Angefunkt: WLAN, GPRS, Zigbee und Co

Wolfram Maag

CSE Mobility

Ziel der Präsentation

- Relevante Funktechnologien bei Cisco aufzeigen
- Möglichkeiten und Grenzen zeigen
- Einsatzszenarien herausarbeiten
- Welche Möglichkeiten haben Sie damit
- Viel heiße Luft auf Tatsachen reduzieren

Agenda

- Prinzipielles zur Funkübertragung
- Öffentlicher Mobilfunk GSM/GPRS/UMTS
- Wimax
- DECT *1992, +29.12.2008
- Bluetooth
- Zigbee
- WLAN

Funk im Allgemeinen

- Elektromagnetische Funkausbreitung
- Komplett reguliert im Frequenznutzungsplan der Bundesnetzagentur

FREQUENZNUTZUNGSPLAN

gemäß TKG über die Aufteilung
des Frequenzbereichs von 9 kHz bis 275 GHz
auf die Frequenznutzungen sowie über
die Festlegungen für diese Frequenznutzungen

Geschichte

- James Clerk Maxwell: Theoretische Grundlagen (Maxwellsche Gleichungen, 1864)

$$\oint_{\partial A} \boldsymbol{E} \cdot \mathrm{d}\boldsymbol{s} + \frac{\mathrm{d}}{\mathrm{d}t}\left(\iint_A \boldsymbol{B} \cdot \mathrm{d}\boldsymbol{A}\right) \equiv 0$$

$$\oint_{\partial A} \boldsymbol{H} \cdot \mathrm{d}\boldsymbol{s} = \iint_A \boldsymbol{j}_l \cdot \mathrm{d}\boldsymbol{A} + \frac{\mathrm{d}}{\mathrm{d}t}\left(\iint_A \boldsymbol{D} \cdot \mathrm{d}\boldsymbol{A}\right)$$

- Bestätigung durch Heinrich Hertz 1888
- Bereits 1899 kommerzielle Nutzung

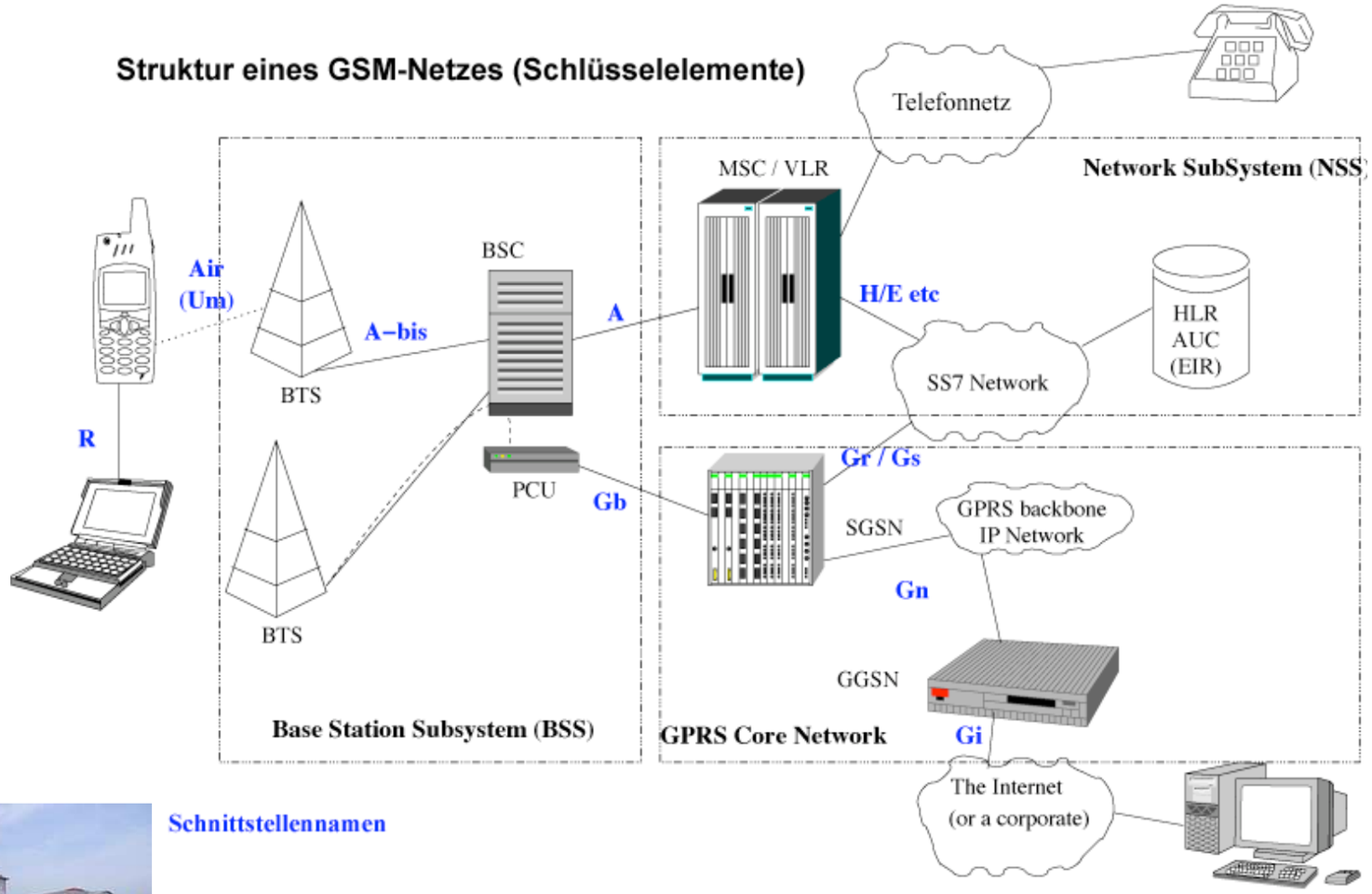
Digital statt Analog

- Heutige Funkverfahren nutzen mehr und mehr Digitaltechnik
- Korrektur von Übertragungsfehlern einfacher
- Beispiel: DVB-T statt analoges Fernsehen
  - 3-6 mal soviele Programme auf derselben Bandbreite
  - Bessere Qualität beim Nutzer

GSM

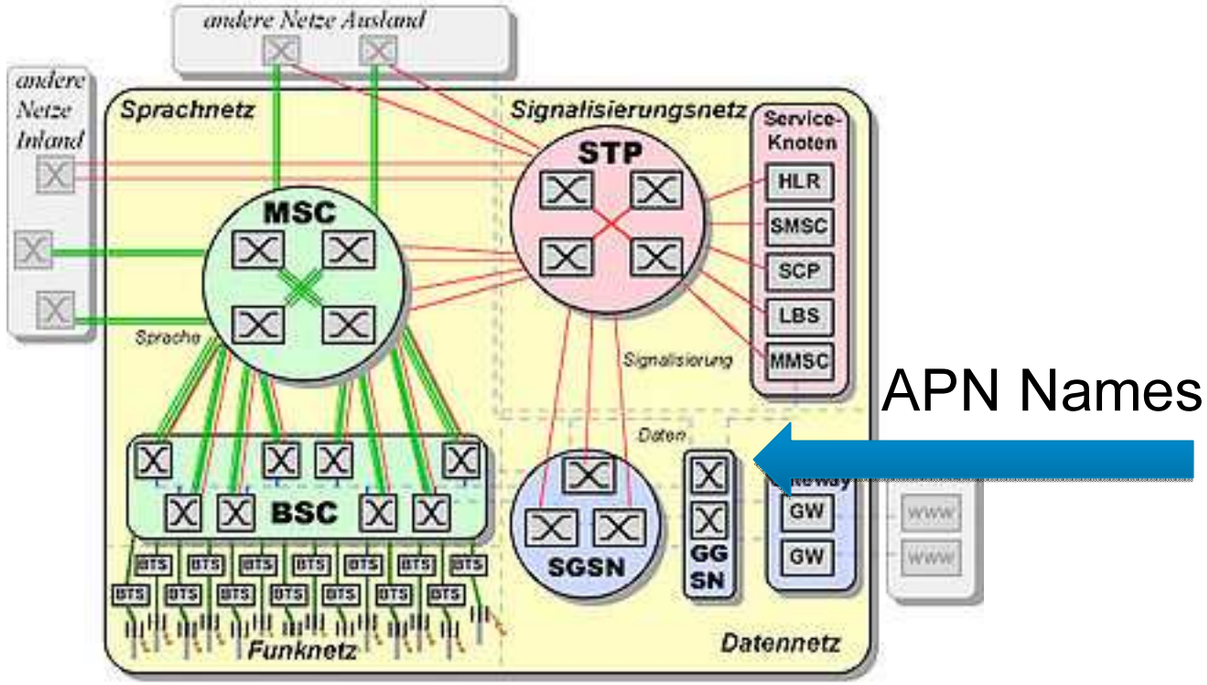
- Global System for Mobile Communication
- Weltweit verbreiteter Funkstandard
- Fokussiert auf Sprachdienste
- Grundlage seit 1992 für den Erfolg von Mobilkommunikation
- Reichweiten von wenigen 100 m bis 35km
- 880-915 MHz, 925 – 960 MHz (D-Netze)
- 1725 – 1780 MHz & 1820 – 1875 MHz (E-Netze)

Aufbau eines GSM Netzes



Schnittstellennamen

GPRS

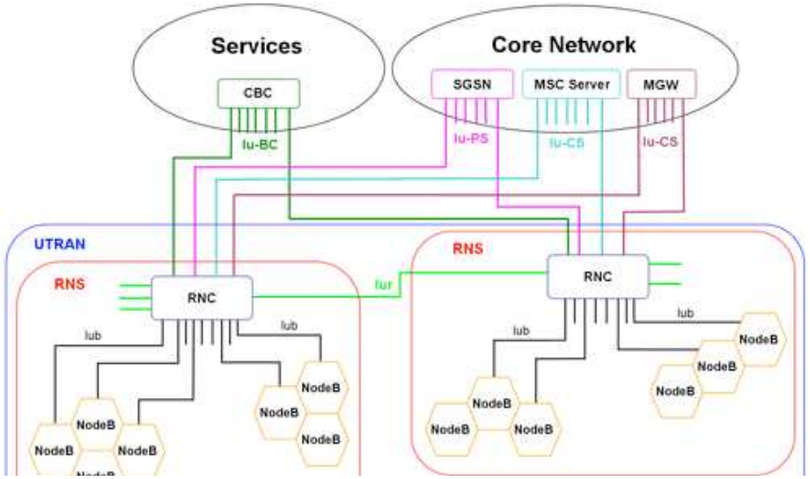


APN Names

- SGSN: Serving GPRS Support Node
- GGSN: Gateway GPRS Service Node (z.B. Cisco)

EDGE / UMTS

- Edge ist die Evolution aus GPRS bis ca. 200kbps
- UMTS: komplett neue Netzstruktur, hohe Frequenzen, geringere Reichweite
- 1920-1980 MHz, 2110-2170MHz
- Mit HSDPA bis 14,4 Mbps theoretisch, tatsächlich 1,4 Mbps



Cisco Produkte

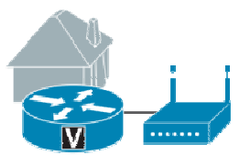
- Cisco 881
- Router für GSM/EDGE/UMTS
- Konfiguration Aussenstelle → Internet (evtl. VPN)
- Keine Dial-In Option
- Oder Einschubmodul für 1841

Wimax

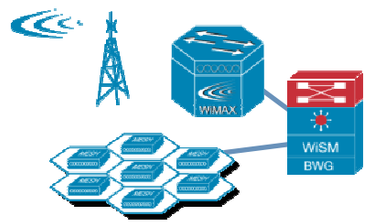
- Lizensierter Bereich
- Genehmigung durch RegTP
- Nachweis der Qualifikation in Frequenzplanung
- Derzeit in Deutschland für WLL genehmigt im Bereich 3,6 GHz als DSL Ersatz
- Vergaben sind bis dato nur an SP´s erfolgt
- Derzeit nur Netze auf Basis 802.16 im Einsatz, kein 802.16e in Betrieb

Cisco Broadband Wireless

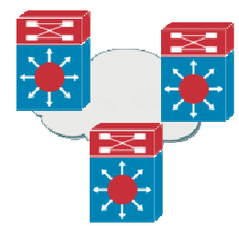
Cisco’s end-to-end Broadband Wireless Architektur besteht aus folgenden Elements



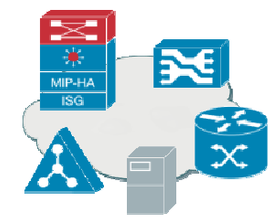
Subscriber Devices and Services



Broadband Wireless Access



Carrier Ethernet

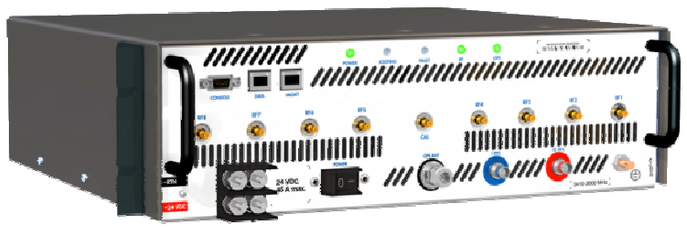


Service Exchange Framework

Cisco Broadband Wireless Access

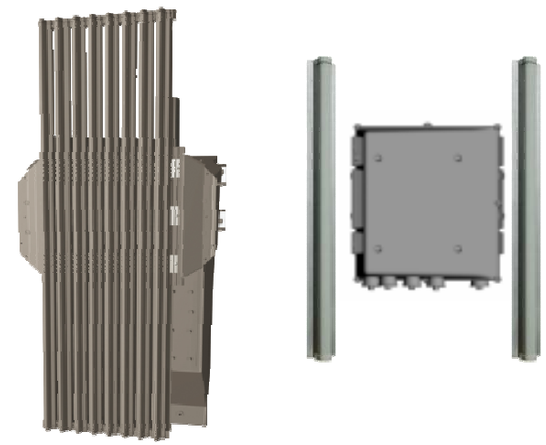
Mobile WiMAX Networking

Cisco BWX 8300 Series Broadband Wireless Access System



BWX 8305 Mobile WiMAX Basestation

- WiMAX 802.16e-2005 zertifizierbar
- Industry-leading RF Link-Budget
- Mobile WiMAX mit Adaptive Beamforming; Advanced Antenna System (AAS)
- Kombiniert Beamforming+MIMO für mehr Kapazität & überragende Performance



BWX 8305 / 2305 Mobile WiMAX Antennas

- BWX 8305 8-Element Array bietet 120° Sector Coverage mit Beamforming & MIMO
- BWX 2305 2-Element Antenna bietet in-fill Coverage mit MIMO & Diversity

Subscriber Stations

- **BWX 110 Desktop Modem** *LMX*
- Dual-mode
- Can connect to single computer or Home LAN of 10 devices
- 2300-2390, 2496-2690, 3410-3525, 3475-3600 MHz

BWX 120 PC Card
PMX

- Dual-mode
- 2300-2390, 2496-2690, 3410-3525, 3475-3600 MHz

- **BWX 210 Desktop Modem**
  Surfer
- Operates in Navini16e beamforming mode
- Allows operators to deploy 802.16e beamforming terminals ahead of 3rd party fully-certified Mobile WiMAX devices
- 2300-2390, 2496-2690, and 3400-3700 MHz

Was bedeutet also Wimax

- Keine / geringe Durchdringung in Gebäuden
- Keine handelsüblichen Clients
- SP – Technologie
- Kosten / Zeit für Lizenzverfahren: derzeit wird über 1 Jahr bis zur Abgabe eines kompletten Antrags und ca. 1 Mio Kosten gesprochen
- Viele Applikationen sind damit nicht abzubilden
- Bandbreiten: bis 70MBps <u>oder</u> 10 km Reichweite

Mobile Inhouse Telefonie

- CT1+ und CT2 ab Ende 2008 in Deutschland verboten

Die Regulierungsbehörde weist darauf hin, dass schnurlose Telefone der Standards CT1+ und CT2 ab dem 1. Januar 2009 im Gebiet der Bundesrepublik Deutschland nicht mehr betrieben werden dürfen. Stellt der Funkmessdienst der Bundesnetzagentur bei der Eingrenzung von Funkstörungen ein solches Schnurlostelefon als Verursacher einer Störung fest, so werde dem Verursacher der Aufwand der Störungssuche in Rechnung gestellt. Da es sich um eine Ordnungswidrigkeit handelt, könne zudem ein Bußgeld fällig werden, betonte die Behörde.

- Analoge Übertragung bei CT1+, CT2 digital
- CT1+:885-887kHz, 930-932kHz
- CT2 864-868kHz

DECT *1992 +29.12.2008

- DECT wird praktisch ausschliesslich im Voicebereich eingesetzt
- Ca. 30 Mio Telefone in Deutschland
- DECT diente als mobile Voice Inhouse Lösung
- Verschlüsselung bei DECT ist optional
- Verschlüsselungsverfahren beruht auf der Geheimhaltung des Verfahren
- Nur ein Teil der Geräte und Basisstationen verschlüsselt tatsächlich

Technische Eigenschaften

- Einfach in der Handhabung
- Vielzahl an Geräten verfügbar
- Max. 250 mW Sendeleistung
- Hauptband weltweit: 1880MHz – 1900MHz + Erweiterungsbänder
- Kombination auf Frequenz und Time Multiplex

Sicherheit

- Am 29.12.2008 beim Chaos Computer Club vorgeführt
- Abhören von DECT / Dialout über DECT Basisstation
- Mithören mit USRP / Com-On-Air oder AVM Box
- Passive Sniffing funktionierte bei der Hälfte der Telefone (no Encryption)
- Teilw. Basisstationen ohne Encryption
- Encryption mit Standard Hardware zu knacken
- Angabe über Sicherheit recht mangelhaft
- Demnächst gibt es Kermit Driver, derzeit läuft beta

Cisco Unified Wireless IP Phone 7921G/7925

- 802.11a,b,g
- AES/TKIP Encryption
- Color display
- lange Gesprächszeit
- hohe Stabilität
- intuitives User Interface

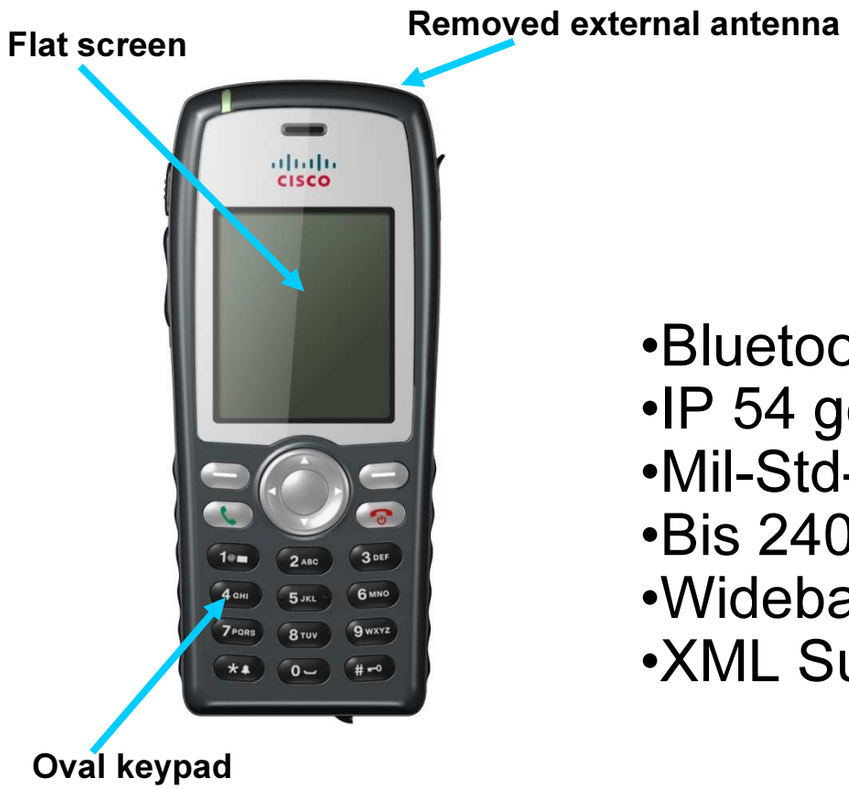
30. Dezember 2008 Artikel verschicken | Artikel drucken | E-Mail an Verfasser

DECT-Telefone lassen sich per Laptop abhören

von Lars Bube

Auf dem 25. Chaos Communication Congress (25C3) in Berlin haben Sicherheitsexperten den Mythos des sicheren Telefonierens mit dem DECT-Standard entzaubert: Mittels einer leicht modifizierten VoIP-Karte für

Voice Over WLAN: 7925G Übersicht



- Bluetooth Headset Support
- IP 54 gegen Staub und Feuchtigkeit
- Mil-Std-810F gegen Erschütterungen
- Bis 240 h Standby, 13h Talk-time
- Wideband audio codec
- XML Support

Bluetooth

- Personal Area Network
- Ersatz von IrDA (Infrared Data Association)
- Häufigster Einsatz: Headsets & Auto
- 2,4 GHz (2,402 – 2,480GHz)
- EDR mit bis zu 2,1 Mbps
- Viele sog. Profiles verfügbar

Sicherheit von Bluetooth

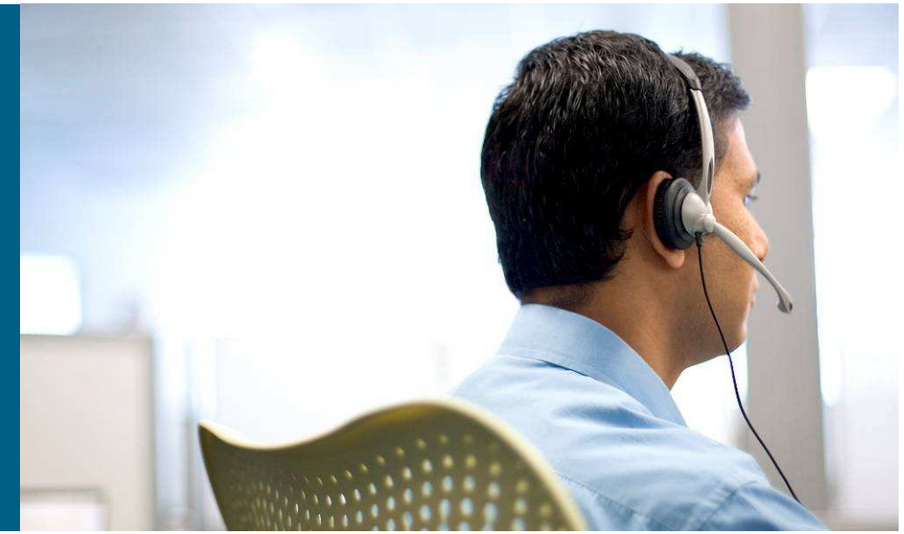
- Sicherheitsbedenken beim Pairing
- Knackbar bei kurzen PINs (4 Stellen)
- Aber: Kurze Reichweiten
- 3 Unterschiedliche Sicherheitsmodi
- Kann Telefonie mit VoiceWLAN beeinflussen

Zigbee

- Technologie zur Vernetzung von Haushaltsgeräten (Heim und Gebäudeautomatisierung)
- Industrie und Automatisierungstechnik
- Standard: IEEE 802.15.4
- Topologien: PAN besteht aus End devices & Router, Router kann auch Coordinator sein
- Baum und Sterntopologien
- 868 MHz in Europe

ZigBee® Alliance

Wireless LAN



2,4 GHz Frequenzband

- 2,4 - 2,4835 GHz
- ISM Frequenzen

  Industrial, Scientific, Medical
- Lizenz- und Gebührenfrei
- www.Bundesnetzagentur.de

  Regulierungsbehörde für Telekommunikation und Post

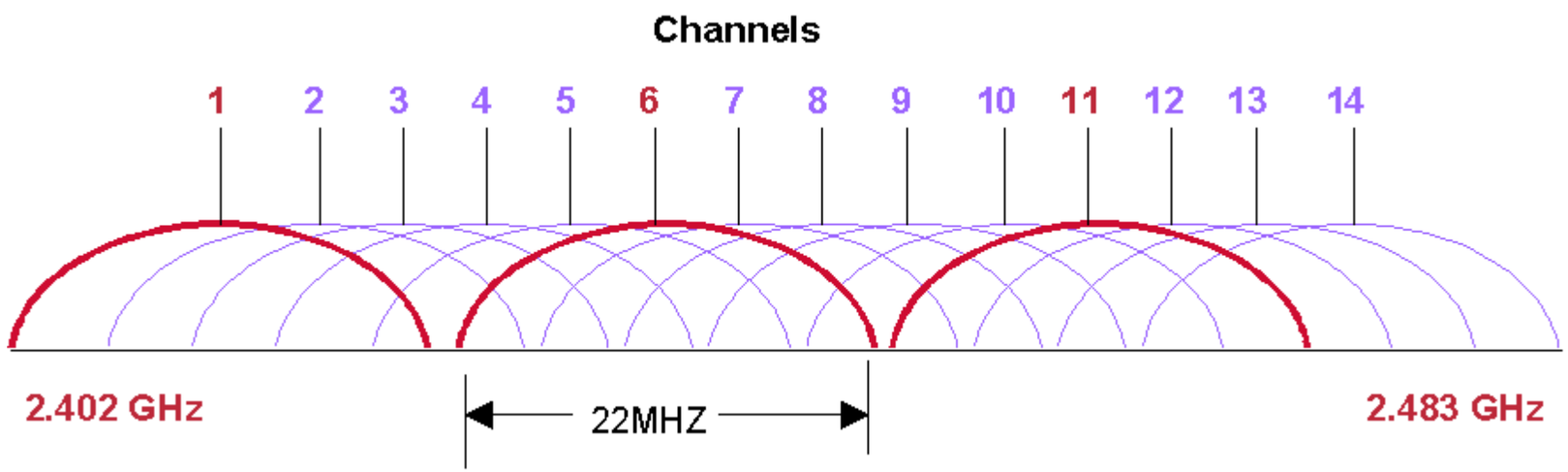
IEEE 802.11 Standard Activities

- 802.11a—5 GHz, ratified in 1999
- 802.11b—11Mb 2.4 GHz, ratified in 1999
- 802.11d—World Wide Roaming
- 802.11e—Quality of Service
- 802.11f—Inter-Access Point Protocol (IAPP) – To be ratified soon
- 802.11g—Higher Data rate (54 Mbps) 2.4 GHz
- 802.11h—Dynamic Frequency Selection and Transmit Power Control mechanisms
- 802.11i—Authentication and Security

802.11b

- Als Standard im Sept. 1999 verabschiedet
- 11 Mbps, 2.4 GHz, Direct Sequence (DSSS)
- 11 US Kanäle
- 13 ETSI Kanäle
- 14 Japan Kanäle
- Power Level: 36 dBm EIRP-FCC
  20 dBm EIRP-ETSI (100 mW)
- Weltweit verfügbar
- sehr große installierte Basis

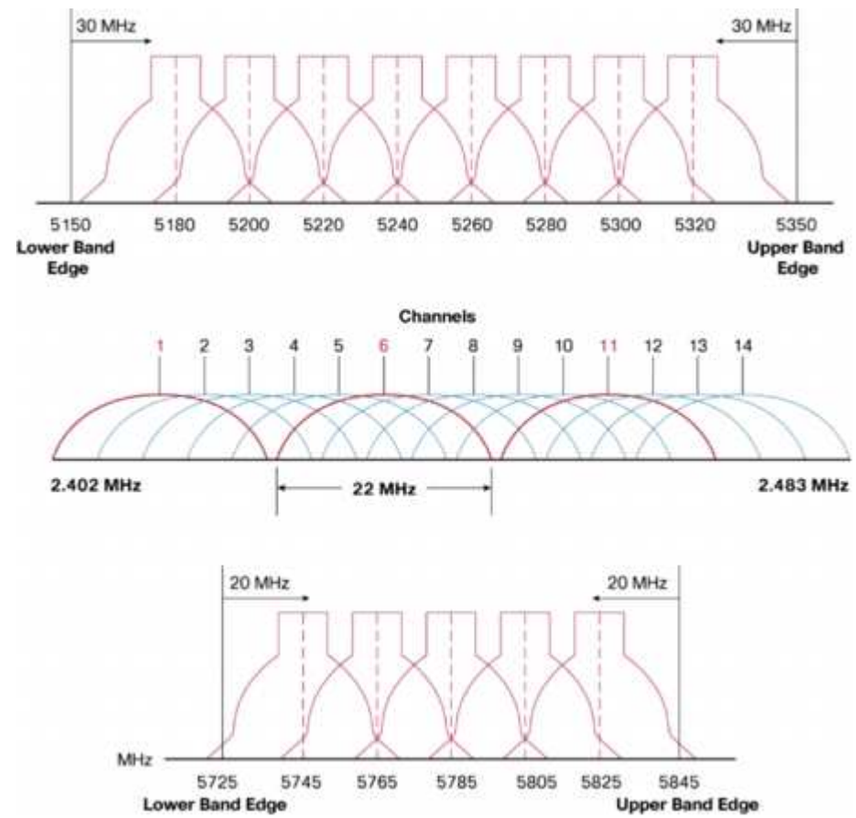
802.11b Übersicht



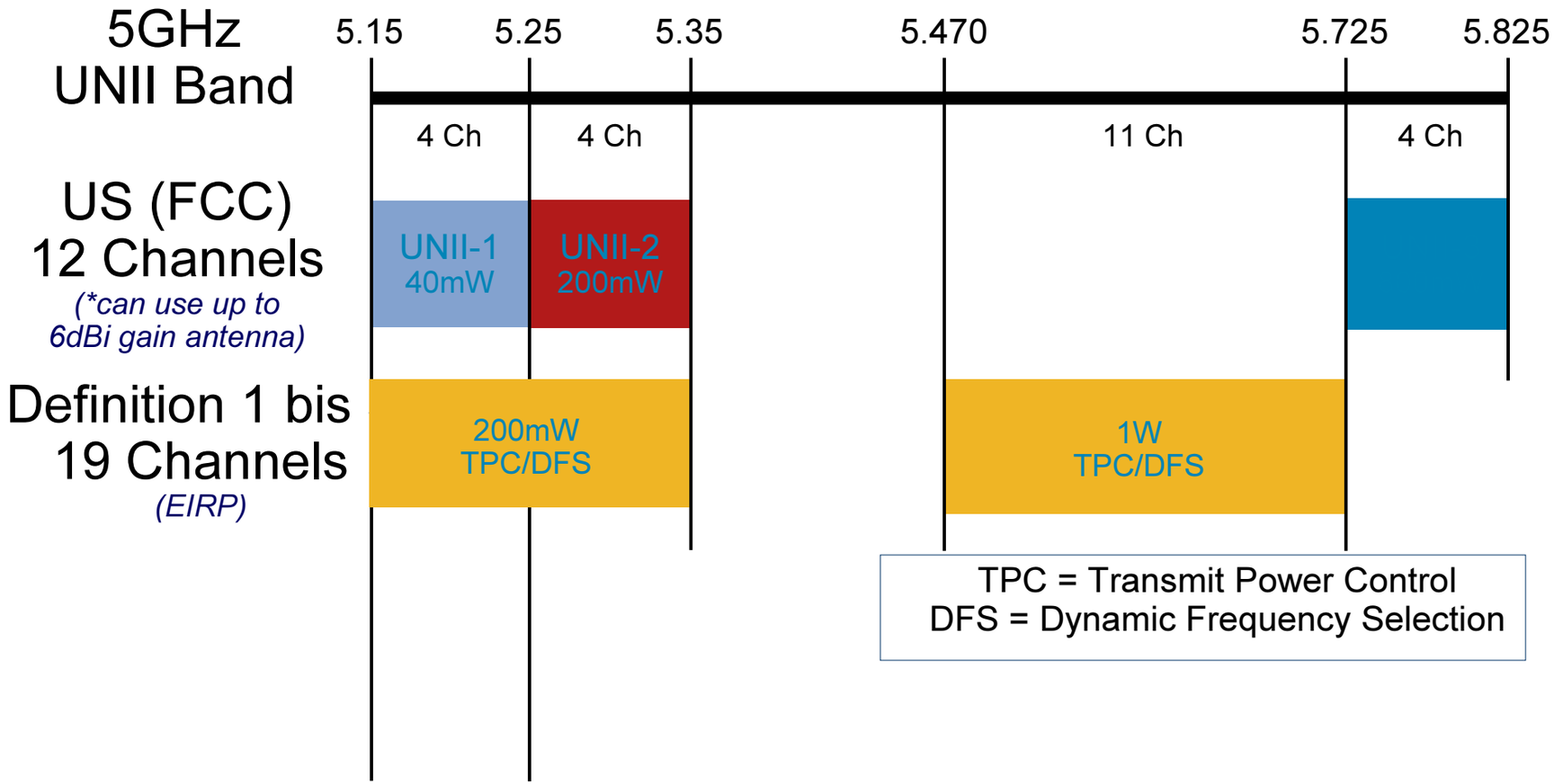
- (3) 22 MHz breite Channels (13 ETSI)
- 3 non-overlapping Channels (1, 6,11)
- 11 Mbps Data Rate / 54 Mbps bei 802.11g
- 3 Access Points oder Bridges können an einer Stelle stehen

802.11a

- Als Standard im Sept. 1999 verabschiedet
- Arbeitet im 5 GHz-Spektrum
- Daten-Raten bis zu 54 Mbps
- Unterstützung von 19 WLAN Kanälen
- Erhebliche Unterschiede in den lokalen Regulierungen

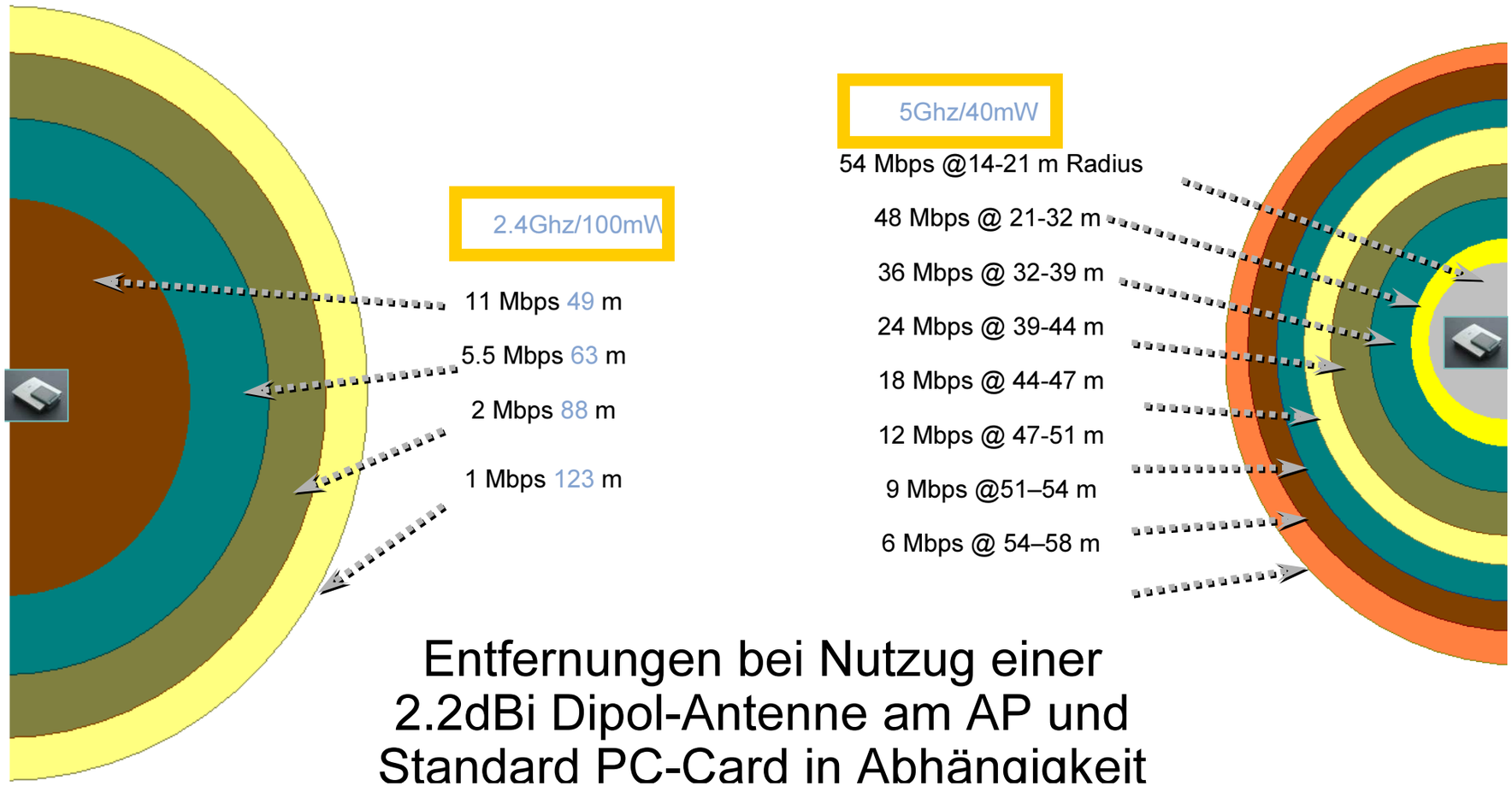


Das 5GHz Spektrum für WLAN



Reg TP Verfügung 35/2002

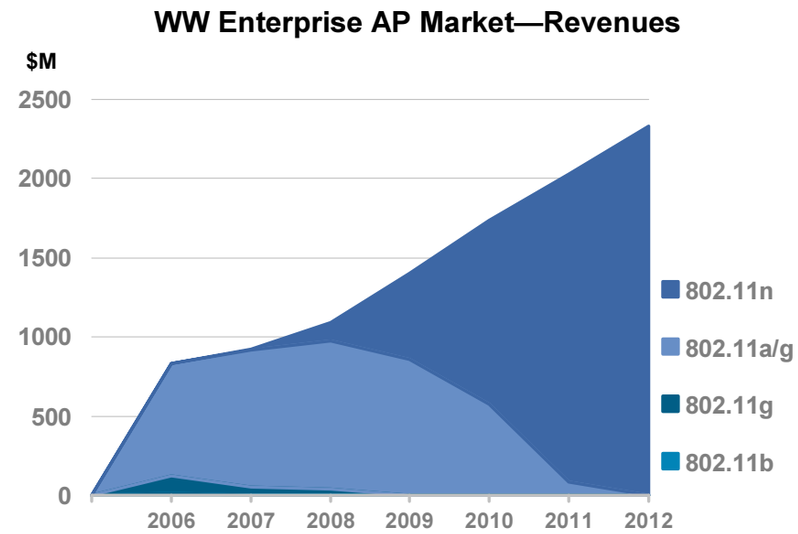
Reichweiten – Vergleich der 2 WLAN-Standards in Europa



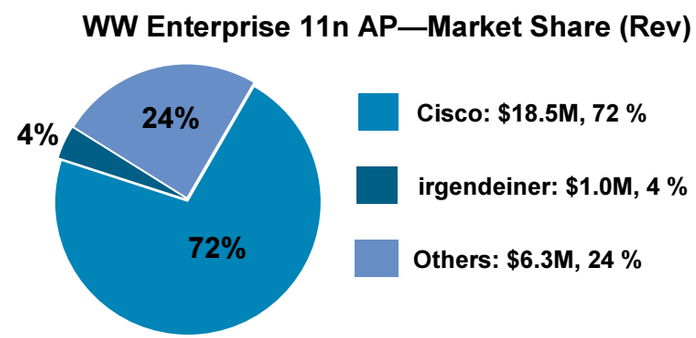
Entfernungen bei Nutzug einer 2.2dBi Dipol-Antenne am AP und Standard PC-Card in Abhängigkeit

802.11n Draft 2.0 entwickelt sich zum Marktstandard

- Mehr als 100,000 AP1250's geshipped
- Intel hat mehr als 17Mio 11n Clients ausgeliefert
- 525 Wi-Fi zertifizierte Produkte



Source: Dell'Oro Group, Q1 CY'08



Aironet AP 1250 Access Point

- Mehr Speed
  - Schnellere CPU für mehr Datendurchsatz
  - Mehr Memory für erweiterte Features
  - 10/100/1000 Ethernet Port
- Als Controller based oder Autonomer AP erhältlich

abg WiFi n DRAFT CERTIFIED®

Cisco Aironet 1140 Access Point

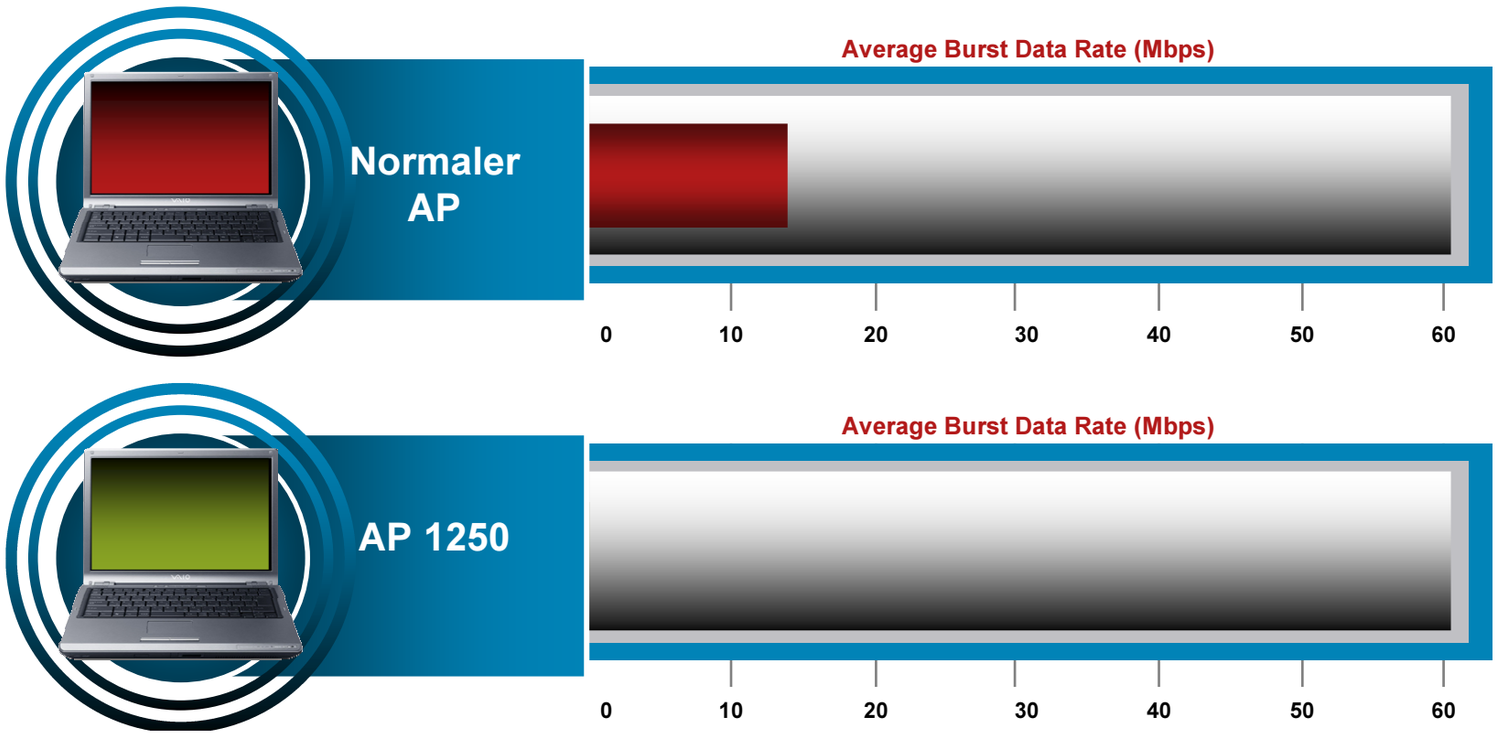
- **AP1140: einfacher zu 802.11n**
  - Garantierte Interoperabilität –WiFi zertifiziert
  - Baut auf der marktführenden Cisco 802.11n Technologie auf
  - Abwärtskompatibilität mit 802.11abg
  - Deutlicher Gewinn an Reichweite/Durchsatz auch für alte Karten
- **Einfache Installation / Energie Effizienz**
  - Ansprechendes Design mit integrierten Antennen
  - Volle 802.3af Unterstützung
  - Upgrade einer AP1130 Installation
- **RF Excellence**
  - Cisco M-Drive Technologie ist ein systemweiter Ansatz zum Management des Funk Spektrums; Verbessert WLAN Abdeckung bringt höhere Kapazität und Performance

6X Performance gg. A/G

abg WiFi n DRAFT CERTIFIED®

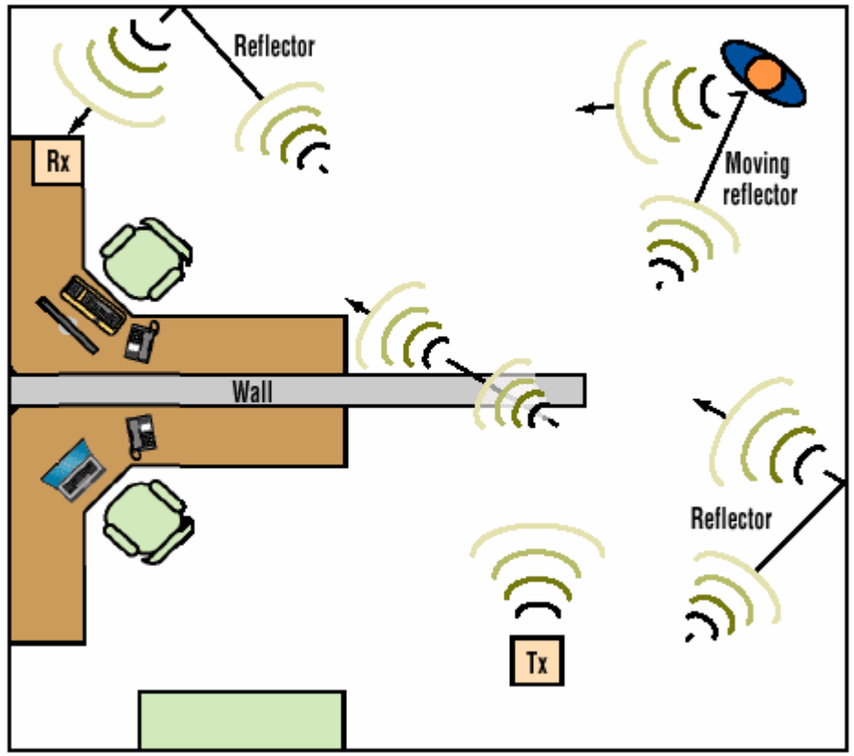
802.11n: Zuverlässigere Abdeckung

- Höherer mittlerer Durchsatz, zuverlässigere Bedingungen für alle Clients
  - höhere Zuverlässigkeit, bessere Nutzer Erfahrung
  - Vorhersehbarer Durchsatz auch in schwierigen Situationen



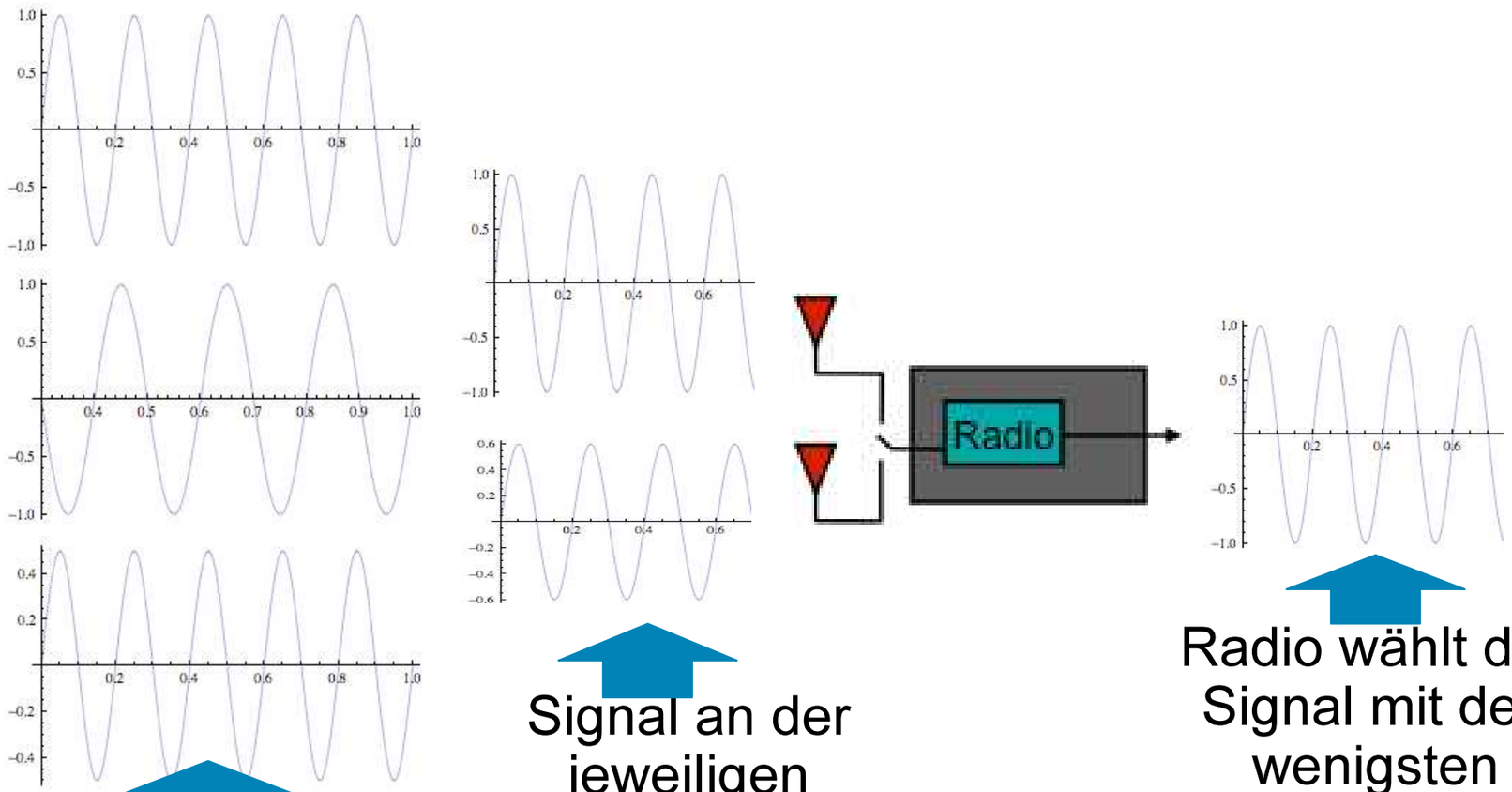
MIMO – Multi Inputs, multiple Outputs

- MIMO nutzt Reflexionen



Reflexionen in einer normalen Büroumgebung
- aber auch unter schwierigen Umständen

Multipath Reflektion bei einem SISO AP

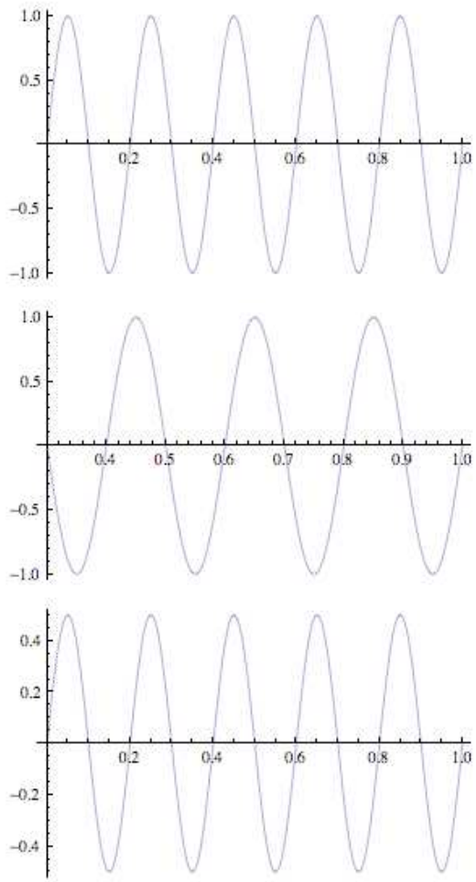


Multipath Reflektionen des

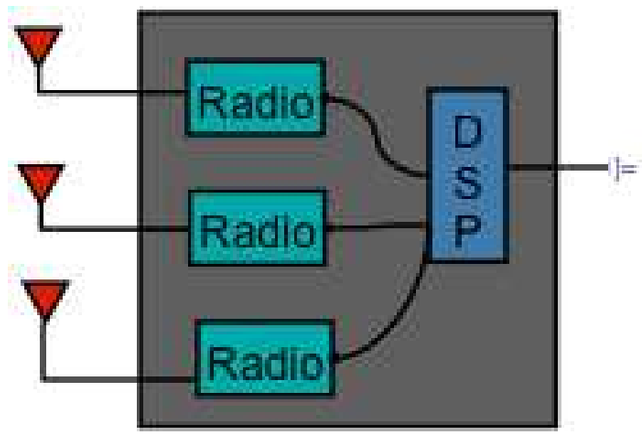
Signal an der jeweiligen Antenne

Radio wählt das Signal mit den wenigsten Multipath Effekten aus

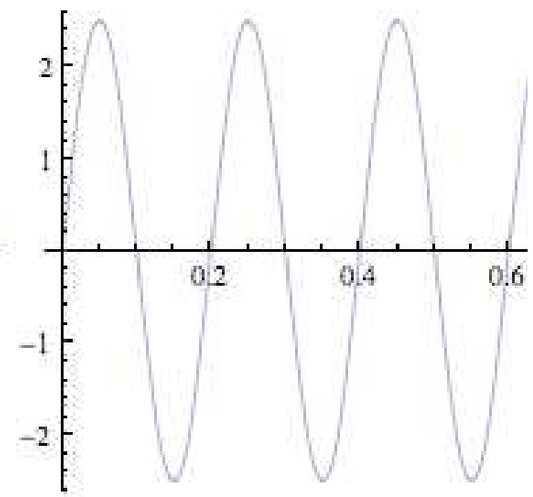
Multipath Reflektionen bei einem MIMO AP



Multipath Reflektionen des



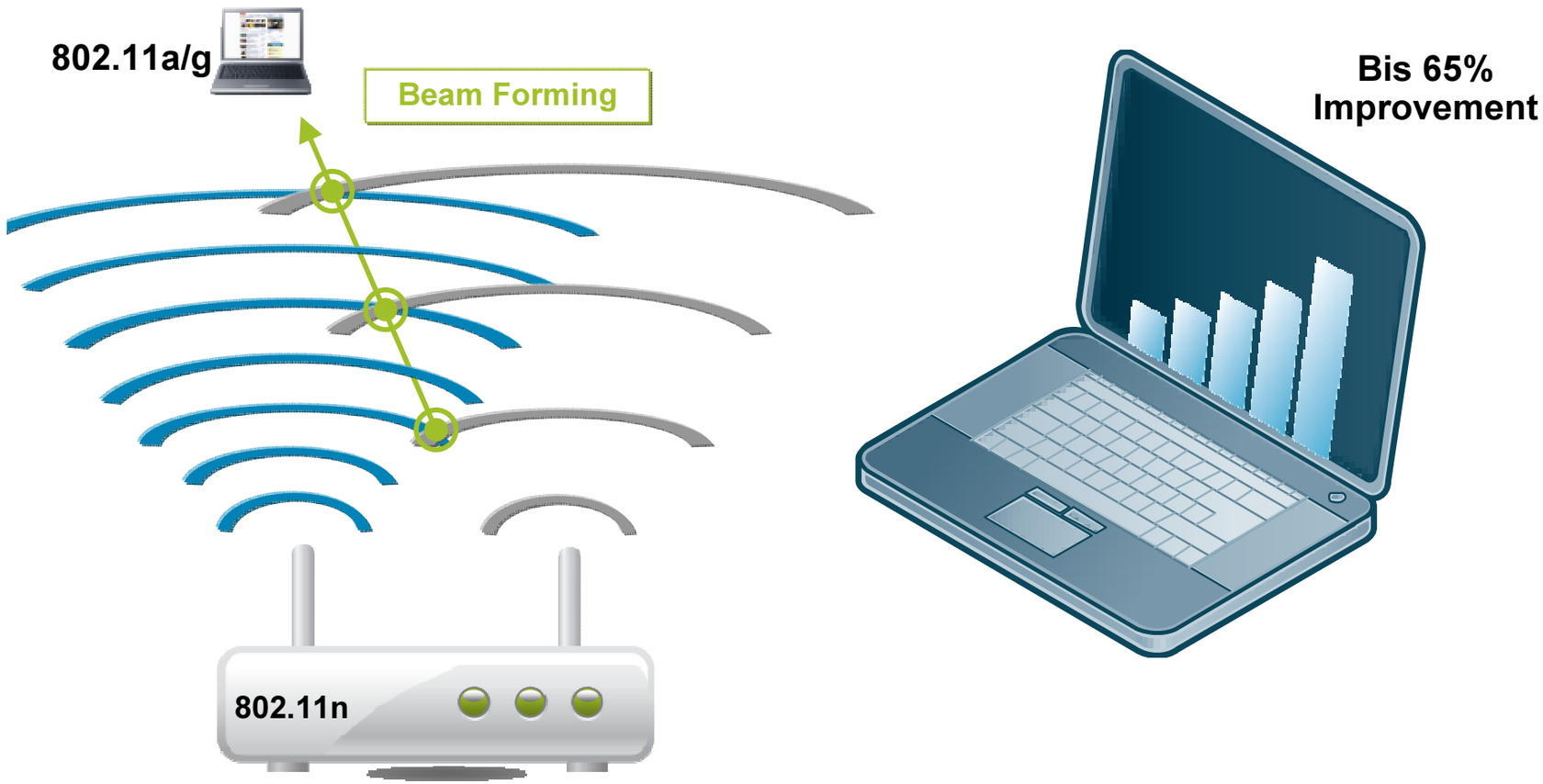
DSP rechnet die Signale zusammen



Das resultierende Signal ist die Addition der empfangenen

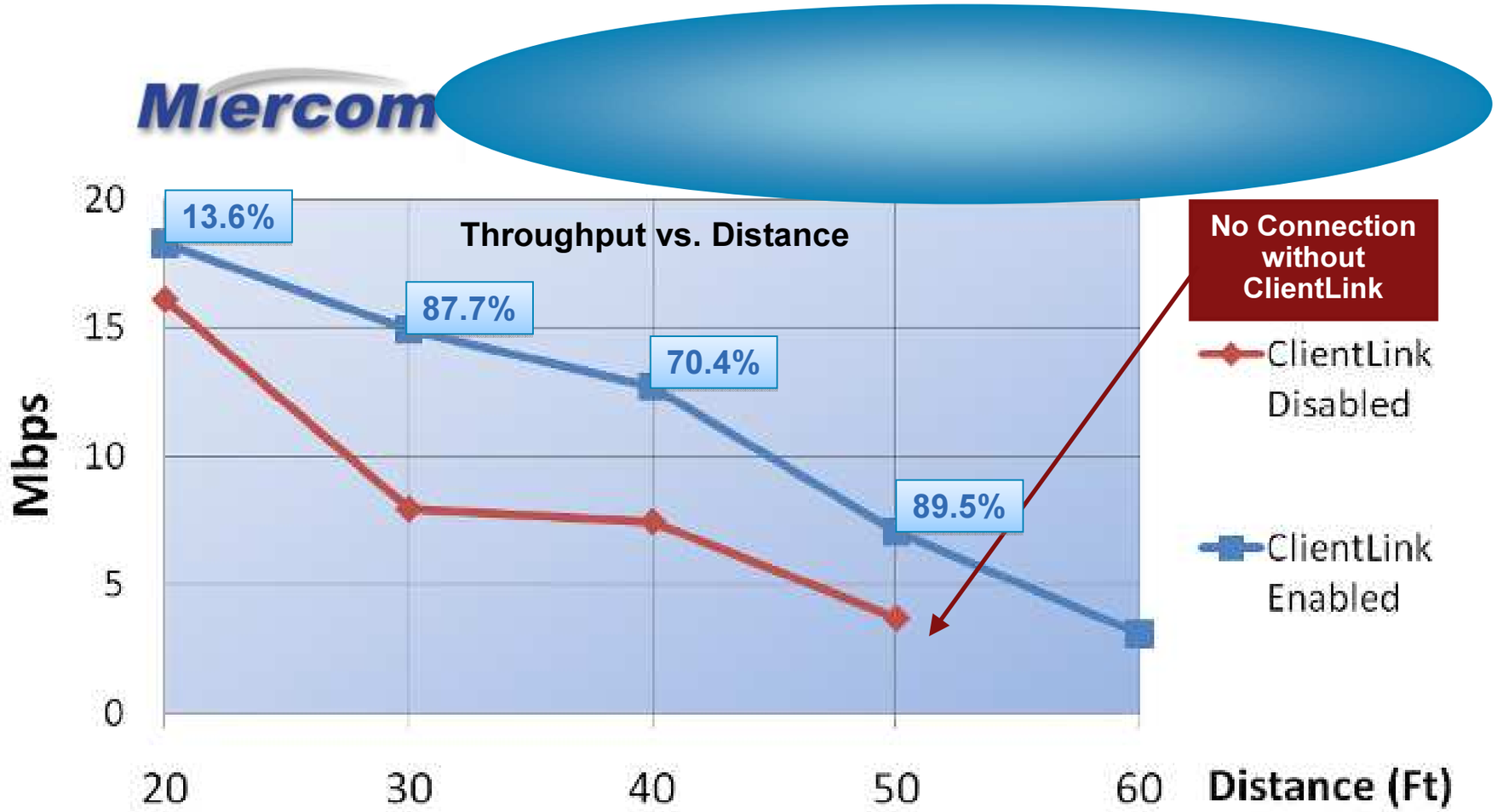
M-Drive mit ClientLink

Cisco Innovation: Beam Forming



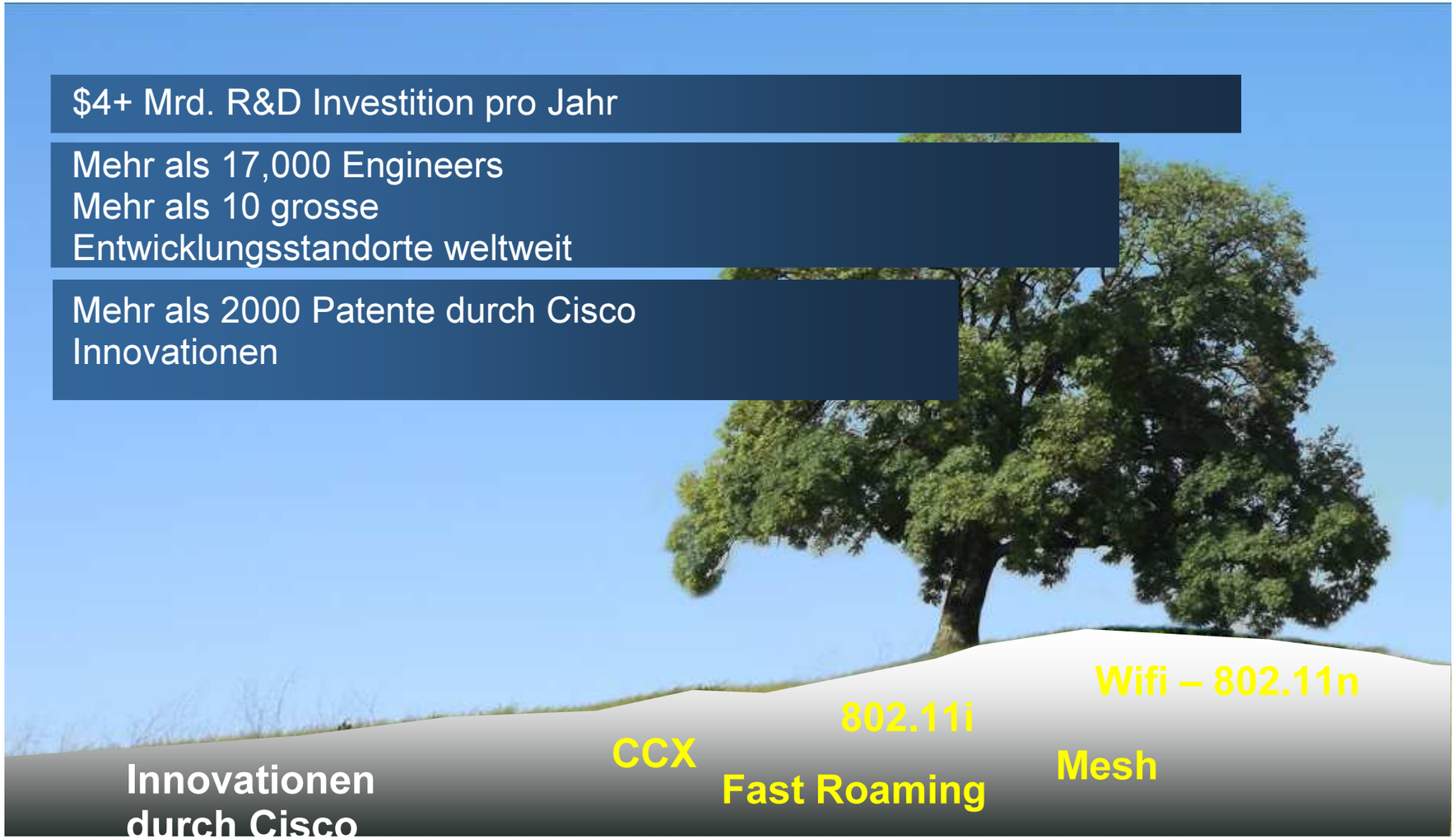
Intelligentes Beam Forming richtet das Signal aus um die Performance und Coverage für 802.11a/g Devices zu verbessern

Mehr Durchsatz für 802.11a/g Devices



Test: 802.11a/g device with 802.11n network

Cisco als Technologie Innovator



CISCO