

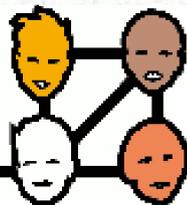
Netzwerk- und Funktechnik

Thomas Osterried

IN-BERLIN e.V.

Vortragsreihe im Rahmen des

moabit.
kiezlan.
de



am 02.07.2011

Lizenz: CC-BY-SA
Version 2011-07-21-02-ab



Überblick des Veranstaltungstags

- 15:00 – 17:00 Uhr
 - Vortrag
 - Rückblick Netzwerkgrundlagen
 - Grundlagen Funktechnik
 - WLAN Funknetz
 - Technik
 - Verschlüsselung
 - Praktische Übungen
- 17:00 – 19:00 Uhr
 - Vortrag
 - Konzepte im Kiezlan
 - Praktische Übungen

..Netzwerktechnik, ein Rückblick..

- Vergleiche Unterlagen zur Grundlagenschulung vom 25.2.2011
 - Layer 2 – MAC Layer
 - Subnetz
 - Switches, Bridges, Hubs
 - Broadcastdomain
 - IP: 192.168.0.0 netmask 255.255.255.0
network 192.168.0.0 broadcast 192.168.0.255
 - oder auch andere Netzwerkprotokolle
 - Computer sprechen „direkt“ miteinander (Layer2)

..Netzwerktechnik, ein Rückblick..

- VLAN
 - Mehrere voneinandergetrennte Netze auf einem Kabel
- Layer 3 - IP-Routing
 - Nachbarnetz ist über Router (aka Gateway) erreichbar (L3)
 - Vollständige Trennung der Netze
 - Nachbarnetz sieht nur die MAC-Adresse des Routers
 - NAT
 - Umsetzung von privaten RFC1918 Adressen auf z.B. die eine IP-Adresse, die der DSL-Router bei Einwahl vom Provider erhalten hat

..Netzwerktechnik, ein Rückblick..

- Sicherheit auf dem Transportlayer
 - ssl / tls
- VPN
 - Verbinden von Subnetzen über das Internet
 - Verschlüsselung und Authentication
 - Die wichtigsten Standards
 - PPTP, L2TP
 - OpenVPN
 - IPsec

..Netzwerktechnik, ein Rückblick..

- Infrastruktur
 - Basisdienste
 - Namensauflösung (DNS)
 - Dienste
 - LAN
 - Druckserver
 - Dateiserver
 - Internet
 - Webserver
 - Mailserver
 - Chatserver
 - u.v.a.m.

..Netzwerktechnik, ein Rückblick

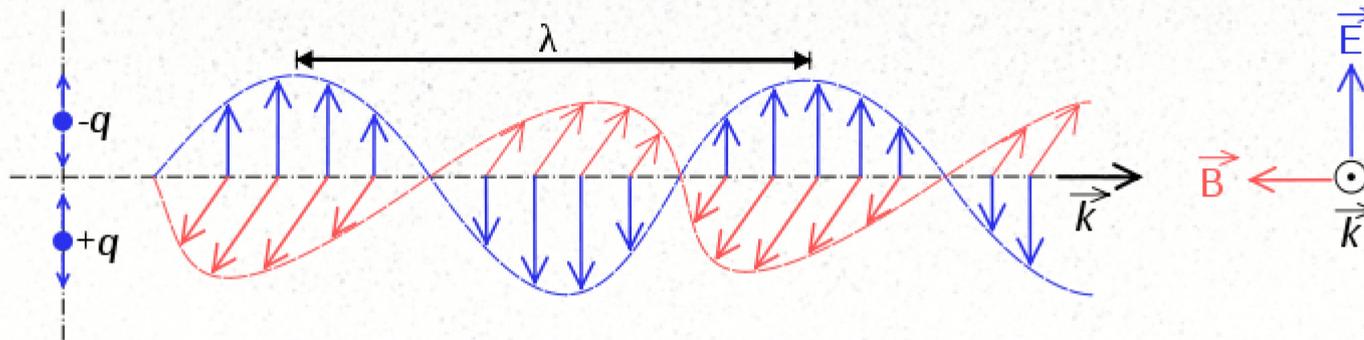
- Übertragungsmedien
 - Kabel (2-Draht, Ethernet, ..)
 - Audiospektrum vs. DSL
 - Licht (LWL / Glasfaser)
 - Funk (z.B. WLAN)

Funk im Allgemeinen..

- Was sind elektromagnetische Wellen / Frequenzen?
 - <http://de.wikipedia.org/wiki/Funktechnik>
 - Die Existenz von Radiowellen wurde 1864 von James Clerk Maxwell auf Grund theoretischer Überlegungen vorhergesagt und 1888 von Heinrich Hertz experimentell bestätigt.
 - Die erste Funkverbindung gelang Guglielmo Marconi 1896 mit einem Knallfunk_ensender und dem Nachbau eines Empfängers von Alexander Stepanowitsch Popow über eine Entfernung von etwa 5 km.

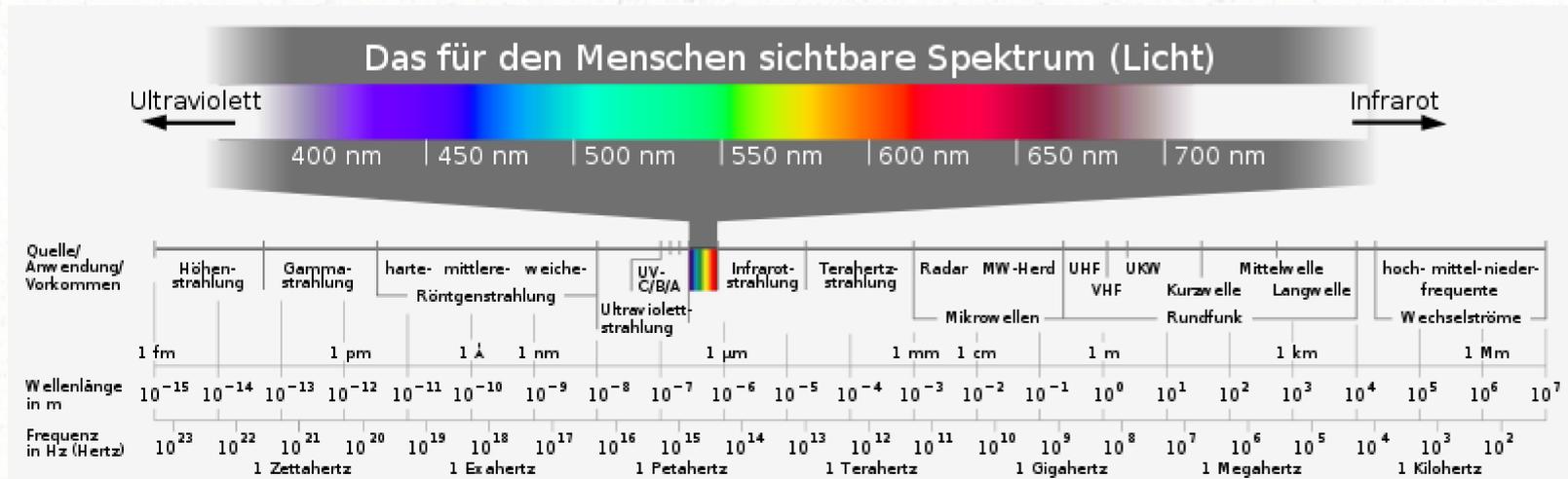
..Funk im Allgemeinen..

- Frequenz
 - Frequenz = Schwingungen / Sekunde = Hertz
- Elektromagnetische Welle
 - http://de.wikipedia.org/wiki/Elektromagnetische_Welle
 - E-Feld und H-Feld



..Funk im Allgemeinen..

- Frequenzspektrum



$$c = \lambda * f \quad [c = \text{Lichtgeschw.}, \lambda = \text{Wellenlänge}, f = \text{Frequenz}]$$

..Funk im Allgemeinen

- Wellenlänge:
niedrige Frequenz
→ große Antennen
 - Vergleiche Antenne
Mittelwellensender
mit SAT-Antenne
WLAN oder Handy.



Funk als Trägermedium für Information..

- Was kann man mit Funk tun?
 - Nachrichten übermitteln
- Signal ein / ausschalten: Morsen
 - Übertragung von Sprache (analog)
 - MW / KW Rundfunk (AM)
 - UKW Radio WideFM
 - kabellose Mikrofone
 - Amateurfunk, CB-Funk, Betriebsfunk (Taxi,..)
 - BOS, Flugfunk, Seefunk
 - Analoges Fernsehen (terrestr. abgesch.; Satellit)

..Funk als Trägermedium für Information..

- Digitale Sprache
 - Handy (GSM, UMTS)
 - DECT
 - Tetra
 - DAB
- Audio/Video
 - Z.B. Liveübertragung Ü-Wagen / Satellit
 - Fernsehen DVB-T, DVB-S

..Funk als Trägermedium für Information..

- Datenkommunikation
 - WLAN, Bluetooth
 - RFID
 - SRD (z.B. dieser Heizung hier)
 - GPS
- Verfahren
 - Jeder mit jedem: Mesh
 - Dezidiert: Richtfunkstrecke
 - Nur Hörer (Radio) vs. Bi-Direktional (GSM)

..Funk als Trägermedium für Information

- Reichweite Abhängig von der Frequenz
 - weltweit (KW, bis 30 MHz),
 - Sichtverbindung (GHz)
 - für Zuhörerkreis geeignete Wahl treffen.

Beispiel privates Telefonat: muß nicht direkt weltweit hörbar sein ;)
- Kabelgebunden (ohne Antenne)
 - DSL, Kabel-TV (DVB-C)
 - Stromleitung (PLC) – gänzlich ungeeignet.
Stromleitung wird zur langen Sendeantenne!

Rechtliche Einordnung..

- Allgemeinzuteilung für die Öffentlichkeit / ehem. "ISM" (Industry, Medical, Science)
- Frequenzen sind NICHT EXCLUSIV, d.h. es gibt hier auch andere Funkdienste, die Schutz vor Störungen genießen
- In Deutschland koordiniert Bundesnetzagentur

http://www.bundesnetzagentur.de/cln_1931/DE/Sachgebiete/Telekommunikation/RegulierungTelekommunikation/Frequenzordnung/Allgemeinzuteilungen/Allgemeinzuteilungen_node.html

..Rechtliche Einordnung..

- Vfg. 89/2003, "Allgemeinzuteilung von Frequenzen im Frequenzbereich 2,4000 GHz - 2,4835 GHz für die Nutzung durch die Allgemeinheit in lokalen Netzwerken; Wireless Local Area Networks (WLAN-Funkanwendungen)".

http://www.bundesnetzagentur.de/DE/Presse/Publikationen/service/WLANFunkanwendungen/WLANFunkanwendungen_node.html

Sendeleistung: 100 mW EIRP

Klassisches WLAN

..Rechtliche Einordnung..

- Vfg. 8/2006, "Allgemeinzuteilung von Frequenzen in den Bereichen 5.150 MHz - 5.350 MHz und 5.470 MHz - 5.725 MHz für Funkanwendungen zur breitbandigen Datenübertragung, WAS/WLAN (Wireless Access Systems including Wireless Local Area Networks)".

Sendeleistung: 1 W EIRP

Strenge Auflagen – 802.11h in Europa
(Radar-Erkennung, automat. frequenzwahl und Leistungsanpassung)

Geräte nach 802.11a sind nicht zugelassen.

Beachte: Indoor- und Outdoor-Bereich!

→ **Niemals auf dem Dach auf Frequenzen kleiner 5470 MHz senden!**

..Rechtliche Einordnung

- BFWA
(Broadband Fixed Wireless Access) -
Providerband). Meldepflichtig; nicht für
Privatpersonen.

Sendeleistung: 4 W EiRP

Noch stärkere Auflagen als in Vfg. 8/2006

- Normen

- ETSI (European Telecommunications Standards Institute)

- 2.4 GHz: WLAN EN 300 328 2.4 GHz

- 5 GHz: EN 301 893 Version 1.5.1

und bei BFWA EN 302 502

Einschub Funktechnik..

- Sendeleistungen
 - EiRP = Senderleistung + Antennengewinn (ggü. Isotropenstrahler) - Kabelverluste
 - Beispiel:
 - Sender habe 10mW. Antenne hat Gewinn von 11dBi, Kabelverluste 1 dB.
 - $10\text{mW} * 10^{((10\text{dBi}-1\text{dB})/10)} = 10 * 10^1 \text{ mW} = 10 * 10 \text{ mW} = 100 \text{ mW}$
→ Betrieb gestattet

..Einschub Funktechnik..

- Signalstärke
 - Nimmt im Quadrat zur Entfernung ab
 - Strahlungsintensität
 - 2.4 GHz: 100 mW Leistung hat Strahlungsintensität von 0.19 W/m^2 . In einem Meter 0.00179 W/m^2 .
 - Freifelddämpfung
 - Doppelte Frequenz → Halbe Entfernung bei gleicher Leistung.
 - Dafür sind die Antennen kleiner..

..Einschub Funktechnik

- Dafür sind auf 5 GHz 1 W EIRP genehmigt, statt 100 mW auf 2.4 GHz
- Empfangsseite:
 - Empfängerempfindlichkeit
 - Antennengewinn
 - Kabelverluste
- es kommt nicht auf ein lautes Mundwerk an, sondern auf gute Ohren ;)
- Linkbudgetrechnung
 - Vor Aufbau eines Links planen und rechnen
http://huizen.deds.nl/~pa0hoo/helix_wifi/linkbudgetcalc/wlan_budgetcalc.htm

Betrachtungen Frequenzen WLAN..

- Einordnung im Frequenzspektrum

LTE < GSM D-Netz < GSM E-Netze < DECT
< UMTS < WLAN 2.4 GHz < LTE <
WIMAX < WLAN 5 GHz

- 2.4 GHz

– Berechnung Wellenlänge

- $300000/2400.0 = 125.0\text{m} = 12.5 \text{ cm}$

→ 1/4-Wellenstrahler wäre 3.125 cm groß

- Vergleichsfrage: weshalb sind die Antennen am Feuerwehrauto so lang?

..Betrachtungen Frequenzen WLAN..

- sehr viele andere WLAN Nutzer
- andere Nutzer wie Videoübertragung, Babyfon, Mikrowellenherde, Amateurfunk
- Eigenschaften von Frequenzen ab 1 GHz
 - Reflektion und Mehrwegausbreitung
 - Dämpfung an Wänden
 - Funkfelddämpfung größer
 - für Nutzerzugänge ist 2.4 GHz besser geeignet als 5 GHz

..Betrachtungen Frequenzen WLAN

- Weshalb ist im GSM auf dem Land die D-Netz-Versorgung besser?
- 5 GHz
 - In diesem Band „sehr wenig los“
 - Bei Richtfunkstrecken höhere Anforderungen an Verfügbarkeit
 - gut geeignet für Richtfunkstrecken
 - Richtantennen mit gutem Gewinn und geringem Öffnungswinkel
 - gut für Paranoiker inhouse ;)

WLAN – Physical Layer..

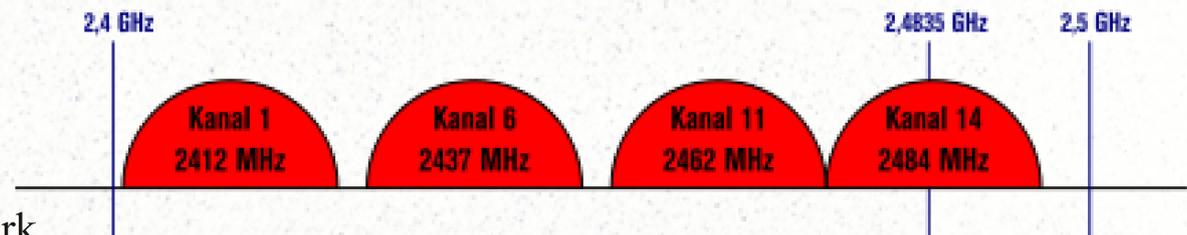
- Modulation
 - alter Standard 802.11b: DirectSpreadSpektrum
22 MHz breites Signal.
 - Neuer Standard 802.11g,a,h: OFDM.
20 MHz breites Signal;
40 MHz: 2*20 MHz bei 802.11n.
- „Kanäle“ (Raster 5 MHz) - vgl. Bandbreite
→ nicht-ueberlappend – Kanäle 1, 6, 11
- Störungen vermeiden: Planung der Kanäle vs.
automatische Kanalwahl

..WLAN – Physical Layer..

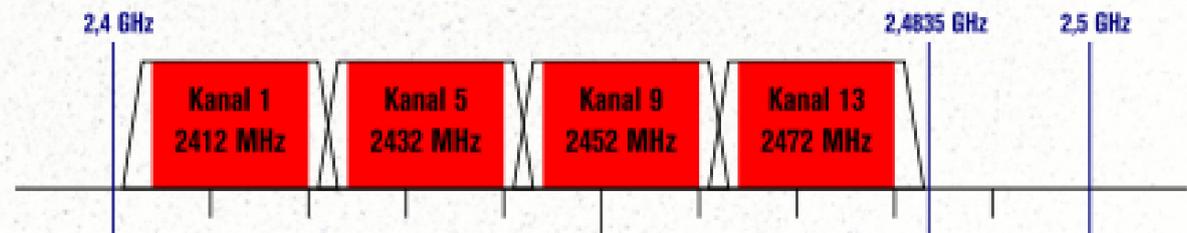
- Bandbreite:
siehe
Grafiken auf
http://de.wikipedia.org/wiki/Wireless_Local_Area_Network

Überlappungsfreie Kanäle 2,4 GHz WLAN

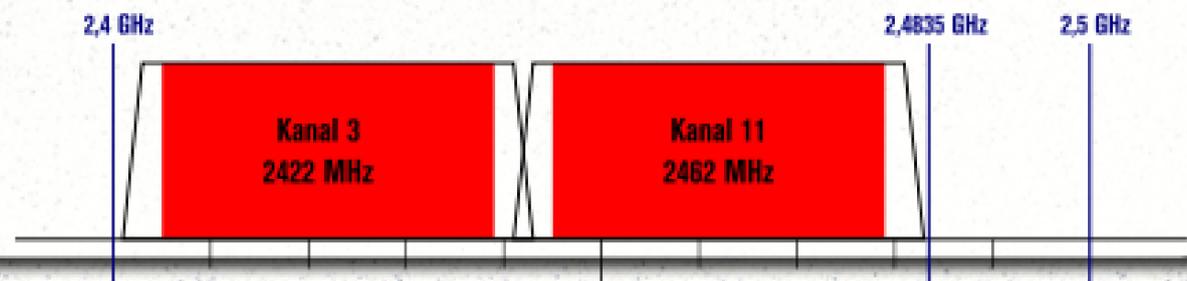
802.11b (DSSS) 22 MHz Kanalbreite



802.11g/n (OFDM) 20 MHz Kanalbreite – 16,25 MHz für Träger



802.11n (OFDM) 40 MHz Kanalbreite – 33,75 MHz für Träger



WLAN – Physical Layer

- Praxis: Spektrum-Analyse mit wi-spy dbx
 - Beispiel Spektrum WLAN-Netze und Mikrowelle
- Standards 802.11b, 802.11g, 802.11a,h, 802.11n - und viele mehr.

Z.B. MIMO, wo man das Prinzip der Mehrwegausbreitung und verschiedene Phasenlagen für sich nutzbar macht.

WLAN – Einfache Nutzbarkeit

- Wir unterscheiden
 - Accesspoint (AP)
 - sendet Beacon (alle 100ms) mit
 - seinem Netzwerknamen (SSID)
 - anderen Parametern (wie z.B. ob verschlüsselt werden soll)
 - Client (STA (Station))
 - Bucht sich in einen ihr bekannten AP ein. Sie sucht sich dabei den stärksten AP gleichen Namens heraus.
 - Bei mehreren APs gleichen Namens: automatisches *Roaming*.

WLAN – Sichere Nutzung..

- Unverschlüsselt
 - nicht empfohlen!
 - Hinweis auf rechtliche Situation
- Verschlüsselung
 - WEP – gilt heute als unsicher
- WPA / WPA2-Personal (802.11i)
 - ein gemeinsames Passwort für alle Nutzer
 - Verschlüsselungsstandards TKIP bzw. AES

..WLAN – Sichere Nutzung

- WPA2 Enterprise (802.1x)
 - Nutzernamen und Passwörter zentral verwaltet.
 - Praktisch für Unternehmen mit vielen Mitarbeitern und Wechsel (Praktikanten, Fluktuation)
 - Autorisierungsprotokolle PEAP oder TTLS
- Literatur:
 - <http://www.heise.de/netze/artikel/WLAN-Verschlueselung-221639.html>
 - <http://www.heise.de/netze/artikel/WLAN-sichern-mit-Radius-1075339.html>
 - <http://www.heise.de/netze/artikel/WLAN-und-LAN-sichern-mit-IEEE-802-1X-und-Radius-979513.html>

Willkommen im KiezLAN..

- Konzept im Kiezlan
 - Aus Erfahrung KuhFunk lernen
 - schlecht
 - Unverschlüsseltes Konzept aufgeben
 - Konfiguration von VPN-Tunnel stellt Nutzer vor Probleme
 - gut
 - dezidierte Linkstrecken, statt Mesh-Netz. Sehr stabil
 - Netzbereiche mit Routing und Bridging

..Willkommen im KiezLAN..

- Design im KiezLan
 - Zuführung der Daten über eine dezidierte verschlüsselte Richtfunkstrecke
 - Nutzerzugang:
 - Accesspoint mit 2 Netzwerknamen (SSIDs):
 - KiezLAN-Info
 - unverschlüsselt. Man kann nur eine einzige Webseite aufrufen: eine Hilfeseite zum KiezLAN
 - KiezLAN
 - verschlüsselt

..Willkommen im KiezLAN

- Zugangspassworte
 - Für Jedermann
 - Nutzername Gast / Passwort Kiezlan
 - Beachte: Auch wenn mehrere Gäste das selbe Passwort verwenden, so ist trotzdem jede WLAN-Verbindung separat verschlüsselt (Teil des Standards)
 - RubbelCode
 - Nutzername xxxxx / Passwort xxxxx
 - IN-Berlin e.V. Teilnehmer
 - Nutzername sitename@in-vpn.de / Passw. xxx

EOF

Ich hoffe es war für jeden etwas interessantes dabei.

Bei Fragen: E-Mail an thomas@in-berlin.de

Die Folien finden sich auch unter

<http://moabit.kiezlan.de/>

und dürfen frei weitergegeben werden

Vielen Dank für's Interesse!

privacy is not a crime ;)