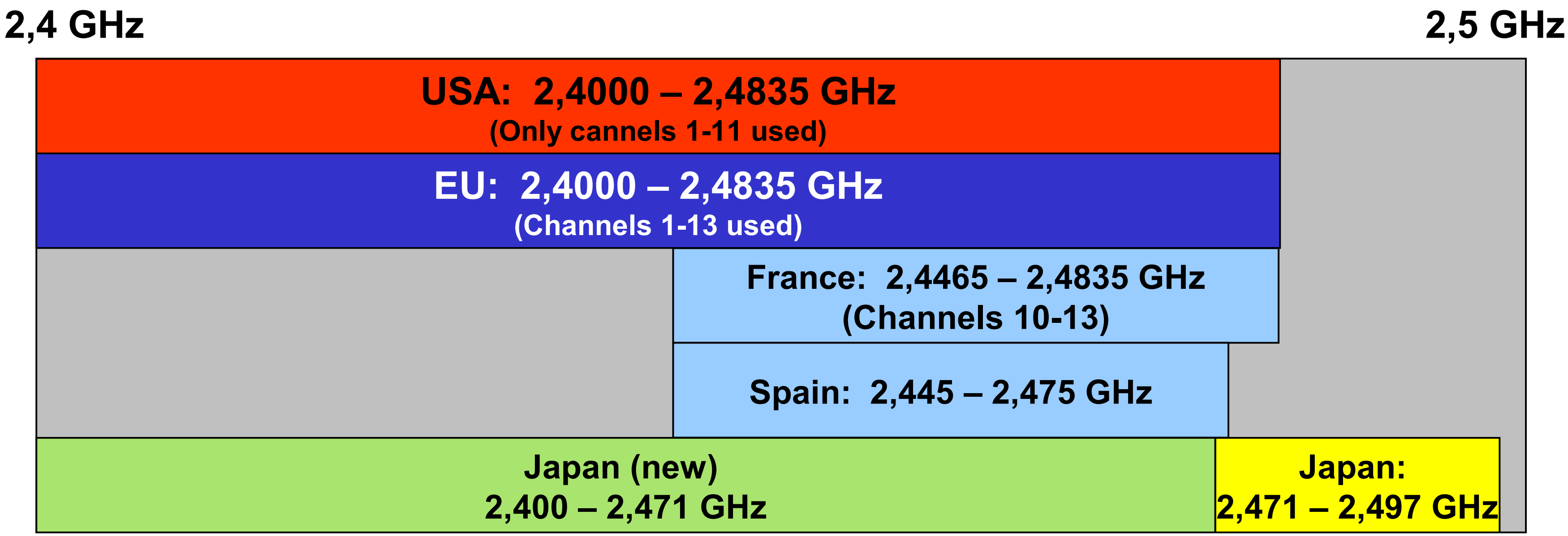
WLAN

Physically

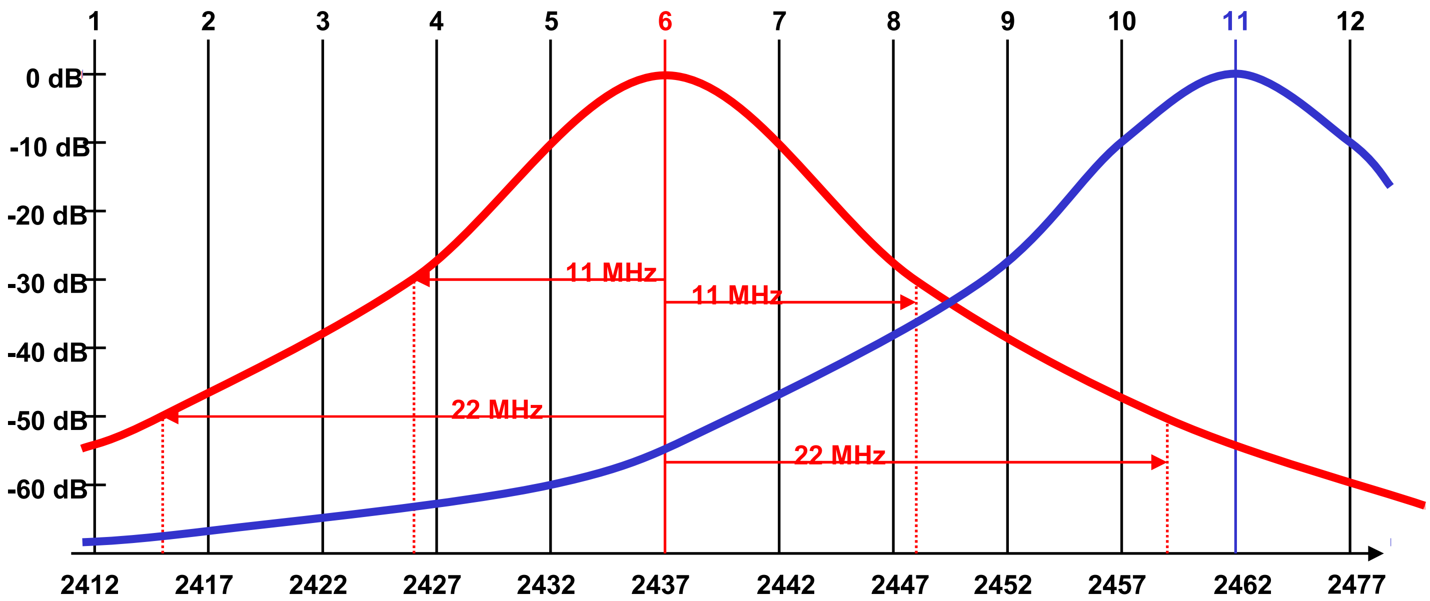
2,4 GHz (802.11b/g) Frequency Overview



- 2.4 GHz ISM band is nearly "the same" world-wide
  - Still ongoing equalization efforts in certain countries
  - Much better than 5 GHz ISM band
- Restrictions only for spread spectrum devices

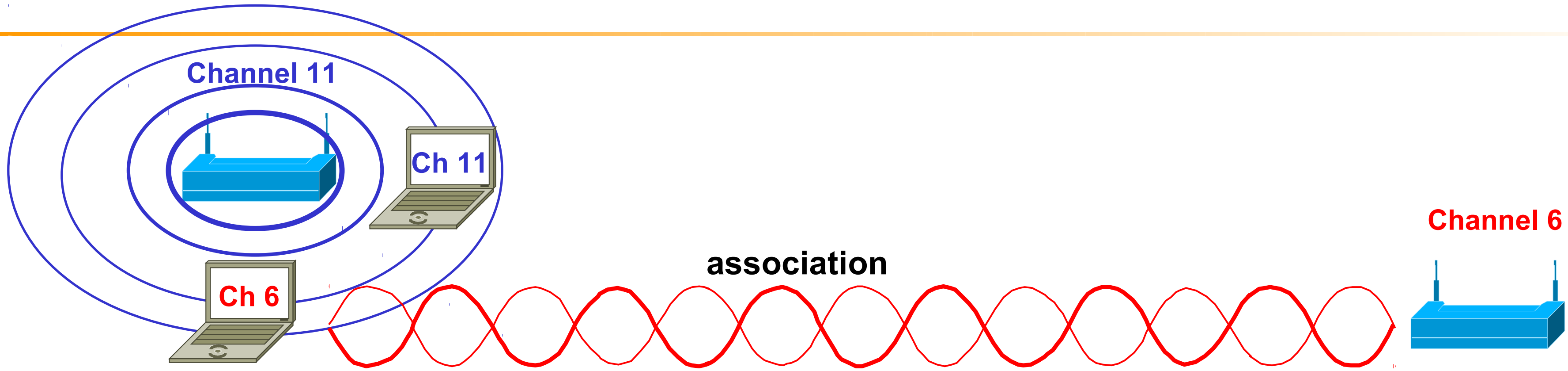
Austria: 100 mW for both 802.11b and 802.11g allowed.
Vendors (and certain countries) may limit the 802.11g power because of high crest factors (typically: 30 mW = 15 dBm max TX power)

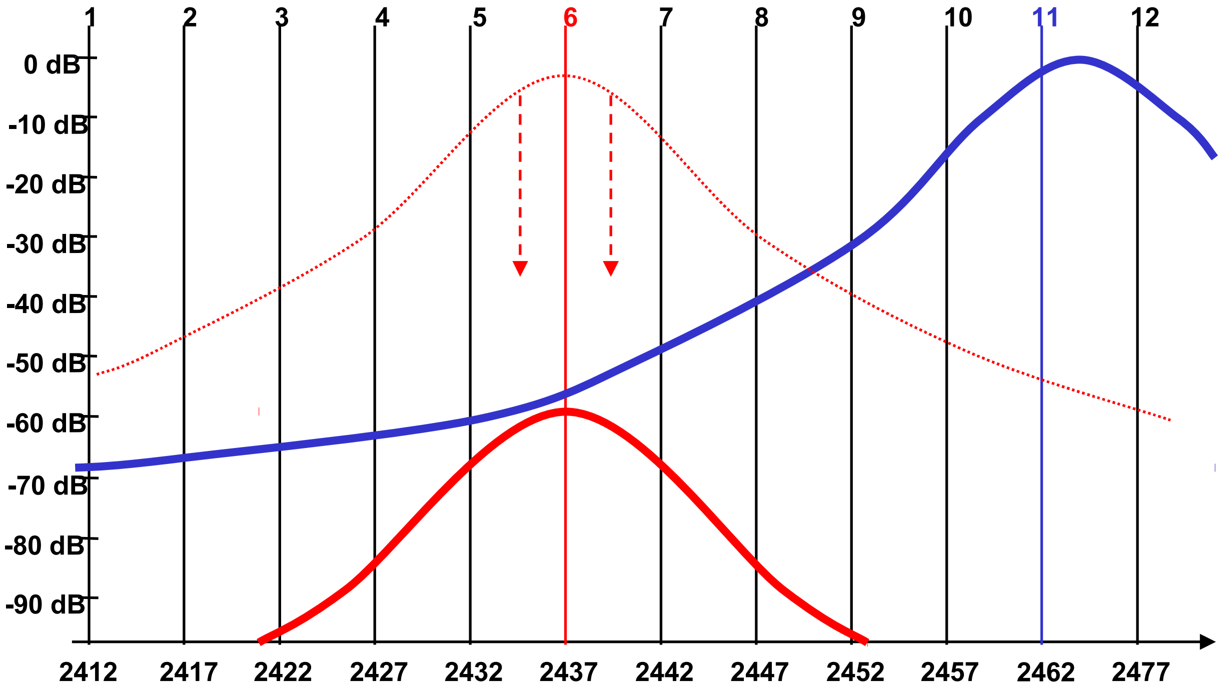
Real Channel Overlapping (2.4 GHz)



- **IEEE 802.11b/g only specifies center frequencies and a spectral mask**
  - **802.11b spectral mask requires that the signal be at least 30 dB down from its peak energy at ±11 MHz from the center frequency and at least 50 dB at ±22 MHz**
- **Therefore, actually ALL channels overlap**
  - **Even the "non-overlapping" channels 1, 6, and 11**
  - **Might be a problem with significant TX-power differences**

The Near/Far Problem





- **Foreign stations are closer and therefore "louder" than distant peer**
- **Only a problem if:**
  - **Stations are very sensitive**
  - **No roaming possible**

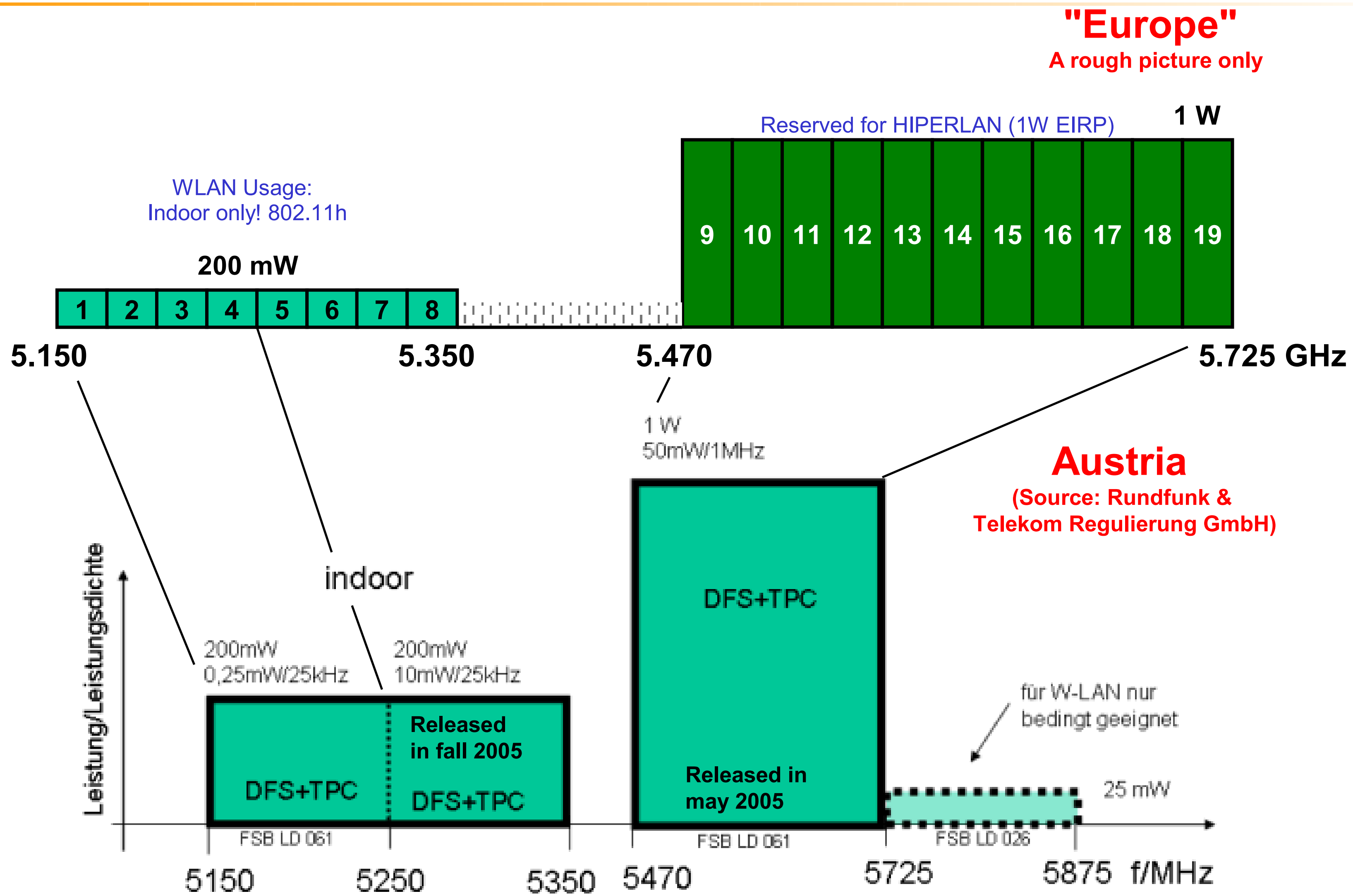
802.11h: TPC and DFS

- ETSI requires TPC and DFS for 5 GHz bands
  - Otherwise only very limited powers allowed
- Transmit Power Control (TPC)
  - Reduces TX power if possible
  - Provides minimum required TX power for *each* user
  - Assures minimal interference
- Dynamic Frequency Selection (DFS)
  - Enables transmitter to move to another channel when it encounters 'Primary Applications' on its channel
  - Basically designed to avoid interferences with military RADAR
  - Interference Threshold I_{th} = −62 dBm/MHz is the maximum aggregate interference (as sensed by a node) allowed for channel access

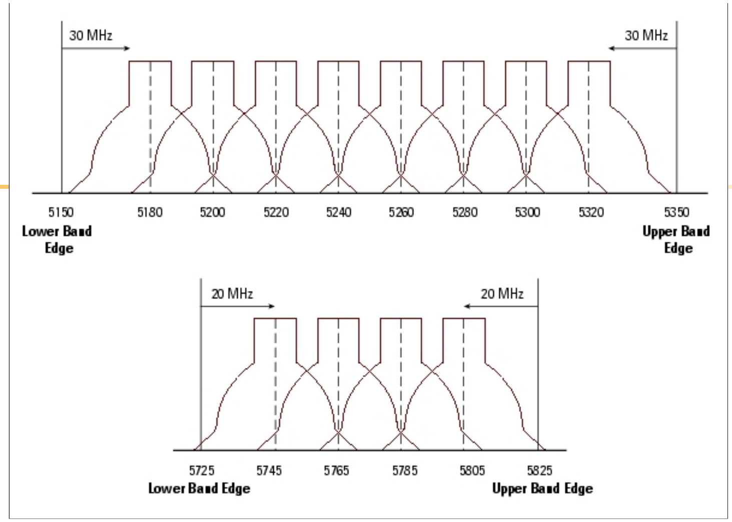
DFS Details

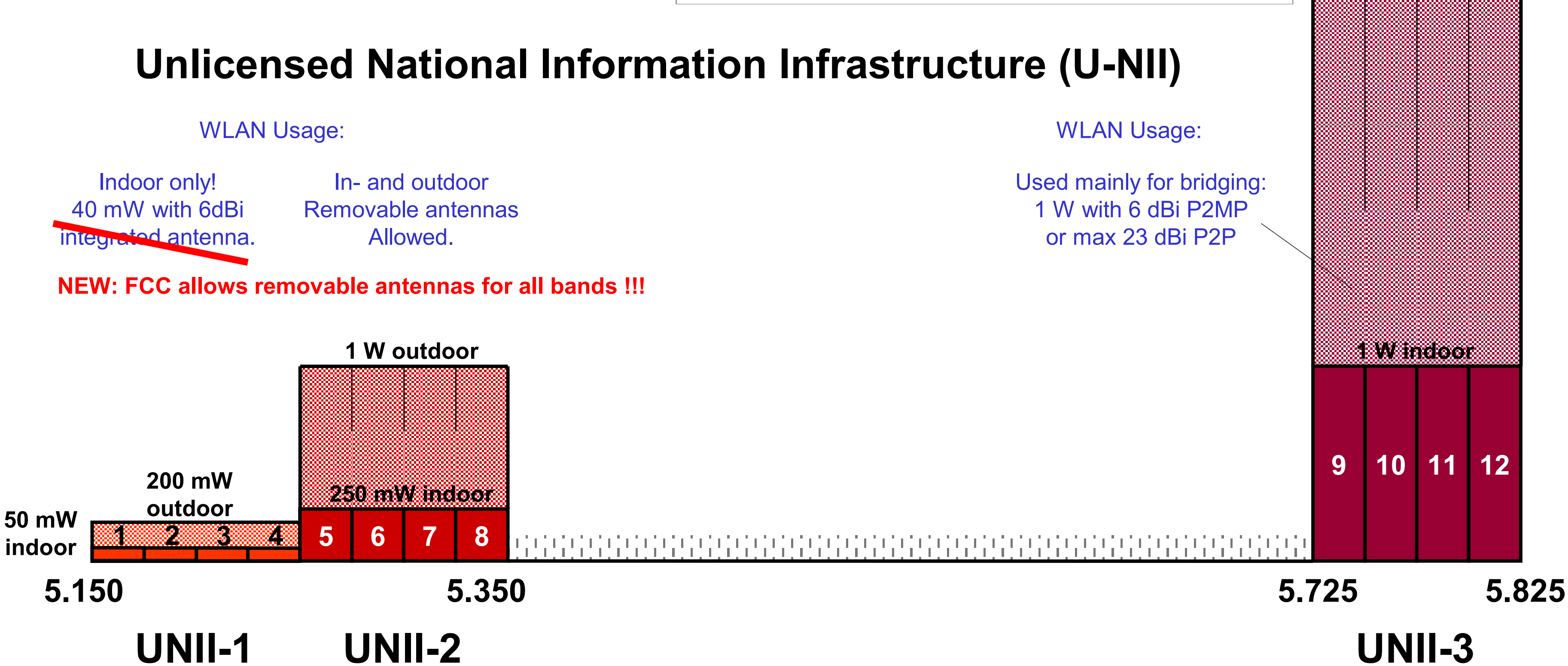
- Non-Occupancy Time: 30 min
  - The time a channel must not be used
- Channel Availability Check: 60 sec
  - Time before using a channel
- Channel Move Time: 10 sec
  - Must leave a channel within that time in case of radar detection
- Channel Closing Transmission Time: 260 msec
  - Total transmission time of certain management traffic during the Channel Move Time (Beacon and Probe Responses)
  - No data traffic within the Channel Move Time!

ISM 5 GHz – Europe [Jan 2007]

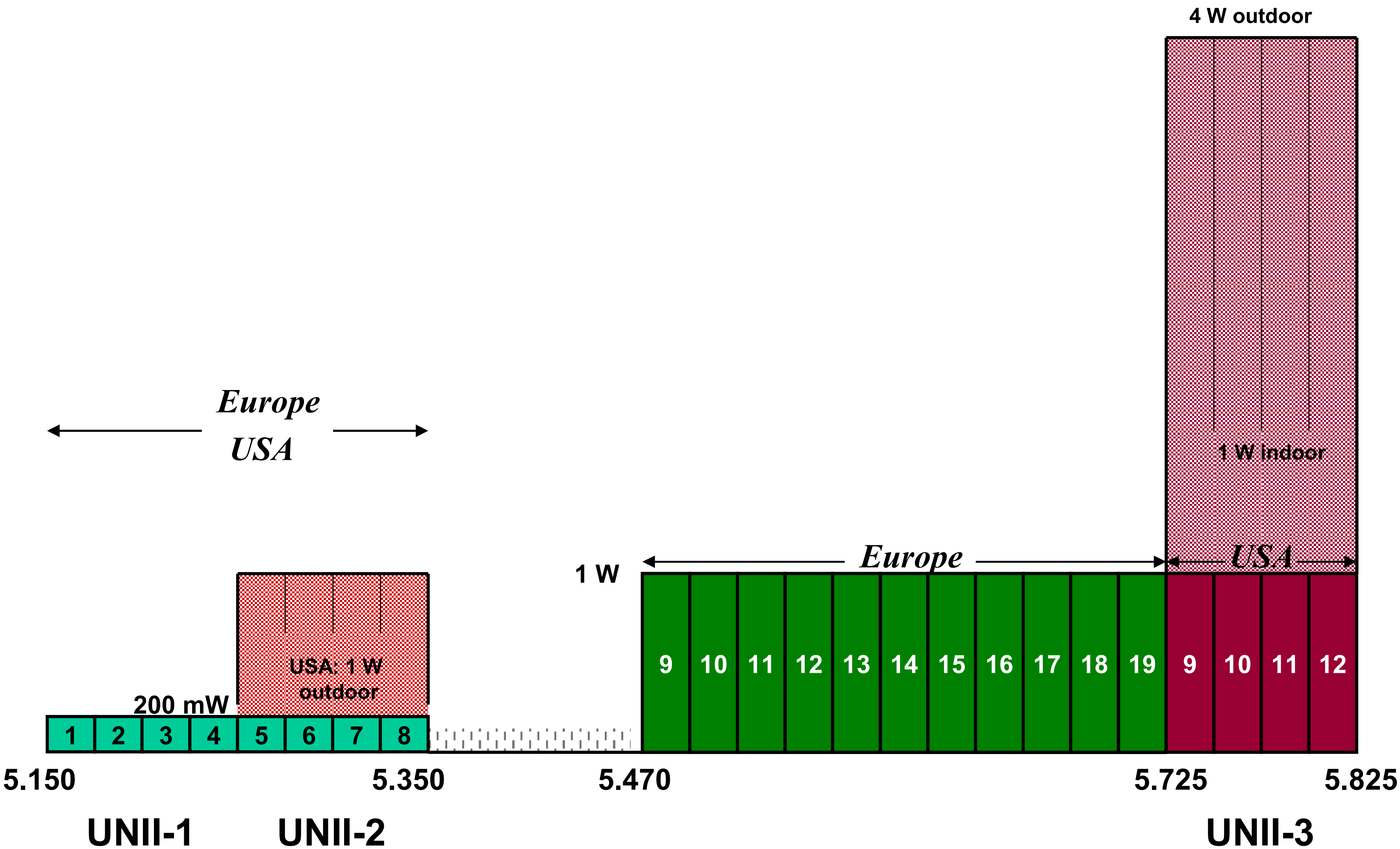


ISM 5 GHz – USA


30 MHz
30 MHz
5150
Lower Band Edge
5180
5200
5220
5240
5260
5280
5300
5320
5350
Upper Band Edge
20 MHz
20 MHz
5725
5745
5765
5785
5805
5825
Lower Band Edge
Upper Band Edge


4 W outdoor
Unlicensed National Information Infrastructure (U-NII)
WLAN Usage:
Indoor only!
40 mW with 6dBi
integrated antenna.
In- and outdoor
Removable antennas
Allowed.
WLAN Usage:
Used mainly for bridging:
1 W with 6 dBi P2MP
or max 23 dBi P2P
NEW: FCC allows removable antennas for all bands !!!
1 W outdoor
1 W indoor
200 mW
outdoor
250 mW indoor
50 mW
indoor
1
2
3
4
5
6
7
8
9
10
11
12
5.150
5.350
5.725
5.825
UNII-1
UNII-2
UNII-3

5 GHz Comparison EU/USA



Regulatories & Law

Germany: www.regtp.de

Regulierungsbehörde für Telekommunikation und Post

Austria: www.rtr.at

Rundfunk & Telekom Regulierungs-GmbH

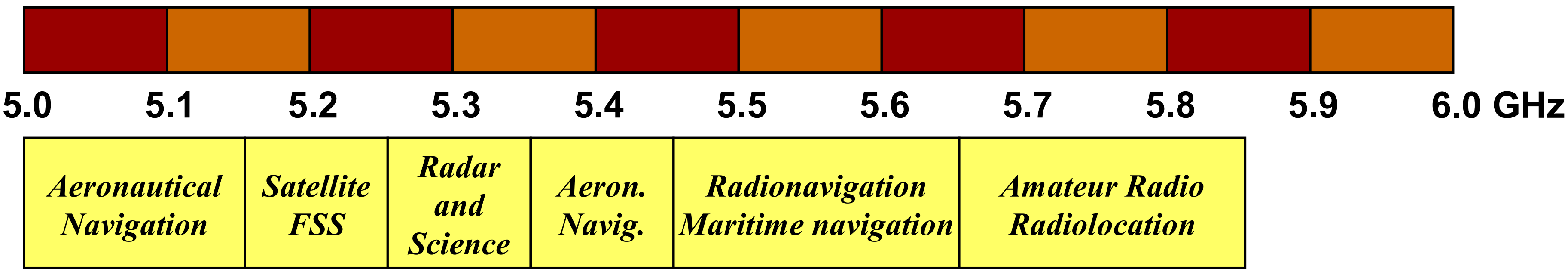
RTR

USA: www.fcc.gov

FCC Federal Communications Commission

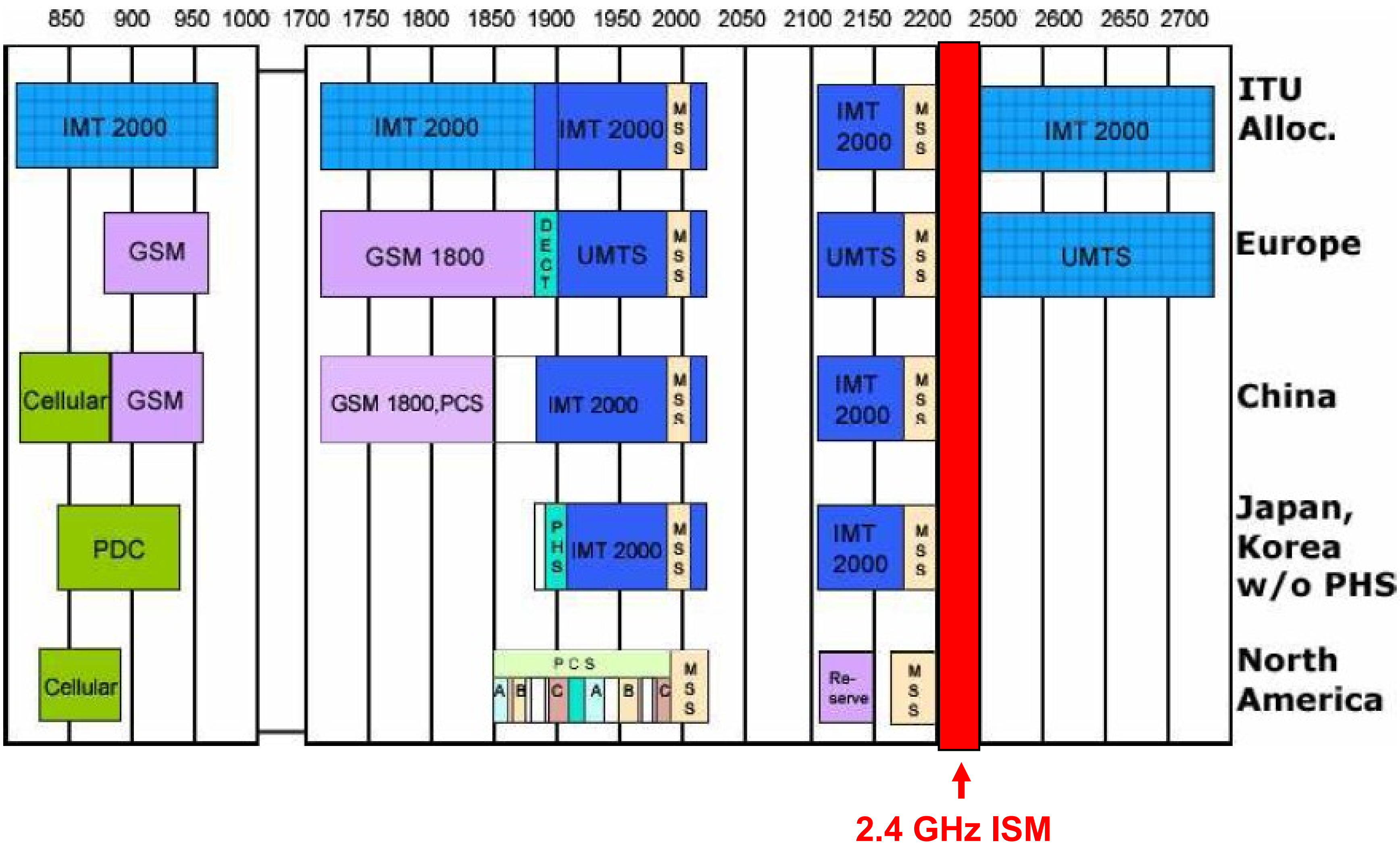
- **WLAN senders *may* radiate beyond premises borders**
  - **Directional antennas which are used to get over a foreign premise *should* be announced (Austria, Germany)**
  - **Therefore still legal problems to sue layer-1 based DoS attacks**

802.11d – "World Mode"

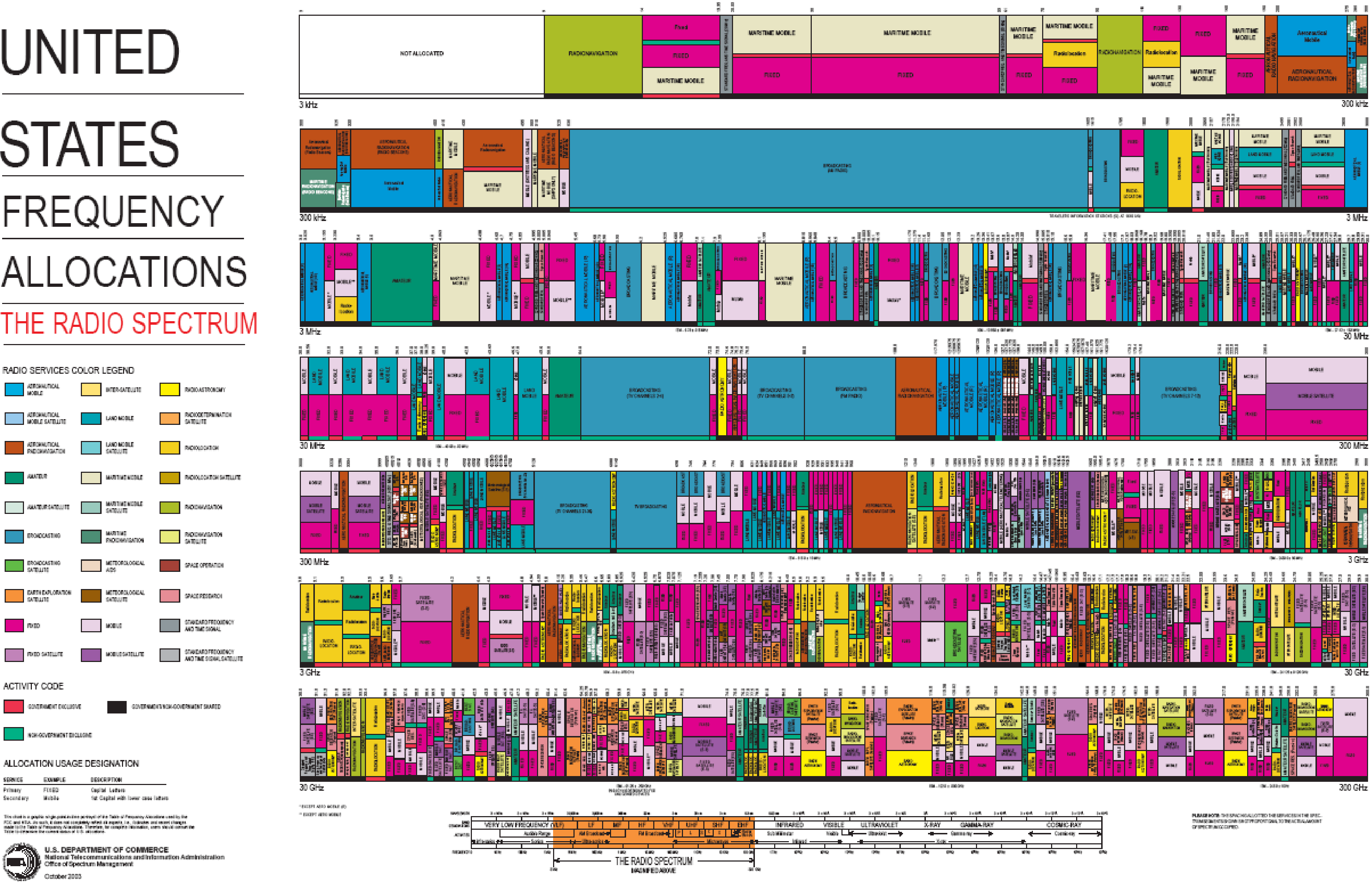


- "Extensions to Operate in Additional Regulatory Domains"
  - Ratified in June, 2001
  - Defines frequency and power limitation for different regulatory domains
- Allows clients to roam across different regulatory domains
  - APs are set to appropriate regulatory domain
  - During association, clients inherit the power and frequency requirements of this regulatory domain

"Surrounding" Applications

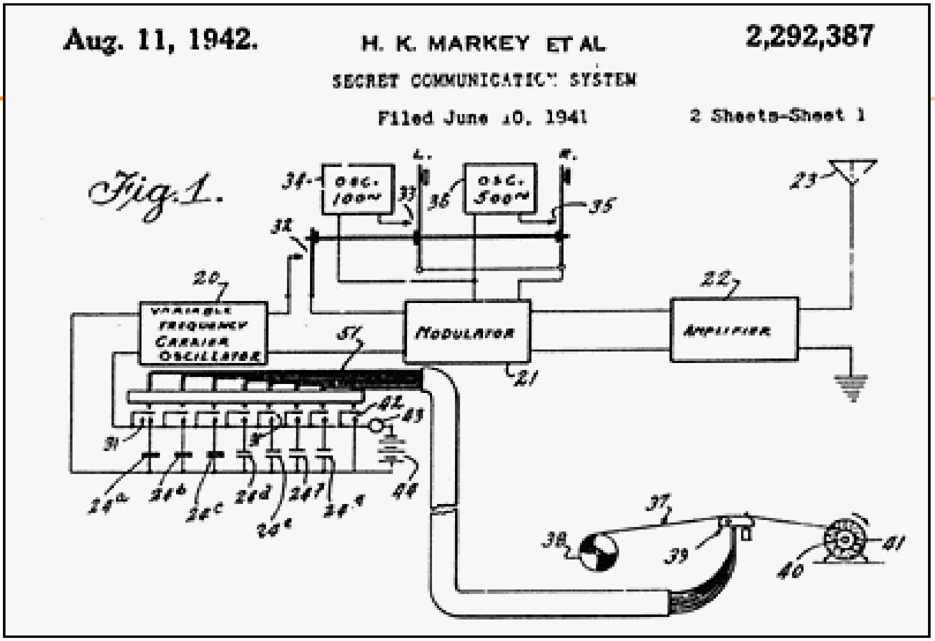


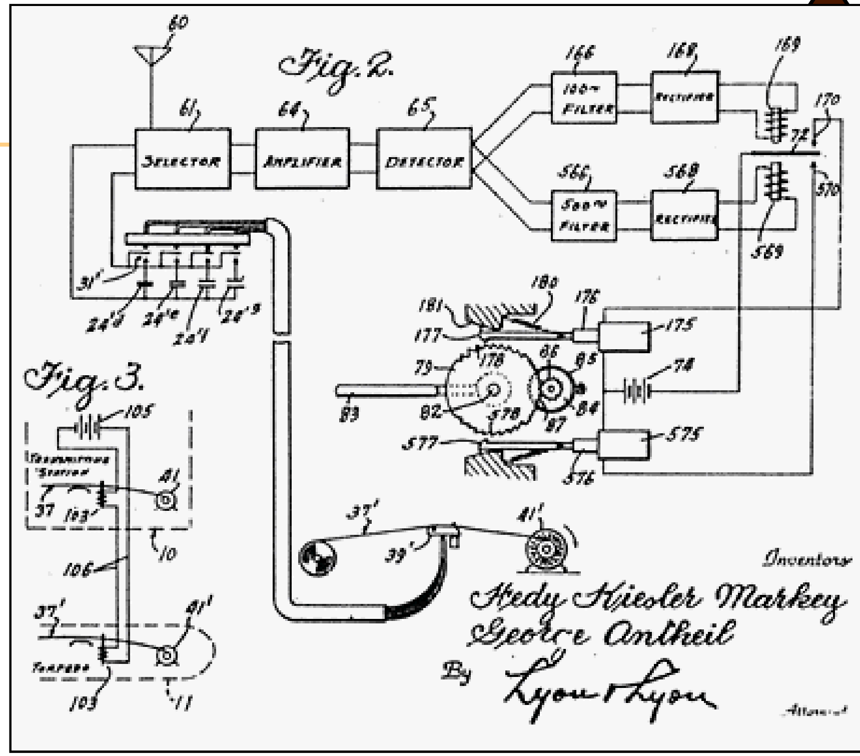
US Frequency Plan (3 kHz – 300 GHz)



Modulation Techniques

Spread Spectrum Basics
FHSS vs. DSSS
QAM Variants and CCK
OFDM





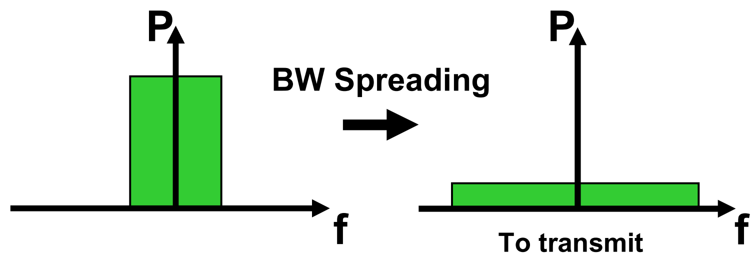
UNITED STATES PATENT OFFICE 2,292,387
SECRET COMMUNICATION SYSTEM
Hedy Kiesler Markey, Los Angeles, and George Antheil, Manhattan Beach, Calif.
Application June 10, 1941, Serial No. 397,412 6 Claims. (Cl. 250-2)

This invention relates broadly to secret communication systems involving the use of carrier waves of different frequencies, and is especially useful in the remote control of dirigible craft, such as torpedoes.
An object of the invention is to provide a method of secret communication which is relatively simple and reliable in operation, but at the same time is difficult to discover or decipher.

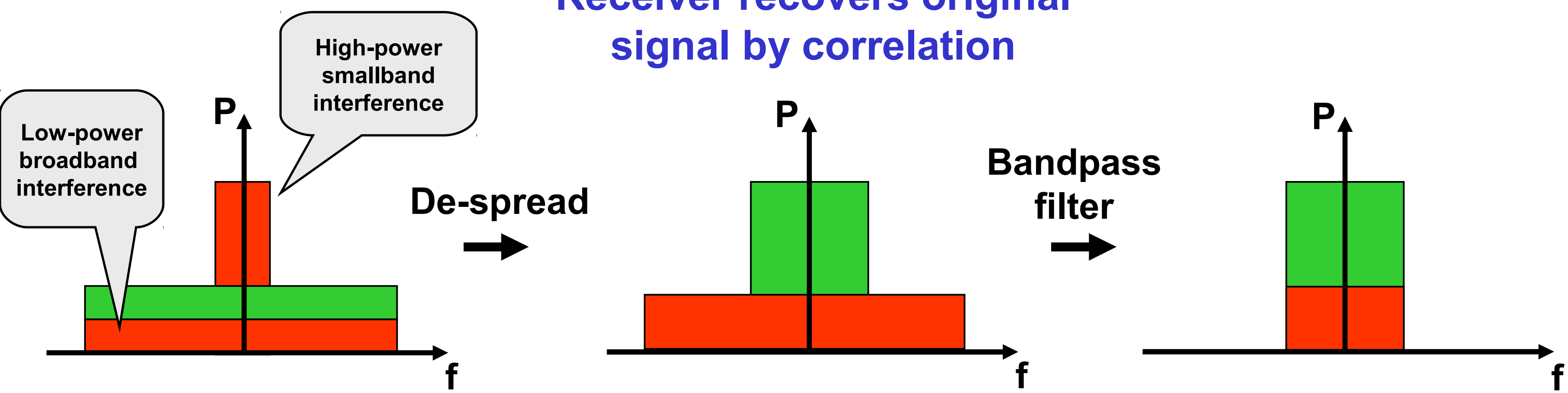
Why Bandwidth Spreading?

- If input power is spread over a large band: hard to intercept
- The noise is reduced (compared to the noise in the total bandwidth used) by the spreading gain $\gamma_c = \frac{T}{T_c}$
- To synchronize, we multiply with all possible shifted versions of the PN sequence
- Fast auto-correlation needed

Sender reduces spectral power density but conserves total energy:



Receiver recovers original signal by correlation



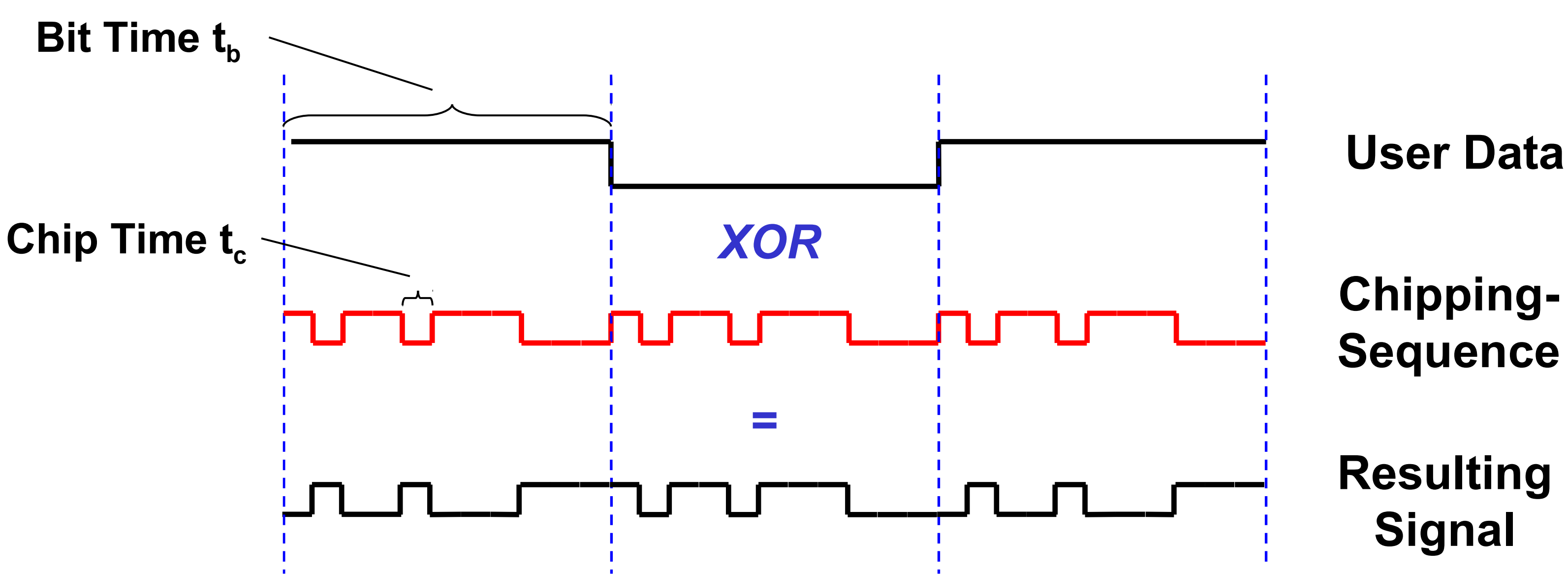
Bandwidth Spreading Methods

- **Direct Sequence Spread Spectrum (DSSS)**
  - 802.11b/g: 14 possible channels – 3 channels can be used simultaneously
  - Can operate with SNR of 12dB
  - Throughput up to 11 Mbit/s (and more)
  - Range up to 40 km (and more)
- **Frequency Hopping Spread Spectrum (FHSS)**
  - 802.11: 79 possible channels – 15 channels can be used simultaneously
  - Can operate with SNR of 18dB
  - Interference tolerant
  - Less multipath problems
  - Technically limited up to 2 Mbit/s
- **OFDM (Multicarrier Modulation)**
  - Actually used to minimize the required bandwidth but often referred as spreading technique in the WLAN context

DSSS

- User bit-pattern is modulated (substituted) with chipping-sequence (“Barker code“)
  - Each bit of data is encoded by 11 bits of the chipping sequence
  - 802.11b: 22 MHz modulation bandwidth

Chipping Sequence: 10110111000 (Barker Code*)

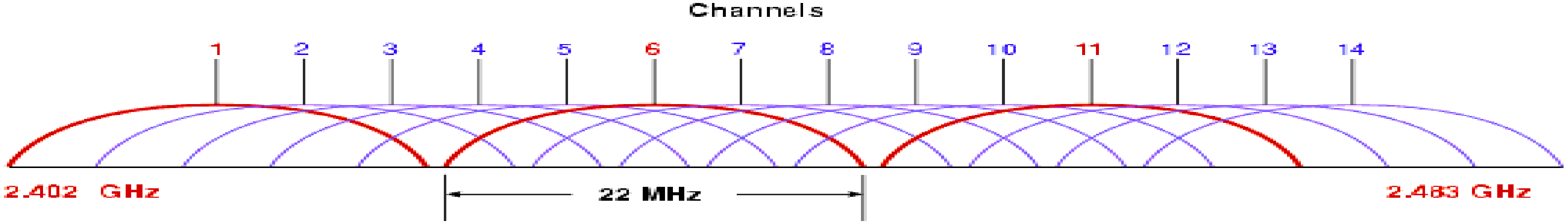


Codes Used

Data Rate	Code Lenght	Modulation	Symbol Rate	Bits/Symbol
1 Mbps	11 (Barker)	DBPSK	1 MSps	1
2 Mbps	11 (Barker)	DQPSK	1 MSps	2
5.5 Mbps	8 (CCK)	DQPSK	1.375 MSps	4
11 Mbps	8 (CCK)	DQPSK	1.375 MSps	8

- **For 5.5 and 11 Mbps data rates, Barker sequences are not used**
- **Instead Complementary Code Keying (CCK) is used (64 8-bit code words)**

802.11b DSSS Channels



Channel	Frequency	Americas	EMEA	Israel	Japan
1	2412	X	X	-	X
2	2417	X	X	-	X
3	2422	X	X	X	X
4	2427	X	X	X	X
5	2432	X	X	X	X
6	2437	X	X	X	X
7	2442	X	X	X	X
8	2447	X	X	X	X
9	2452	X	X	X	X
10	2457	X	X	-	X
11	2462	X	X	-	X
12	2467	-	X	-	X
13	2472	-	X	-	X
14	2484	-	-	-	X

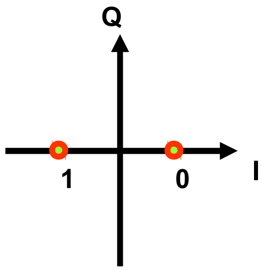
FHSS

- Available bandwidth spilt into several smaller channels with smaller bandwidth
- Sender and receiver uses one of this smaller channels for a part of time, then jump to next one
  - Pseudo-random jump sequence
  - Avoids being stuck in a bad frequency band
  - Slow hopping: multiple bits before frequency hop
  - Fast hopping: multiple frequency hops per bit
- On multi-access media, collisions are only rare
- ISM bandwidth (2.4 GHz) = 83 MHz is divided into 1 MHz channels for FHSS
- FCC requires that any FHSS radio must visit at least 79 of the channels at least once in 30 seconds
  - Minimum hop rate: 2.5 hops/second

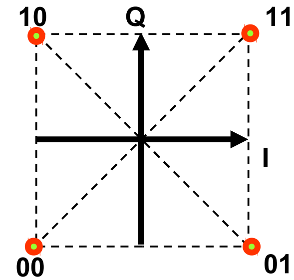
Note: The original 802.11 implementations only used FHSS, but it is still used in critical environments today (airports etc)

QAM

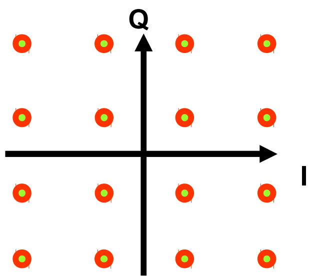
Standard PSK



Quadrature PSK (QPSK)

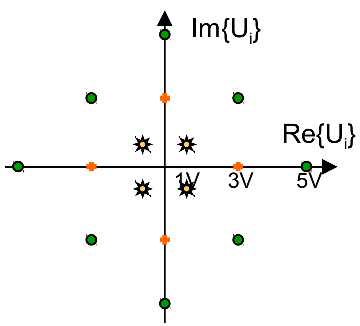


16-QAM



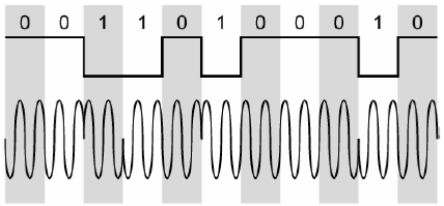
Other example:
Modem V.29

2400 Baud
Max. 9600 Bit/s



- 802.11a and Hiperlan
  - Wireless Medium: OFDM
  - BPSK @ 6 and 9 Mbps
  - QPSK @ 12 and 18 Mbps
  - 16-QAM @ 24 and 36 Mbps
  - 64-QAM @ 48 and 54 Mbps
- 802.11b
  - Wireless Medium: DSSS
  - DBPSK @ 1 Mbps
  - DQPSK @ 2 Mbps
  - 16 CCK @ 5.5 Mbps
  - 256 CCK @ 11 Mbps

DBPSK: Only "1" causes periodic phase shifts.

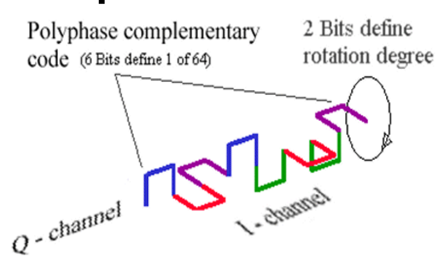


CCK

- Based on Marcel J. E. Golay (1951) polyphase complementary codes
  - Has ideal AKF properties
- Complex codes
  - 6 bits of each byte select one of 64 unique orthogonal eight chips long polyphase complementary codes
  - The other two bits rotate the whole code word (0, 90, 180 or 270 degrees)
- 8 chips => 1 symbol hence 1,375 Mbaud => 11 Mchips/s
- Symbol is a 8-dimensional vector with complex components:

$$X = \{e^{j(\phi_1+\phi_2+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_3+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_4)}, -e^{j(\phi_1+\phi_4)}, e^{j(\phi_1+\phi_2+\phi_3)}, e^{j(\phi_1+\phi_3)}, -e^{j(\phi_1+\phi_2)}, e^{j\phi_1}\}$$

  - Data bits encode component phases using DQPSK
  - Φ_1 is contained in all 8 chips => rotates the vector
- Same spectrum shape as with Barker code words



Example:

Assuming that the bits of a 8-bit word control the phase components according

d1	d0	φ1
d3	d2	φ2
d5	d4	φ3
d7	d6	φ4

and the following QPSK specification is true

0	0	0
0	1	π
1	0	π/2
1	1	-π/2

then the codeword

10110101

transforms into

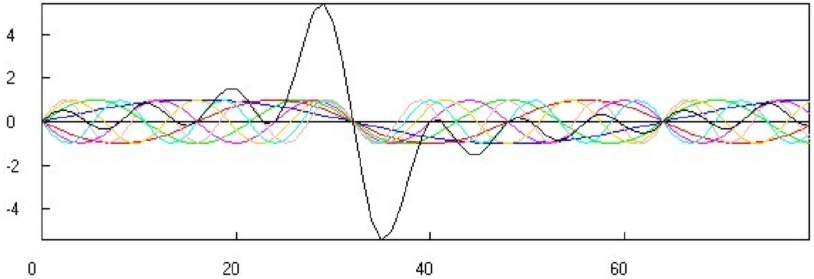
{1,-1, j, j, -j, j, -1,-1}

OFDM

- Orthogonal Frequency Division Multiplexing (OFDM)
  - Avoids multipath-induced interferences that always occur at higher symbol rates
  - 1966: Chang (Bell Labs) issued OFDM paper and patent
  - 1993: Morris implemented first experimental OFDM WLAN at 150 Mbit/s
- Basic idea:
  - 1) Split data stream in multiple lower-rate streams
  - 2) Convert n bits into m QAM symbols
  - 3) Regard the m QAM symbols as discrete complex spectrum and convert it into the time domain via FFT^{-1}
    - The m complex QAM symbols must be "mirrored" appropriately in order to get real-valued time-domain values (hint: amplitudes even, phase odd)
  - Each element of the "QAM-vector" can be interpreted as a subchannel
- Subchannels overlap!
  - Approx. 50% less total bandwidth necessary than FDM
  - ISI is minimized because of orthogonal sub-bands
  - Equivalent to Nyquist-pulses in time domain

OFDM – 802.11a Details (1)

- Channel BW is 20 MHz (occupied BW is 16.6 MHz)
  - 52 subcarriers are used per channel
  - 48 subcarriers carry the data
  - 4 subcarriers are pilots which facilitate phase tracking for coherent demodulation
  - Subcarrier separation: 312,5 kHz (20 MHz/64)
- Each of these subcarriers can be a BPSK, QPSK, 16-QAM or 64-QAM coded signal

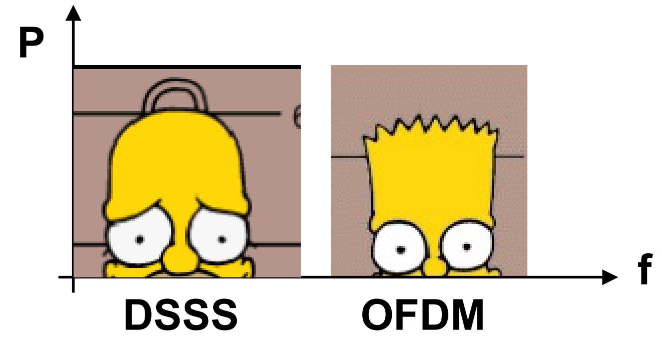


TIME DOMAIN construction of an OFDM signal from its constituent carriers

OFDM – 802.11a Details (2)

- Symbol duration is 4 microseconds (250 symbols/sec)
  - With a guard interval of 800 ns
  - Optional shorter guard interval of 400 ns may be used in small indoor environments
- Generation of orthogonal components is done in baseband (via DSPs) which is then upconverted to 5 GHz at the transmitter
  - Each subcarrier can be represented as complex number
  - The time domain signal is generated by IFFT
- The receiver downconverts, samples at 20 MHz and does an FFT to retrieve the original complex coefficients

OFDM – Pros and Cons



- Advantages
  - High spectrum efficiency
  - High multipath resistance
  - General better interference resistance
  - All this results in longer distances
- Drawbacks
  - More expensive circuits
  - Higher power consumption (compared to 802.11b)
  - Envelope of Multi-carrier modulation results in high Crest factors (peak to average power)
    - Nonlinear effects in analog devices and ADCs
    - Results in BW spreading (higher order signals)
    - Four-Wave Mixing
    - Neighbor channel interference degrades receiver sensitivity
  - Therefore 30 mW EIRP limitation (2.4 GHz)
  - Channel overlapping is more critical ('Bart Simpson Head')

Antennas

…and a bit physics.

$$\nabla \times \vec{E} = -\frac{\partial \vec{B}}{\partial t}$$

$$\nabla \cdot \vec{B} = 0$$

$$\nabla \times \ \vec{B} = \frac{1}{c^2}\frac{\partial \vec{E}}{\partial t} + \mu_0(\vec{J}_{free} + \frac{\partial \vec{P}}{\partial t} + \nabla \times \vec{M})$$

$$\nabla \cdot \vec{E} = \frac{\rho_{free} - \nabla \cdot \vec{P}}{\epsilon_0}$$

$$\nabla \cdot \vec{J}_{free} = -\frac{\partial \rho_{free}}{\partial t}$$

The famous "Maxwell Equations", a complete description of the EM field

James Clerk Maxwell

"Was it not the God who wrote these signs, that have calmed alarm of my soul and have opened to me a secret of nature?"

Ludwig Boltzmann quoting "Faust" as he first saw the Maxwell equations.

Decibels

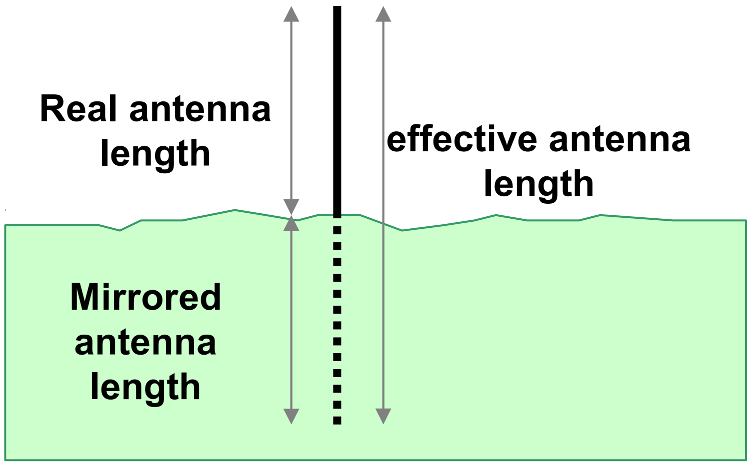
- **Why use decibels?**
  - **Extremely large and extremely small factors are mapped into a small interval**
  - **Multiplication and division is transformed into addition and subtraction**

Increase	Factor	Decrease	Factor
0 dB	1 x	0 dB	1 x
1 dB	1.25 x	-1 dB	0.8 x
3 dB	2 x	-3 dB	0.5 x
6 dB	4 x	-6 dB	0.25 x
10 dB	10 x	-10 dB	0.10 x
12 dB	16 x	-12 dB	0.06 x
20 dB	100 x	-20 dB	0.01 x
30 dB	1000 x	-30 dB	0.001 x
40 dB	10,000 x	-40 dB	0.0001 x

We mostly need dB, dBm, and dBi,
and only rarely dBw and dBd (at least in the WLAN context)

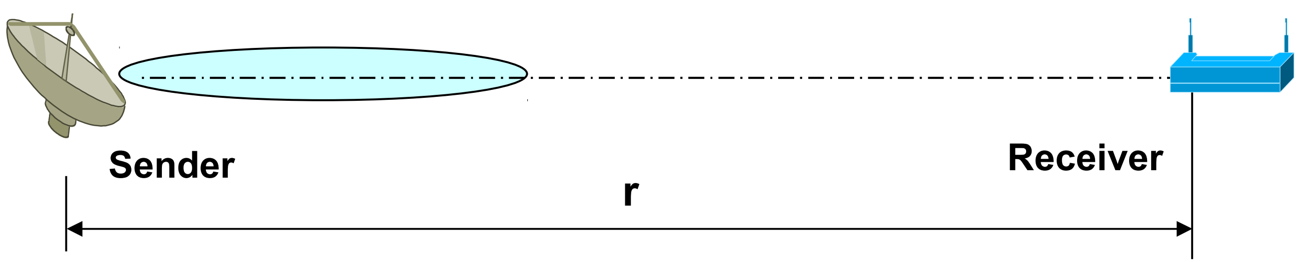
Generating Radio Waves

- Goal: Inject the waveguide wave from the sender into free space
- Antennas are "opened" oscillator-circuits
  - Radio waves are generated by accelerated electrons in the antenna
- Antenna length L
  - Good efficiency if L ≅ λ
  - L=λ/2 (dipole)
  - L=λ/4 (monopole)
- To concentrate power in a desired direction requires L > λ



Antenna Gain

$G = \dfrac{\text{maximum power density towards specific direction}}{\text{mean power density (isotropic radiation)}}$	$G = \dfrac{4 \pi A_e}{\lambda^2}$
▪ Hertz' Dipole: G = 1.5 ▪ $\lambda/2$ Dipole: G = 1.64 (= 2.14 dBi = 0 dBd) ▪ Parabolic dish with 4 m diameter and $\lambda_{2.4GHz}$: $G = 10^4$	$G_{[dB]} = 10 \log G$



Power Density: $S_R = \dfrac{P_S G_S}{4 \pi r^2}$

Power at receiver's antenna output: $P_R = P_S G_S G_R \left(\dfrac{4 \pi r}{\lambda} \right)^{-2}$

Polarization

- **Linear polarization**
  - Vertical or horizontal
  - Requires linear antenna elements
- **Elliptical polarization**
  - Circular polarization is only a special case
  - Requires bended antenna elements
- **Transmitter and receiver antennas should be aligned for same polarization to achieve best performance**
  - Otherwise "infinite" attenuation with "opposite" antennas
  - Or 3 dB attenuation between linear and circular antennas
  - Polarization change with diffractions and reflection
- **Vertical polarization is preferred for long range transmission (ground effect attenuate the signal power in horizontal polarization)**
- **Circular polarization antennas mitigate the effect of reflections**
  - Principle also used for GPS
  - See helical antennas (for example)

Other Antenna Facts

- Impedance Matching
  - Free space impedance is 377 Ohm
  - Antenna cables have 50 Ohm (typically)
  - Antenna must transform 50 to 377 Ohm
- Without impedance matching
  - Reflections will result into standing waves
  - TX power will not be transferred efficiently to the antenna
- Voltage Standing Wave Ratio (VSWR)
  - $s = U_{max} / U_{min} \geq 1$
  - s = 1 means ideal impedance matching
  - s > 1 means reflections and high ripples
    - => higher rms-values
    - => higher loss

Other Antenna Facts

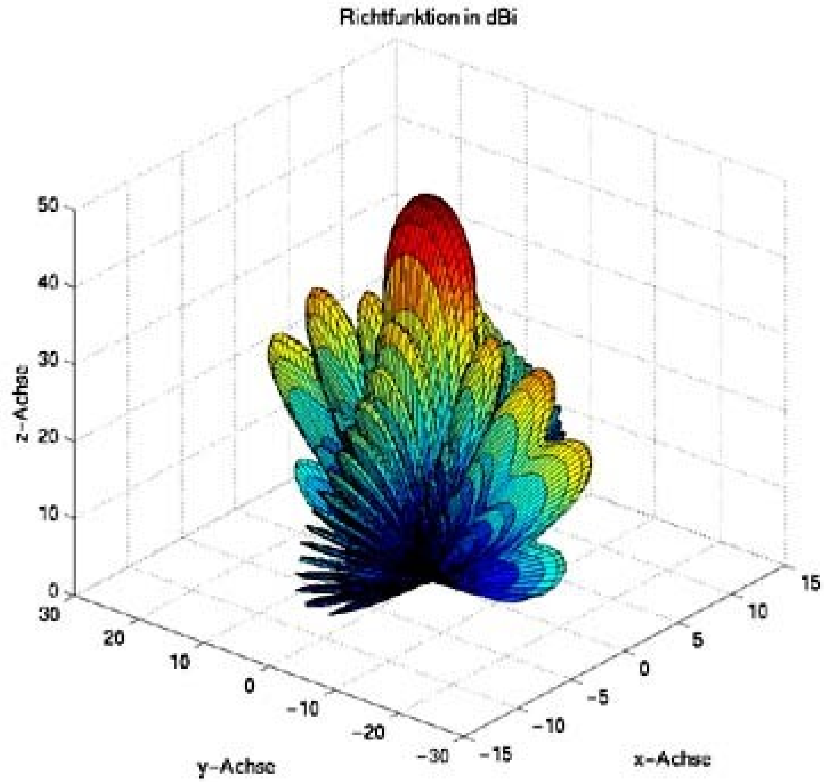
- **Theorem of Reciprocity**
  - Antenna impedance, Gain, as well as antenna diagrams are equivalent for RX and TX
- **Near field versus far field**
- **Shortening effect**
  - Slower wave propagation in antenna ($c_{wire} < c_0$) plus capacitive effects on antenna-ends demands for shortening the antenna
  - Typically 3-8 %

Wave Propagation

- Free space:
  - Fields E, H ~ 1/r
  - Power density $S = E \times H \sim 1/r^2$
  - Compared to cables: attenuation ~ e^{-r}
- Along earth's surface also surface waves must be considered
  - Fields E, H ~ e^{-r}
- The higher the frequencies the lower the effect of surface waves
  - "Quasi-optical" propagation

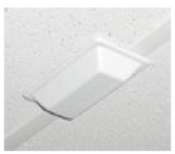
Antenna Patterns

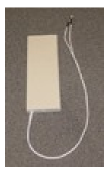
- Field strengths as polar diagram
  - Scaled to maximum value (0 dB)
  - Logarithmic or linear (F~1/r)
- Elevation and Azimuth
  - Often used for simple linear polarized antennas
  - Often corresponds to co- and cross-polarized patterns
- E and H patterns
  - For linear polarized antennas
  - Distinguish:
    - E-Field and H-Field
    - Elevation and Horizontal
    - Both types are common (!)
- High-gain antennas have significant null-angles

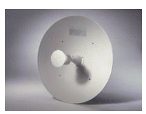


WLAN Antenna Examples









Cisco
(21 dBi)

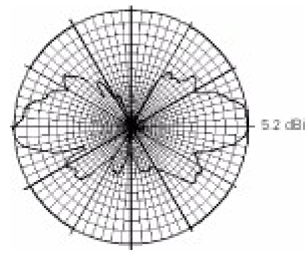




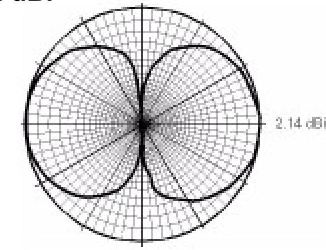
- Circular polarity (5 dBi)
- Microstrip patch (6-18 dBi)
- Omni (2-10 dBi)
- Parabolic dish (20-30 dBi)
- Sector (14 dBi)
- Yagi (8-16 dBi)

Antennas & Patterns

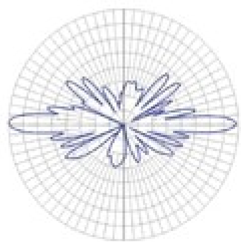
Omni, 5.2 dBi



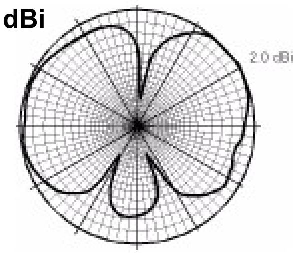
Diversity, 2.2 dBi



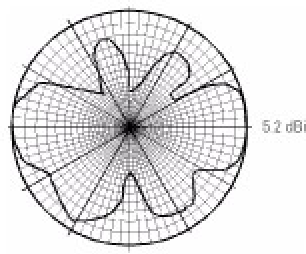
Omni, 12 dBi



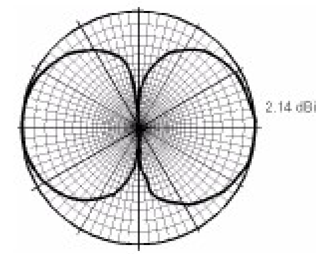
Patch, 2.0 dBi



Omni, 5.2 dBi



Dipole, 2.0 dBi

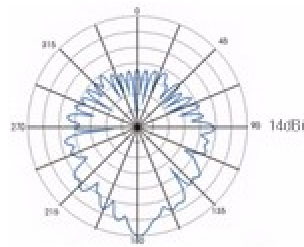


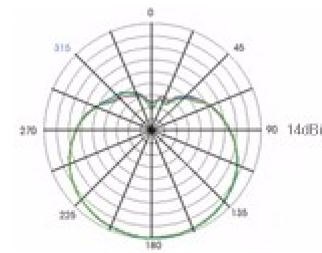
- Cisco WLAN Antennas and vertical radiation shown only

Some Cisco Antennas

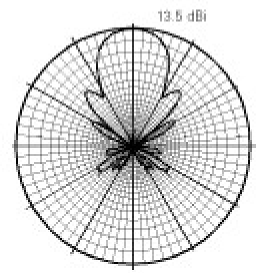
Horizontal | **Vertical**

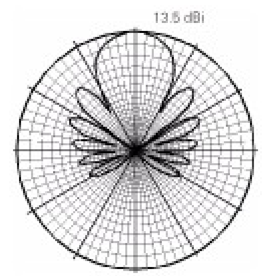
Sector, 14 dBi



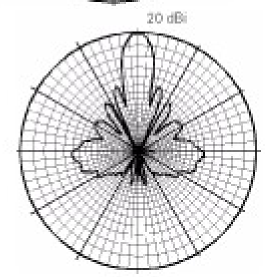


Yagi, 13.5 dBi

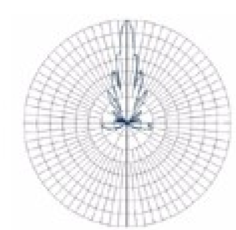


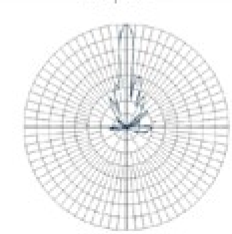


Dish, 21 dBi



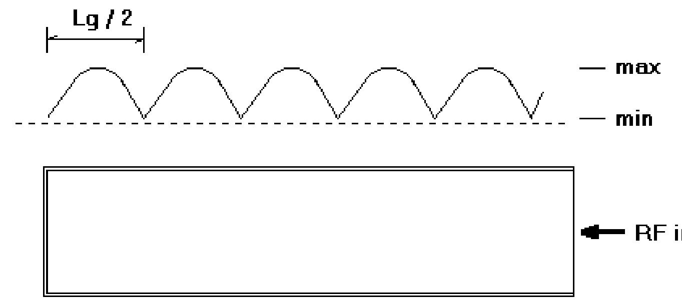
Dish, 28 dBi
5.8 GHz





Waveguide Antennas

- Standing wavelength λ_g depends on
  - Tube diameter D
  - Open air wavelength λ_o
- First maximum point is $\lambda_g/4$ from the closed end
  - Flat maximum area
- Total tube length: Open end should match (next) maximum
  - Ideally 3/4 λ_g



$$\lambda_o = 300 / f_{[MHz]}$$

$$\lambda_{at} = 1.706 \times D$$

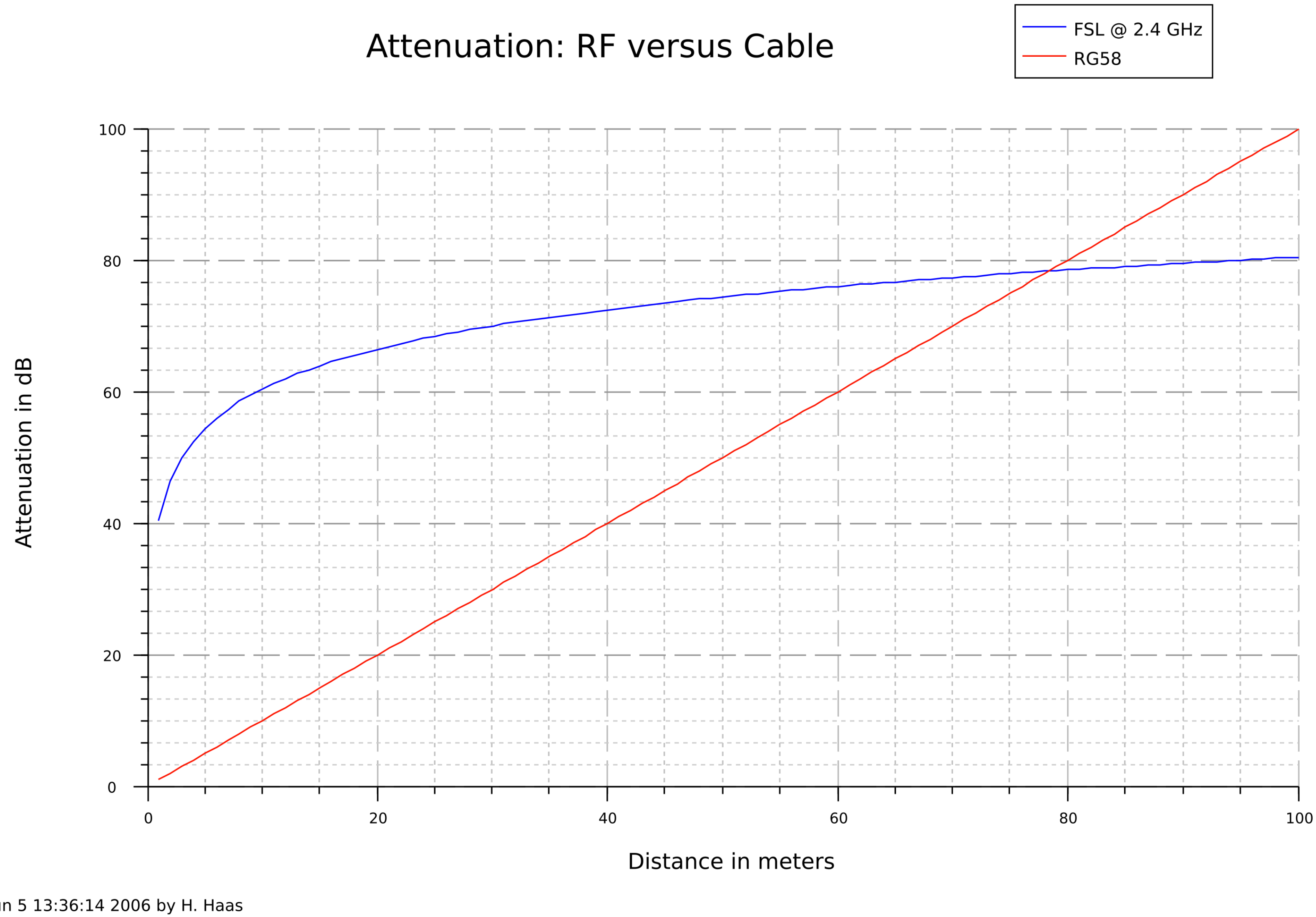
$$1/\lambda_o = 1/\lambda_{at} + 1/\lambda_g$$

FSL

- Free Space Loss (FSL)
  - Real Loss > FSL
  - Reflects the RF power law $P \sim 1 / r^2$
  - Defined as $10 \log P_S/P_R$
- Double distance means
  - Additional 6 dB loss
  - Because power decreases by factor 4
  - Only with cables the total loss can be multiplied by two
    - Exponential law

$$FSL = \left(\frac{4 \pi r}{\lambda} \right)^2$$

Why Radio Is Better For Long Distances



FSL – Simple Formulas

General

$$FSL_{dB} = 22 + 20 \log (r/\lambda)$$

$$FSL_{dB} = 20 \log (f_{MHz}) + 20 \log (r_{km}) + 32.45$$

$$FSL_{dB} = 20 \log (f_{GHz}) + 20 \log (r_{km}) + 92.45$$

2.4 GHz

$FSL_{dB} = 20 \log (r_{km}) + 100$	$r_{km} = 10$^((FSL -100)/20)

5.3 GHz

$FSL_{dB} = 20 \log (r_{km}) + 107$	$r_{km} = 10$^((FSL -107)/20)

General Attenuation Considerations

- **For isotropic antennas in free space, the attenuation of 5 GHz is higher**
  - **Friis: 20 log (5.25/2.4) = 6.8 dB**
- **However only little material differences 'in general'**
  - **Typically 5 GHz is only 1-2 dB worse**
- **Exceptions:**
  - **<u>Grid spacing</u> of enforced concrete could match wavelengths**
  - **<u>Red brick</u> introduces approx. 10 dB additional attenuation for 5 GHz and <u>wood lumber</u> additional 3-6 dB**
- **Note: Reflections is a completely different story (and more complicated)**

EIRP (for Spread Spectrum)

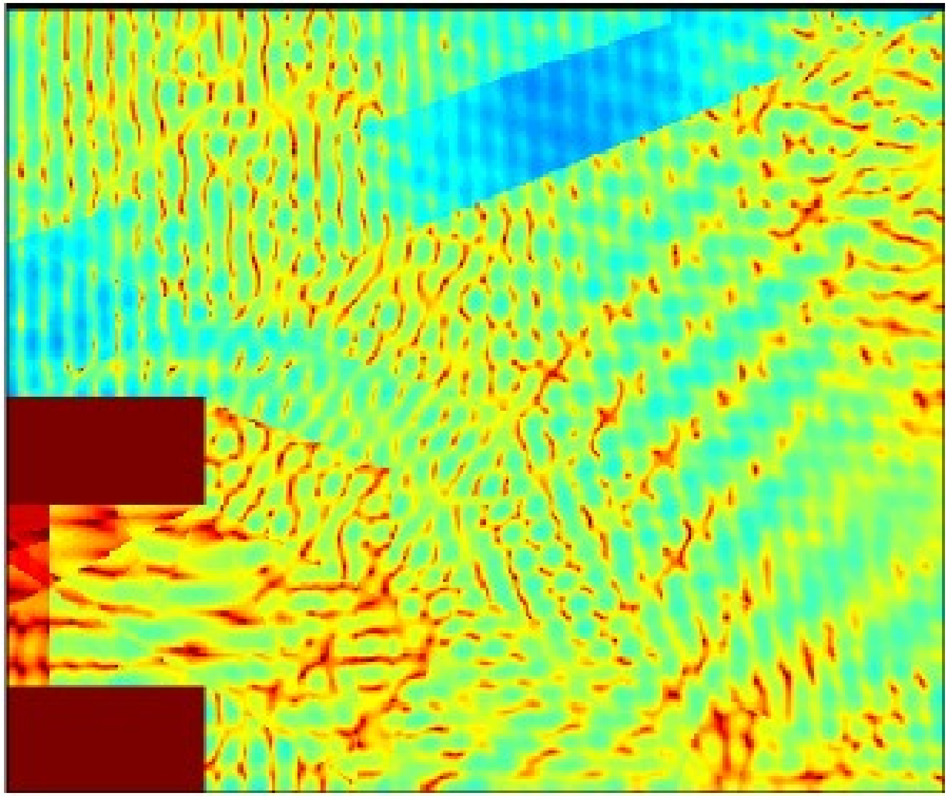
- Equivalent Isotropically Radiated Power
  - Theoretical power for an isotropic antenna to reach same PSD as directional antenna
  - EIRP = $10^{(g_{dBi}/10)} * P$ [W]
  - National band-specific EIRP limits
- Europe (ETSI) max EIRP
  - 100 mW or 20 dBm for DSSS
    - = 17 dBm (50 mW) + 3 dBi
  - 30 mW or 15 dBm for OFDM (typically)

EIRP In Other Countries

- America (FCC)
  - Point-to-multipoint (typical AP usage)
    - 30 dBm (1 W) and 1:1 power/gain reduction/increase
  - Point-to-point (typical bridging usage)
    - 36 dBm (4 W) = 30 dBm + 6 dBi
    - G>6dBi requires minus 1dBm for each 3 dBi more gain
- Japan, China: EIRP 10 mW

Diversity Antennas

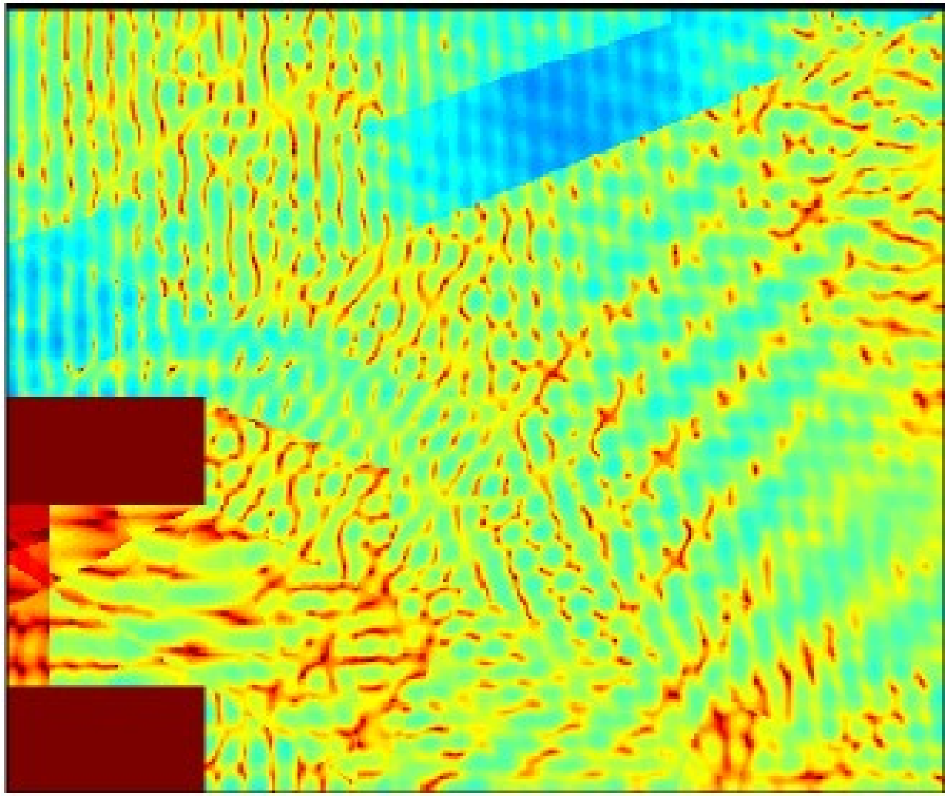
- Due to reflections, a short-time standing field is produced – with ripples, peaks and lows
  - Same picture for every frame if "nobody moves"
- Therefore, use multiple antennas: one will likely pick up more energy than the other



Indoor office signal intensity map (source unknown)

The EM Field

- Reflections, diffractions and scattering are highly dynamic
  - Consider static and dynamic configurations
- Multipath problems
  - "High signal strengths but low quality"



Indoor office signal intensity map
(source unknown)

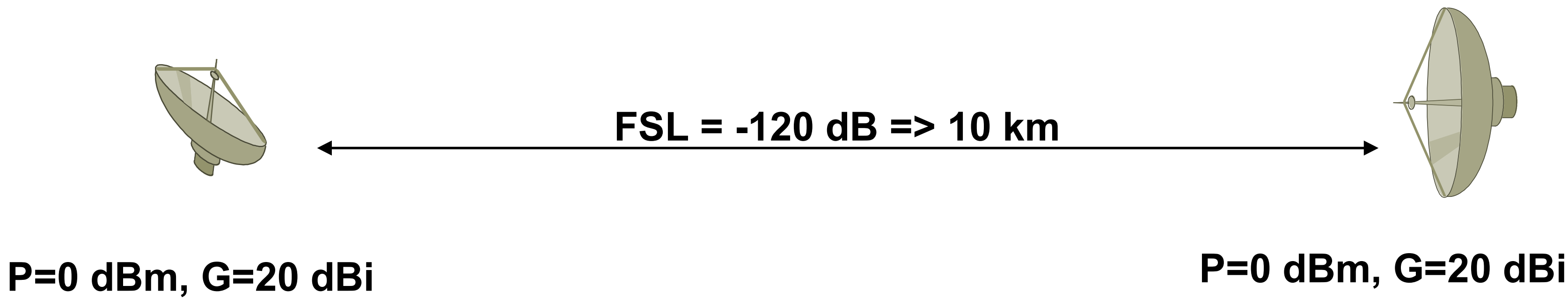
Why are bigger antennas better?

- Assume we comply to 20 dBm EIRP
- Then this can be reached in various ways:

P_{TX}	Gain		Gain	P_{TX}
17 dBm	3 dBi	FSL + 17 dBm + 6 dBi	3 dBi	17 dBm
10 dBm	10 dBi	FSL + 10 dBm + 20 dBi	10 dBi	10 dBm
0 dBm	20 dBi	FSL + 0 dBm + 40 dBi	20 dBi	0 dBm

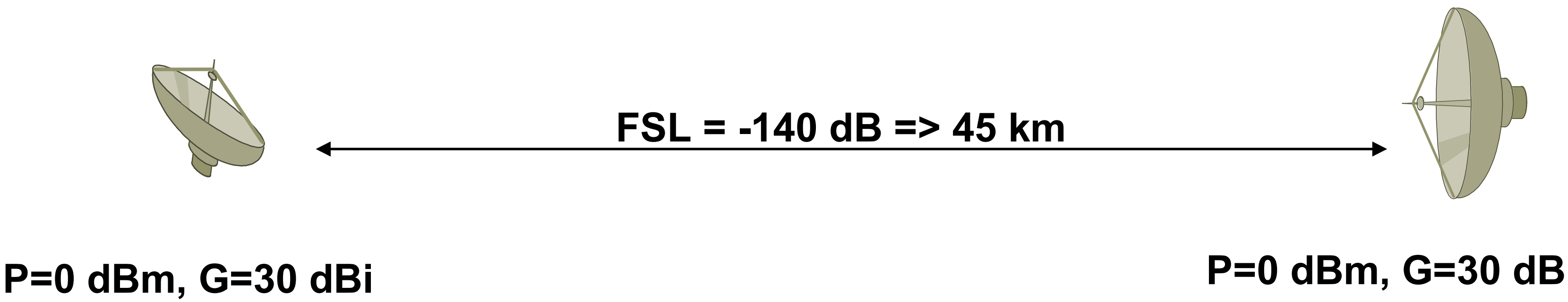
- Additionally, SNR is improved with higher gains
- Therefore, try to maximize antenna gains !!!

Practical 2.4 GHz Distance Limits



- **ETSI limits 2.4 GHz EIRP to 20 dBm**
  - **(Also for P2P links)**
- **A minimum RX power of -80 dBm can be assumed as practical limit**
- **Then a maximum FSL of -120 dB is allowed**
- **This results in a maximum distance of <u>10 km</u>**

Practical 5 GHz Distance Limits



- **Completely different situation**
  - HIPERLAN band (5470-5725 MHz) released for WiFi
  - ETSI allows EIRP = 1 W = 30 dBi !!!
- Also a minimum RX power of -80 dBm can be assumed as practical limit
- Then a maximum FSL of -140 dB is allowed
- This results in a maximum distance of <u>45 km</u>

Exploit Diversity (5.4 GHz)

- Example:
  - TX-Antenna is 30 dBi parabola (1 W = 30 dBm EIRP = 0 dBm + 30 dBi)
  - RX-Antenna is 40 dBi parabola
- Allows 150 dB FSL => 140 km !!!
- Optionally an additional preamp can be used
  - E. g. + 10 dB => 160 dB FSL => 444 km *theoretically*
- Problem: CSMA/CA timing must consider signal propagation time
  - 140 km => 466 usec delay (but SIFS = 16 usec)

SNR

- **Sensitivity is not the only important parameter for the receiver quality**
  - **Low noise level: Sensitivity is limiting**
  - **High noise level: SNR is limiting**
- **Shannon 1948: Channel Capacity**
  - **Depends on Bandwidth and SNR**
- **Example: Required SNR for the Orinoco PCMCIA Silver/Gold**
  - **11 Mbps** — **SNR_{min} = 16 dB**
  - **5.5 Mbps** — **SNR_{min} = 11 dB**
  - **2 Mbps** — **SNR_{min} = 7 dB**
  - **1 Mbps** — **SNR_{min} = 4 dB**
- **Although TX-power regulated (EIRP) the RX-SNR has the same effect!**
  - **See e. g. RX 2400-o from SSB “Receive Booster” (8-10 db plus)**

Typical Receiver Sensitivities

- Orinoco cards PCMCIA Silver/Gold
  - 11Mbps -82 dBm
  - 5.5Mbps -87 dBm
  - 2Mbps -91 dBm
  - 1Mbps -94 dBm
- CISCO cards Aironet 350
  - 11 Mbps -85 dBm
  - 5.5 Mbps -89 dBm
  - 2 Mbps -91 dBm
  - 1 Mbps -94 dBm
- Edimax USB client
  - 11Mbps -81 dBm
- Belkin router/AP
  - 11 Mbps -78 dBm

Typical noise floor: -95 dB, only +/- 2dB differences between a, b, g

Cable Loss

- **Typical loss in common coaxial cables at 2.45 GHz**
  - RG 58 (quite common, used for Ethernet): 1 dB per meter.
  - RG 213 ("big black", quite common): 0.6 dB per meter.
  - RG 174 (thin, seems to be the one used for pigtail adapter cables): 2 dB per meter.
  - Aircom : 0.21 dB/m.
  - Aircell : 0.38 dB/m.
  - LMR-400: 0.22 dB/m
  - IEEE 802.3 (thick 'yellow' Ethernet coax) 0.3 dB/m

Connector Loss

- Add connector loss to cable loss before calculating the Link Budget
  - Typically between 0.1 and 0,5 dB at 2,45 GHz
  - Use as few connectors as possible
- Loss depends on the quality of the connectors
  - Dielectric material, Geometry, etc
  - Best: N connectors or SMA connectors
  - Worse: Old BNC connectors
- Avoid Pigtails
  - (=short cables with different connectors on each side)
  - 30 cm may have ~ 1.5 dB!
  - Use single-unit converters instead

WLAN Connectors

N
Female

RP-SMA
Female

RP-TNC
Female

N
Male

RP-SMA
Male

RP-TNC
Male

MC

MMCX

MC

Cisco uses reverse polarity for spread spectrum products to prevent connecting wrong antennas.

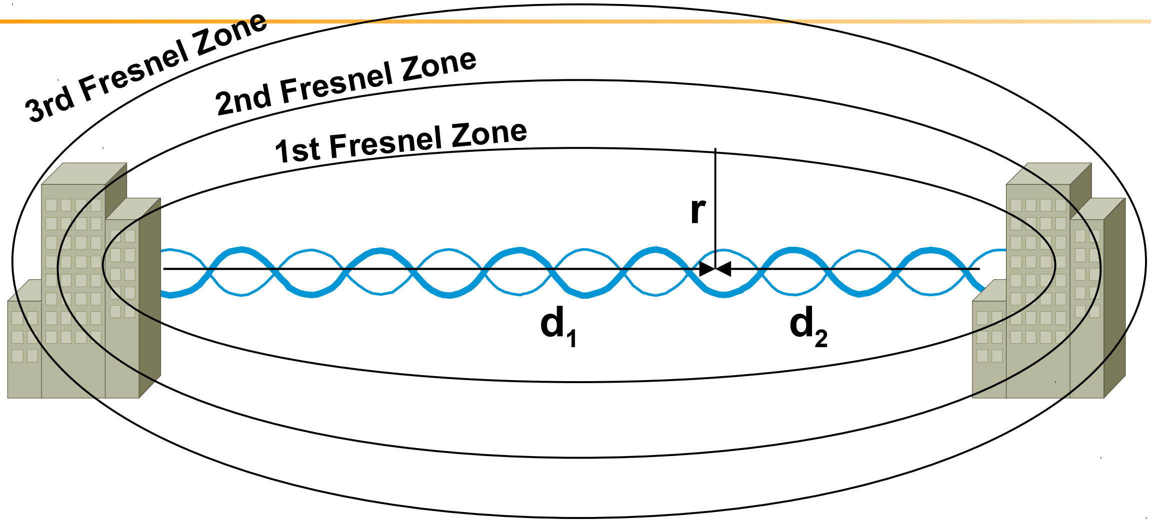
Link Example

- Given 24 dB dish
- Output power must be reduced to -4 dBm
  - That is 0.4 mW (!) to stay within the legal limits of 20 dBm in Europe
- Theoretical maximum range for a reliable link will be 8 km
  - Assuming 15 dBm fade margin
  - Due to highly increased antenna gain in the receiver path (SNR)

Quasi-optical Propagation

- Requires "line-of-sight"
  - Reliable connections due to steady field strengths (no variabilities)
  - Small TX powers possible
  - Free-space wave propagation
- Fading through interferences
  - Multiple waves with different phases
  - Fading-controllers at the receivers (GSM, UMTS)
  - Diversity antennas (WLAN, GSM and UMTS)

The Fresnel Zones (1)



Fresnel zones radius:

$$r = \sqrt{\frac{n\lambda \cdot d_1 \cdot d_2}{d_1 + d_2}} \quad [m]$$

- Surfaces where reflected rays would reach the receiver with an extended path by λ/2
  - => Destructive interference
- TX and RX located at focal points
  - Any path connecting F1, F2, and surface has same length
- Rule of thumb:
  - If 60% of first Fresnel Zone is clear of obstructions then nearly same link as a clear path
  - However might be unstable under bad weather conditions
  - Try to achieve full Fresnel zone clearance

The Fresnel Zones (2)

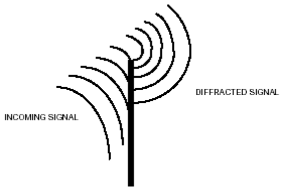
- **Consideration especially important when Earth's bulge touches Fresnel zones**
  - **Distances >9 km => high poles are required for antenna mount**

Distance (km)	Fresnel zone (radius)	Earth Curvature	Total
1,6	3	1	4
8	9	1,5	10,5
16	13	4	17
24	16	8,5	24,5
32	20	15	35
40	22	23	45

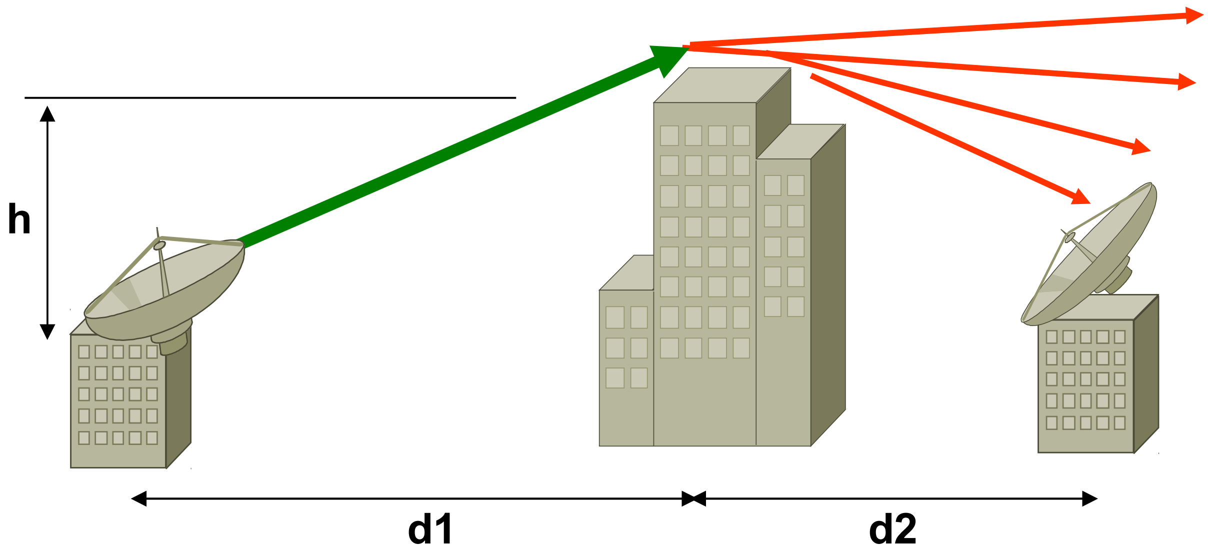
Optical horizon:
$R_{[km]} = 3.57 \, (\mathrm{sqrt}(h_S) + \mathrm{sqrt}\,(h_R) \,)$

Radio horizon:
$R_{[km]} = 4.12 \, (\mathrm{sqrt}(h_S) + \mathrm{sqrt}\,(h_R) \,)$

Diffraction



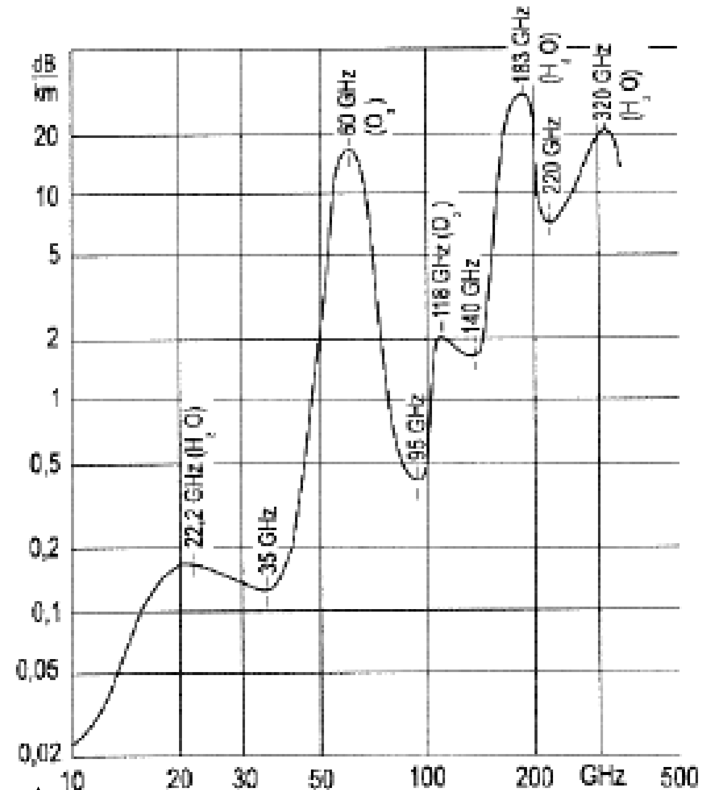
- Radio waves will be distracted on edges from objects.
- It is possible to catch receiver behind objects



$$\text{Loss} = 20 \log \left[\frac{0.225}{h} \left(\frac{0.12\, d_1 d_2}{2\,(d_1 + d_2)} \right)^{1/2} \right]$$

Natural Attenuation

- Fog and rain:
  - Approx 0.5 dB/km @ 2,4 GHz—still little effect
- Dense snow storm is more critical
  - Signal scattering effect
- Problem becomes really serious for higher frequencies
  - Molecule absorption effects
  - Therefore be lucky with WLANs…

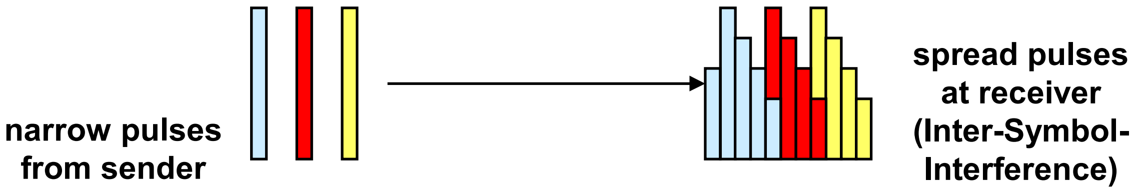


WLANs

(No fog, no rain)

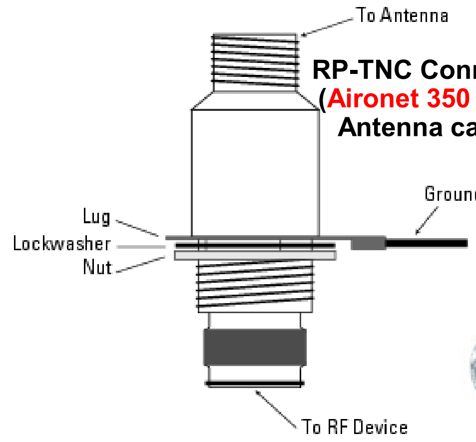
Delay Spread

- <u>Consequence of multipath propagation</u>
  - Receiver needs equalizer
  - Manufacturers specify delay spread limit
- Example: Orinoco Frame Error Rate (FER) < 1%
  - 11Mbps 65 ns
  - 5.5 Mbps 225 ns
  - 2 Mbps 400 ns
  - 1Mbps 500 ns
- Note: Delay spread in wide areas with lots of multipaths can reach several μs !
  - Rule of thumb: Path length difference of 15 meters leads to 50 ns spreading
- <u>Solutions:</u>
  - Directive antennas
  - Circular polarization
  - OFDM



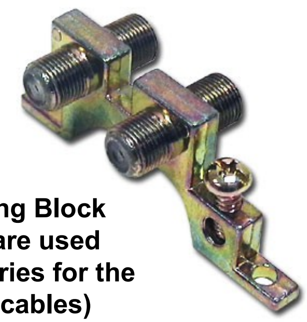
Outdoor Antenna Safety

- **Antenna cables connect indoor and outdoor EM-environment**
  - **Prone to (in-) direct lightning**
  - **Can pick up electrical fields (=> currents) through dry air or EMI**
- **There is no 100% solution to protect your equipment !!!**
  - **But good chances to protect the indoor area (health, fire)**
- **Use lightning arrestors (antenna cable) or grounding blocks (pwr/console coax) against surges**
  - **DC-continuity type needed for WLAN with coax power supply (gas tube or spark gap)**
  - **Proper low-impendance grounding critical (not that easy!)**
  - **Keep tower and coax at same potential (to prevent “side flashes)**



RP-TNC Connectors (Aironet 350 series, Antenna cables)

0-3 GHz Lightning Protector HyperGain® Model HGLN-F



Dual F Grounding Block (F-connectors are used in Aironet 1400 series for the Bridge supply cables)

World Record (early 2005)

Nevada

4 m dish, 300 mW

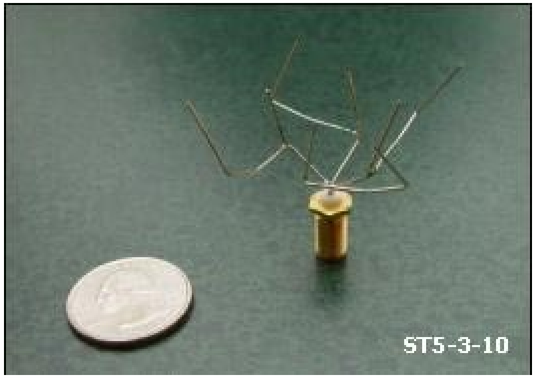
200 km

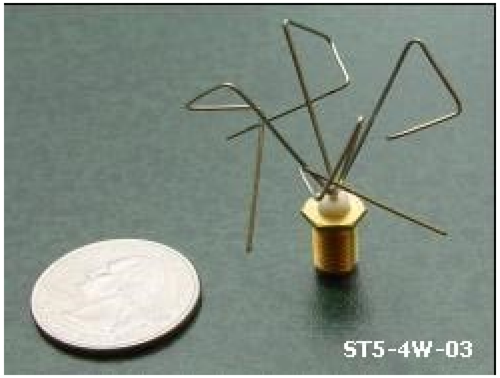
Utah

3 m dish, 300 mW

- 200 km without amplifiers
  - But an EIRP beyond legal limits
- See
  - http://www.wifiworldrecord.com/
  - http://www.wifi-shootout.com/

Tomorrow's Antenna Design





- **Microwave antenna design using genetic algorithms**
  - **http://ic.arc.nasa.gov/projects/esg/research/antenna.htm**