# mobile business

## *Lecture 3*

### Wireless Internet-oriented Infrastructures and Protocols

**Mobile Business I (WS 2016/17)**

Prof. Dr. Kai Rannenberg

Deutsche Telekom Chair of Mobile Business & Multilateral Security
Johann Wolfgang Goethe University Frankfurt a. M.

**mobile business**

- **Wireless LAN**
  - Basics
  - Components and Infrastructures
  - State-of-the art Encryption
  - Mobility and Roaming
- Mobile IP – Mobility support for TCP/IP
- IP-based Radio Access Networks

- Wireless communication based on radio as transport medium

- Cell based architecture

- Extension to a (wire based) LAN

- One cell serves an area in which PCs, laptops, and other connected devices can move freely.

- The term "Wi-Fi" is
  - used in general English as synonym for a Wireless Local Area Network (WLAN),
  - a trademark owned by the *Wi-Fi Alliance*, a trade association promoting Wi-Fi technology.

- 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 WLAN radio cell can be an add-on for already existing cable-based networks.
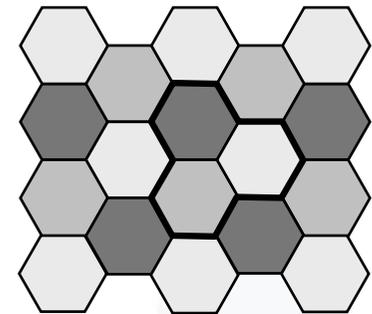
- The Access Point is transferring a periodical beacon. A beacon communicates the Service Set Identifier (SSID) and other important operational parameters (channel, …)

- 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].

| 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 **up to 54 MBit/s** at 5 GHz |
| 802.11b | Wireless LAN **up to 11 MBit/s** 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| 802.11f | Roaming between access points of different manufacturers (published in 2003 and withdrawn by IEEE in 2006) [IEEE2010] |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 **up to 54 MBit/s** at 2,4 GHz |
| 802.11i | Extended security features: AES, 802.1x, TKIP |
| 802.11n | Wireless LAN **up to 450 MBit/s** when using 3 spatial streams (3x 150 Mbit/s) at 2,4 GHz or 5 GHz *) |
| 802.11r | Fast Roaming/Fast BSS Transition |
| 802.11ac | Wireless LAN using 3 spatial streams at 5 GHz: **Up to 1.3 GBit/s** (3x 433 Mbit/s) or even **up to 2.6 GBit/s** (3x 867 Mbit/s, part of *802.11ac Wave2*)  *) **) |
| 802.11ad | Wireless LAN at 60GHz: **Up to 7GBit/s** |
| 802.11ah | Wi-Fi HaLow for Smart Home and connected devices (900 MHz,increased distance, ~1km) |

*) 802.11n and 802.11ac data rates depend on the number of antennas and spatial streams ("parallele räumliche Inhaltsströme")
supported by the hardware. 802.11ac devices often support 3 streams at most. 802.11n specifies a maximum of 4 streams,
802.11ac a maximum of 8 streams.

**) 802.11ac is a 5 GHz-only standard, so dual-band access points and clients will probably continue to use 802.11n at 2.4 GHz in parallel.

[IEEE]  [Sauter 2008]

- 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 |

[Lanz 2003]

- **802.11b** uses the **2.4 GHz frequency band.** Reach depends even more on local circumstances when using newer IEEE standards together with **5 GHz frequency band.**

**Wireless Internet-oriented Infrastructures & Protocols**

- # Wireless LAN
  - Basics
  - Components and Infrastructures
  - State-of-the art Encryption
  - Mobility and Roaming

- # Mobile IP – Mobility support for TCP/IP

- # IP-based Radio Access Networks

# Wireless LAN Components

- Components (802.11b)
    - Access Point (AP)

        Sender and receiver station that allows the connecting of many 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)
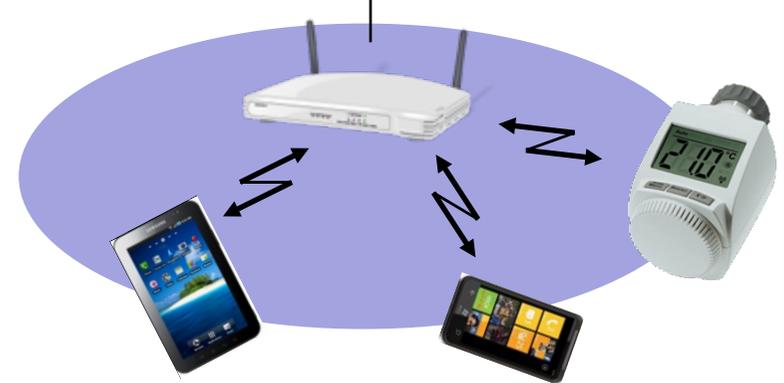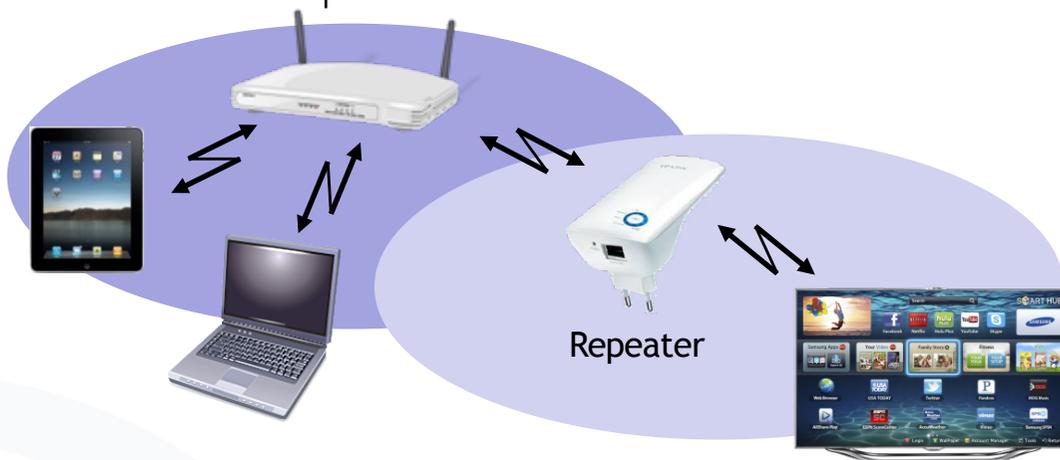
# Wireless LAN Infrastructures

Infrastructure Network

Access Point

Existing cable based Network

Repeater

Ad hoc Networks

Wireless Internet-oriented Infrastructures & Protocols

- ## Wireless LAN
    - Basics
    - Components and Infrastructures
    - State-of-the art Encryption
    - Mobility and Roaming

- ## Mobile IP – Mobility support for TCP/IP

- ## IP-based Radio Access Networks

- There are numerous methods for Wireless LAN encryption.

- We are only looking at methods that use a pre-shared key (PSK).

- WEP encryption methods are outdated and hence insecure:
  - Wired Equivalent Privacy (WEP) 64-bit
  - Wired Equivalent Privacy (WEP) 128-bit

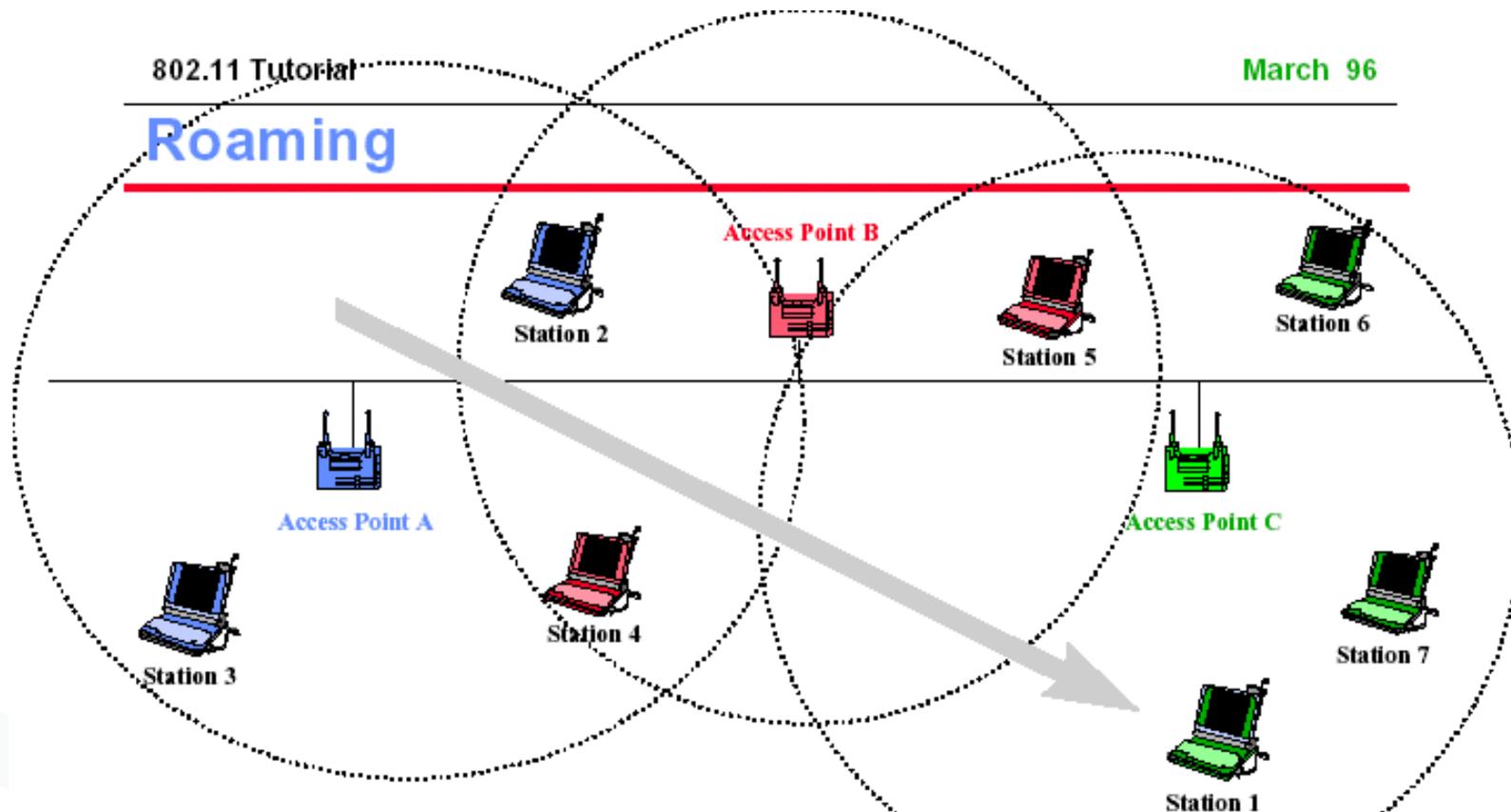- WEP 128-bit can be by-passed within minutes. [Heise 2007]

- **Wi-Fi Protected Access (WPA)** 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, but is **outdated and insecure** as it has various weaknesses:
    - Vulnerability to dictionary attacks when using a weak PSK
    - Other weaknesses inherited from earlier standards [ArsT 2008]

  - **WPA2** includes **802.11i** to its full extent and also the Advanced Encryption Standard (AES).

Wireless Internet-oriented Infrastructures & Protocols

- # Wireless LAN
  - Basics
  - Components and Infrastructures
  - State-of-the art Encryption
  - Mobility and Roaming
- # Mobile IP – Mobility support for TCP/IP
- # IP-based Radio Access Networks

- No existing standard for "handover" or "roaming" between:
  - Access points (AP)
  - Different providers of APs

- Change of AP leads to
  - Connection interrupt
  - New connection/authentication

- Non-uniform accounting / user administration

→ Some of the reasons why WLAN will not replace mobile communication networks

802.11 Tutorial

March 96

## Roaming

Access Point B

Station 2

Station 5

Station 6

Access Point A

Access Point C

Station 3

Station 4

Station 7

Station 1

- **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**

[IEEE 1996]

16

- **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 points (which may use the same SSID, but a different transmission channel) 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.

# Wireless LAN "Roaming"
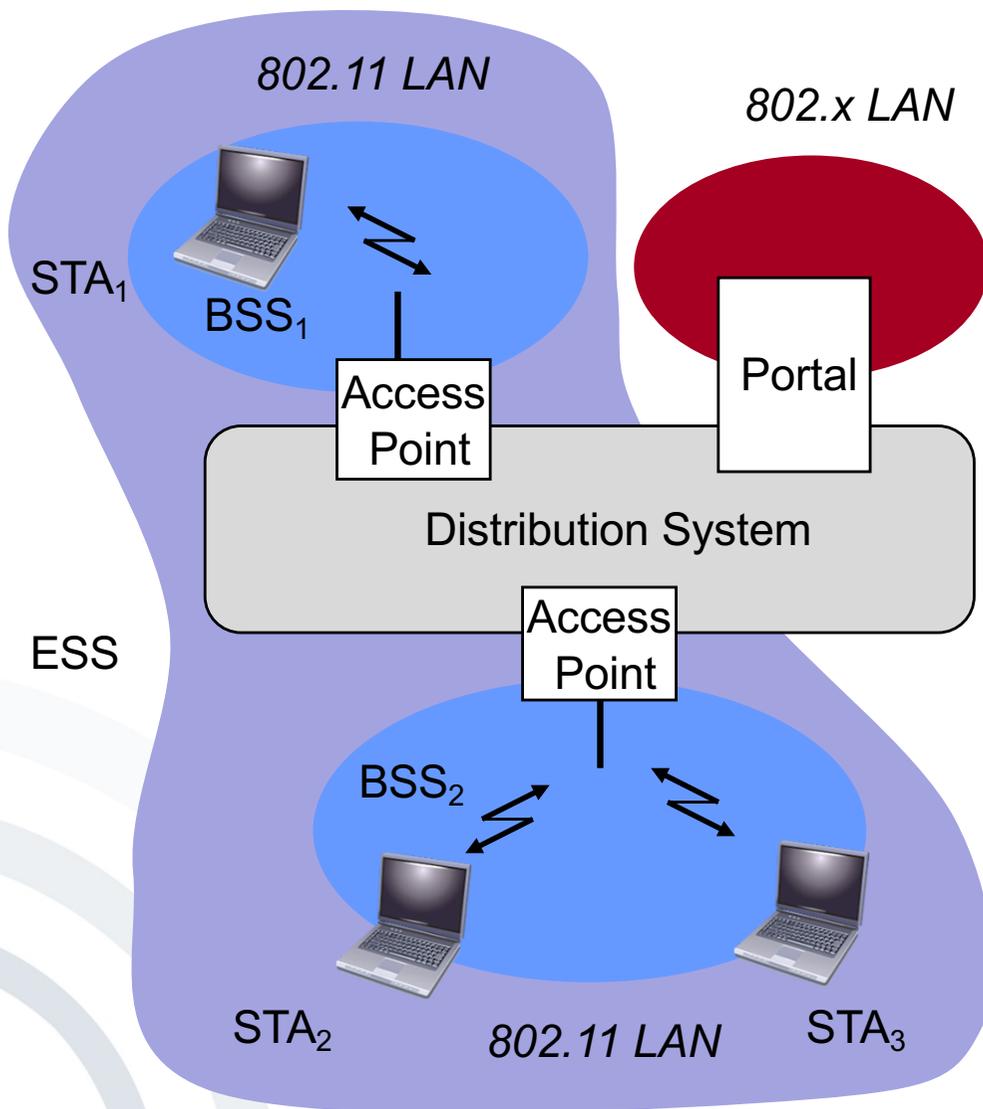


**Station (STA)**
- Computer with access to the wireless medium and radio connect to the AP

**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 a larger network (ESS: Extended Service Set)

- **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

  - As of February 2013, no Intel devices support the 802.11r standard. [Intel 2013]
  - For Apple devices iOS 6 introduced support for 802.11r (optimized client roaming on enterprise Wi-Fi networks). [Apple 2012]

Wireless Internet-oriented Infrastructures & Protocols

- ## Wireless LAN
  - Basics
  - Components and Infrastructures
  - State-of-the art Encryption
  - Mobility and Roaming
- ## Mobile IP – Mobility support for TCP/IP

- ## IP-based Radio Access Networks

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 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

**mobile business**

Partner B
IP address, e.g.
61.9.193.200

Router

Router

Router
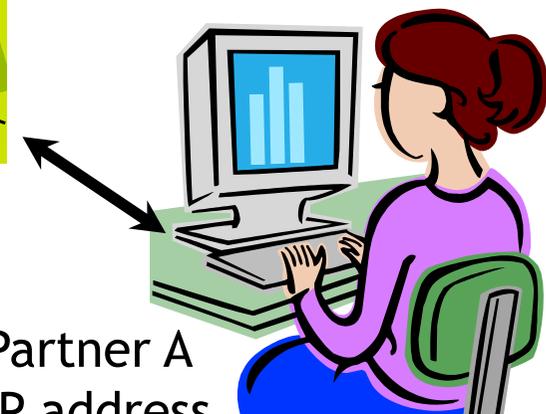
Router

Partner A
IP address,
e.g. 141.2.74.211

22

## Standards

- Internet Engineering Task Force (IETF)
  www.ietf.org

- RFC 2002: IP Mobility Support

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

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

Home address
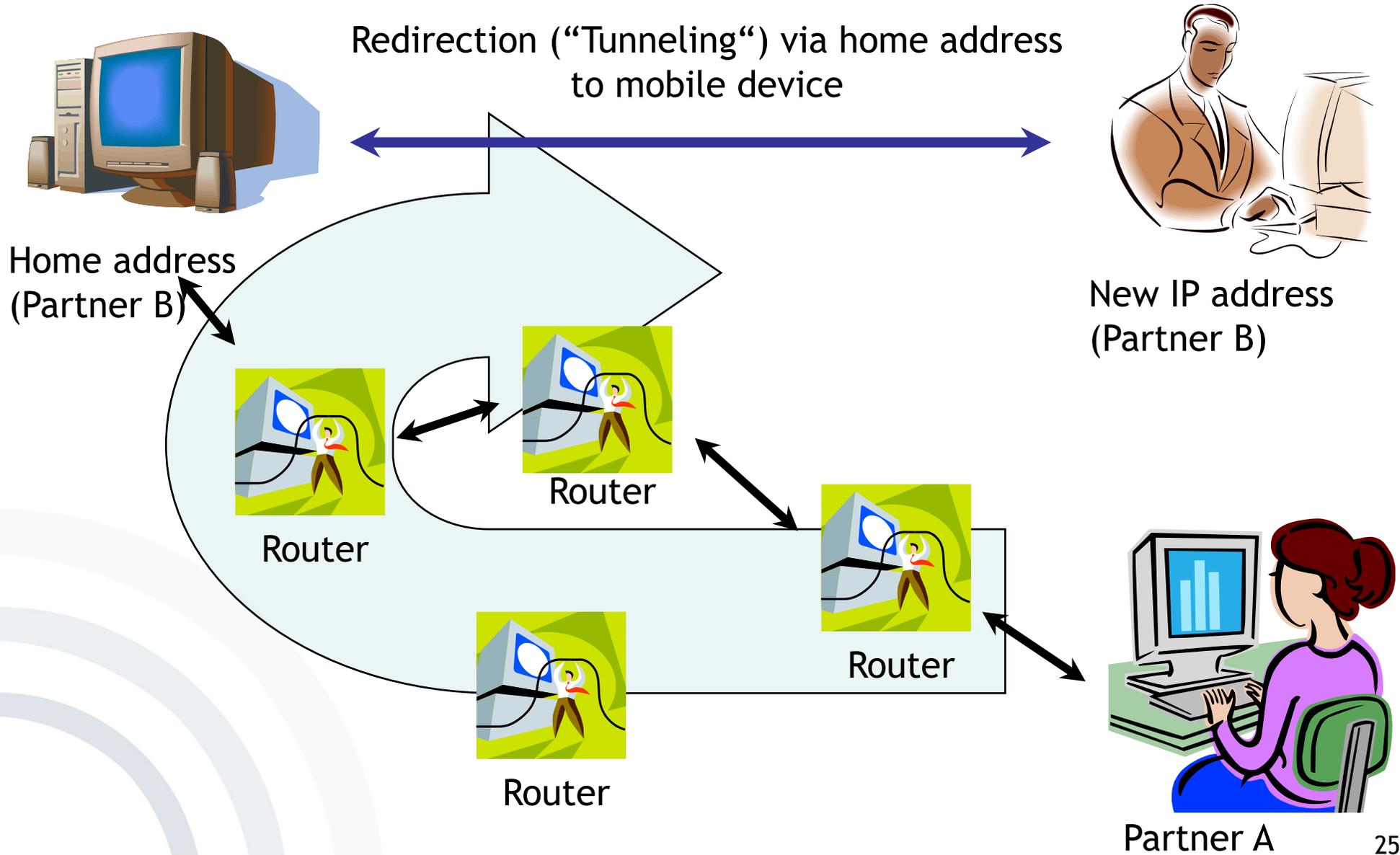(Partner B)

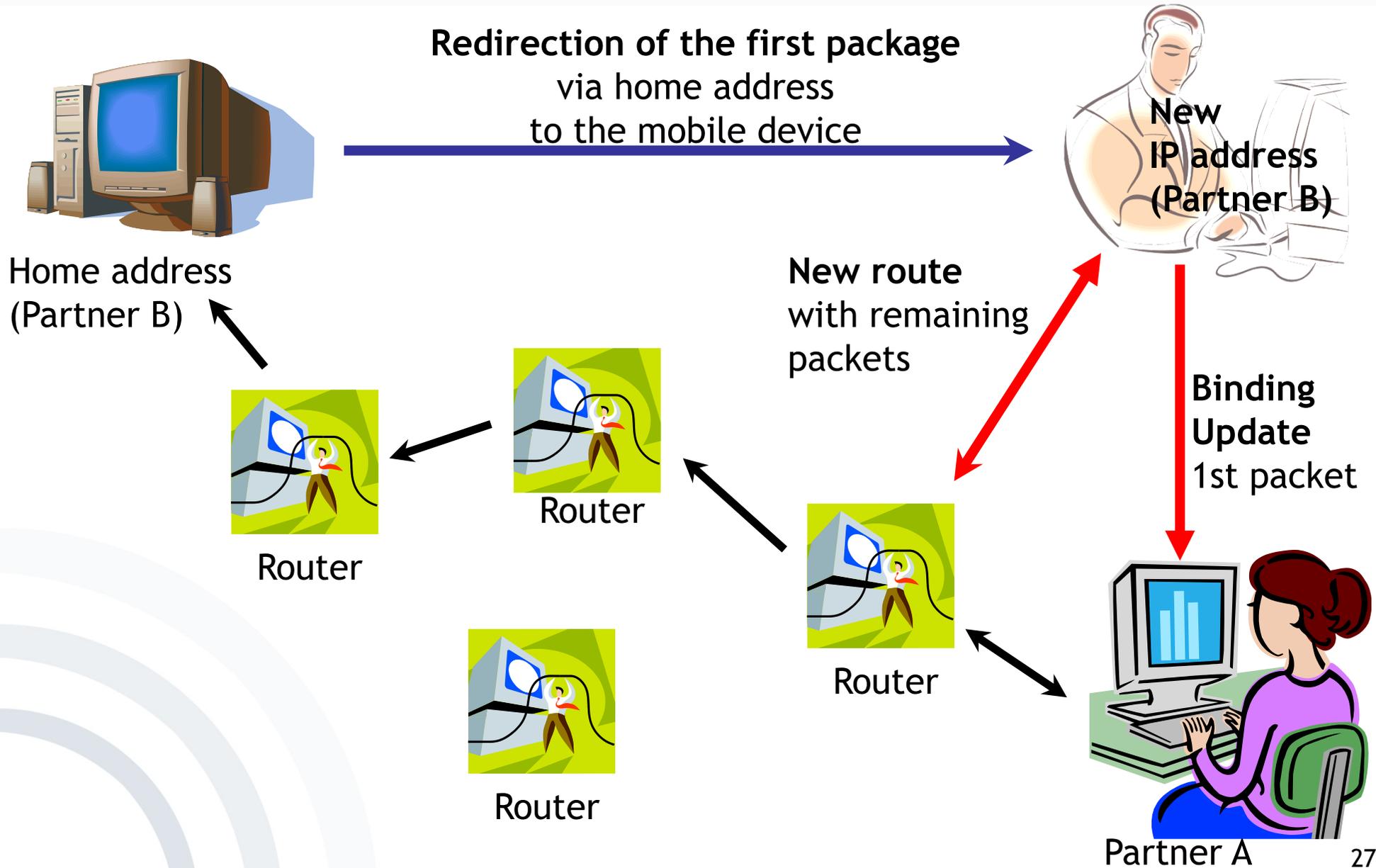New IP address
(Partner B)

Router

Router

Router

Router

Partner A

25
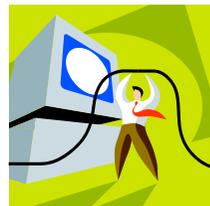
- **But** redirection implies

  - A longer route than before
  - Higher runtime
  - Avoidable usage of resources

# Mobility 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

27

- 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 System** 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.
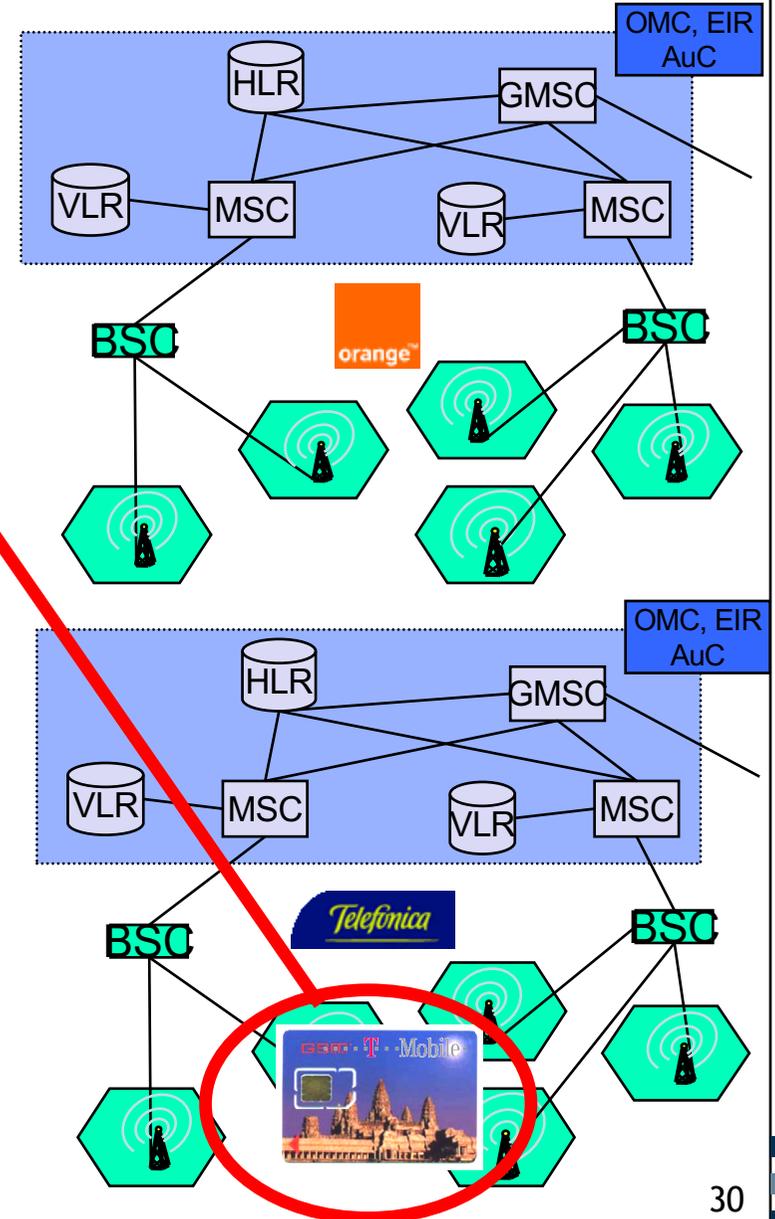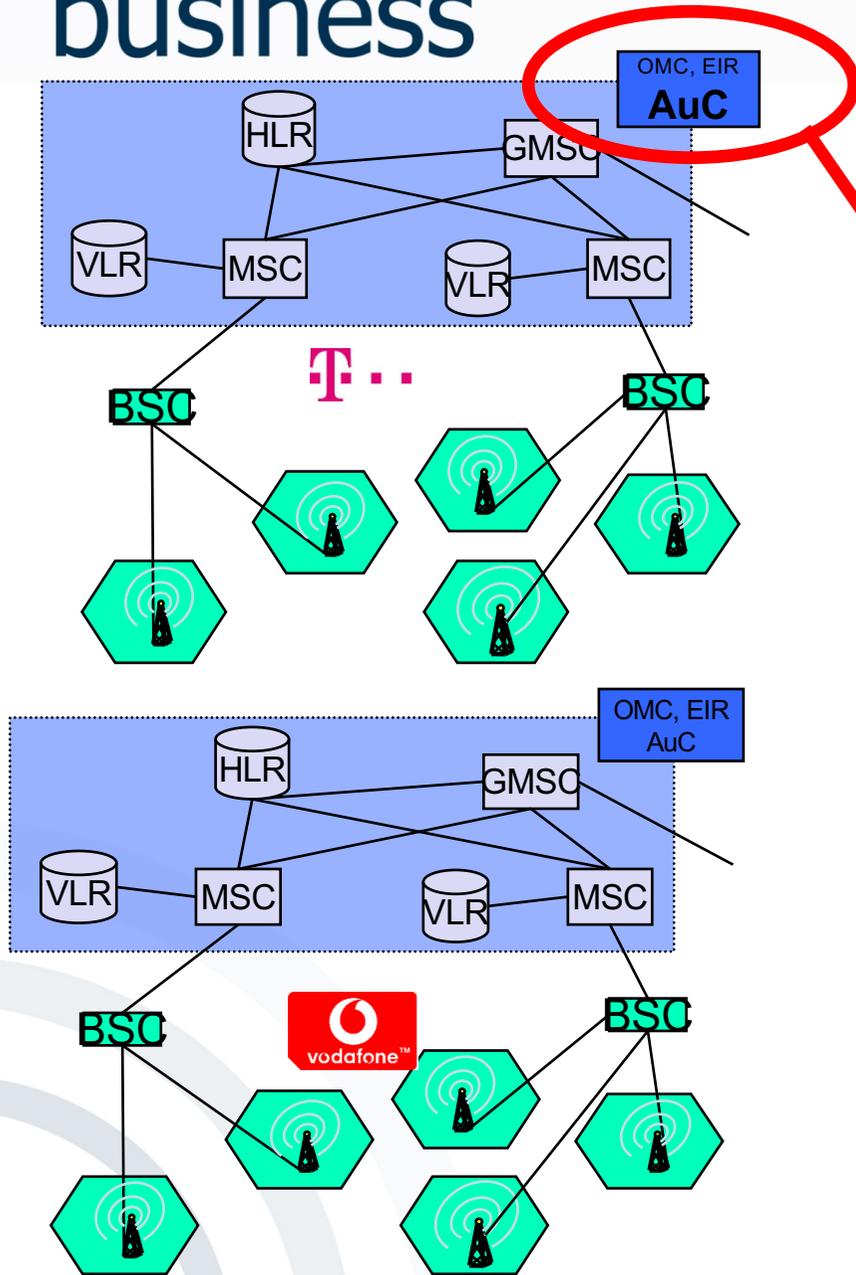
Wireless Internet-oriented Infrastructures & Protocols

- ## Wireless LAN

    - Basics

    - Components and Infrastructures

    - State-of-the art Encryption

    - Mobility and Roaming

- ## Mobile IP – Mobility support for TCP/IP

- ## IP-based Radio Access Networks

# UMTS (3G) System Architecture

- *UTRAN:* **UMTS Terrestrial Radio Access Network**

- *RNS:* Radio Network Subsystem

- *RNC:* Radio Network Controller (controls the Node Bs)

- *Node B:* UMTS base stations (equivalent to base transceiver stations (BTS) in GSM)
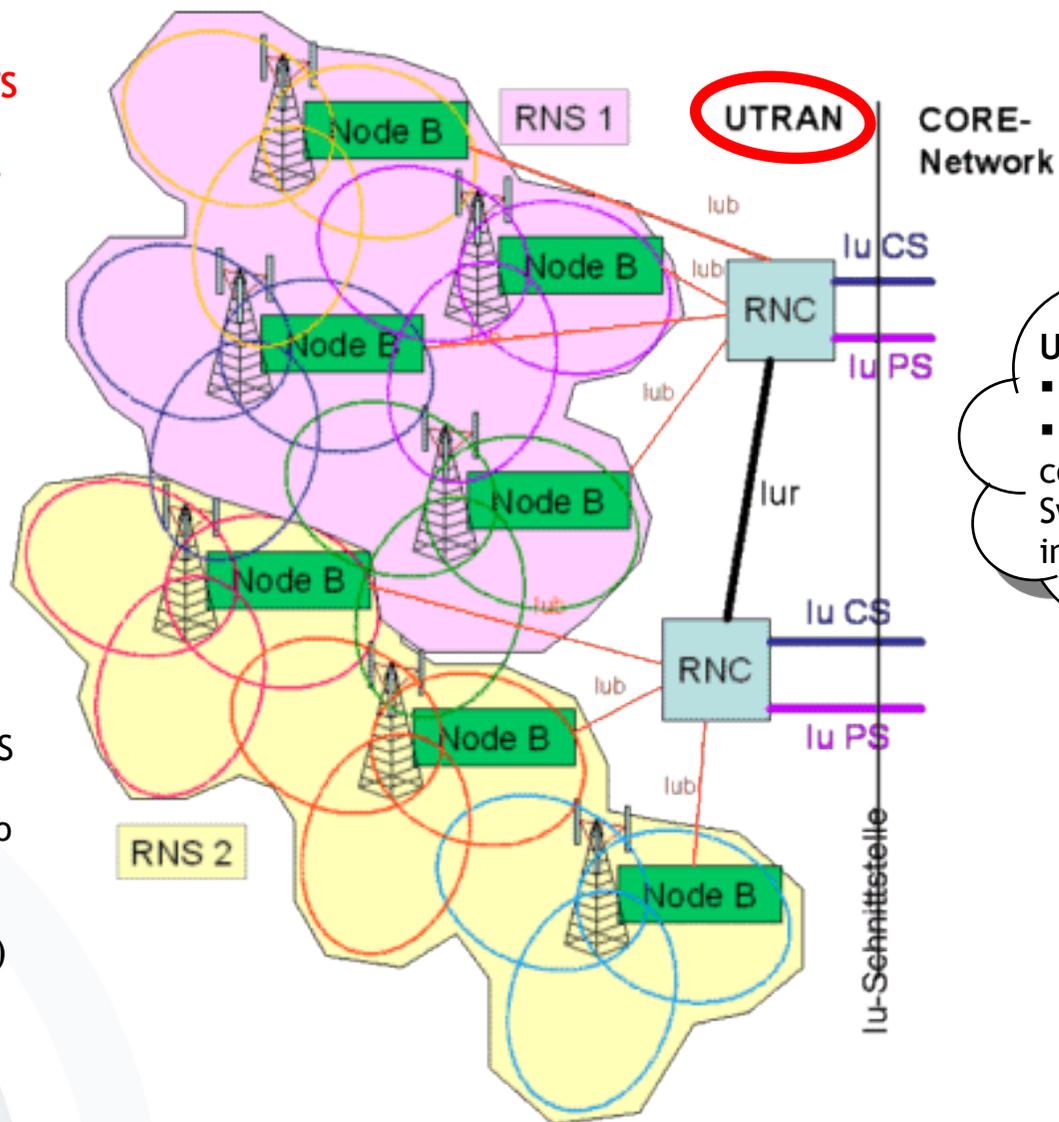


**UMTS Core network**
- is not shown here in detail
- UMTS Core network corresponds to Network- & Switching Subsystem (NSS) in GSM

# Radio Access Networks (RAN)

- Part of a mobile telecommunication system

- Provides connection between device (phone, computer, or machine) and core network

- Implements certain radio access technologies, e.g. GSM or 3G

- Examples of radio access network types are:

  - **GRAN:** GSM radio access network

  - **GERAN:** essentially the same as GRAN but specifying the inclusion of EDGE packet radio services

  - **UTRAN:** UMTS radio access network

  - **E-UTRAN:** Long Term Evolution (LTE) high speed, low latency radio access network

- Some handsets have capability to be simultaneously connected to multiple RANs (dual-mode handsets).

[Wiki 2014]

- All different backhaul technologies may be collapsed onto a single IP/MPLS network (MPLS = Multiprotocol Label Switching) → End-to-end IP approach
- Support for legacy services and reduced cost per bit
- 2G, 3G, and 4G radio technologies transparently supported
- Cost savings possible due to alternative transport media (such as Ethernet and DSL)



[Cisco 2011]  [Cisco 2014]
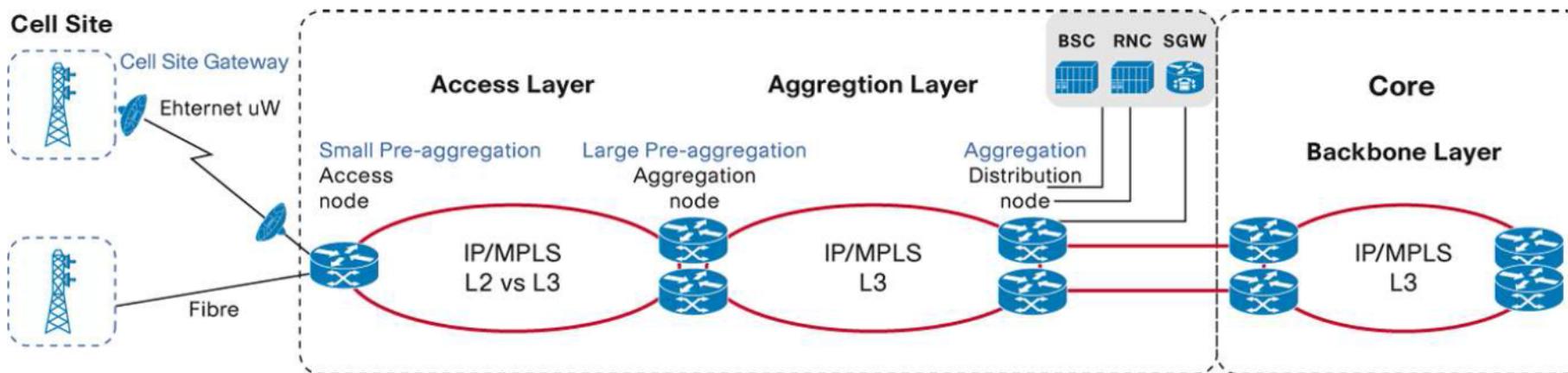
- [Apple 2012] Apple Inc. iOS 6: Wi-Fi network roaming with 802.11k and 802.11r. http://support.apple.com/kb/HT5535, accessed 2013-10-11.

- [ArsT 2008] Battered, but not broken: understanding the WPA crack". Ars Technica. 2008-11-06, accessed 2013-10-11.

- [Cisco 2011] Benefits to Using Layer 3 Access for IP Radio Access Networks (2011), http://www.cisco.com/c/en/us/solutions/collateral/service-provider/unified-ran-backhaul/white_Paper_c11-663732.pdf, accessed 2014-10-28.

- [Cisco 2014] IP RAN - Radio Access Networks, http://www.cisco.com/web/IN/solutions/sp/mobile_internet/ipran_radio _access_networks.html#~overview, accessed 2014-10-28.

- [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 2013-10-09.

- [IEEE 1996] IEEE (1996), 802.11 Tutorial – MAC Entity, 1996, http://grouper.ieee.org/groups/802/11/Tutorial/MAC.pdf, accessed 2013-10-28

- [IEEE 2010] OFFICIAL IEEE 802.11 WORKING GROUP PROJECT TIMELINES http://grouper.ieee.org/groups/802/11/Reports/802.11_Timelines.htm, accessed 2010-10-10.

- [Intel 2013] Intel Support Community. https://communities.intel.com/thread/34273, accessed 2013-10-11.
- [Lanz 2003] Lanz, R. (2003) „Wireless Local Area Network", Berner Fachhochschule, Hochschule für Technik und Architektur
- [Radmacher 2004] Radmacher, M. (2004), "Sicherheits- und Schwachstellenanalyse entlang des Wireless-LAN-Protokollstacks", Universität Duisburg-Essen, p. 116
- [Sauter 2008] Sauter, M. (2008): Grundkurs Mobile Kommunikationssysteme (3., erweiterte Auflage), Vieweg, Wiesbaden.
- [Wiki 2014] Wikipedia, the free encyclopedia (2014): Radio access network, http://en.wikipedia.org/wiki/Radio_access_network, accessed 2014-10-28.
- [Winter 2003] Winter M.-A. (2003) „WLAN: Kostenlos durch Sicherheitslücken surfen", http://www.teltarif.de/arch/2003/kw06/s9809.html, accessed 2013-10-28
- [Wi-Fi 2010] The Wi-Fi Alliance, http://www.wi-fi.org, accessed 2013-10-28.