
Rechnernetze und Telekommunikation

WLANs

Übersicht

- ◆ **WLAN-Einführung**
- ◆ **Wichtige Standards**
- ◆ **Netzwerk-Typen**
- ◆ **Frequenzen und Antennen**
- ◆ **WLAN und VLANs**
- ◆ **Sicherheit**

Wireless LAN – Was ist das?

◆ Standard IEEE 802.11 (WLAN)

- OSI Layer 1 und 2
- Nutzung des 2,4 GHz und 5 GHz Band (lizenzfrei)
- Bandbreite bis zu 1,3 GBit/s
- Reichweiten bis zu 100 m
- Kompatibel zu Ethernet
- Strahlungsbelastung vergleichbar mit DECT-Telefonen

◆ Im Vergleich

- Schneller und billiger als 4G Mobilfunk
- Geringere Reichweite
- Hoher Energie-Verbrauch



WLAN-Anwendungen

◆ Im Unternehmensnetz

- Zur Anbindung von mobilen Arbeitsplätzen
- Im Bürobereich, Produktion und Logistik

◆ In Steuerungsanwendungen

- Zur Kommunikation und Kontrolle von mobilen Einheiten

◆ Als Hotspot

- Internet-Connectivity für Gäste

◆ Im privaten Bereich

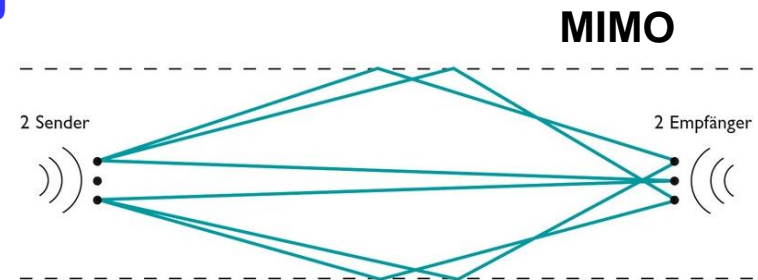
- Heimnetzwerk für gemeinsamen Internetzugang und zunehmend Multimediaanwendungen

Drahtlose Netzwerke im Vergleich zu Festnetzen

- ◆ **Restriktivere Regulierungen der Frequenzbereiche**
 - Frequenzen müssen koordiniert werden, die sinnvoll nutzbaren Frequenzen sind schon fast alle vergeben
- ◆ **Höhere Fehlerraten durch Interferenzen**
 - Andere Sender im freien Frequenzbereich, Dämpfung und Beugung
- ◆ **Niedrigere Übertragungsraten**
 - Max. 1 Gbit/s gegenüber 10 Gbit/s
- ◆ **Stets geteiltes Medium**
 - Alle Stationen teilen sich dieses Medium (und die Bandbreite)
- ◆ **Große Schwankungen der Bandbreite**
 - Einige Mbit/s bis 1 Gbit/s in einem Netz möglich
- ◆ **Geringere Sicherheit gegenüber Abhören, aktive Attacken**
 - Luftschnittstelle ist für jeden einfach zugänglich, Basisstationen können vorgetäuscht werden

WLAN – Die wichtigsten Standards (1)

- ◆ **IEEE 802.11**
 - Basis-Standard von 1997
 - Ziel: Layer 1 und 2 wireless, kompatibel zu Ethernet (IEEE 802.3)
- ◆ **IEEE 802.11b**
 - Bis zu 11 Mbit/s im 2,4-GHz-Band (1999)
- ◆ **IEEE 802.11g**
 - Bis zu 54 Mbit/s im 2,4-GHz-Band
- ◆ **IEEE 802.11n**
 - Bis zu 600 Mbit/s im 2,4 und 5-GHz-Band
 - Nutzt MIMO (mehrere Antennen, Mehrwegeausbreitung)
 - Rückwärtskompatibel zu IEEE 802.11b/g
- ◆ **IEEE 802.11ac**
 - Seit Dezember 2013
 - Bruttodatenrate bis 1,3 Gbit/s
 - ausschließlich im 5-GHz-Band



WLAN – Die wichtigsten Standards (2)

◆ IEEE 802.11i

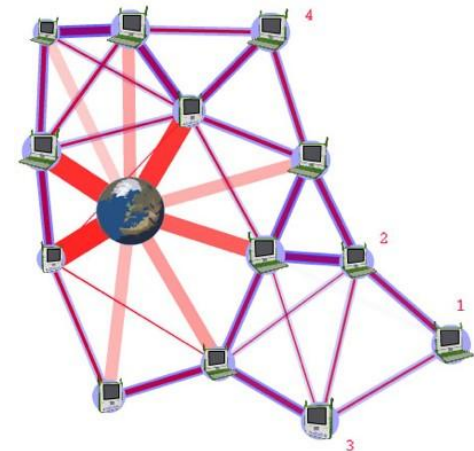
- Heutige Standard-Sicherheit für alle WLANs
- entspr. etwa WPA/WPA2

◆ IEEE 802.11e

- Multimedia-Erweiterungen
- Zur Übertragung von zeitkritischen Daten (Quality of Service QoS)

◆ IEEE 802.11s

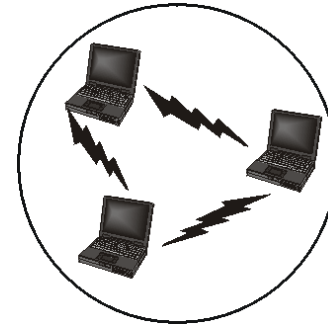
- Mesh-Networking
- Vernetzung von Station untereinander
- Weiterleitung und Routing auf Layer 2



Netzwerk-Typen

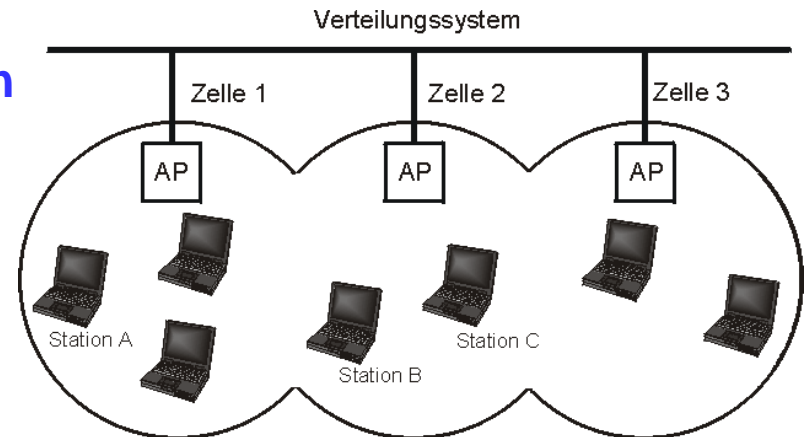
◆ Ad-hoc-Netzwerk

- Spontane Vernetzung von wechselseitig erreichbaren Knoten
- Sehr selten genutzt



◆ Infrastruktur-Netzwerk

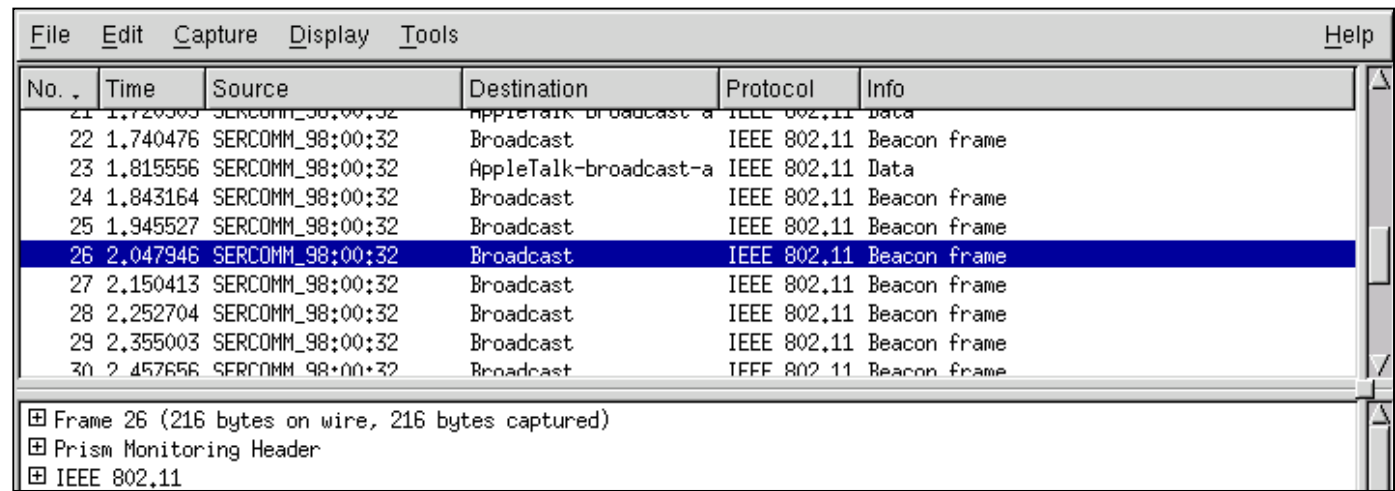
- Access Points (APs) als eine Art von Hubs, an die Stationen (STAs) assoziiert sind
- Aps sind untereinander über anderes Netz (i.d.R. Ethernet) verbunden



◆ Mesh-Netzwerk (s.o.)

Der Beacon-Frame

- ◆ Beacon = „Leuchtfener“
- ◆ Zur Erkennung eines Netzes und der Zell-Informationen
- ◆ In Infrastruktur-Netzwerken
 - Jeder AP sendet Beacon-Frames
 - Kann den Namen des Netzwerkes beinhalten („SSID“)
 - Ein AP kann mehrere SSIDs und damit unterschiedliche Beacon senden
- ◆ Kann mit einem WLAN-Monitor empfangen werden



No.	Time	Source	Destination	Protocol	Info
21	1.720303	SERCOMM_98:00:32	AppleTalk-broadcast-a	IEEE 802.11	Data
22	1.740476	SERCOMM_98:00:32	Broadcast	IEEE 802.11	Beacon frame
23	1.815556	SERCOMM_98:00:32	AppleTalk-broadcast-a	IEEE 802.11	Data
24	1.843164	SERCOMM_98:00:32	Broadcast	IEEE 802.11	Beacon frame
25	1.945527	SERCOMM_98:00:32	Broadcast	IEEE 802.11	Beacon frame
26	2.047946	SERCOMM_98:00:32	Broadcast	IEEE 802.11	Beacon frame
27	2.150413	SERCOMM_98:00:32	Broadcast	IEEE 802.11	Beacon frame
28	2.252704	SERCOMM_98:00:32	Broadcast	IEEE 802.11	Beacon frame
29	2.355003	SERCOMM_98:00:32	Broadcast	IEEE 802.11	Beacon frame
30	2.457656	SERCOMM_98:00:32	Broadcast	IEEE 802.11	Beacon frame

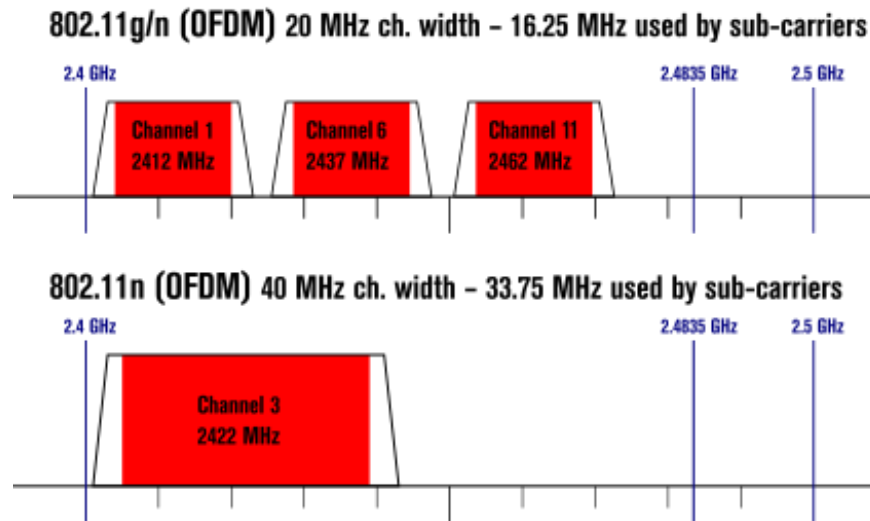
Frame 26 (216 bytes on wire, 216 bytes captured)
Prism Monitoring Header
IEEE 802.11

Scanning

- ◆ „In welcher Zelle bin ich?“
- ◆ **Passives Scanning**
 - Abhören aller Kanäle nach einem Beacon-Frame
- ◆ **Aktives Scanning**
 - Senden eine Management-Frames „Probe-Request“
 - Antwort Management-Frame „Probe-Response“
 - Enthält alle Daten, die auch im Beacon-Frame stehen
- ◆ **Entscheidung der scannenden Station, wo sie sich assoziieren will**
 - Anhand der Signalstärke oder
 - Anhand der Zell-Adresse

Frequenzen

- ◆ Im 2,4 GHz-Band nominell 13 Kanäle möglich, ABER
 - Kanalbreite 5 MHz, Bandbreite der Übertragung min. 20 MHz
 - Abstand von 5 Kanälen vermeidet Beeinflussung (1,6,13)
 - Bei 40 MHz Übertragungsbandbreite (11n) nur noch 1 Kanal!



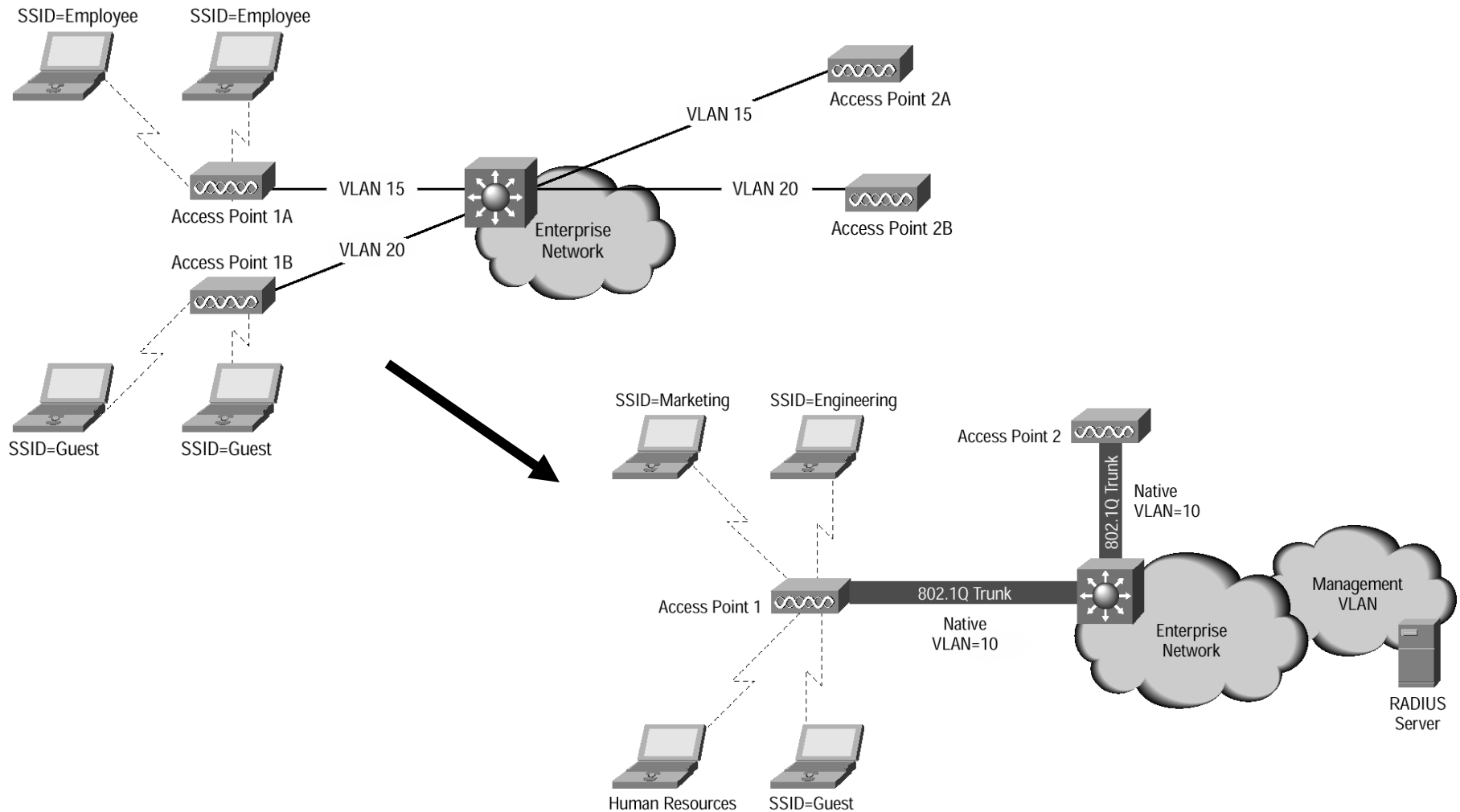
- ◆ Im 5-GHz-Band
 - 8 Kanäle zu 20 MHz

Antennen

- ◆ „Verstärken“ die Leistung des Signals
 - Beim Sender und Empfänger
- ◆ Verschiedene Abstrahlcharakteristika
 - z.B. Sektor, Keule, ...
- ◆ Verstärkung wird gemessen in dBi
 - Verhältnis in Dezibel zu einem isotropen Kugelstrahler
 - Faktor = $10^{\text{dB-Wert}/10}$
 - 100 ~ 20 dB
 - 50 ~ 17 dB
 - 30 ~ 15 dB
 - 20 ~ 13 dB
 - 5 ~ 7 dB
 - 1 ~ 0 dB
- ◆ Maximale Abstrahlleistung
 - 100 mW bei isotropen Kugelstrahler (vergl. Mobilfunk: 2W)



WLAN und VLANs (IEEE802.1Q) (1)



WLAN und VLANs (IEEE802.1Q) (2)

- ◆ **Ermöglicht Trennung von Verkehr verschiedener logischer Segmente/Subnetze**
 - Mehr als drei verschiedene (logische) Netze an einem Ort störungsfrei möglich
 - Bandbreite wird aber weiterhin geteilt

- ◆ **Abbildung von VLAN-ID auf WLAN-SSID**
 - Pro SSID verschiedene Verschlüsselung
 - Eine primäre SSID (die ständig ausgesendet wird)
 - Nur eine unverschlüsselte SSID

Bedrohungen

- ◆ **Denial of Service (DoS)**
 - **Auf der physikalischen Ebene**
 - „Jamming“ durch andere ISM-Band Geräte (Mikrowelle)
 - **Auf der MAC-Ebene**
 - Durch andere WLAN-Devices

- ◆ **Abhören**
 - **Von Kommunikationsmustern und Inhalten**

- ◆ **Senden**
 - **Von nicht-autorisierten Nachrichten**

- ◆ **Betrieb von nichtautorisierten Geräten**
 - **zusätzliche „Fake“-APs als Man-in-the-Middle**
 - **zusätzliche Stationen als Brücken in anderer Netze**

IEEE 802.11i

- ◆ **IEEE802.11i ist Standard für Layer 2-Sicherheit im WLAN**
 - „Nachfolger“ des alten WEP (komplett nutzlos)
 - Auch als WPA-2 von der WiFi-Alliance zertifiziert
 - Verhindert Abhören, unautorisiertes Senden und Fake-Geräte
- ◆ **Bestandteile**
 - „Enterprise“-Security
 - IEEE 802.1x mit verschiedenen Authentifizierungsprotokollen
 - erfordert User-Verzeichnis und Zertifikate (siehe “Campus-WLAN”)
 - “Home“-Security
 - WPA2-PSK (Preshared-Key)
 - **Frame-Verschlüsselung**
 - TKIP (optional)
 - AES (mandatorisch)