

## ***Lecture 3***

Wireless Internet-oriented  
Infrastructures and Protocols

**Mobile Business I (WS 2010/11)**

Prof. Dr. Kai Rannenber

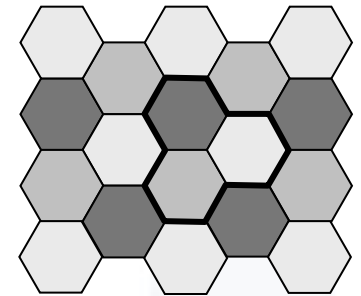
T-Mobile Chair of Mobile Business & Multilateral Security  
Johann Wolfgang Goethe University Frankfurt a. M.



- Wireless LAN
  - Basics
  - Components and Infrastructure
  - Legal Basics
  - Wireless LAN state-of-the art encryption
  - Problems
    - Packet Collision / RTS-CTS Mechanism
    - Wireless LAN Roaming and Mobility
- Mobile IP – Roaming with TCP/IP
- Annex: Wireless Application Protocol (WAP) and Wireless Markup Language (WML)

- Wireless communication based on radio as transport medium
- Cell based architecture
- Possible extension to a (wire based) LAN
- One cell serves a circular area in which PCs, laptops, and other connected devices can move freely.

- The basic module of a Wireless LAN is a so-called radio cell.
- A radio cell covers a circular area that PCs or laptops and other connected devices are able to use.
- A Wireless LAN can be an add-on for already existing cable-based networks.



## ■ Beacon Frame

- The Access Point is transferring a periodical beacon. A beacon communicates the Service Set Identifier (SSID) and other important operational parameters (channel, ...)
- A Wireless LAN client sends a probe request. The Access Point answers with a probe response. If there is an agreement, the Wireless LAN client starts the communication over the Access Point.
- A more detailed description of beacon frames can be found in [Sauter2008].

- Wireless LAN bandwidth depends on the chosen standard, the distance between client and access point, and the construction and quantity of walls.

Bandwidth 802.11b	Outside	Inside (Office)	Inside (House)
11 Mbps	~ 160 m	~ 50 m	< 20 m or max. 1 wall
5.5 Mbps	~ 270 m	~ 70 m	< 30 m or max. 2 walls
2 Mbps	~ 400 m	~ 90 m	< 40 m or max. 3 walls
1 Mbps	~ 550 m	~ 115 m	< 50 m or max. 4 walls

[Lanz2003]

- Germany:** 13 channels with a frequency range from 2399,5 MHz to 2484,5MHz

## ■ Standard IEEE 802.11

Some norms:

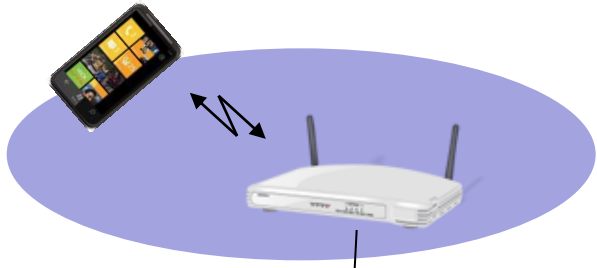
Standard	Description
802.11	Protocol for transmission methods for wireless networks, defined in 1997 for 2 MBit/s at 2,4 GHz
802.11a	Wireless LAN <b>up to 54 MBit/s</b> at 5 GHz
802.11b	Wireless LAN <b>up to 11 MBit/s</b> at 2,4 GHz
802.11f	Roaming between access points of different manufacturers (published in 2003 and withdrawn by IEEE in 2006) [IEEE2010]
802.11g	Wireless LAN <b>up to 54 MBit/s</b> at 2,4 GHz
802.11i	Extended security features: AES, 802.1x, TKIP
802.11n	Wireless LAN <b>up to 600 MBit/s</b> using multiple antennas (Multiple Input Multiple Output = MIMO)
802.11r	Fast Roaming/Fast BSS Transition

- Wireless LAN
  - Basics
  - Components and Infrastructure
  - Legal Basics
  - Wireless LAN state-of-the art encryption
  - Problems
    - Packet Collision / RTS-CTS Mechanism
    - Wireless LAN Roaming and Mobility
- Mobile IP – Roaming with TCP/IP
- Annex: Wireless Application Protocol (WAP) and Wireless Markup Language (WML)

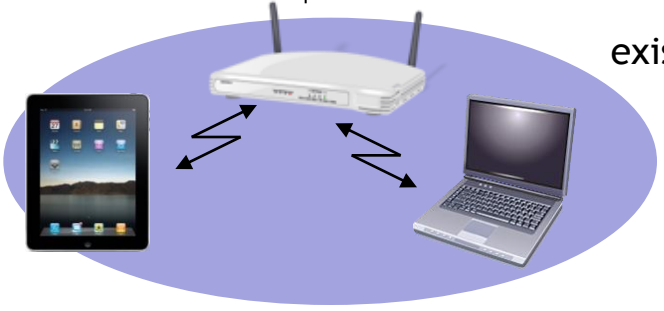
- Components (802.11b)
  - Access Point (AP)  
Sender and receiver station that allows the connecting of multiple receiving stations
  - Stations  
End-systems that establish a wireless connection e.g. by using an Access Point (e.g. a notebook with built-in Wireless LAN)



## Infrastructure Network



## existent cable based Network



## Ad hoc Networks





[Based on Sauter2008]

- Wireless LAN
  - Basics
  - Components and Infrastructure
  - Legal Basics
  - Wireless LAN state-of-the art encryption
  - Problems
    - Packet Collision / RTS-CTS Mechanism
    - Wireless LAN Roaming and Mobility
- Mobile IP – Roaming with TCP/IP
- Annex: Wireless Application Protocol (WAP) and Wireless Markup Language (WML)

- The grey area of the Internet is comparable with the usage of Wireless LAN. The border between legal and illegal is not clearly defined. Most cases the courts decide are precedents.
- What is important?
  - § 202a Strafgesetzbuch  
Spying on data (Ausspähen von Daten)
  - § 88 Telekommunikationsgesetz  
Secrecy of telecommunications (Fernmeldegeheimnis)
  - § 89 Telekommunikationsgesetz  
Ban on eavesdropping (Abhörverbot), receiver operator's confidentiality duty (Geheimhaltungspflicht der Betreiber von Empfangsanlagen)

- Current interpretations of the law permit the following scenarios:
  - By using an ftp-connection a user downloads prototype information about a new car that is unprotected. He prints out this information and pins it to a wall in his flat. As long as no third party can get this information there is no breach of law [Winter2003].

- Wireless LAN
  - Basics
  - Components and Infrastructure
  - Legal Basics
  - Wireless LAN state-of-the art encryption
  - Problems
    - Packet Collision / RTS-CTS Mechanism
    - Wireless LAN Roaming and Mobility
- Mobile IP – Roaming with TCP/IP
- Annex: Wireless Application Protocol (WAP) and Wireless Markup Language (WML)

- There are numerous methods for Wireless LAN encryption.
- We are only looking at methods that use a pre-shared key (PSK).
- Most encryption methods are outdated and hence insecure:
  - Wired Equivalent Privacy (WEP) 64-bit 
  - Wired Equivalent Privacy (WEP) 128-bit 
- WEP 128-bit can be by-passed within minutes [Heise 2007].



- **Wi-Fi Protected Access** was developed by the Wi-Fi Alliance [Wi-Fi 2010]



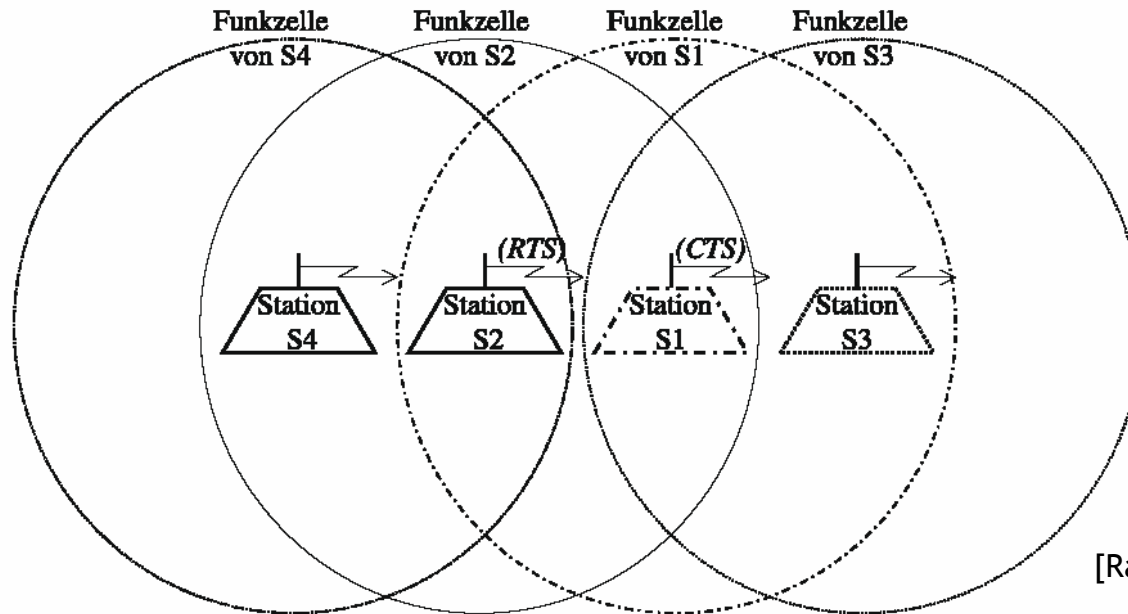
- There are two versions of **Wi-Fi Protected Access**, WPA and WPA2:
  - **WPA** includes most of the 802.11i standard.
  - **WPA2** includes 802.11i to full extent and also the Advanced Encryption Standard (AES).

- Wireless LAN
  - Basics
  - Components and Infrastructure
  - Legal Basics
  - Wireless LAN state-of-the art encryption
  - Problems
    - Packet Collision / RTS-CTS Mechanism
    - Wireless LAN Roaming and Mobility
- Mobile IP – Roaming with TCP/IP
- Annex: Wireless Application Protocol (WAP) and Wireless Markup Language (WML)

- Description of problem and solution for **Packet Collision**

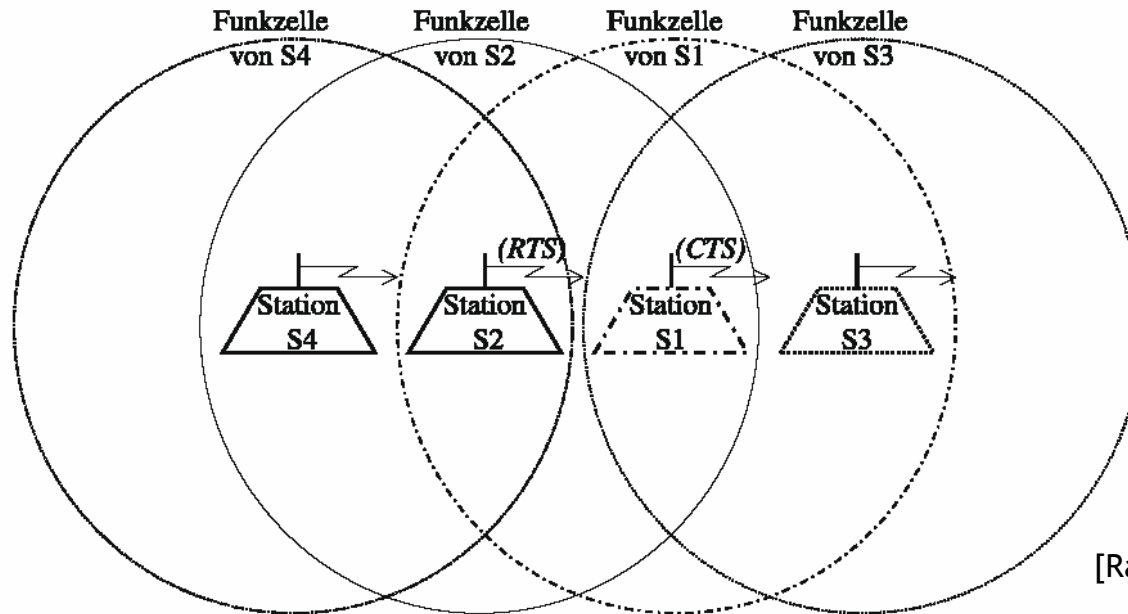
RTS-CTS (Request to send - Clear to send)

- Wireless LAN uses “Air” as medium
- There is no CSMA/CD (Carrier Sense Multiple Access / Collision Detection) available for Wireless LAN.
- CSMA/CA (Carrier Sense Multiple Access / Collision Avoidance) is possible.
- The following figure shows typical problems in air transmission systems.



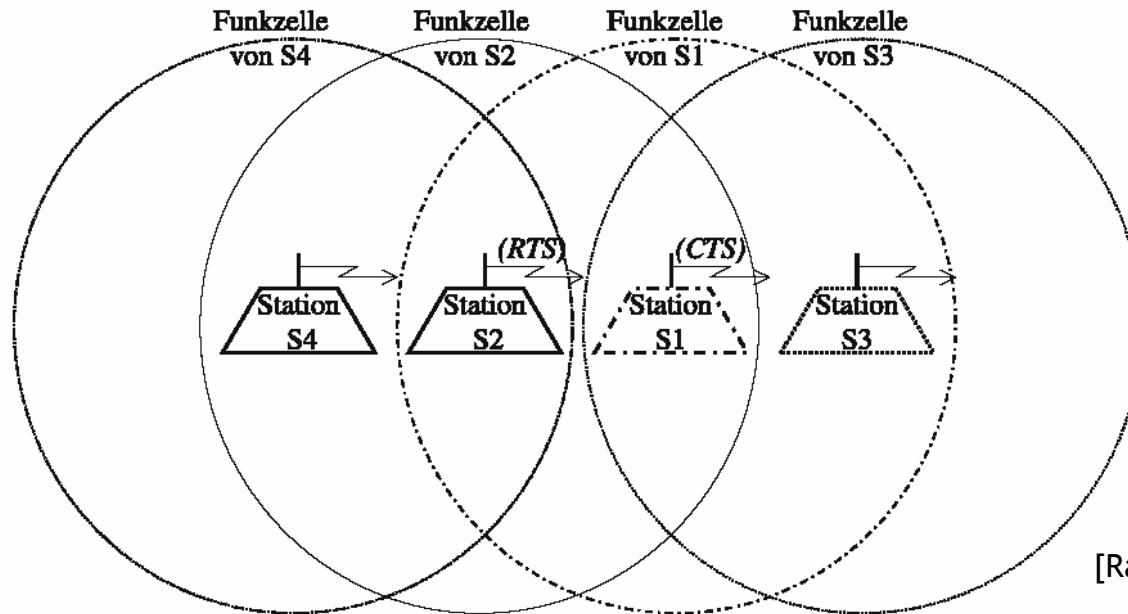
[Radmacher2004]

- Hidden station problem (S2 and S3)
- S2 can't hear S3 and the other way round.
- Starting a communication by both of them leads to a collision at S1



[Radmacher2004]

- **Solution:** before communication, S2 sends an RTS-frame to S1
  - If there is no other communication a CTS-frame is the response and the communication starts.
  - If there is a communication, no CTS-frame is sent, S2 follows a back-up strategy.

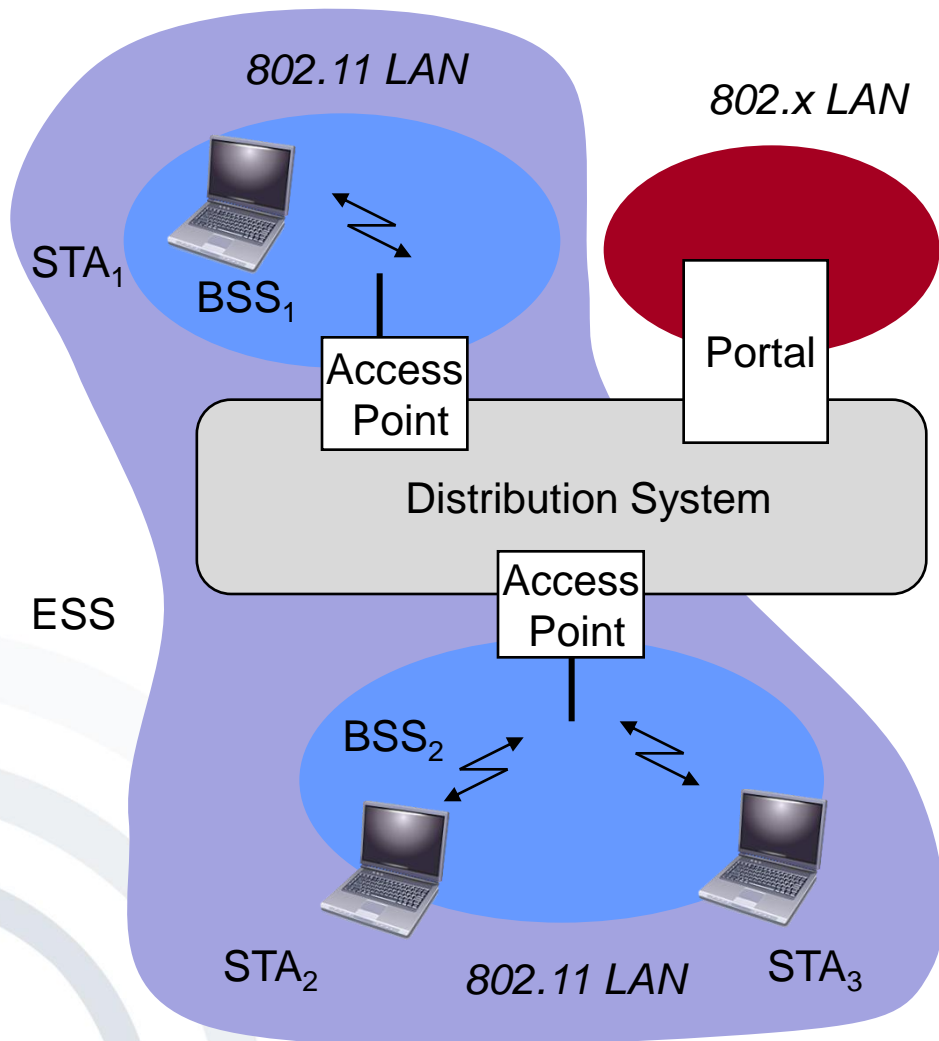


[Radmacher2004]

- After some time, based on the back-up strategy, S2 starts again sending a new RTS-frame.
- Without a CTS-frame there is no beginning of a communication.

- Back-up strategy
  - Communication attempt failed
  - After a time-interval based on a special algorithm the sender tries again to send a RTS-frame.

- Wireless LAN
  - Basics
  - Components and Infrastructure
  - Legal Basics
  - Wireless LAN state-of-the art encryption
  - Problems
    - Packet Collision / RTS-CTS Mechanism
    - Wireless LAN Roaming and Mobility
- Mobile IP – Roaming with TCP/IP
- Annex: Wireless Application Protocol (WAP) and Wireless Markup Language (WML)



## Station (STA)

- Computer with access to the wireless medium and radio
- Contact to the AP

## Basic Service Set (BSS)

- Group of stations, which use the same radio frequency

## Access Point

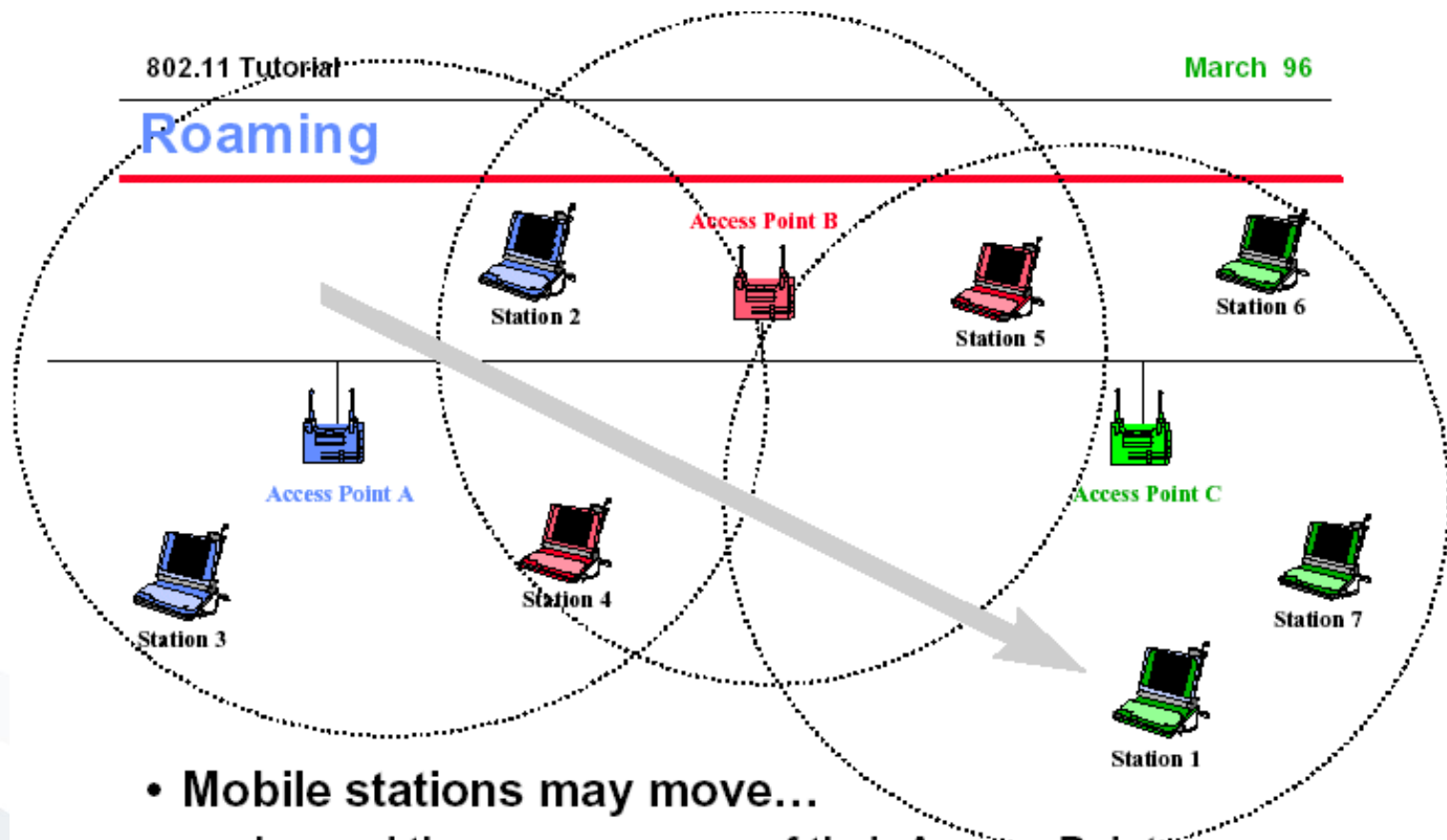
- Station which is integrated into the radio as well as the fixed local area network (distribution system)

## Portal

- Transfer into another network

## Distribution systems

- Connection of different cells for building up a larger network (EES: Extended Service Set)



- Mobile stations may move...
  - beyond the coverage area of their Access Point
  - but within range of another Access Point
- Reassociation allows station to continue operation

- Approaches to perform roaming
  - By a combination of several Access Points a so-called distribution system is growing.
  - Every Access Point covers one radio cell.
  - Upon leaving a radio cell the station starts scanning for other existing Access Point and tries to connect.
  - Following the connection to a new Access Point the distribution system and the Access Point that was used before will be informed.

- **BSS = Basic Service Set.**  
*A Basic Service Set (BSS) is one Wireless LAN access point + all associated stations.*
- The client decides which access point to (re)connect to in case the connection to the previous access point is lost (e.g. due to the client moving out of range)
- Wireless security protocols induce interruptions of several seconds during necessary reconnection (problem when using Voice-over-IP telephony connections!)
- Since 2008 a standard for roaming between Wireless LAN access points is available:  
IEEE 802.11r = fast roaming and fast BSS transition

- Wireless LAN
  - Basics
  - Components and Infrastructure
  - Legal Basics
  - Wireless LAN state-of-the art encryption
  - Problems
    - Packet Collision / RTS-CTS Mechanism
    - Roaming and Mobility
- Mobile IP – Roaming with TCP/IP
- Annex: Wireless Application Protocol (WAP) and Wireless Markup Language (WML)

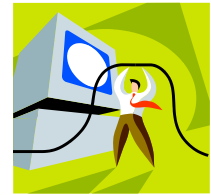
The situation today:

- Separate IP addresses in the office and at home
- DHCP - dynamic IP address assignment
- Dial-up with dynamic IP addresses
  - Continuous accessibility via one IP address is not guaranteed.
  - Connection interruptions during access point switches

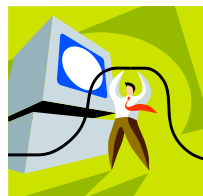
## Routing in TCP/IP



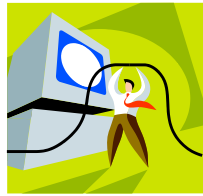
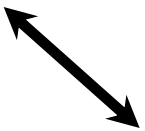
Partner B  
IP address, e.g.  
61.9.193.200



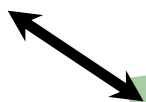
Router



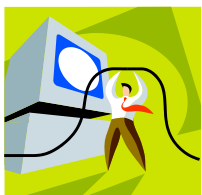
Router



Router



Partner A  
IP address,  
e.g. 141.2.74.211



Router

- Routing takes place from Partner A node to Partner B node and in reverse direction.
- Both nodes have their own address.
- The route follows the addresses.
- Routing of data packets by routers

## Standards

- Internet Engineering Task Force (IETF)

[www.ietf.org](http://www.ietf.org)

- RFC 2002: IP Mobility Support
- RFC 2977: Mobile IP Authentication, Authorization, and Accounting Requirements

## Roaming problem

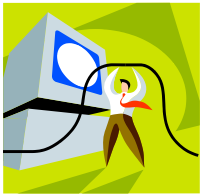


Partner B changes network

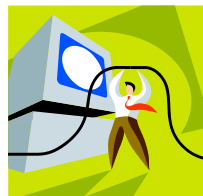


Old IP address (Partner B)

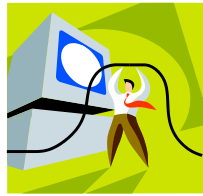
New IP address (Partner B)



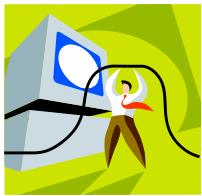
Router



Router



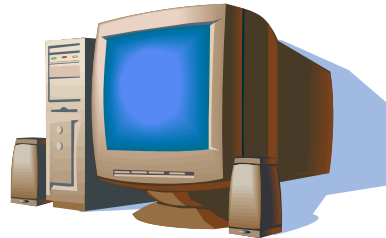
Router



Router



Partner A

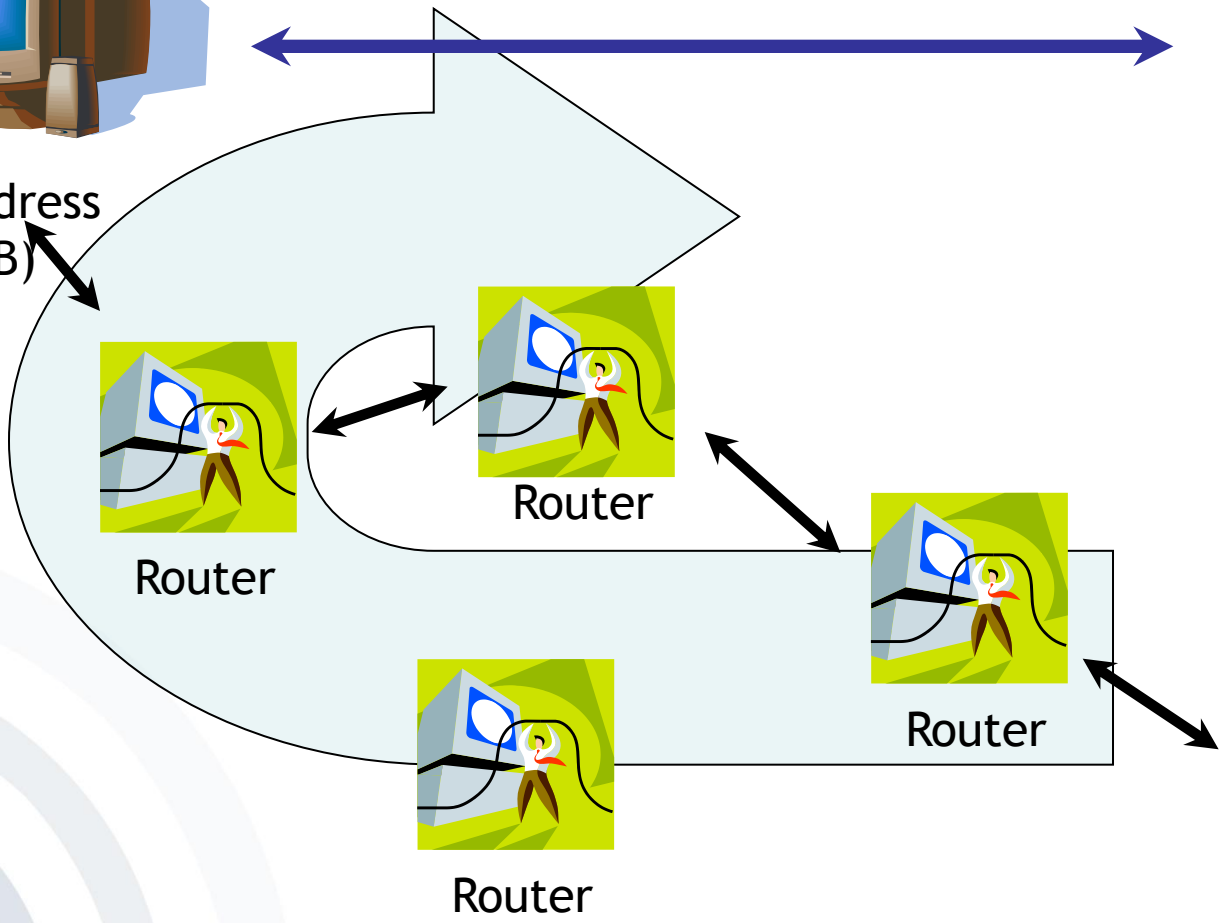


Redirection ("Tunneling") via home address to mobile device



New IP address (Partner B)

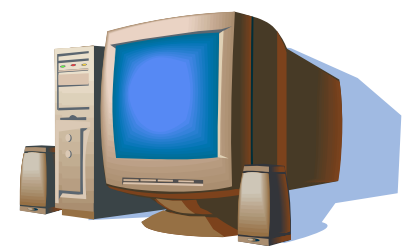
Home address (Partner B)



Partner A

- **But redirection implies**
  - A longer route than before
  - Higher runtime
  - Avoidable usage of resources

## Roaming solution Binding Update



Redirection of the first package  
via home address  
to the mobile device

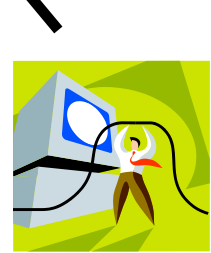


New  
IP address  
(Partner B)

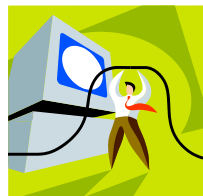
Home address  
(Partner B)

New route  
with remaining  
packets

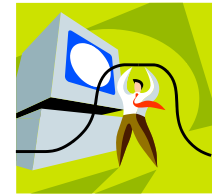
Binding  
Update  
1st packet



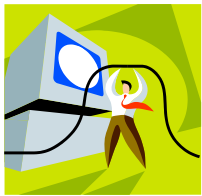
Router



Router



Router



Router



Partner A

- Possible attack with illegitimate binding update: **Capture the route** and redirect the TCP/IP session.
  - ➔ Therefore, authentication of Binding Update (BU) messages and address check is required.
- In addition, **observation** of user movements through their Binding Updates!
  - ➔ Anonymous communication-channels are necessary to protect privacy.

- In the **Domain Name Service** a domain-name belongs to a fixed IP address (e.g. `www.m-lehrstuhl.de = 141.2.66.180`).
  - **Changing** these addresses requires an update-time of several hours ➔ this is no usable solution.
- **Better solution: Dynamic DNS**
  - Modification time: 15 minutes
  - Problem: applications resolve a name just once and do not query possible address changes thereafter.

- Wireless LAN
  - Basics
  - Components and Infrastructure
  - Legal Basics
  - Wireless LAN state-of-the art encryption
  - Problems
    - Packet Collision / RTS-CTS Mechanism
    - Roaming and Mobility
- Mobile IP – Roaming with TCP/IP
- Annex: Wireless Application Protocol (WAP) and Wireless Markup Language (WML)



## Wireless Application Protocol (WAP)

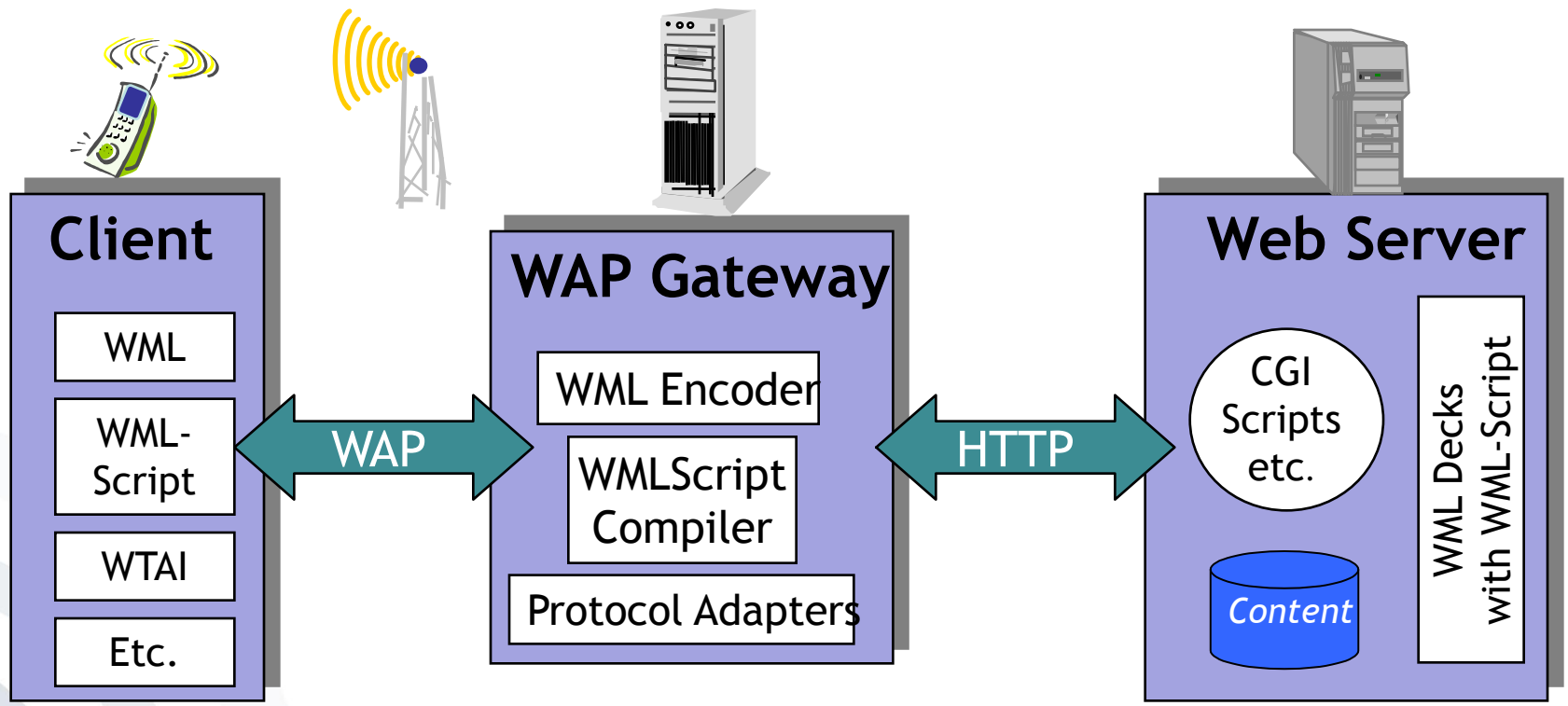
- In 1997, Ericsson, Motorola, Nokia and Unwired Planet founded the WAP Forum.
- The WAP Forum is a nonprofit-organization with the objective to build up an open standard (protocol) for wireless data-communication.
- More than 300 members worldwide (Manufacturers, software industry, computer and telecommunication companies & network-operators)

- Protocol-family, developed by the WAP forum to provide internet contents on mobile devices
- Universal use, independent from used network technology (GSM, UMTS, etc.)

- **Objectives**

- Interoperability (support of devices from different manufacturers)
- Scalability (services have to be extendable on demand)
- Efficiency (quality of services should be as good as possible in wireless networks)
- Reliability (consistent & predictable platform)
- Security (Protection of integrity & confidentiality)

- Application environment: WAP Gateway



ANNEX



**WTLS**

Connection is secure only to the WAP gateway



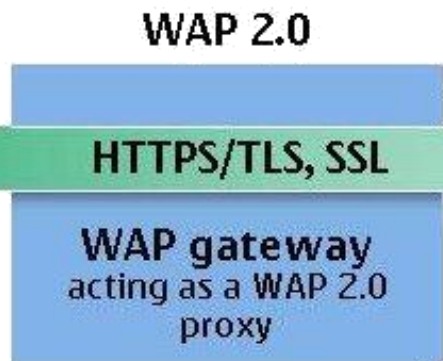
The whole end-to-end security cannot be assured due to the security gap in the gateway

**SSL**

Secure as such but data may have been manipulated or read in the gateway



**HTTPS/TLS, SSL**



Security is comparable to the Internet model – transaction all the way to the origin server will be secure



ANNEX



wap.bahn.de



pda.bahn.de

- **Wireless Markup Language (WML)**
  - Markup language used to define contents which are transmitted via WAP
  - Specified in 1998 by W3C as XML-document type
  - **Challenges:**
    - Attributes of mobile devices
    - Bandwidth of mobile networks

- Small language (in comparison with HTML) to manipulate the display.
- Segmentation of WML documents in cards & decks (n:1)
- Navigation between Cards inside a WML document
- Navigation between Decks by opening a new WML document

## ■ Demo



```
<?xml version="1.0"?>
<!DOCTYPE wml PUBLIC "-//WAPFORUM//DTD
WML 1.2//EN" "http://www.wapforum.org/DTD/
wml_1.2.xml">
<wml>
<head>
  <meta name="Author" content="Jan Muntermann"/>
  <meta name="Description" content="IWI Home"/>
</head>
<card id="startPage">
  <p align="center">
    <img src='images/iwi.wbmp' alt='Body' />
  </p>
  <p align="center">
    Institut für Wirtschaftsinformatik<br/>
    <small>WAP-Demopage</small><br/>
    &#187;<a href="navigate.asp">weiter</a>&#171;<br/>
  </p>
</card>
</wml>
```

- [Heise 2007] Heise Online: WEP-Verschlüsselung von WLANs in unter einer Minute geknackt (04.04.2007), accessed 2010-10-10.
- [IEEE] IEEE, <http://grouper.ieee.org/groups/802/11/>, accessed 2010-10-10.
- [IEEE1996] IEEE (1996), 802.11 Tutorial - MAC Entity, 1996, <http://grouper.ieee.org/groups/802/11/Tutorial/MAC.pdf#>; accessed 2005-03-01
- [IEEE2010] OFFICIAL IEEE 802.11 WORKING GROUP PROJECT TIMELINES [http://grouper.ieee.org/groups/802/11/Reports/802.11\\_Timelines.htm](http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm), accessed 2010-10-10.
- [Lanz2003] Lanz, R. (2003) „Wireless Local Area Network“, Berner Fachhochschule, Hochschule für Technik und Architektur
- [Radmacher2004] Radmacher, M. (2004), "Sicherheits- und Schwachstellenanalyse entlang des Wireless-LAN-Protokollstacks“, Universität Duisburg-Essen, p. 116
- [Sauter2008] Sauter, M. (2008): Grundkurs Mobile Kommunikationssysteme (3., erweiterte Auflage), Vieweg, Wiesbaden.
- [Winter2003] Winter M.-A. (2003) „WLAN: Kostenlos durch Sicherheitslücken surfen“, [www.teletarif.de/arch/2003/kw06/s9809.html](http://www.teletarif.de/arch/2003/kw06/s9809.html), accessed 2003-05-04
- [Wi-Fi 2010] The Wi-Fi Alliance, <http://www.wi-fi.org>, accessed 2010-10-10.