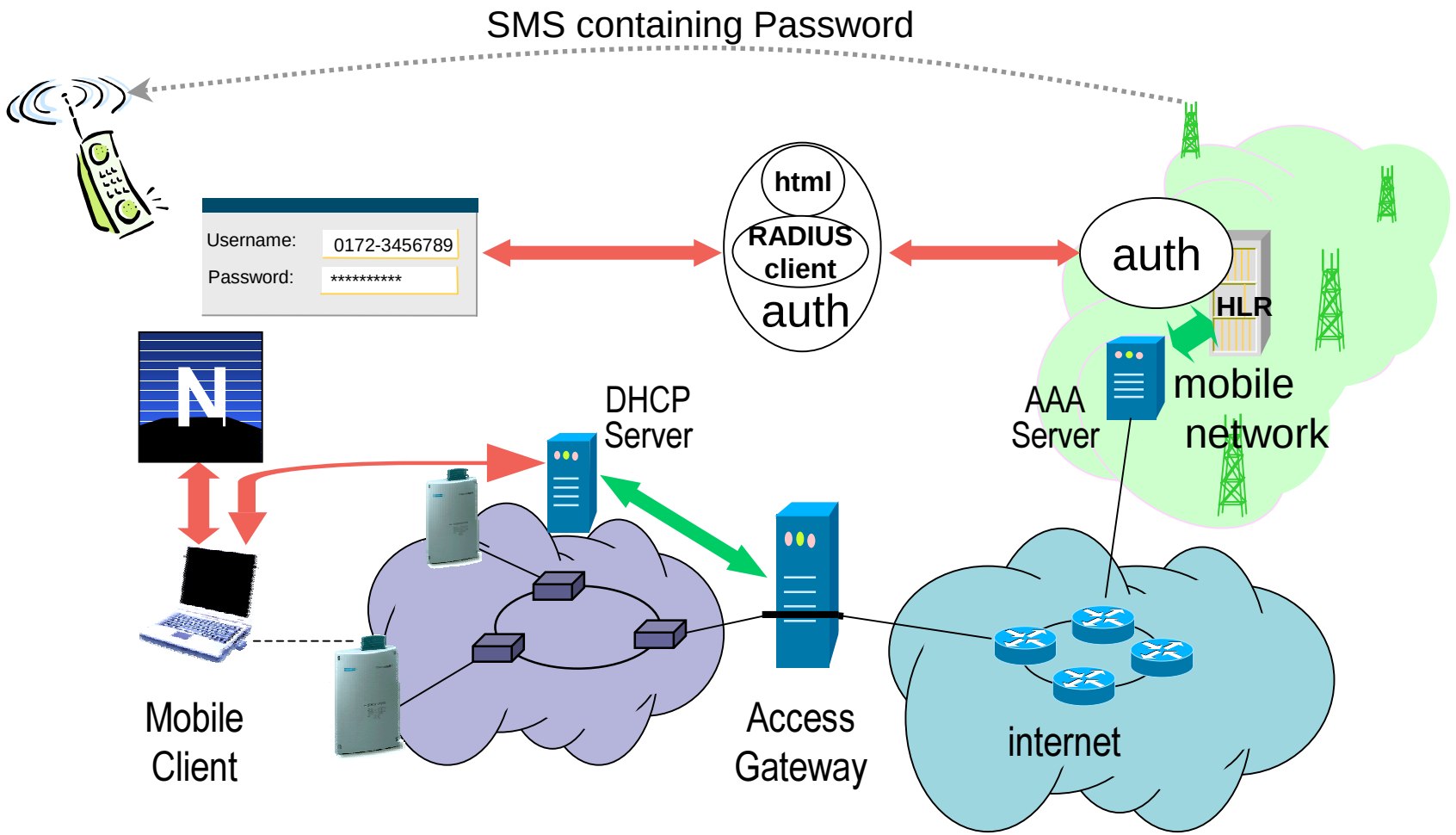
# Konsequenz für Mobilfunkbetreiber

SIEMENS mobile

Wenn man sie nicht aufhalten kann
und wenn man sie nicht schlagen kann
dann sollte man sich mit ihnen verbünden.

- **Die schwierigste und aufwendigste Funktion eines WLAN Hotspot Betreibers ist die Abrechnung der Benutzungskosten.**
- **Mobilfunkbetreiber haben sichere Abrechnungsmöglichkeiten mit vielen potentiellen WLAN Nutzern.**
- **Die Bereitstellung der Abrechnung für WLAN Hotspots kann ein wesentlicher Meilenstein für die Einführung von „Mobile Payment“ sein.**
- **Es gibt keine Zeit zu verlieren!**
  **Der Markt für WLAN Hotspots explodiert und es ist zu erwarten, dass der WLAN Zugang in einigen Jahren in vielen Hotspots ‚kostenlos‘ ist (2...4 Jahre).**

# Ein Beispiel für die Authentisierung und Bezahlung über den Mobilfunkbetreiber



# Standardisierung für WLAN/UMTS interworking

SIEMENS mobile

- **3GPP**
  - R5: SA1 - erledigt:
    „Requirements of 3GPP system – WLAN interworking“.
  - R6: SA2
    Weiterführung mit der Spezifikation einer Architektur
- **ETSI BRAN**
  **Untergruppe “Interworking between HiperLAN/2 and 3rd generation cellular and other public systems”.**
  - Detaillierte Architekturbeschreibung im wesentlichen basierend auf dem von Siemens eingebrachten ‘loose coupling’ Prinzips
  - IEEE802.11 und ARIB MMAC haben sich dieser Aktivität angeschlossen.
    => Wireless Interworking Group (WIG).
- **Wi-Fi Alliance ‘Wireless ISP Roaming Initiative’**
  - Detaillierte Spezifikation für den Zugang zu und das Roaming zwischen IEEE802.11 WLAN Hotspots.
  - Spezifikation ist eigentlich im WISP Umfeld entstanden, kann aber auch problemlos für die Anbindung an Mobilfunknetze genutzt werden.

# Das Ende.

SIEMENS mobile

- **Danke für Ihre Aufmerksamkeit.**
- **Fragen, Kommentare?**

**Maximilian Riegel** **(maximilian.riegel@siemens.com)**
**(http://www.max.franken.de)**

**Literatur zu IEEE802.11:**

- **The IEEE 802.11 Handbook – A Designer‘s Companion**
  **Bob O‘Hara, Al Patrick; IEEE press, ISBN 0-7381-1855-9**
- **802.11 Wireless Networks – The Definitive Guide**
  **Matthew S. Gast; O‘ Reilly, ISBN 0-596-00183-5**