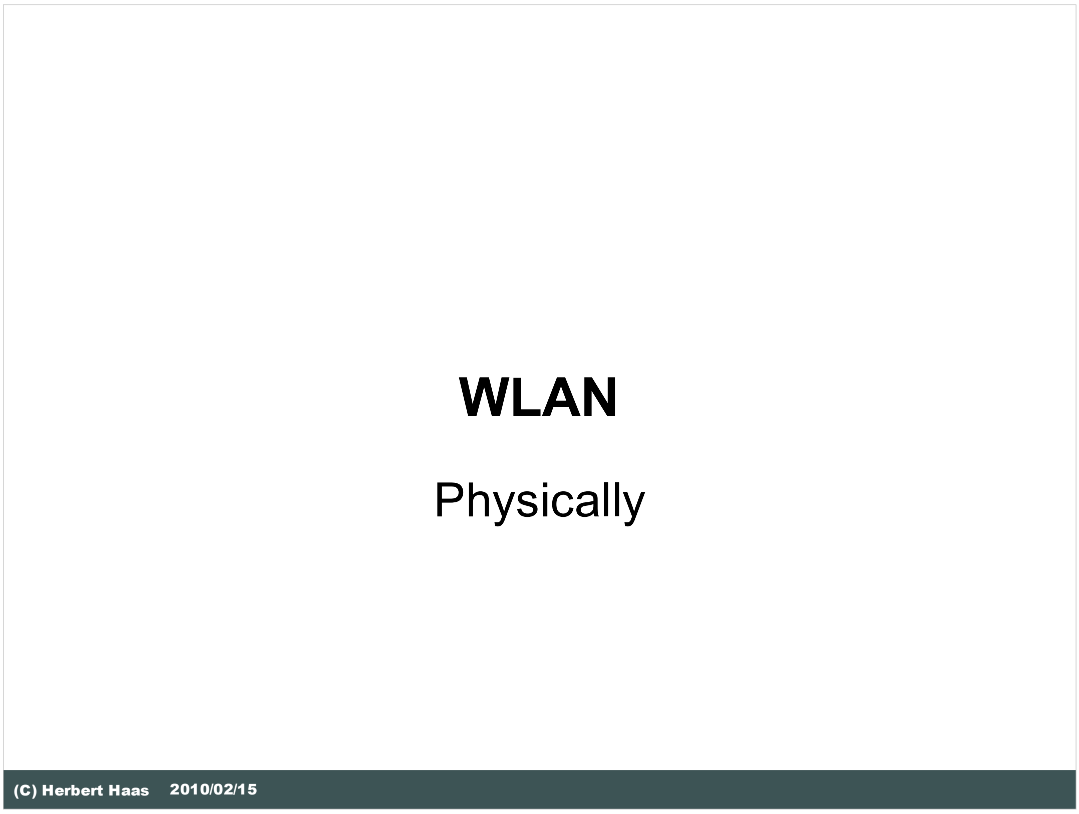
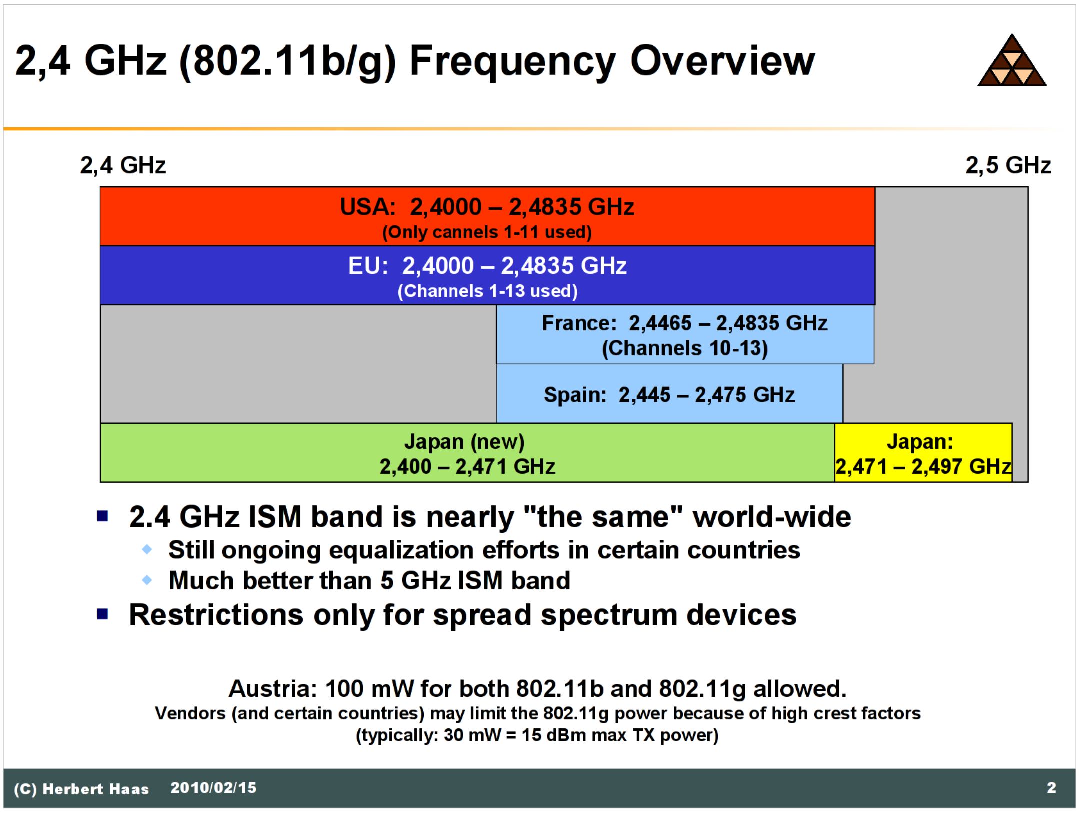


WLAN

Physically

(C) Herbert Haas 2010/02/15

In this chapter we discuss basic communication issues, such as synchronization, coding, scrambling, modulation, and so on.



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

2,4 GHz

2,5 GHz

USA: 2,4000 – 2,4835 GHz
(Only cannels 1-11 used)

EU: 2,4000 – 2,4835 GHz
(Channels 1-13 used)

France: 2,4465 – 2,4835 GHz
(Channels 10-13)

Spain: 2,445 – 2,475 GHz

Japan (new)
2,400 – 2,471 GHz

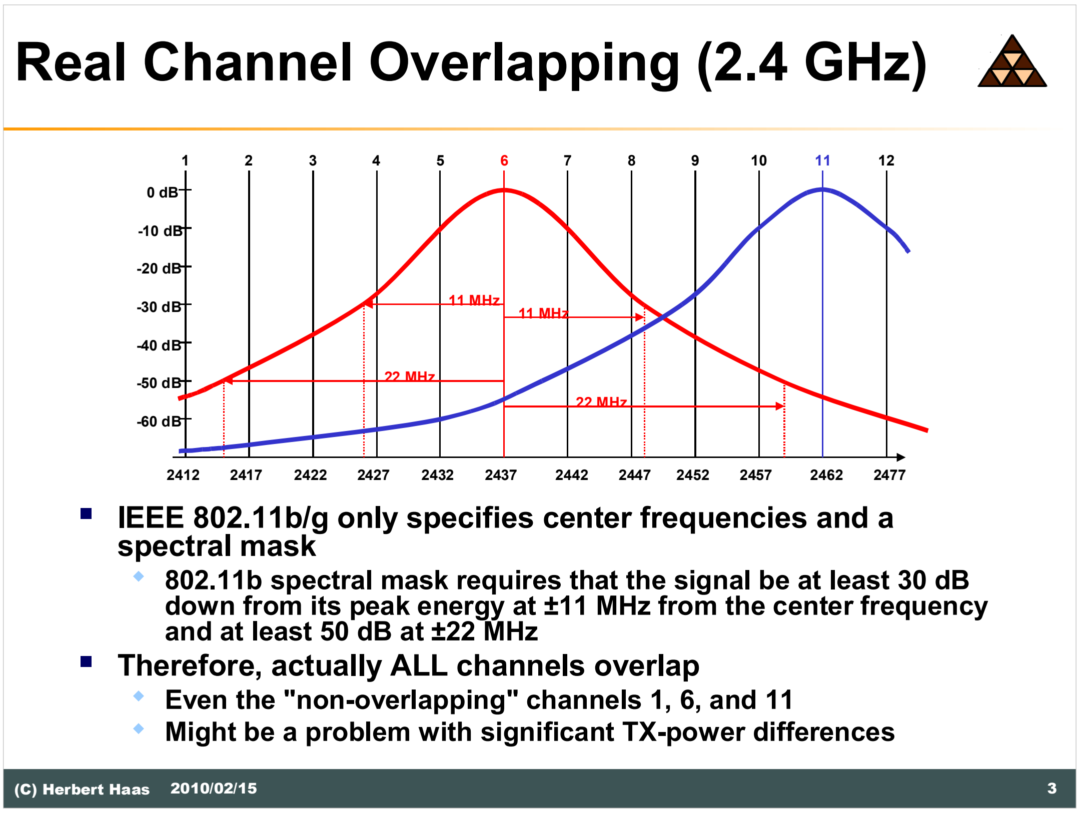
Japan:
2,471 – 2,497 GHz

- 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)

(C) Herbert Haas 2010/02/15 2

It is important to know the limits specified by your regulatory. Violations are handled very differently. In many countries when a company or private user violates these limits and is reported the first time, there is typically no penalty involved.



Real Channel Overlapping (2.4 GHz)

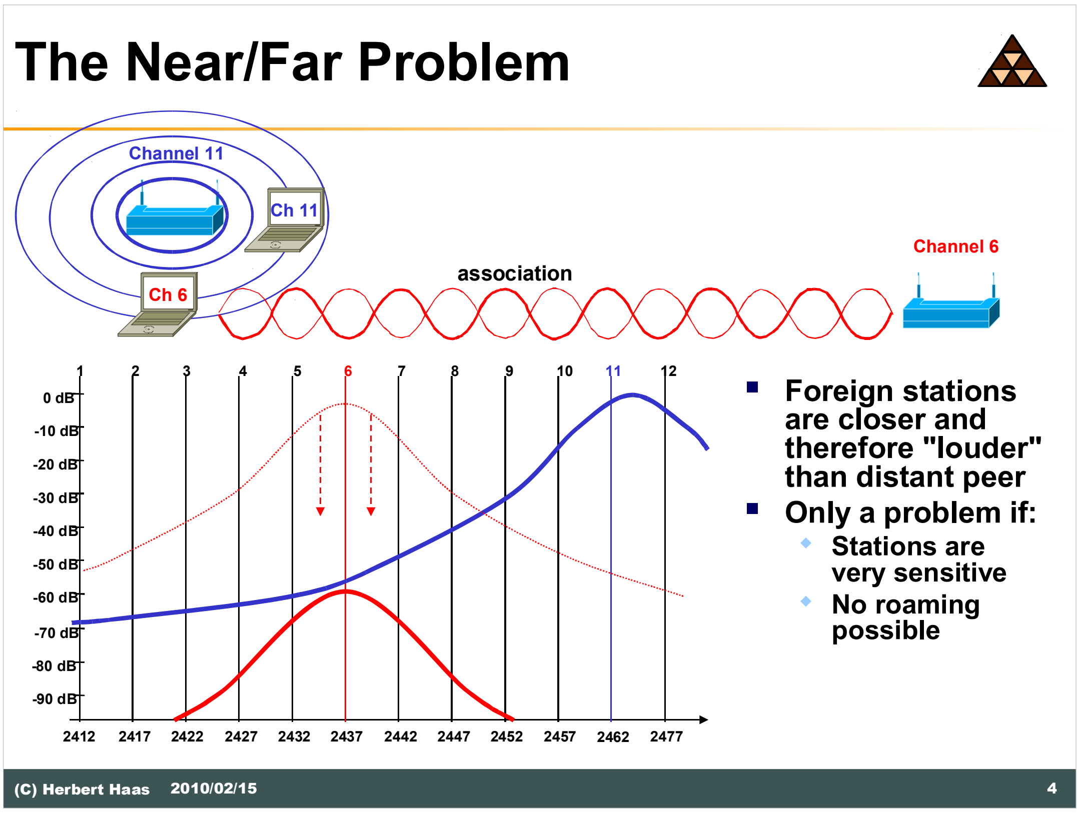
- IEEE 802.11b/g only specifies center frequencies and a spectral mask
  - 802.11b spectral mask requires that the signal be at least 30 dB down from its peak energy at ±11 MHz from the center frequency and at least 50 dB at ±22 MHz
- Therefore, actually ALL channels overlap
  - Even the "non-overlapping"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

Since the spectral mask only defines power output restrictions up to ±22 MHz from the center frequency, some people assume that the channel's energy doesn't extend any further than that, but in reality, it does. In fact, if the transmitter is sufficiently powerful, the signal can be quite strong even beyond the ±22 MHz point.

From this the so-called **near/far-problem** follows: two communicating stations encounter interferences when a foreign station that transmits on an adjacent channel is much closer to the receiver as the expected transmitter.

Therefore, it is incorrect to say that channels 1, 6, and 11 do not overlap. It is more correct to say that, given the separation between channels 1, 6, and 11, the signal on any channel should be sufficiently attenuated to minimally interfere with a transmitter on any other channel.

But this is not universally true. For example, a powerful transmitter on channel 1 can easily overwhelm a weaker transmitter on e.g. channel 6. In one lab test, throughput on a file transfer on channel 11 decreased slightly when a similar transfer began on channel 1, indicating that even channels 1 and 11 can interfere with each other a little bit.



The Near/Far Problem

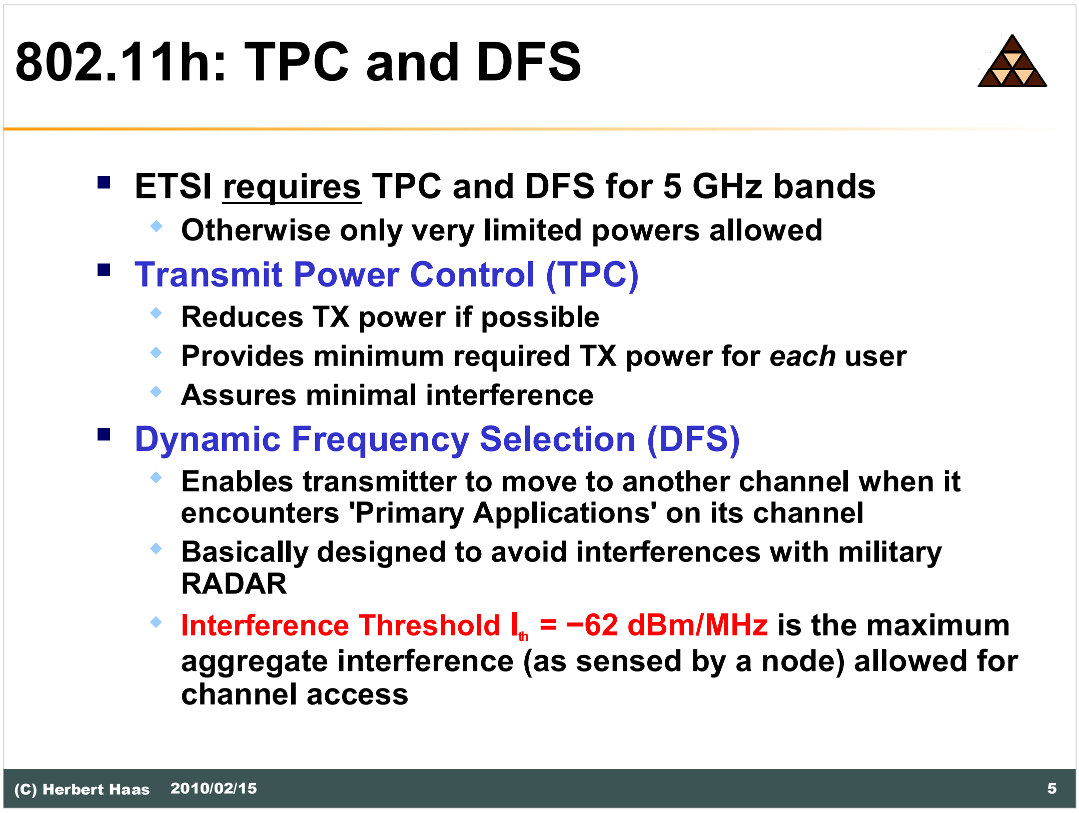
- Foreign stations are closer and therefore "louder" than distant peer
- Only a problem if:
  - Stations are very sensitive
  - No roaming possible

Since the spectral mask only defines power output restrictions up to ±22 MHz from the center frequency, some people assume that the channel's energy doesn't extend any further than that, but in reality, it does. In fact, if the transmitter is sufficiently powerful, the signal can be quite strong even beyond the ±22 MHz point.

From this the so-called **near/far-problem** follows: two communicating stations encounter interferences when a foreign station that transmits on an adjacent channel is much closer to the receiver as the expected transmitter.

Therefore, it is incorrect to say that channels 1, 6, and 11 do not overlap. It is more correct to say that, given the separation between channels 1, 6, and 11, the signal on any channel should be sufficiently attenuated to minimally interfere with a transmitter on any other channel.

But this is not universally true. For example, a powerful transmitter on channel 1 can easily overwhelm a weaker transmitter on e.g. channel 6. In one lab test, throughput on a file transfer on channel 11 decreased slightly when a similar transfer began on channel 1, indicating that even channels 1 and 11 can interfere with each other a little bit.



802.11h: TPC and DFS

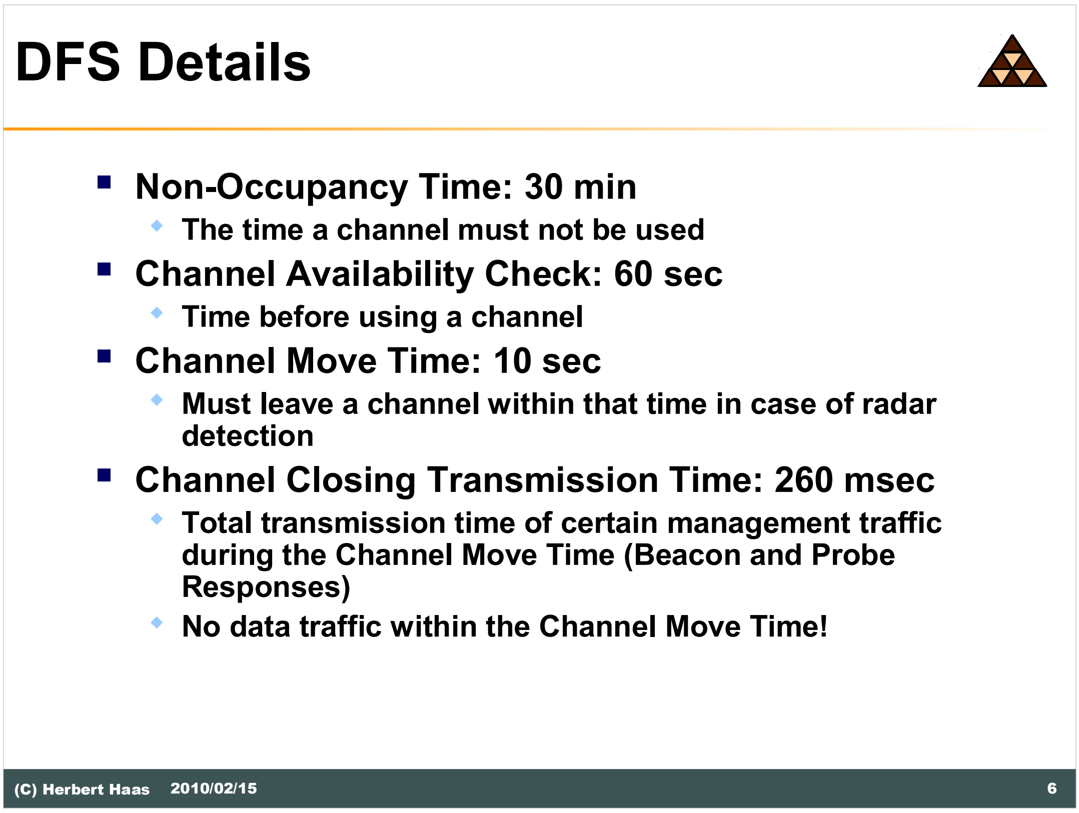
- ETSI requires TPC and DFS for 5 GHz bands
  - Otherwise only very limited powers allowed
- Transmit Power Control (TPC)
  - Reduces TX power if possible
  - Provides minimum required TX power for *each* user
  - Assures minimal interference
- Dynamic Frequency Selection (DFS)
  - Enables transmitter 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

Sharing Rules:

1. Non-Greedy Occupancy: No user may occupy the channel with rate 0 (no data to send). This rule, for instance, prohibits devices to use jamming techniques to have exclusivity to a channel.

2. Channel Select: A channel is deemed accessible at a node if the aggregate interference power at the intended receiver is less than Ith. The rules recognize that a connection needs to be established between nodes before this rule can come into operation. The channel width chosen is at the discretion of the node. A node should be able to access any available channel in the allocation in question.

3. Range & Power Select: Nodes should reduce transmit power to the minimum necessary to achieve the link margin they require. For the purposes of compliance testing, for every reduction of transmit range by factor A, the node must reduce transmit power by a minimum of 20 log10 A dB. Practical transmit power control should be operational over a dynamic range of 12 dB with step size of 1 dB.

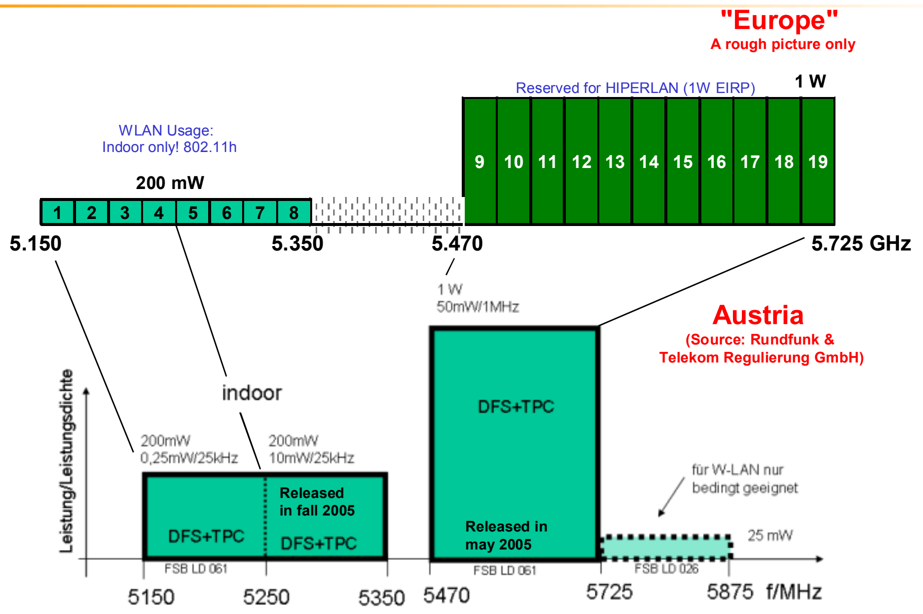


DFS Details

- 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!

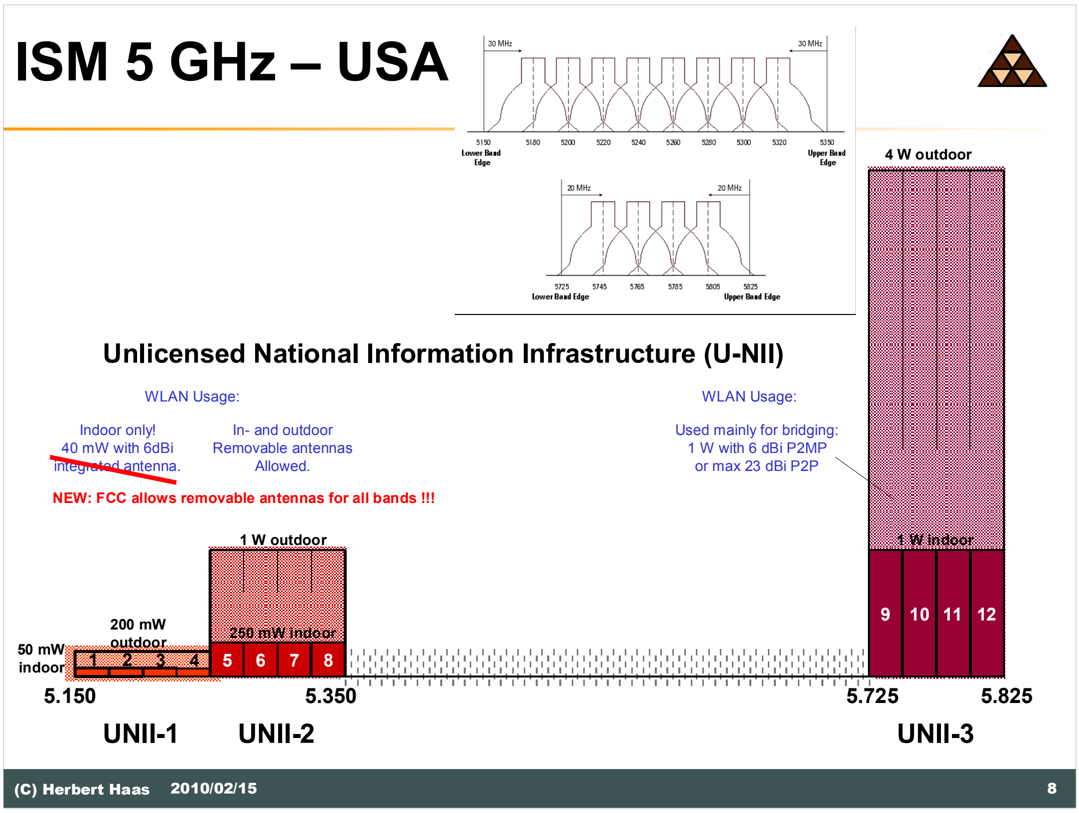
Lightweight APs save a list of their current radar detections in flash, therefore after reset the LAP will still continue the non-occupancy time

ISM 5 GHz – Europe [Jan 2007]



There are RADAR applications working at 5725-5825 MHz.

2003 World Radiotelecommunications Conference made 802.11a easier for worldwide use (opened the 5 GHz bands)



ISM 5 GHz – USA

Unlicensed National Information Infrastructure (U-NII)

WLAN Usage:

Indoor only!
40 mW with 6dBi
~~integrated antenna.~~

In- and outdoor
Removable antennas
Allowed.

NEW: FCC allows removable antennas for all bands !!!

WLAN Usage:

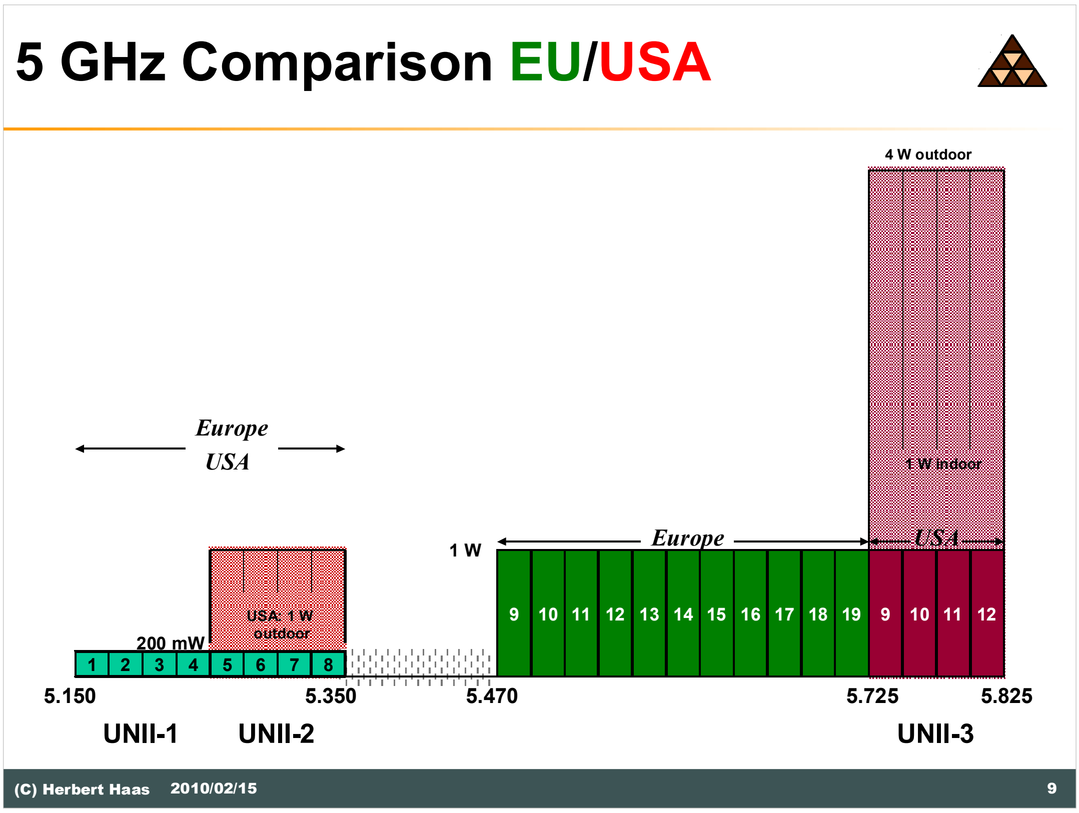
Used mainly for bridging:
1 W with 6 dBi P2MP
or max 23 dBi P2P

(C) Herbert Haas 2010/02/15 8

Generally the FCC allows much higher TX powers.

Additionally there is a high-frequency 5 GHz range close to 6 GHz providing four non-overlapping channels. This third band (UNII-3) is intended for long distance outdoor WLAN bridging which can be done with 4 Watts. The Cisco Aironet 1400 Bridge is designed for that UNII-3 band.

(ODU = Outdoor Unit)



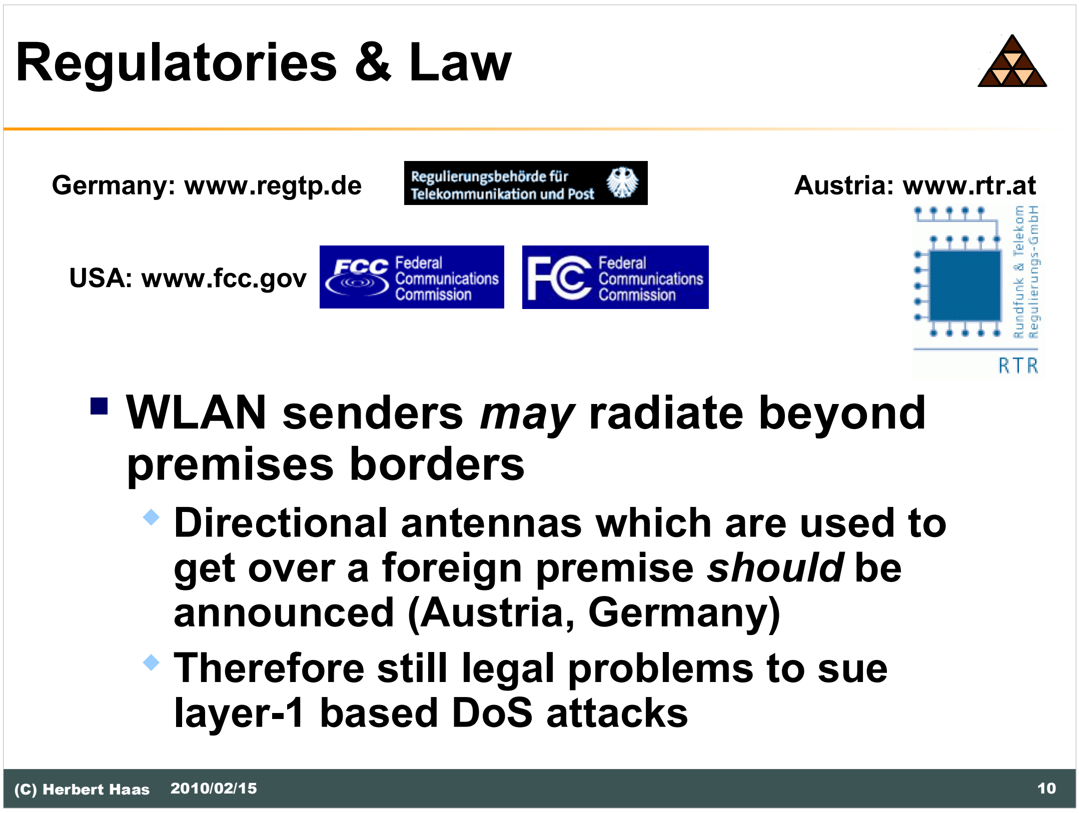
5 GHz Comparison EU/USA

(C) Herbert Haas 2010/02/15 9

Generally the FCC allows much higher TX powers.

In the ETSI domain there are additional 11 channels in the middle of the 5-6 GHz band which can be used with (up to) 1 Watt.

These high powers (more than 30 times higher compared with 802.11g) and the reduced noise and interference in that band overcompensate the 5-GHz free space loss which results in remarkably long communication distances (kilometers).



Regulatories & Law

Germany: www.regtp.de

USA: www.fcc.gov

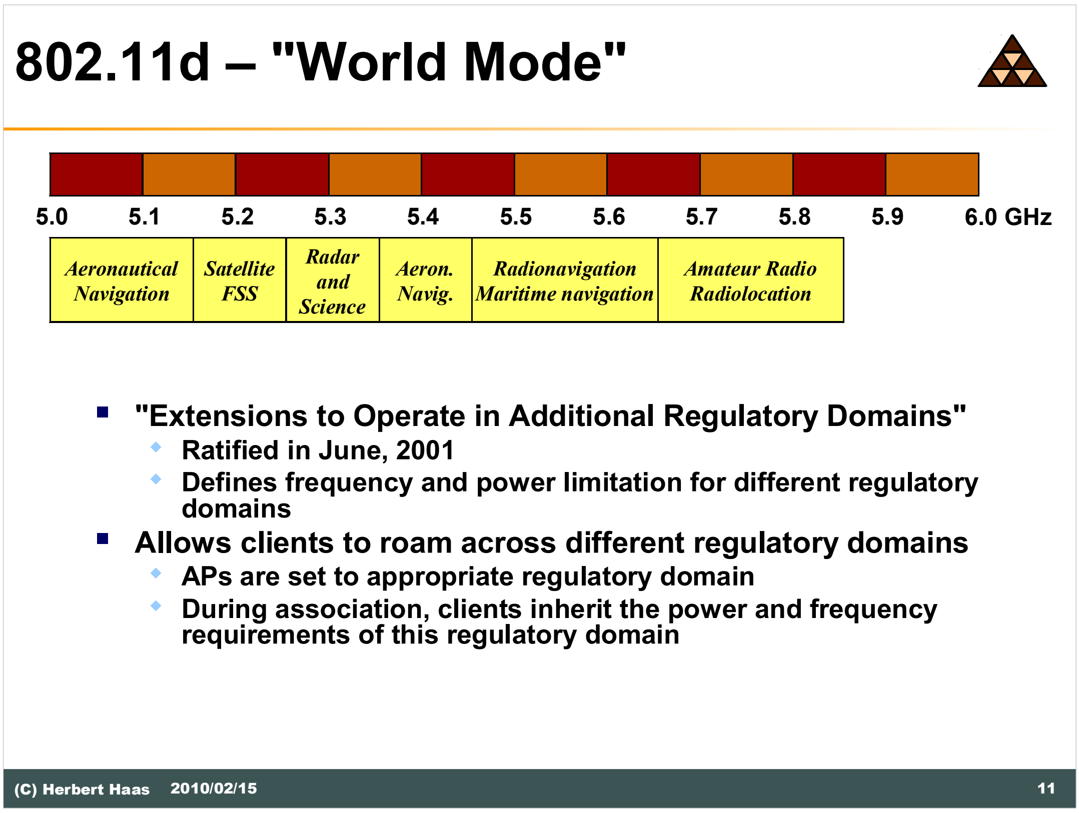
Austria: www.rtr.at

- **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**

In the Europe (ETSI) domain each country may still specify local requirements additional to the ETSI limits. However (fortunately) these country-specific deviations seem to disappear.

Regarding the Austrian situation only:

> Die Rundfunks & Telekom Regulierungs GmbH in Österreich arbeitet eng mit der Telekom-Control-Kommission (TKK) und der Kommunikationsbehörde Austria (KommAustria, Ressortbereich des Bundeskanzleramtes) zusammen.
>
> Die Funk-Schnittstellenbeschreibungen sind im Internet abrufbar unter:
>
> http://www.rtr.at/de/tk/FRQSP2400MHz [Nov 2007]
>
> (ehemals http://www.bmvit.gv.at/radiointerfaces)



802.11d – "World Mode"

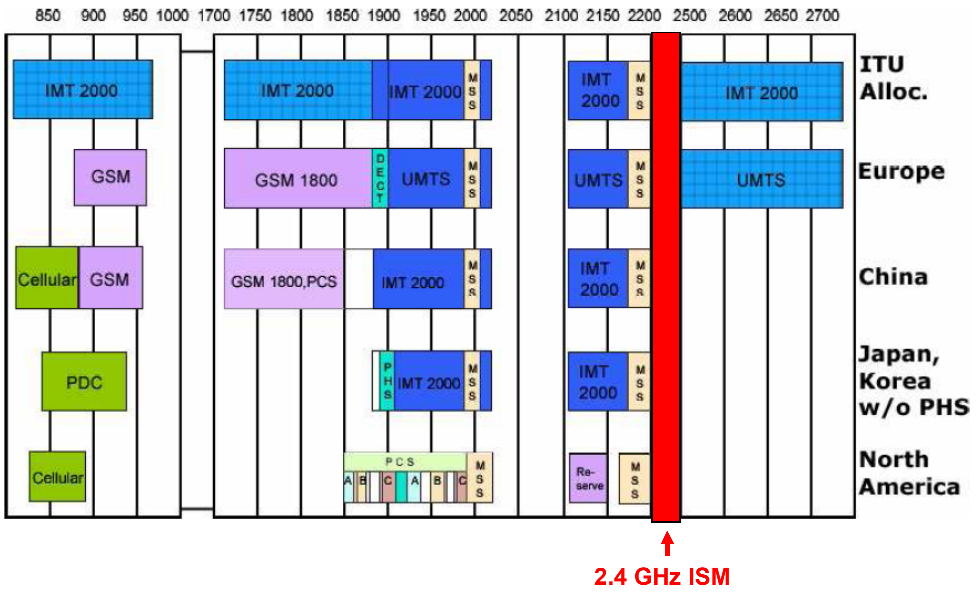
5.0 5.1 5.2 5.3 5.4 5.5 5.6 5.7 5.8 5.9 6.0 GHz

Aeronautical Navigation	*Satellite FSS*	*Radar and Science*	*Aeron. Navig.*	*Radionavigation Maritime navigation*	*Amateur Radio Radiolocation*

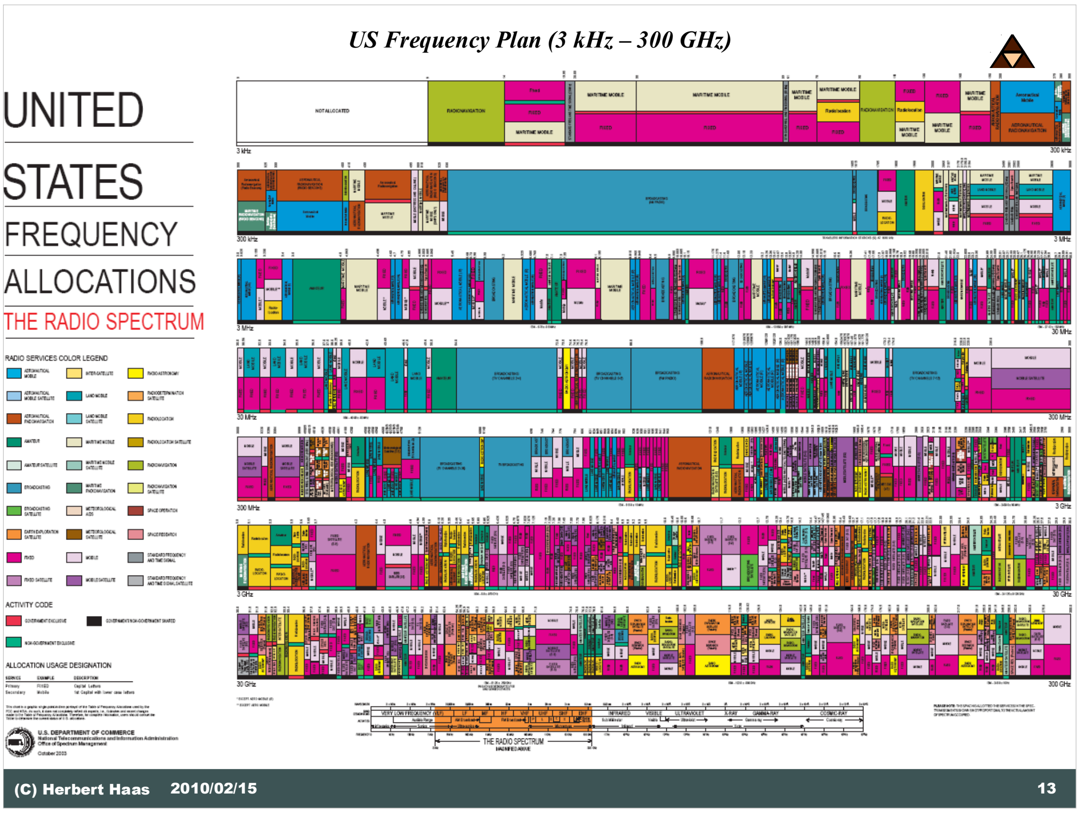
- "Extensions to Operate in Additional Regulatory Domains"
  - Ratified in June, 2001
  - Defines frequency and power limitation for different regulatory domains
- Allows clients to roam across different regulatory domains
  - APs are set to appropriate regulatory domain
  - During association, clients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

802.11d world mode allow a world-wide WLAN operator to announce the local RF limits for its roaming clients via the AP.

"Surrounding" Applications



This is just for your interest and to get a feeling where GSM and UMTS work in comparison to WLAN.



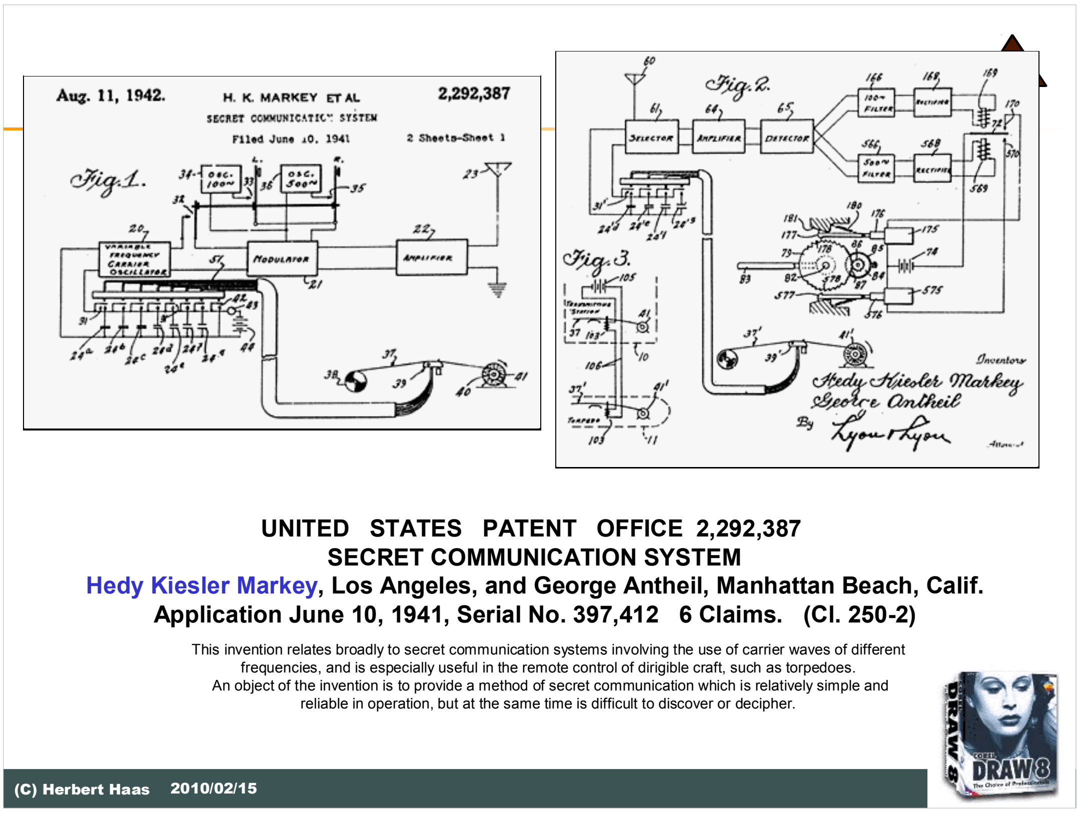
US Frequency Plan (3 kHz – 300 GHz)

This picture should simply provide an impression of the FCC frequency plan, from 3 kHz to 300 GHz (Extremely Low Frequency to Far Infrared).

Clearly it is not that easy to find a free frequency range for new applications…

Modulation Techniques

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



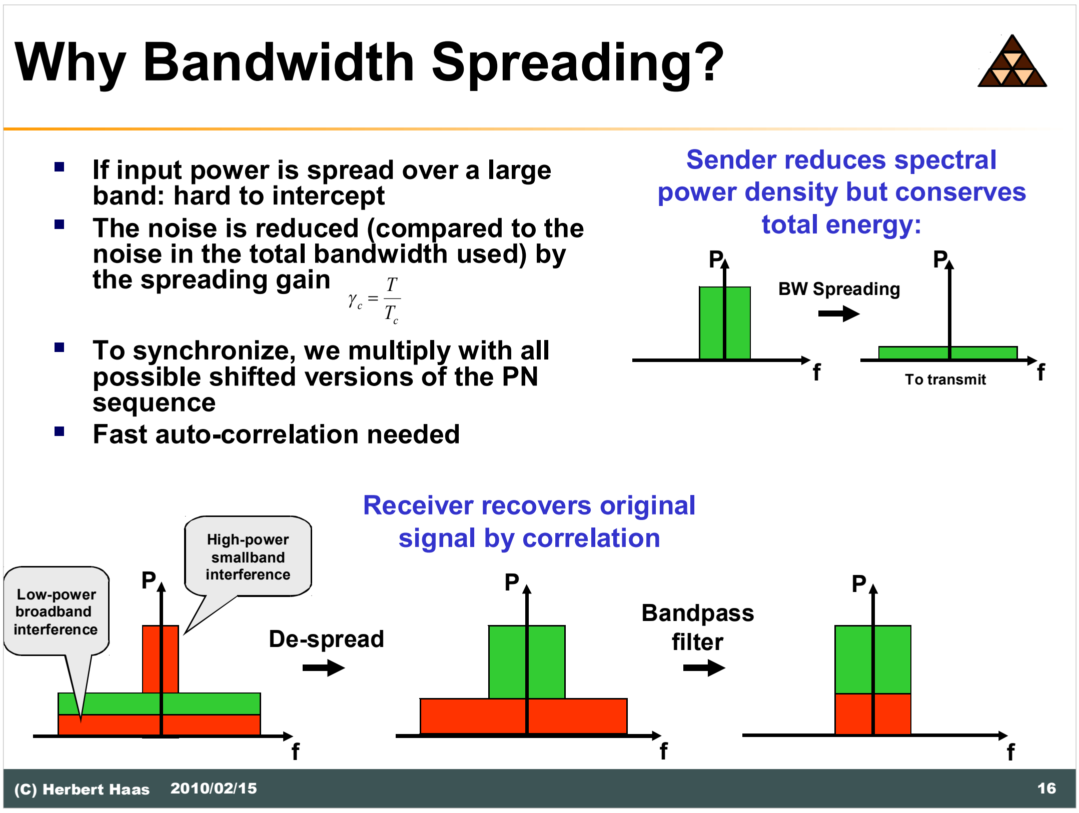
UNITED STATES PATENT OFFICE 2,292,387
SECRET COMMUNICATION SYSTEM
Hedy Kiesler Markey, Los Angeles, and George Antheil, Manhattan Beach, Calif.
Application June 10, 1941, Serial No. 397,412 6 Claims. (Cl. 250-2)

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.

(C) Herbert Haas 2010/02/15

Hedy Lamarr was honored with the Viktor Kaplan Medal of the Austrian Association of Patent Holders and Inventors on October 16, 1998. The medal, considered the highest award which can be bestowed upon inventors in Austria, was presented to Miss Lamarr for her pioneering contribution to enabling radio communications to be made secure from interference and eavesdropping. Miss Lamarr was proposed for the medal by Dr. Peter Paul Sint of the Austrian Academy of Sciences. In support of the nomination, Dr. Sint stated that her invention was decades ahead of its time and anticipated "essential elements of digital logic." Hedy Lamarr was the recipient of a number of technology prizes in the US during 1997. The presentation of the Viktor Kaplan Medal is the first such recognition of her achievement in her homeland Austria. As with prior awards, Miss Lamarr did not personally attend the Kaplan Medal presentation ceremony in Esterhazy Palace in Eisenstadt, Austria. She was represented by her son, Anthony Loder.

BTW: The tremendous fame of the movie "Ecstasy" is due above all to a single scene in which the audience sees Hedy Lamarr swimming nude in a lake and then running through a nearby forest. This sequence - lasting several minutes - is considered the first nude scene in cinematic history and caused a worldwide scandal in the 1930s. "Ecstasy" was then banned in many countries of the world - most notably in the US - or only a radically expurgated version of it was permitted to be shown.



Why Bandwidth Spreading?

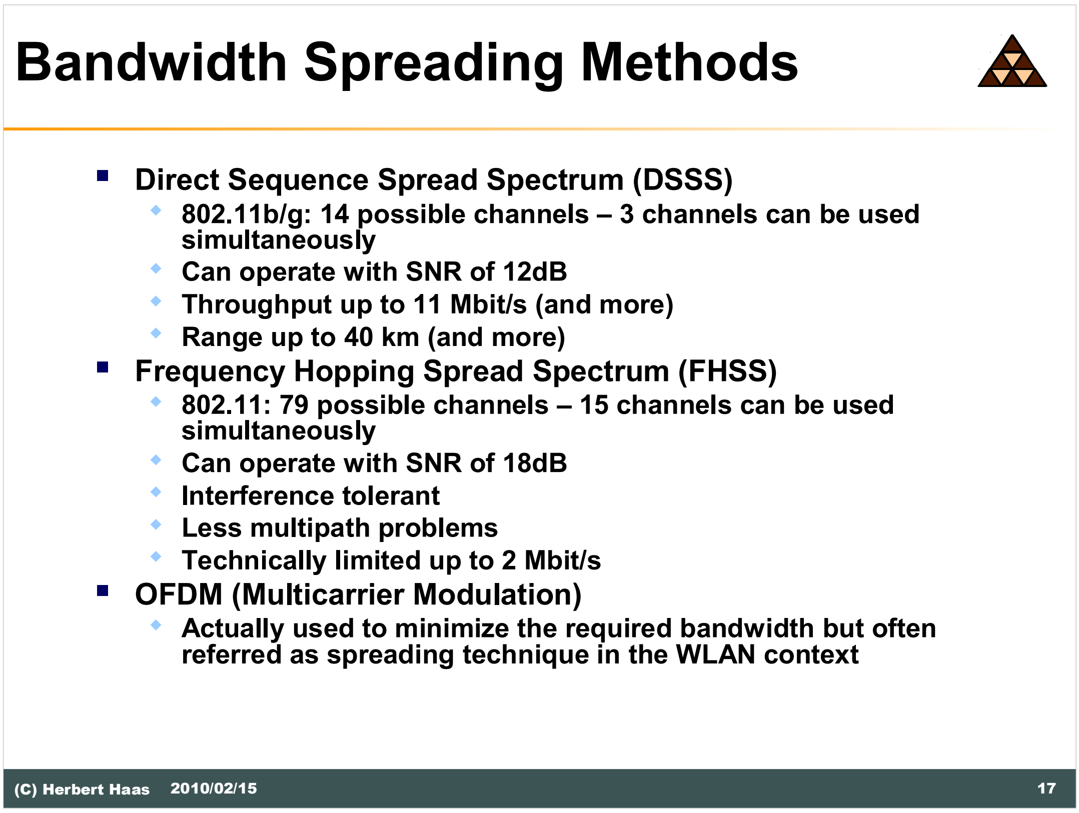
- If input power is spread over a large band: hard to intercept
- The noise is reduced (compared to the noise in the total bandwidth used) by the spreading gain $\gamma_c = \frac{T}{T_c}$
- To synchronize, we multiply with all possible shifted versions of the PN sequence
- Fast auto-correlation needed

Sender reduces spectral power density but conserves total energy:

Receiver recovers original signal by correlation

Low-power broadband interference
High-power smallband interference
P
f
De-spread
P
f
Bandpass filter
P
f

While transmission small- and broadband interferences add to the user signal. Power density could be smaller than in the smallband signal. It is also possible that the power density is smaller then the ambient noise.



Bandwidth Spreading Methods

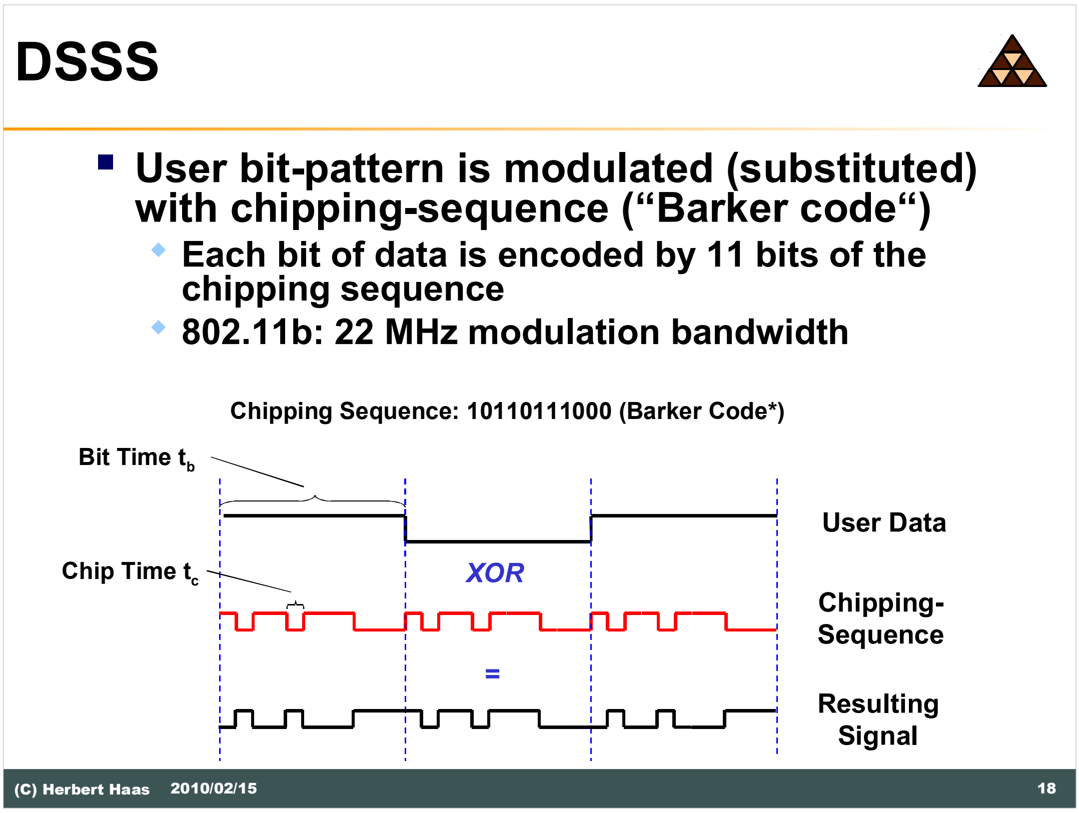
- Direct Sequence Spread Spectrum (DSSS)
  - 802.11b/g: 14 possible channels – 3 channels can be used simultaneously
  - Can operate with SNR of 12dB
  - Throughput up to 11 Mbit/s (and more)
  - Range up to 40 km (and more)
- Frequency Hopping Spread Spectrum (FHSS)
  - 802.11: 79 possible channels – 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

(C) Herbert Haas 2010/02/15 17

DSSS defines a set of channels spaced across the whole radio bandwidth. There are 14 of these channels, but channel 14 is reserved for Japan. DSSS modulates the data with a spreading code (chipping) and transmits the result on only one of these channels. There has to be 30MHz between the carrier frequencies for multiple access points to operate within the same area without interference. Since the entire bandwidth is 83.5MHz, only a maximum of 3 DSSS access points can operate within the same area. The limited available total bandwidth is also the methods vulnerability. If narrow band interference occurs in the used channel, one can only wait until it disappears before communications can be resumed. In return DSSS gives a longer range. The modulation technique can operate with a signal to noise ratio (SNR) of 12dB where FHSS operates with SNR of 18dB.

FHSS defines a set of channels spaced across the whole radio bandwidth. Here in Norway, there are 79 such channels. When transmitting, FHSS uses only one channel at a time in a predetermined sequence and dwell time between hops. There are 78 such sequences and they are orthogonal so that they do not interfere with each other. This enables as many as approx. 15 access points belonging to different systems, to coexist. Because the whole bandwidth is available and the signal is sent/received on only a small part of it at a time, this is the method most tolerant to narrow band interference. This would not block the communication entirely but only when the hopping pattern happens to hit the interfering frequency and only for the duration of the dwell time, often set to 128ms. All band interference would of course stop FHSS also. FHSS also has lowest power consumption.

Orthogonal Frequency Division Multiplexing (OFDM) is a multicarrier transmission method and actually tries to reduce the required bandwidth. Using OFDM together with QAM (see later) very high data rates can be achieved, therefore a given bandwidth (20-22 MHz with WLANs) is optimally utilized.



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*)

(C) Herbert Haas 2010/02/15 18

In 802.11, the chipping sequence is known as the Barker code, which is an 11-bit sequence (10110111000) that has certain mathematical properties making it ideal for modulating radio waves. The basic data stream is XORed with the Barker code to generate a series of data objects called chips. Each bit is "encoded" by the 11 bit Barker code, and each group of 11 chips encodes one bit of data.

Direct Sequence Spread Spectrum (DSSS) uses a XOR – Chipping Sequence on the userdata to spread the signal (digital modulation). The spreaded signal is modulated to a carrier (analog modulation).

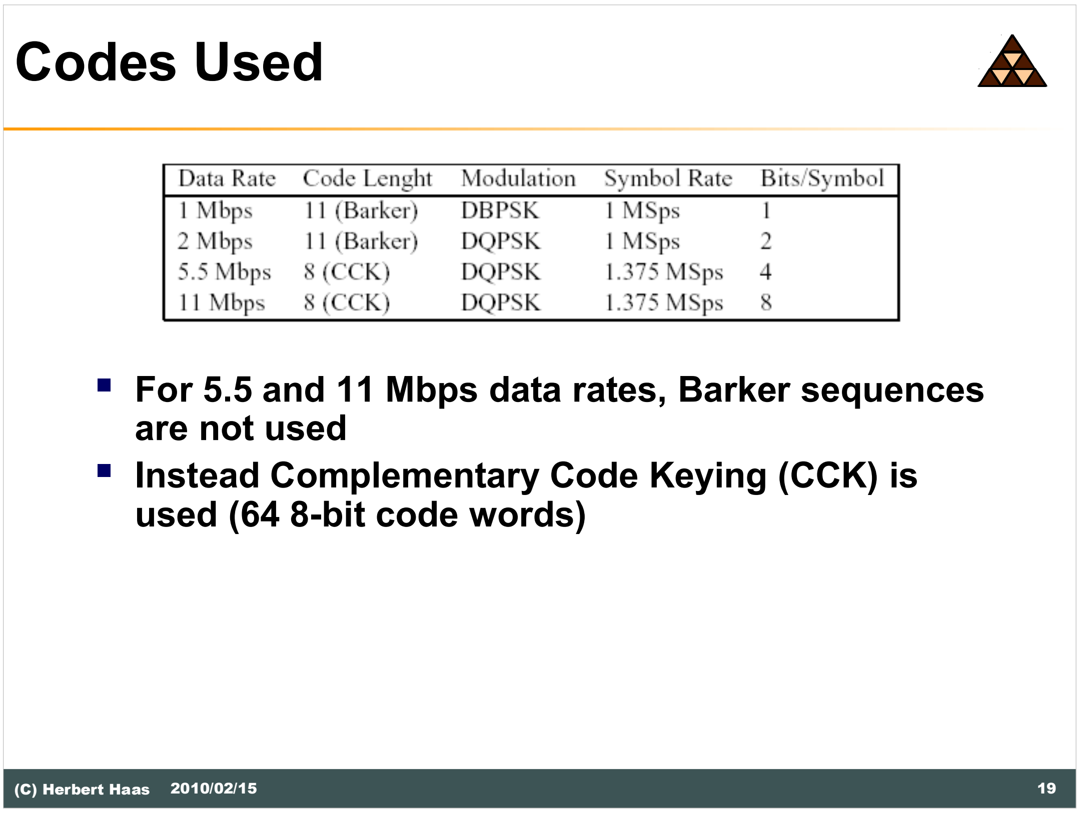
Userdata bit → bit length of t_b

Chipping Sequence → smaller bit length of t_c (chips)

Spreading Factor: $s = t_b/t_c$

Bandwidth of spreaded signal → s*w

Civil uses → spread factor of 10-100 (Barker-Code has factor 11), Military → spread factor up to 10000



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)**

(C) Herbert Haas 2010/02/15 19

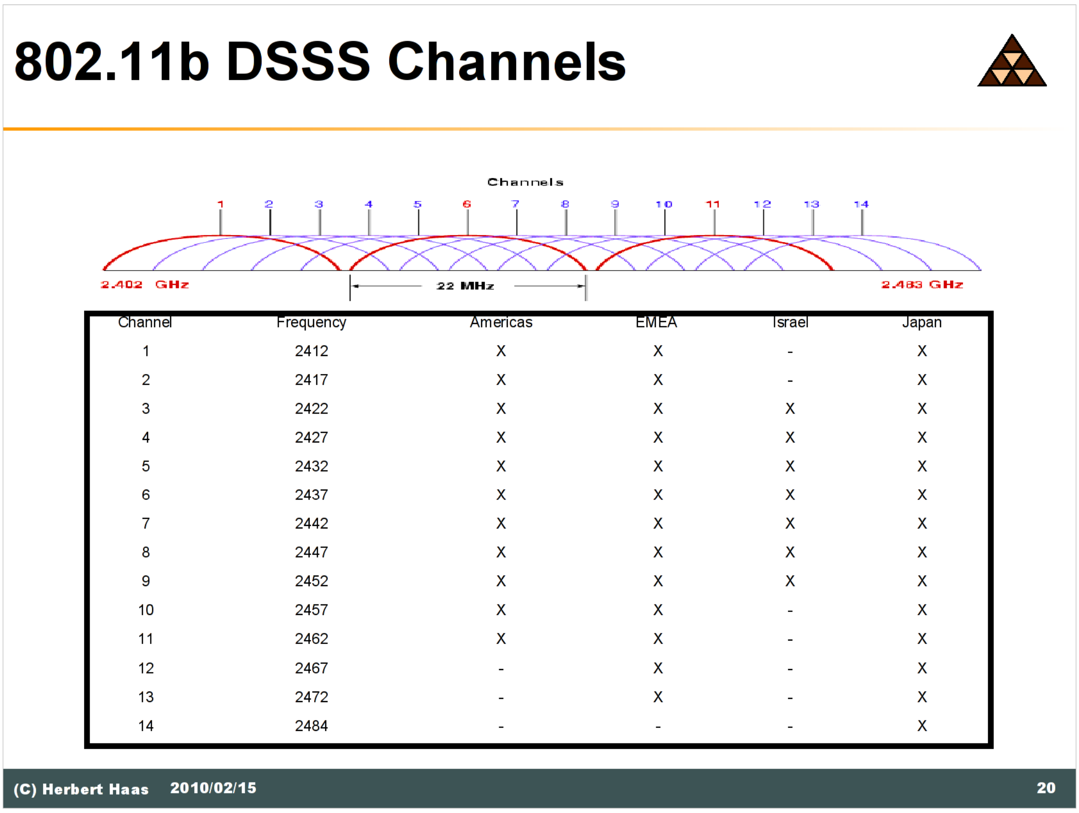
By regulations, a DSSS system in the ISM band must have a minimum of 10 dB processing gain

1 Mbps 11 bit Barker code processing gain = 10.4 dB

11 Mbps CCK processing gain = 11 dB

Any highrate modulation is more susceptible to jamming, multipath interference and filter distortion than lower rate modulation because of the higher required SNR (E_S/N_0)

Processing gain is the reason why DS is relatively jamming resistant provided that the WLAN hardware is designed well (which is often not the case with cheap hardware).

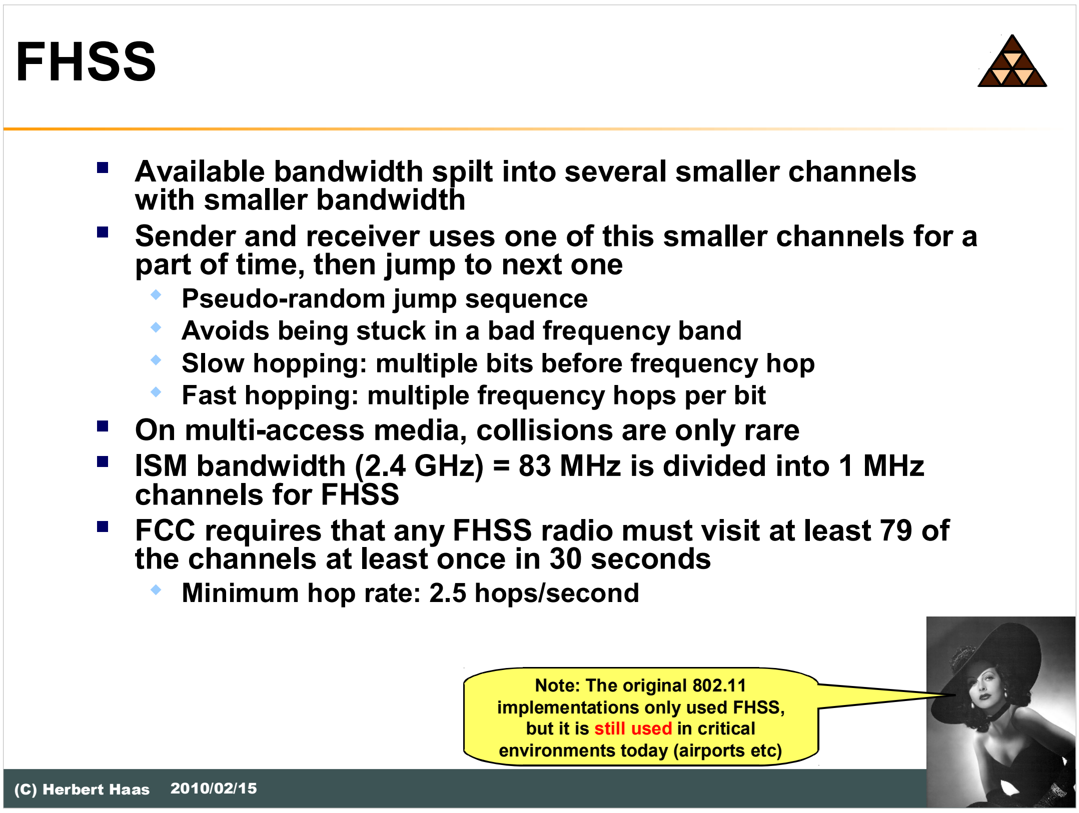


802.11b DSSS Channels

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

Fourteen channels are defined in the IEEE 802.11b Direct Sequence (DS) channel set. Each DS channel as transmitted is 22 MHz wide, however the channel center separation is only 5 MHz. This leads to channel overlap such that signals from neighboring channels can interfere with each other. In a 14-channel DS system (11 usable in the US), only three non-overlapping (and hence, non-interfering) channels, 25 MHz apart are possible (for example, Channels 1, 6, and 11).

This channel spacing governs the use and allocation of channels in a multi-access points environment such as an office or campus. Access points are usually deployed in "cellular" fashion within an enterprise where adjacent access points are allocated non-overlapping channels. Alternatively, access points can be collocated using Channels 1, 6, and 11 to deliver 33 Mbps bandwidth to a single area (but only 11 Mbps to a single client).



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)

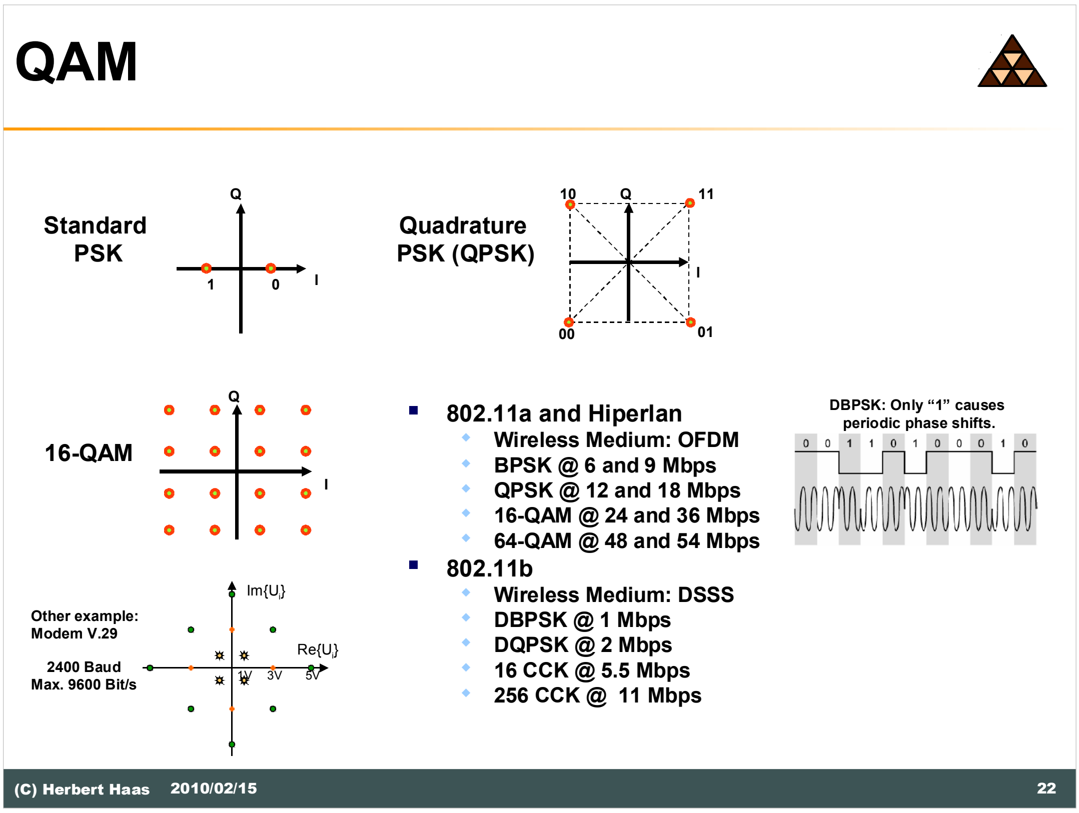
Frequency Hopping Spread Spectrum (FHSS) uses a radio that moves or hops from one frequency to another at predetermined times and channels. The hopping pattern is specified in the WLAN beacons.

The regulations require that the maximum time spent on any one channel is 400mS. For the 1- and 2-Mb FH systems, the hopping pattern must include 75 different channels, and must use every channel before reusing any one.

For the Wide Band Frequency Hopping (WBFH) systems, that permit up to 10-Mb data rates, the rules require use of at least 15 channels, and they cannot overlap. With only 83MHz of spectrum, it limits the systems to 15 channels, thereby causing scalability issues.

GFSK is used for the modulation process.

FHSS was used for the initial IEEE 802.11 standard, providing up to 2 Mbit/s but it is still available today, manufactured by certain vendors, to allow wireless data transmission in difficult environments such as airports etc.



QAM

- 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

It is important to understand that spread spectrum (or OFDM) techniques are always combined with a symbol modulation scheme. Quadrature Amplitude Modulation (QAM) is a general method where practical methods such as BPSK, QPSK, etc are derived from.

The main idea of QAM is to combine phase and amplitude shift keying. Since orthogonal functions (sine and cosine) are used as carriers, they can be modulated separately, combined into a single signal, and (due to the orthogonality property) de-combined by the receiver.

And since A*cos(wt + phi) = A/2{cos(wt)cos(phi) – sin(wt)sin(phi)} QAM can be easily represented in the complex domain as Real{ A*exp(i*phi)*exp(i*wt)}.

The standard PSK method only use phase jumps of 0° or 180° to describe a binary 0 or 1. In the right picture above you see a enhanced PSK method, the Quadrature PSK (QPSK) method. While using Quadrature PSK each condition (phase shift) represent 2 bits instead of 1. Now it is possible to transfer the same datarate by halved bandwidth.

The QSK signal uses (relative to reference signal)

- 45° for a data value of 11

- 135° for a data value of 10

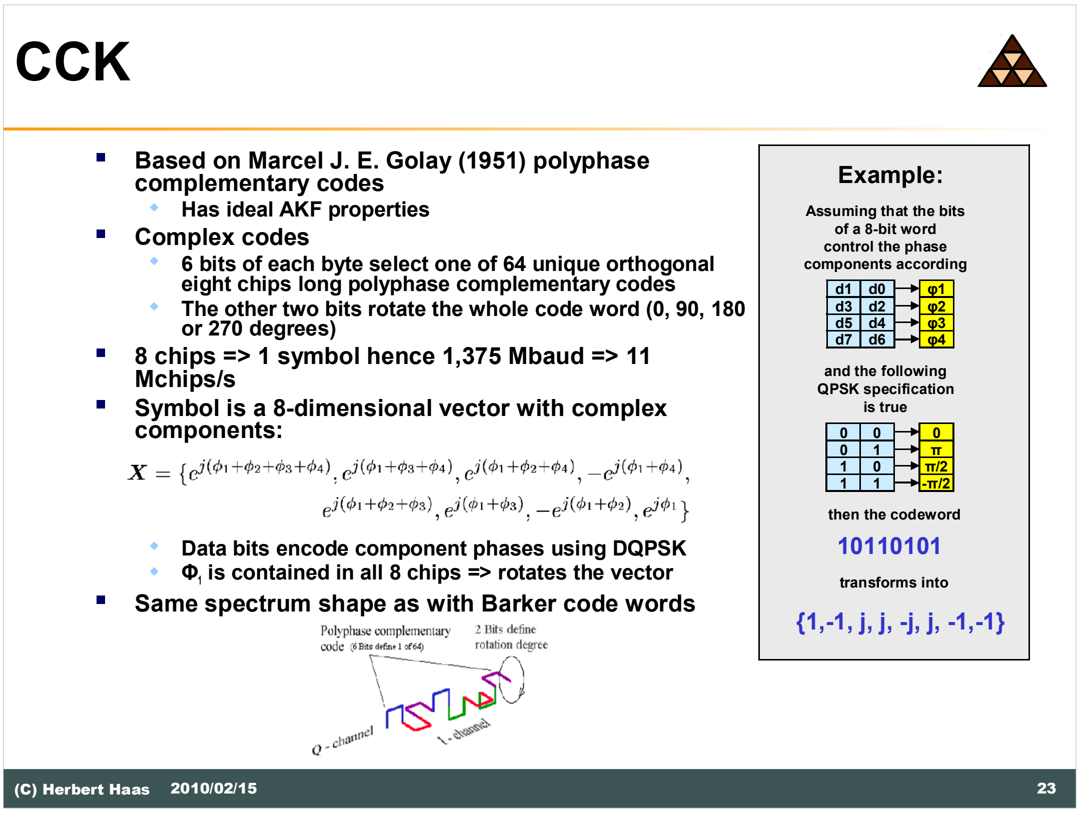
- 225° for a data value of 00

- 315° for a data value of 01

To reconstruct the original data stream the receiver need to compare the incoming signal with the reference signal. The synchronization is very important.

<u>Why not coding more bits per phase jump ?</u>

Especial in the mobile communication there are to much interferences and noise to encode right. As more bits you use per phase jump, the signal gets more “closer”. It is getting impossible to reconstruct the original data stream. In the wireless communication the QPSK method has proven as a robust and efficient technique.



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:

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

  - 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

Polyphase complementary code (6 Bits define 1 of 64)
2 Bits define rotation degree
Q - channel
I - channel

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

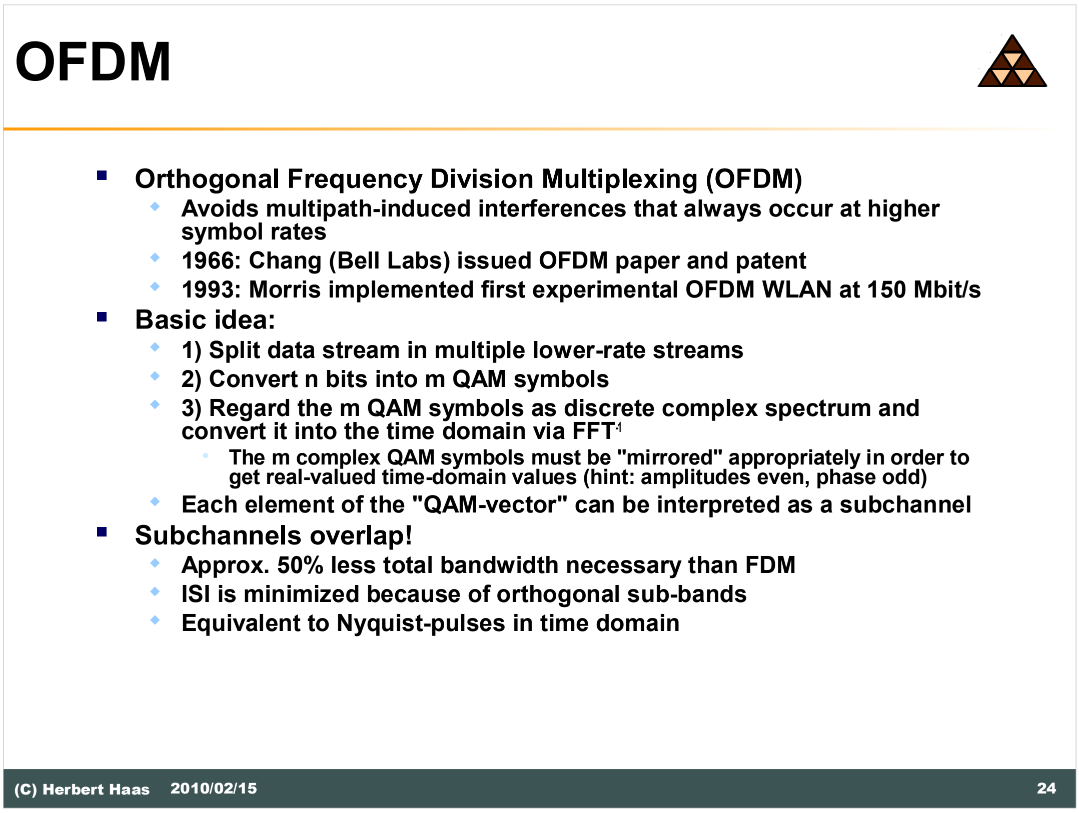
transforms into

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

(C) Herbert Haas 2010/02/15 23

Based on Marcel J. E. Golay, 1951, spectrometer application. The Walsh transform is a special case of the Fourier transform and used for the correlation. The eight components of the 8-dimensional vector are complex chips, as shown in the example on the right (1, -1, j, j, -j, j, -1, -1).

CCK is a variation on M-ary Orthogonal Keying modulation, which uses I/Q modulation architecture with complex symbol structures. CCK allows the 80211b for multi-channel operation in the 2.4 GHz band using the existing 802.11 DSSS channel structure scheme. The spreading employs the same chipping rate and spectrum shape as the 802.11 Barker's code word. The spread function for CCK in 802.11b is chosen from a set of M nearly orthogonal vectors by the data word. CCK uses one vector from a set of 64 complex (QPSK) vectors for the symbol and thereby modulates 6 bits (one of 64) on each 8 chips spreading code symbol. In the 802.11b, the formula that defines the CCK codewords has 4 phase terms. The first of them modulates all of the chips and this is used for the QPSK rotation of the whole code vector. The second modulates every odd chip, the third modulates every odd pair of chips and the forth modulates every odd quad of chips.



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

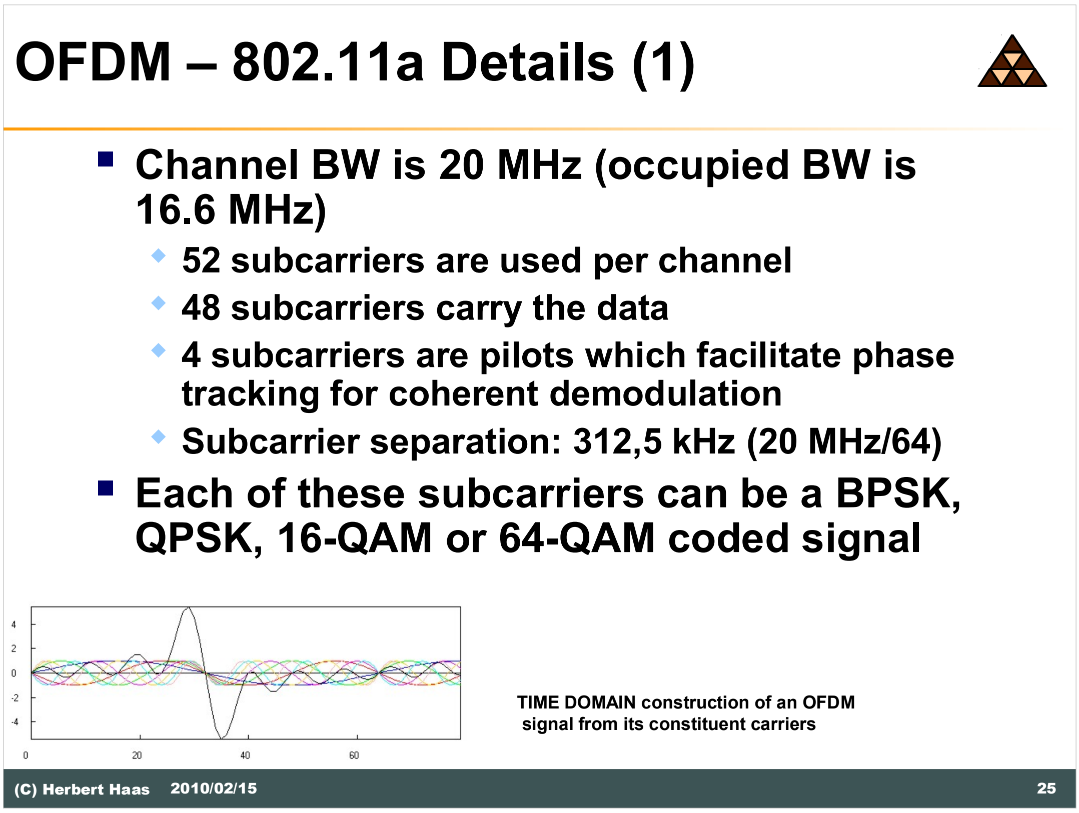
(C) Herbert Haas 2010/02/15 24

In Europe a special modulation type for digital radio, called Digital Audio Broadcast (DAB) is used. This modulation method uses many frequencies at the same time (Multicarrier Modulation (MCM)). The big advantage is the robustness against ISI. As higher the symbol rate as higher the ISI effect. Because of this reason MCM splits the symbol rate into more stream with lower rate on a own carrier.

For example:

n Symbols per second uses *c* new carrier. Then only *n*/*c* symbols per second need to be transferred, and each symbol represent 2 bits (like QPSK). Only small parts of the signal will be destroyed while strong interferences.

The DAB standard can use 192-1536 carrier at the same time.


4
2
0
-2
-4
0
20
40
60

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

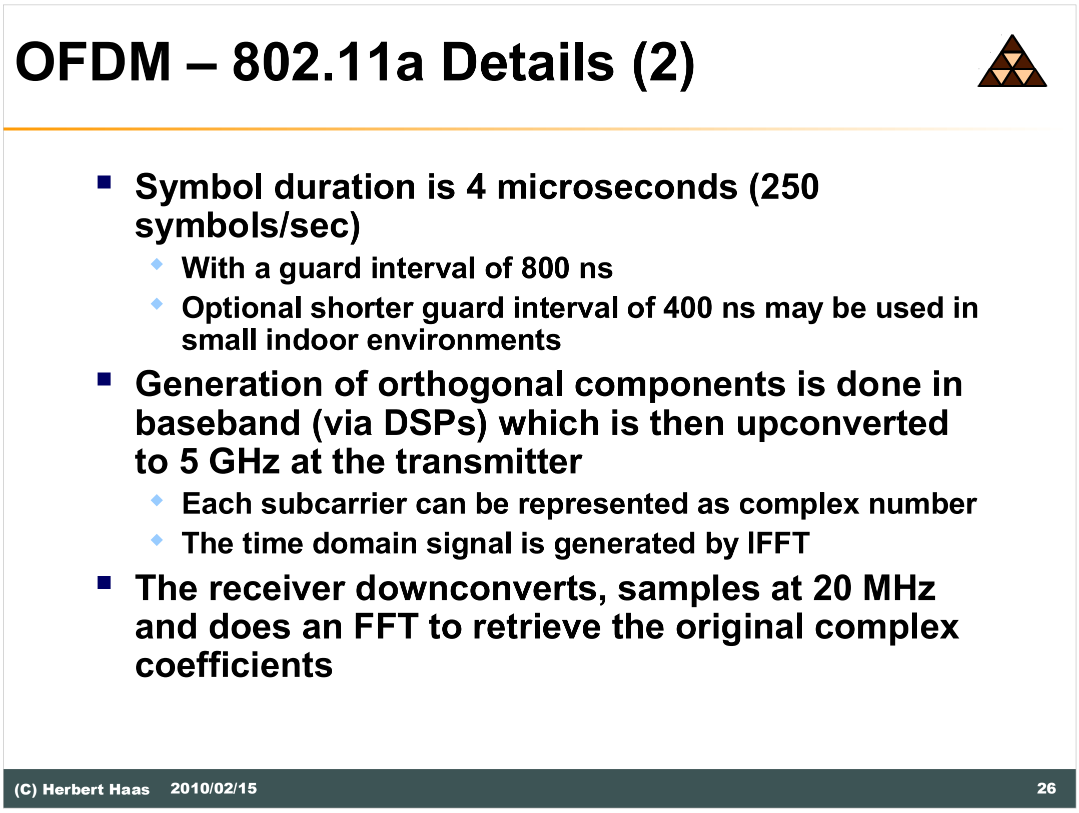
TIME DOMAIN construction of an OFDM signal from its constituent carriers

(C) Herbert Haas 2010/02/15 25

OFDM is efficiently realized by the use of effective signal processing, fast-fourier transform, in the transmitter and receiver. This significantly reduces the amount of required hardware compared to earlier FDM-systems. One of the benefits of OFDM is the robustness against the adverse effects of multipath propagation with respect to intersymbol interference. It is also spectrally efficient because the subcarriers are packed maximally close together. OFDM also admits great flexibility considering the choice of and realization of different modulation alternatives.

OFDM, Orthogonal Frequency Division Multiplex, is a special form of multicarrier modulation. The basic idea is to transmit broadband, high data rate information by dividing the data into several interleaved, parallel bit streams, and let each one of these bit streams modulate a separate subcarrier. In this way the channel spectrum is passed into a number of independent non-selective frequency subchannels. These sub channels are used for one transmission link between the AP and the MNs.

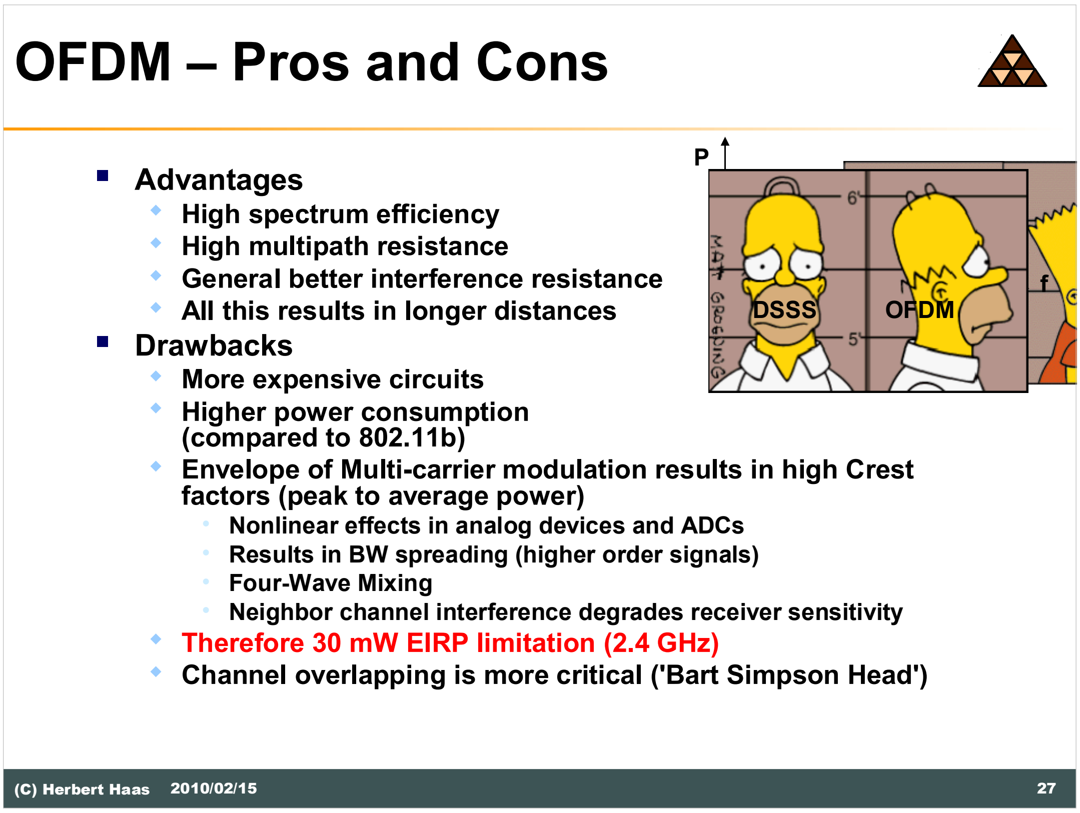
The time domain construction of an OFDM signal from its constituent carriers is shown above. The data values can be adjusted. For some data combinations the peak power is much higher than for others and this can complicate analog amplifier design in OFDM systems. In multipath channels, the delays can cause symbol overlap, destroying the perfect sum of sinusoids. This is easily fixed by cyclicly extending the signal by a length longer than the channel delay.



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

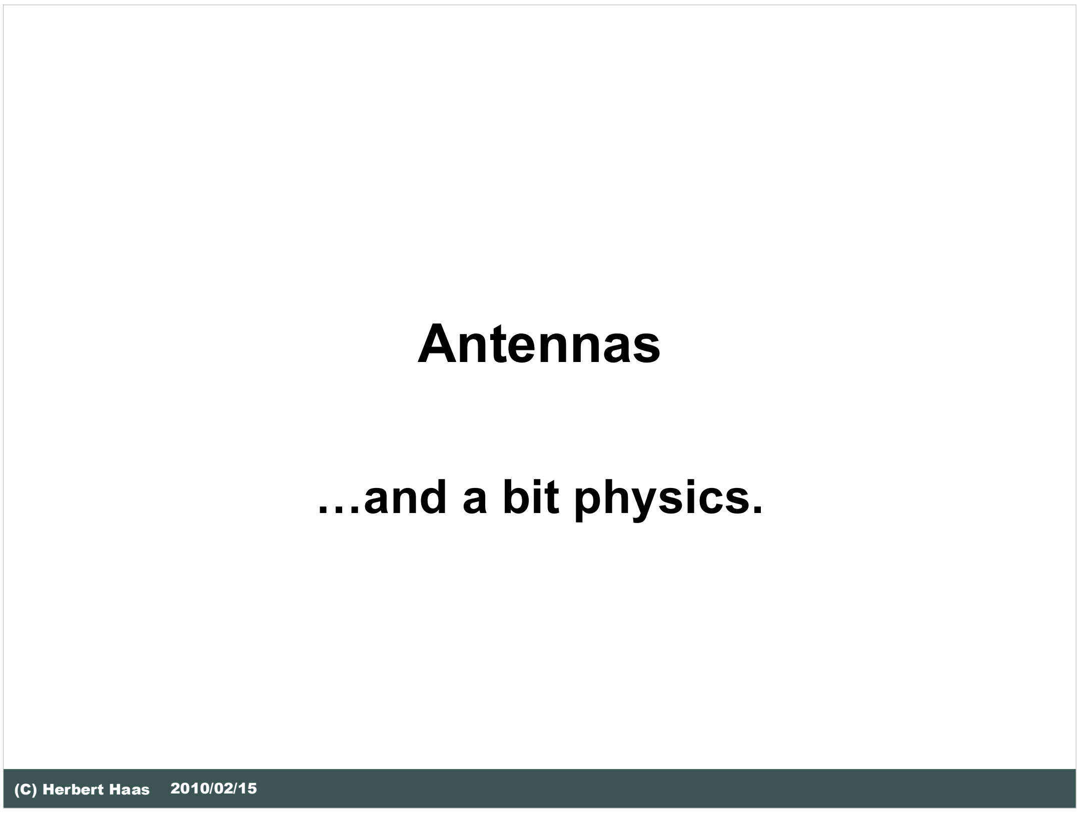
The guard interval is needed to achieve the desired spectral shape.



OFDM – Pros and Cons

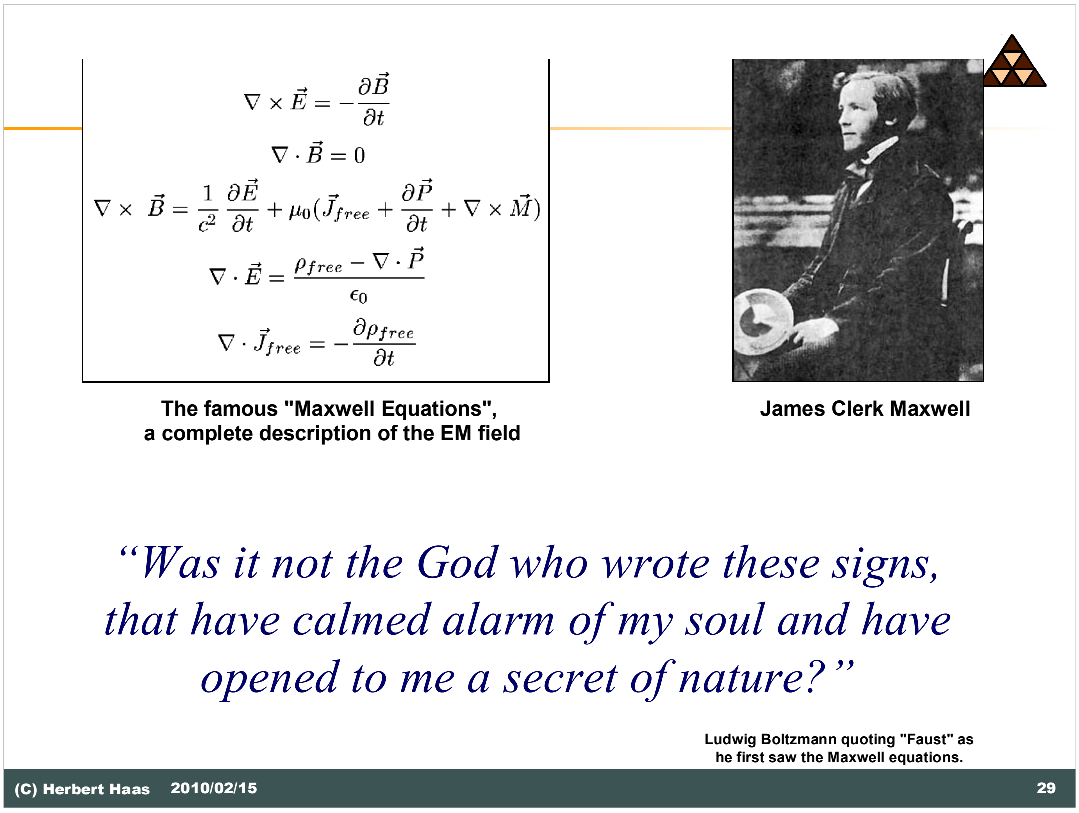
- Advantages
  - High spectrum efficiency
  - High multipath resistance
  - General better interference resistance
  - All this results in longer distances
- Drawbacks
  - More expensive circuits
  - Higher power consumption (compared to 802.11b)
  - Envelope of Multi-carrier modulation results in high 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')

Note: OFDM was originally only planned for 802.11a in the "clean" 5 GHz band since the QAM used here is relatively noise-sensitive, much more compared to DSSS. Considering this, how will 802.11g really perform in noisy 2,4 GHz environments?



Antennas

…and a bit physics.



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

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

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

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

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

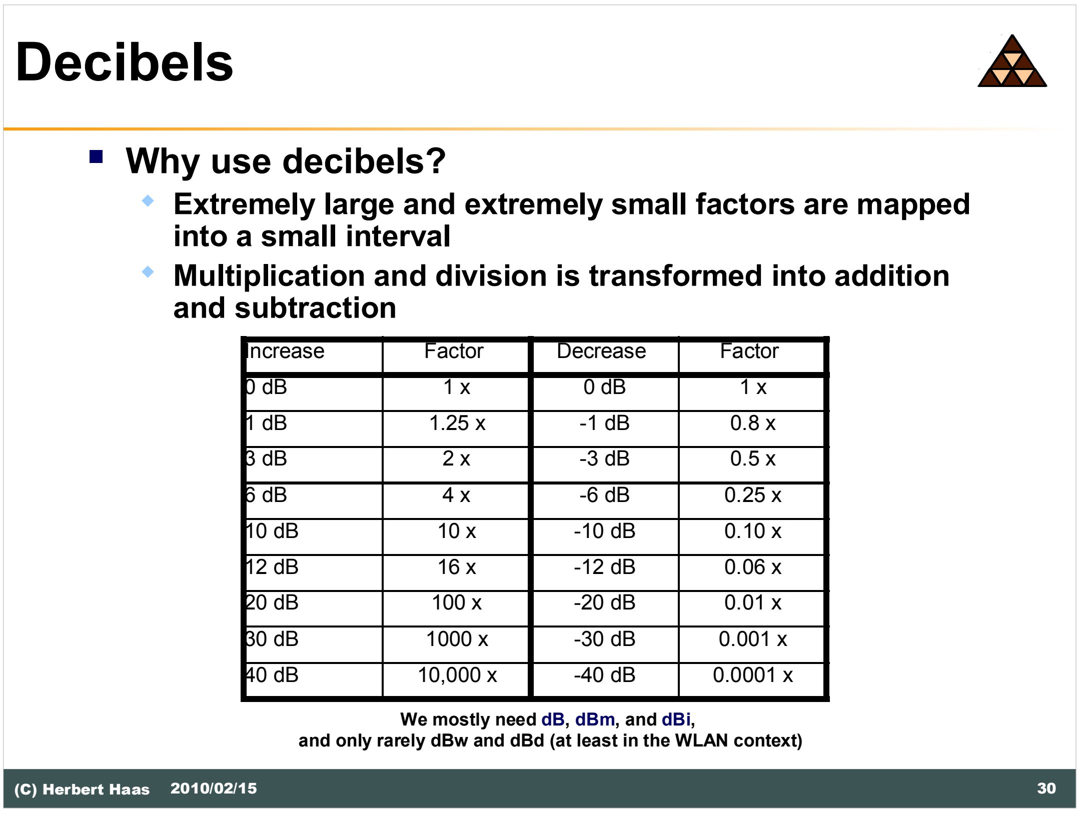
The famous "Maxwell Equations",
a complete description of the EM field

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.

All phenomena of the electromagnetic field are covered by the famous Maxwell's equations. Fortunately (or not?) we do not need these equations in the following sections but since they are so remarkable, short, and the basis of all this, they are presented here in order to praise Maxwell.



Decibels

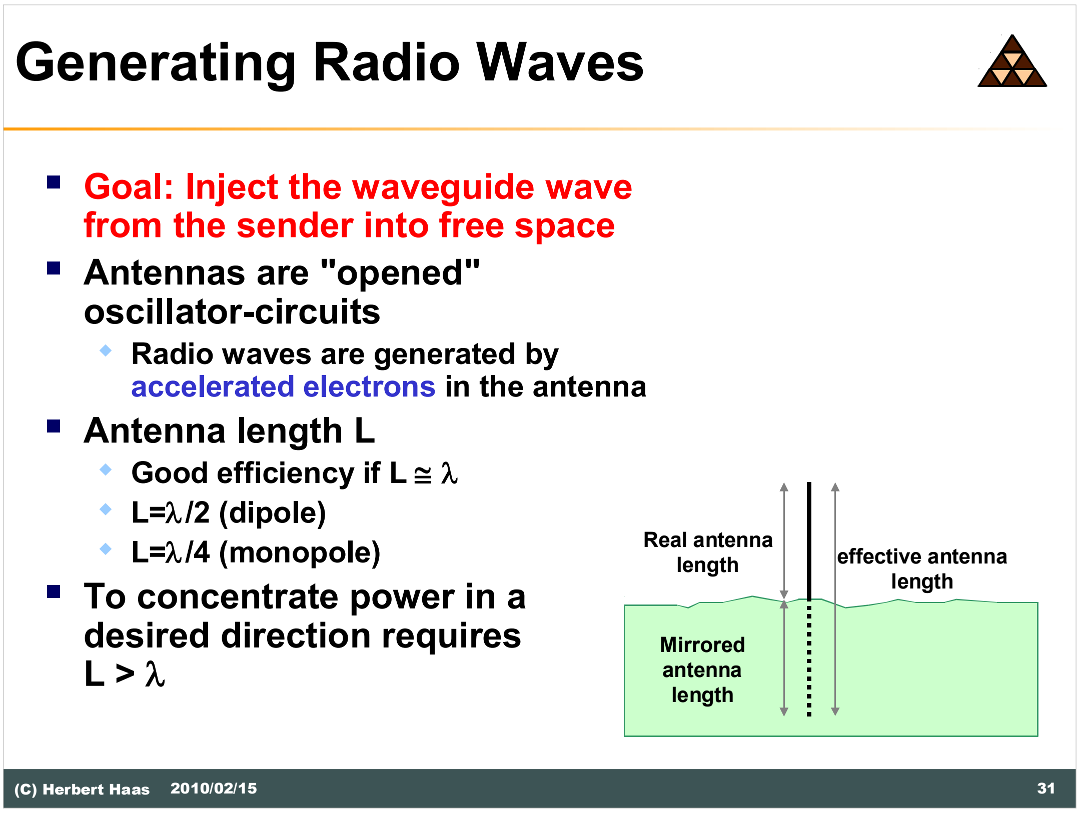
- **Why use decibels?**
  - **Extremely large and extremely small factors are mapped into a small interval**
  - **Multiplication and division is transformed into addition and subtraction**

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)

Radio Frequency signals are subject to various losses and gains as they pass from transmitter through cable to antenna, through air (or solid obstruction), to receiving antenna, cable and receiving radio. With the exception of solid obstructions, most of these figures and factors are known and can be used in the design process to determine whether an RF system such as a WLAN will work.

In the table above you see some examples, list by dB. An increase of 3 dB indicates a doubling (2x) of power. An increase of 6 dB indicates a quadrupling (4x) of power. Conversely, a decrease of 3 dB is a halving (1/2) of power, and a decrease of 6 dB is a quarter (1/4) the power.



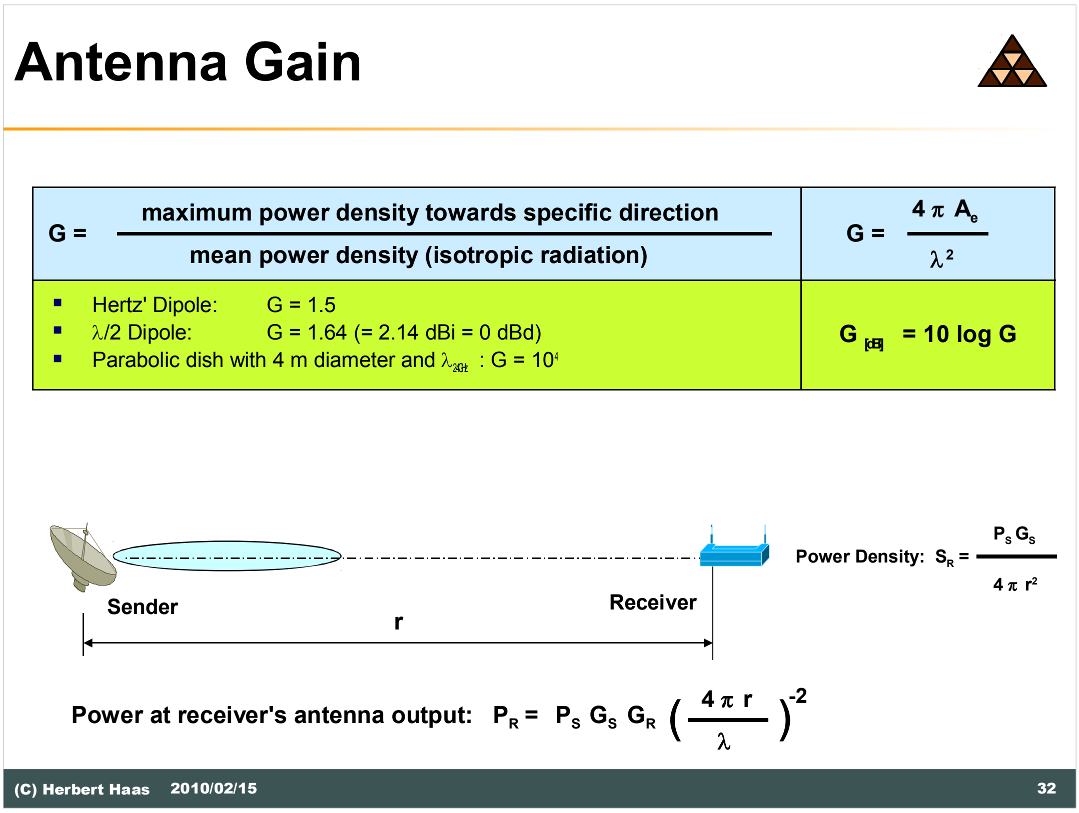
Generating Radio Waves

- 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

Real antenna length
effective antenna length
Mirrored antenna length

(C) Herbert Haas 2010/02/15 31

An applied alternating voltage (e. g. oscillating at 2.4 GHz) force the electrons to move along the axis of an antenna (back and forth). Each time the electrons change the direction they emit radiation. This radiation is similarly 'oriented' or polarized as the current from which is was originated.



Antenna Gain

$$G = \frac{\text{maximum power density towards specific direction}}{\text{mean power density (isotropic radiation)}}$$

$$G = \frac{4 \pi A_e}{\lambda^2}$$

- Hertz' Dipole: $G = 1.5$
- $\lambda/2$ Dipole: $G = 1.64$ (= 2.14 dBi = 0 dBd)
- Parabolic dish with 4 m diameter and λ_{2GHz} : $G = 10^4$

$$G_{[dB]} = 10 \log G$$

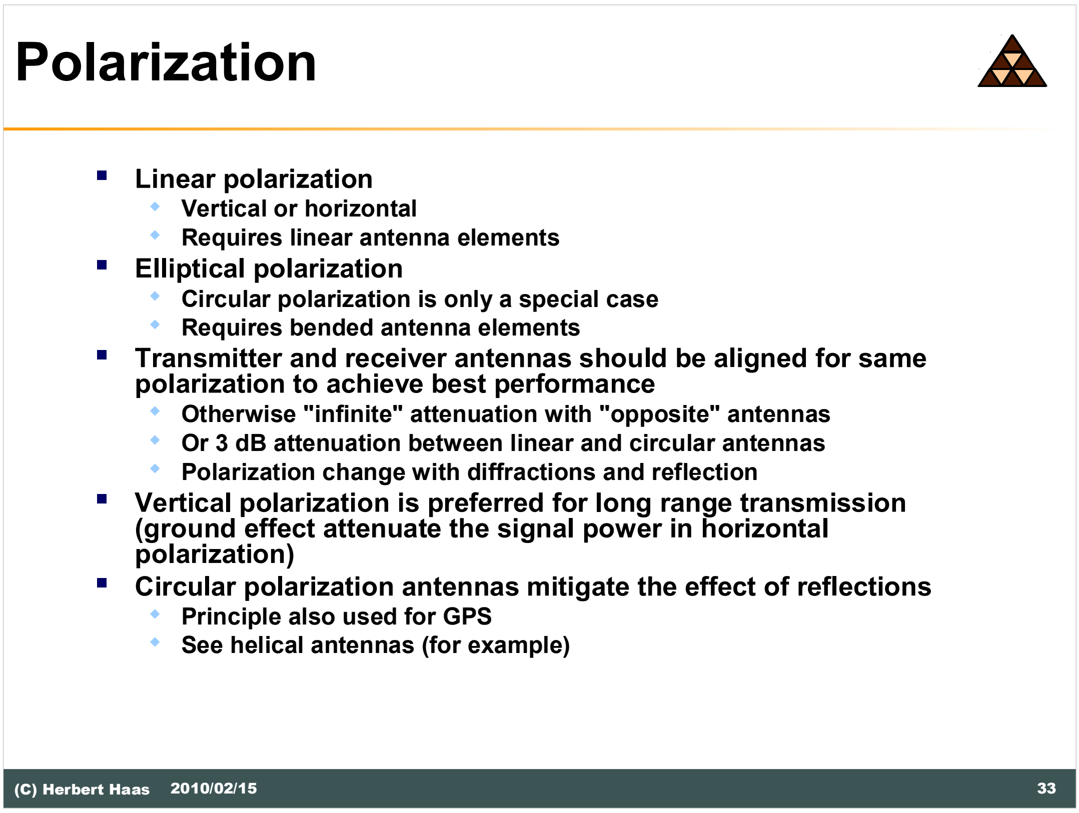
Power Density: $S_R = \frac{P_S G_S}{4 \pi r^2}$

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

Ae ... effective antenna surface ("aperture").

The equation for the received power is sometimes also called "Friis' transmission equation".

Note that for real world (especially indoor) calculations, the effective antenna gain is smaller because of obstacles, multipath, etc.

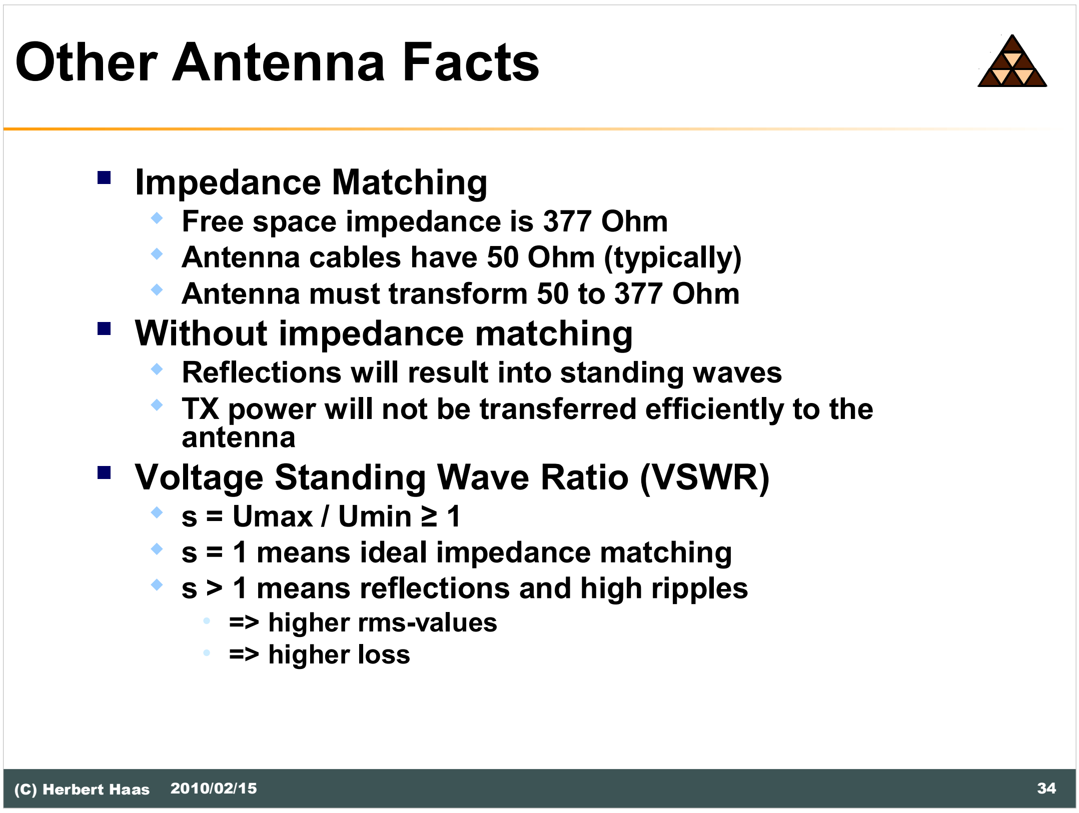


Polarization

- 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)

Vertical polarization is the first choice for WLAN applications because most deployments require to maximize the distance in the horizontal direction. As it can be seen in antenna diagrams, vertically polarized antennas are perfectly suited for horizontal transmissions.

Vertical polarization is also preferred for long range transmission because the ground effect attenuate the signal power in horizontal polarization case in long range.



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 = Umax / Umin ≥ 1
  - s = 1 means ideal impedance matching
  - s > 1 means reflections and high ripples
    - => higher rms-values
    - => higher loss

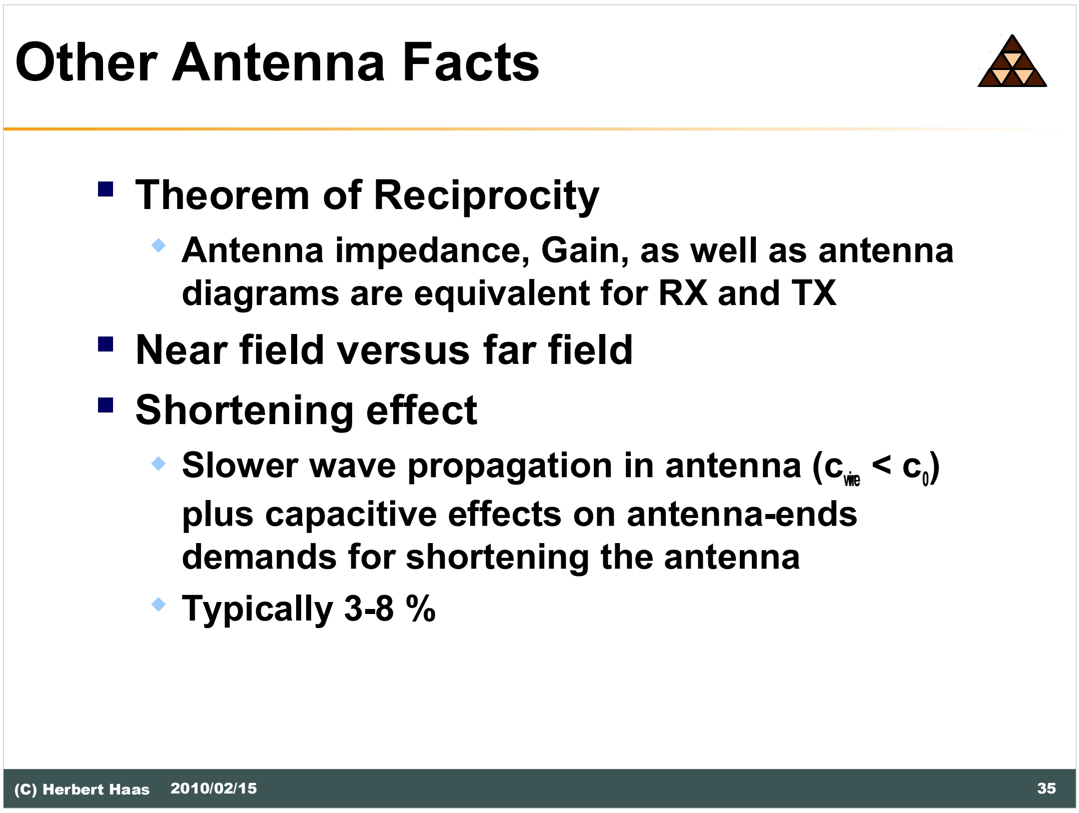
Zo = sqrt (mu_o / eps_o) = 377 Ohm … far field.

Voltage maximum on open end, no current.

Umax = |U_incident| + |U_reflection|

Umin = |U_incident| - |U_reflection|

VSWR should be measured at antenna feedpoint (where the reflection occurs) which is typically not possible.

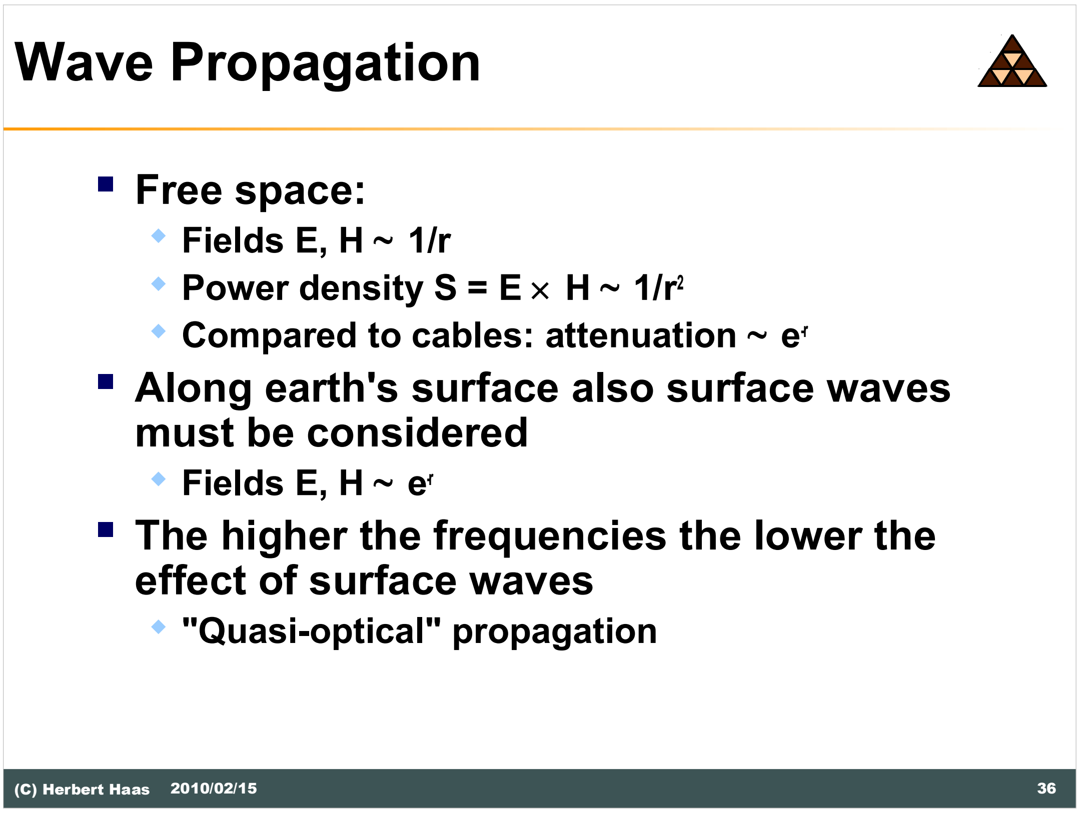


Other Antenna Facts

- 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 %

The reciprocity theorem was first stated by Rayleigh and Helmholtz and it was later applied to the problem of antennas by Carson. This theorem basically says that the antenna parameters remain the same no matter whether the antenna is used for sending or receiving. More practically, upon using two different antennas, one for sending, the other for receiving, we would measure the same currents on the receiving-antenna, even if we switch TX and RX. The reciprocity theorem can be proved from Maxwell's equations and are only valid in isotropic media between the antennas (e. g. certain ferrites are not isotropic).

Mostly the antenna endpoints contribute to the shortening effect, while inner half-wave "pieces" remain constant. Therefore, the longer the antenna the less dramatic the effect.



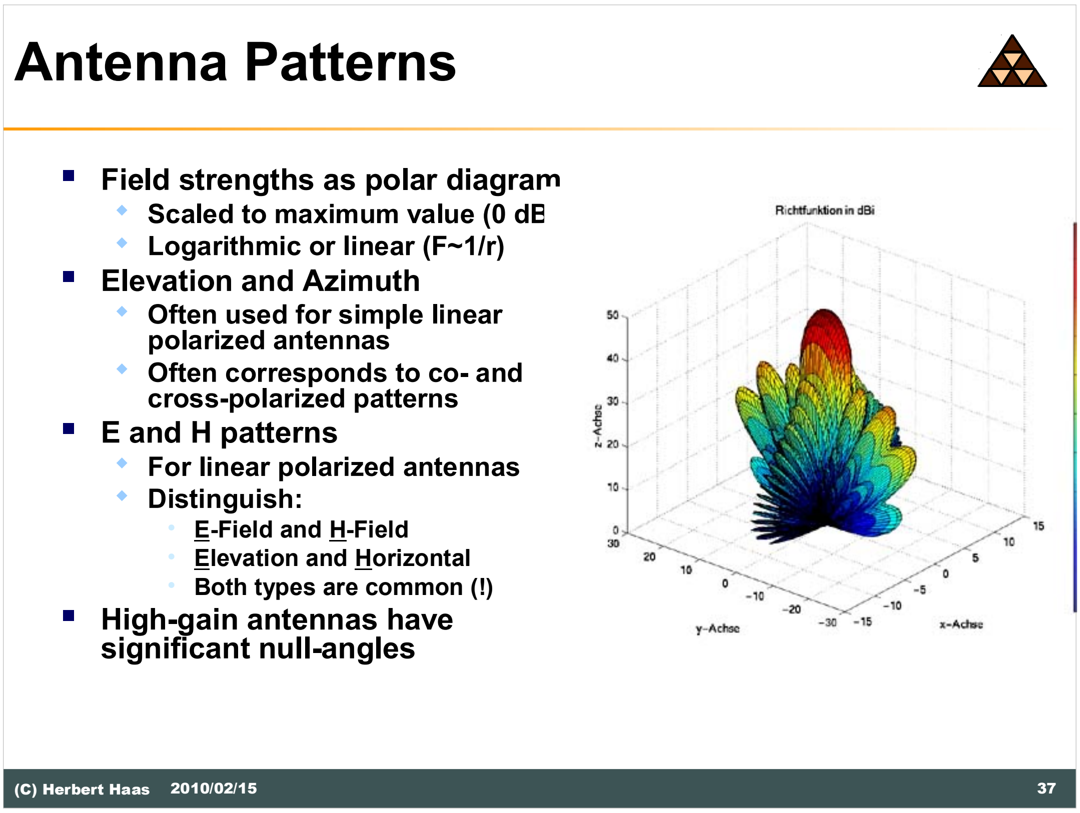
Wave Propagation

- Free space:
  - Fields E, H ~ 1/r
  - Power density S = E × H ~ $1/r^2$
  - 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

(C) Herbert Haas 2010/02/15 36

The 'inverse square law' is only valid for powers not for field strengths.

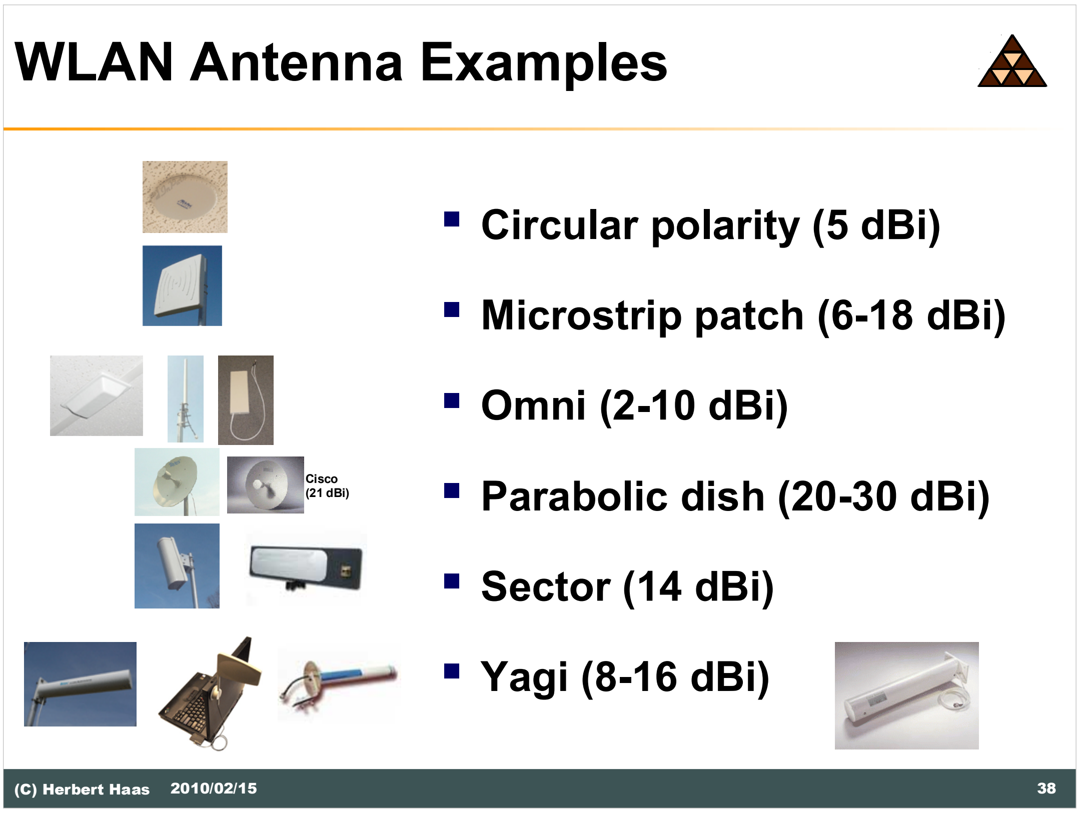
Note that in general the energy is radiated over multiple wave components, for example also surface waves may exist along the earth surface (usually only with longer wavelengths).



Antenna Patterns

- Field strengths as polar diagram
  - Scaled to maximum value (0 dE
  - 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

Complex antennas, such as many television broadcast antennas, include a significant signal in both the horizontal and vertical polarizations. The azimuth pattern for these antennas is often supplied for both polarizations, and the complexity of the antenna can result in significantly different azimuth patterns for the two polarizations.



WLAN Antenna Examples

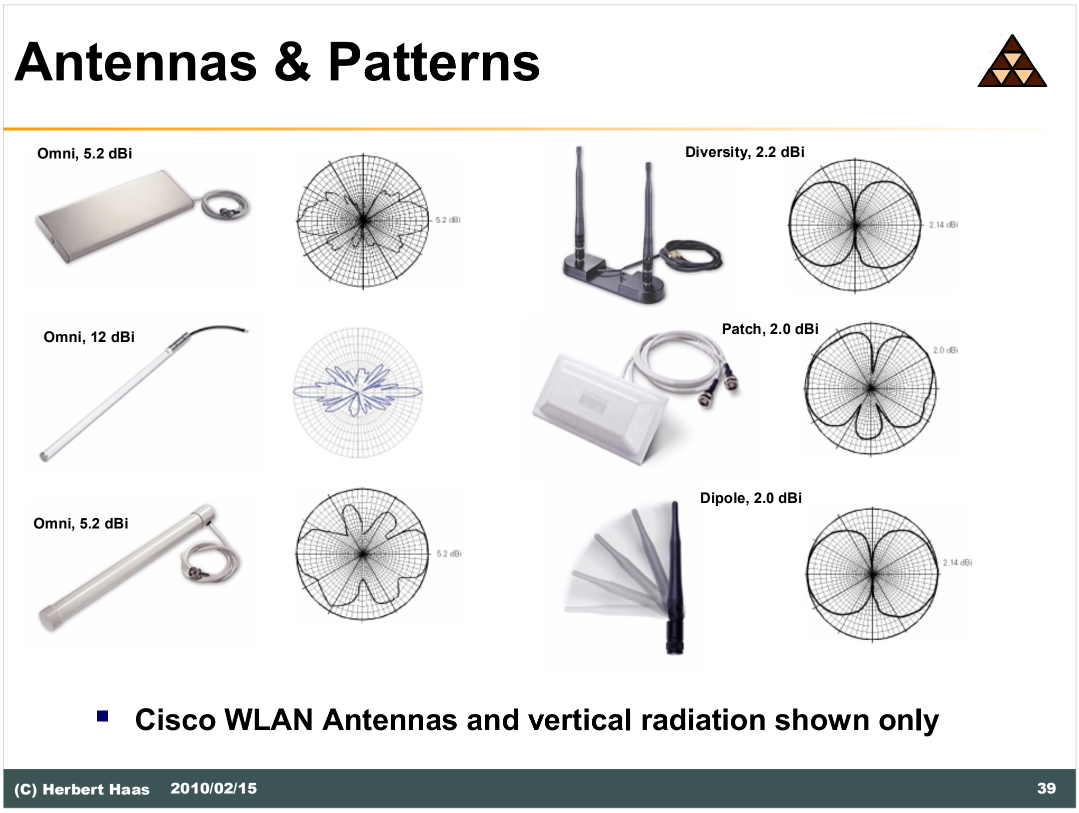
- Circular polarity (5 dBi)
- Microstrip patch (6-18 dBi)
- Omni (2-10 dBi)
- Parabolic dish (20-30 dBi)
- Sector (14 dBi)
- Yagi (8-16 dBi)

(C) Herbert Haas 2010/02/15 38

Use circular polarity wireless antennas where metal or reflective materials are present.

Note: Vertical poles for antenna mounting have significant influence in case vertical polarized antennas are used (field distortions). Especially critical for Yagi antennas.

Hidetsugu Yagi (1886-1976) and Shintaro Uda (1896-1976), University of Tohoku in Sendai/Japan.



Antennas & Patterns

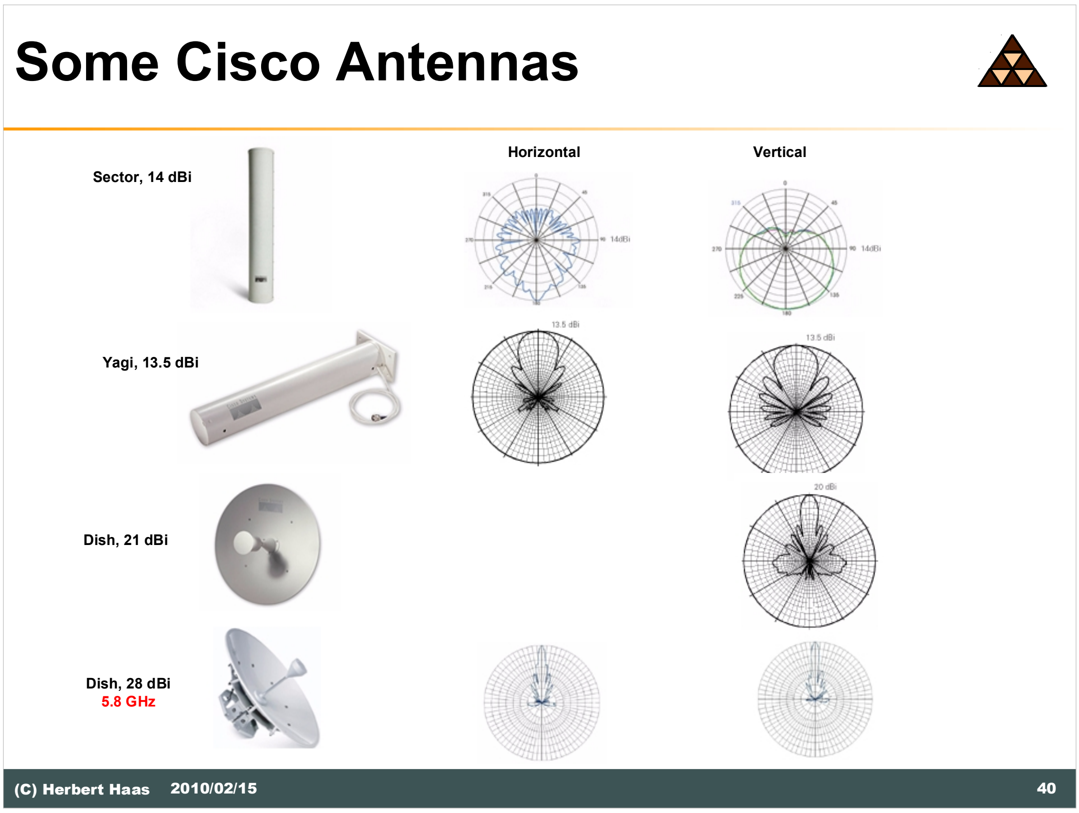
- Cisco WLAN Antennas and vertical radiation shown only

(C) Herbert Haas 2010/02/15 39

Consider the following two Cisco antennas for practical indoor installations in larger halls:

The 6 dBi **AIR-ANT2012** is a diversity patch antenna and offers 80 degrees illumination angle horizontally and 55 degrees vertically. With this antenna the distances compared to a omni (rubber) can be easily doubled.

Using the **AIR-ANT3549** with 8.5 dBi the distance might be increased by a factor of 2.7 compared to an omni. However, the tradeoff is smaller angles: 60/55 degrees, which is often a good thing for long but narrow halls (1:3).



Some Cisco Antennas

Horizontal

Vertical

Sector, 14 dBi

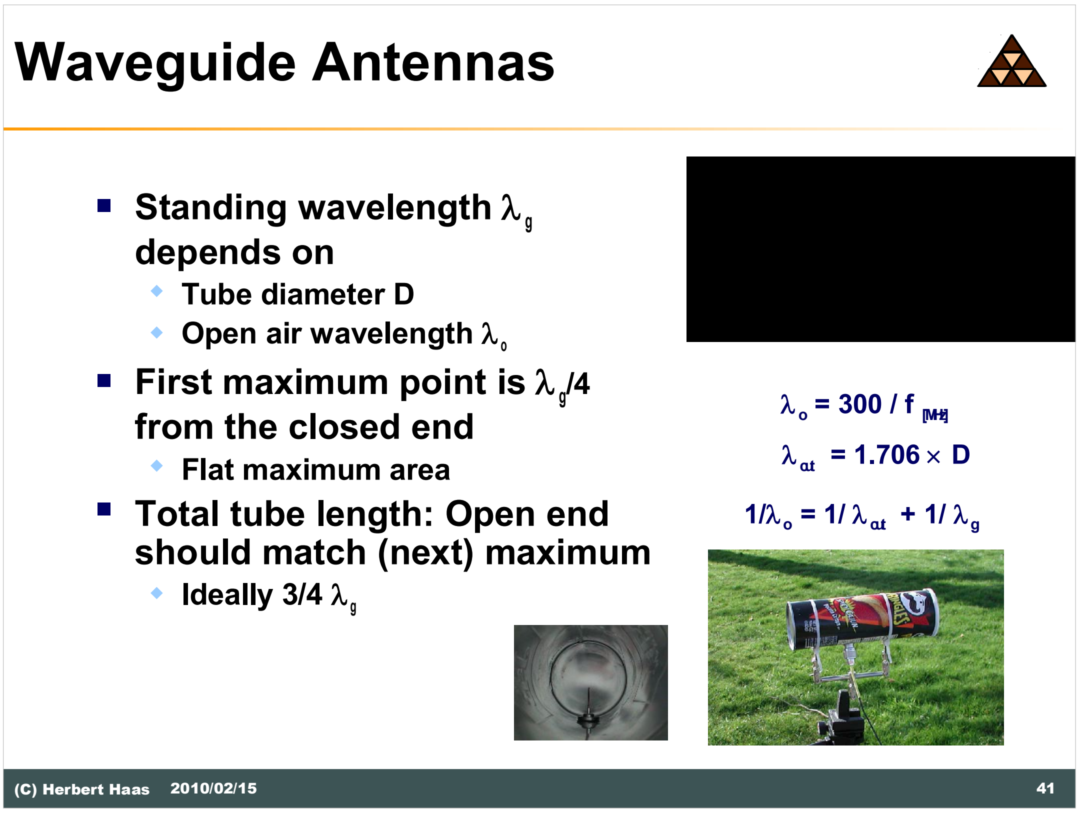
Yagi, 13.5 dBi

Dish, 21 dBi

Dish, 28 dBi
5.8 GHz

Some radio equipment manufacturers specifically warn against this because it damages the transmitter. Most pieces of amateur or commercial radio equipment carry this warning because they operate at a much higher transmitter power. The reflected wave standing wave ratio (SWR) caused by a lack of a proper antenna or load can damage the final amplifier stage known as the power amplifier (PA).

For Cisco Aironet equipment, the transmitter power output is 100 mW for the 350 series and 30 mW for the 340 series, so damage is unlikely but possible. If you absolutely have a requirement to run the devices without antennas, it is recommended that you turn the transmitter power down to 1-5 mW or use a 50-52 ohm "dummy load," just to be safe.



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

[redacted]

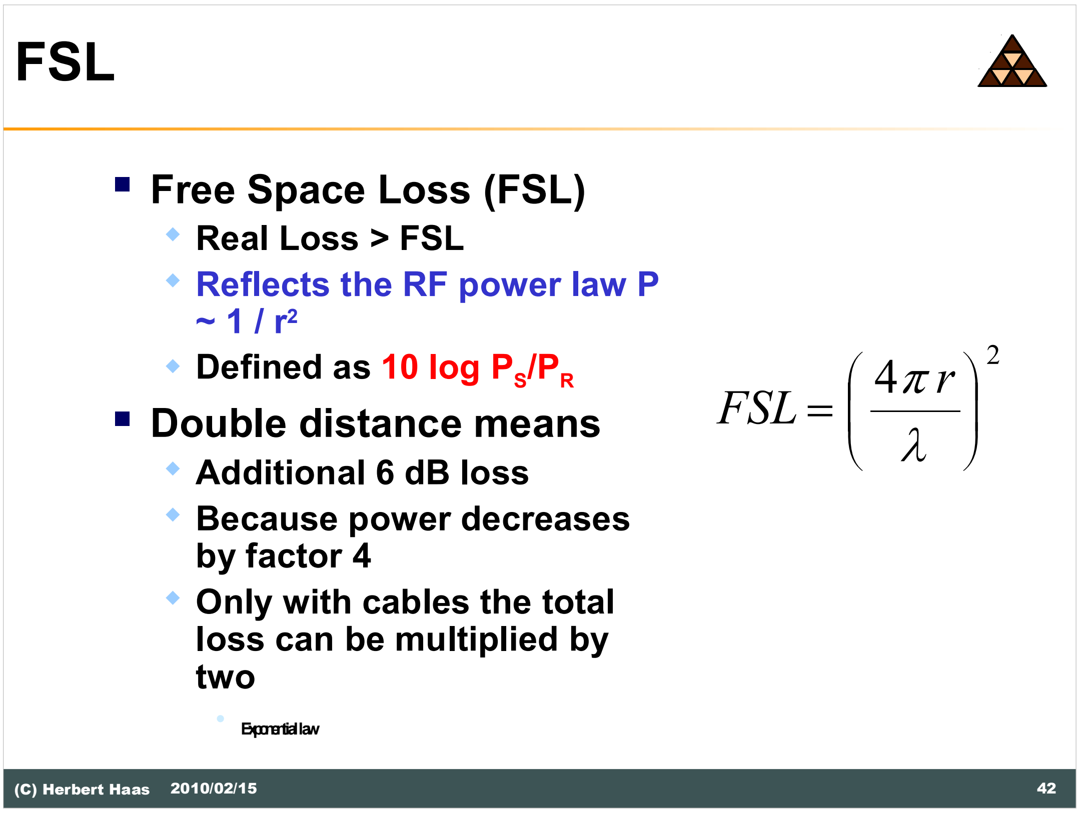
$\lambda_o = 300 / f_{[MHz]}$

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

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

Waveguide antennas act as opened waveguide. Standing waves and modes, high pass behavior. Goal: Find the point of maximum field strength of the standing wave

It is important to notice that the standing wavelength Lg is not the same as wavelength Lo counted from hf signal. Large tubes are near as open air where Lg and Lo are almost same but when tube diameter becomes smaller the Lg increases effective until there becomes a point when Lg becomes infinite. It corresponds the diameter when hf signal doesn't come to the tube at all. So the waveguide tube acts as a high pass filter which limit wavelength Lc = 1.706 x D. Lo can be calculated from nominal frequency: Lo/mm = 300/(f/GHz).



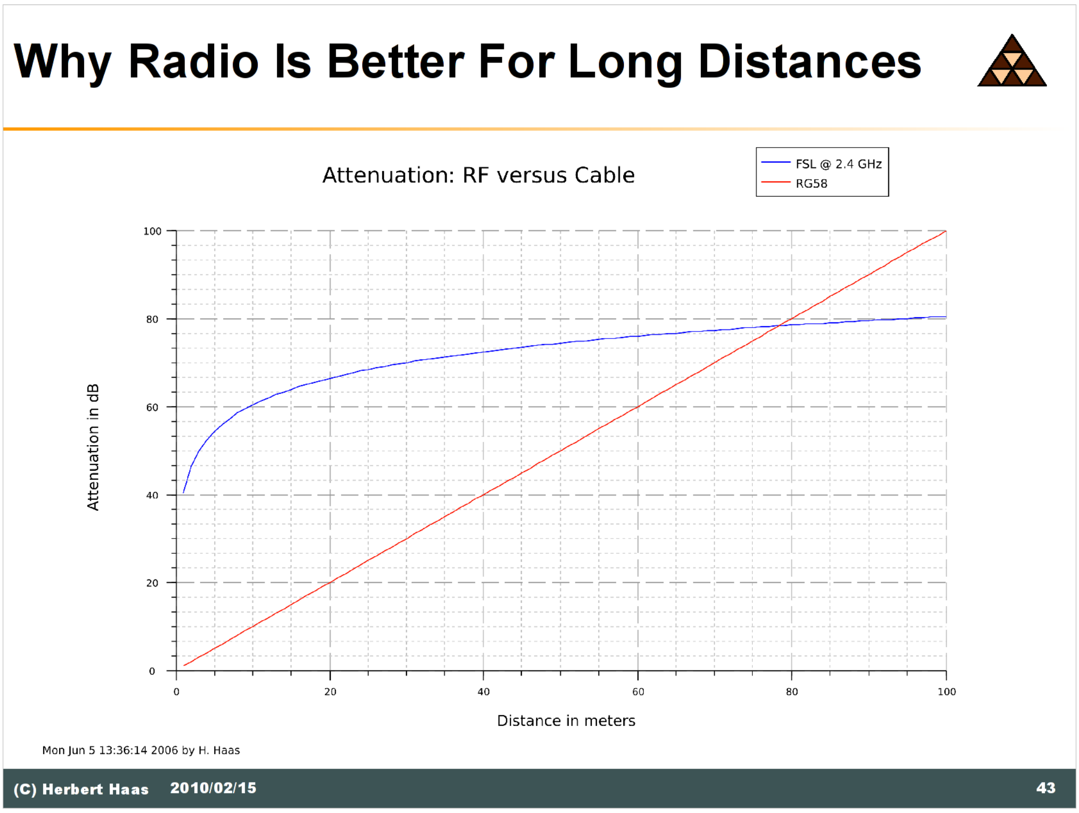
FSL

- Free Space Loss (FSL)
  - Real Loss > FSL
  - Reflects the RF power law P ~ 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

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

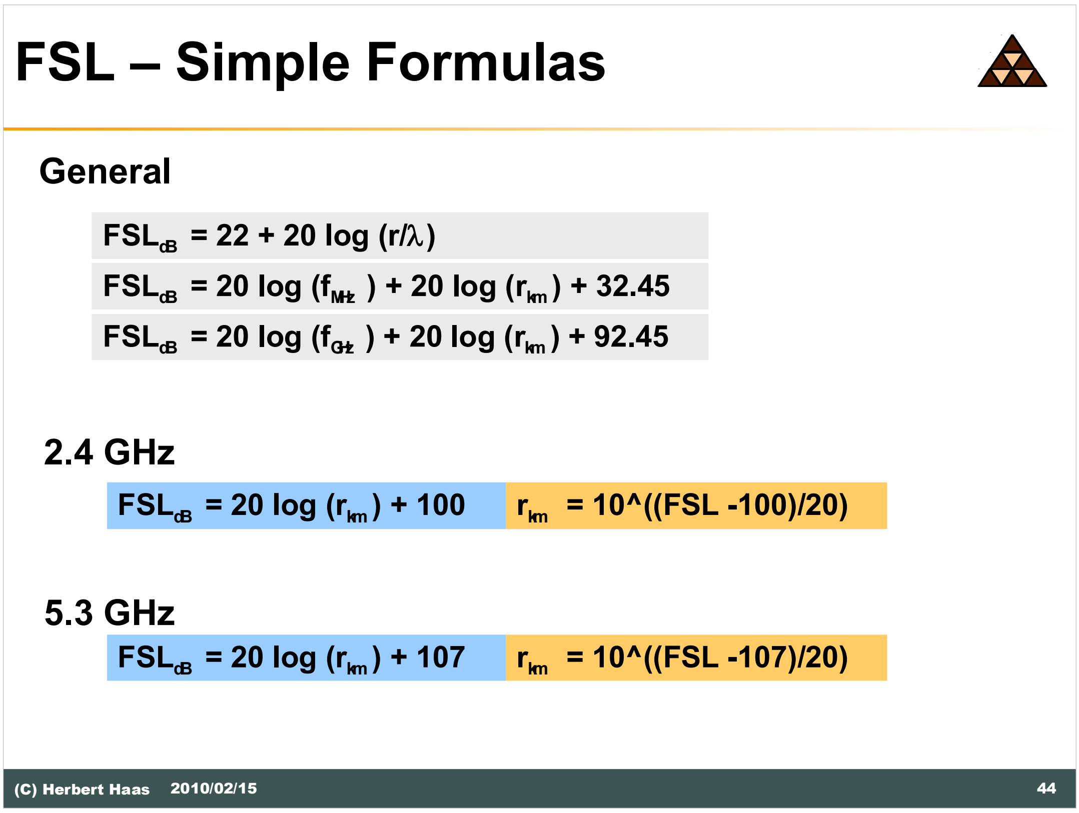
Free Space Loss: No Fresnel zone encroachment assumed!

In German it is called "Freiraumdämpfung".



Why Radio Is Better For Long Distances

Notice that with radio propagation there are always (only) additional 6 dB loss if the distance is doubled.



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

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

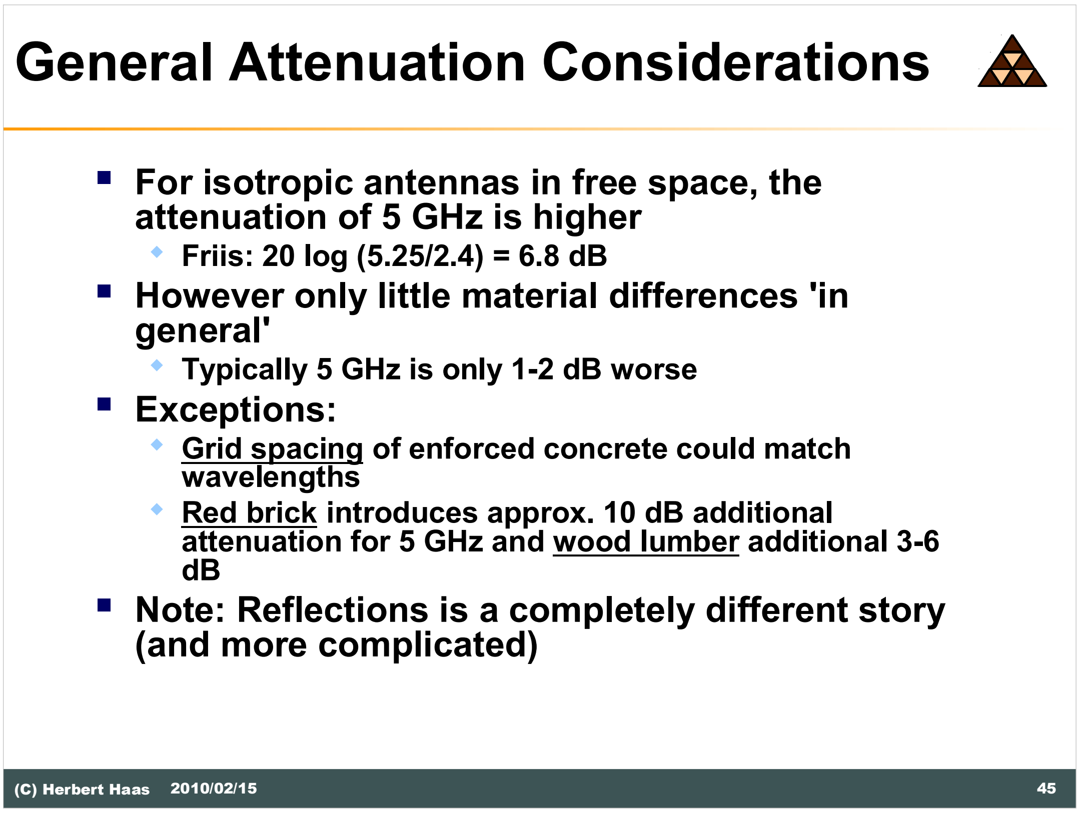
5.3 GHz

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

(C) Herbert Haas 2010/02/15 44

The formulas highlighted in blue are the most important for quick estimations of the Free Space Loss.

Note that the inverse formulas are very sensitive regarding their exponent. Slightly differences in the FSL result in huge deviations of the distance.

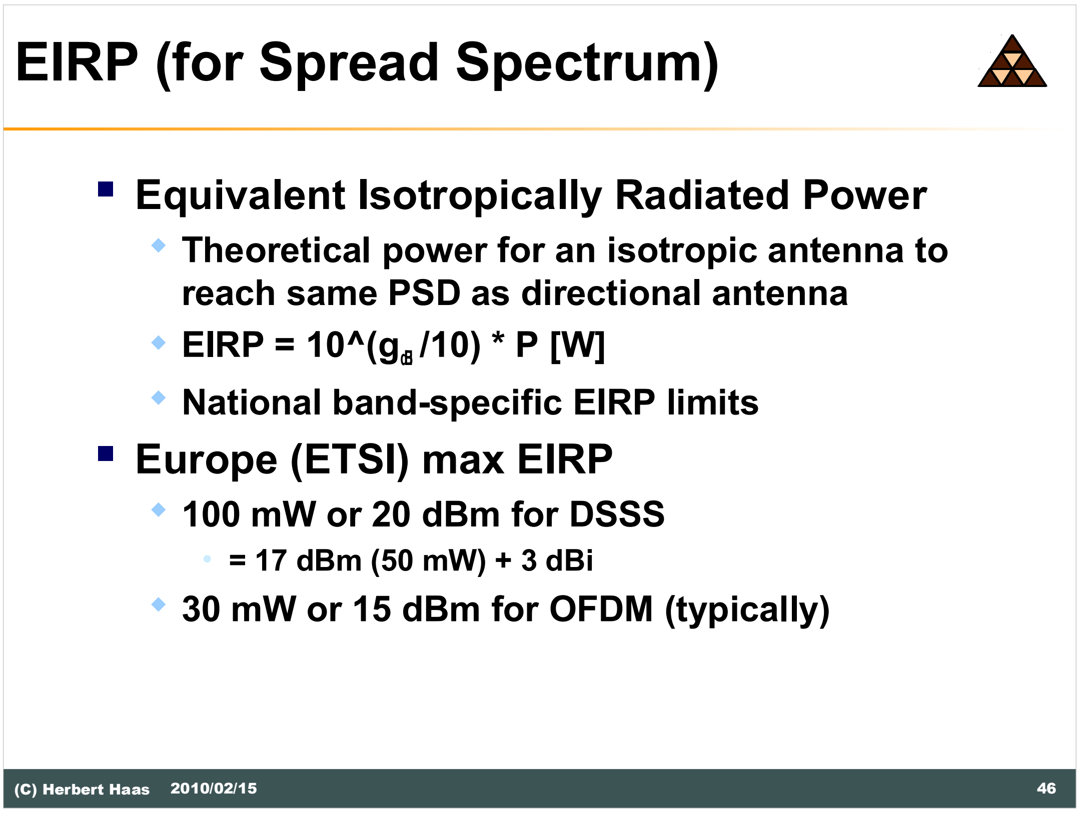


General Attenuation Considerations

- 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:
  - Grid spacing of enforced concrete could match wavelengths
  - Red brick introduces approx. 10 dB additional attenuation for 5 GHz and wood lumber additional 3-6 dB
- Note: Reflections is a completely different story (and more complicated)

(Wood lumber = German: Bauholz)

The reflection characteristics heavily depend on the wavelength used and the particular thickness of the considered layer.



EIRP (for Spread Spectrum)

- Equivalent Isotropically Radiated Power
  - Theoretical power for an isotropic antenna to reach same PSD as directional antenna
  - EIRP = 10^(g_{dB}/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)

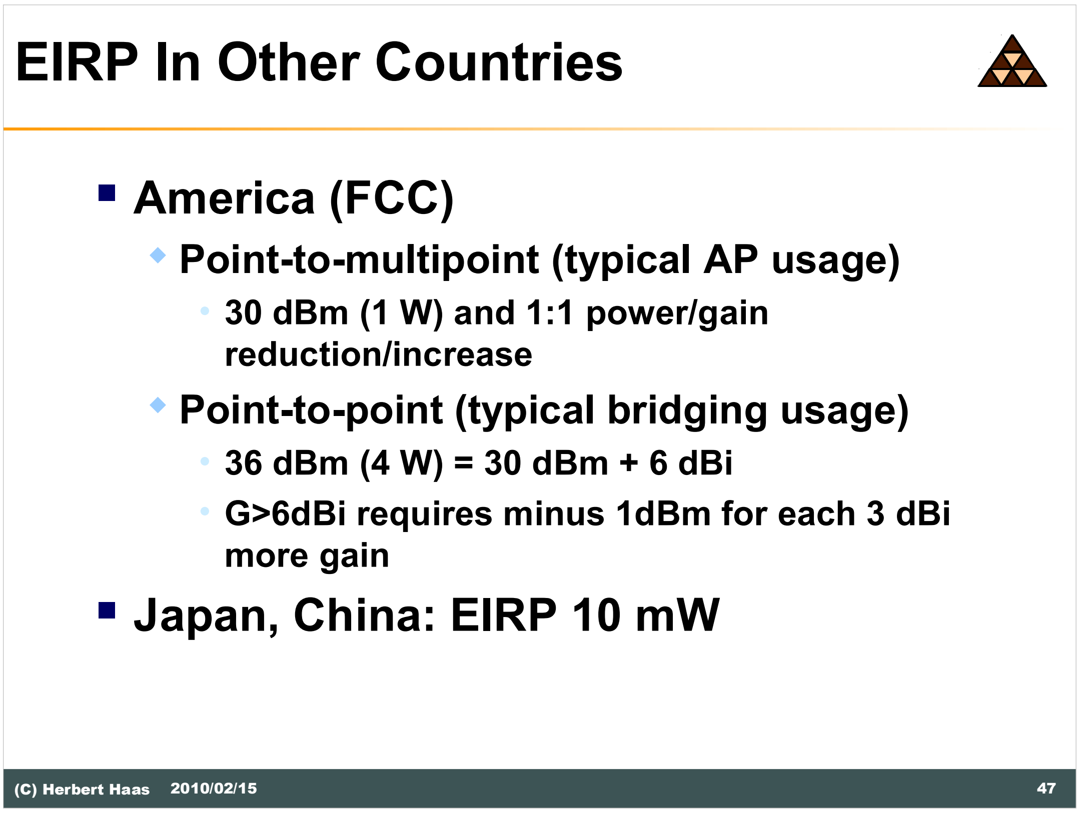
Europe 100 mW except France: France is only 7 dBm (5 mW).

In the U.S., the FCC (Federal Communications Commission) defines power limitations for wireless LANs in FCC Part 15.247. Manufacturers of 802.11 products must comply with **Part 15** to qualify for selling their products within the U.S. Regulatory bodies in other countries have similar rules.

The FCC eases EIRP limitations for fixed, point-to-point systems that use higher gain directive antennas. If the antenna gain is at least 6 dBi, the FCC allows operation up to 4 watts EIRP. This is 1 watt (the earlier limitation) plus 6 dB of gain.

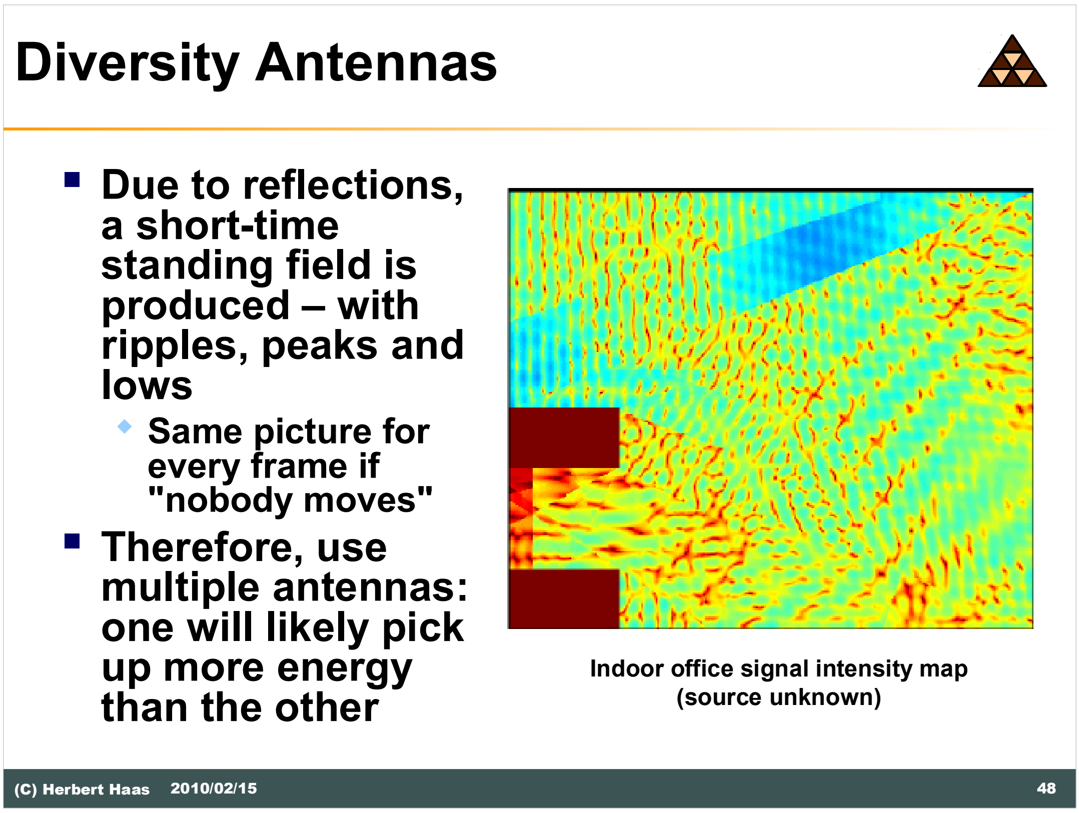
For antennas having gain greater than 6 dBi, the FCC requires you to reduce the transmitter output power if the transmitter is already at the maximum of 1 watt. The reduction, however, is only 1 dB for every 3 dB of additional antenna gain beyond the 6 dBi mentioned above. This means that as antenna gain goes up, you decrease the transmitter power by a smaller amount. As a result, the FCC allows EIRP greater than 4 watts for antennas having gains higher than 6 dBi.

Note: Effective Radiated Power (ERP) restrictions exist for unlicensed service only. **Amateur radios** may have MUCH more power...



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

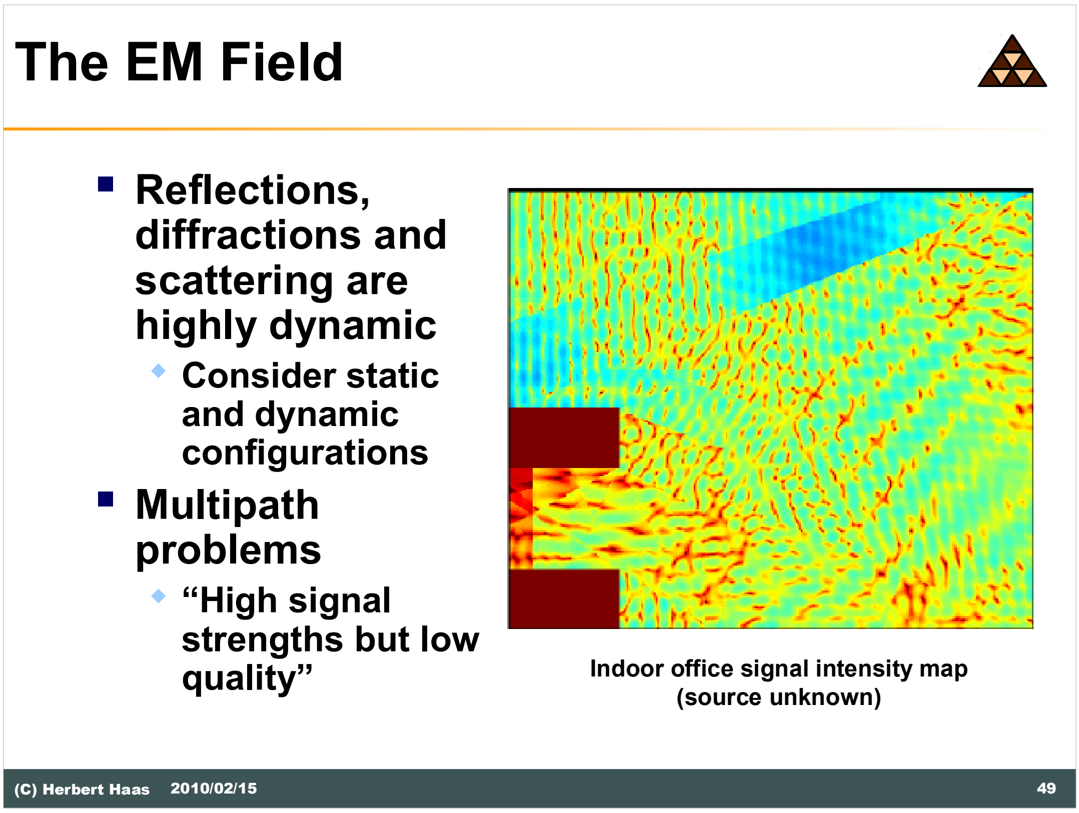
Indoor office signal intensity map (source unknown)

For small distances (rooms) the speed of light is approximately infinite

On the other hand, the data rate is limited and every frame produces a nearly instantaneous EM-field (for a short period of time)

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.



The EM Field

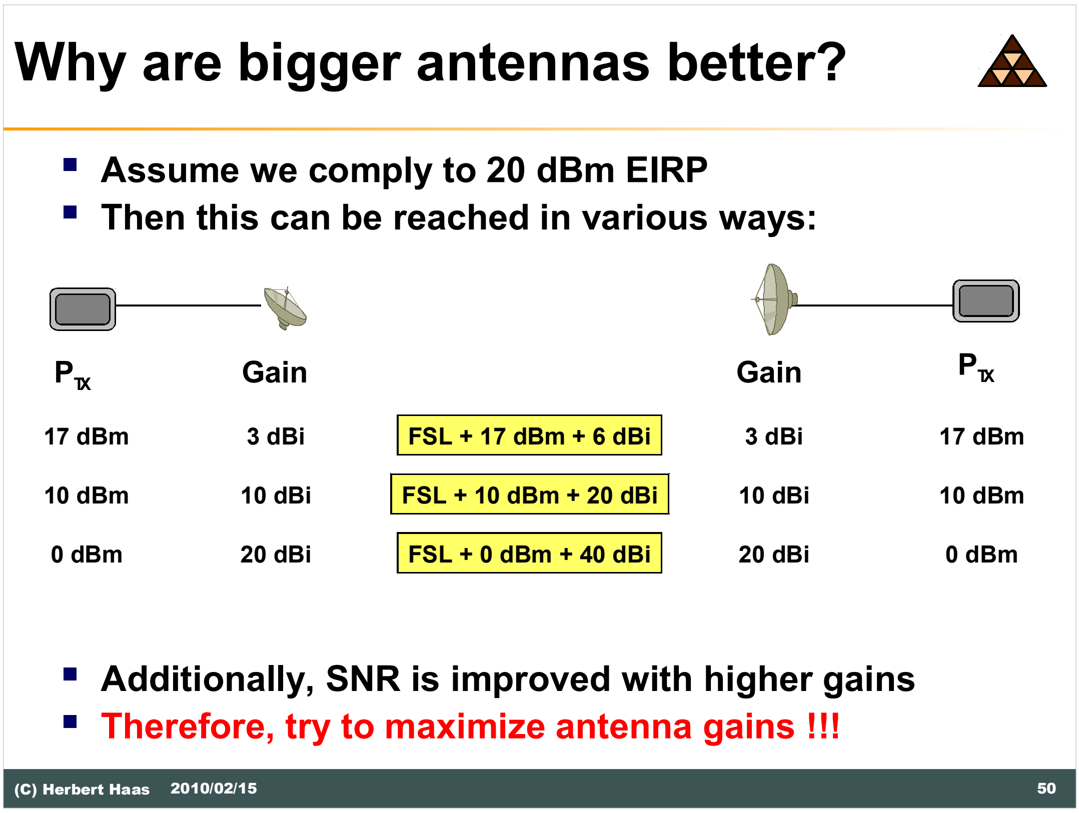
- Reflections, diffractions and scattering are highly dynamic
  - Consider static and dynamic configurations
- Multipath problems
  - “High signal strengths but low quality”

Indoor office signal intensity map (source unknown)

Source: www.intersil.com

This picture shows the usefulness of diversity antennas.

Similar pictures can easily be made with 4NEC2X available for windows (or NEC2 the free Linux version).



Why are bigger antennas better?

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

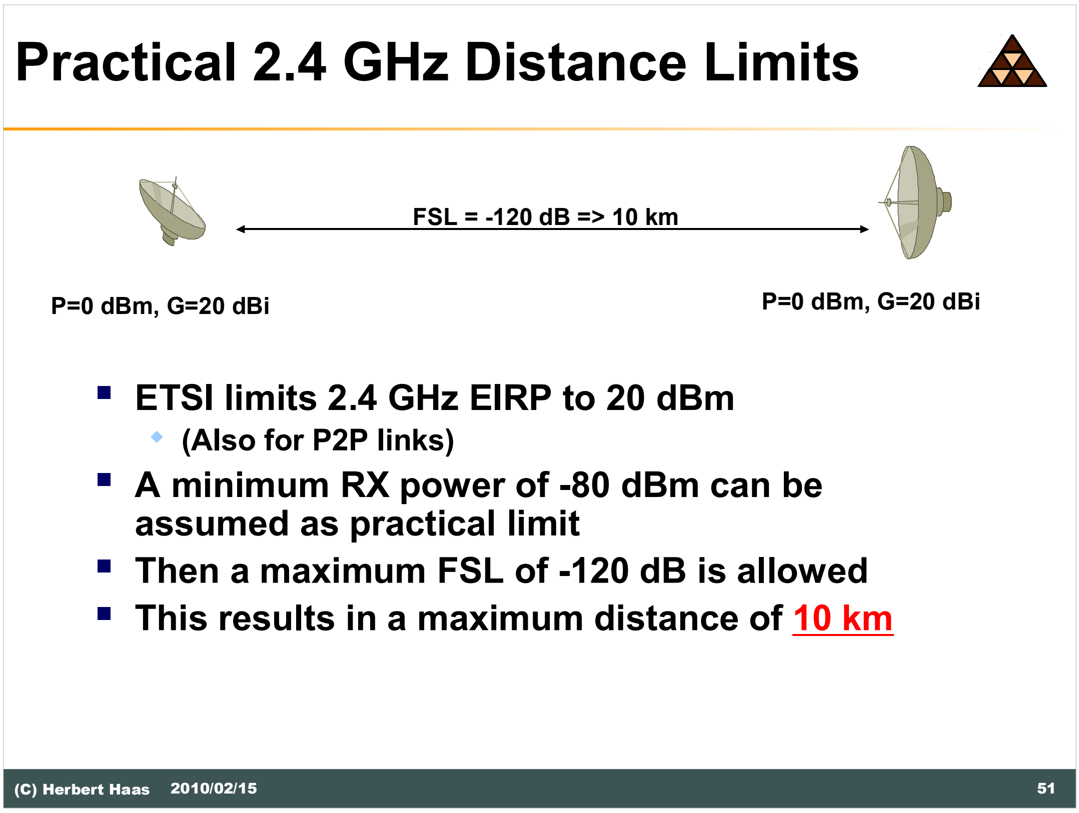
P_{TX}	Gain		Gain	P_{TX}
17 dBm	3 dBi	FSL + 17 dBm + 6 dBi	3 dBi	17 dBm
10 dBm	10 dBi	FSL + 10 dBm + 20 dBi	10 dBi	10 dBm
0 dBm	20 dBi	FSL + 0 dBm + 40 dBi	20 dBi	0 dBm

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

It is important to understand the true importance of a high gain antenna. While the TX power is limited by regulatory it makes no difference when using a perfect omni antenna with 100 mW or a 20 dBi dish with 1 mW.

But when signals are to be received the antenna gain (of the receiver) significantly increases the sensitivity and therefore lengthens the maximum distance.

Note that in the yellow boxes above the FSL is assumed to have the same (unknown) value each time. What changes is the TX power and the antenna gain.



Practical 2.4 GHz Distance Limits

FSL = -120 dB => 10 km

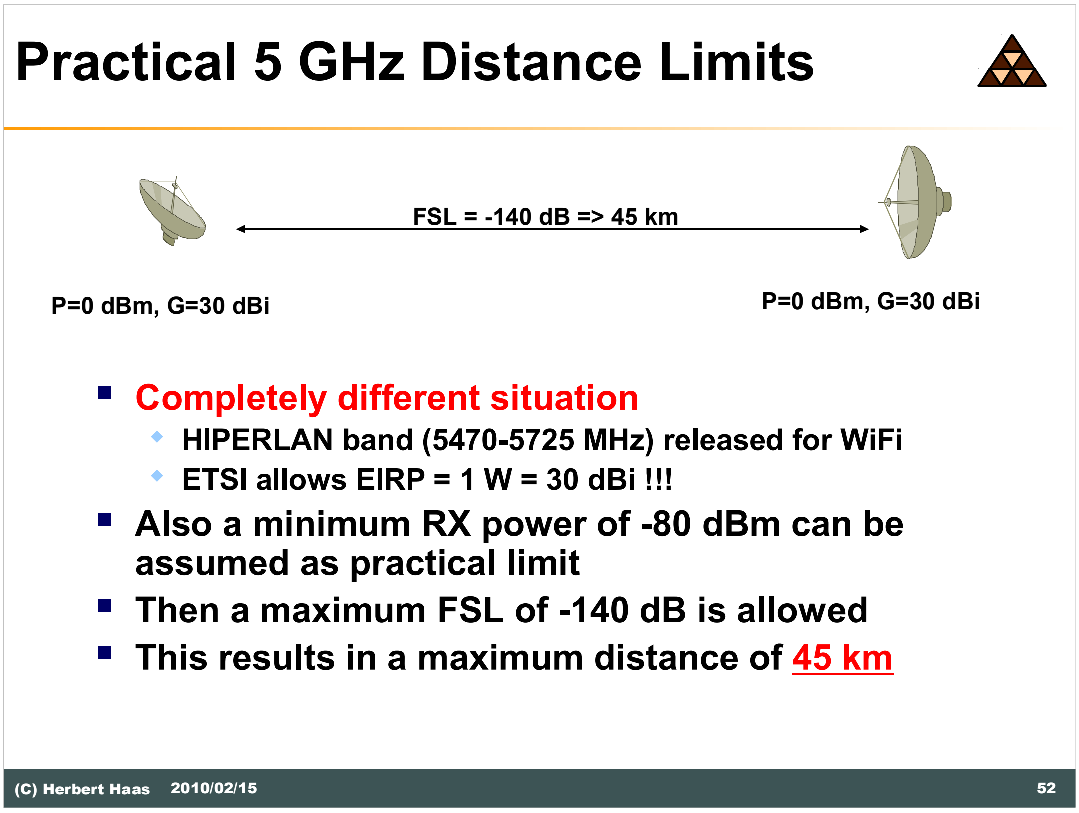
P=0 dBm, G=20 dBi

P=0 dBm, G=20 dBi

- 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 10 km

The typical practical distance limit of wireless bridges operating in an ETSI domain at 2.4 GHz is approximately 10 km.

Assuming a RX power of -80 dBm a data rate of **11 Mbit/s** can be easily achieved (the minimum signal level for 11 Mbit/s is -85 dB or less).



Practical 5 GHz Distance Limits

FSL = -140 dB => 45 km

P=0 dBm, G=30 dBi

P=0 dBm, G=30 dBi

- 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 45 km

(C) Herbert Haas 2010/02/15 52

Note: the 5 GHz band is nearly 750 MHz wide – this results in significant different wavelengths:

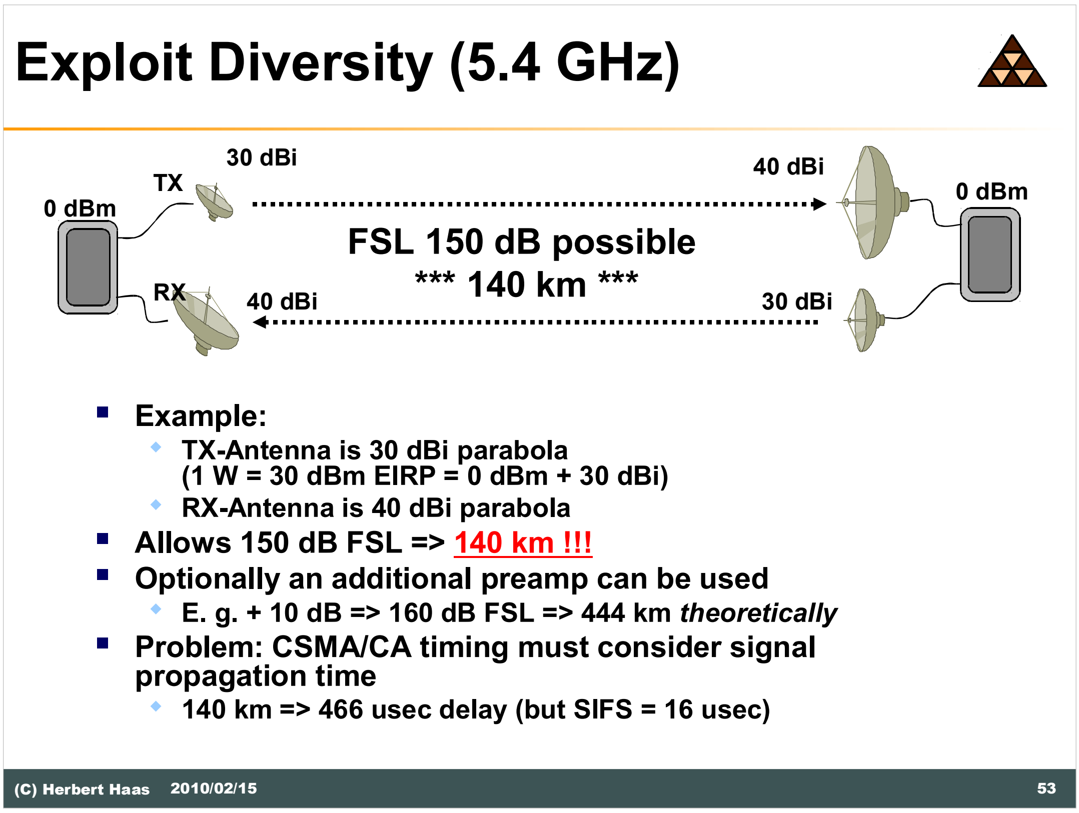
299.792.458 m/s / 5150 MHz = 0.0582 m

299.792.458 m/s / 5470 MHz = 0.0548 m

299.792.458 m/s / 5725 MHz = 0.0524 m

That is the wavelength differences are about 10%.

Therefore a FSL of 140 dB can be reached either using 5150 MHz and 46.31 km or 5725 MHz and 41.7 km. Currently only the upper bands can be used for outdoor applications and 1 W EIRP, so we reasonably only consider 5470 MHz, for which 140 dB FSL corresponds to 43.61 km.



Exploit Diversity (5.4 GHz)

0 dBm
TX
30 dBi
RX
40 dBi
40 dBi
0 dBm
30 dBi

FSL 150 dB possible
*** 140 km ***

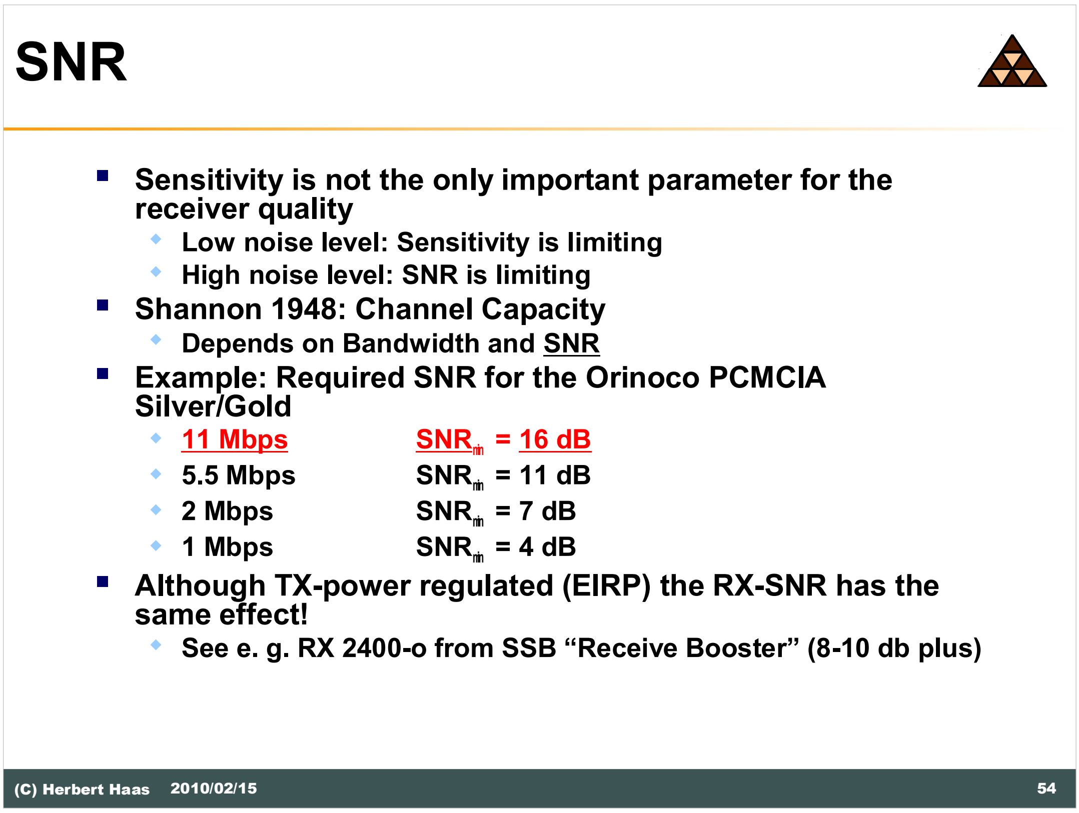
- Example:
  - TX-Antenna is 30 dBi parabola (1 W = 30 dBm EIRP = 0 dBm + 30 dBi)
  - RX-Antenna is 40 dBi parabola
- Allows 150 dB FSL => 140 km !!!
- Optionally an additional preamp can be used
  - E. g. + 10 dB => 160 dB FSL => 444 km *theoretically*
- Problem: CSMA/CA timing must consider signal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

The regulatory only limits the EIRP but not the sensitivity of a receiver. Therefore the total distance can be easily increased with better RX-only antennas.

This can only be achieved by reusing the diversity antenna ports and disabling diversity. Simply configure one port for TX and the other port (with the higher gain antenna) for RX.

Although this sounds interesting this involves a non-trivial **antenna-pointing** challenge. Additionally the bridges must support CSMA/CA timing adaptations otherwise frames cannon be acknowledged properly.

The frequency of 2.44 GHz is equal to a 0.122 m wavelength.



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

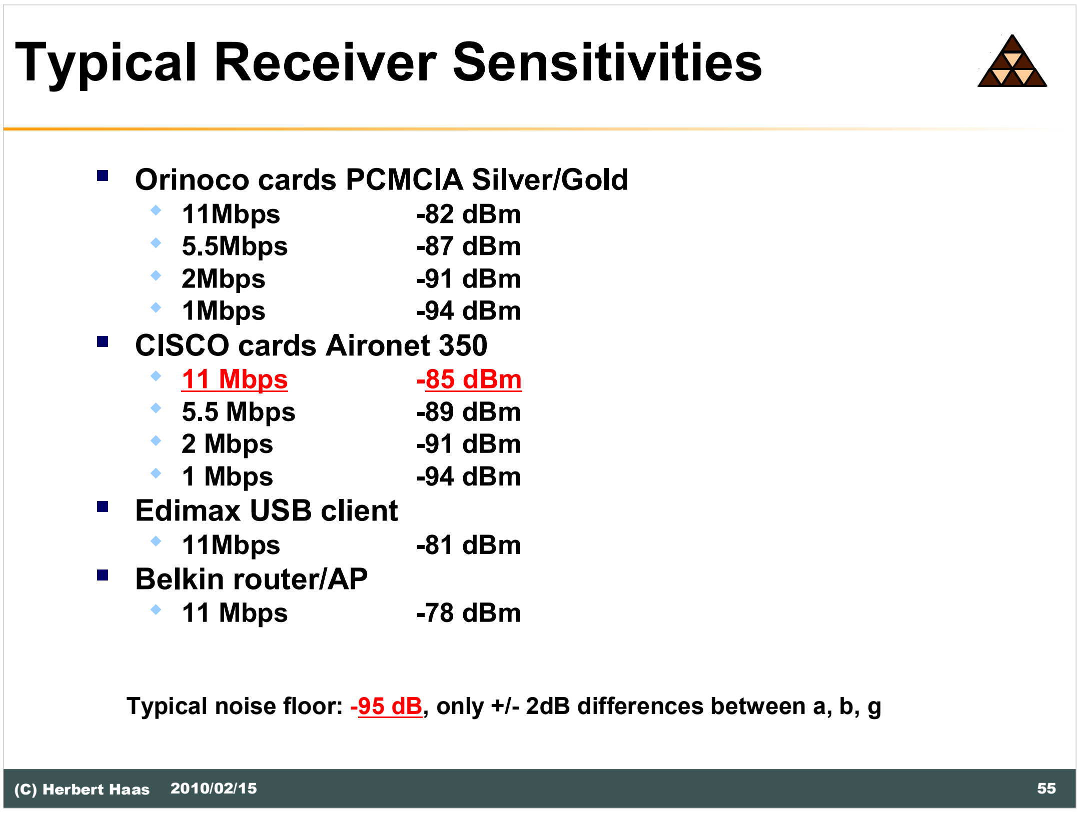
11 Mbps	SNR_{min} = 16 dB
5.5 Mbps	SNR_{min} = 11 dB
2 Mbps	SNR_{min} = 7 dB
1 Mbps	SNR_{min} = 4 dB

- 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)

The most important parameter to keep an eye on is the Signal-to-Noise-Ratio (SNR).

The effect is simple: the more SNR a client and AP observes the higher the data rate possible.

Therefore the longer the distance between client and AP the lower the data rate.



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

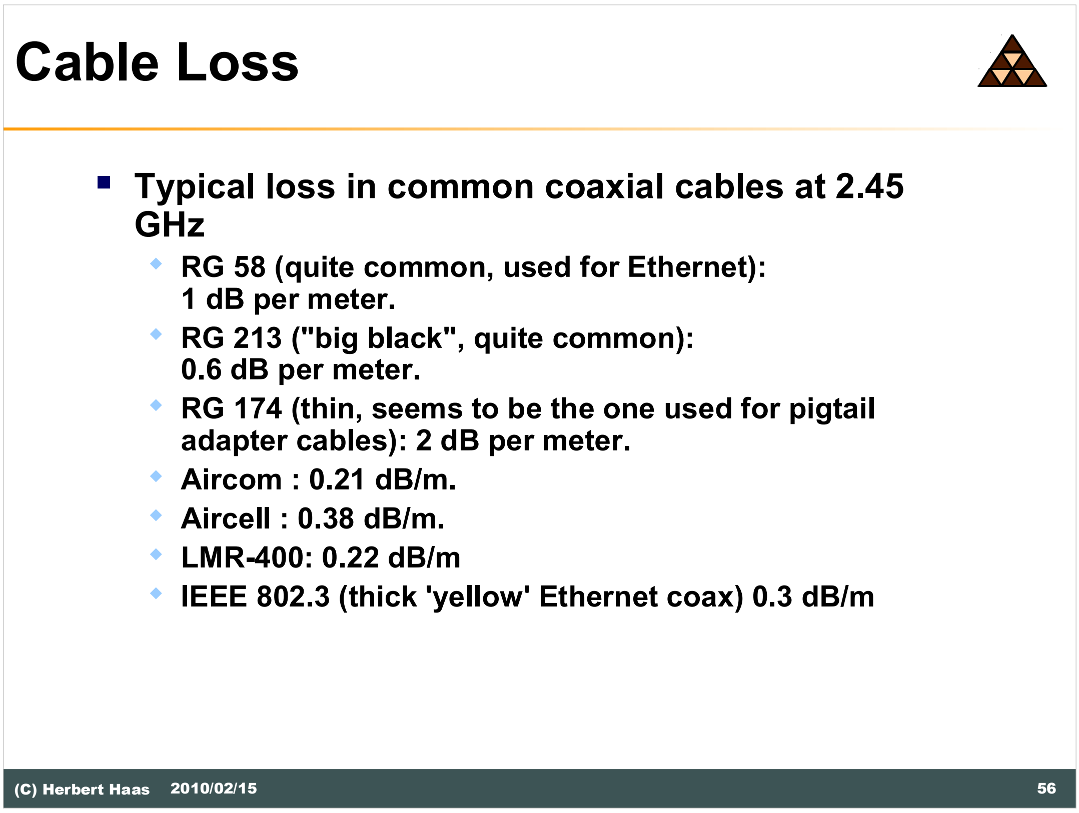
- Belkin router/AP

11 Mbps	-78 dBm

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

The Cisco 1240AG Access Point has the following sensitivity levels:

1 Mbit/s (2.4 GHz)	-96 dBm
11 Mbit/s (2.4 GHz)	-88 dBm
54 Mbit/s (both 2.4 and 5 GHz)	-73 dBm

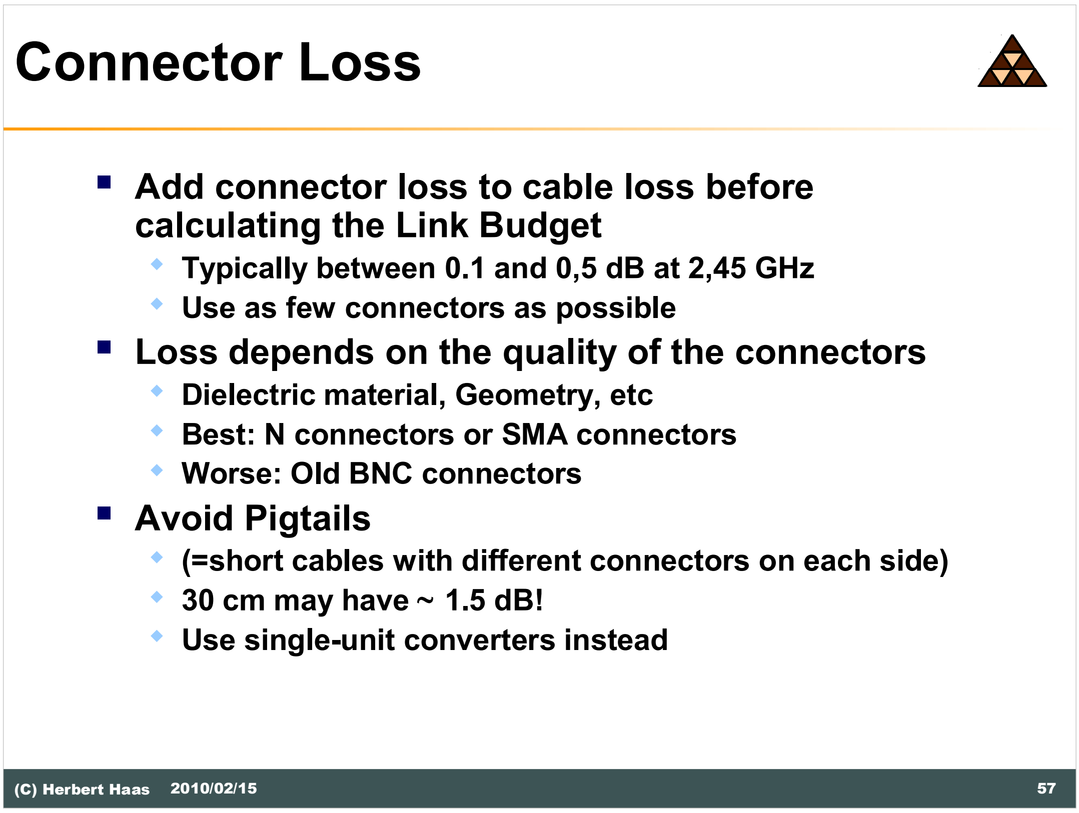


Cable Loss

- 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

This is a very boring slide. Don't spend too much time on it.

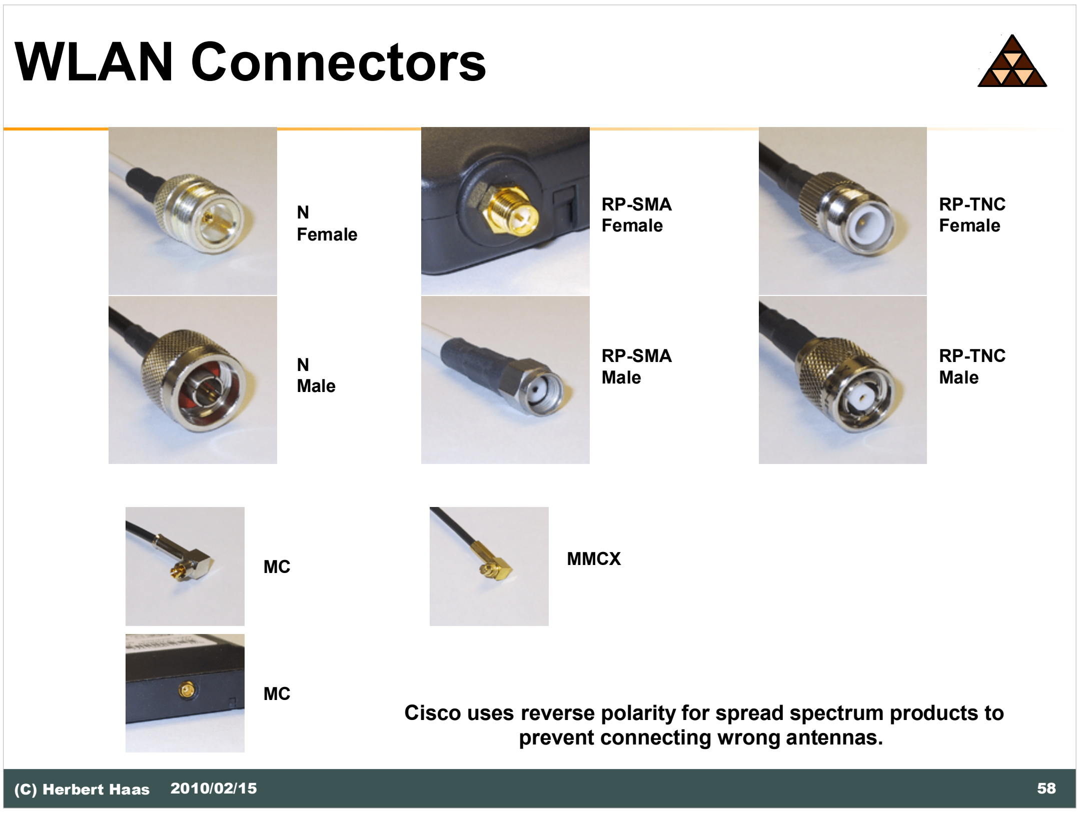
OF COURSE it is IMPORTANT to know about cable attenuation.



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

…also don't forget to consider connector losses…



WLAN Connectors

N
Female

RP-SMA
Female

RP-TNC
Female

N
Male

RP-SMA
Male

RP-TNC
Male

MC

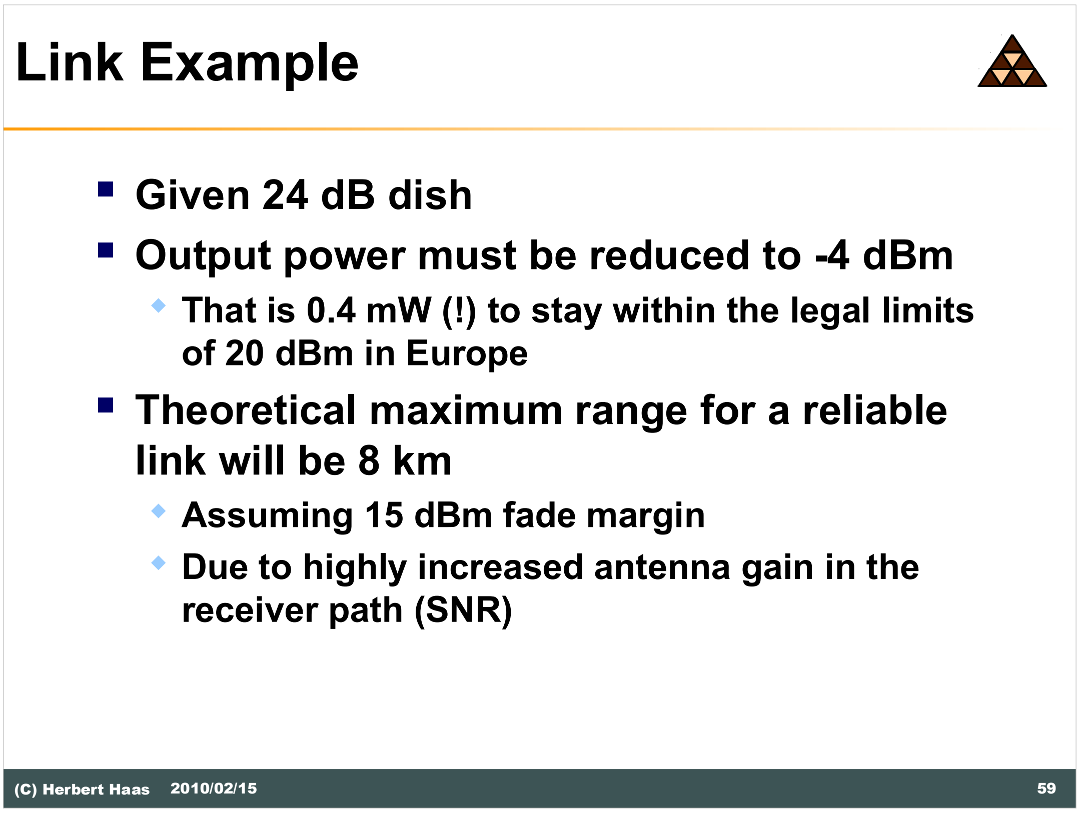
MMCX

MC

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

(C) Herbert Haas 2010/02/15 58

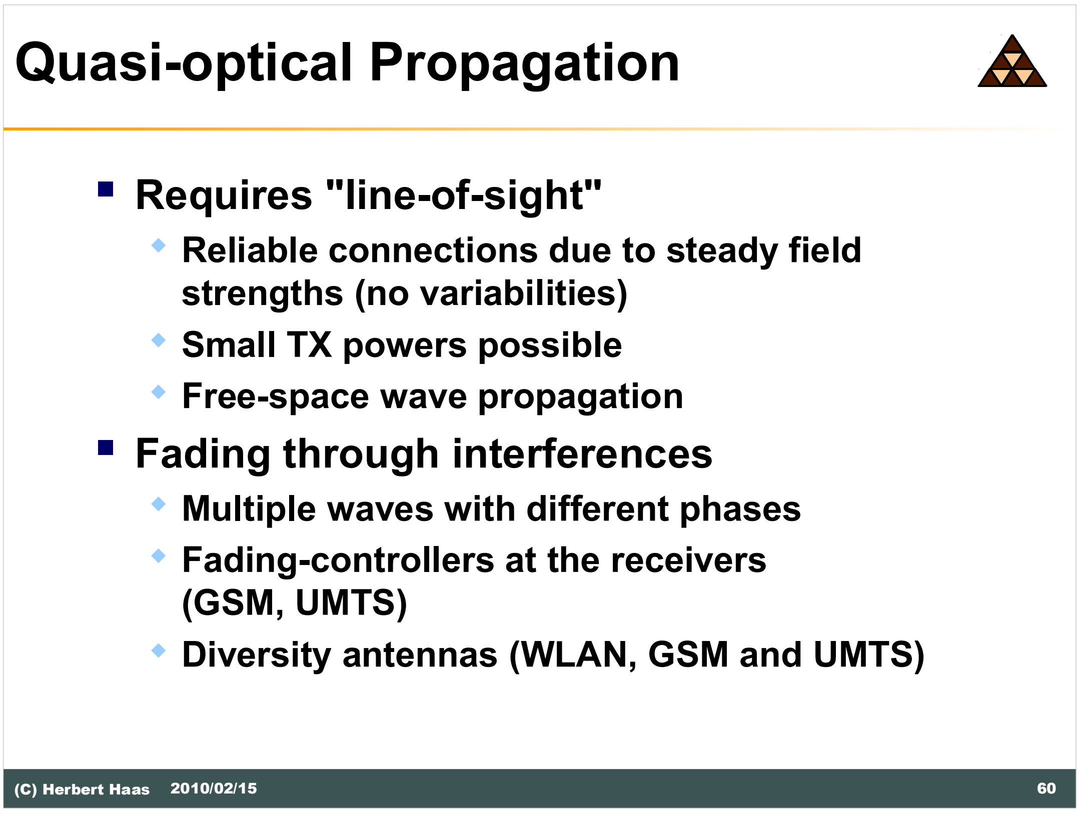
Cisco prefers the Reverse Polarity Threaded Naval Connector (RP-TNC) to prevent connecting a non-certified antenna inadvertently.



Link Example

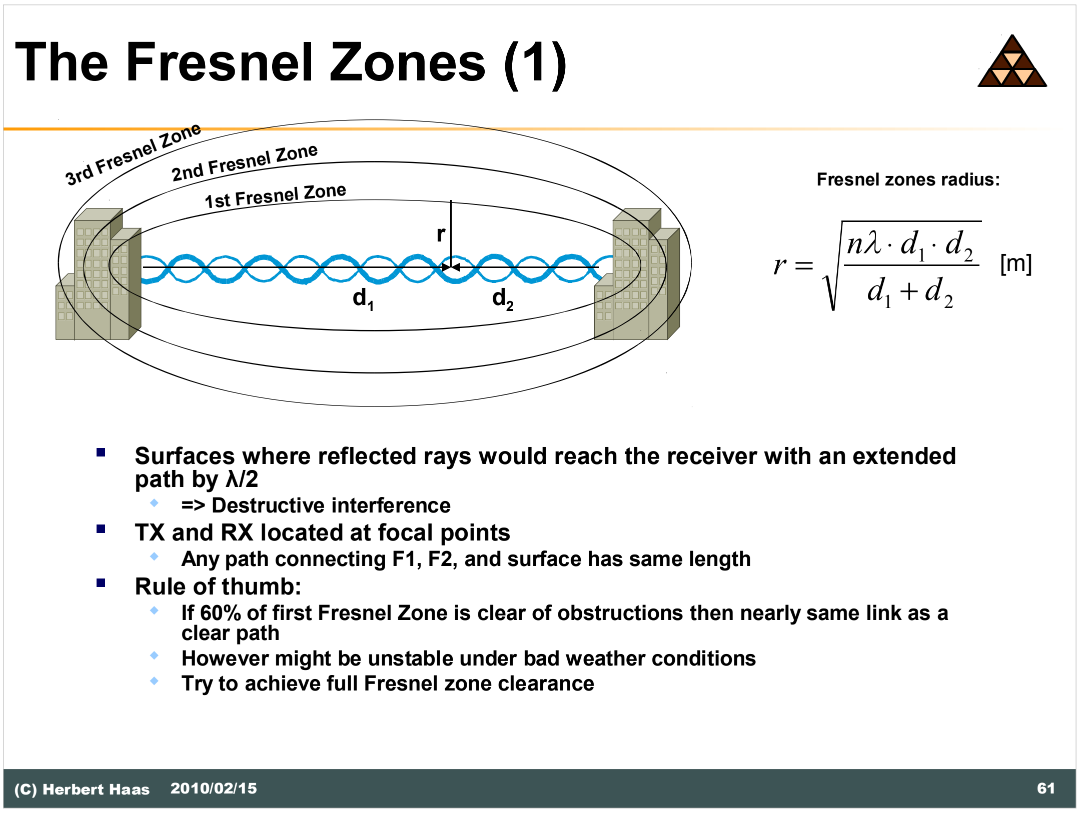
- Given 24 dB dish
- Output power must be reduced to -4 dBm
  - That is 0.4 mW (!) to stay within the legal limits of 20 dBm in Europe
- Theoretical maximum range for a reliable link will be 8 km
  - Assuming 15 dBm fade margin
  - Due to highly increased antenna gain in the receiver path (SNR)

Here is a final link budget example.



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:

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

- 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

(C) Herbert Haas 2010/02/15 61

The range of a wireless link is dependent upon the maximum allowable path loss. For outdoor links this is a straightforward calculation as long as there is clear line of sight between the two antennas with sufficient clearance for the Fresnel zone. For line of sight, you should be able to visibly see the remote locations antenna from the main site. There should be no obstructions between the antennas themselves. This includes trees, buildings, hills, and so on.

Fresnel Zone (pronounced 'fre-nel' the "s" is silent)

Fresnel zone is an elliptical area immediately surrounding the visual path. It varies depending on the length of the signal path and the frequency of the signal. The Fresnel zone can be calculated, and it must be taken into account when designing a wireless link.

The area around the visual line-of-sight that radio waves spread out into after they leave the antenna. This area must be clear or else signal strength will weaken.

Fresnel Zone is an area of concern for 2.4 GHz wireless systems. The table above provides a guideline on height requirements for antennas based on both line of sight and Fresnel zone requirements (for 2.4 GHz). Outdoors, every increase of 6 dB will double the distance. Every decrease of 6 dB will halve the distance. Shorter cable runs and higher gain antennas can make a significant difference to the range.

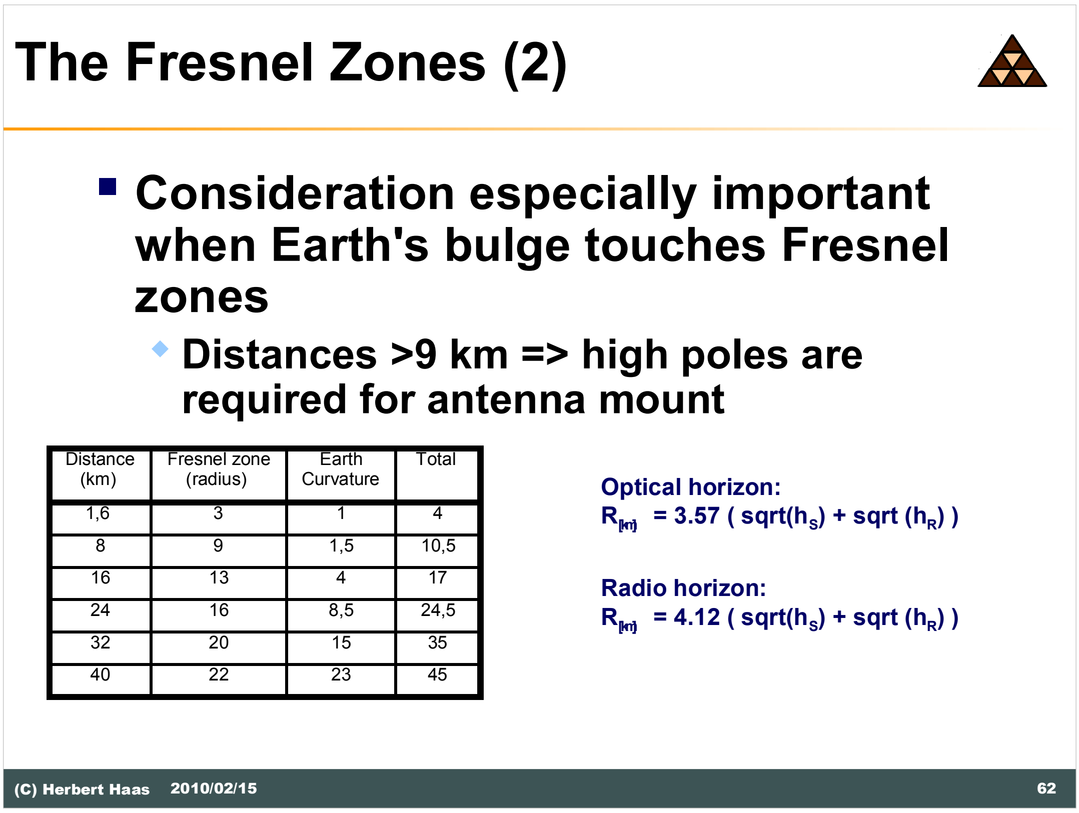
Point-to-Point

When connecting two points together (such as an Ethernet bridge), the distance, obstructions, and antenna location must be considered. If the antennas can be mounted indoors and the distance is very short (several hundred meters), the standard dipole or mast mount 5.2 dBi omni-directional may be used. An alternative is to use two patch antennas. For very long distances (1/2 km or more) directional high gain antennas must be used. These antennas should be installed as high as possible, and above obstructions such as trees, buildings, and so on. With a line-of-site configuration, distances of up to 20 km at 2.4GHz can be reached using parabolic dish antennas, if a clear line-of-site is maintained.

Point-to-Multipoint Bridge

In this case (in which a single point is communicating to several remote points) the use of an omni-directional antenna at the main communication point must be considered. The remote sites can use a directional antenna that is directed at the main point antenna.

As a rule of thumb, the earth curvature becomes significant at distances greater than 10 km.



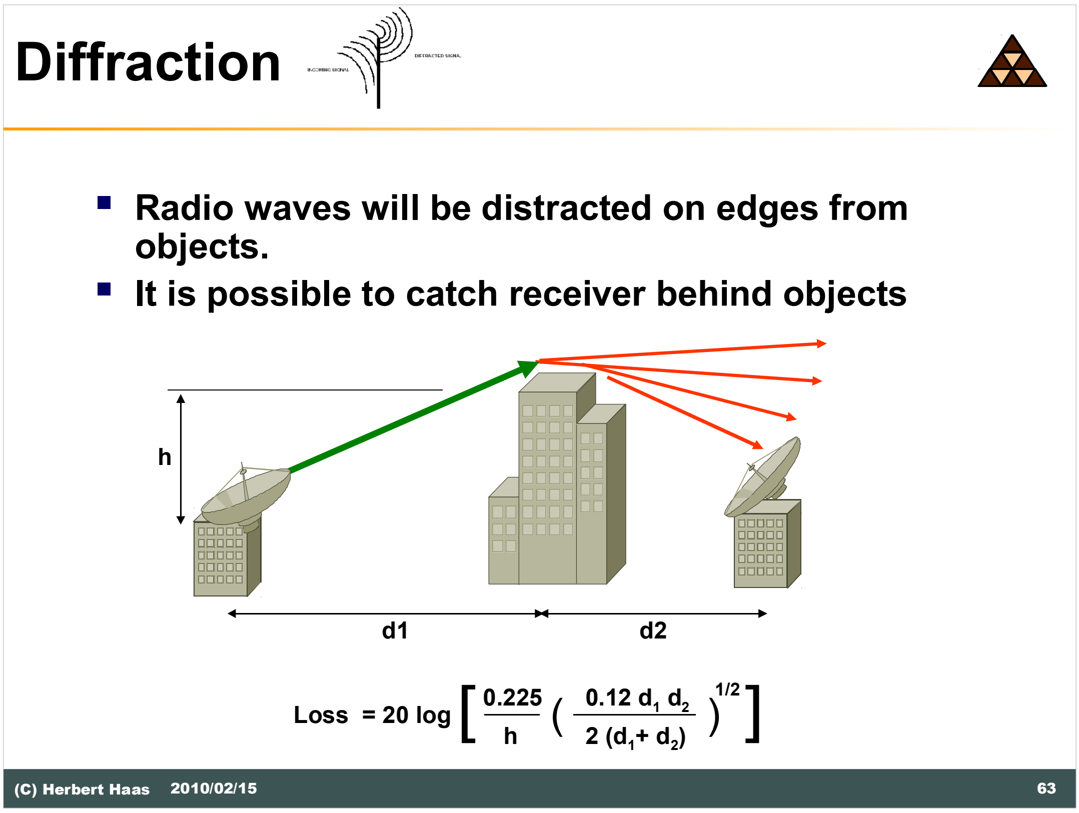
The Fresnel Zones (2)

- 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

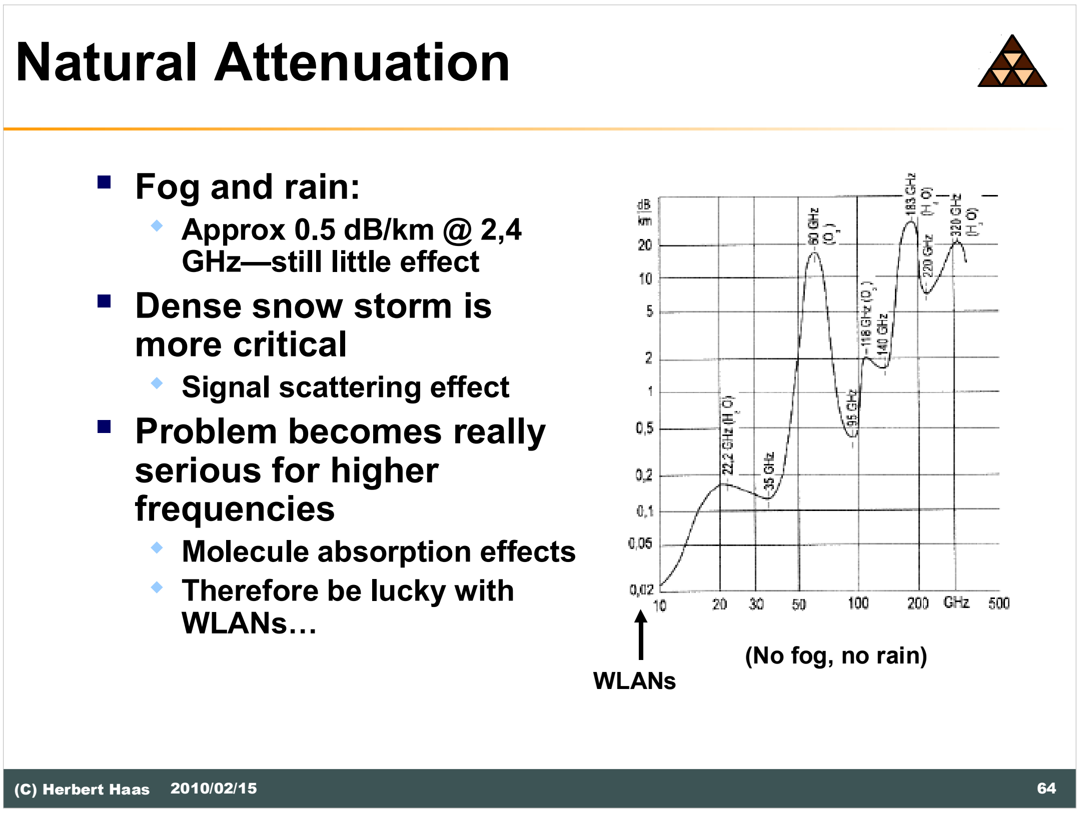
$$\text{Loss} = 20 \log \left[\frac{0.225}{h} \left(\frac{0.12\, d_1\, d_2}{2\,(d_1 + d_2)} \right)^{1/2} \right]$$

(C) Herbert Haas 2010/02/15 63

Also called "Inflexion"

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

However it's a bad design – don't expect high-quality signals…

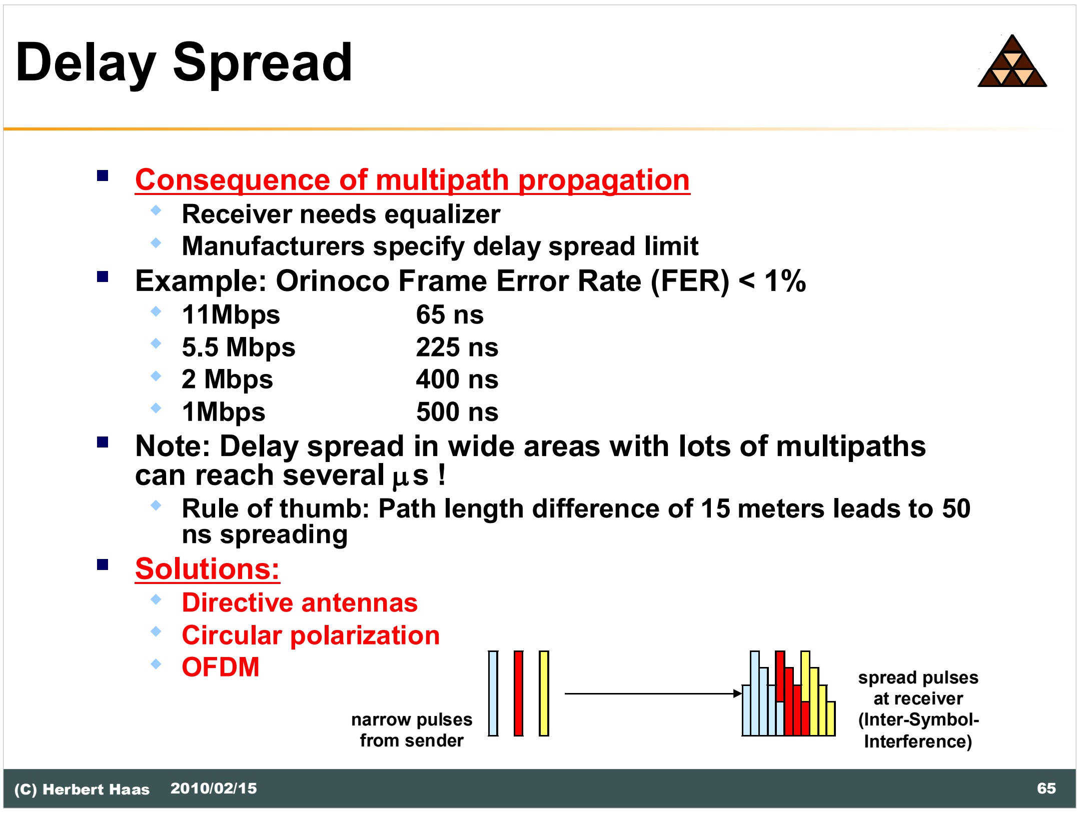


Natural Attenuation

- 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…

(No fog, no rain)

Although 2.4 GHz signals pass rather well through walls, they have a tough time passing through trees. The main difference is the water content in each. Walls are rather dry: trees contain high levels of moisture. Radio waves in the 2.4 GHz band absorb into water quite well.



Delay Spread

- Consequence of multipath propagation
  - Receiver needs equalizer
  - Manufacturers specify delay spread limit
- Example: Orinoco Frame Error Rate (FER) < 1%

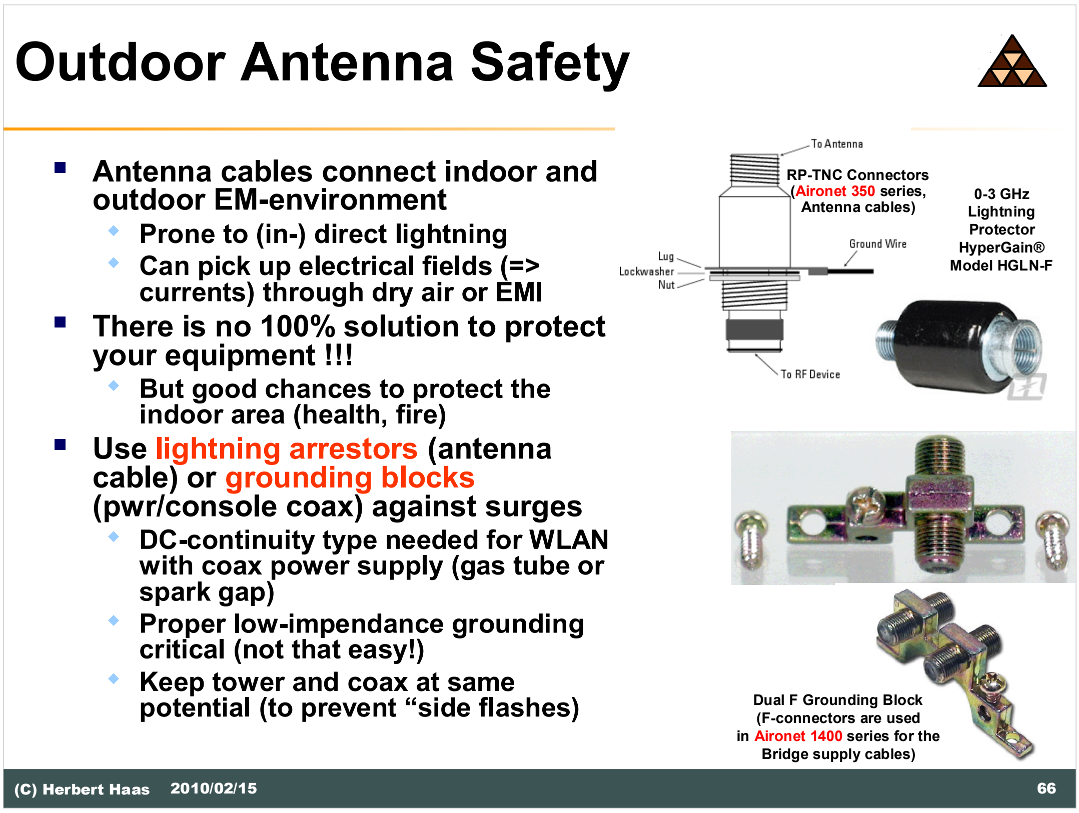
11Mbps	65 ns
5.5 Mbps	225 ns
2 Mbps	400 ns
1Mbps	500 ns

- 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
- Solutions:
  - Directive antennas
  - Circular polarization
  - OFDM

narrow pulses from sender

spread pulses at receiver (Inter-Symbol-Interference)

In order to minimize the reflection rate it is better using directive antennas, even if you are at short distance, and being in line of sight. Another possibility is also to use **circular wave polarisation** antennas (helical antenna) that cancel quite well the first reflexions. (that is because the reflected signal has the opposite circulation direction (left becomes right), so the receiver is insensitive to this reflected signal) The helical would be ideal.



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)

WLAN equipment can be damaged by various electrical disturbances such as power line switching transients and voltage surges, as ell as static build-up on outside wires and antennas.

Arrestors for coaxial cable also come in several types, each of which functions somewhat differently. DC blocking-type arrestors have a fixed frequency range and must be selected for a specific application. Their main advantage is that they present a high-impedance path to the frequencies found in lightning (less than 1 MHz) while offering a low impedance to signals created by your radio.

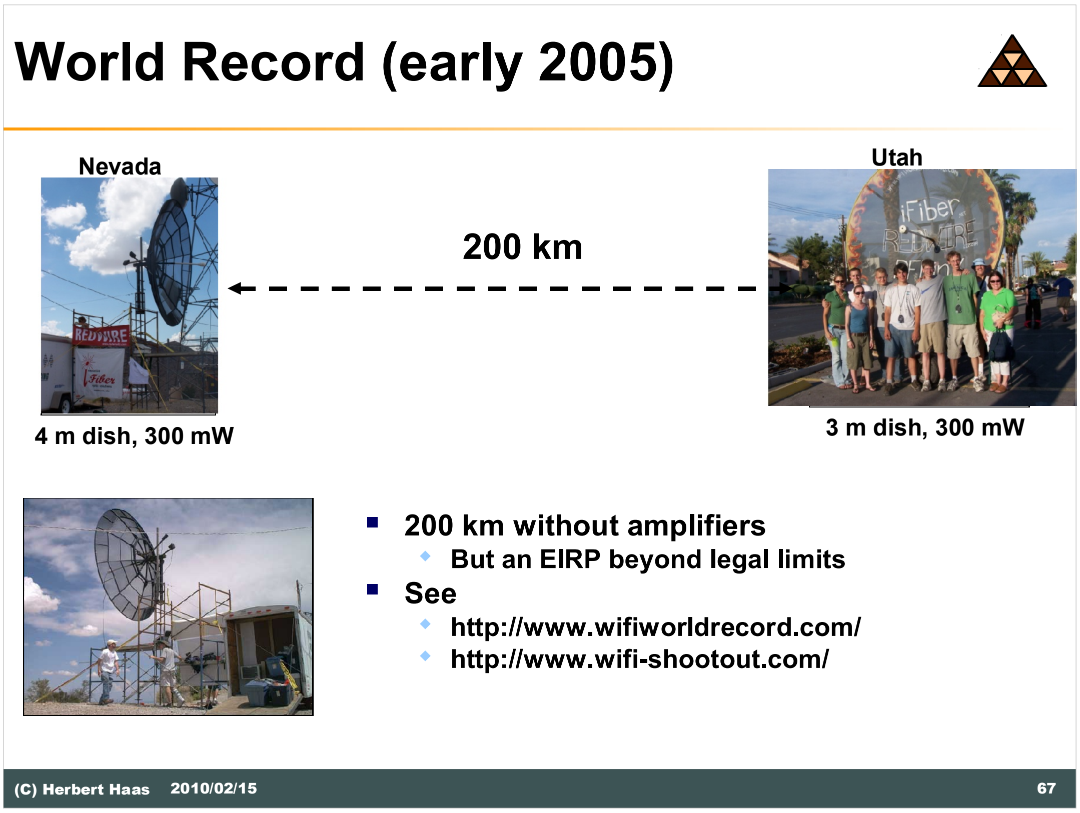
Arrestors that have **dc continuity** (gas tube and spark gap types) are broad-band and can be used over a wider frequency range than the dc-blocking types. Also, in installations where the coax is also used to **supply voltages to a remote device** (such as a mast-mounted preamp or remote coax switch), the dc continuity-type arrestor must be used.

The **Cisco Aironet Lightning Arrestor** prevents energy surges from reaching the RF equipment by the shunting effect of the device. Surges are limited to less than 50 volts, in about .0000001 seconds (100 nano seconds). A typical lightning surge is about .000002 (2 micro seconds). The accepted IEEE transient (surge) suppression is 8 usec. The Lightning Arrestor is a 50-ohm transmission line with a gas discharge tube positioned between the center conductor and ground. This gas discharge tube changes from an open circuit to a short circuit almost instantaneously in the presence of voltage and energy surges, providing a path to ground for the energy surge.

Note: Lightning can occur even without a thunderstorm - whenever and wherever there is a sufficient charge build-up.
Note: Some towers, especially AM radio towers, are not grounded because the tower is actually isolated from ground, being used as the antenna. This is known as a *hot* tower, and you must isolate the bridge and all grounds from this type of tower.

However, the ARRL Antenna Book states, "The best protection from lightning is to disconnect all antennas from equipment and disconnect all equipment from power lines."

When lightning strikes, it will always try to find the shortest electrical path to ground. Proper grounding is critical to lightning protection. Lightning contains energy in a wide range of frequencies therefore provide a low-impedance path to ground for the energy.



World Record (early 2005)

Nevada

4 m dish, 300 mW

200 km

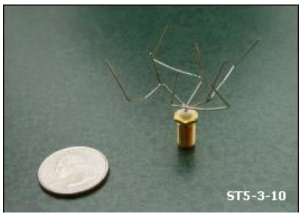
Utah

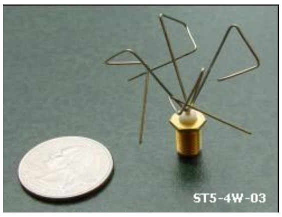
3 m dish, 300 mW

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

3m dish => 35 dBi

Tomorrow's Antenna Design





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