SIEMENS

mobile

Wireless LAN IEEE802.11 Tutorial

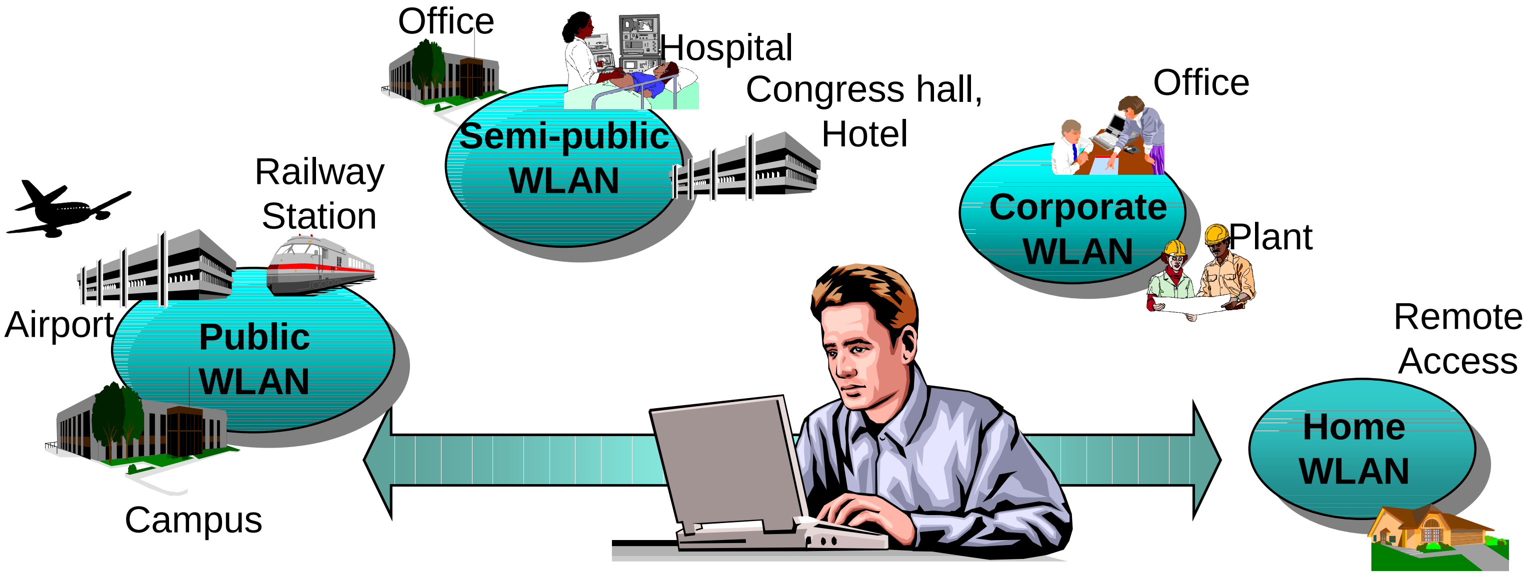
Maximilian Riegel

ICM Networks, Advanced Standardization

Prolog:
The ubiquitous WLAN

SIEMENS mobile

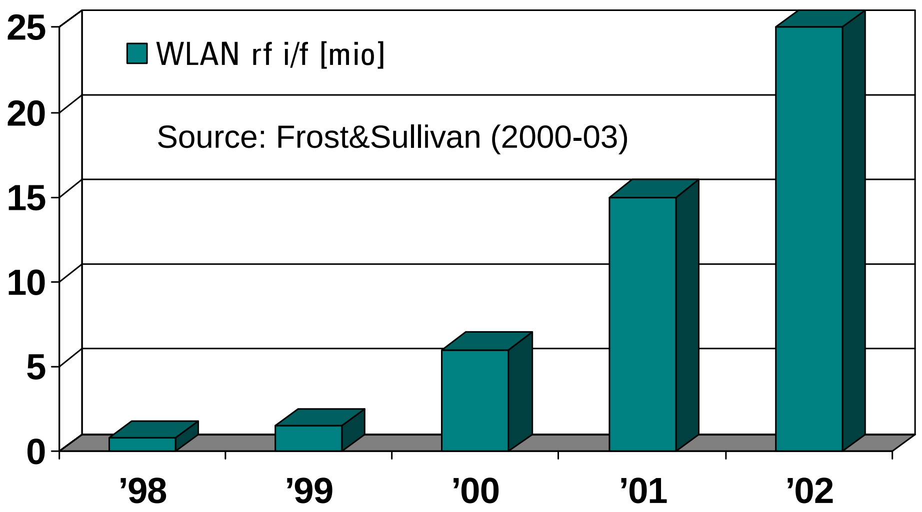
- Today's road worriers require access to the Internet everywhere.
- WLAN is more than just cable replacement, it provides hassle-free broadband Internet access everywhere.



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

Prolog:
WLAN has taken off ...

- **Lots of serious WLAN activities have been started**
  – All big players have products (Cisco, Intel, …)
  – Integrated WLAN solutions appearing (Apple, IBM, ...)
- **The prediction have been exceeded by actual market.**
  For comparison:
  Total PC world market in '01: ~ 120 Mio pcs.; > 30 % portable.



- **Ruling technology is IEEE802.11b (Wi-Fi) [11Mb/s, 2.4 GHz].**

Outline

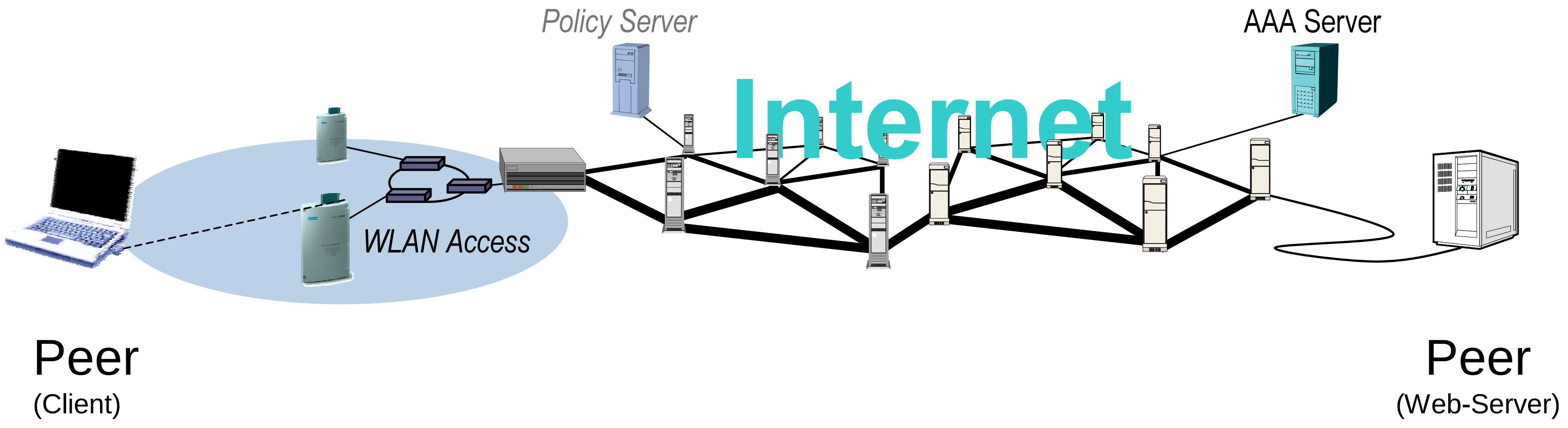
- Part 1: Wireless Internet System Architecture
- Part 2: IEEE802.11 Overview
- Part 3: Physical Layer
- Part 4: Medium Access Control
- Part 5: MAC Layer Management
- Part 6: WLAN Mobility
- Part 7: WLAN Security
- Part 8: Public Hotspot Operations
- Part 9: WLAN – UMTS Interworking

Part 1:
Wireless Internet system architecture

SIEMENS mobile

- **Generic Internet network architecture**
- **Layering means encapsulation**
- **IEEE802.11 – seamless integration into the Internet**
- **IP based network architecture**
- **Wireless LAN IEEE802.11 basic architecture**
- **What is unique about wireless?**

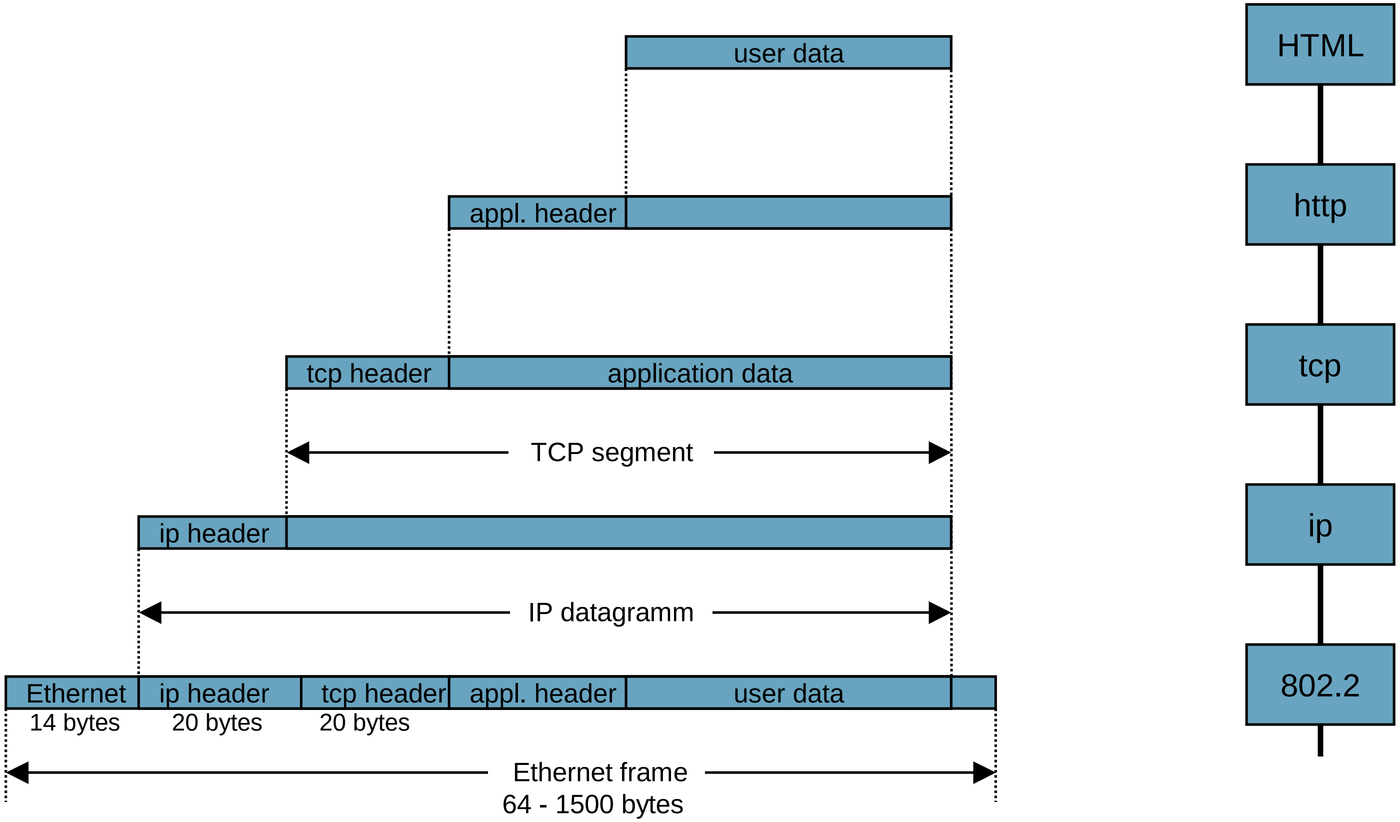
Generic Internet network architecture



Internet/Web Applications

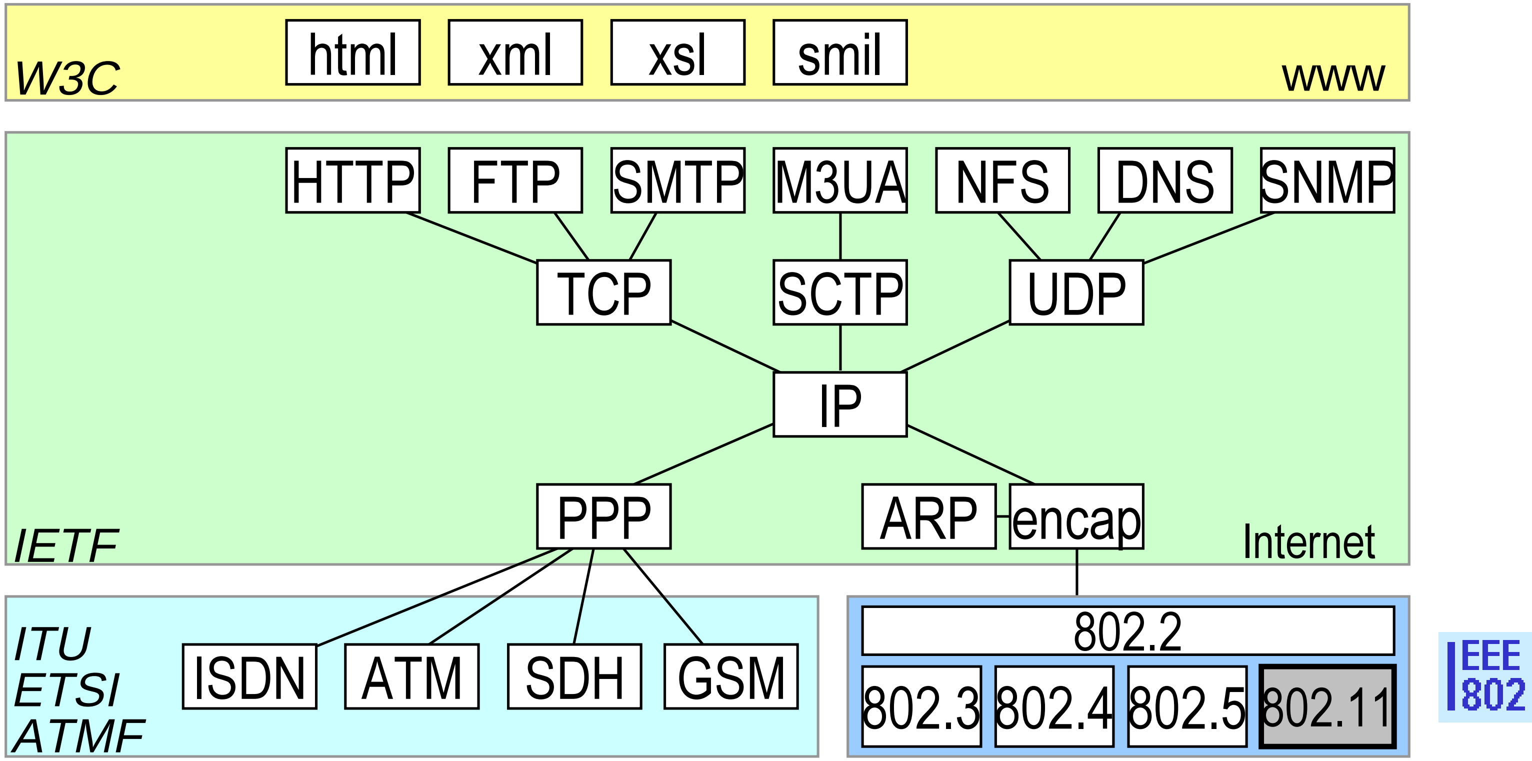
Client	WLAN AP		Router		Router		Router		Web-Server
www									www
http									http
tcp									tcp
ip			ip	ip	ip	ip	ip	ip	ip
802.2	802.2	802.2	802.2	link	link	link	link	link	link
802.11	802.11	802.3	802.3	phy	phy	phy	phy	phy	phy

Layering means encapsulation



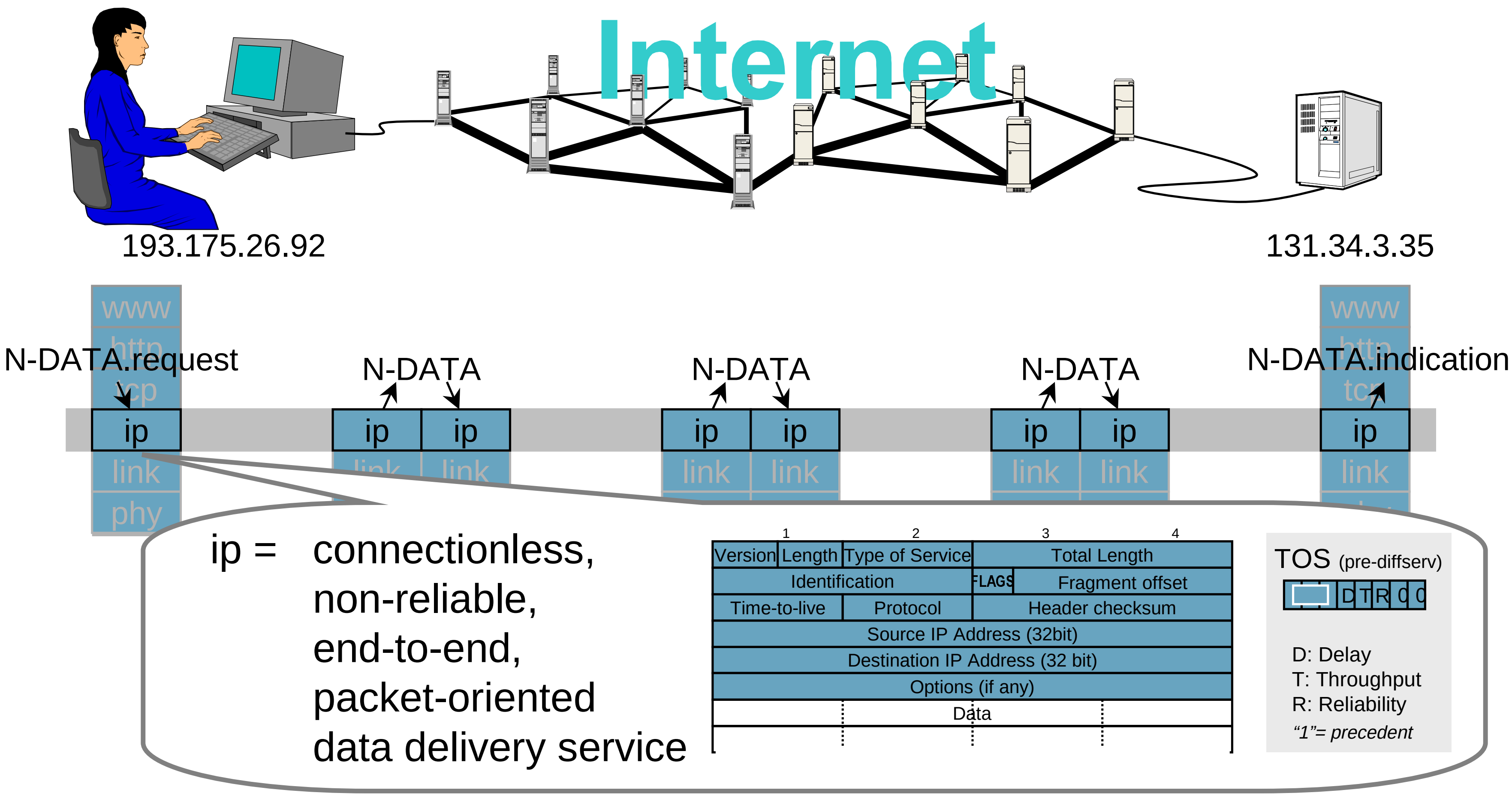
IEEE802.11 - seamless integration into the Internet

SIEMENS mobile

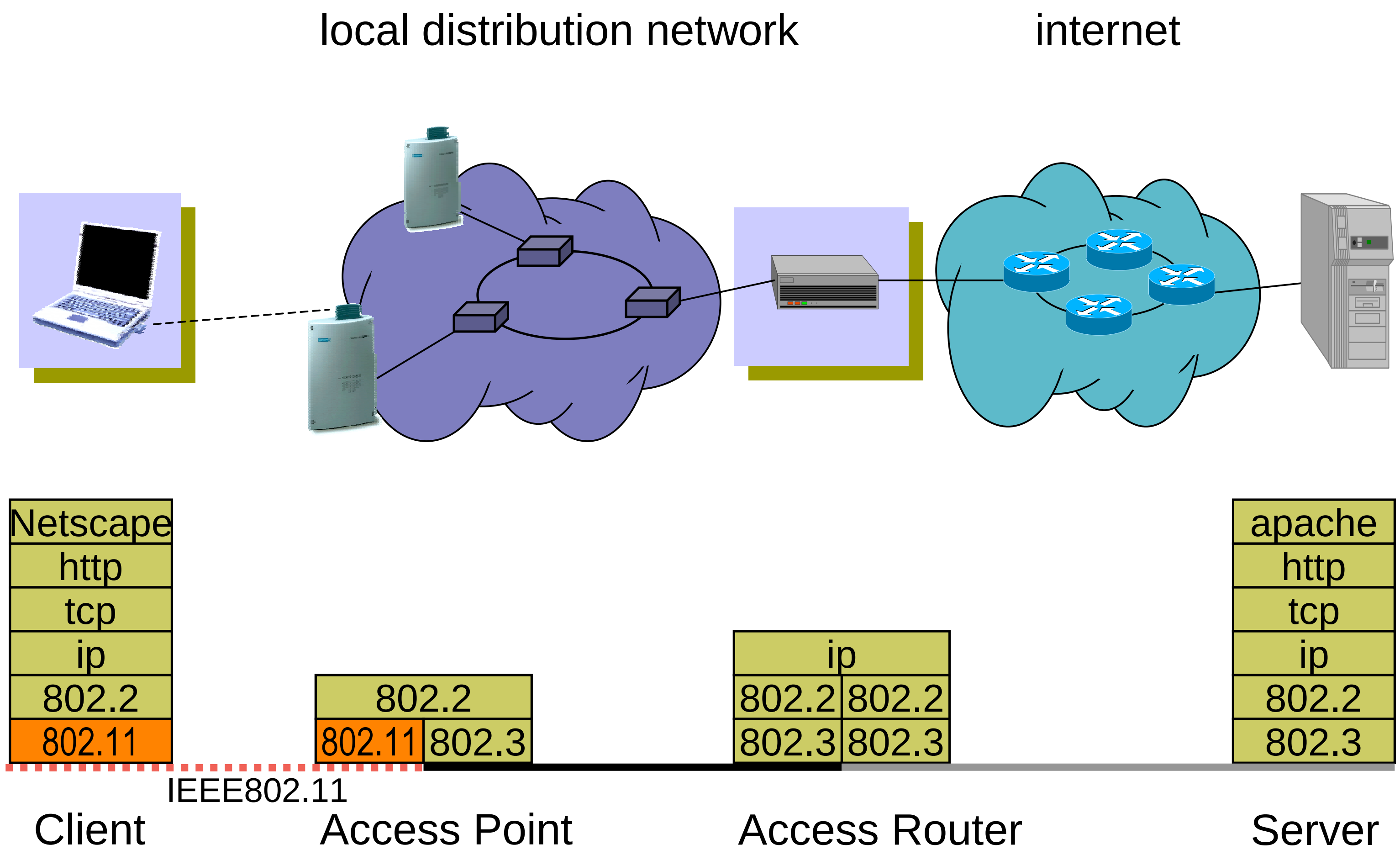


IP based network architecture

SIEMENS mobile



Wireless LAN IEEE802.11 basic architecture



What is unique about wireless?

SIEMENS mobile

- **Difficult media**
  - interference and noise
  - quality varies over space and time
  - shared with “unwanted” 802.11 devices
  - shared with non-802 devices (unlicensed spectrum, microwave ovens)
- **Full connectivity cannot be assumed**
  - “hidden node” problem
- **Mobility**
  - variation in link reliability
  - battery usage: requires power management
  - want “seamless” connections
- **Security**
  - no physical boundaries
  - overlapping LANs
- **Multiple international regulatory requirements**

Part 2: IEEE802.11 Overview

- Wireless IEEE802.11 Standard
- IEEE802.11 Configurations
- IEEE802.11 Architecture Overview
- IEEE802.11 Protocol Architecture
- Wireless LAN Standardization

Wireless IEEE802.11 Standard

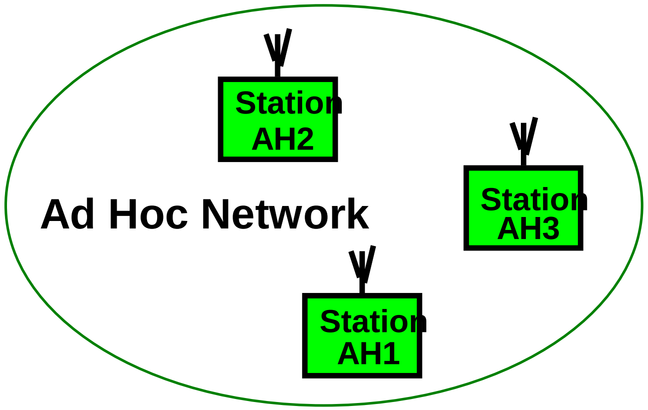
SIEMENS mobile

Approved June 1997
802.11b approved September 1999

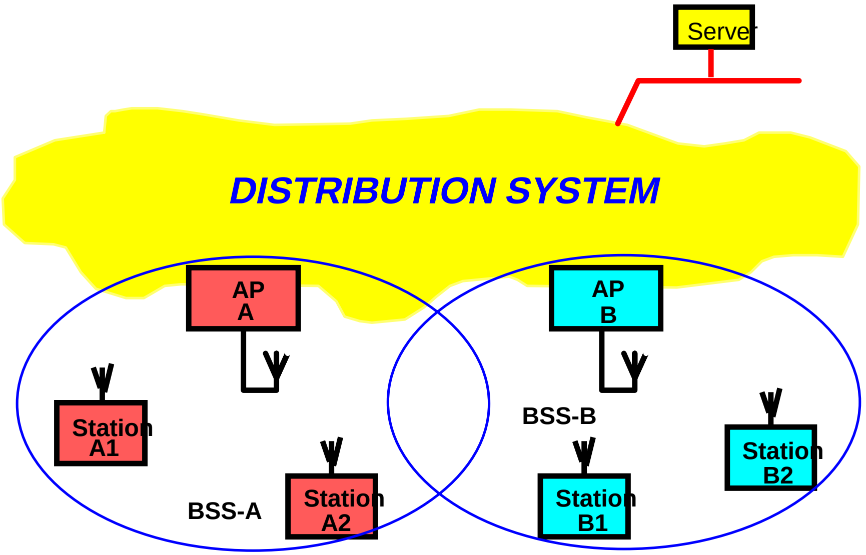
- **Operation in the 2.4GHz ISM band**
  - North America: FCC part 15.247-15.249
  - Europe: ETS 300 - 328
  - Japan: RCR - STD-33A
- **Supports three PHY layer types: DSSS, FHSS, Infrared**
- **MAC layer common to all 3 PHY layers**
- **Robust against interference**
- **Provides reliable, efficient wireless data networking**
- **Supports peer-to-peer and infrastructure configurations**
- **High data rate extension IEEE802.11b with 11 Mbps using existing MAC layer**

IEEE802.11 Configurations

- **Independent**
  - one “Basic Service Set”, BSS
  - “Ad Hoc” network
  - direct communication
  - limited coverage area



- **Infrastructure**
  - Access Points and stations
  - Distribution System interconnects Multiple Cells via Access Points to form a single Network.
    - extends wireless coverage area



IEEE802.11 Architecture Overview

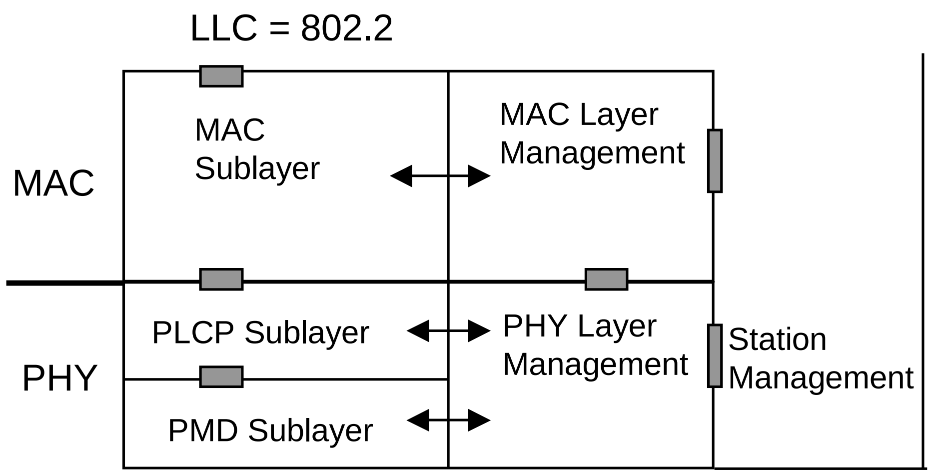
SIEMENS mobile

- **One common MAC supporting multiple 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)**
- **Security (WEP)**
- **Power savings (Sleep intervals)**

IEEE802.11 Protocol Architecture

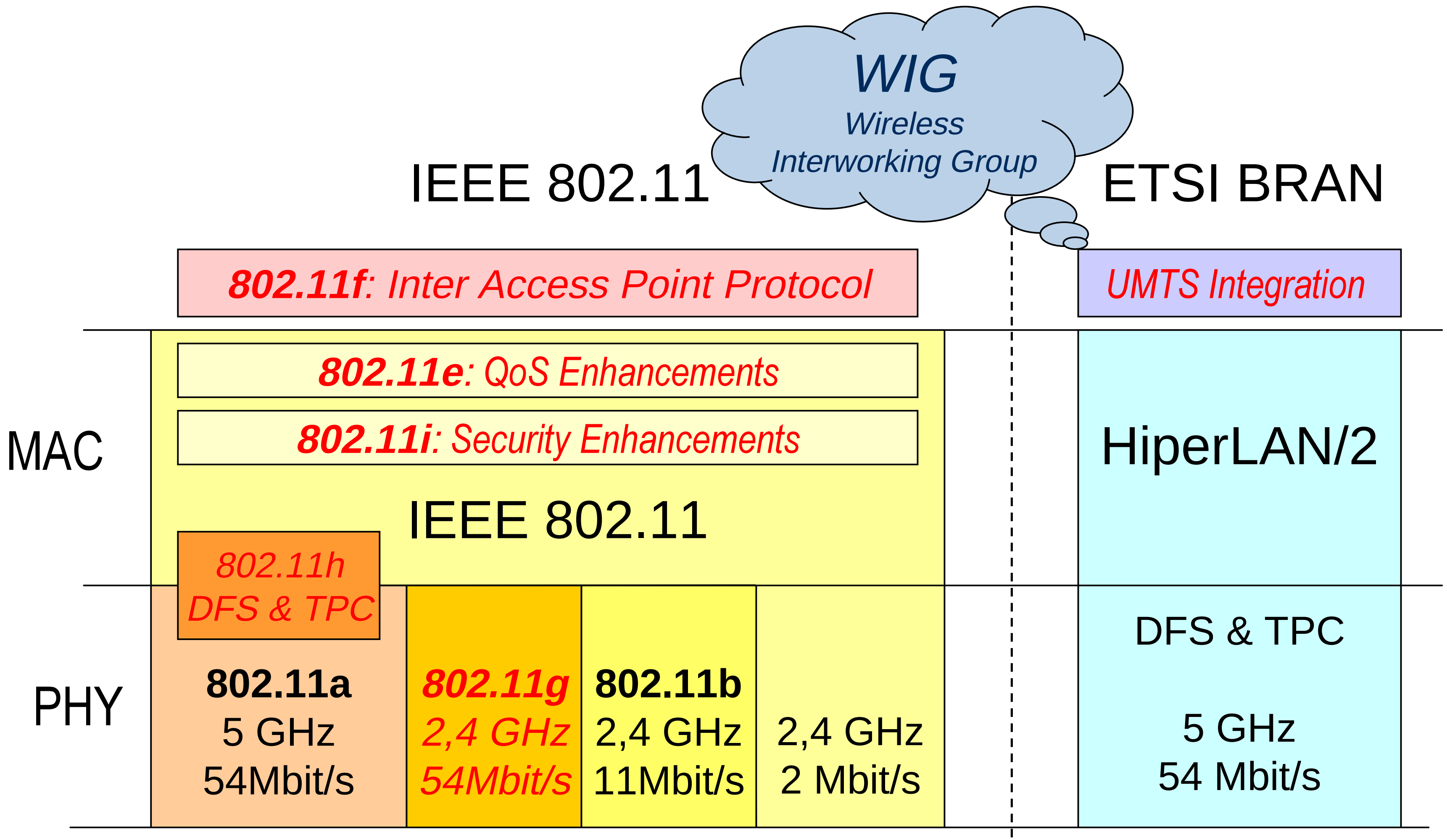
SIEMENS mobile

- **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



Wireless LAN Standardization

SIEMENS mobile



Current standardization topics

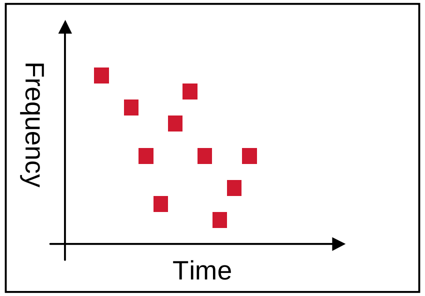
Part 3: Physical layer

- IEEE802.11 2.4 GHz & 5 GHz Physical Layers
- Frequency Hopping Spread Spectrum
- Direct Sequence Spread Spectrum
- DSSS Transmit Spectrum and Channels
- IEEE802.11a 5GHz PHY Layer
- IEEE802.11g: Further Speed Extension for the 2.4 GHz Band
- Spectrum Designation in the 5GHz range
- IEEE802.11h: Spectrum and Transmit Power Management
- ... when will 5 GHz WLANs come?
- PHY Terminology
- Physical Layer Convergence Protocol (PLCP)

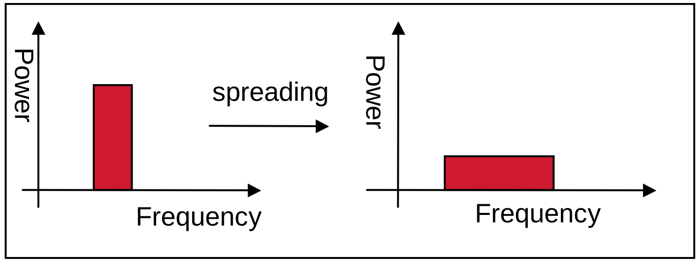
IEEE802.11
2.4 GHz & 5 GHz Physical Layers

SIEMENS mobile

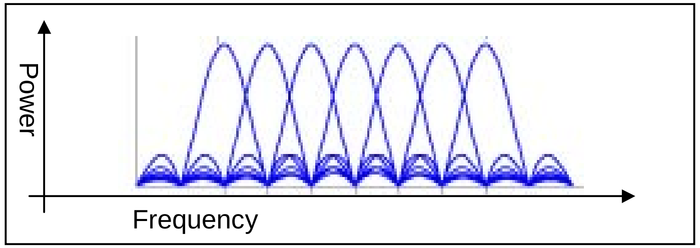
- ***Baseband IR, 1 and 2Mbps, 16-PPM and 4-PPM***
- **2.4 GHz *Frequency Hopping Spread Spectrum***
  - 2/4 FSK with 1/2 Mbps
  - 79 non overlapping frequencies of 1 MHz width (US)



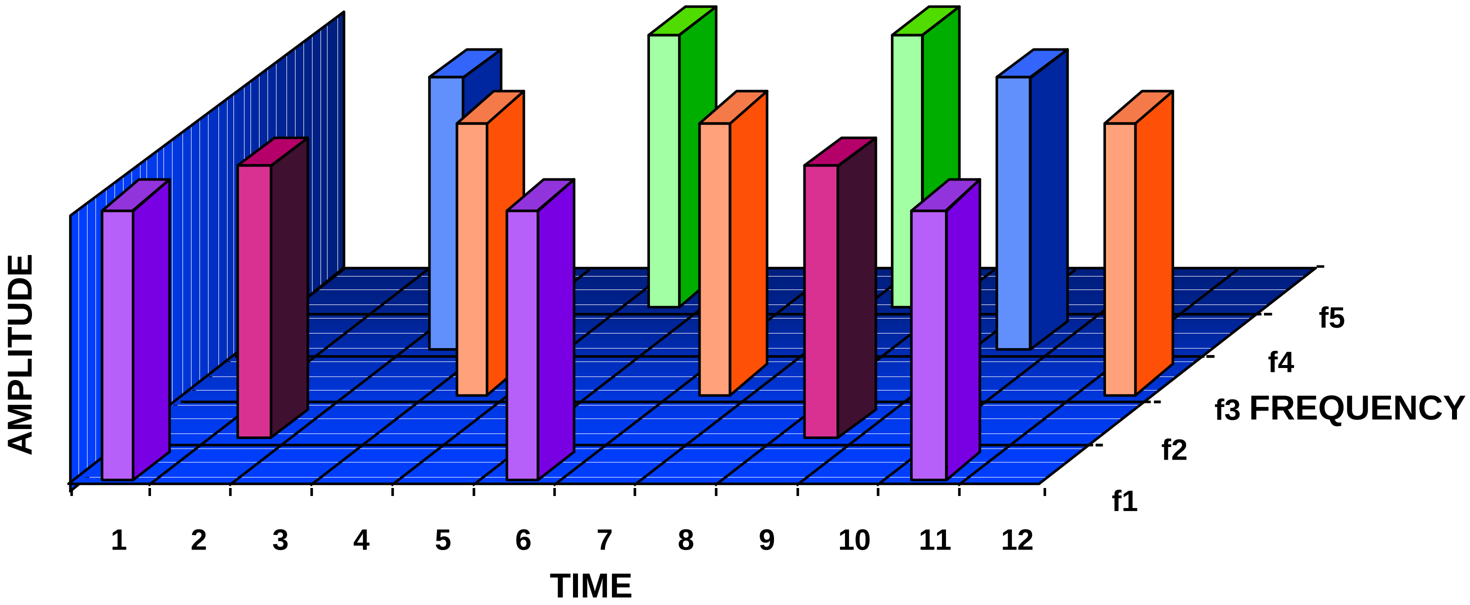
- **2.4 GHz *Direct Sequence Spread Spectrum***
  - DBPSK/DQPSK with 1/2 Mbps
  - Spreading with 11 Bit barker Code
  - 11/13 channels in the 2.4 GHz band



- **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



Frequency Hopping Spread Spectrum

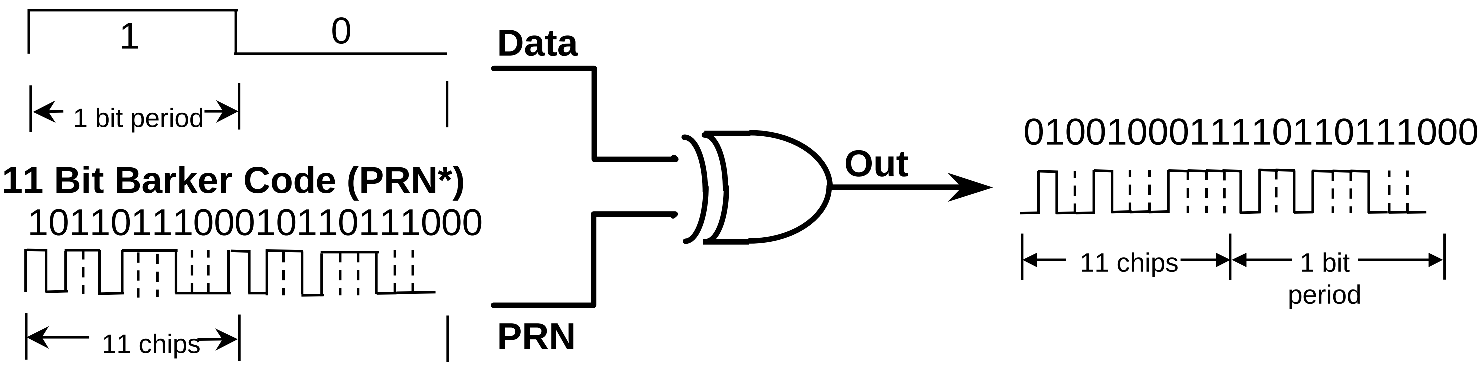


- 2.4GHz band is 83.5MHz wide (US & Europe)
- Band is divided into at least 75 channels
- Each channel is < 1MHz wide
- Transmitters and receivers hop in unison among channels in a pseudo random manner
- Power must be filtered to -20db at band edge

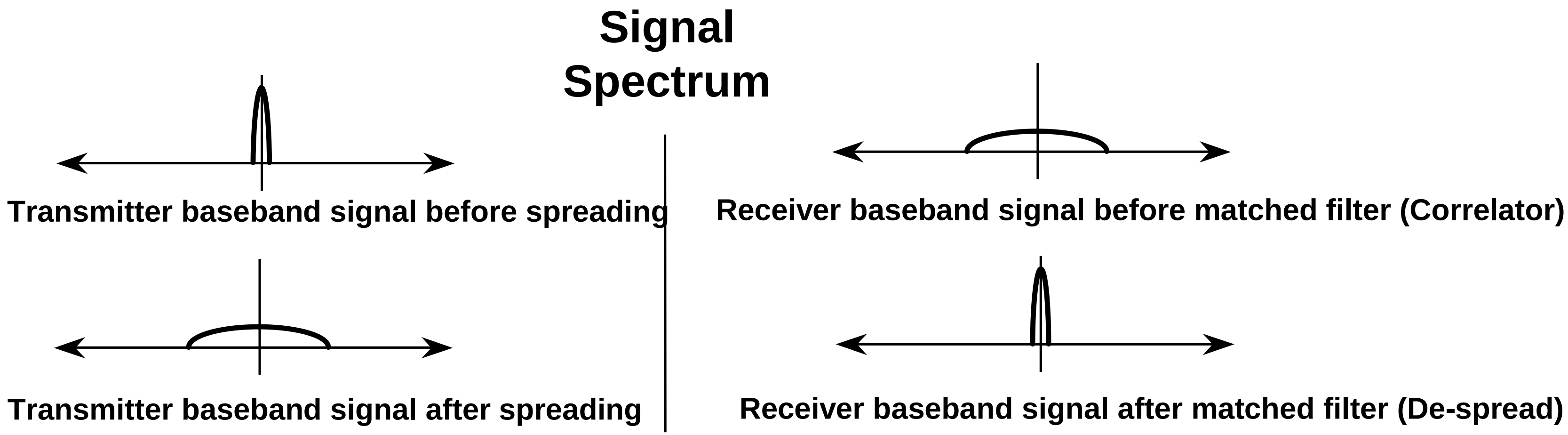
Direct Sequence Spread Spectrum

SIEMENS mobile

RF Energy is Spread by XOR of Data with PRN Sequence

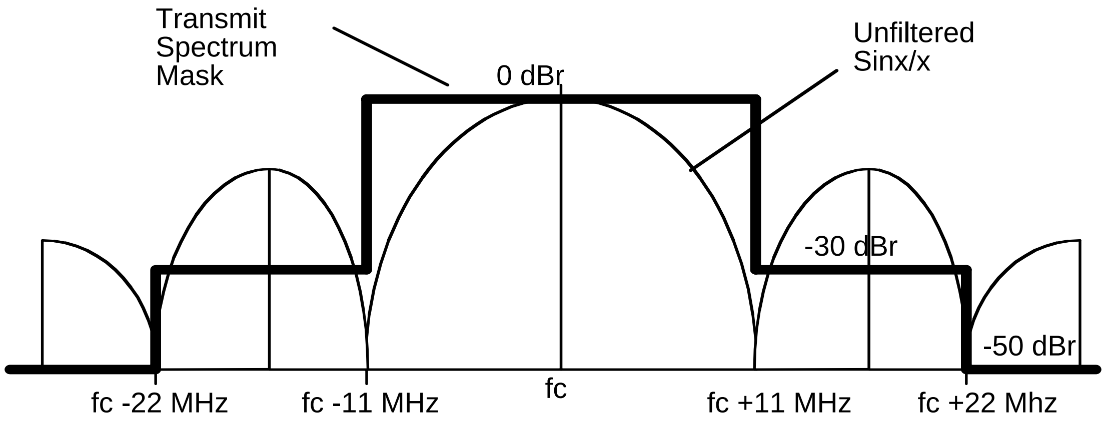


*** PRN: Pseudorandom Number**



DSSS Transmit Spectrum and Channels

SIEMENS mobile



Cannel	USA	ETSI	Japan
1	2412 MHz	2412 MHz	N/A
2	2417 MHz	2417 MHz	N/A
3	2422 MHz	2422 MHz	N/A
4	2427 MHz	2427 MHz	N/A
5	2432 MHz	2432 MHz	N/A
6	2437 MHz	2437 MHz	N/A
7	2442 MHz	2442 MHz	N/A
8	2447 MHz	2447 MHz	N/A
9	2452 MHz	2452 MHz	N/A
10	2457 MHz	2457 MHz	N/A
11	2462 MHz	2462 MHz	N/A
12	N/A	2467 MHz	N/A
13	N/A	2472 MHz	N/A
14	N/A	N/A	2484 MHz

IEEE802.11a 5GHz PHY Layer

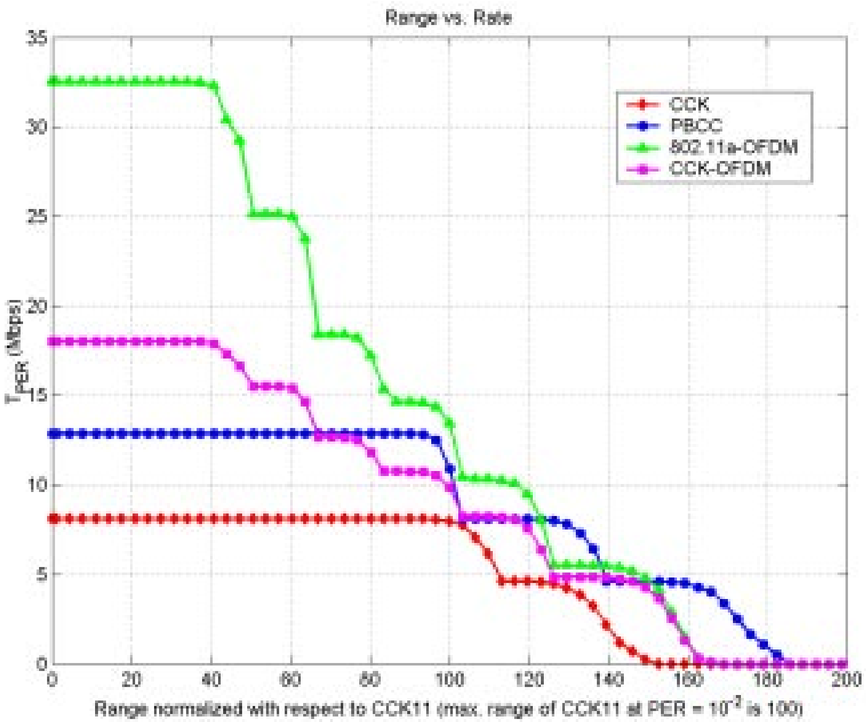
- **Specifications**
  - Modulation type OFDM
  - Data rates: 6, 12, 18, 24, 36, 48, 54Mbps
  - 48 sub-carriers
  - Sub-carrier modulation: BPSK, QPSK, 16QAM, 64QAM
  - Bit interleaved convolutional coding, K=7, R=1/2, 2/3, 3/4
  - OFDM frame duration: 4µs guard interval: 0.8ms
  - 18MHz channel spacing, 9-10 channels in 200MHz bandwidth
- **Key milestones**
  - First letter ballot by working group from November 1998 meeting
  - January 1999 joint meeting with ETSI-BRAN

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

SIEMENS mobile

Upcoming

- **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**



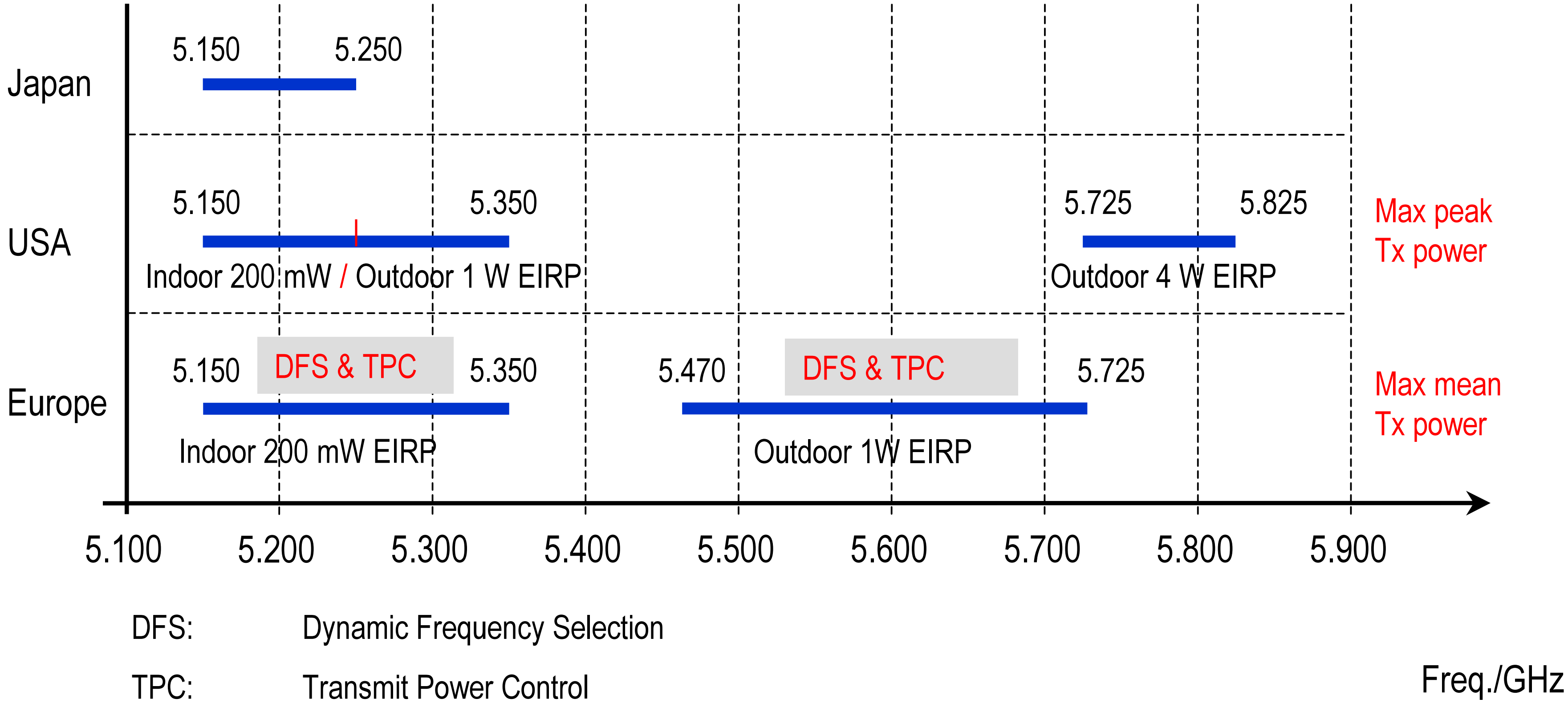
Range vs. throughput rate comparison of

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

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

Spectrum Designation in the 5 GHz range

SIEMENS mobile



DFS: Dynamic Frequency Selection

TPC: Transmit Power Control

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

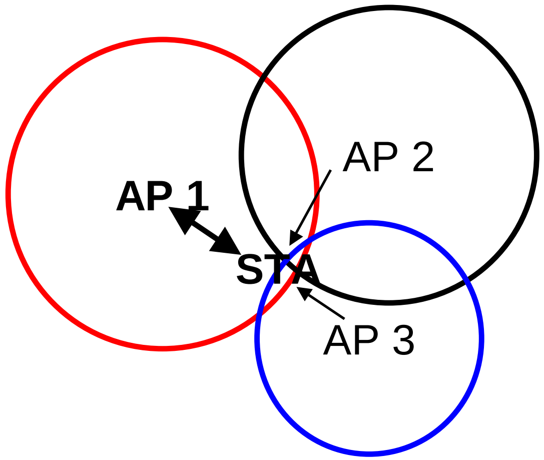
IEEE802.11h: Spectrum and Transmit Power Management

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.



… 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

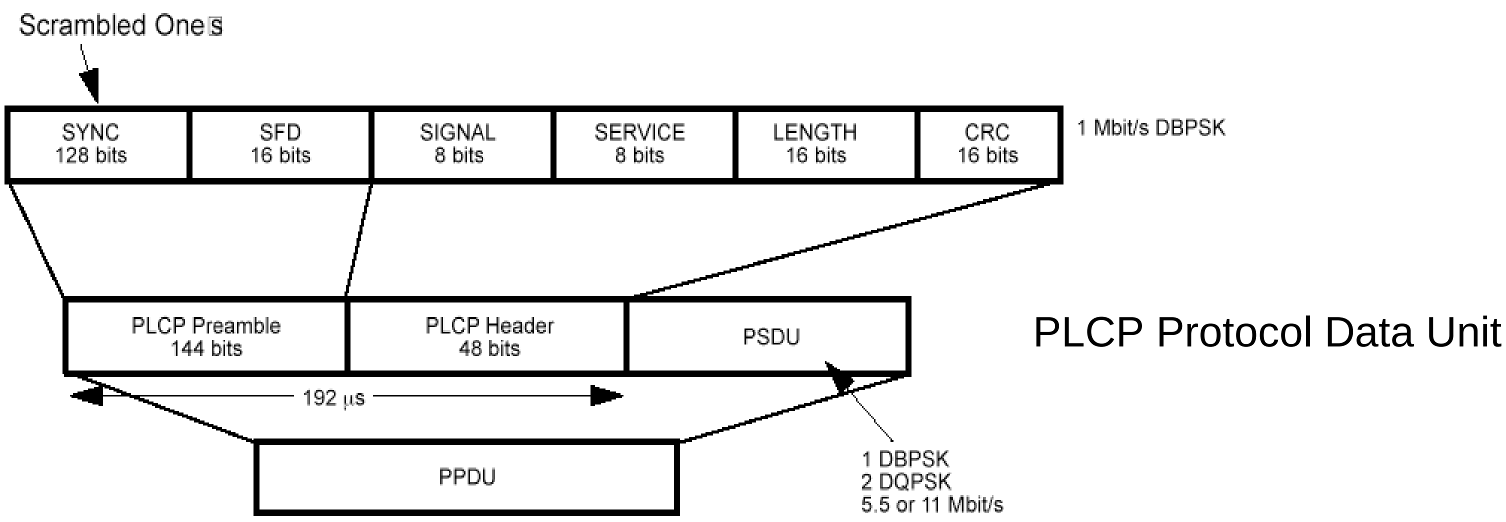
PHY Terminology

SIEMENS mobile

- FHSS Frequency Hoping Spread Spectrum
- DSSS Direct Sequence Spread Spectrum
- OFDM Orthogonal Frequency Division Multiplex

- PPM Pulse Position Modulation
- GFSK Gaussian Frequency Shift Keying
- DBPSK Differential Binary Phase Shift Keying
- DQPSK Differential Quadrature Phase Shift Keying
- CCK Complementary Code Keying
- PBCC Packet Binary Convolutional Coding
- QAM Quadrature Amplitude Modulation

Physical Layer Convergence Protocol (PLCP)



- **SYNC** **(gain setting, energy detection, antenna selection, frequency offset compensation)**
- **SFD** **(Start Frame Delimiter; bit synchronization)**
- **SIGNAL** **(rate indication; 1, 2, 5.5, 11 Mbit/s)**
- **SERVICE** **(reserved for future use)**
- **LENGTH** **(number of octets in PSDU)**
- **CRC** **(CCITT CRC-16, protects signal, service, length field)**

Part 4: Medium Access Control

SIEMENS mobile

- Basic Access Protocol Features
- CSMA/CA Explained
- CSMA/CA + ACK protocol
- Distributed Coordination Function (DCF)
- „Hidden Node“ Provisions
- IEEE802.11e: MAC Enhancements for Quality of Service (EDCF)
- Point Coordination Function (PCF)
- IEEE802.11e: MAC Enhancements for Quality of Service (HCF)
- Frame Formats
- Address Field Description
- Summary: MAC Protocol Features

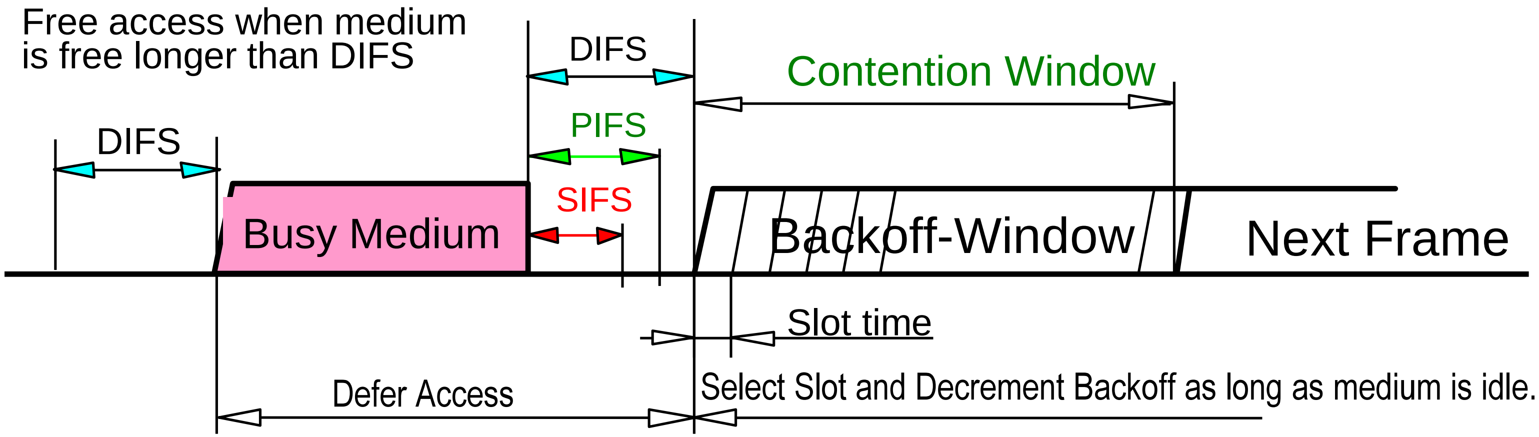
Basic Access Protocol Features

SIEMENS mobile

- **Use Distributed Coordination Function (DCF) for efficient medium sharing without overlap restrictions.**
  - Use CSMA with Collision Avoidance derivative.
  - Based on Carrier Sense function in PHY called Clear Channel Assessment (CCA).
- **Robust for interference.**
  - CSMA/CA + ACK for unicast frames, with MAC level recovery.
  - CSMA/CA for Broadcast frames.
- **Parameterized use of RTS / CTS to provide a Virtual Carrier Sense function to protect against Hidden Nodes.**
  - Duration information is distributed by both transmitter and receiver through separate RTS and CTS Control Frames.
- **Includes fragmentation to cope with different PHY characteristics.**

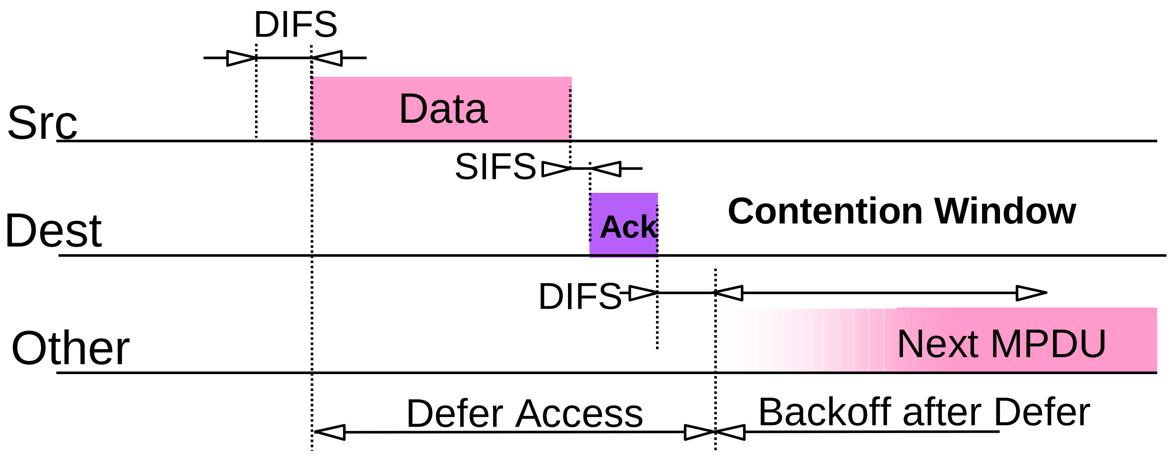
CSMA/CA Explained

IFS: Inter Frame Space



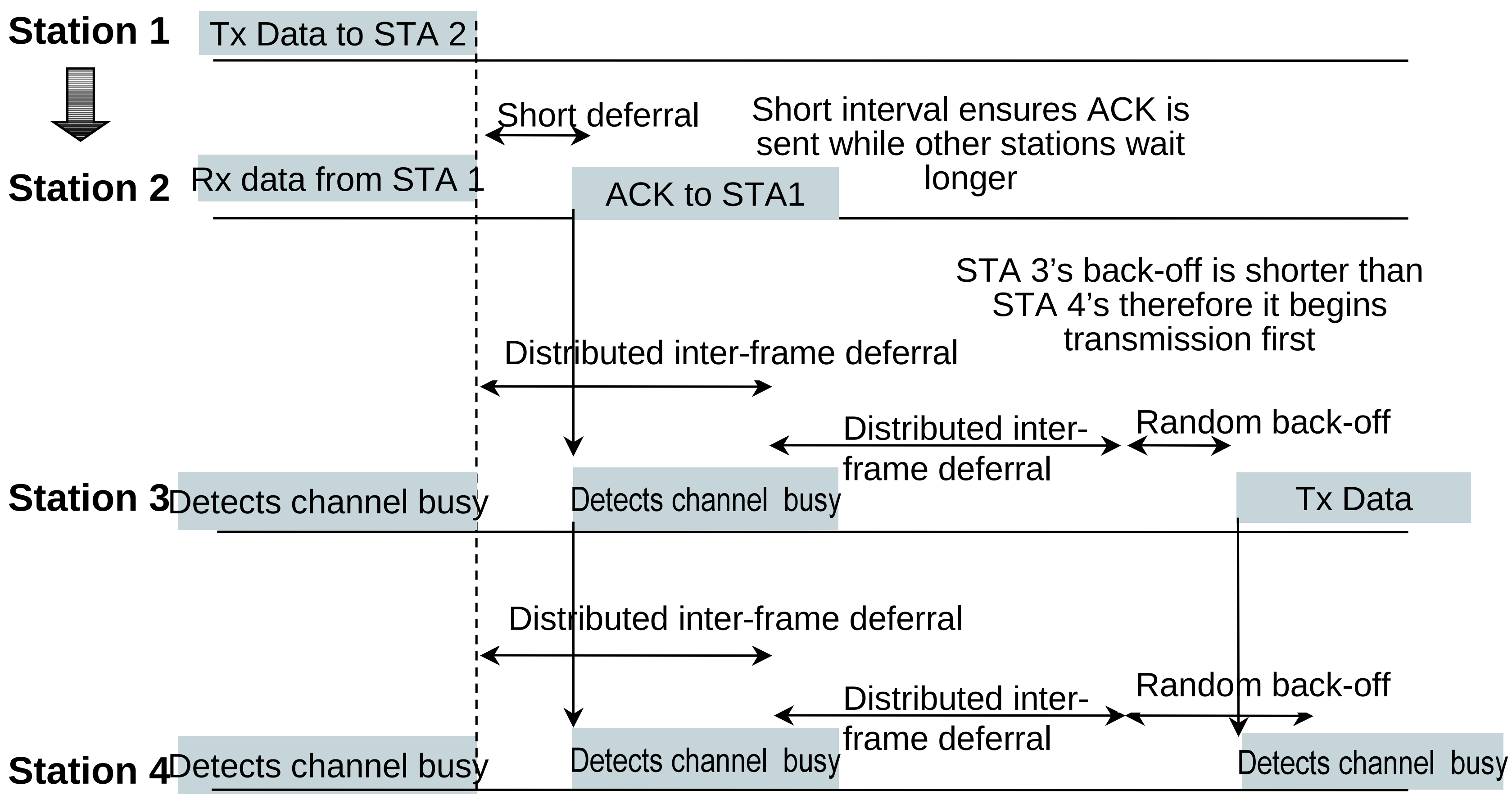
- **Reduce collision probability where mostly needed.**
  - Stations are waiting for medium to become free.
  - Select Random Backoff after a Defer, resolving contention to avoid collisions.
- **Efficient Backoff algorithm stable at high loads.**
  - Exponential Backoff window increases for retransmissions.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

CSMA/CA + ACK protocol



- **Defer access based on Carrier Sense.**
  - CCA 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).

Distributed Coordination Function (DCF)

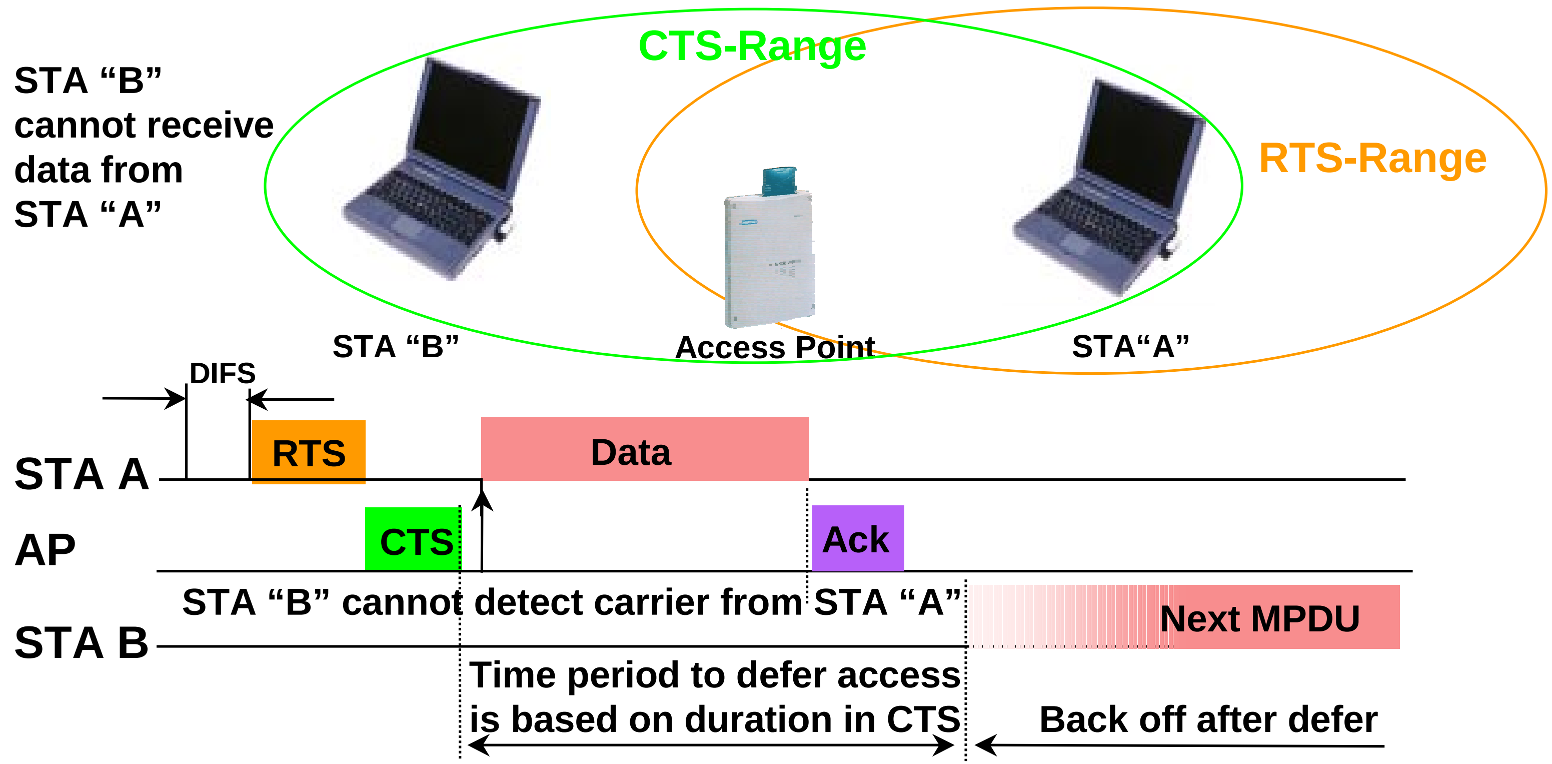


“Hidden Node” Provisions

SIEMENS mobile

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

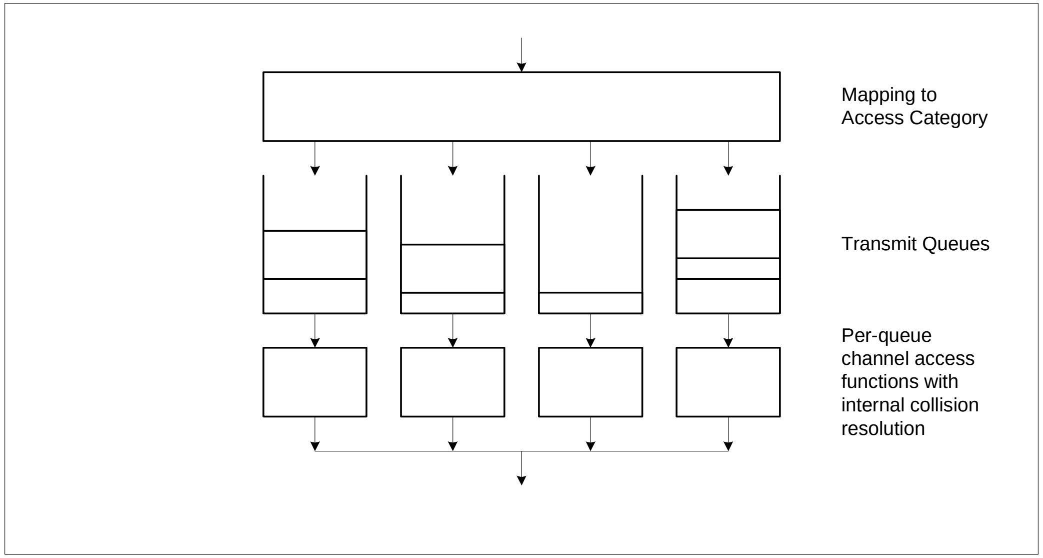


IEEE802.11e: MAC Enhancements for Quality of Service (EDCF)

SIEMENS mobile

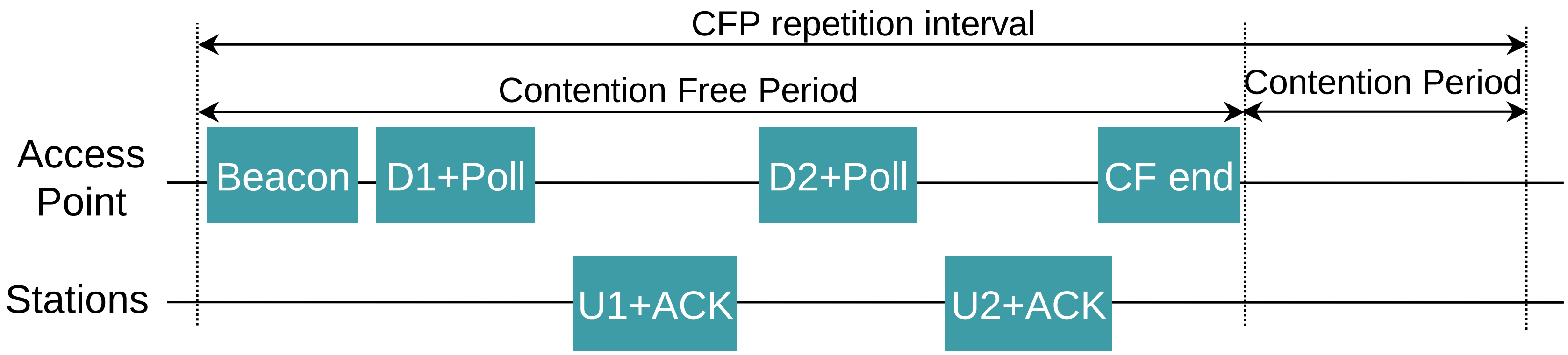
Upcoming

- **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



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, ...*

Frame Formats

SIEMENS mobile

802.11 MAC Header

Bytes:	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration ID	Addr 1	Addr 2	Addr 3	Sequence Control	Addr 4	Frame Body	CRC

Bits:	2	2	4	1	1	1	1	1	1	1	1
	Protocol Version	**Type**	**SubType**	**To DS**	**From DS**	**More Frag**	**Retry**	**Pwr Mgt**	**More Data**	**WEP**	**Rsvd**

- **MAC Header format differs per Type:**
  - Control Frames (several fields are omitted)
  - Management Frames
  - Data Frames
- **Includes Sequence Control Field for filtering of duplicate caused by ACK mechanism.**

Address Field Description

SIEMENS mobile

To DS	From DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	N/A
0	1	DA	BSSID	SA	N/A
1	0	BSSID	SA	DA	N/A
1	1	RA	TA	DA	SA

- **Addr 1 = All stations filter on this address.**
- **Addr 2 = Transmitter Address (TA)**
  – Identifies transmitter to address the ACK frame to.
- **Addr 3 = Dependent on To and From DS bits.**
- **Addr 4 = Only needed to identify the original source of WDS (Wireless Distribution System) frames.**

Summary: MAC Protocol Features

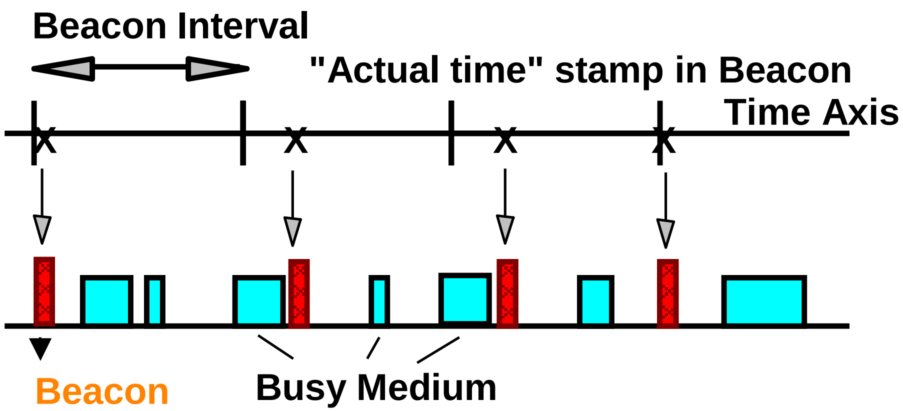
SIEMENS mobile

- **Distributed Coordination Function (DCF) provides efficient medium sharing**
  - Use Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)
  - MAC uses the PHY layer Clear Channel Assessment (CCA) function for CSMA/CA
- **Robust for interference**
  - CSMA/CA + ACK for unicast frames, with MAC level recovery
  - CSMA/CA for broadcast frames
- **Virtual carrier sense function provided to protect against hidden nodes**
- **Includes fragmentation to cope with different PHY characteristics**
- **Point Coordination Function (PCF) option for time bounded data**
- **Frame formats to support multiple configurations and roaming**

Part 5: MAC layer management

- Infrastructure Beacon Generation
- Timing Synchronization Function
- Scanning
- Active Scanning Example
- Power Management Considerations
- Power Management Approach
- Power Management Procedure
- MAC Management Frames

Infrastructure Beacon Generation



- **APs send Beacons in infrastructure networks.**
- **Beacons scheduled at Beacon Interval.**
- **Transmission may be delayed by CSMA deferral.**
  - subsequent transmissions at expected Beacon Interval
  - not relative to last Beacon transmission
  - next Beacon sent at Target Beacon Transmission Time
- **Timestamp contains timer value at transmit time.**

Timing Synchronization Function (TSF)

- **All stations maintain a local timer.**
  - Used for Power Management
    - All station timers in BSS are synchronized
  - Used for Point Coordination Timing
    - TSF Timer used to predict start of Contention Free burst
- **Timing Synchronization Function (TSF)**
  - keeps timers from all stations in synch
  - AP controls timing in infrastructure networks
  - distributed function for Independent BSS
- **Timing conveyed by periodic Beacon transmissions**
  - Beacons contain Timestamp for the entire BSS
  - Timestamp from Beacons used to calibrate local clocks
  - not required to hear every Beacon to stay in synch
  - Beacons contain other management information
    - also used for Power Management, Roaming

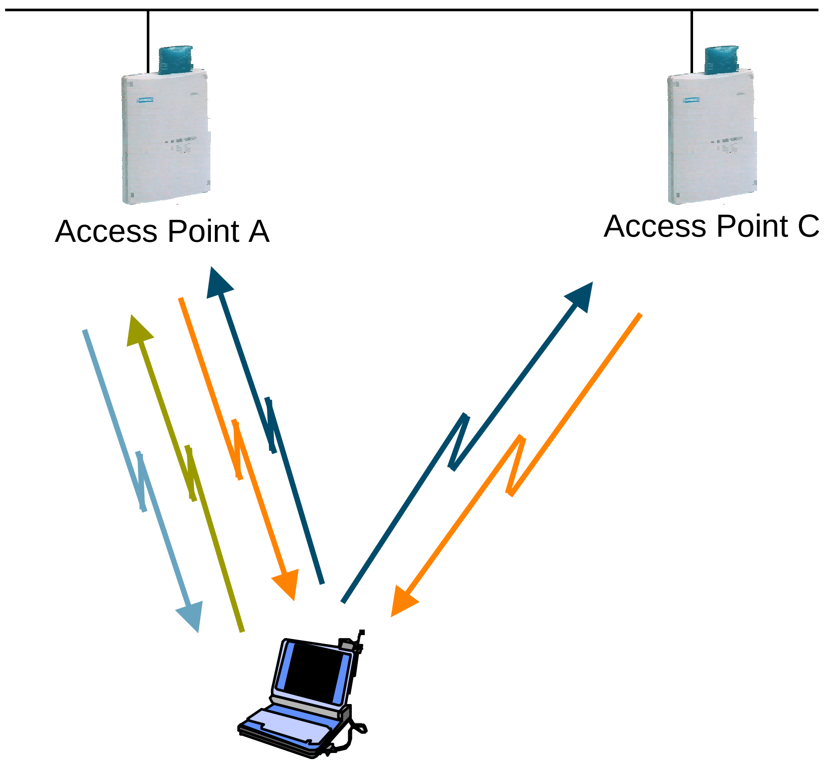
Scanning

- **Scanning required for many functions.**
  - finding and joining a network
  - finding a new AP while roaming
  - initializing an Independent BSS (ad hoc) network
- **802.11 MAC uses a common mechanism for all PHY.**
  - single or multi channel
  - passive or active scanning
- **Passive Scanning**
  - Find networks simply by listening for Beacons
- **Active Scanning**
  - On each channel
    - Send a Probe, Wait for a Probe Response
- **Beacon or Probe Response contains information necessary to join new network.**

Active Scanning Example

SIEMENS mobile

- **Initial connection to an Access Point**
  – Reassociation follows a similar process



Steps to Association:

- Station sends Probe.
- APs send Probe Response.
- Station selects best AP.
- Station sends Association Request to selected AP.
- AP sends Association Response.

Power Management Considerations

SIEMENS mobile

- **Mobile devices are battery powered.**
  – Power Management is important for mobility.
- **Current LAN protocols assume stations are always ready to receive.**
  – Idle receive state dominates LAN adapter power consumption over time.
- **How can we power off during idle periods, yet maintain an active session?**
- **802.11 Power Management Protocol:**
  – allows transceiver to be off as much as possible
  – is transparent to existing protocols
  – is flexible to support different applications
    - possible to trade off throughput for battery life

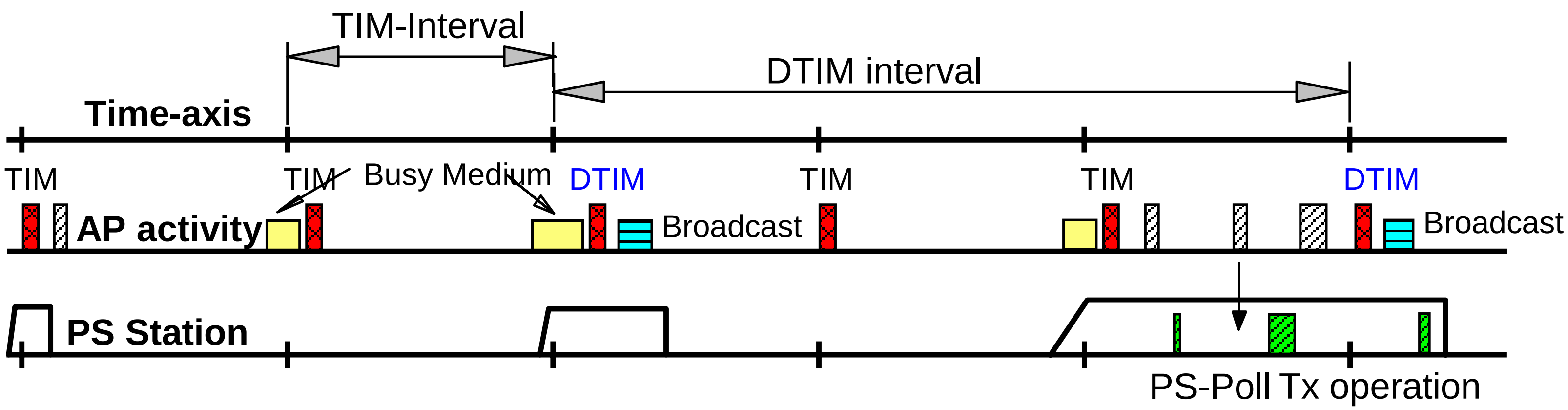
Power Management Approach

SIEMENS mobile

- **Allow idle stations to go to sleep**
  - station's power save mode stored in AP
- **APs buffer packets for sleeping stations.**
  - AP announces which stations have frames buffered
  - Traffic Indication Map (TIM) sent with every Beacon
- **Power Saving stations wake up periodically**
  - listen for Beacons
- **TSF assures AP and Power Save stations are synchronized**
  - stations will wake up to hear a Beacon
  - TSF timer keeps running when stations are sleeping
  - synchronization allows extreme low power operation
- **Independent BSS also have Power Management**
  - similar in concept, distributed approach

Power Management Procedure

SIEMENS mobile



- **Stations wake up prior to an expected DTIM (Delivery Traffic Indication Message).**
- **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 DTIM.
  – DTIM interval is a multiple of TIM interval

MAC Management Frames

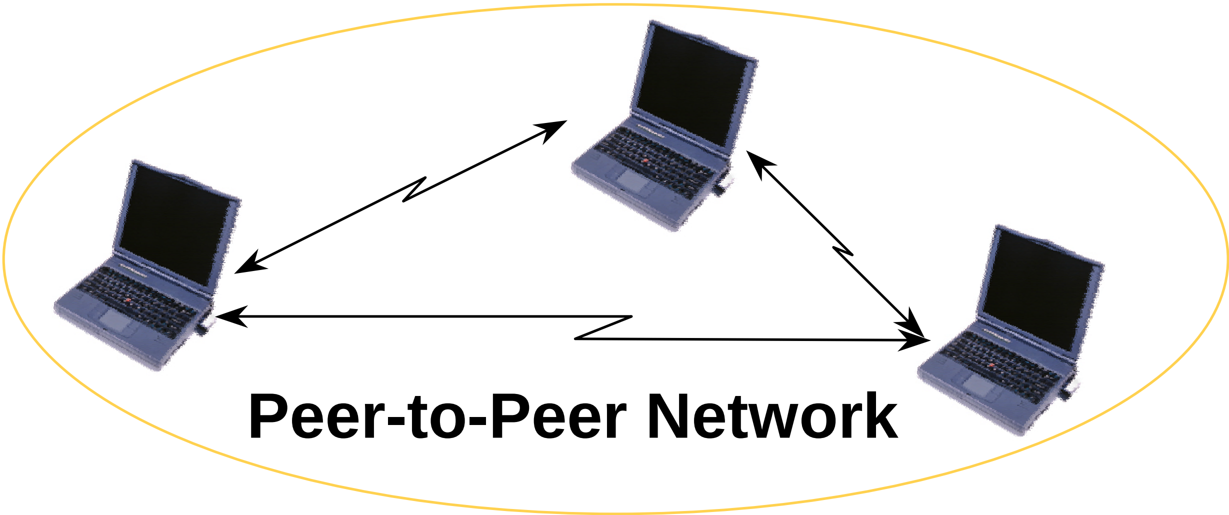
SIEMENS mobile

- **Beacon**
  - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, parameters
  - Traffic Indication Map
- **Probe**
  - ESSID, Capabilities, Supported Rates
- **Probe Response**
  - Timestamp, Beacon Interval, Capabilities, ESSID, Supported Rates, pars
  - same for Beacon except for TIM
- **Association Request**
  - Capability, Listen Interval, ESSID, Supported Rates
- **Association Response**
  - Capability, Status Code, Station ID, Supported Rates
- **Reassociation Request**
  - Capability, Listen Interval, ESSID, Supported Rates, Current AP Address
- **Reassociation Response**
  - Capability, Status Code, Station ID, Supported Rates
- **Disassociation**
  - Reason code

Part 6: WLAN Mobility

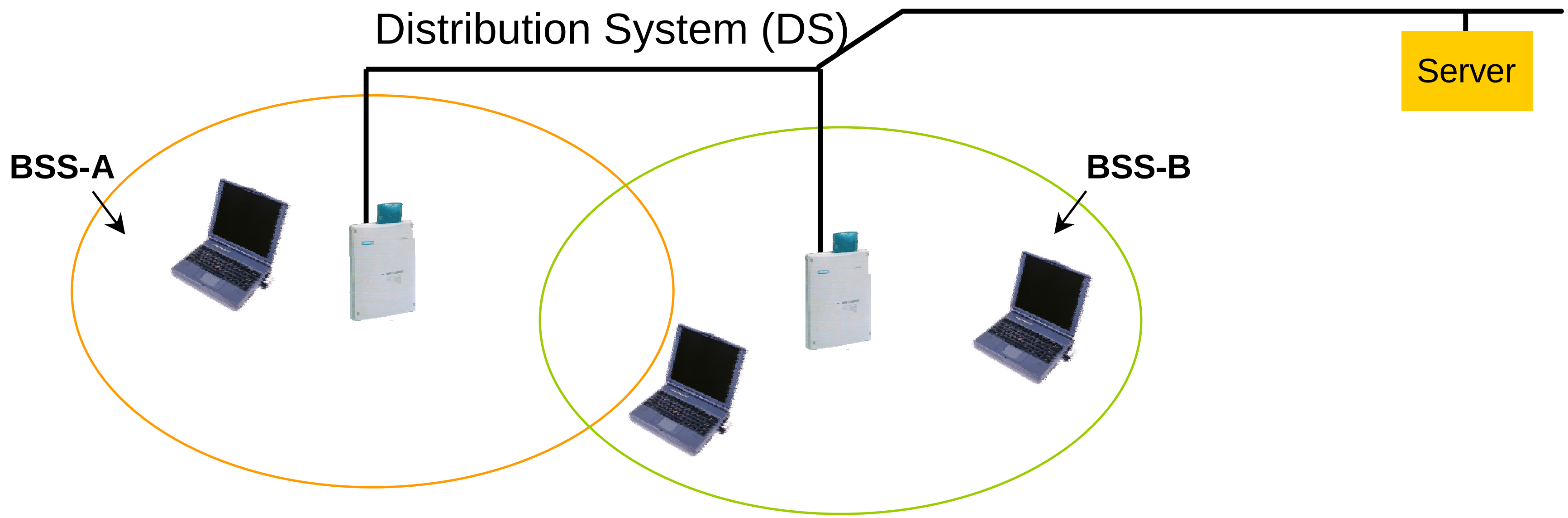
- **IEEE802.11 Ad Hoc Mode**
- **IEEE802.11 Infrastructure Mode**
- **Mobility inside a WLAN ‚hotspot' by link layer functions...**
- **IEEE802.11f: Inter-Access Point Protocol (IAPP)**

IEEE802.11 Ad Hoc Mode



- **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

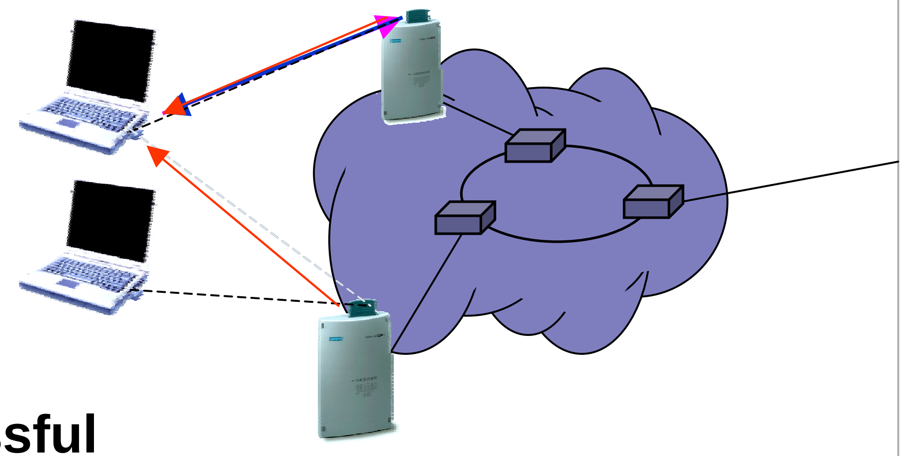
IEEE802.11 Infrastructure Mode



- 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

Mobility inside a WLAN 'hotspot' by link layer functions...

- **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**



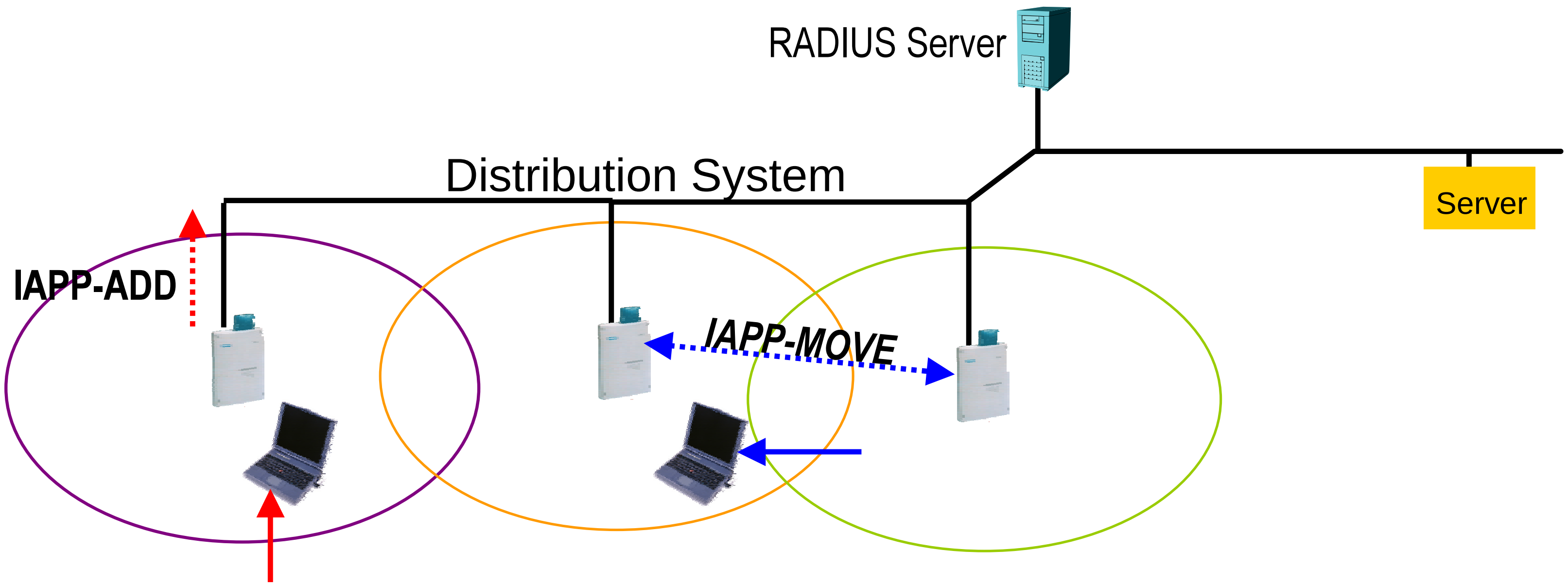
- **If Reassociation Response is successful**
  - then station has roamed to the new AP
  - else station scans for another AP
- **If AP accepts Reassociation Request**
  - normally old AP is notified through Distribution System
  - AP indicates Reassociation to the Distribution System

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



Part 7: WLAN security

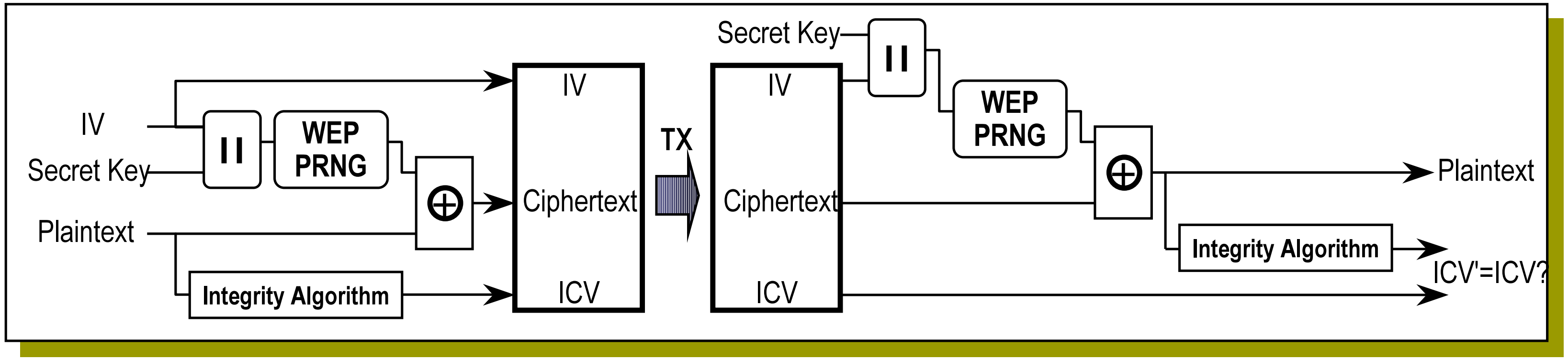
- IEEE802.11 Privacy and Access Control
- WEP privacy mechanism
- Shared key authentication
- Shortcomings of plain WEP security
- IEEE802.11i: Robust Security Network (RSN)
- A last word about WLAN security:
- Summary: MAC Functionality

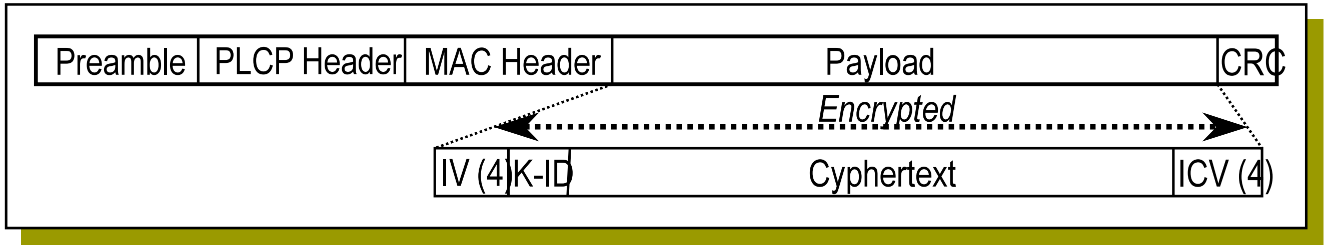
IEEE802.11 Privacy and Access Control

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.

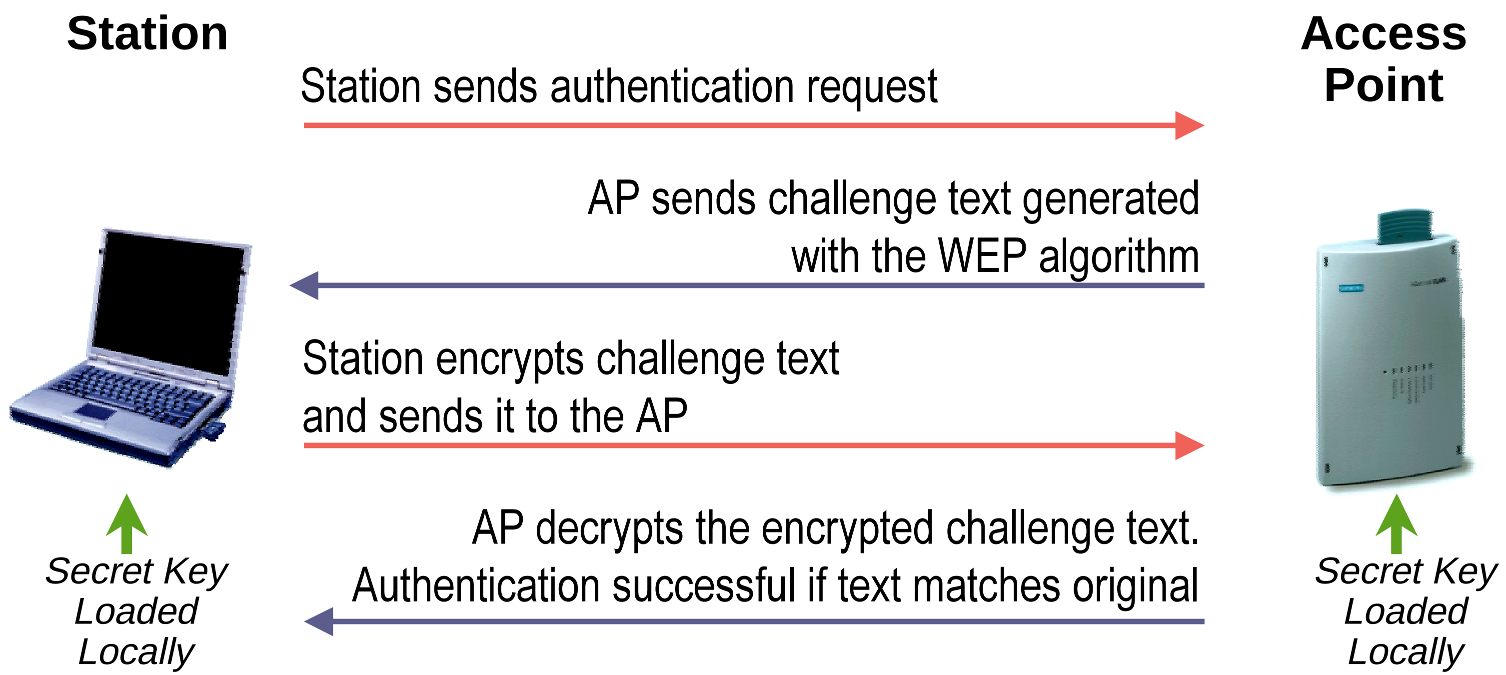
WEP privacy mechanism





- **WEP bit in Frame Control Field indicates WEP used.**
  – Each frame can have a new IV, or IV can be reused for a limited time.

Shared key authentication



- **Shared key authentication requires WEP**
- **Key exchange is not specified by IEEE802.11**
- **Only one way authentication**

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.

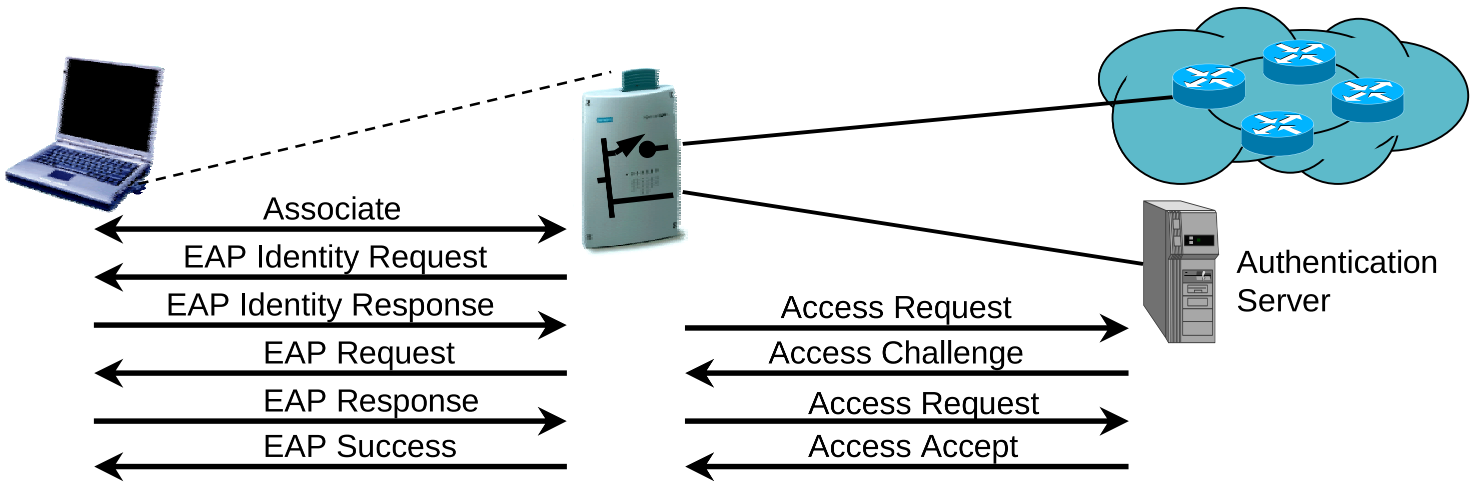
IEEE802.11i: Robust Security Network (RSN)

Upcoming

SIEMENS mobile

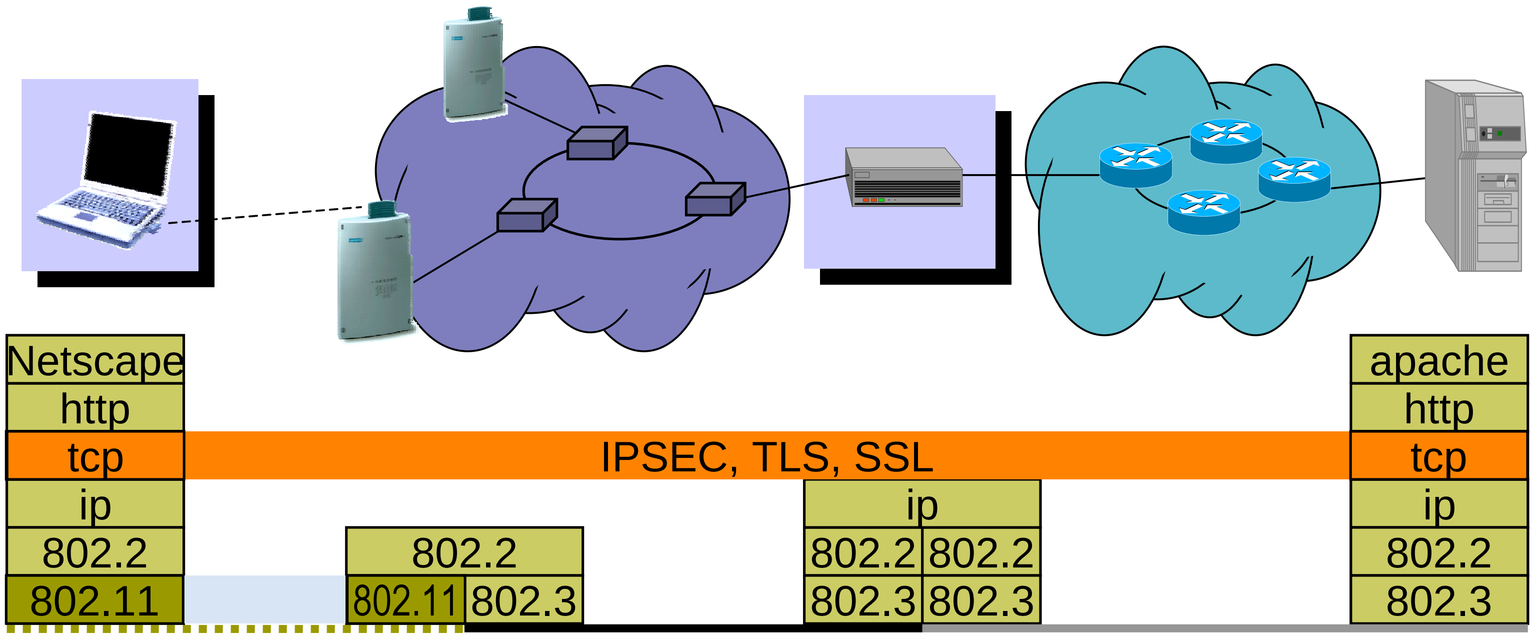
Additional enhancement to existing IEEE802.11 functions:

- **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:

- **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.**

Summary: MAC Functionality

SIEMENS mobile

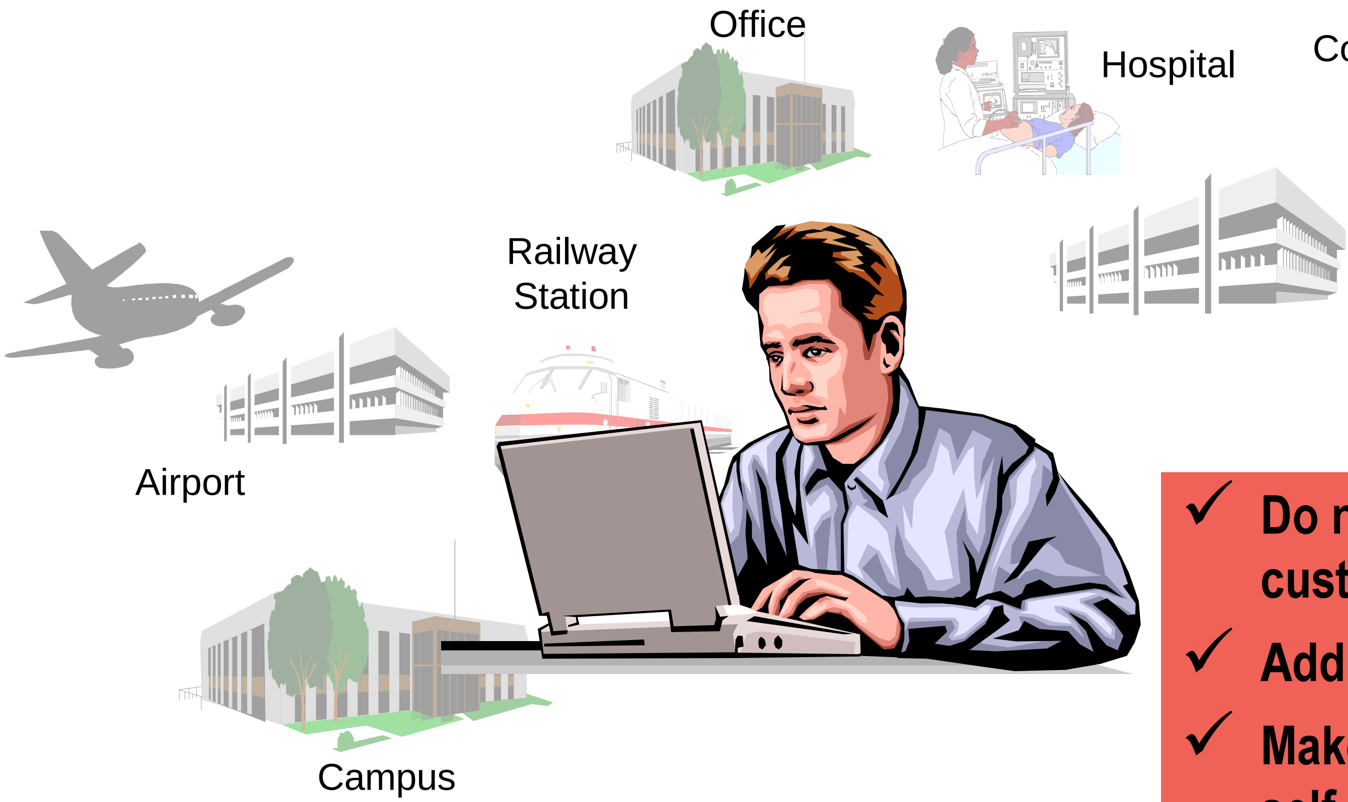
- **Independent and Infrastructure configuration support**
  - Each BSS has a unique 48 bit address
  - Each ESS has a variable length address
- **CSMA with collision avoidance**
  - MAC-level acknowledgment
  - allows for RTS/CTS exchanges (hidden node protection)
  - MSDU fragmentation
  - "Point Coordination" option (AP polling)
- **Association and Reassociation**
  - station scans for APs, association handshakes
  - Roaming support within an ESS
- **Power management support**
  - stations may power themselves down
  - AP buffering, distributed approach for IBSS
- **Authentication and privacy**
  - Optional support of "Wired Equivalent Privacy" (WEP)
  - Authentication handshakes defined

Part 8: Public hotspot operation

- **Serving customers in public hot spots...**
- **One solution for every place (hotspot)**
- **Becoming a WLAN operator is easy.**
- **Selling WLAN access in public hot-spots: Probably to consider...**
- **Using a web page for initial user interaction**
- **How does it work: Web based access control**
- **Web based access control: Enabler for mCommerce and location based services**
- **Functions of an integrated access gateway (User Management)**
- **Functions of an integrated access gateway (Network services)**

Serving customers in public hot spots...

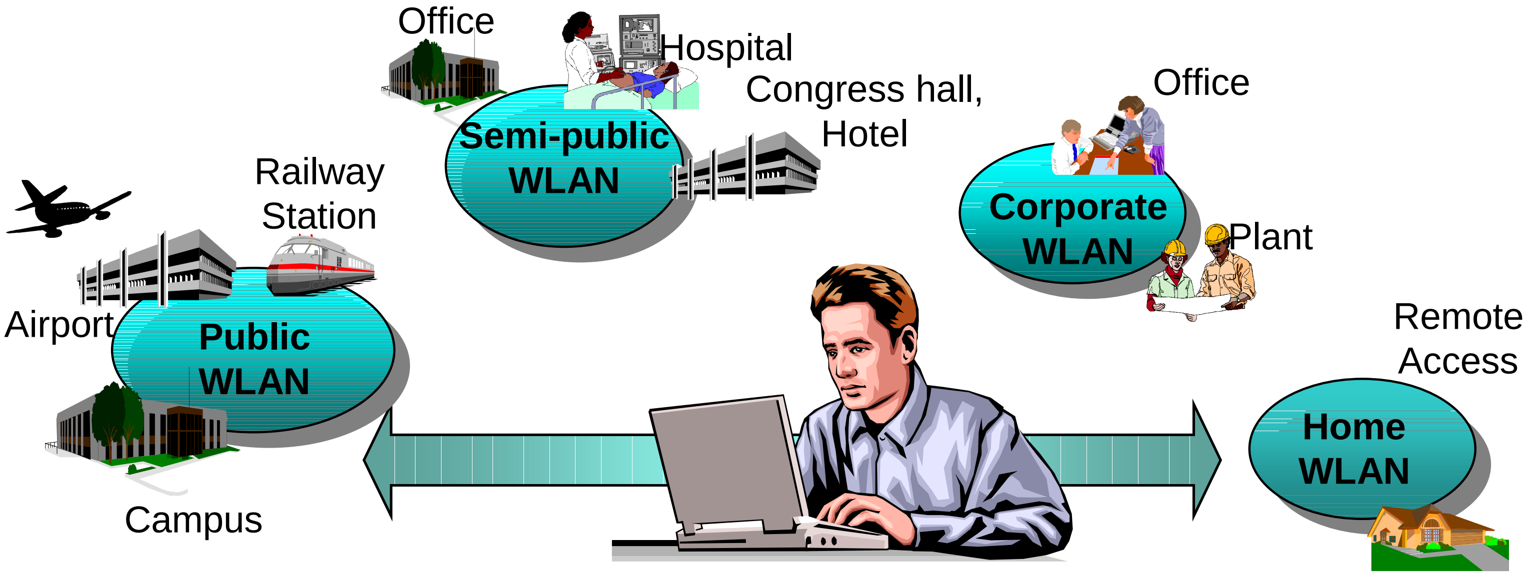
SIEMENS mobile



- ✓ Do not touch customer equipment
- ✓ Address all customers
- ✓ Make access procedure self explaining

One solution for every place (hotspot)

- There is a wide variety of notebooks each having more or less its unique configuration.
- Only a very common dominator can be assumed for the software installations available on all notebooks.



- Most WLAN-enabled notebooks will use DHCP for basic IP configuration.
- A web-browser will likely be available on all notebooks.

Becoming a WLAN operator is easy.

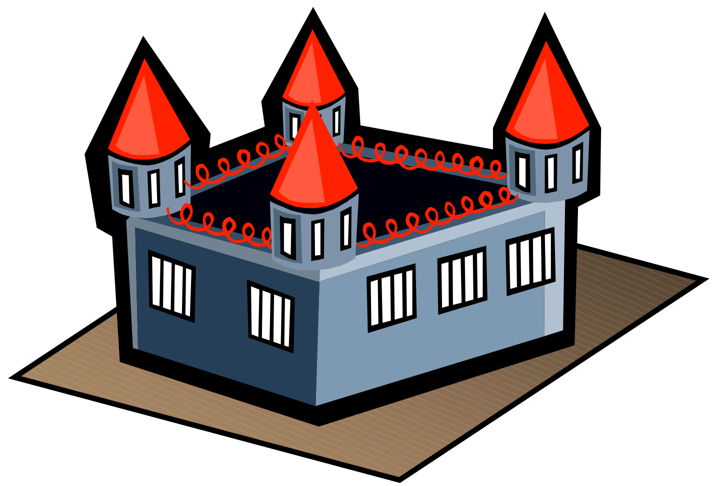
SIEMENS mobile

- **Legal aspects (in Germany):**
  - 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!

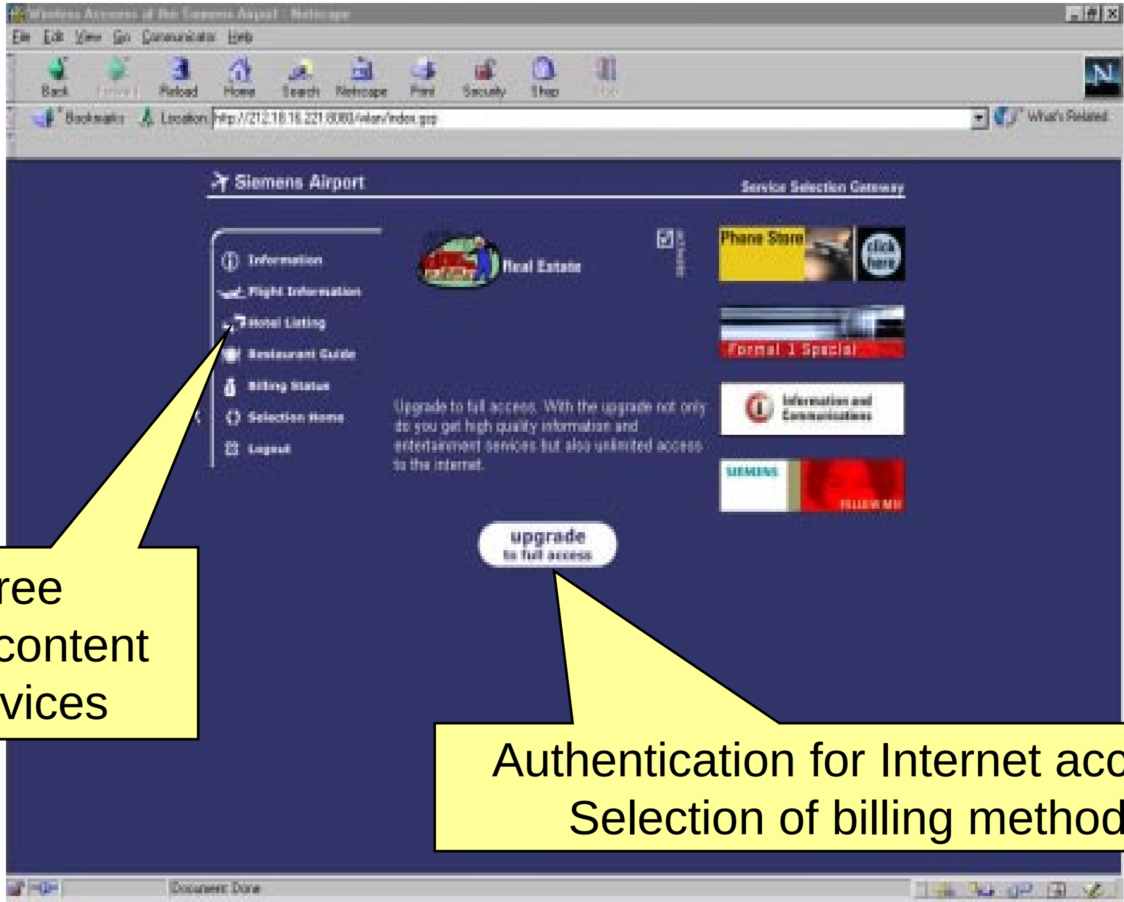
Selling WLAN access in public hot-spots: Probably to consider …

- **How does your favorite storefront look like?**



Too much security might hinder your business!

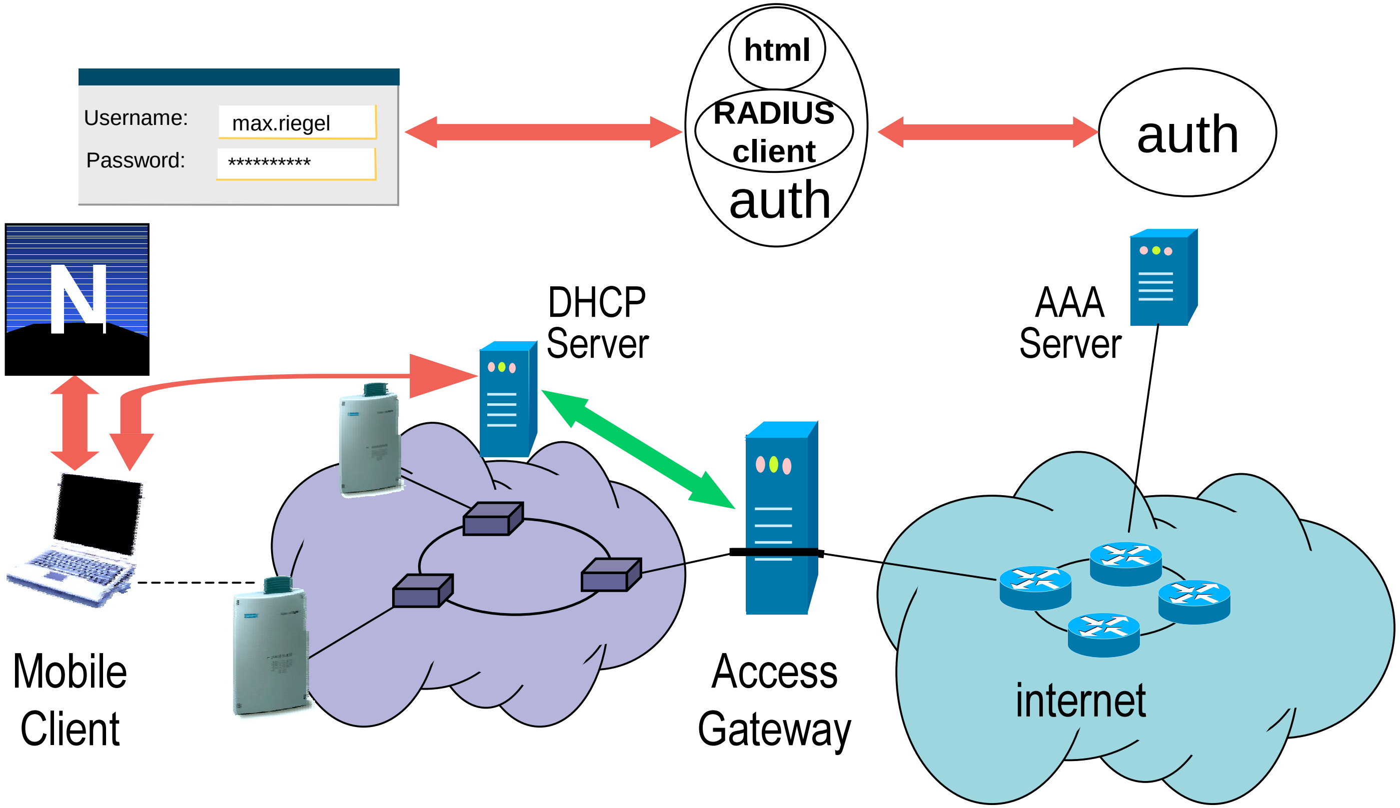
Using a web page for initial user interaction



Free
local content
services

Authentication for Internet access
Selection of billing method

How does it work: Web based access control



Web based access control: Enabler for mCommerce and location based services

SIEMENS mobile

- Puting a mCommerce application into a web-page for WLAN access control enables further services to be billed.

=> there is far more business for the operator than just WLAN access

- Due to its limited coverage services delivered by WLAN in hot-spots can easily tailored to their locations.

=> Operators can start with location based services without huge investments for full geographic coverage.

Functions of an integrated access gateway (User management)

SIEMENS mobile

- **Authentication via secure (HTTPS) web-based GUI for registered and unknown users based on**
  - External database, supports ISP roaming via RADIUS
  - Integrated LDAP directory
  - GSM phone (Transmission of one-time passwords by SMS)
  - Credit card
- **Authorization based on user profiles assigned to different user groups having particular access**
  - Dynamic subscribtion to additional services
  - Personalized portal page
- **Real-time accounting based on service, duration and volume**
  - Instant user feedback on portal page or by SMS

Functions of an integrated access gateway (Network services)

SIEMENS mobile

- **DHCP server for assigning IP addresses to WLAN clients**
  – Retaining session if user is temporarily out of WLAN coverage
  – Detection of session end
- **Policy engine**
  – Loadable user profiles
  – User-specific routing configuration
  – Dynamic firewalling rules
- **IP router with NAT engine**
  – Assignment of private addresses for free services
  – Must allow IPSEC connections

Part 9: WLAN – UMTS Interworking

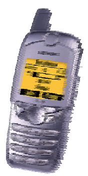
SIEMENS mobile

- UMTS and Wireless LAN are different
- WLAN – UMTS Interworking: Ancient approach: ‚tight coupling‘
- WLAN as an exension of a mobile network
- WLAN is much cheaper than 2G/3G
- Conclusions for Mobile Network Operators
- WLAN – UMTS Interworking: Now widely accepted: ‚loose coupling‘
- WLAN loosely coupled to a Mobile Network
- E.g.: Web based authentication and mobile network security
- Standards for WLAN – UMTS Interworking

UMTS and Wireless LAN are different.

GSM/GPRS/UMTS

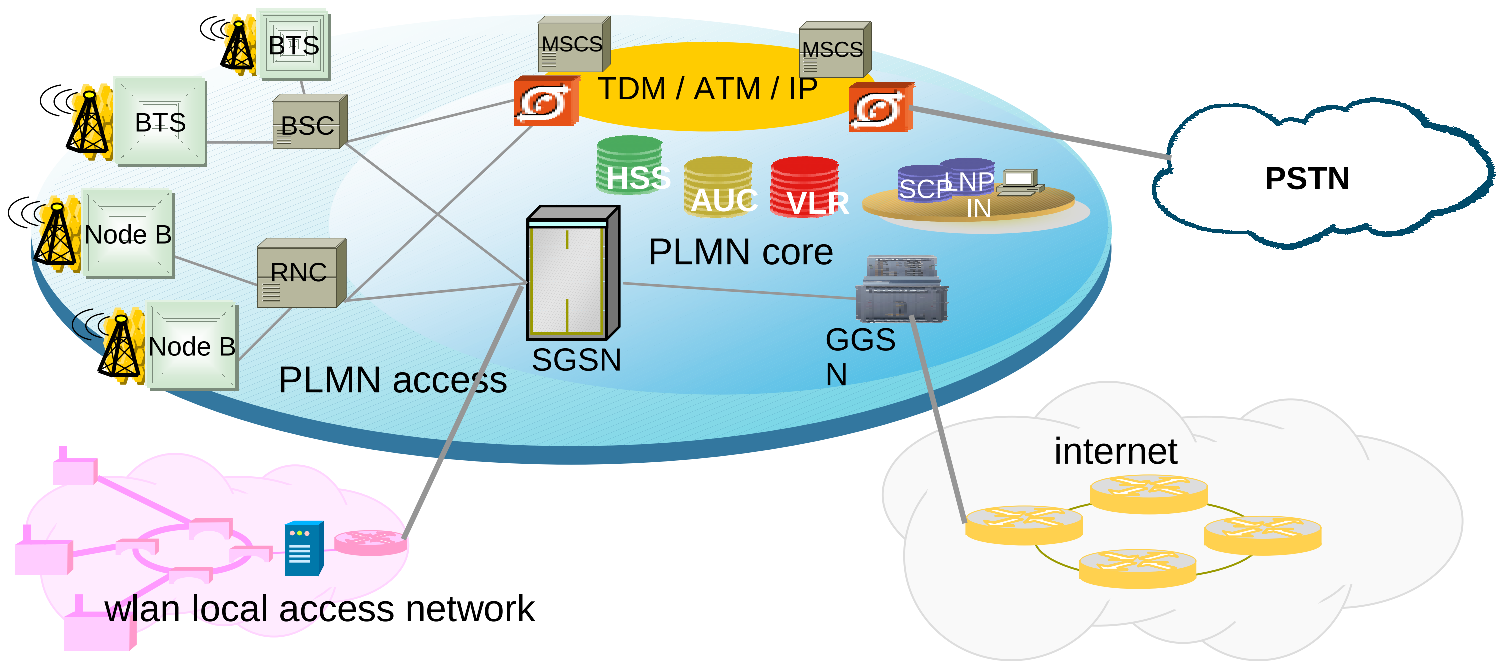
- anytime / everywhere
- voice, realtime messaging
- QoS
- precious bandwidth
- carrier grade
- operator driven
- huge customer base
- high revenues



WLAN IEEE802.11

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

WLAN – UMTS Interworking: Ancient approach: 'tight coupling'



WLAN as just another radio access technology of UMTS

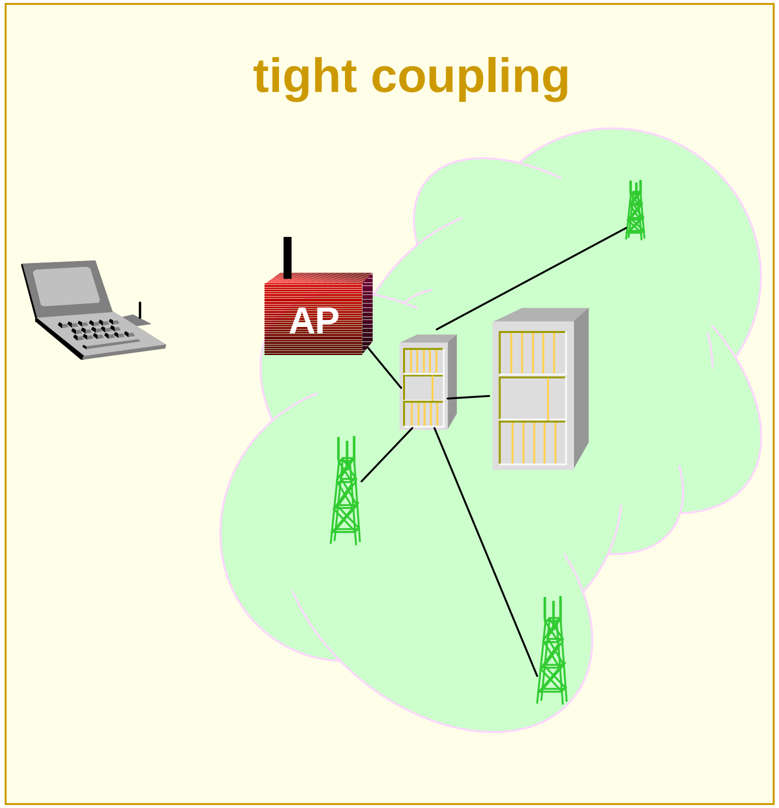
- **All UMTS services become available over WLAN.**

but:

- **PLMN is burdened with high bandwidth WLAN traffic.**
- **Wi-Fi does not provide all the functionality needed (QoS, security).**

WLAN as an extension of a mobile network

SIEMENS mobile

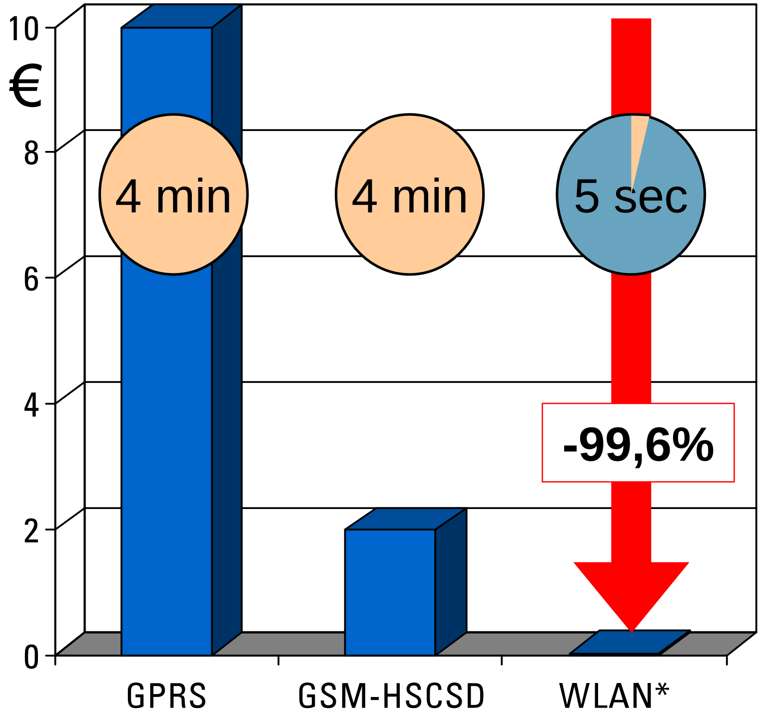


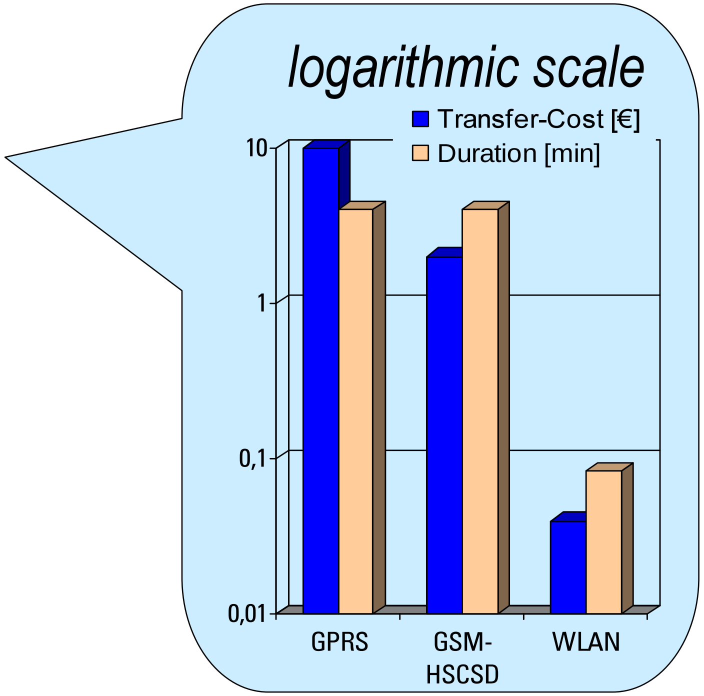
- **WLAN just as another radio access technology**
- **MNOs are the WLAN operators**
  - – OA&M
  - – agreement with siteowner
  - – very dense PLMN
- **Full competition with open ISP market.**
- **Mobile network is carrier of the WLAN traffic.**
- **Dynamics of growth may differ.**
- **very complex**
  - – SIM / USIM cards required
  - – new standards necessary

WLAN is much cheaper than 2G/3G

SIEMENS mobile

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

Conclusions for Mobile Network Operators

SIEMENS mobile

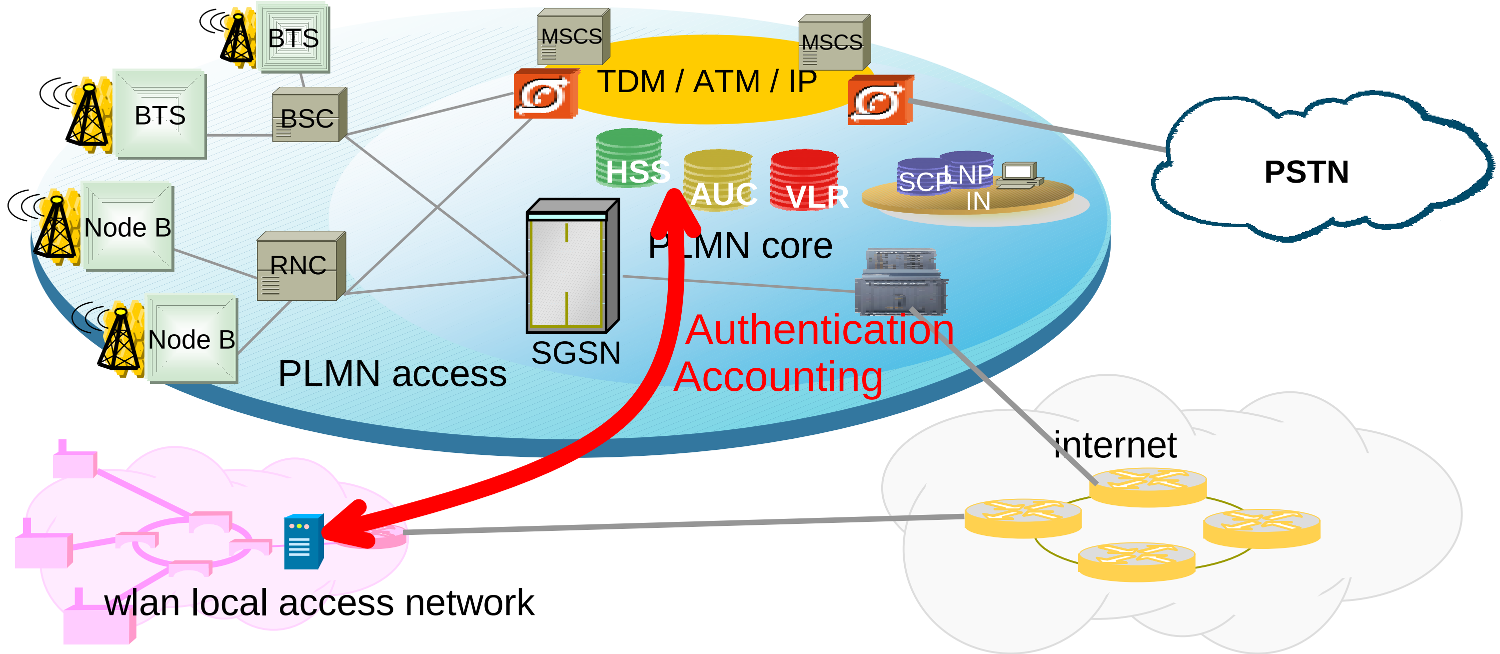
When you can't stop them, when you can't beat them, then you should join them.

- **The most complicated and appealing task of a WLAN operator is charging and billing.**
- **MNOs have large customer bases, secure authentication and accounting facilities and they like to go into mobile business.**
- **Providing electronic payment services to WLAN operators can be an important market entry into mobile business for MNOs.**
- ***There is no time to wait!***
  The WLAN access market is exploding, and WLAN access may be 'for free' in many hot-spots in a few years (~3-5 years).

WLAN – UMTS Interworking:
Now widely accepted: 'loose coupling'

SIEMENS mobile

Siemens contributed ‚loose coupling' to standardization.

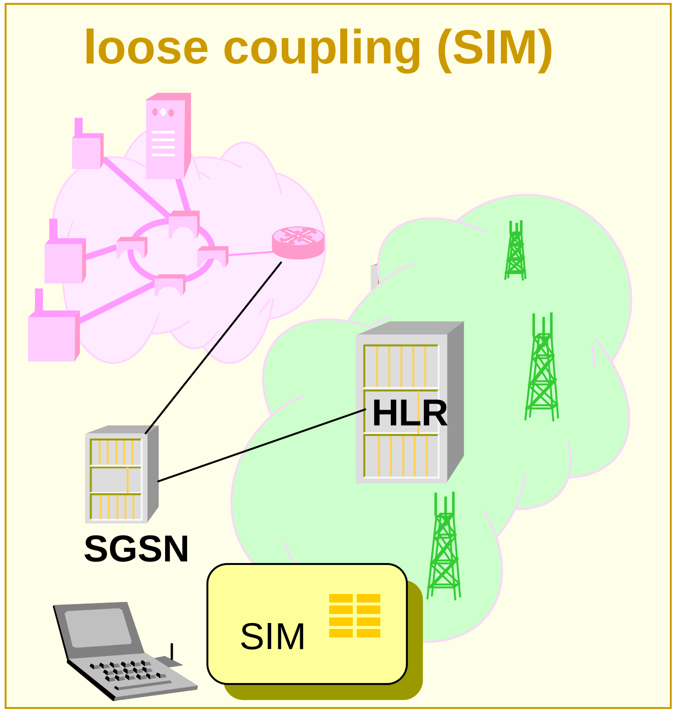


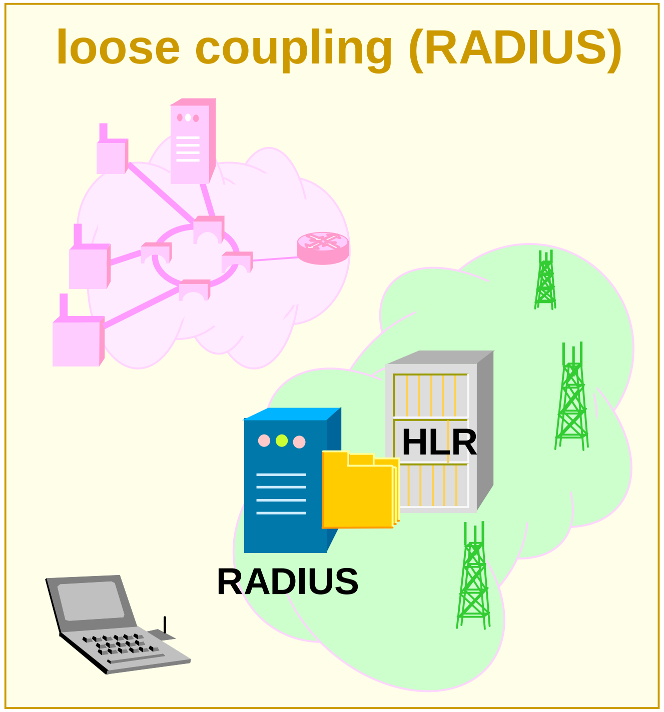
Only Authentication, Authorization and Accounting of WLAN access is performed by the mobile network operator.

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

WLAN loosely coupled to a Mobile Network

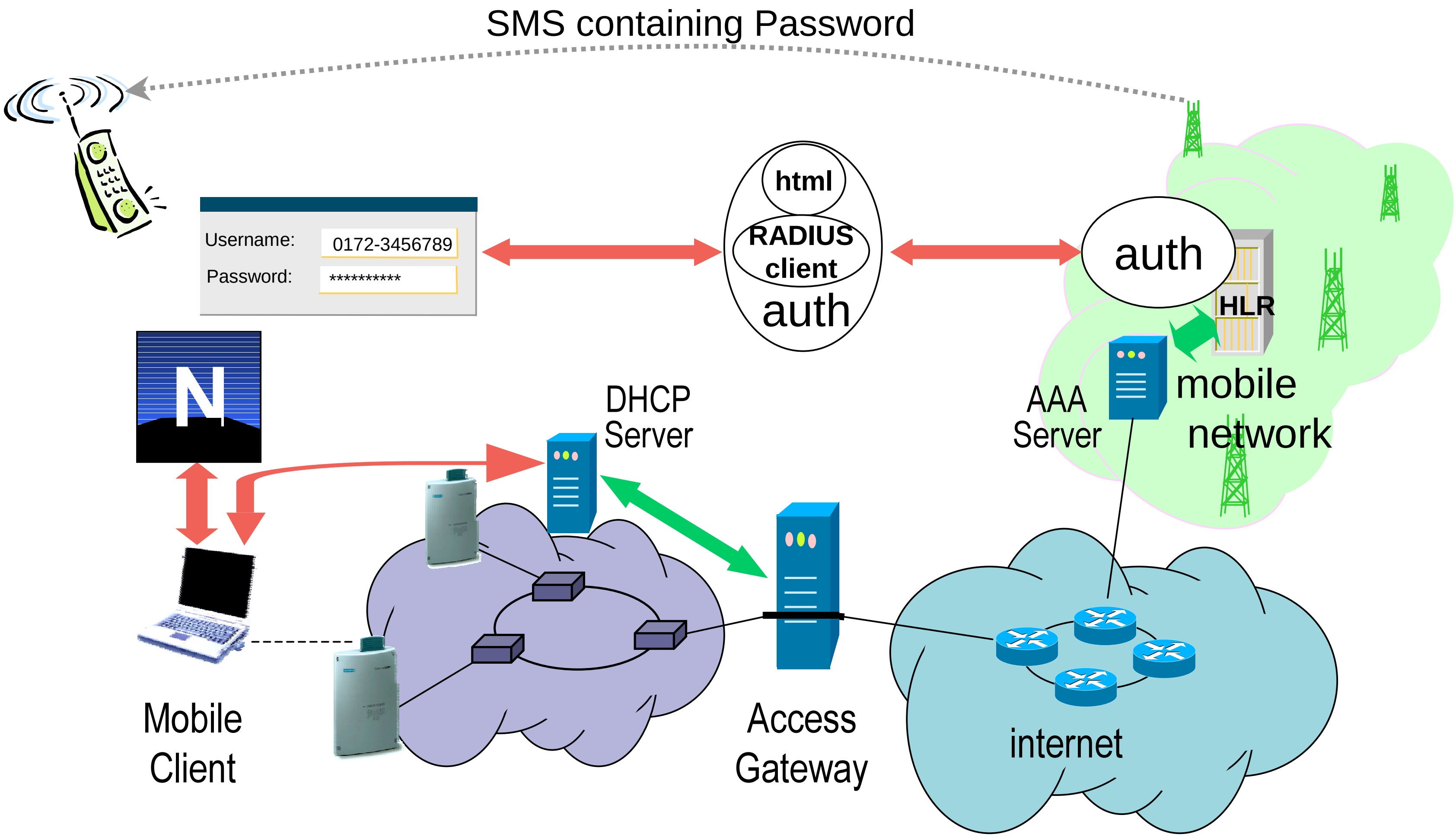
SIEMENS mobile





- **Each hotspot is SS7 endpoint**
  - SIM cards required
  - SGSN or MSC functionality at access network
- **Tight userbase to HLR**
  - Standalone capability
  - Flexibility in security

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 applicable for MNOs.

The end

SIEMENS mobile

- Thank you for your attention.

- Questions and comments?

Maximilian Riegel (maximilian.riegel@icn.siemens.de)

Literature:

- 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

