SIEMENS mobile

Aktuelle Entwicklungen in der Standardisierung für drahtlose lokale Netzwerke

Maximilian Riegel

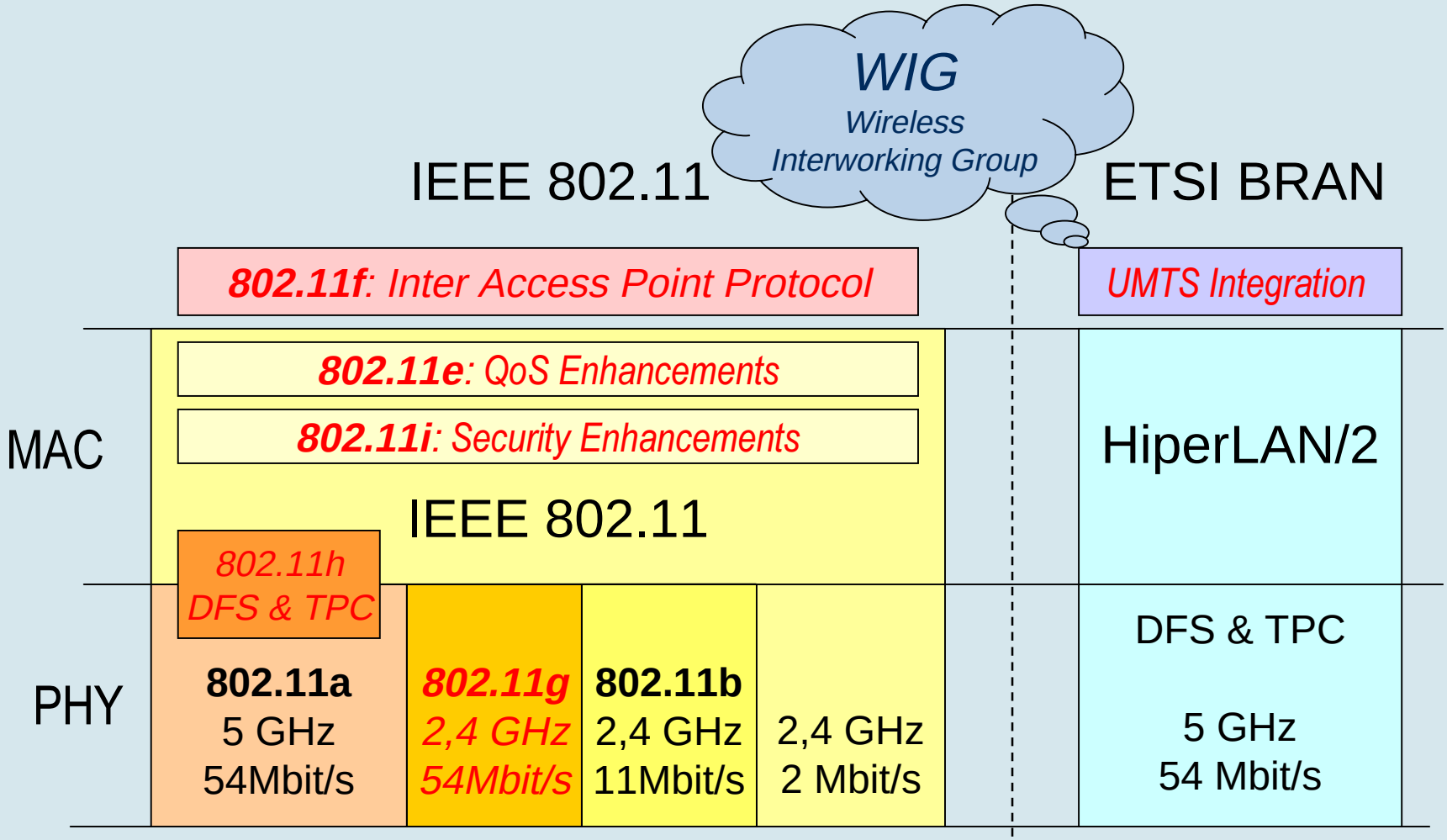
Siemens AG, ICM Networks

2002-10-02

Outline

- **WLAN standardization overview**
- **The IEEE802.11 WLAN standard and its enhancements**
  - Architecture
  - Physical layer
  - Spectrum issues
  - MAC layer functions
  - Configurations
  - Handover
  - Privacy and access control
- **WLAN security**
- **WLAN – UMTS interworking**
  - Tight coupling approach
  - Market and application considerations
  - “Loose” coupling
  - Standardization activities

Wireless LAN Standardization

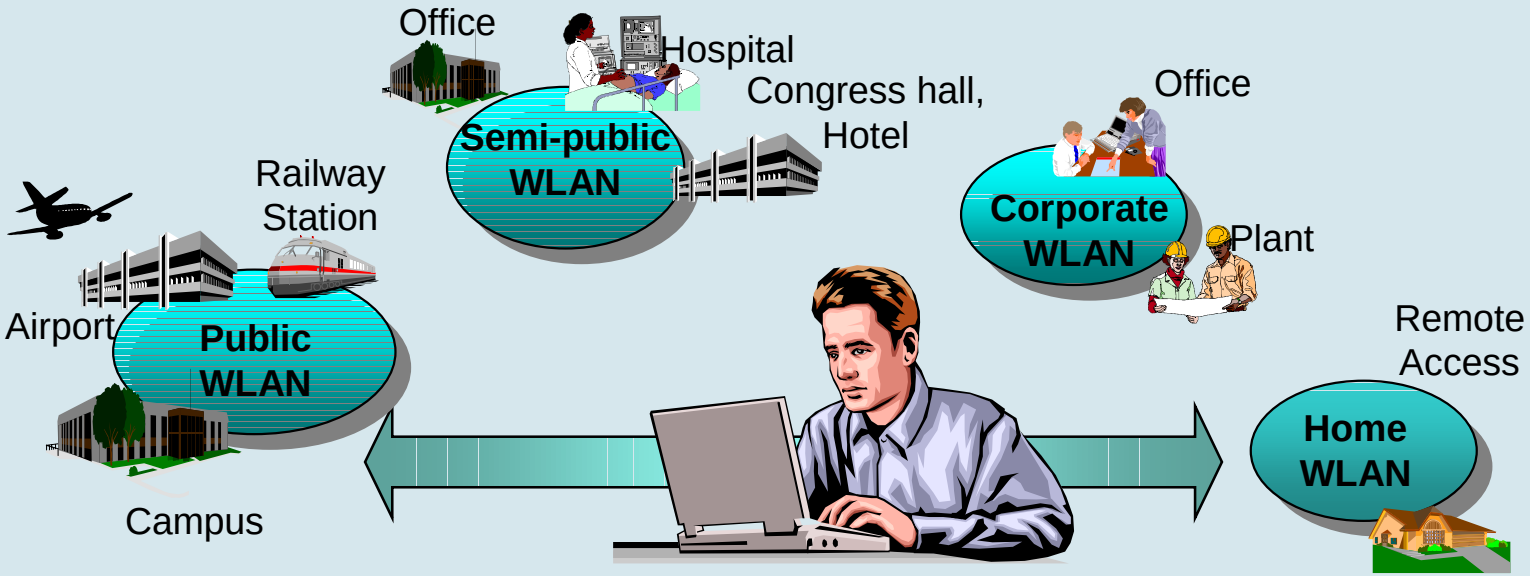


Current standardization topics

The ubiquitous WLAN

SIEMENS mobile

- Today's road worriers require access to the Internet everywhere.
- WLAN is more than just cable replacement, it provides hassle-free broadband Internet access everywhere.



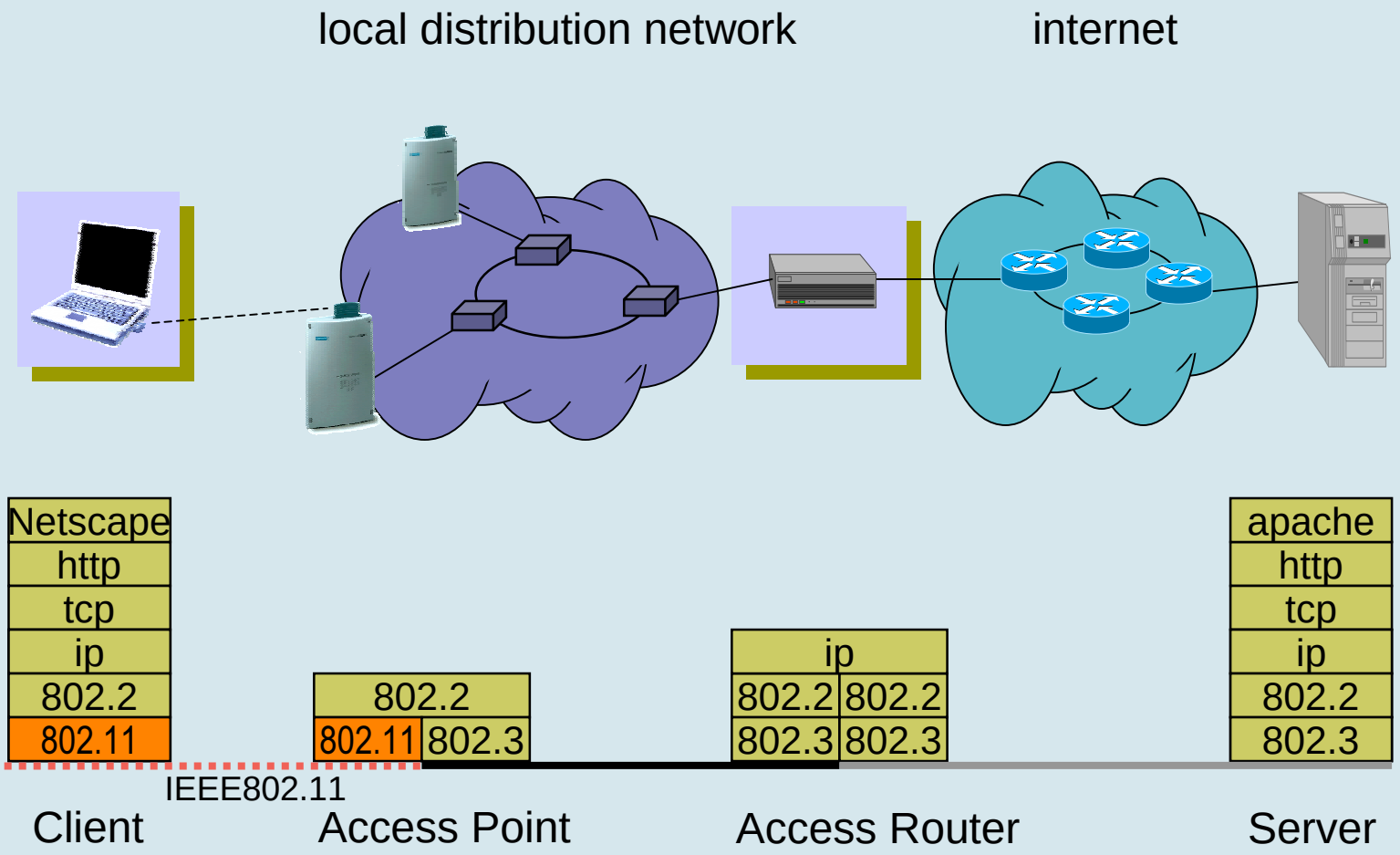
- Coverage in 'hot-spots' sufficient.
- IEEE802.11b meets the expectations for easiness, cost and bandwidth.

Wireless IEEE802.11 Standard

SIEMENS mobile

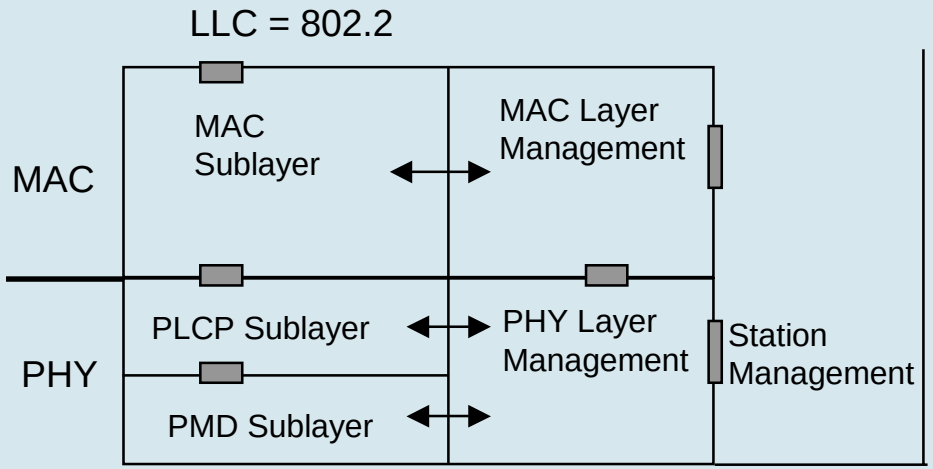
- **Base standard approved June 1997**
  - 802.11b approved Sept. 1999
- **Operation in the 2.4GHz ISM band**
  - USA: FCC part 15.247-15.249
  - Europe: ETS 300-328
  - Japan: RCR-STD-33A
- **Supports three PHY layer types: DSSS, FHSS, Infrared**
- **MAC layer common to all 3 PHY layers**
- **Supports peer-to-peer and infrastructure configurations**
- **IEEE802.11b high data rate extension with 11 Mbps using existing MAC layer**
- **IEEE802.11a for operation in the 5 GHz band with up to 54 Mbit/s using the same MAC layer**

Wireless LAN IEEE802.11
Basic Architecture



IEEE802.11 Protocol Architecture

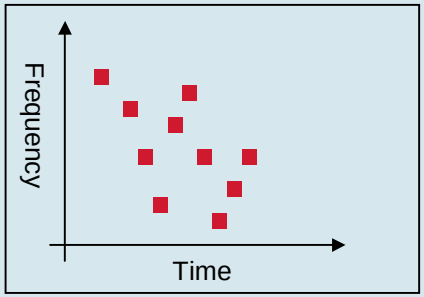
- **Station Management**
  - interacts with both MAC Management and PHY Management
- **MAC Layer Management Entity**
  - power management
  - handover
  - MAC MIB
- **MAC Entity**
  - basic access mechanism
  - fragmentation
  - encryption
- **PHY Layer Management**
  - channel tuning
  - PHY MIB
- **Physical Layer Convergence Protocol (PLCP)**
  - PHY-specific, supports common PHY SAP
  - provides Clear Channel Assessment signal (carrier sense)
- **Physical Medium Dependent Sublayer (PMD)**
  - modulation and encoding



IEEE 802.11
2.4 GHz & 5 GHz Physical Layers

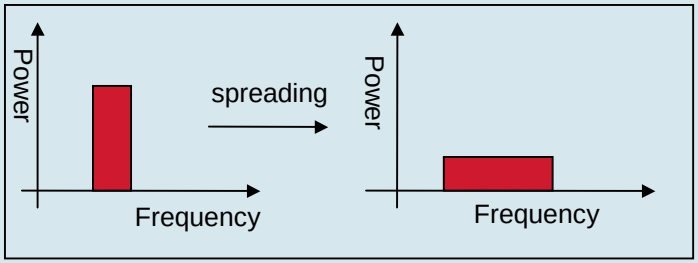
SIEMENS mobile

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



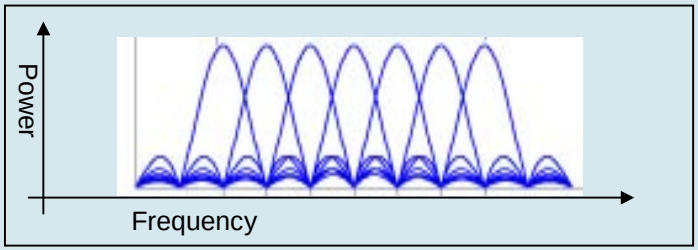
- **2.4 GHz *Frequency Hopping Spread Spectrum***
  - 2/4 FSK with 1/2 Mbps
  - 79 non overlapping frequencies of 1 MHz width (US)

- **2.4 GHz *Direct Sequence Spread Spectrum***
  - DBPSK/DQPSK with 1/2 Mbps
  - Spreading with 11 Bit barker Code
  - 11/13 channels in the 2.4 GHz band



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

- **5 GHz *OFDM* PHY (802.11a)**
  - Basic parameters identical to HiperLAN2 PHY
  - European regulatory issues unsolved

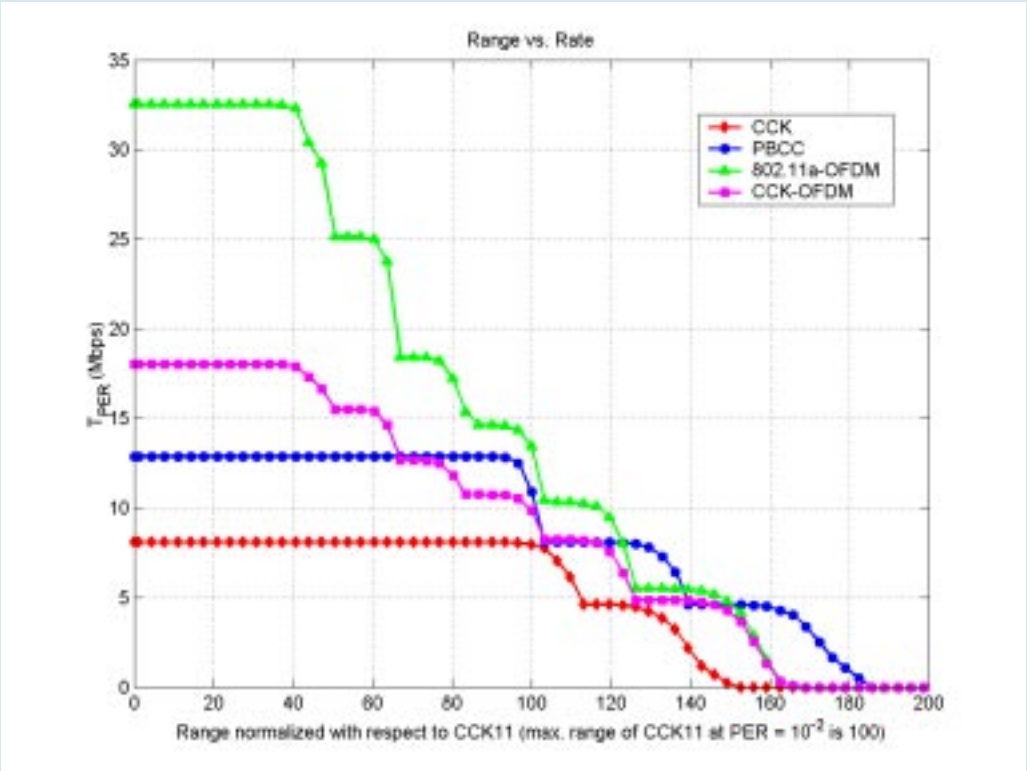


IEEE802.11g: Further Speed Extension for the 2.4GHz Band

Upcoming

SIEMENS mobile

- **Mandatory:** CCK w/ short preample (802.11b) and OFDM (802.11a applied to 2.4 GHz range).
- **Optional:** PBCC proposal for 22 Mbit/s from Texas Instruments
- **Optional:** CCK-OFDM proposal for up to 54 Mbit/s from Intersil

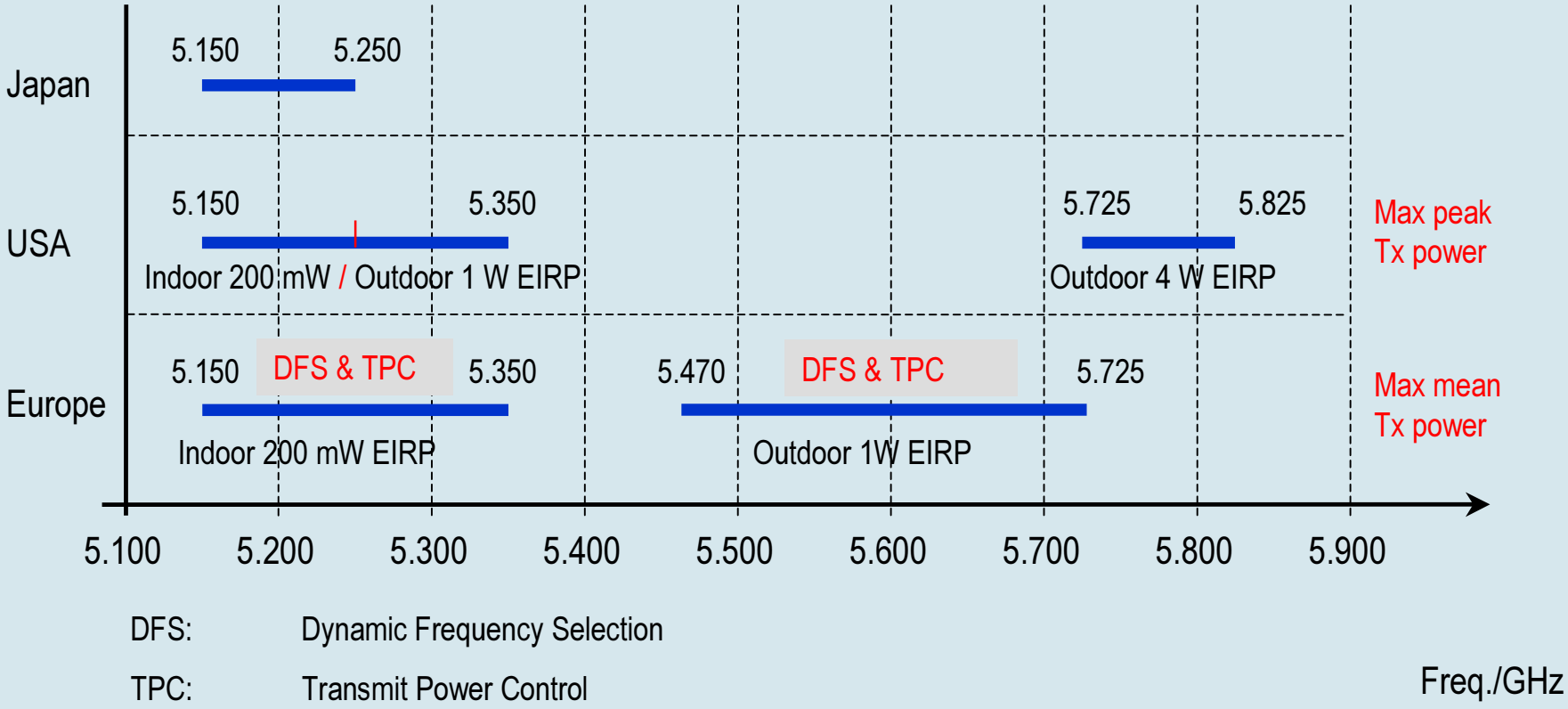


Range vs. throughput rate comparison of

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

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

Spectrum Designation in the 5 GHz range



- **Many European countries are currently opening the 5 GHz range for radio LANs.**

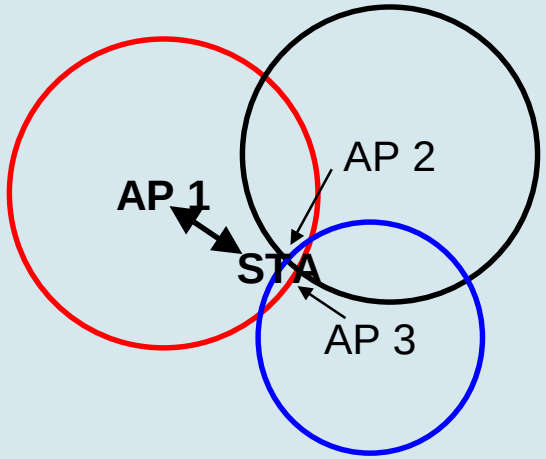
IEEE802.11h: Spectrum and Transmit Power Management

Upcoming

SIEMENS mobile

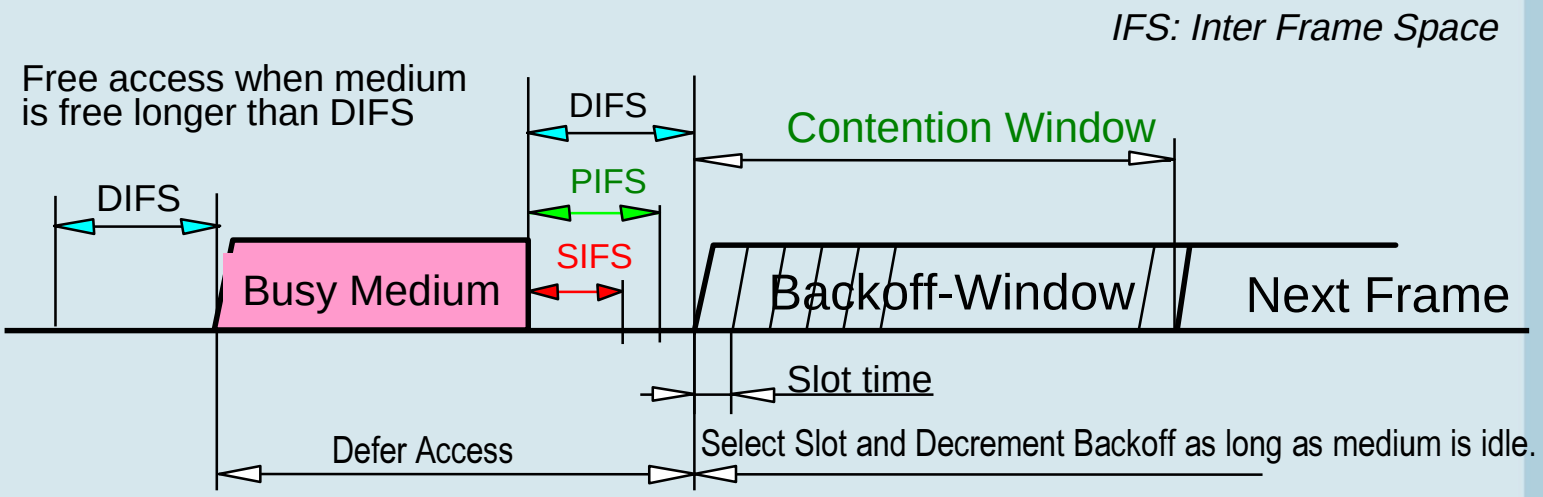
- **TPC (Transmission Power Control)**
  - supports interference minimisation, power consumption reduction, range control and link robustness.
  - TPC procedures include:
    - AP‘s define and communicate regulatory and local transmit power constraints
    - Stations select transmit powers for each frame according to local and regulatory constraints

- **DFS (Dynamic Frequency Selection)**
  - AP‘s make the decision
  - STA‘s provide detailed reports about spectrum usage at their locations.



CSMA/CA Explained

SIEMENS mobile



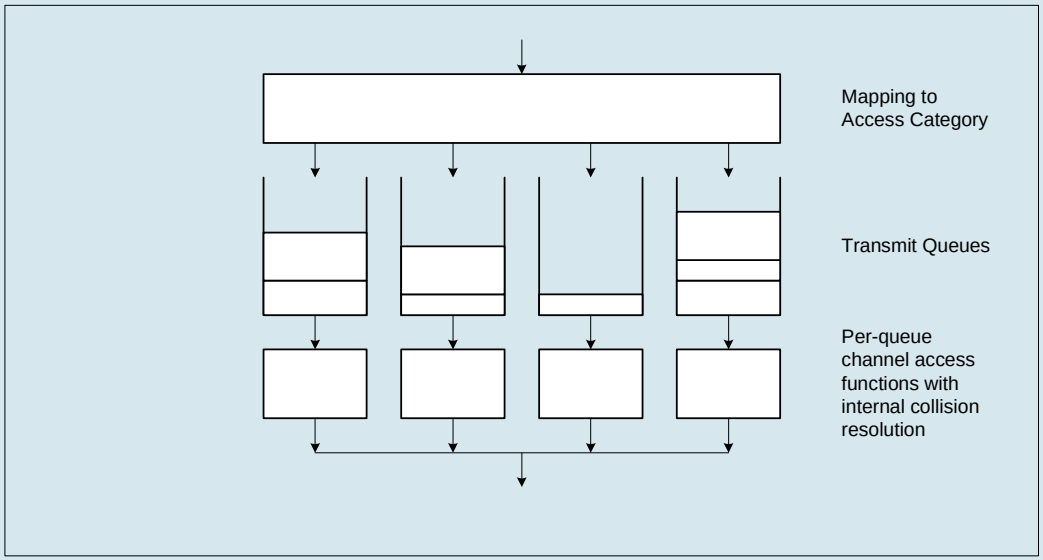
- **Reduce collision probability where mostly needed.**
  - Stations are waiting for medium to become free.
  - Select Random Backoff after a Defer, resolving contention to avoid collisions.
- **Efficient Backoff algorithm stable at high loads.**
  - Exponential Backoff window increases for retransmissions.
  - Backoff timer elapses only when medium is idle.
- **Implement different fixed priority levels**

IEEE802.11e: MAC Enhancements for Quality of Service (EDCF)

Upcoming

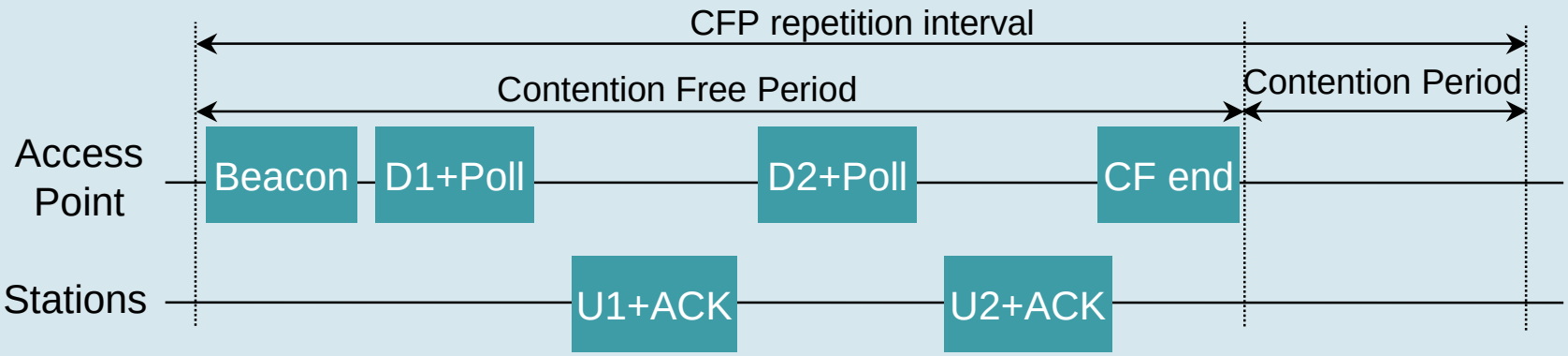
SIEMENS mobile

- **EDCF (Enhanced Distributed Coordination Function)**
  - differentiated DCF access to the wireless medium for prioritized traffic categories (4 different traffic categories)
  - output queue competes for TxOPs using EDCF wherein
    - the minimum specified idle duration time is a distinct value
    - the contention window is a variable window
    - lower priority queues defer to higher priority queues



IEEE802.11
Point Coordination Function (PCF)

SIEMENS mobile



- **Optional PCF mode provides alternating contention free and contention operation under the control of the access point**
- **The access point polls stations for data during contention free period**
- **Network Allocation Vector (NAV) defers the contention traffic until reset by the last PCF transfer**
- **PCF and DCF networks will defer to each other**
- **PCF improves the quality of service for time bounded data**

IEEE802.11e: MAC Enhancements for Quality of Service (HCF)

Upcoming

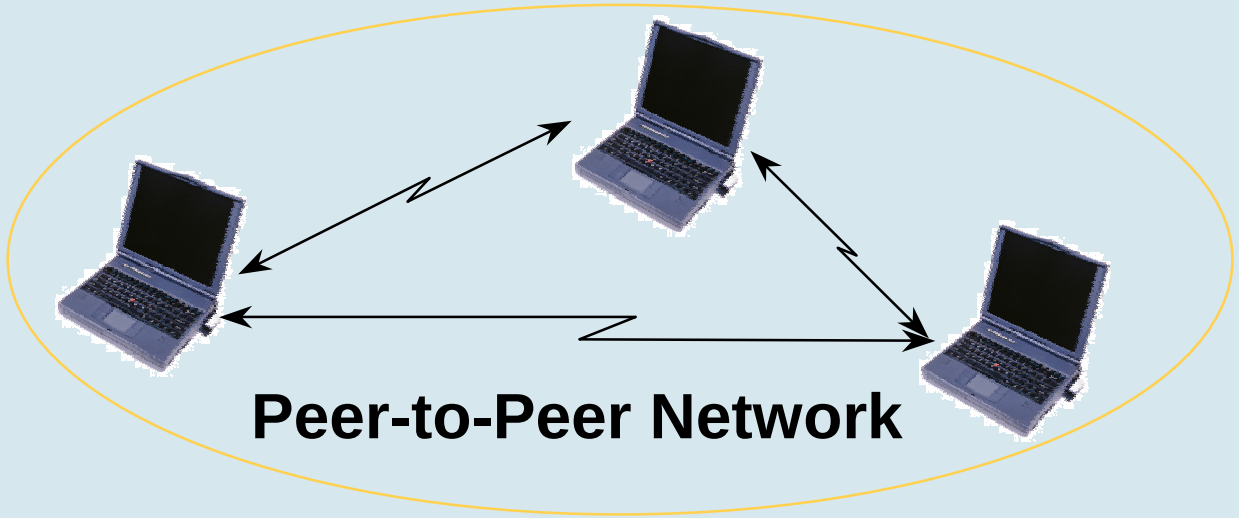
SIEMENS mobile

- **HCF (Hybrid coordination function)**
  - only usable in infrastructure QoS network configurations
  - to be used during both the contention period (CP) and the contention free period (CFP)
  - uses a QoS-aware point coordinator („hybrid coordinator“)
    - by default collocated with the enhanced access point (QAP)
    - uses the point coordinator's higher priority to allocate transmission opportunities (TxOPs) to stations
  - meets predefined service rate, delay and/or jitter requirements of particular traffic flows.

  - *Caused long delays in standardization process due to its complexity*
  - *Recently widely supported „Fast –Track“ proposal to come to a conclusion in TGe*
    - *Most complex functions eliminated, streamlined HCF, ...*

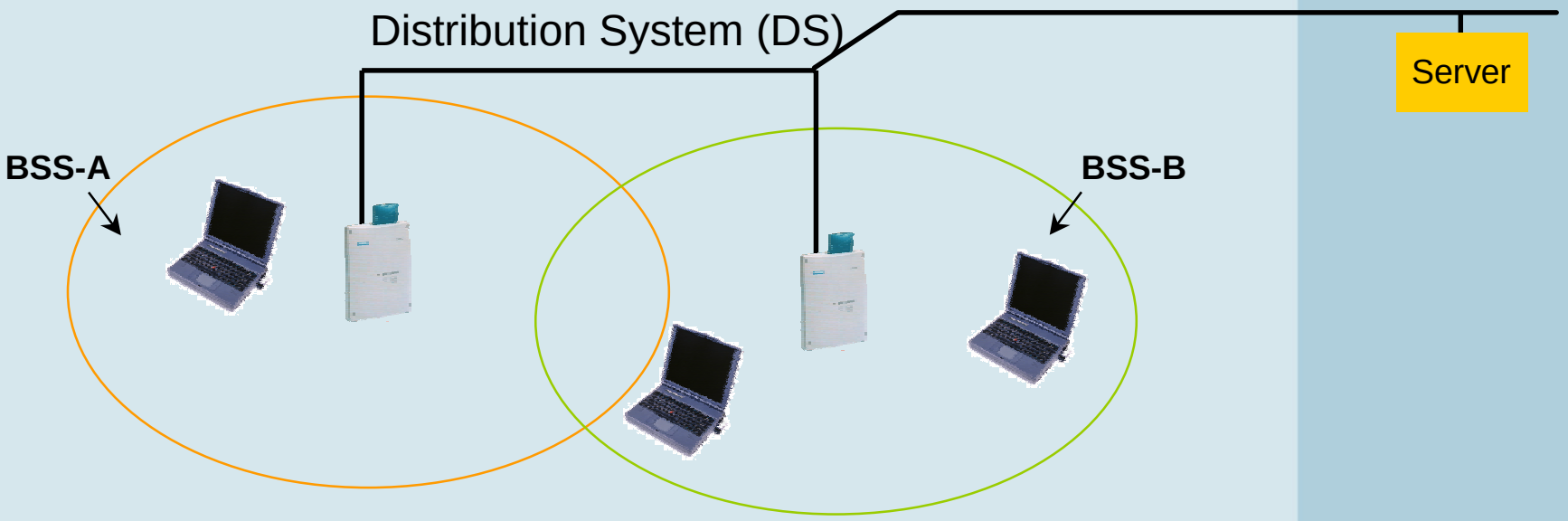
IEEE802.11 Ad Hoc Mode

SIEMENS mobile



- **Independent networking**
  - Use Distributed Coordination Function (DCF)
  - Forms a Basic Service Set (BSS)
  - Direct communication between stations
  - Coverage area limited by the range of individual stations

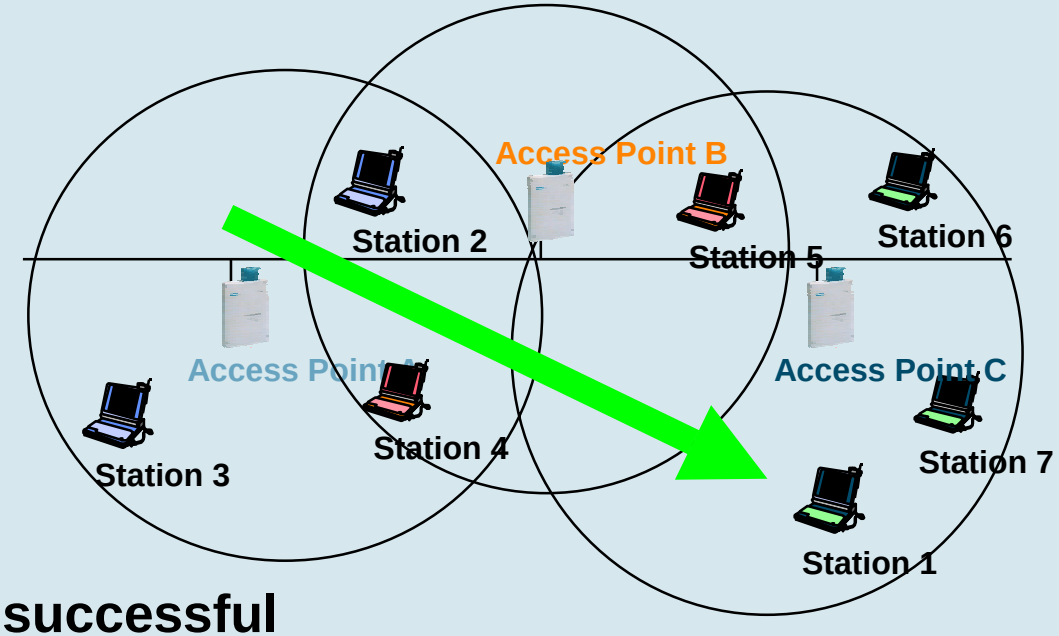
IEEE802.11 Infrastructure Mode



- Access Points (AP) and stations (STA)
- BSS (Basic Service Set): a set of stations controlled by a single coordination function
- Distribution system interconnects multiple cells via access points to form a single network
- Extends wireless coverage area and enables roaming

IEEE802.11 Handover

- **Station decides that link to its current AP is poor**
- **Station uses scanning function to find another AP**
  - or uses information from previous scans
- **Station sends Reassociation Request to new AP**
- **If Reassociation Response is successful**
  - then station has roamed to the new AP
  - else station scans for another AP
- **If AP accepts Reassociation Request**
  - AP indicates Reassociation to the Distribution System
  - Distribution System information is updated
  - normally old AP is notified through Distribution System

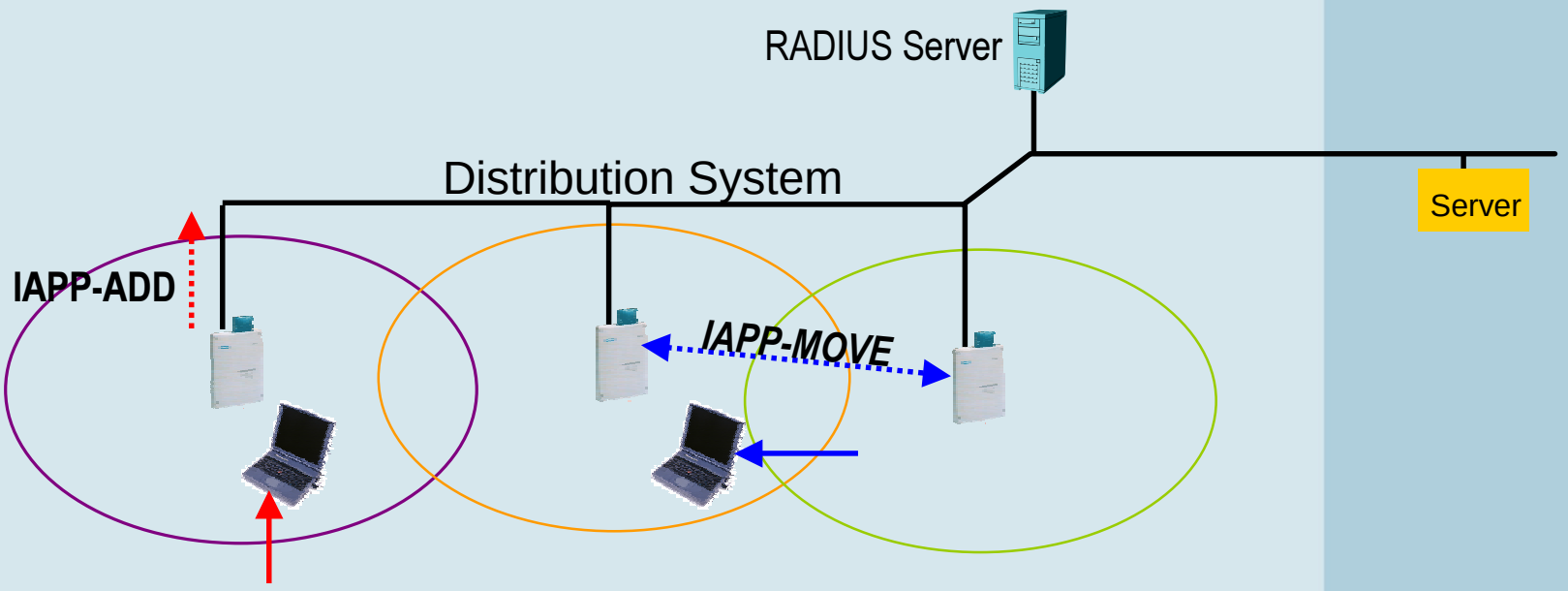


IEEE802.11f: Inter-Access Point Protocol (IAPP)

Upcoming

SIEMENS mobile

- **IAPP defines procedures for**
  - context transfer between APs when stations move
  - automatic configuration handling of access points



IEEE802.11 Privacy and Access Control

SIEMENS mobile

- **Goal of 802.11 was to provide "Wired Equivalent Privacy" (WEP)**
  - Usable worldwide
- **802.11 provides for an authentication mechanism**
  - To aid in access control.
  - Has provisions for "OPEN", "Shared Key" or proprietary authentication extensions.
- **Shared key authentication is based on WEP privacy mechanism**
  - Limited for station-to-station traffic, so not "end to end".
  - Uses RC4 algorithm based on:
    - a 40 bit secret key
    - and a 24 bit IV that is send with the data.
    - includes an ICV to allow integrity check.

Shortcomings of plain WEP security

SIEMENS mobile

- **WEP unsecure at any key length**
  - IV space too small, lack of IV replay protection
  - known plaintext attacks
- **No user authentication**
  - Only NICs are authenticated
- **No mutual authentication**
  - Only station is authenticated against access point
- **Missing key management protocol**
  - No standardized way to change keys on the fly
  - Difficult to manage per-user keys for larger groups

- **WEP is no mean to provide security for WLAN access,**
  - … but might be sufficient for casual uses.

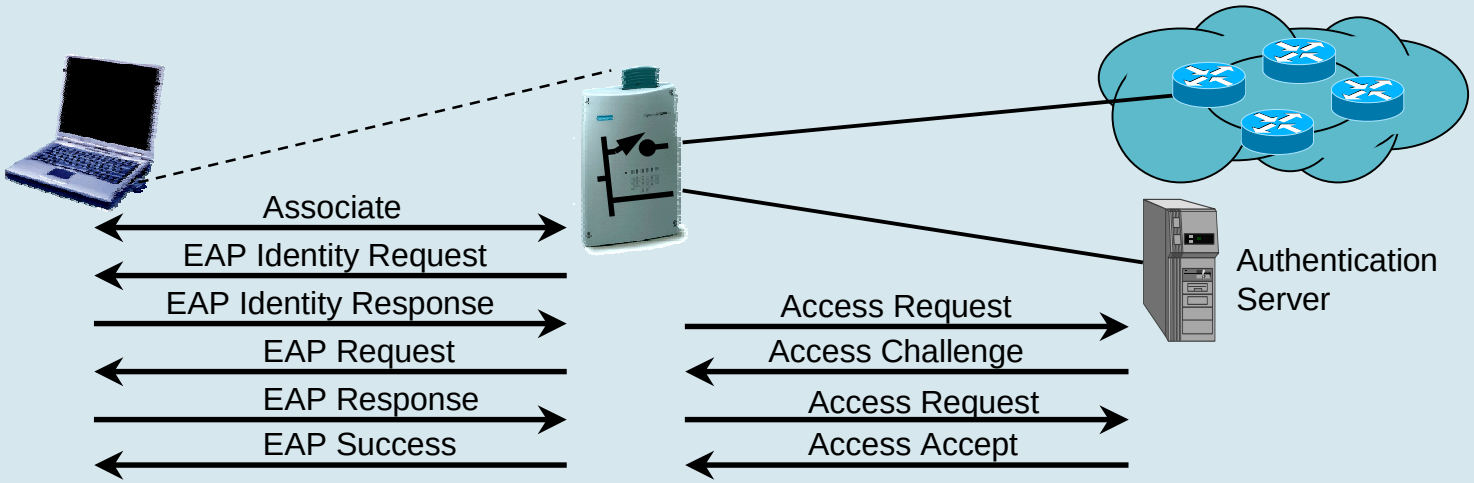
IEEE802.11i: Robust Security Network (RSN)

Upcoming

SIEMENS mobile

Additional enhancement to existing IEEE802.11 functions:

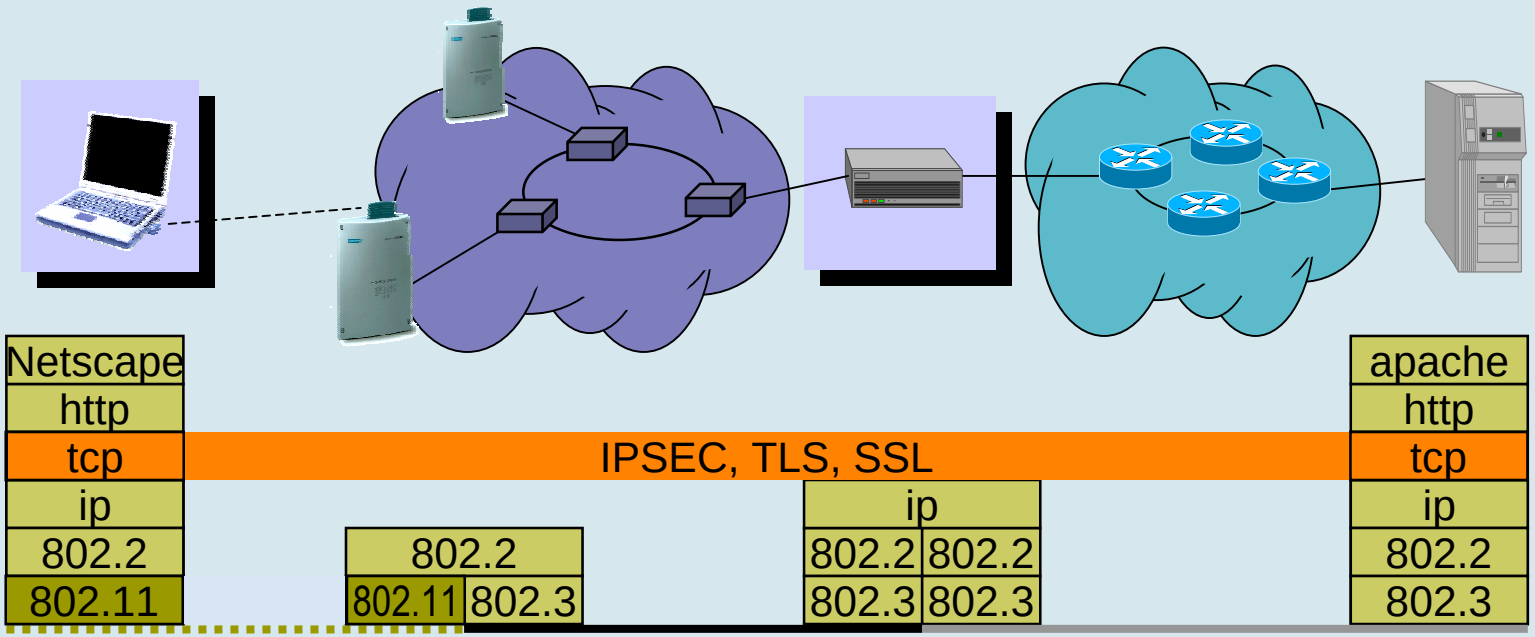
- **Data privacy mechanism:**
  - TKIP (Temporal Key Integrity Protocol) to enhance RC4-based hardware for higher security requirements, or
  - WRAP (Wireless Robust Authenticated Protocol) based on AES (Advanced Encryption Standard) and OCB (Offset Codebook)
- **Security association management:**
  - RSN negotiation procedures for establishing the security context
  - IEEE802.1X authentication and key management



A last word about WLAN security:

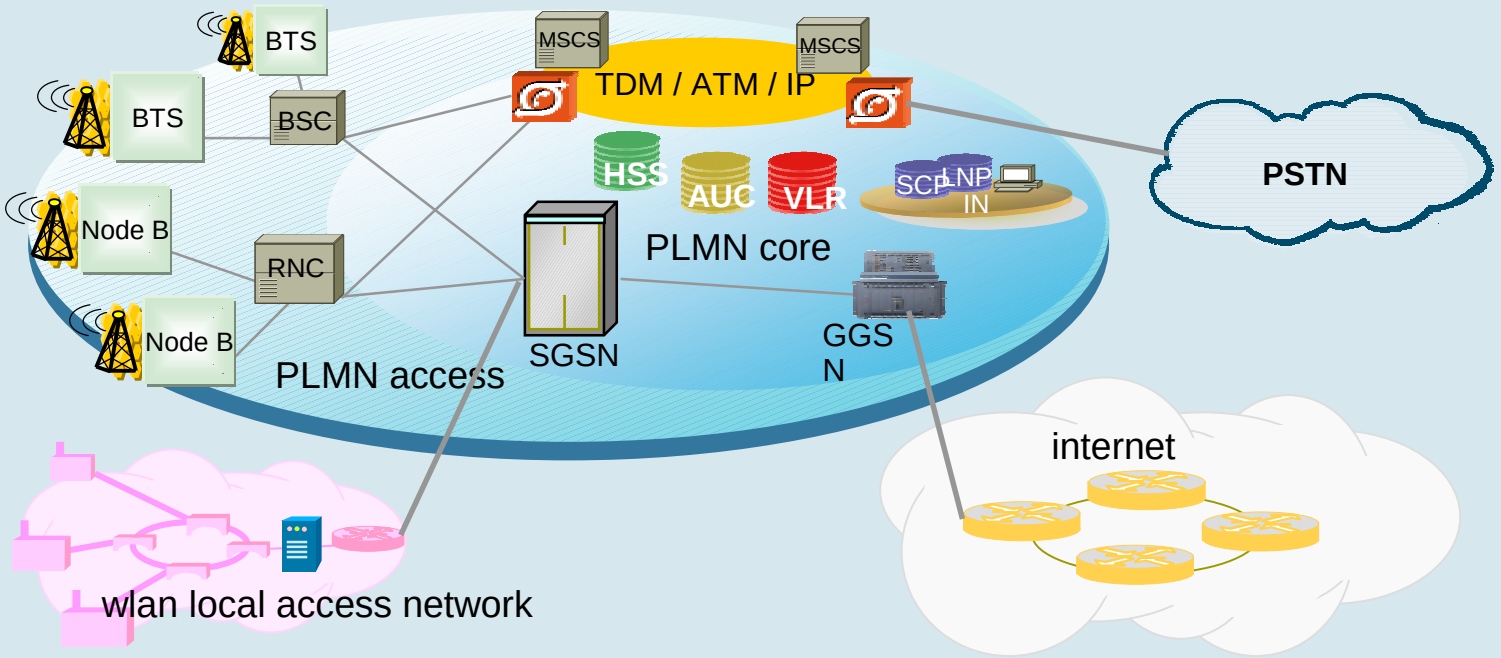
SIEMENS mobile

- **Even IEEE802.11i may not be sufficient for public hot-spots:**



- **Only VPN technologies (IPSEC, TLS, SSL) will fulfil end-to-end security requirements in public environments.**
- **VPN technologies might even be used in corporate WLAN networks.**

WLAN – UMTS Interworking: Ancient approach: ‘tight coupling’



WLAN as just another radio access technology of UMTS

- **All UMTS services become available over WLAN.**
  but:
- **PLMN is burdened with high bandwidth WLAN traffic.**
- **Wi-Fi does not provide all the functionality needed (QoS, security).**

UMTS and Wireless LAN are different.

SIEMENS mobile

GSM/GPRS/UMTS

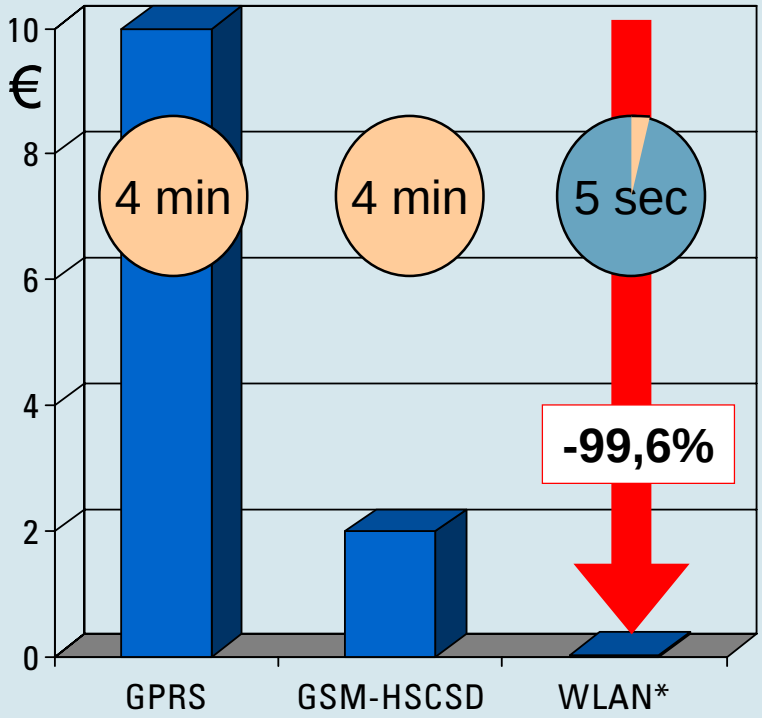
- anytime / everywhere
- voice, realtime messaging
- QoS
- precious bandwidth
- carrier grade
- operator driven
- huge customer base
- high revenues

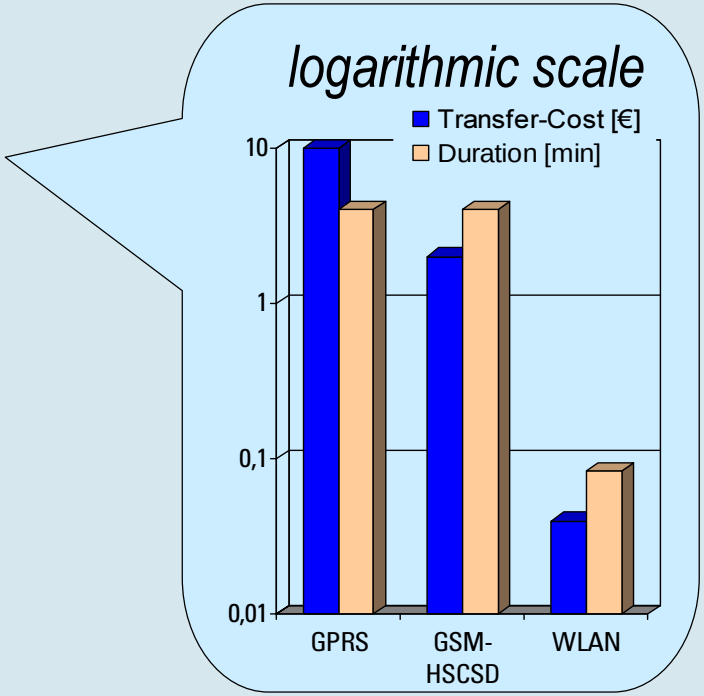
WLAN IEEE802.11

- sometimes / somewhere
- standard web applications
- best effort
- cheap bandwidth
- corporate technology
- market driven
- casual users
- low revenues

WLAN is much cheaper than 2G/3G

Transfer cost/duration of an 1 Mbytes .ppt/.doc/.xls File...





* **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

Becoming a WLAN operator is easy.

SIEMENS mobile

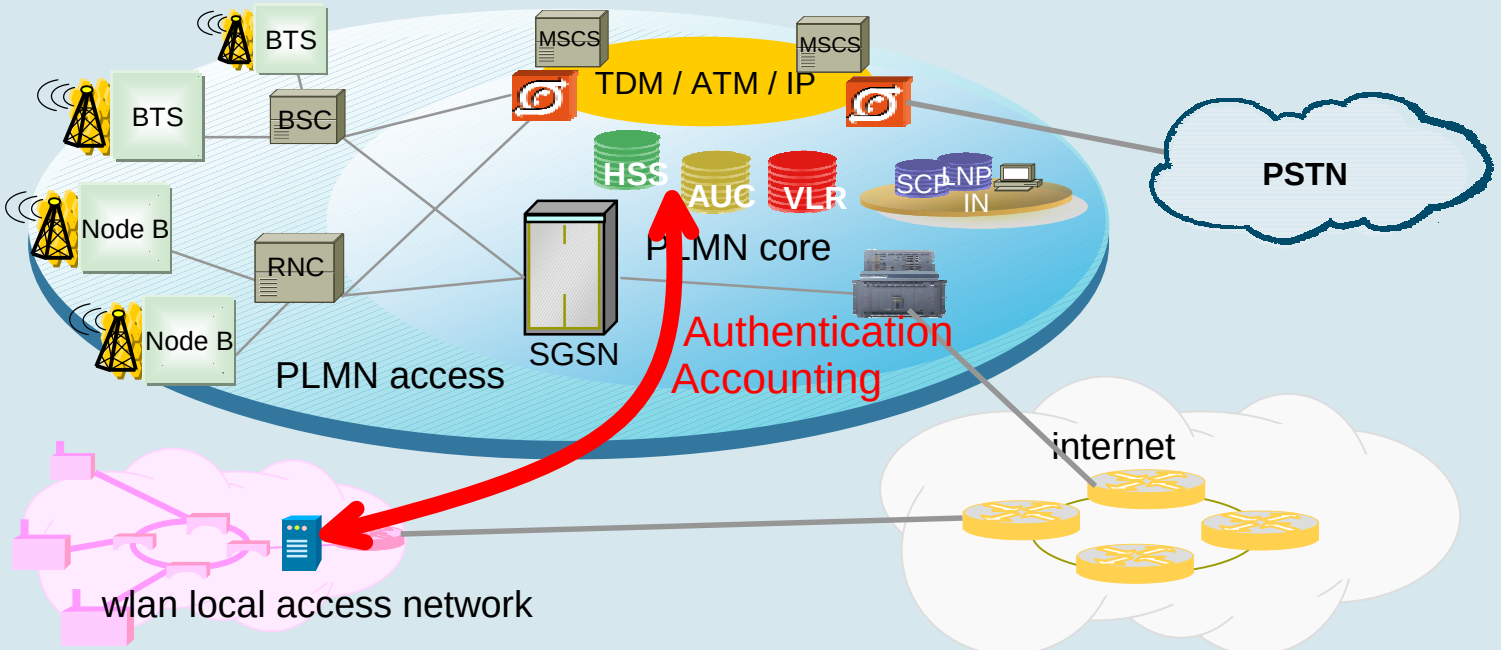
- **Legal aspects:**
  - Usage of license free spectrum (2,4 GHz ISM band)
  - No telecommunication license necessary, as long as
    - not providing telephony services,
    - not providing network access across borders of private premises.
- **Cost issues:**
  - The lower bound:
    Investment: WLAN Access Point /w DSL Router (~ 350 €)
    Monthly operation cost: ~ 60 € for DSL Flat Rate
  - Most commercial installations are much more expensive due to charging and billing.
- **It is very easy and extremely cheap to become a WLAN operator, but most people did not yet know about it.**

...but wait until they have installed WLAN in their living rooms!

WLAN – UMTS Interworking: Now widely accepted: ‘loose coupling’

SIEMENS mobile

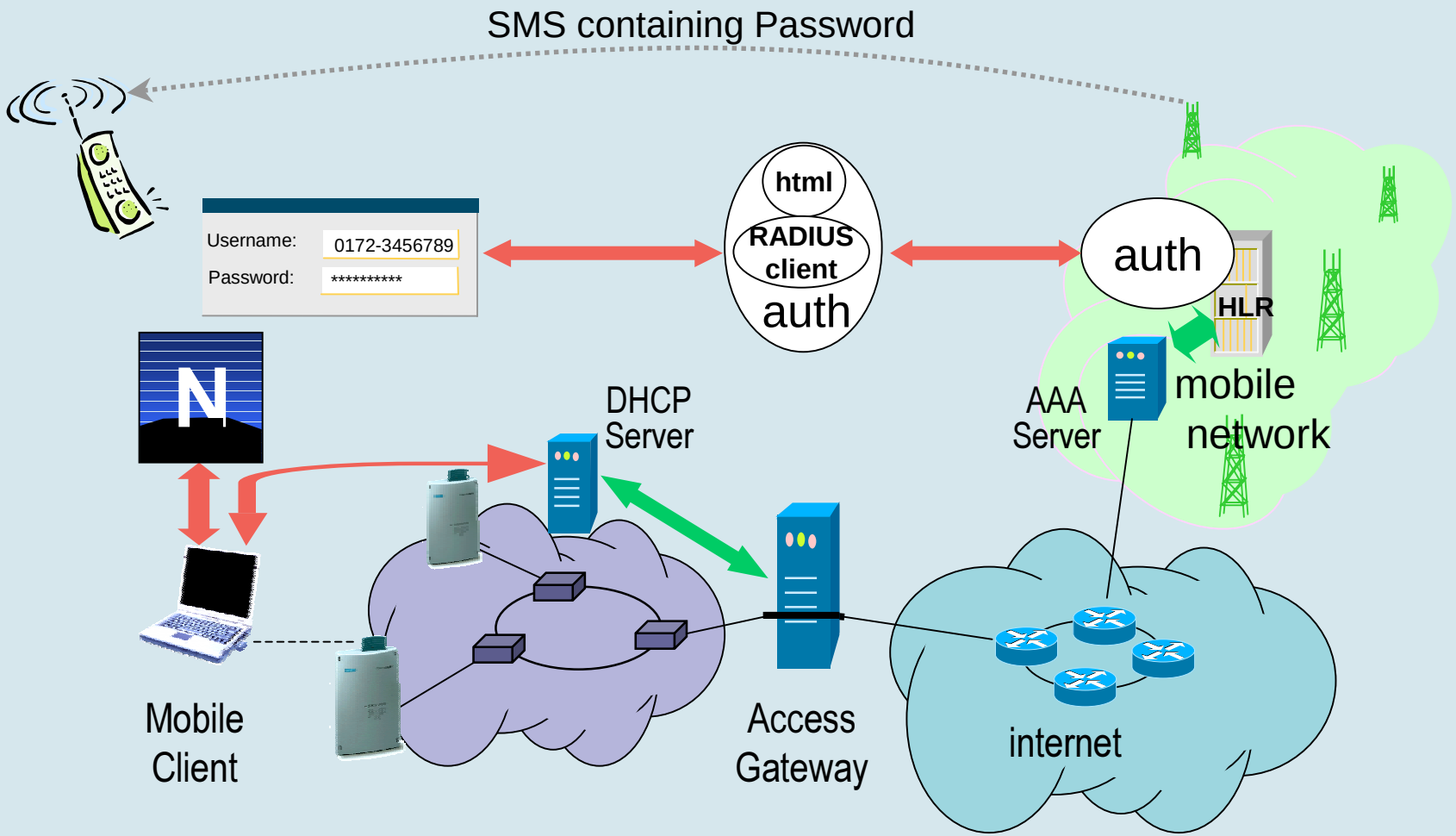
Siemens contributed ‚loose coupling‘ to standardization.



Only Authentication, Authorization and Accounting of WLAN access is performed by the mobile network operator.

- **Revenues without competing against aggressive WLAN operators.**
- **Perfect model for leveraging the huge customer base and establishing a widely accepted platform for mobile commerce.**

E.g.: Web based authentication and mobile network security



Standards for WLAN/UMTS interworking

SIEMENS mobile

- **3GPP**
  - R5: SA1
    Requirements of 3GPP system – WLAN interworking.
  - R6: SA2
    Continuation with architectural considerations
- **ETSI BRAN**
  Subgroup on "Interworking between HiperLAN/2 and 3rd generation cellular and other public systems".
  - Detailed architectural description mainly based on the Siemens 'loose coupling' principle established
  - IEEE802.11 and MMAC are now joining this effort.
    => Wireless Interworking Group (WIG).
- **WECA (Wireless Ethernet Compatibility Alliance)**
  'Wireless ISP Roaming Initiative'
  - Detailed functional specification for roaming (loose coupling) between IEEE802.11 WLAN networks available.
  - Mainly aimed for roaming between ISPs but also well applicable for MNOs.

The end

SIEMENS mobile

- Thank you for your attention.
- Questions and comments?
- Maximilian Riegel

  maximilian.riegel@icn.siemens.de

  http://www.max.franken.de/

