Standards Konzepte für drahtlose Kommunikationsnetze

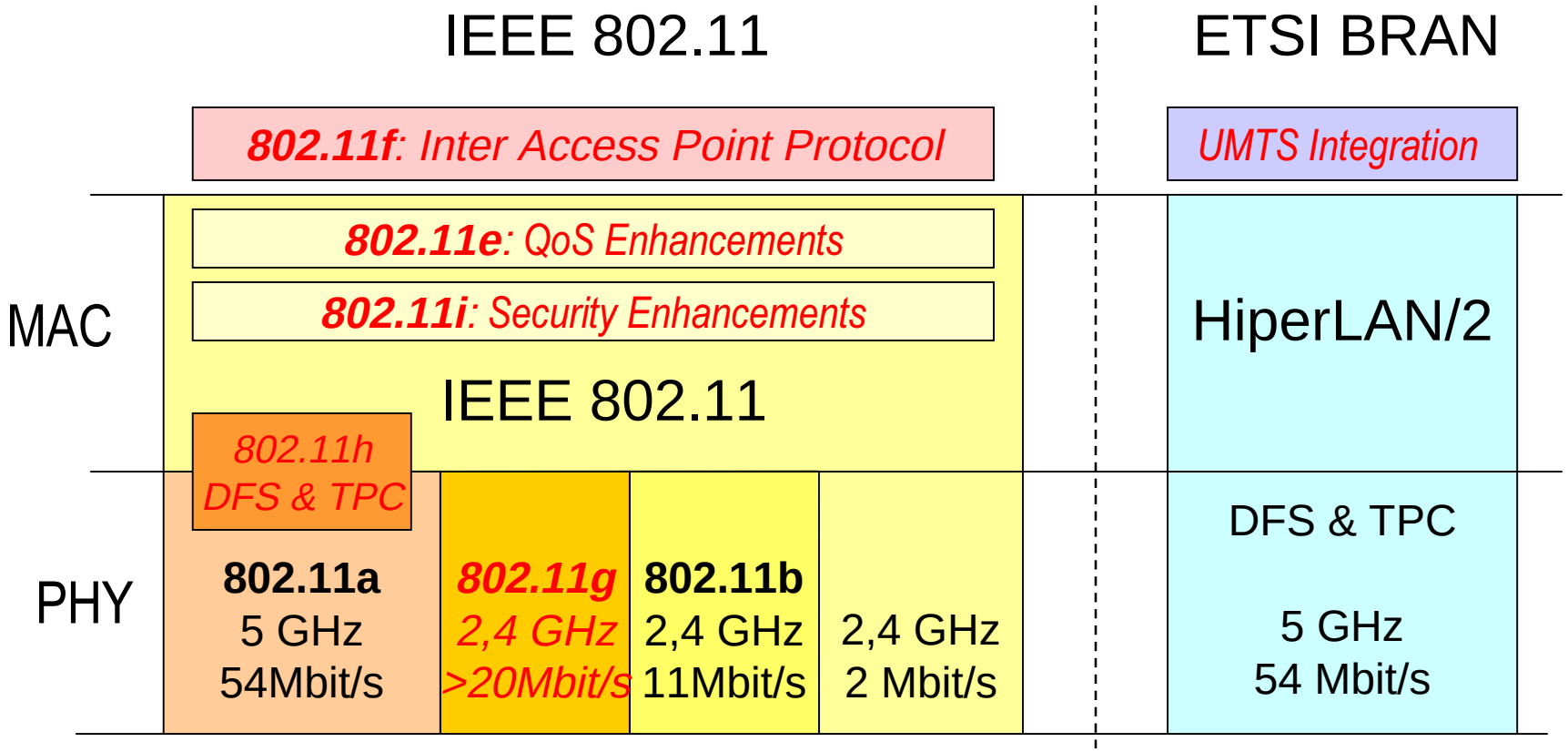
Schnittstellen und Protokolle für Wireless LANs

Maximilian Riegel
<maximilian.riegel@icn.siemens.de>

Outline

- Standardization overview
- The IEEE802.11 architecture
- IEEE802.11 functions and enhancements
  - Physical layer
  - MAC layer functions
  - Configurations
  - Roaming
  - Power Management
  - Privacy and access control
- 5 GHz Harmonization
- Interworking between WLAN and mobile networks

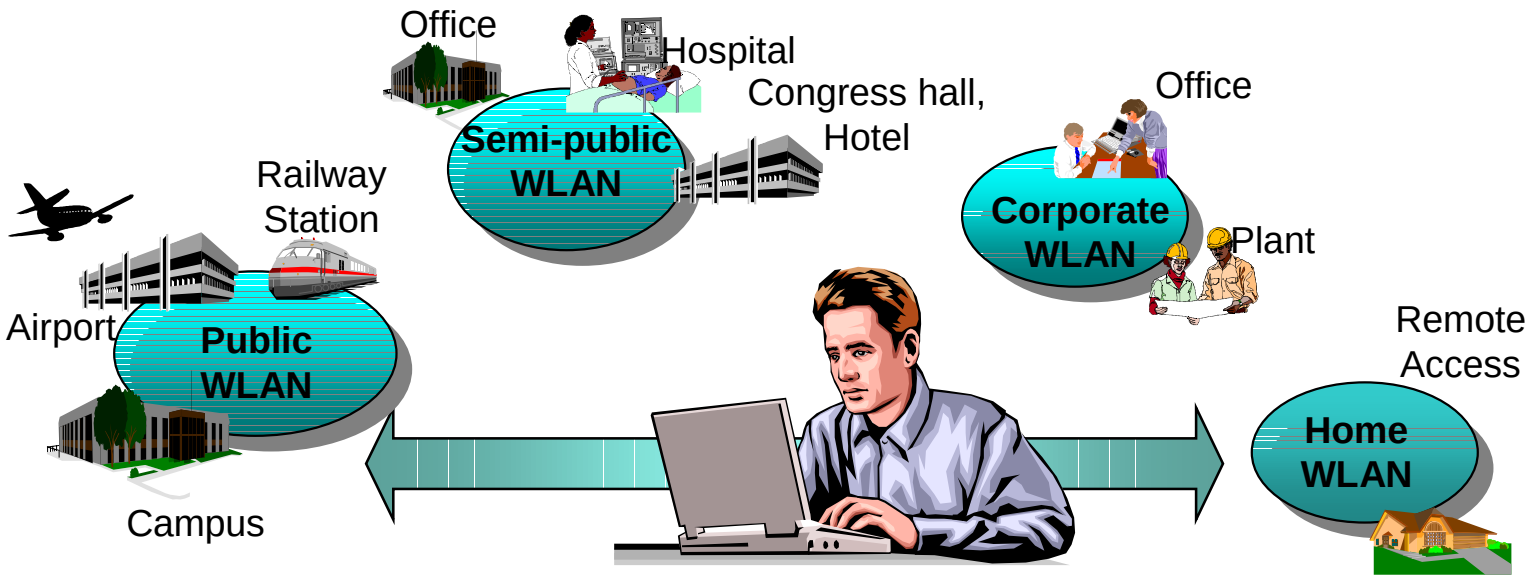
Wireless LAN Standardization



Current standardization topics

WLAN has taken of…

- WLAN is more than just cable replacement!
- It provides hastlefree broadband Internet access everywhere.



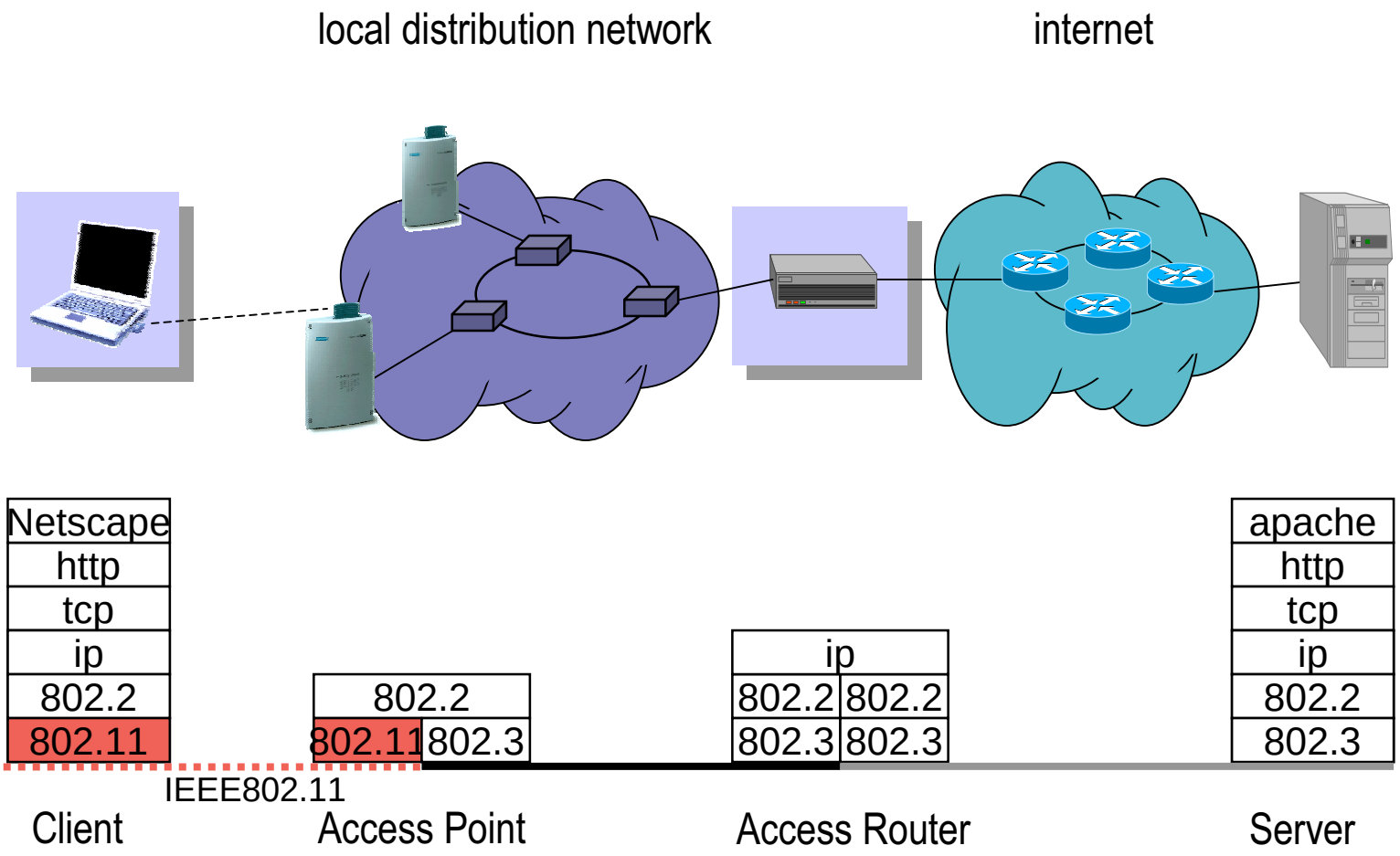
- Today's road worriers require access to the Internet everywhere.
- Only coverage in 'hot-spots' needed.
- IEEE802.11b meets the expectations for easyness, cost and bandwidth.

Wireless IEEE802.11 Standard

Approved June 1997
802.11b approved Sept. 1999

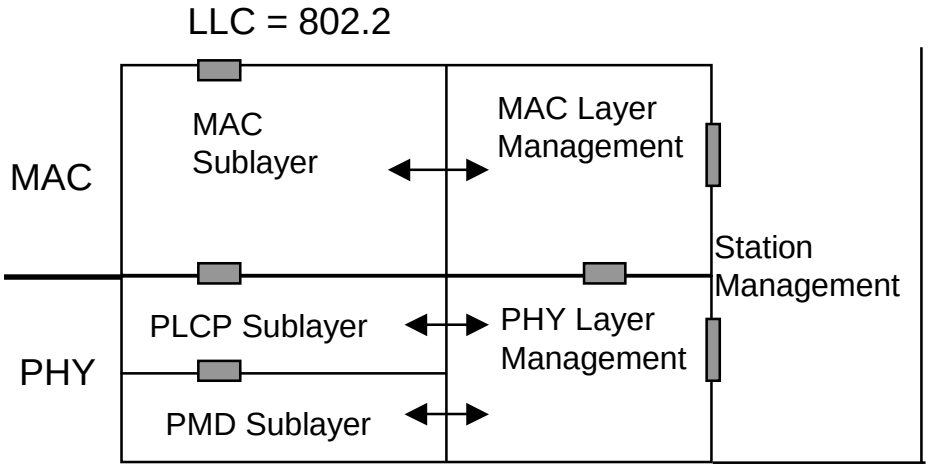
- Operation in the 2.4GHz ISM band
  - USA: FCC part 15.247-15.249
  - Europe: ETS 300-328
  - Japan: RCR-STD-33A
- Supports three PHY layer types: DSSS, FHSS, Infrared
- MAC layer common to all 3 PHY layers
- Supports peer-to-peer and infrastructure configurations
- **IEEE802.11b** high data rate extension 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



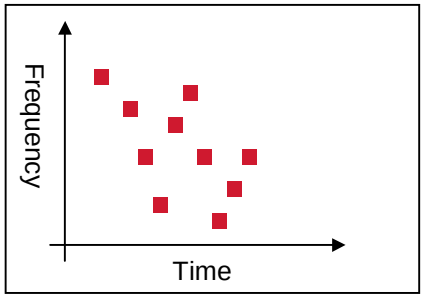
IEEE802.11 Protocol Architecture

- MAC Entity
  - basic access mechanism
  - fragmentation
  - encryption
- MAC Layer Management Entity
  - synchronization
  - power management
  - roaming
  - MAC 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
- PHY Layer Management
  - channel tuning
  - PHY MIB
- Station Management
  - interacts with both MAC Management and PHY Management

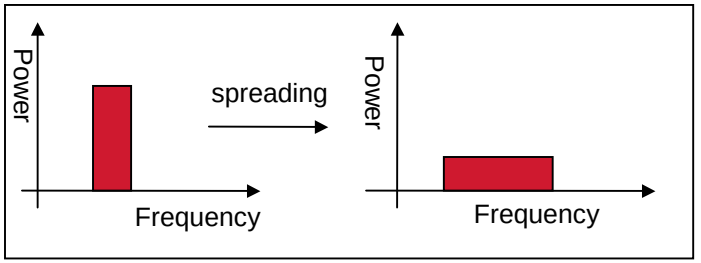


IEEE 802.11 – 2.4 & 5 GHz Physical Layers

- 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)

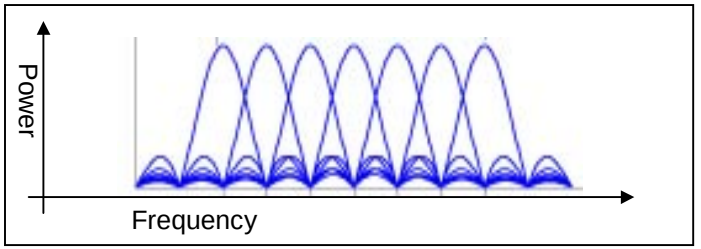


- 2.4 GHz *Direct Sequence Spread Spectrum*
  - DBPSK/DQPSK with 1/2 Mbps
  - Spreading with 11 Bit barker Code
  - 11/13 channels in the 2.4 GHz band



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

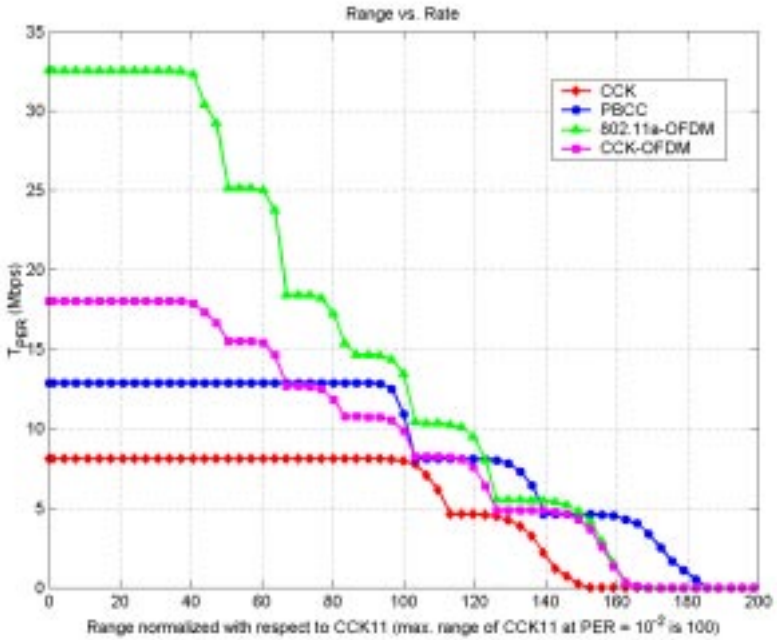
- 5 GHz *OFDM* PHY (802.11a)
  - Basic parameters identical to HiperLAN2 PHY
  - European regulatory issues unsolved



Upcoming

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

- *Mandatory:* CCK (802.11b) w/ short preample 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

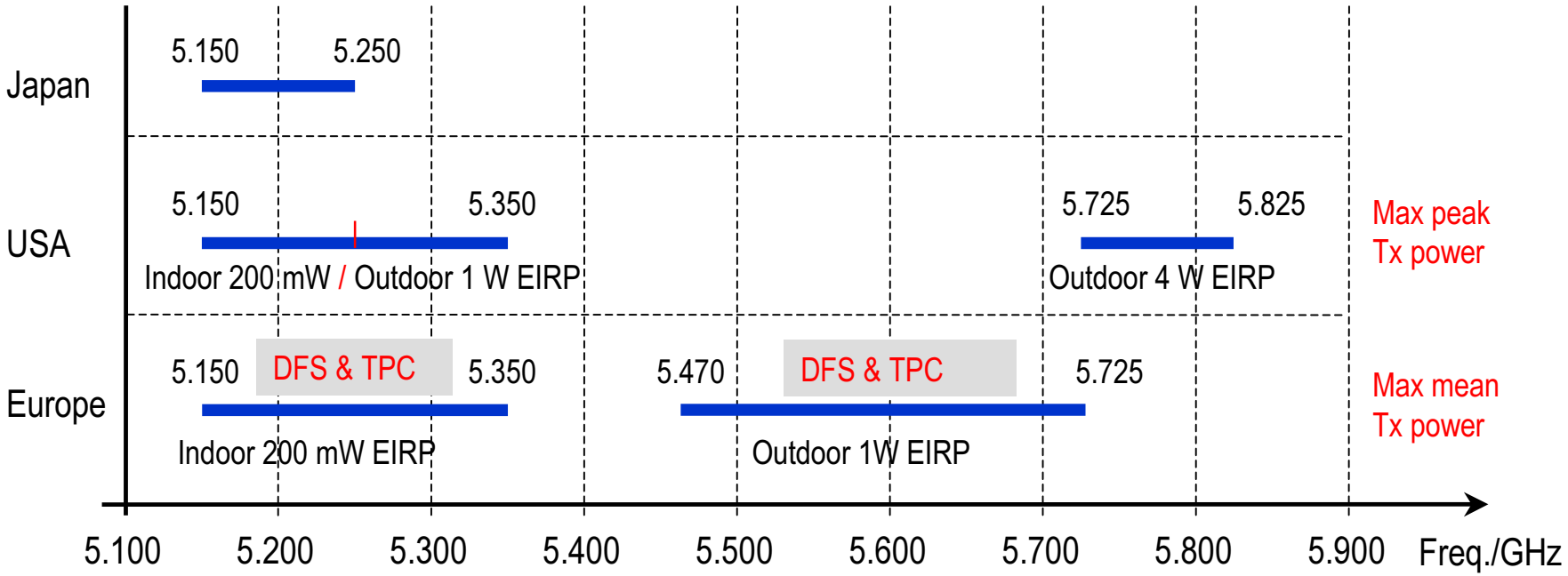


Range vs. throughput rate comparison of

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

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

Spectrum Designation in the 5 GHz range



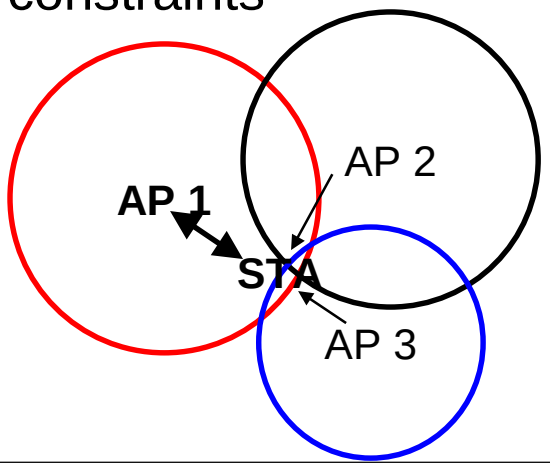
DFS: Dynamic Frequency Selection

TPC: Transmit Power Control

Upcoming

IEEE802.11h
Spectrum and Transmit Power Management

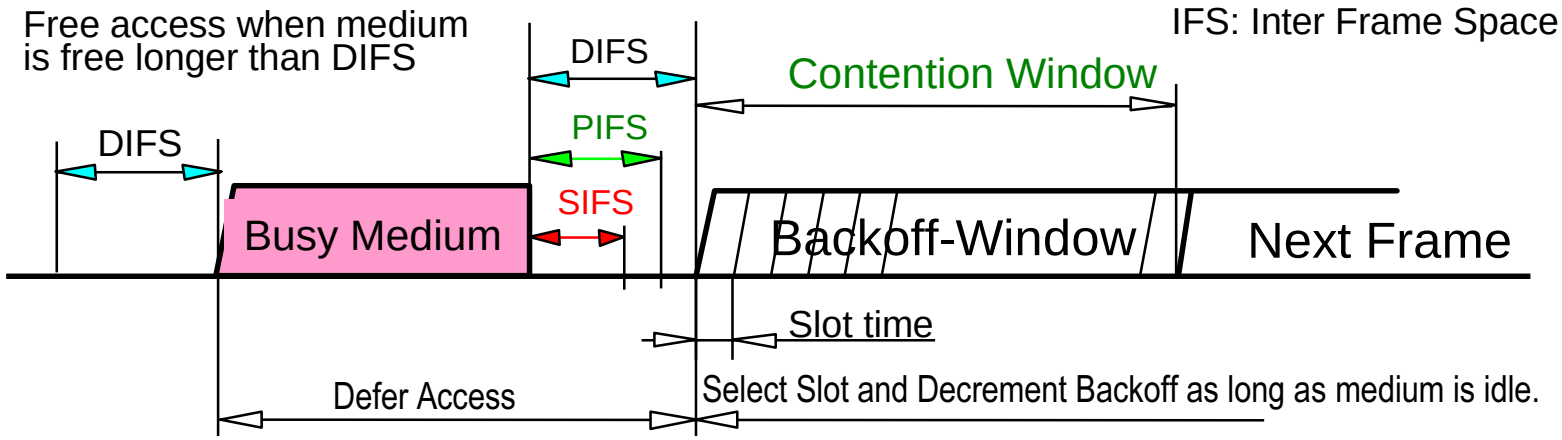
- TPC (Transmission power control)
  - supports interference minimisation, power consumption reduction, range control and link robustness.
  - TPC procedures include:
    - AP‘s define and communicate regulatory and local transmit power constraints
    - Stations select transmit powers for each frame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



When will 5 GHz WLANs come...

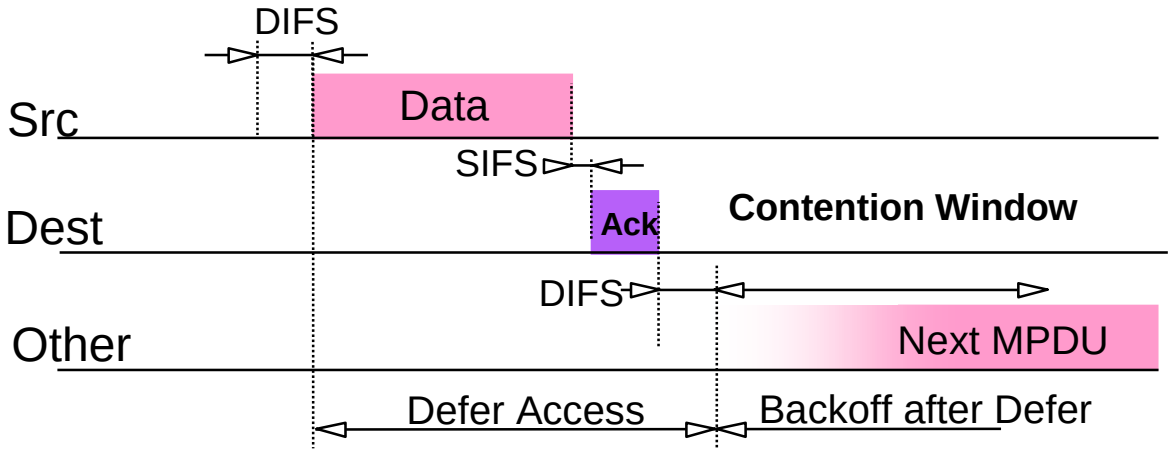
- IEEE802.11b (2.4 GHz) is now taking over the market.
- There are developments to enhance IEEE802.11b for
  - more bandwidth (up to 54 Mbit/s)
  - QoS (despite many applications do not need QoS at all)
  - network issues (access control and handover).
- 5 GHz systems will be used when the 2.4 GHz ISM band will become too overcrowded to provide sufficient service.
  - TCP/IP based applications are usually very resilient against ‘error proune’ networks.
- Issues of 5 GHz systems:
  - Cost: 5 GHz is more expensive than 2.4 GHz
  - Power: 7dB more transmission power for same distance
  - Compatibility to IEEE802.11b/g necessary

CSMA/CA Explained



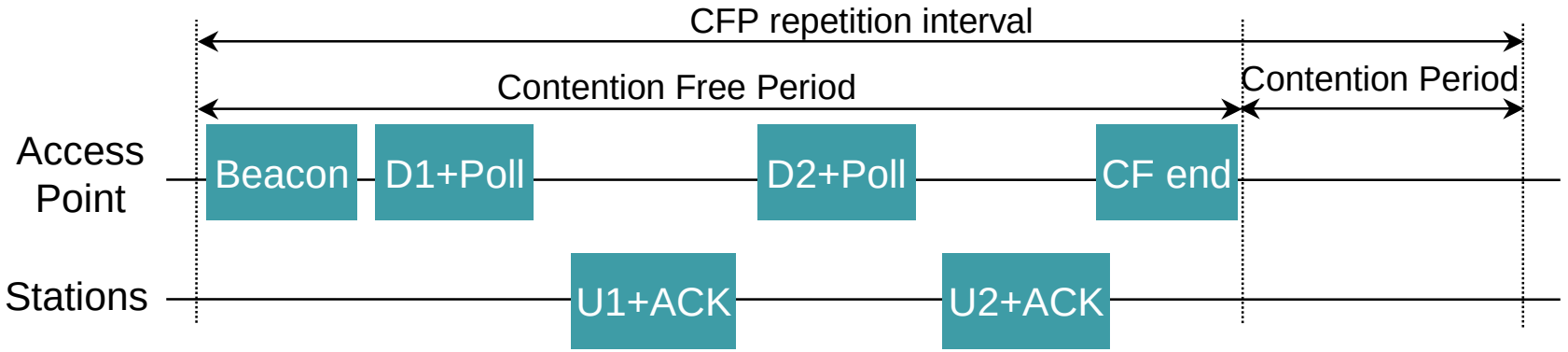
- Reduce collision probability where mostly needed.
  - Stations are waiting for medium to become free.
  - Select Random Backoff after a Defer, resolving contention to avoid collisions.
- Efficient Backoff algorithm stable at high loads.
  - Exponential Backoff window increases for retransmissions.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

CSMA/CA + ACK protocol



- Defer access based on Carrier Sense.
  - Information from PHY and Virtual Carrier Sense state.
- Direct access when medium is sensed free longer then DIFS, otherwise defer and backoff.
- Receiver of directed frames to return an ACK immediately when CRC correct.
  - When no ACK received then retransmit frame after a random backoff (up to maximum limit).

IEEE802.11 Point Coordination Function (PCF)



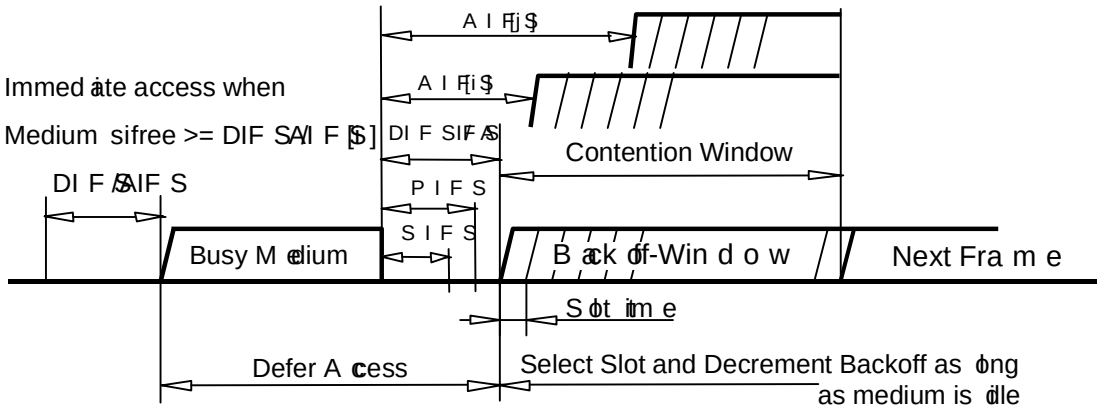
- Optional PCF mode provides alternating contention free and contention operation under the control of the access point
- The access point polls stations for data during contention free period
- Network Allocation Vector (NAV) defers the contention traffic until reset by the last PCF transfer
- PCF and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

Upcoming

IEEE802.11e

Medium Access Control Enhancements for Quality of Service

- EDCF (Enhanced Distributed Coordination Function)
  - differentiated DCF access to the wireless medium for prioritized traffic categories (8 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



Upcoming

IEEE802.11e

Medium Access Control Enhancements for Quality of Service

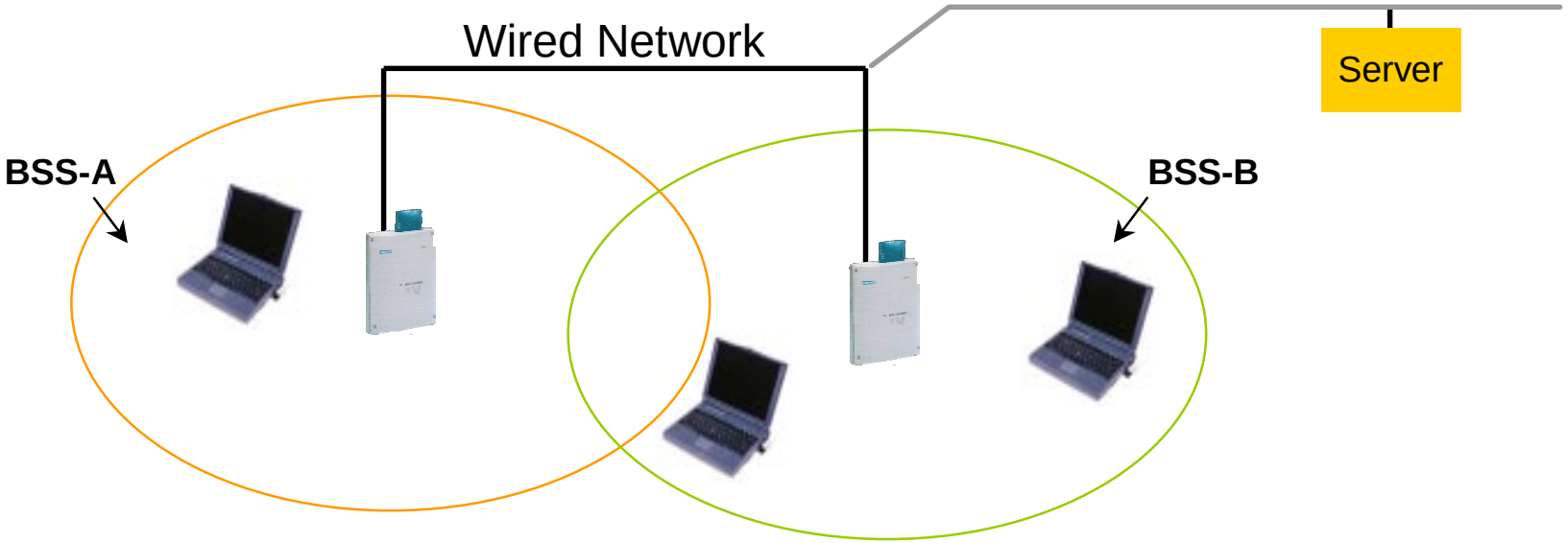
- HCF (Hybrid coordination function)
  - only usable in infrastructure QoS network configurations
  - allow a uniform set of frame exchange sequences to be used during both the contention period (CP) and contention free period (CFP)
  - uses a QoS-aware point coordinator, called a hybrid coordinator
    - by default collocated with the enhanced access point (EAP)
    - uses the point coordinator's higher priority to allocate transmission opportunities (TxOPs) to stations
  - provides limited-duration contention free bursts (CFBs) to transfer QoS data.
  - meets predefined service rate, delay and/or jitter requirements of particular traffic flows.
  - ...
  - „Quite complex method still under definition“

IEEE802.11 Ad Hoc Mode

Peer-to-Peer Network

- 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



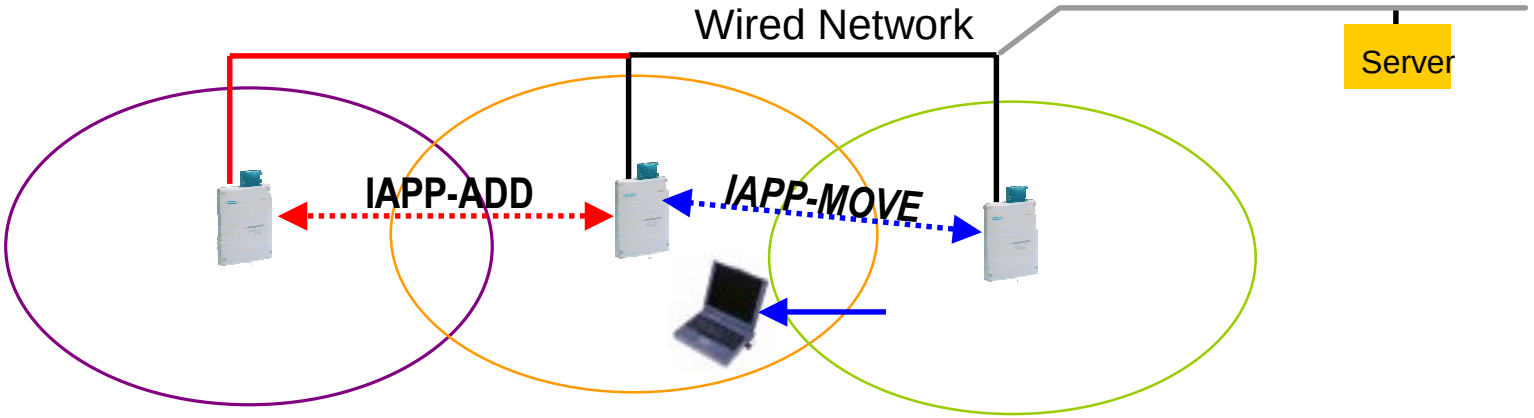
- Access Points (AP) and stations (STA)
- BSS (Basic Service Set): a set of stations controlled by a single coordination function
- Distribution system interconnects multiple cells via access points to form a single network
- Extends wireless coverage area and enables roaming

Upcoming

IEEE802.11f

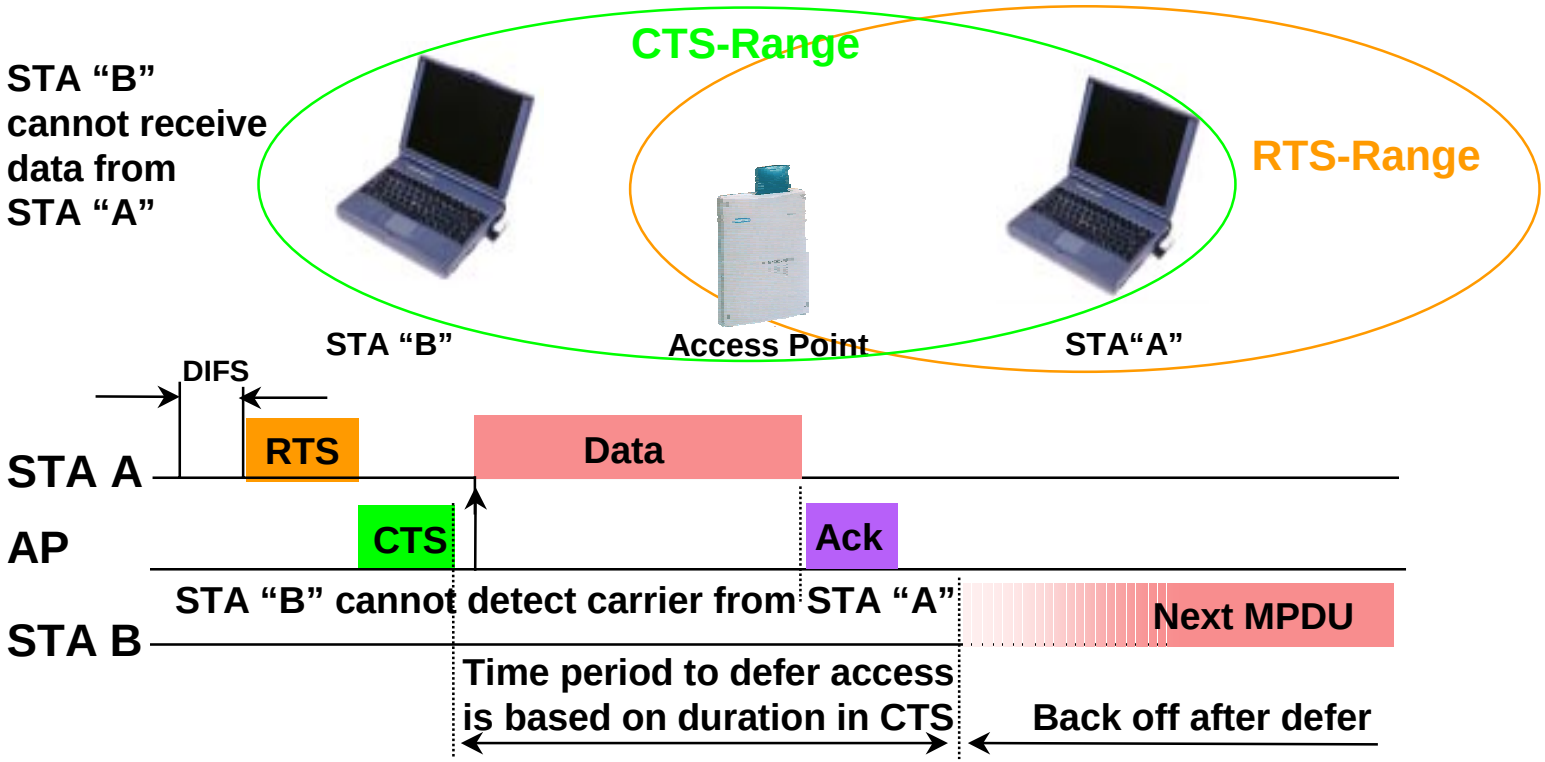
Inter-Access Point Protocol (IAPP) across Distribution Systems

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



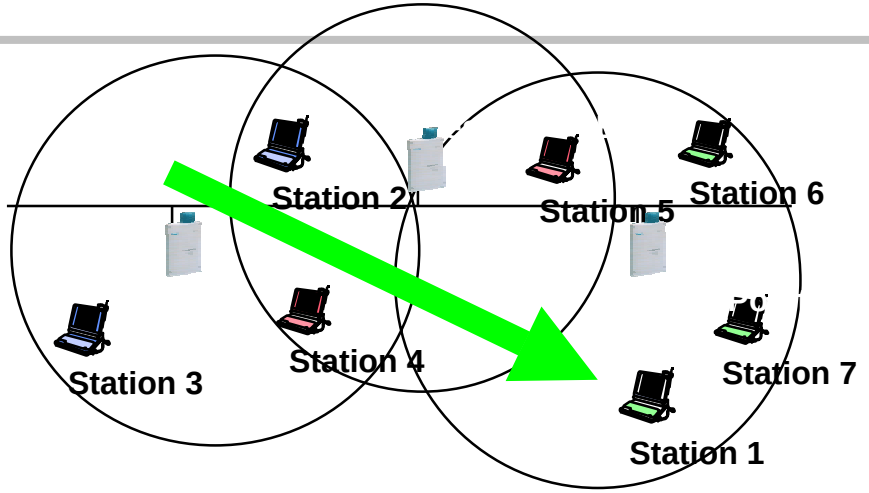
“Hidden Node” Provisions

Problem – Stations contending for the medium do not *Hear* each other
Solution – Optional use of the *Duration* field in RTS and CTS frames with AP



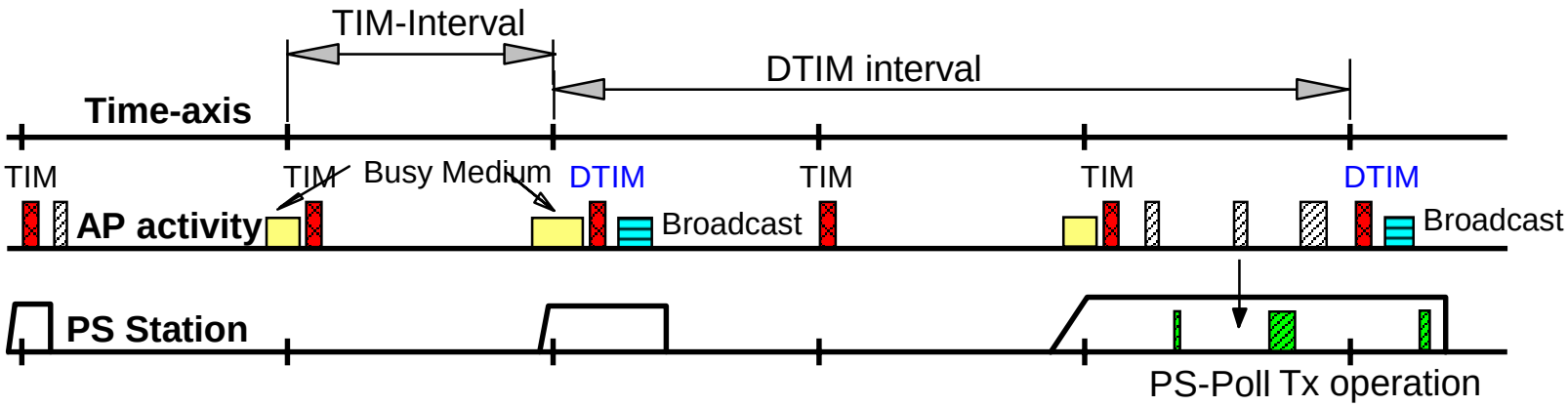
Roaming Approach

- 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

Power Management



- Stations wake up prior to an expected DTIM.
- If TIM indicates frame buffered
  - station sends PS-Poll and stays awake to receive data
  - else station sleeps again
- Broadcast frames are also buffered in AP.
  - all broadcasts/multicasts are buffered
  - broadcasts/multicasts are only sent after Delivery Traffic Indication Message (DTIM)
  - DTIM interval is a multiple of TIM interval

IEEE802.11 privacy and access control

- Goal of 802.11 is 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

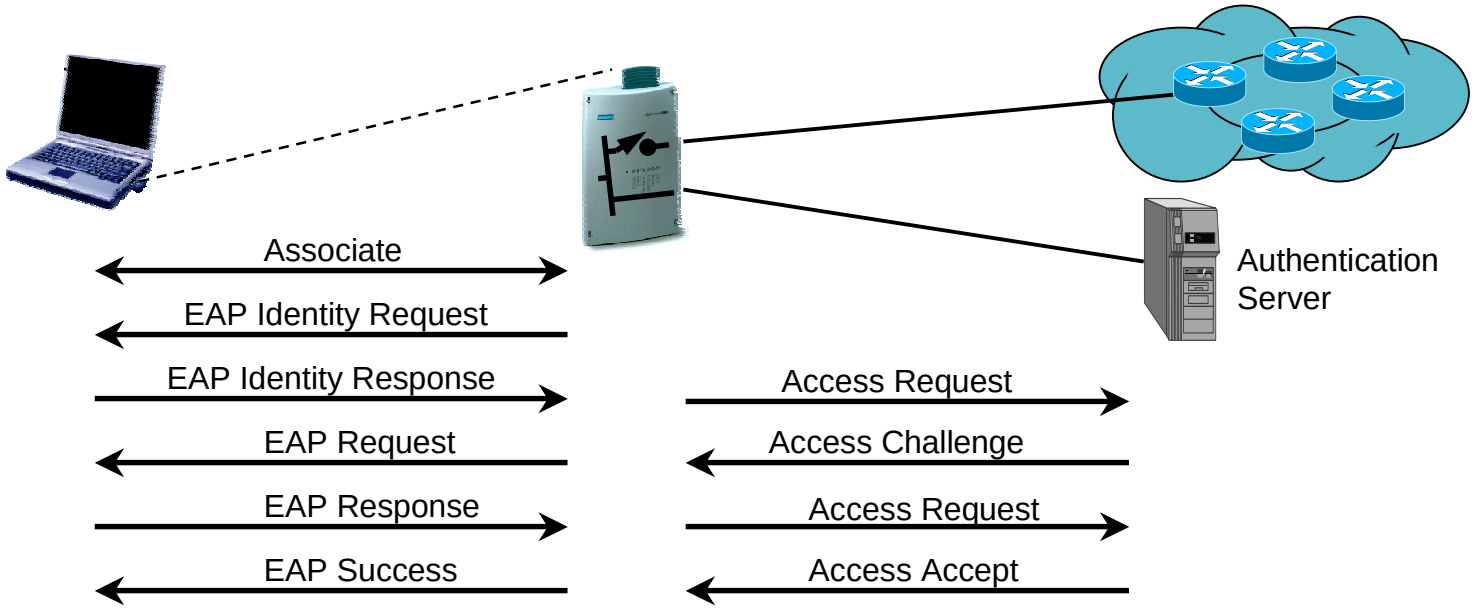
- WEP unsecure at any key length
  - IV space too small, lack of IV replay protection
  - known plaintext attacks
- No user authentication
  - Only NICs are authenticated
- No mutual authentication
  - Only station is authenticated against access point
- Missing key management protocol
  - No standardized 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 cases.

IEEE802.11i
Enhanced security

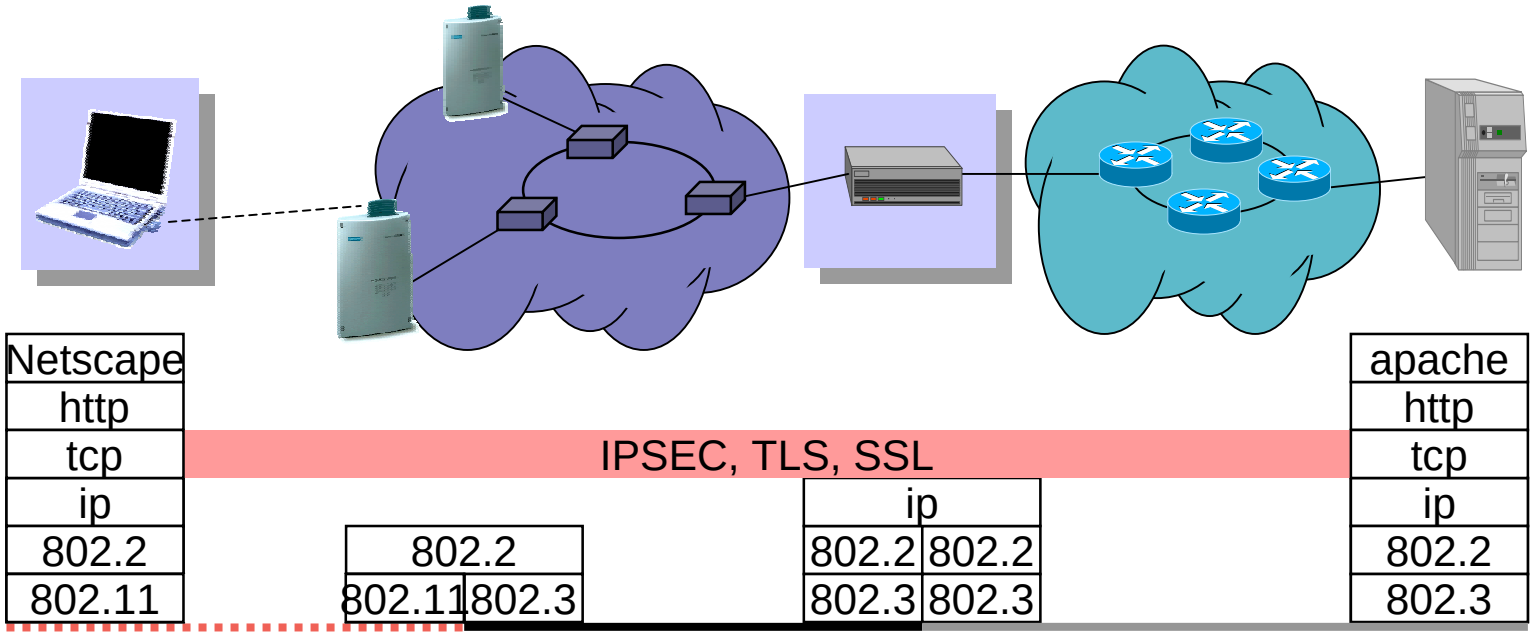
Upcoming

- Enhanced encryption
  - WEP2 w/ increase IV space to 128bit, key length 128bit
  - optional: Advanced Encryption Standard (AES)
- Authentication and key management by adoption of IEEE802.1X Standard for Port Based Network Access Control



A last word about WLAN security:

- WEP/WEP2 is probably not sufficient in public hot-spots:

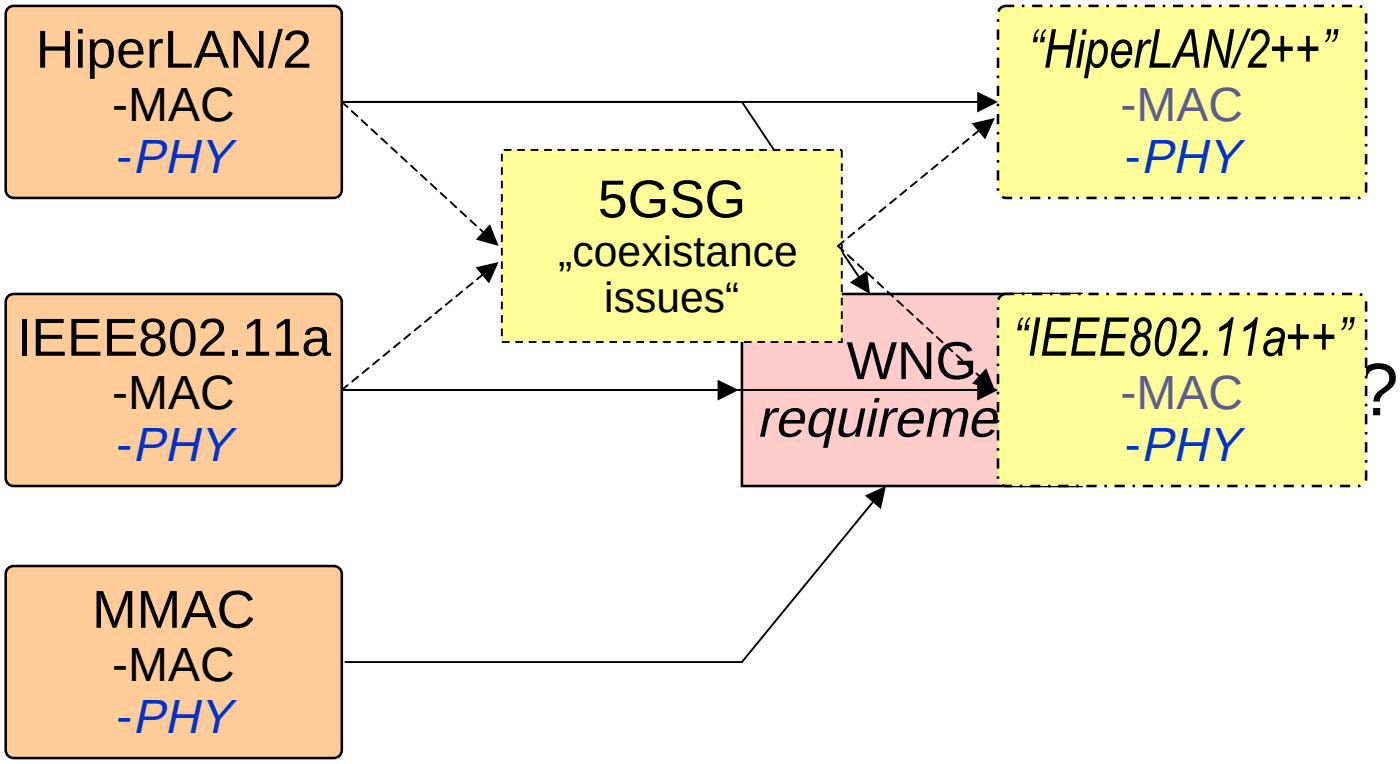


- Only VPN technologies (IPSEC, TLS, SSL) will fulfil end-to-end security requirements.
- VPN technologies might even be used in corporate networks.

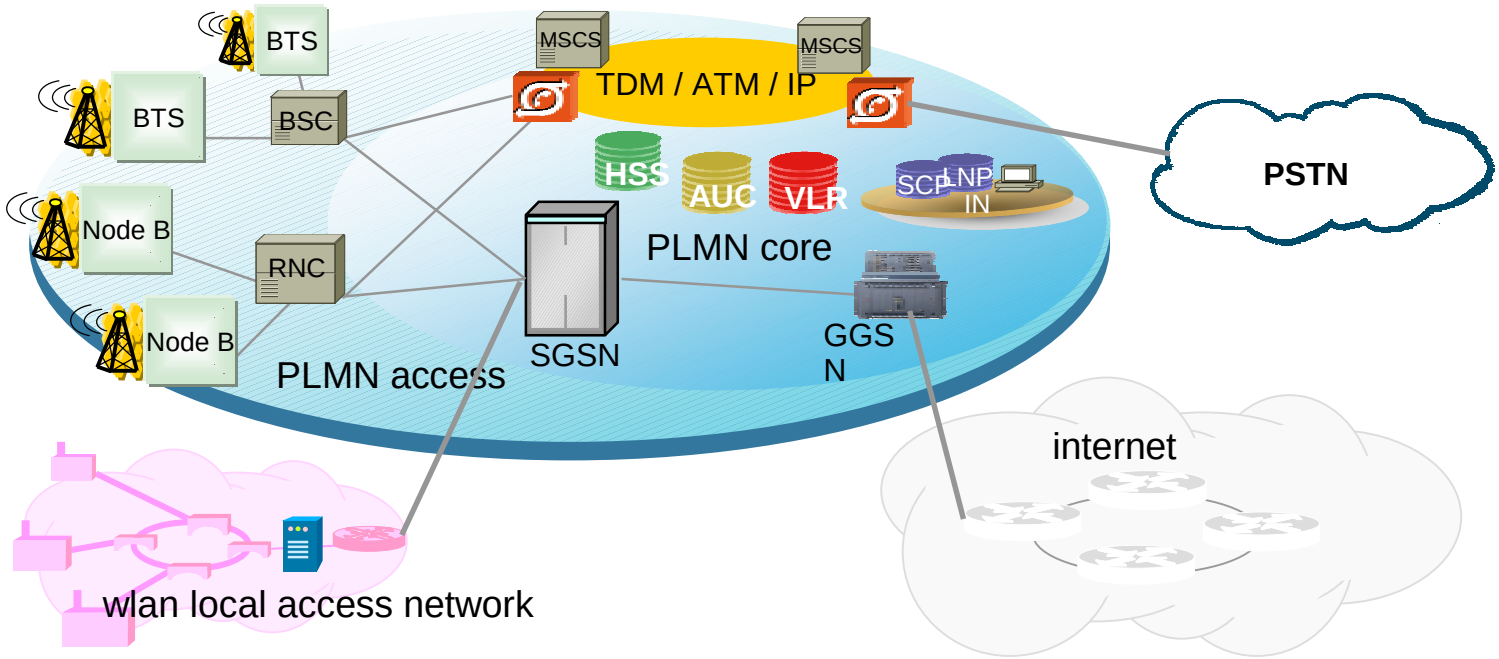
Summary: IEEE802.11 Architecture

- One MAC supporting multiple PHYs
  - currently Frequency Hopping, Direct Sequence, OFDM and Infrared PHYs
- Two configurations
  - “Independent” (ad hoc) and “Infrastructure”
- CSMA/CA (collision avoidance) with optional “point coordination”
- Connectionless Service
  - Transfer data on a shared medium without reservation
  - data comes in bursts
  - user waits for response, so transmit at highest speed possible
  - is the same service as used by Internet
- Isochronous Service
  - reserve the medium for a single connection and provide a continues stream of bits, even when not used
  - works only when cells (using the same frequencies) are not overlapping.
- Robust against noise and interference (ACK)
- Hidden Node Problem (RTS/CTS)
- Mobility (Hand-over mechanism)
- Power savings (Sleep intervals)
- Security (WEP)

Harmonization of 5 GHz WLAN Standards



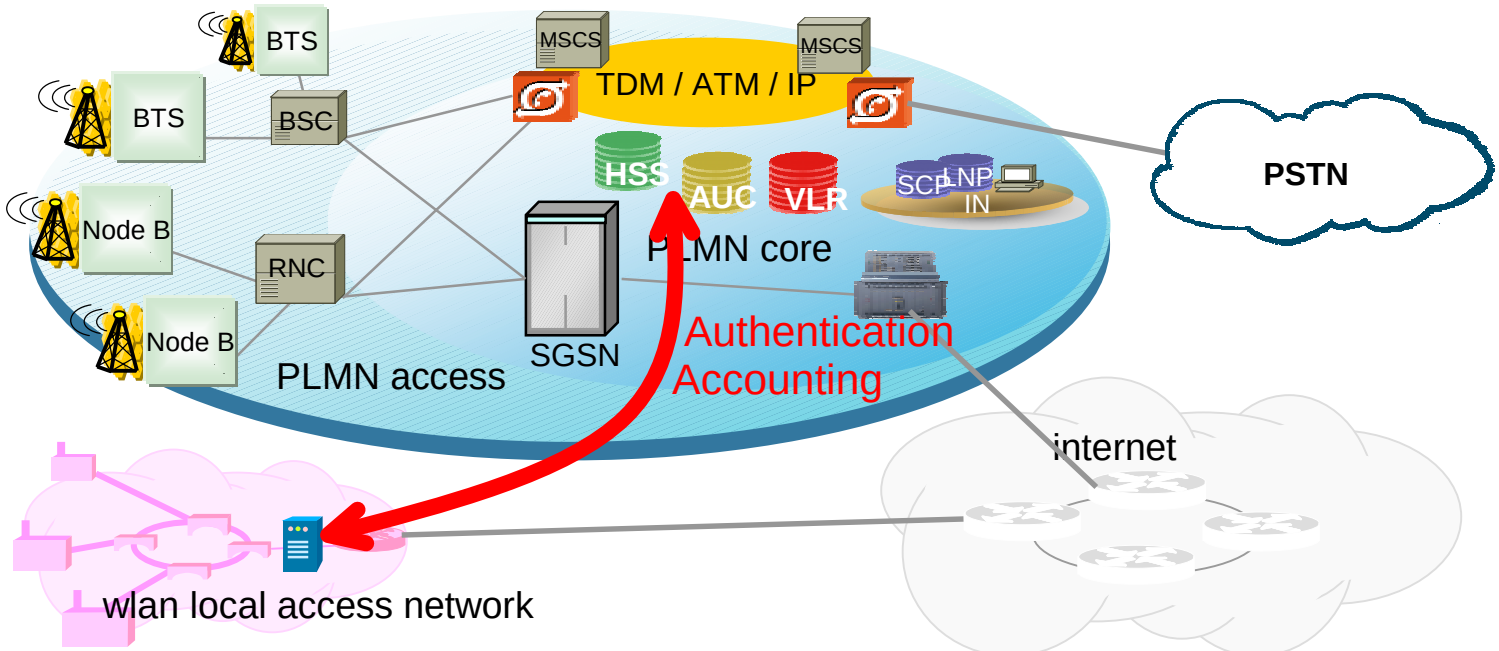
Interworking between WLAN and mobile networks:
Many vendors and operators were in favor of ‘tight coupling’



WLAN as just another radio access technology

- Wi-Fi does not provide all the functionality needed (QoS, security).
- Legacy terminals (today’s WLAN enabled notebooks) can’t be served.
- PLMN is burdened with high bandwidth WLAN traffic.

Interworking between WLAN and mobile networks: Siemens contributed the ‘loose coupling’ concept



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

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

The end

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

- Maximilian Riegel <maximilian.riegel@icn.siemens.de>
- http://www.max.franken.de