Wireless LAN @ DESY Zeuthen

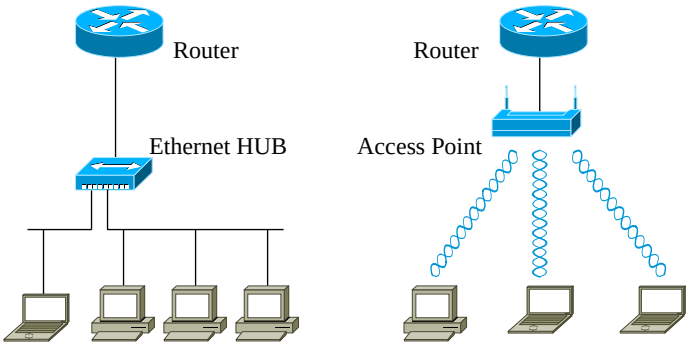
Wireless LAN at DESY Zeuthen

Agenda

- Applications (IEEE 802.11)
- Wireless Technologies and Standards
- Components and Features
- Wireless LAN & Security
- WLAN ínstallation at DESY Zeuthen

Applications (IEEE 802.11)

Wireless Connections



10 Mbps shared bandwidth

CSMA/CD

11 Mbps shared bandwidth

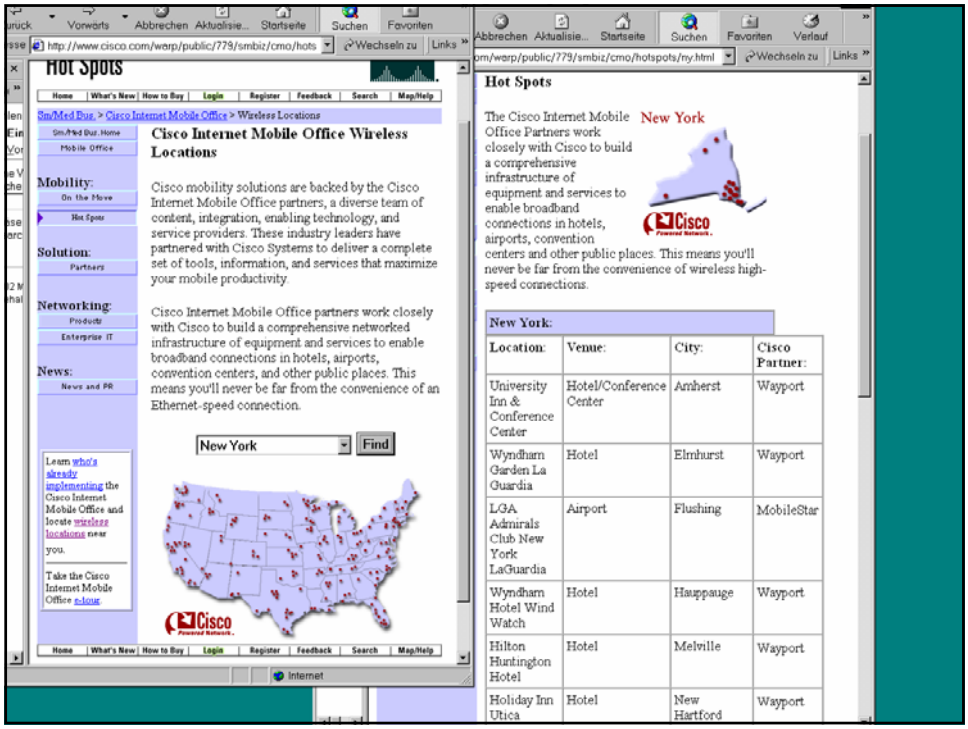
CSMA/CA

Mobile Office

- Home Office
- Head Office
- Branch Office
- Airports
- Convention Center
- Hotels
- Industries
- Education
- ...

Hot Spots

IP anywhere anytime



Why Wireless LAN

- Office mobility
- Common areas, meeting rooms
- Temporary offices
- Office expansion
- Quick installation
- Cost effective alternative
  - Minimale infrastructure costs
  - Flexible growth

Wireless Technologies and Standards

Wireless Technologies

- **Wireless Personal Area Network** **IEEE 802.15** (100 m)
  Bluetooth (10 m) HomeRF 1.2 (100 m) HomeRF 2.0 (100 m)
  Bandwidth: 0.8 - 10 Mbps

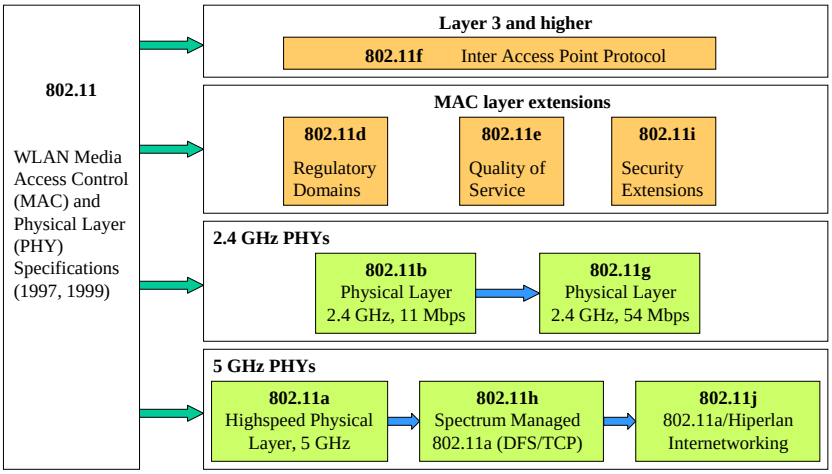
- **Wireless Local Area Network** **IEEE 802.11** (100 m)
  802.11 **802.11b** 802.11a **802.11g**
  HiperLAN-1 HiperLAN-2
  Bandwidth: 1 – 54 (100) Mbps

- **Wide Area Network** (GSM, GPRS: 2 km, UMTS: 1 km)
  GSM (9.6 kbps) **GPRS** (14.4 – 115 kbps) CDMA
  UMTS (14.4 kbps – 2 Mbps)

802.11 Task Group Outline

• 802.11a	54 Mbps, 5 GHz (PHY for UNII), ratified in 1999	
• **802.11b**	11 Mbps, **2.4 GHz**, ratified in 1999	
• 802.11d	additional regulatory domains	
• 802.11e	MAC Enhancements, Quality of Service	(Draft 4.0)
• 802.11f	Inter Access Point Protocol (IAPP)	(Draft 4.0)
• **802.11g**	higher datarate (> 20 Mbps), **2.4 GHz**	(Draft 3.0)
• 802.11h	Managed Spectrum for 802.11a, Dynamic Channel Selection and Transmit Power Control Mechanisms	
• 802.11i	Authentication and Security	
• 802.11j	802.11a/HiperLAN Internetworking	

802.11 Task Group Outline

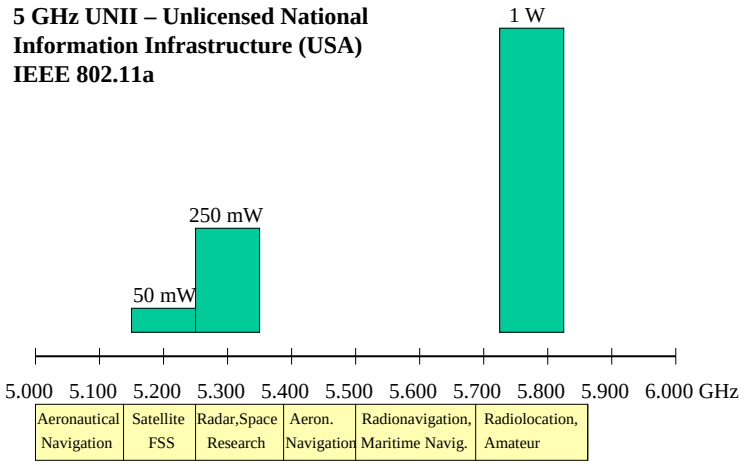


Wireless LAN Standards

IEEE 802.11	1 or 2 Mbps	2.4 GHz	IEEE	WLAN
IEEE 802.11b	1, 2, 5.5, 11 Mbps (22+ Mbps in future)	2.4 GHz	IEEE	WLAN
IEEE 802.11g	1 – 54 Mbps	2.4 GHz	IEEE	WLAN
IEEE 802.11a	1 – 54 Mbps (100 Mbps in future)	5 GHz	IEEE	WLAN
HiperLAN-1	24 Mbps	5.2 GHz	ETSI	WLAN
HiperLAN-2	20 - 54 Mbps	5.2 GHz	ETSI	WLAN -- ATM
HomeRF 1.2	0.8 or 1.6 Mbps	2.4 GHz	HomeRF	home
HomeRF 2.0	0.8, 1.6, 5, 10 Mbps	2.4 GHz	HomeRF	home
Bluetooth	1 Mbps	2.4 GHz	Bluetooth SIG	personal

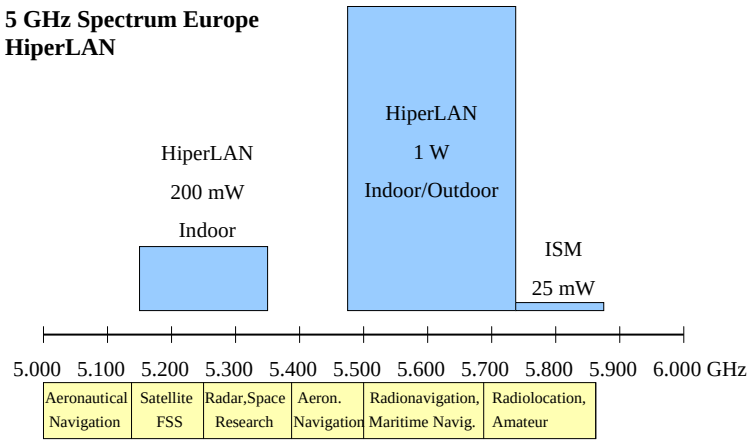
5 GHz Frequence Band – HiperLAN & IEEE 802.11a

5 GHz UNII – Unlicensed National Information Infrastructure (USA) IEEE 802.11a



5 GHz Frequence Band – HiperLAN & IEEE 802.11a

5 GHz Spectrum Europe HiperLAN



5 GHz Frequence Band – HiperLAN & IEEE 802.11a

- **HiperLAN**
  - ETSI (European Telecommunications Standards Institute) standard
  - Ratified in 1996
  - HiperLAN-1 5 GHz radio band up to 24 Mbps
  - HiperLAN-2 5 GHz radio band up to 54 Mbps
    connection-oriented protocol for sharing access among end-user devices

5 GHz Frequence Band – HiperLAN & IEEE 802.11a

- **IEEE 802.11a**
  - 5 GHz radio band up to 54 Mbps (100 Mbps in future)
  - Orthogonal Frequency-Division Multiplexing (OFDM)
  - 3 UNII bands per 100 MHz bandwidth and 4 nonoverlapping channels of 20 MHz
  - each 20 MHz channel comprises 52 300-kHz-wide subchannels
  - 48 subchannels for data transmission, 4 subchannels for error correction
  - UNII-1: 5.15-5.25 GHz frequency range
    maximum transmit power: 50 mW
    maximum antenna gain: 6 dBi
    only indoors

5 GHz Frequence Band – HiperLAN & IEEE 802.11a

- UNII-2: 5.25-5.35 GHz frequency range
  maximum transmit power: 250 mW
  removeable antennas possible
  maximum antenna gain: 6 dBi
  indoors and outdoors

- UNII-3: 5.725-5.825 GHz frequency range
  maximum transmit power: 1W
  removeable antennas
  maximum antenna gain: 23 dBi for point-to-point installations
  6 dBi for point-to-multipoint inst.
  only outdoors

HiperLAN – IEEE 802.11a Implementation Comparison

- HiperLAN/2 & 802.11a share common components
  - Similar Physical Layer (Orthogonal-Frequency-Division-Multiplexing modulation (OFDM), similar radio)

- different MAC implementation
  - HiperLAN/2: QoS and Radio Link Control Features
  - 802.11a: MAC classic Ethernet
  - Hiperlan/2: uses ATM like scheme

2.4 GHz Frequence Band– IEEE 802.11g

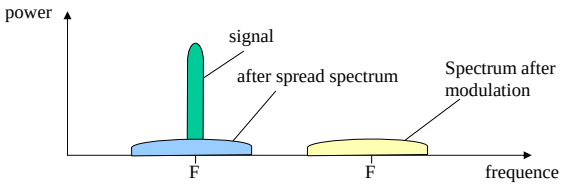
- provides higher data rates at 2.4 GHz
- similar speeds as 802.11a
- backward compatible with 802.11b
- modulation
  - BPSK (Binary Phase Shift Keying) ➔ 1 Mbps
  - QPSK (differential Quaternary Phase Shift Keying) ➔ 2 Mbps
  - CCK (Complementary Code Keying) ➔ 5.5 Mbps, 11 Mbps
  - OFDM (Orthogonal Frequency Devision Multiplexing) ➔ 12 – 54 Mbps
- same modulation as 802.11a (OFDM)
- Draft-Status (3.0)
- more information: IEEE 802.11 website
  www.ieee802.org/11

2.4 GHz Frequence Band– IEEE 802.11b

- **IEEE 802.11b Standard**
  - 2.4 GHz-ISM-Band (Industrial, Scientific and Medical)
  - frequency spectrum classed as unlicensed ➔ anyone can use it as it complies with FCC regulations (public radio spectrum)
  - max. transmit power of radios, type of encoding and frequency modulation
  - WECA (Wireless Ethernet Compatibilty Alliance) ➔ Wi-Fi (Wireless-Fidelity) compliant devices
  - LLC-Layer (Logical-Link-Control Layer 2)
  - 48 bit MAC address (classic Ethernet)
  - max. 11 Mbps
  - Wireless LAN Radio Frequency Methods
    - FHSS (Frequency Hopping Spread Spectrum) ➔ 2 Mbps
    - DSSS (Direct-Sequence-Spread-Spectrum) ➔ 1, 2, 5.5, 11 Mbps

2.4 GHz Frequence Band– IEEE 802.11b

- spread spectrum technology
  - 2.4 GHz ISM band has other primary owners, operates at 600 W power level; IEEE 802.11b: max. 100 mW
  - spread-spectrum-technology



  - non-sensitive against narrow-band interference (e.g. noise)

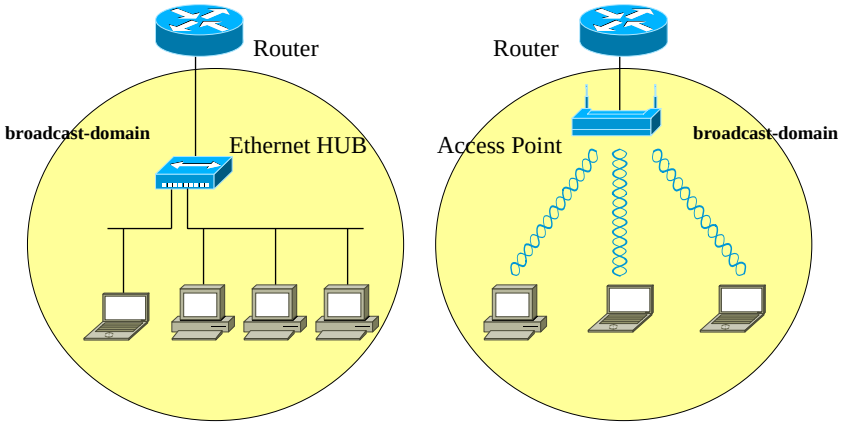
2.4 GHz Frequence Band– IEEE 802.11b

- 2 different types of layer 1 physical interfaces
  - Frequency-hopping architecture
  - Direct-sequencing architecture (single-frequency approach) DSSS
- Frequency Hopping
  - 2.4 GHz ISM band provides 83.5 MHz of available frequency spectrum
  - frequency-hopping-architecture: transmit radio on 1 of 79x 1-MHz-wide frequencies (channel) for max. 0.4 sec
  - ➔ interference tolerant network
  - one channel stumbles across an interference => because frequency-hopping data retransmission is realized on another frequency
  - achievable data rate: 2 Mbps

2.4 GHz Frequence Band– IEEE 802.11b

- Direct-Sequence-Spread-Spectrum (DSSS)
  - 11x 22-MHz overlapping channels of 83.5 MHz (2.4 GHz – 2.4835 GHz)
  - 3x 22-MHz-wide non-overlapping channels
  - large bandwidth & modulation based on Complementary Code Keying (CCK) primary reason for higher data rates (11 Mbps)
  - 3 channels without overlap ➔ 3 Access Points can be used to provide aggregate data rate of combination of the 3 available channels
  - ➔ 11/22/33 Mbps data rate

WLAN Media Access Control



10 Mbps shared bandwidth

CSMA/CD

11 Mbps shared bandwidth

CSMA/CA

WLAN Media Access Control

- **CSMA/CA** - **C**arrier-**S**ense-**M**ultiple-**A**ccess with **C**ollision **A**voidence
- **frames**
  - data frames
  - control frames (RTS,- CTS-, ACK-frames)
  - management frames (beacon frames)

- **frame format**

Praeambel	PLCP-header	MAC-data	CRC

  - Praeambel: - 80 bit synchronization sequence
    - 16 bit start-delimeter-frame
  - PLCP-header: - contains information about encryption on physical layer, packet length

WLAN Media Access Control

  - MAC-data field

frame control	duration	address1	address2	address3	sequence control	address4	frame body	CRC

- **control frames**
  - RTS Request to Send packet
  - CTS Clear to Send packet
  - ACK Acknowledgement packet

frame format

Byte 2 **Frame Control**	**2** **Duration**	**6** **Receiver**	**6** **Sender**	**4** **CRC**

Wireless LAN Components and Features

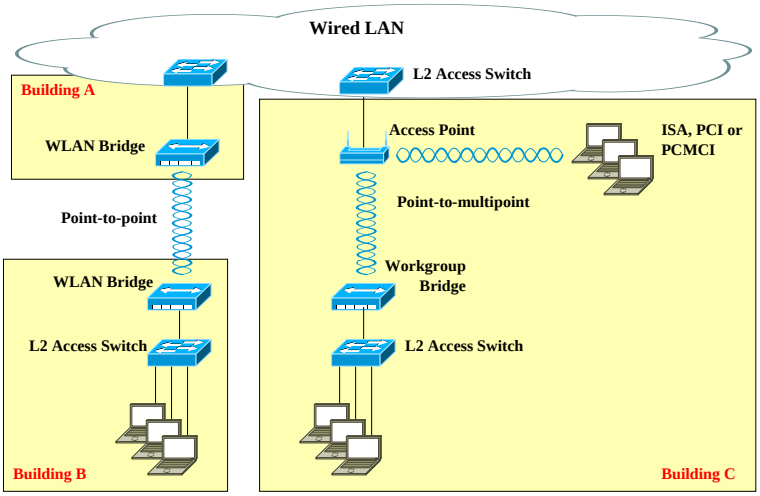
WLAN Components

Components

- Bridge
- Access Point
- Workgroup-Bridge
- NIC (WLAN Network Interface Card (ISA, PCI, PCMCIA))

- Router with WLAN-extension
  (xDSL-Router, ISDN-Router)

WLAN Components and Features

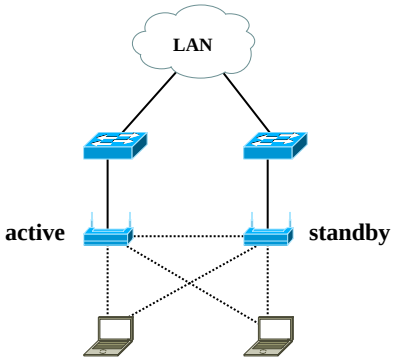


WLAN Components and Features

- point-to-point and point-to-multipoint installation
- inline power over Ethernet, up to 100 m with Cat.5
- selectable transmit power (1, 5, 20, 30, 50, 100 mW)
- antenna flexibility
- variable data rate (1, 2, 5.5, 11 Mbps)
- aggregate bandwidth 33 Mbps
- hot standby implementation, increase availability
- roaming
- load balancing

- **but:**
  - no Quality of Service
  - Voice over IP & multimedia applications supported on „best efford“

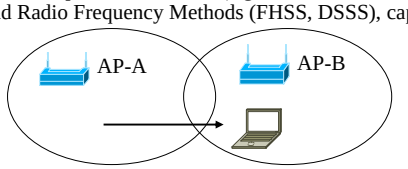
Availability



- access points with identical configuration
- hot standby access point per RF channel
- transparent failover from active to standby access point

Roaming

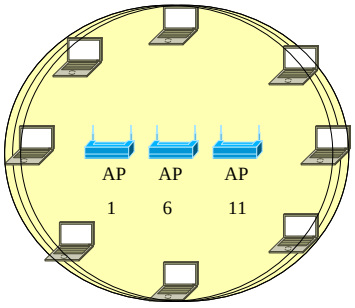
- Media Access Control
  - CSMA/CA
- Beacon Frames
  - are broadcast from access point at regular intervals
  - contain access-point information (e.g. Service Set Identifier (SSID), supported data rates and Radio Frequency Methods (FHSS, DSSS), capacity)



  - client triggers „Roaming Event“ (max. retries) ➔ starting scanning process for available access points
  - new association to AP-B based on criteria such
    - Signal strength 20% better?
    - Fewer hops to backbone?
    - Count of associations (AP-B) + 4 < count of associations (AP-A)?

Load Balancing

- only 3 non-overlapping cells available
- max. Bandwidth for single client 11 Mbps
- load balance criteria
  - signal strength
  - number of users
  - transmit load
  - hops to backbone



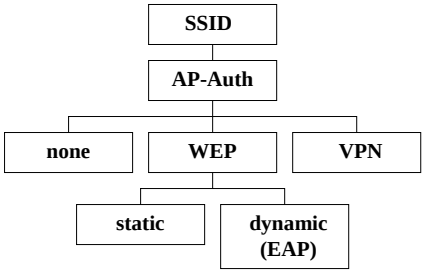
Wireless LAN & Security

Wireless LAN & Security

„... As standardized by the IEEE, security for 802.11 networks can be simplified into two main components: encryption and authentication. The implementation of these components has been proven and documented as insecure by the security community at large. ...“

SAFE: Wireless LAN Security in Depth, White Paper
Cisco Systems, Inc., 2001
http://www.cisco.com/go/safe

Security Mechanisms



SSID	Service Set Identifier
AP-Auth	Access Point Authentication (open/shared key authentication)
WEP	Wired Equivalent Privacy (encryption)
static WEP	static key
dynamic WEP	dynamic key derivation
	EAP (Extensible Authentication Protocol) / LEAP (Ligth EAP)

Network Selection

Service Set Identifier (SSID)

- defines the **name** of the network, ASCII-string
- SSID is not a security mechanism
- transmitted as clear text in Probe & Probe Response frames
- „Broadcast SSID“ disabled stops SSID in beacon frames only
- association to dedicated networks/access points

Access Point Authentication

- **Open authentication**

  open authentication = „null“ authentication

authentication request packet
authentication response packet

- **Shared Key Authentication and static WEP-encryption**

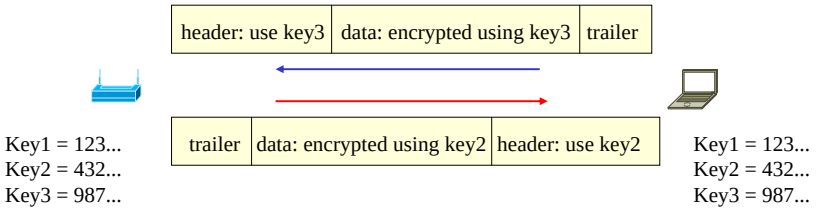
challenge text packet for authentication

cryptographically insecure

plaintext and corresponding encrypted text are visible

authentication request packet
challenge text packet (plaintext)
challenge response packet with predet. WEP
authentication response packet

Static Wired Equivalent Privacy (WEP)



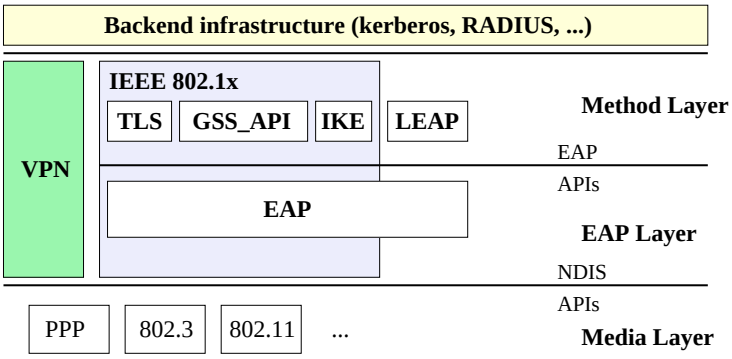
- knowledge of WEP key required
- key needs to be changed frequently
- key distribution and management problematic

MAC Authentication

- MAC address filter on Access Points
- Cisco supports centralized configuration and management of permitted MAC addresses in RADIUS database (Remote Access Dial-In User Service)
- easily spoofed

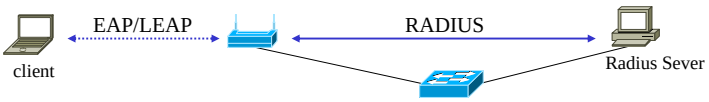
2nd Generation Security Mechanisms

- WLAN IEEE 802.11b is in secure
- security extensions necessary



EAP/LEAP

- EAP - Extensible Authentication Protocol
  (centralized authentication and dynamic key distribution)
- LEAP – Ligth Extensible Authentication Protocol (Cisco)



- client authenticates to access point which disables all further IP requests
- next step: user network logon (username, password; Radius-Server)
- WEP session key calculation based on username/password
- Radius server sends key to access point
- Access point enables network connection

VPN - Virtual Private Network

- support a variety of cryptographically strong options to authenticate the client at the VPN concentrator
- encrypted IP-tunnel client – VPN concentrator
- Triple DES encryption

- connection access point – VPN concentrator is not authenticated

WLAN installation at DESY Zeuthen

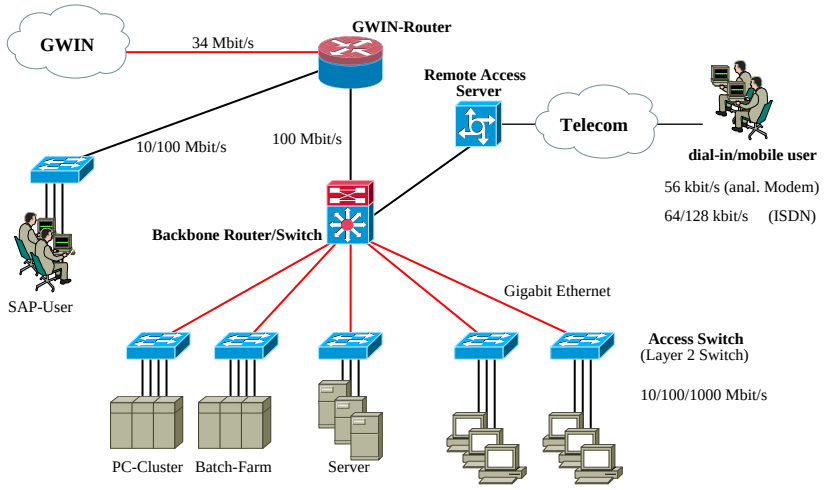
deficits

- **security policies**
  - security zones
  - Firewall
  - Intrusion Detection System (IDS)
  - mobile computing
    - → notebooks, PDA, Bluetooth
- **„Benutzerordnung“**
- **central notebook support (MS Windows/Linux)**
  - system installation/administration
  - security patches
  - root password
  - application software

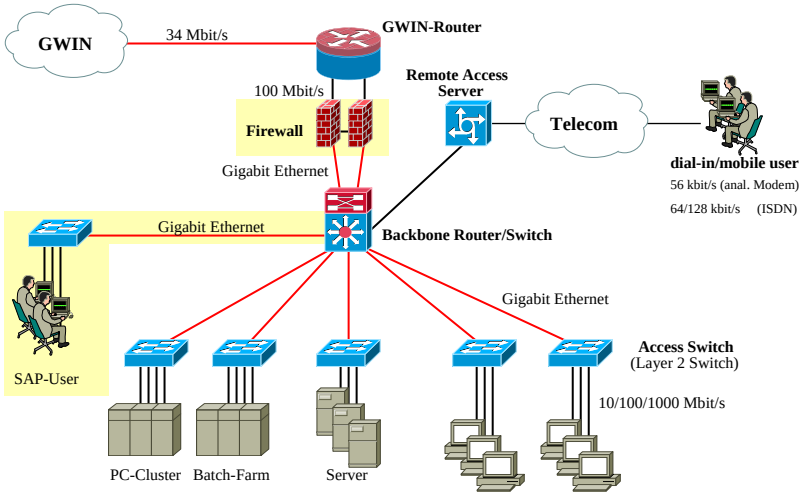
Supported network features

- **network access**
  - Ethernet
  - analogous modem
  - ISDN
  - DSL
  - WLAN
  - DHCP
  - RADIUS
  - EAP
  - VLAN
- **IEEE 802.11b (11 Mbps, 2.4 GHz)**
- **support meetings, workshops, conferences**
- **seminar room SR1, SR2, SR3, Foyer**

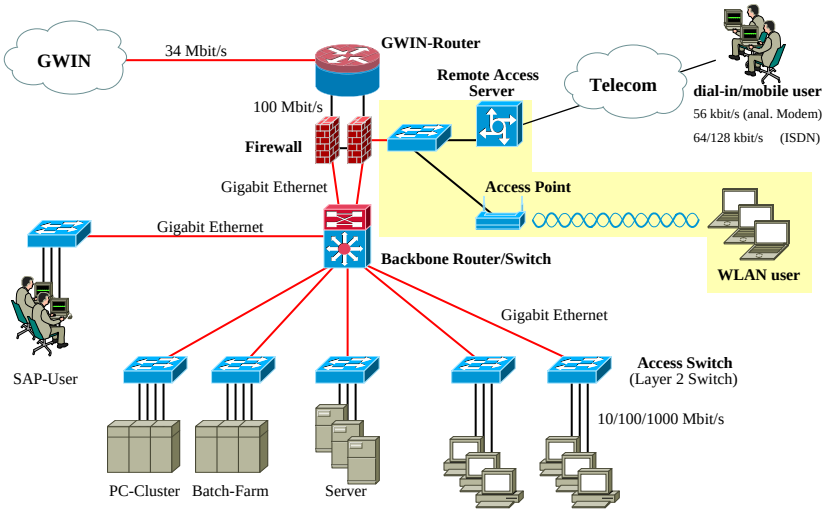
Network Structure (Phase I, August 2002)



Network Structure (Phase II, October 2002)



Network Structure (Phase III)



Abbreviations

• ETSI	European Telecommunication Standards Institute (➔ Hiperlan1/2)
• IEEE	Institute of Electrical and Electronic Engineers, Inc.
• ITU	International Telecommunication Union (CCITT, CCIR)
• RegTP	Regulierungsbehörde für Telekommunikation und Post
• TKG	Telekommunikationsgesetz
• WRC	World Radio Conference (Verwaltung der Funkfrequenzen)
• Bluetooth SIG	Bluetooth Special Interest Group
• RR	Radio Regulations (weltweit gültiges Regelwerk für den Funkverkehr, vom WRC erarbeitet)
• Wi-Fi	Wireless-Fidelity
• ÍSM-Band	2.4 GHz Frequence-Band for Industrial, Scientific and Medical, unlicensed
• UNII-Band	5-GHz Frequence-Band for Unlicensed-National-Information-Infrastructure

Abbreviations

- DSSS Direct Sequencing Spread Spectrum
- WEP Wired Equivalent Privacy (40/128 bit encryption)
- RC4 encryption algorithm invented by Ron Rivest of RSA Data Security Inc. (RSADSI)
- IPSec IP Security Protocol (framework of open standards for secure communication over IP networks)
- VPN Vitual Private Network
- DES Data Encryption Standard
- 3DES Triple DES, encrypts data 3 times with up to 3 different keys

Abbreviations

- SSID Service Set Identifier (32 char ASCII-string)
- AP Access Point
- CSMA/CD Carrier-Sense-Multiple-Access with Collision Detection
- CSMA/CA Carrier-Sense-Multiple-Access with Collision-Avoidence
- EAP/802.1X Extensible Authentication Protocol (centralized authentication and dynamic key distribution)
- LEAP Ligth Extensible Authentication Protocol (Cisco)
- MIC Message-Integrity-Protocol
- TKIP Temporal-Key- Integrity-Protocol
- EAP-TLS EAP Transport Level Security
- RADIUS Remote Access Dial-In User Service
- DHCP Dynamic Host Configuration protocol