ITSC 301: Wireless Security

Module 2 – Basic RF Theory

Table of Contents

Review Module 1 Lecture & Lab

Review Module 1

- RF terminology
- Radio spectrum
- Regulatory bodies
  - Canada (DIESC)
  - US (FCC)
- Standards bodies
  - IEEE
- Lab/Assignment

RF Terminology

Introduction

This module will examine RF measurements and characteristics.

Learning Outcome:

- Analyze radio frequency characteristics and behaviour to solve wireless application problems.

RF Terminology

- Wavelength: Length from crest to crest (or trough to trough). Unit in meters with typical values in the nano-meter range.
- Frequency: 1/Wavelength. Unit in hertz (Hz) with typical values being in the KHz-GHz range.

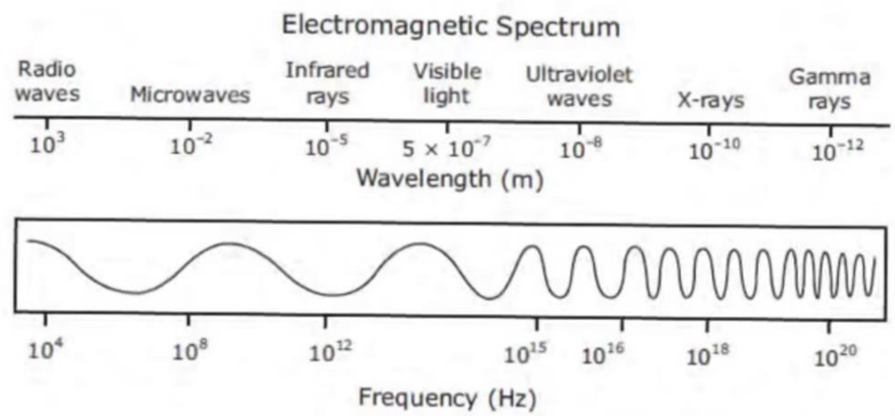


Figure 1: Electromagnetic Spectrum
Source?

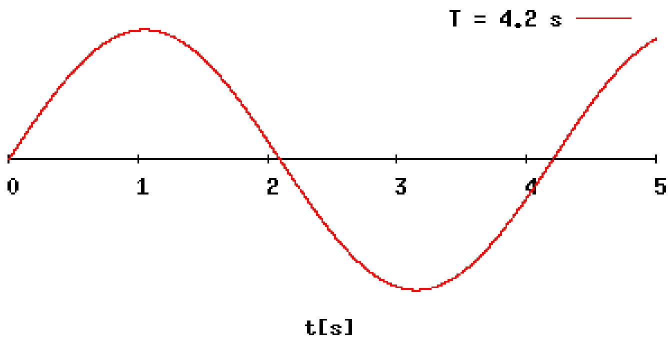


Figure 2: Wave Change Due to Increase of Period
© Superborsuk, 2006, https://commons.wikimedia.org/wiki/File:Wave_period.gif (CC-BY-SA 3.0)

RF Terminology

- Modulation: Process of varying one or more properties of a periodic waveform, called the *carrier signal*, with a modulating signal that typically contains information to be transmitted.
  - Used in most 802.11 WiFi: orthogonal frequency-division multiple access (OFDM), frequency-hopping spread spectrum (FHSS), direct-sequence spread spectrum (DSSS)

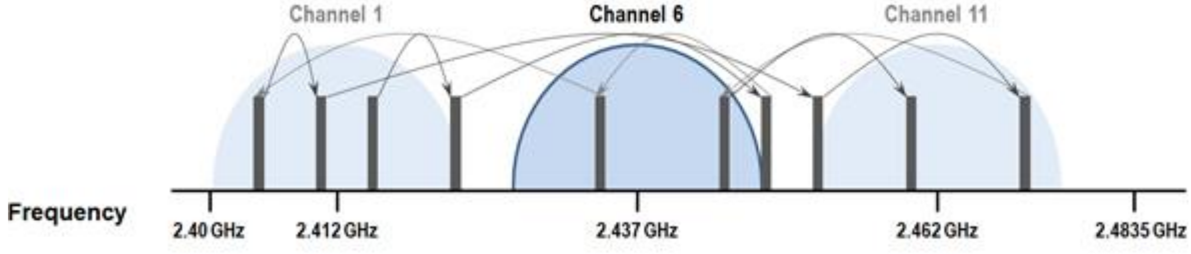


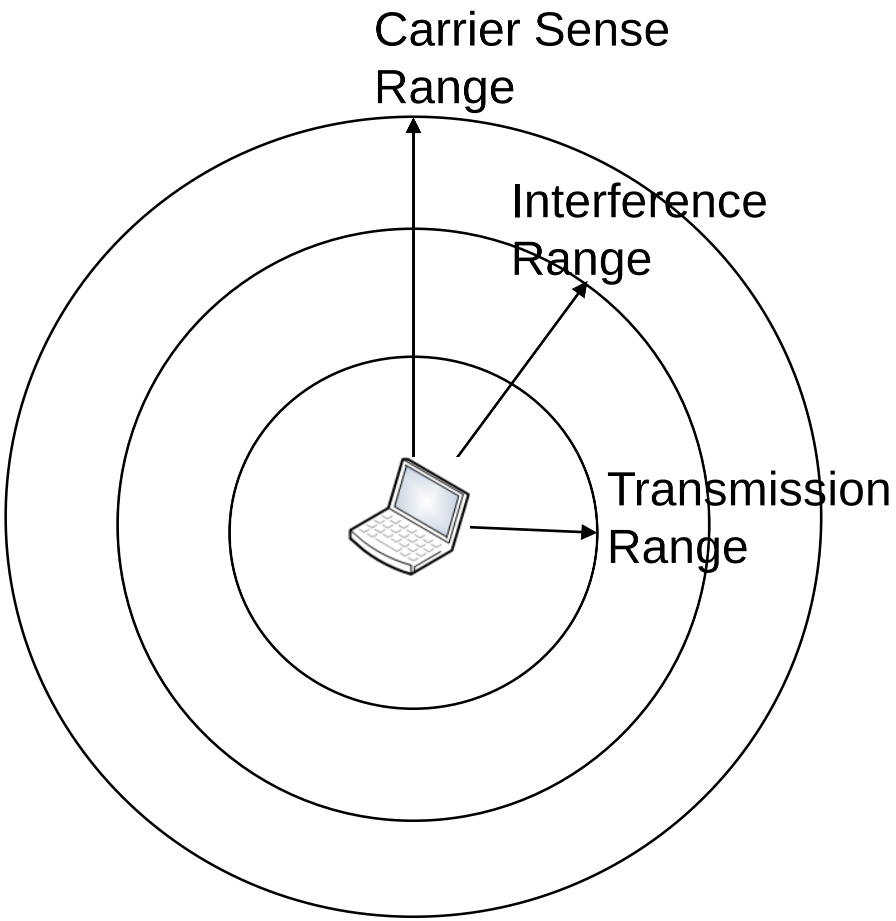
Figure 3: Title

Source: Laird Technologies, 2012. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

RF Terminology

- Transmission Range: The range within which the receiver of a packet can receive and decode the packet correctly
- Interference Range: The range within which the transmission cannot be decoded correctly by the receiver but is of sufficient power/energy to disrupt the correct reception of other packets that the receiver could also be receiving
- Carrier Sense Range: The range where the transmission does not necessarily interfere with other packets being received by the receiver

Ranges


Carrier Sense
Range
Interference
Range
Transmission
Range

RF Terminology

- RF interference: The suppression of communication between two nodes due to simultaneous communication by two or more other nodes.
  - Detecting the existence of RF interference can be extremely difficult because of its variability
- Non-uniform coverage area: An irregular coverage area results from inaccurate prediction of signal coverage for a wireless network, creating dead spots. One solution is to deploy additional access points to guarantee coverage.
- Dynamic coverage area: As well as being irregular, coverage areas are also dynamic. Changes can occur due to furniture movement (e.g., metal cabinet) or the opening/closing of a door.

RF Terminology

- Radio spectrum: The electromagnetic spectrum with frequencies from 3 Hz to 3,000 GHz (3 THz). Electromagnetic waves in this frequency range called radio waves.

- Frequency allocation: The allocation and regulation of the electromagnetic spectrum into radio frequency bands, performed by governments in most countries.

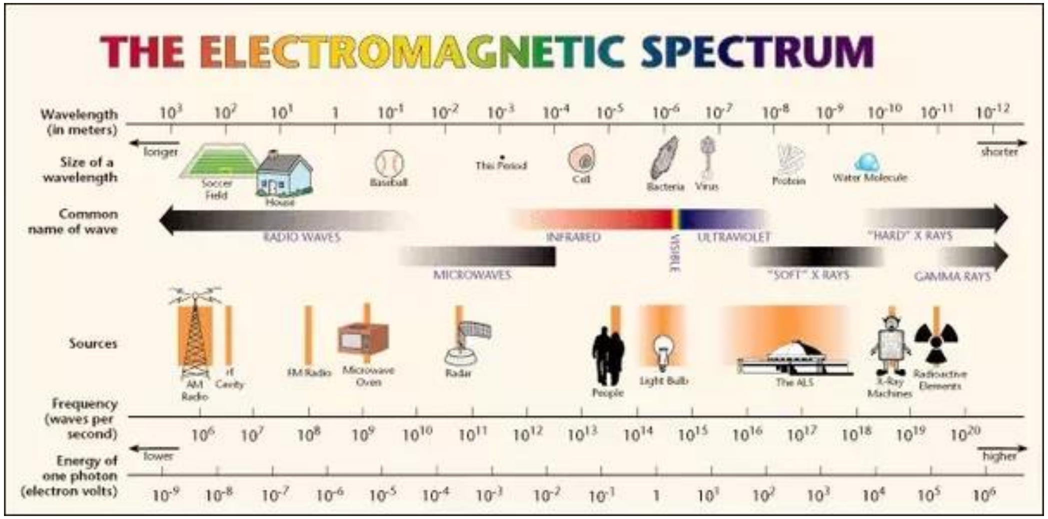


Figure 5: The Electromagnetic Spectrum
Source: NASA, 2010. https://commons.wikimedia.org/wiki/File:Cont_emspec2.jpg (CC0)

RF Basics & History

Learning Objectives

- Outline RF signal characteristics.
- Describe the basic concepts of RF behaviour.
- Explain decibel (dB) as it is used in RF measurements and calculations.
- Perform calculations on frequency and wavelength conversions by employing the basic components of RF mathematics.
- Configure autonomous environments.

Basic Wireless Elements

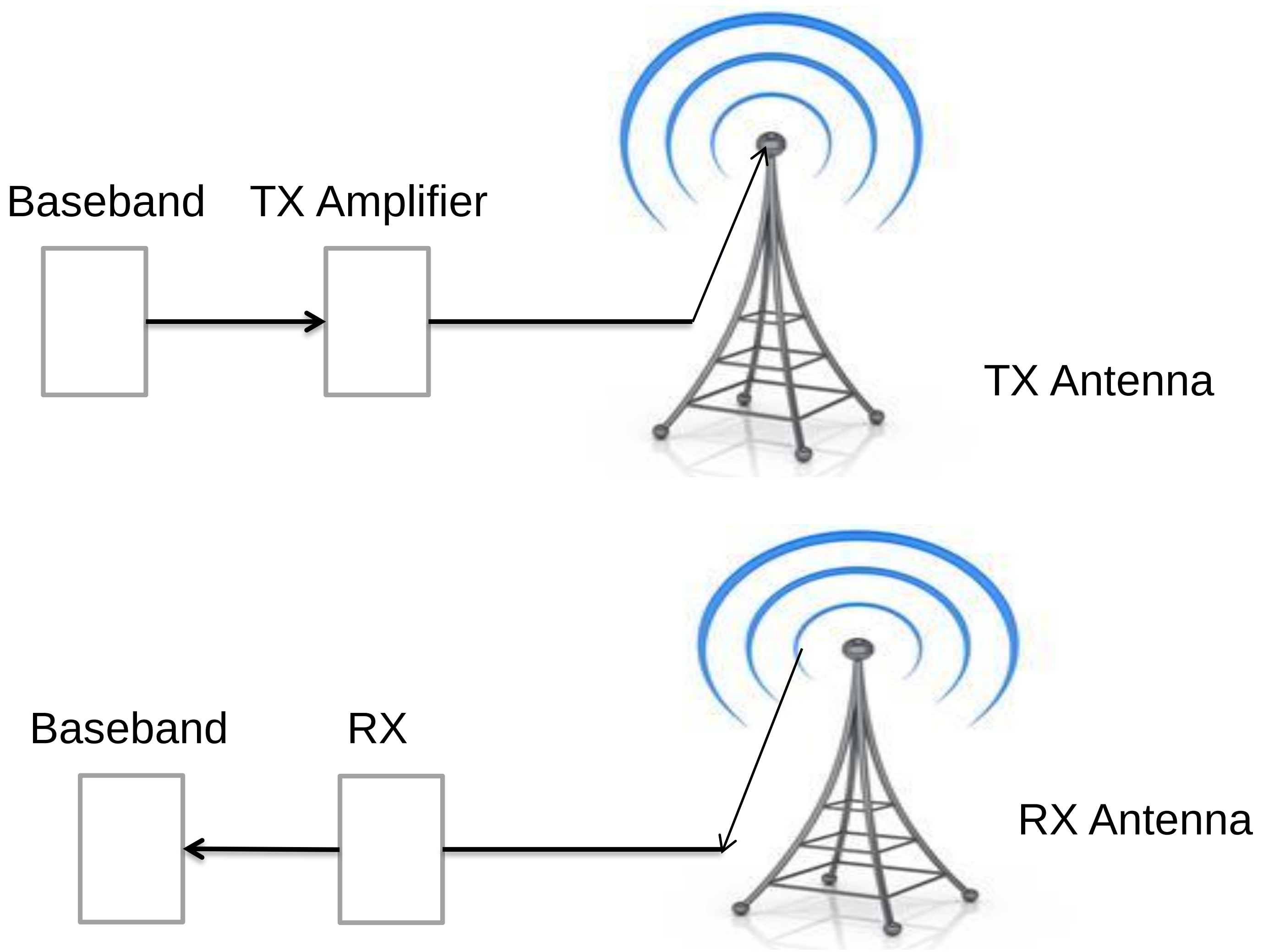


Figure 6: Title
© 2018, Southern Alberta Institute of Technology

Basic Wireless Elements

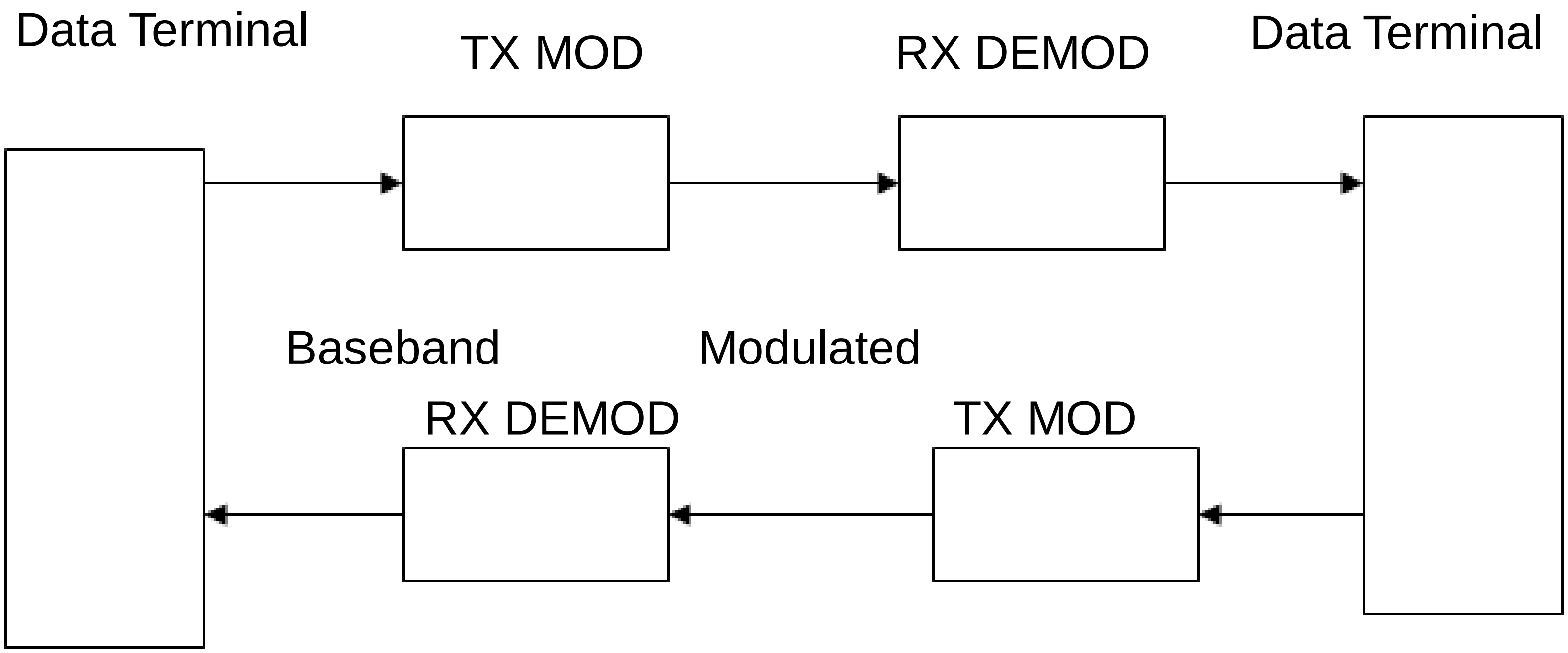


Figure 7: Title

Frequency and Wavelength

- Frequency: number of complete cycles per unit of time.
- One complete cycle of a sine wave = one hertz
- One wavelength = One complete wave's distance as measured units of meters.

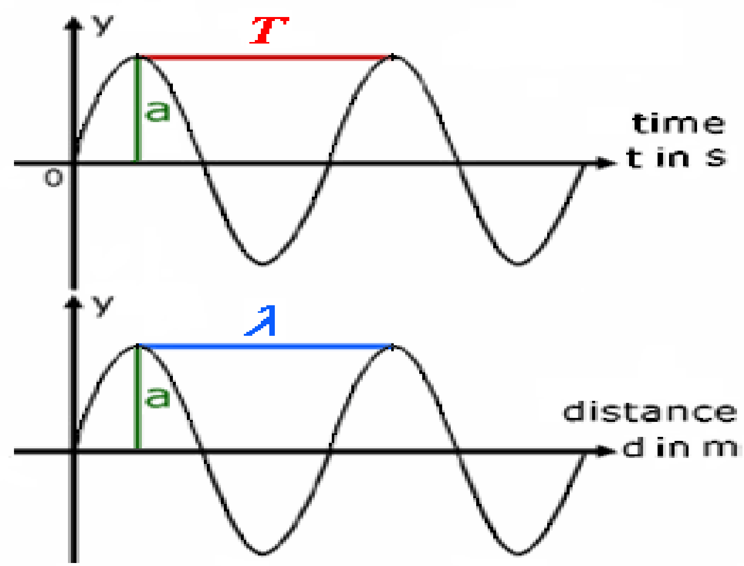


Figure 8: Title
© 2016, A-level Physics Tutor, http://www.a-levelphysicstutor.com/wav-wave-props.php# (CC-BY-NC-ND 4.0)

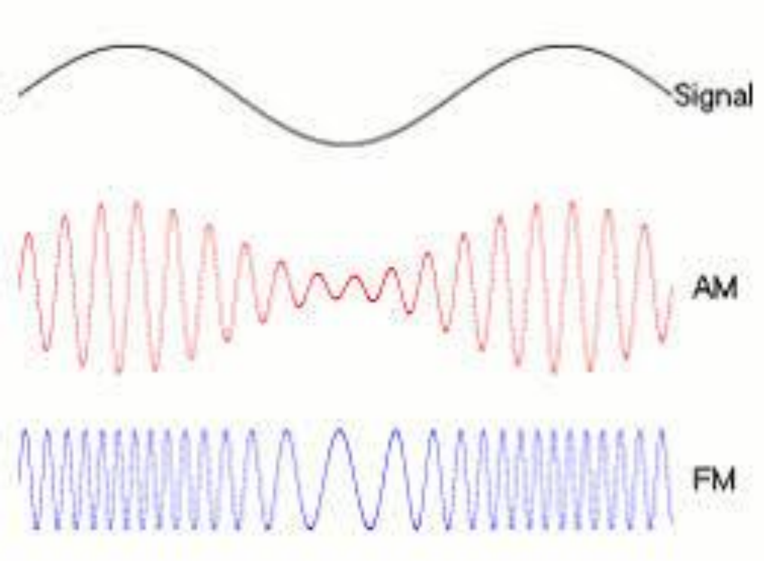


Figure 9: A low-frequency message signal (top) may be carried by an AM or FM radio wave
© 2008, Berserkerus, https://commons.wikimedia.org/wiki/File:Amfm3-en-de.gif (CC-BY-SA 2.5)

Time Domain vs. Frequency Domain

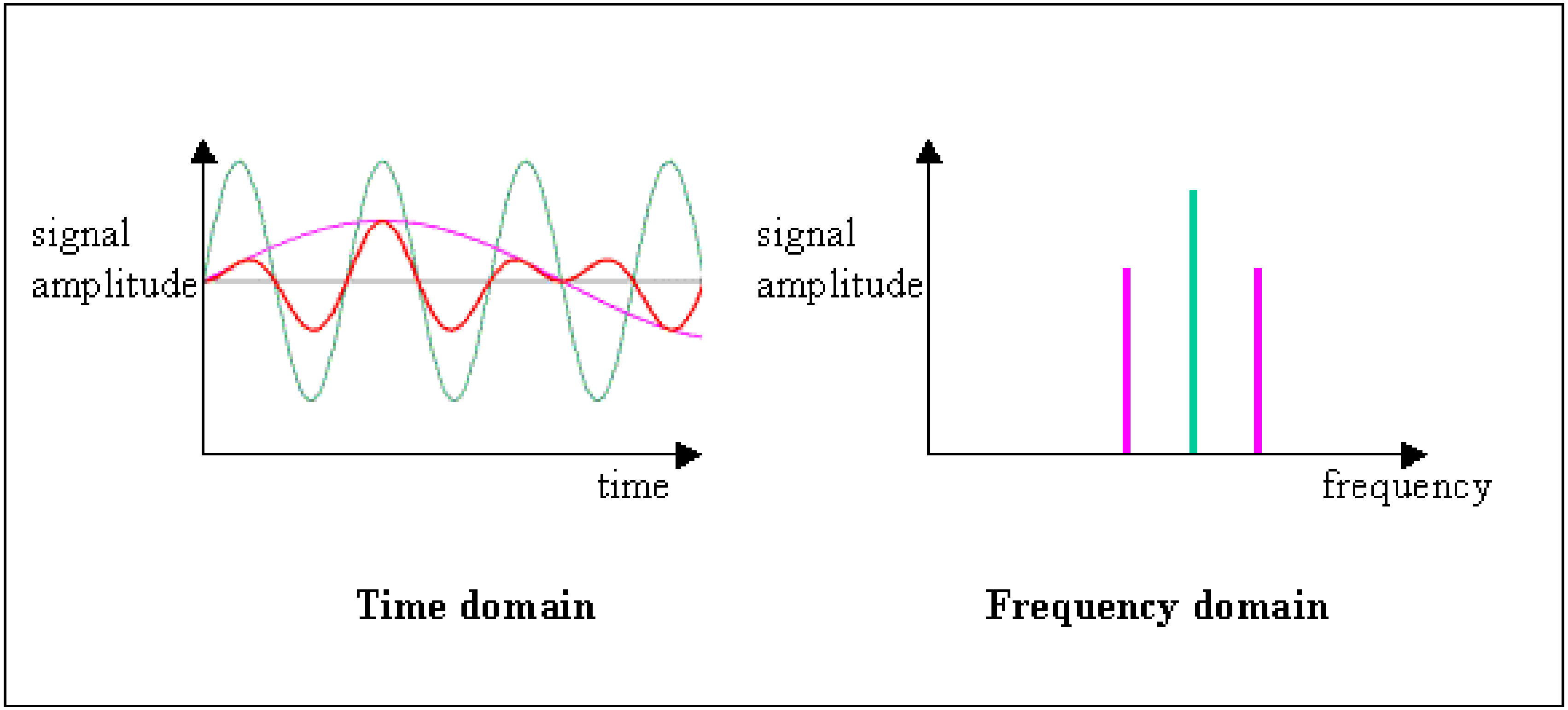


Figure 10: Time Domain vs. Frequency Domain

Source: National Instruments, 2016. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Frequency vs. Wavelength

Wavelength is the length of a cycle at its propagation rate.

$$\lambda = \frac{C}{f}$$

Where:
λ = wavelength (meters)
C = rate of travel (meters/second) [in this case the speed of light]
f = frequency

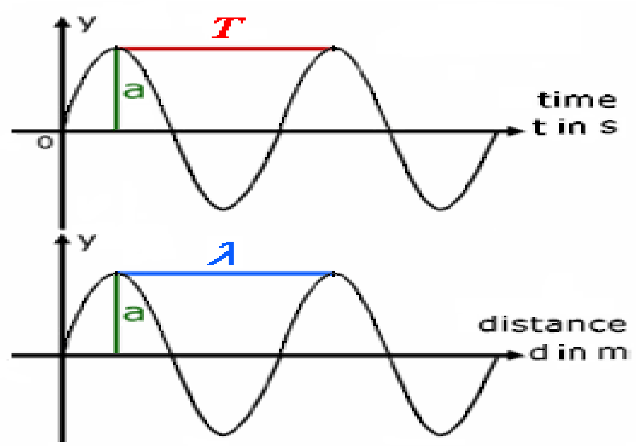


Figure 10: Title

If the frequency were 300,000,000 Hz,
at the speed of light (approx. 300,000,000 m/s), the wavelength would be
1 meter.

Frequency to Wavelength Conversion

- Frequency identifies a particular path through spectrum
- Wavelength describes the particular path through spectrum
- Frequency and wavelength are inversely proportional
  - C = Velocity (c in a vacuum = 300,000 km/s)
  - F = Frequency
  - λ = Wavelength

$$\lambda = \frac{C}{f}$$

Radio Wave Propagation

- As the signal leaves the antenna it propagates, or disperses, into space. The antenna selection determines how much propagation occurs.
- At 2.4 GHz, it is extremely important to ensure a that a path (or tunnel) between the two antennas is clear of any obstructions. Should the propagating signal encounter any obstructions in the path, signal degradation occurs.

Radio Wave Propagation: Dispersion

- Behaves as an expanding sphere equally in all directions.

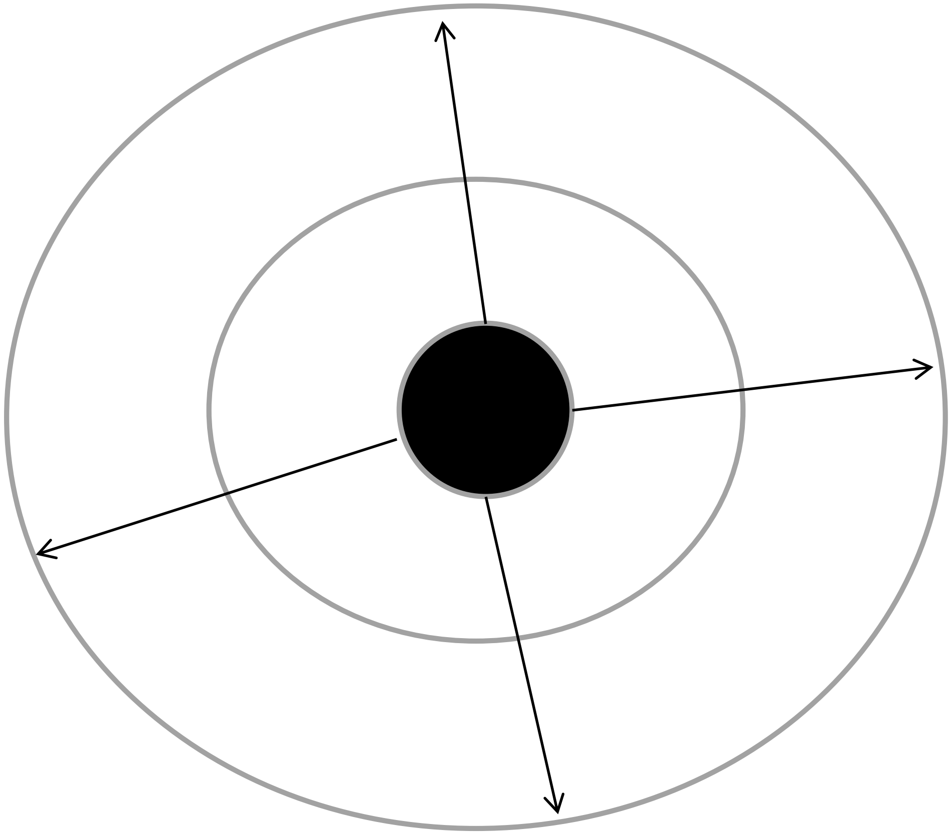


Figure 11: Dispersion
© 2018, Southern Alberta Institute of Technology

Radio Wave Propagation

The greatest amount of loss in your wireless system is from *free space propagation*. The *free space loss* is predictable and given by the formula:

$$FSL(dB) = 32.45 + 20Log10F(MHz) + 20Log10D(km)$$

The free space loss at 1 km using a 2.4 GHz system is:

$$FSL(dB) = 32.45 + 20Log10(2400) + 20Log10(1)$$

$$= 32.45 + 67.6 + 0$$

$$= 100.05 \text{ dB}$$

Radio Wave Propagation

- Attaining Line of Sight (LOS) between the sending and receiving antenna is essential in both point-to-point and point-to-multipoint installations.
- Generally, there are two types of LOS that are used during installations:
  - Optical LOS: the ability to see one site from the other
  - Radio LOS: the ability of the receiver to ‘see’ the transmitted signal. 1/3 greater distance than optical.

Radio Wave Propagation

The distance between the transmitter and receiver over average terrain is a factor of frequency, K factor, the height of the tower, temperature, barometric pressure and humidity.

d = sqrt17ht + sqrt17hr

- d: distance in km
- sqrt: square root
- ht: height of transmitting antenna in meters
- hr: height of receiving antenna in meters

Radio Wave Propagation: Refraction

- The bending of waves as they change speed through differing mediums.

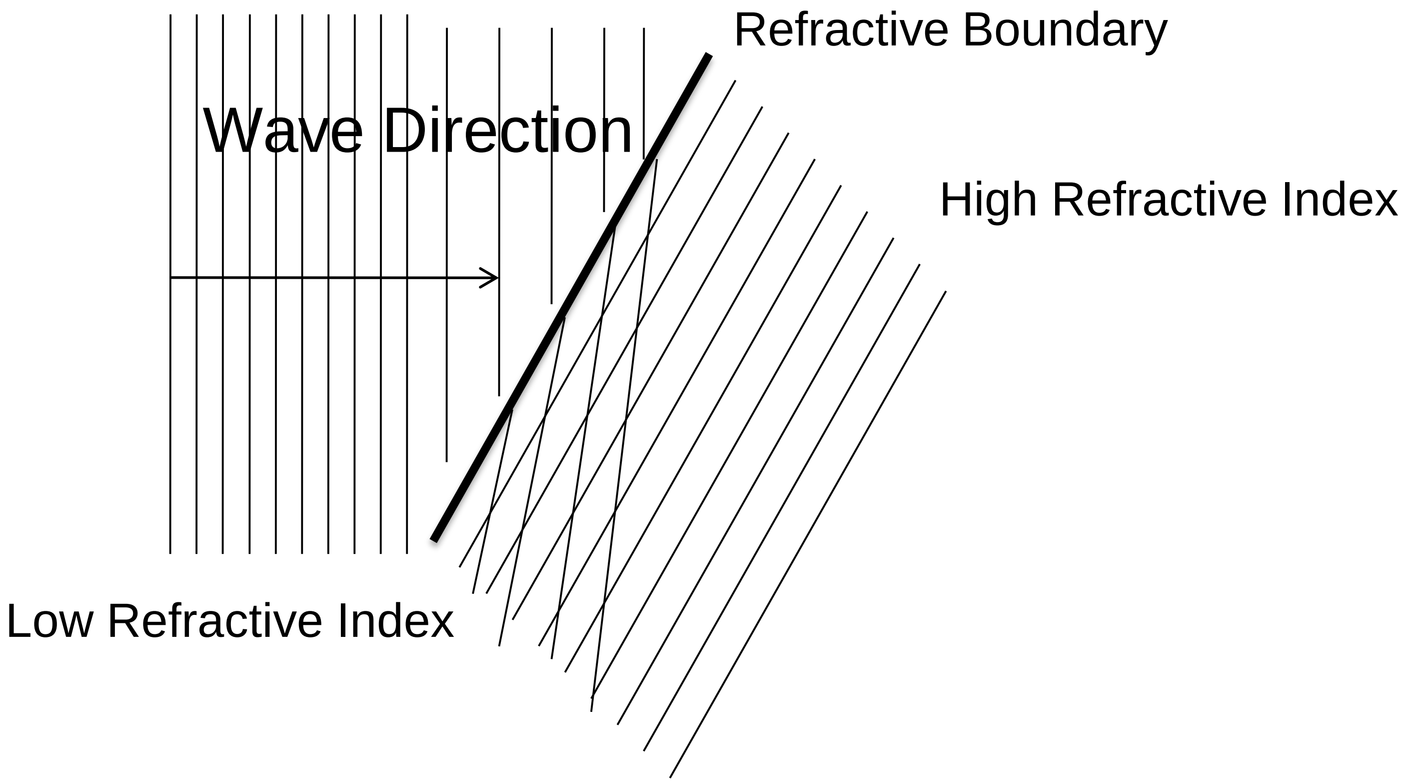


Figure 12: Refraction
© 2018, Southern Alberta Institute of Technology

Radio Wave Propagation: Reflection

- The bending of waves back towards their source.

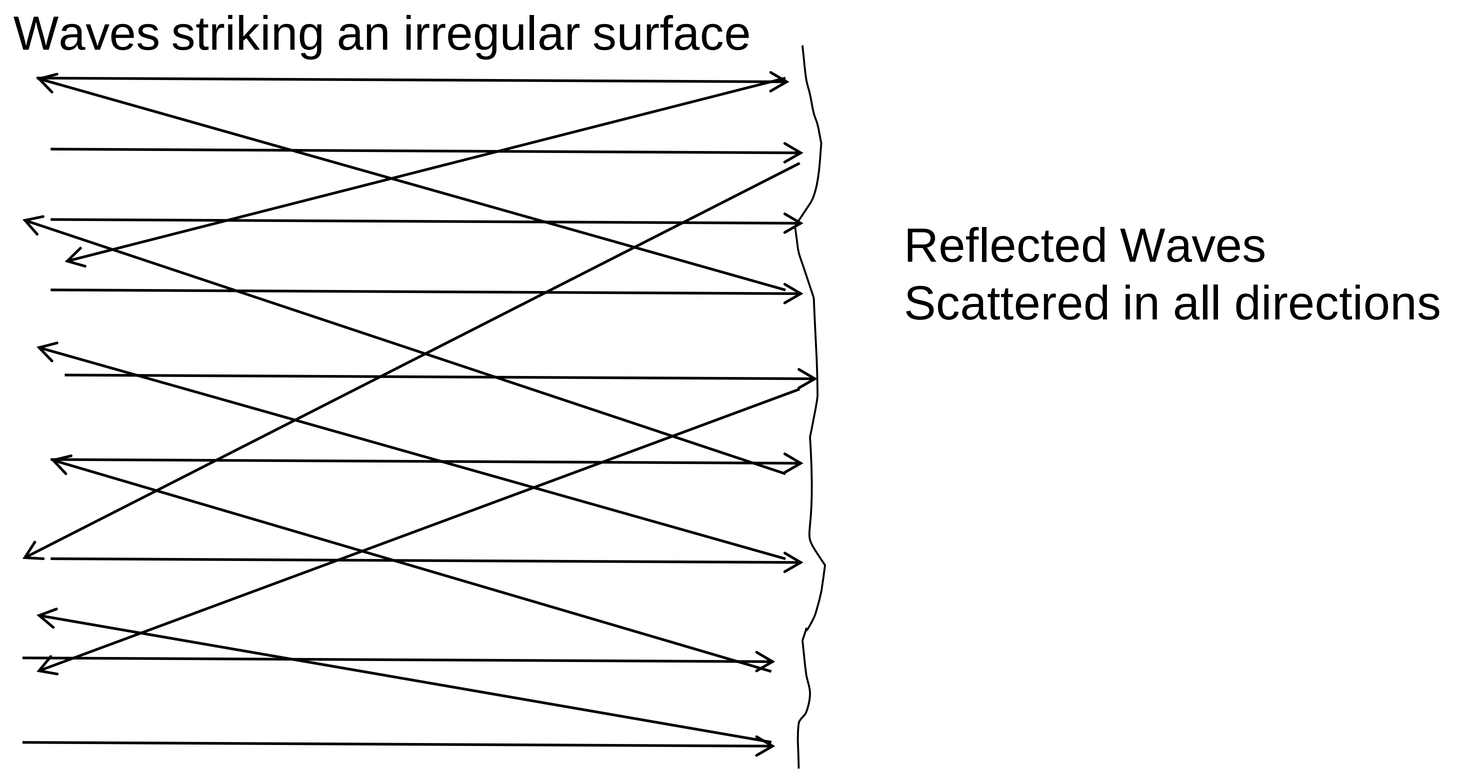


Figure 13: Reflection
© 2018, Southern Alberta Institute of Technology

Radio Wave Propagation: Diffraction

- Interference caused when two waves of differing frequency or phase interact.

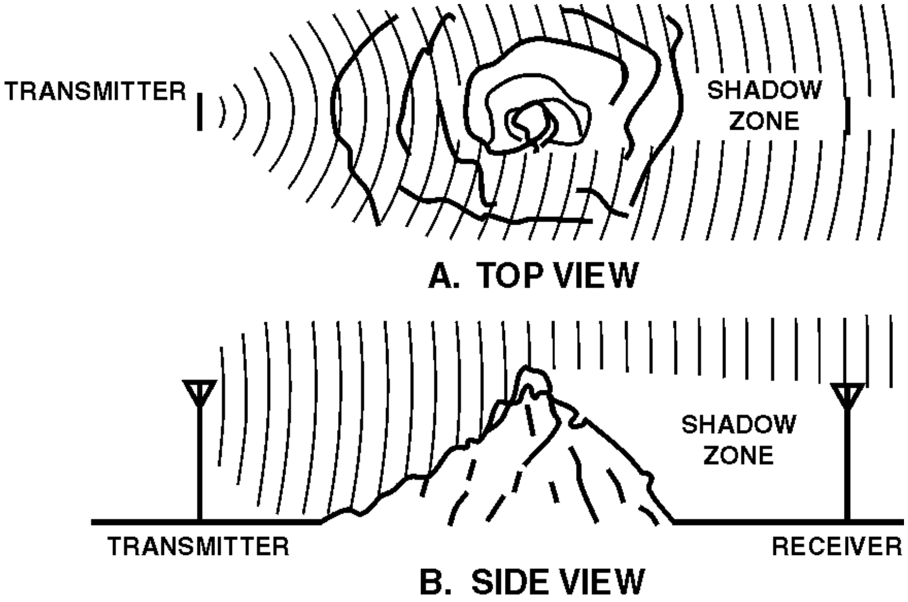


Figure 14: Title
Source: Integrated Publishing, Inc., n.d. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Figure 15: Title
© 2018, PE1MEW.
http://radiomobile.pe1mew.nl/?Calculations:Propagation_calculation:Radio_propagation&q=diffraction (CC BY-SA 3.0 NL)

Radio Wave Propagation: Absorption

- Energy that becomes part of another entity.

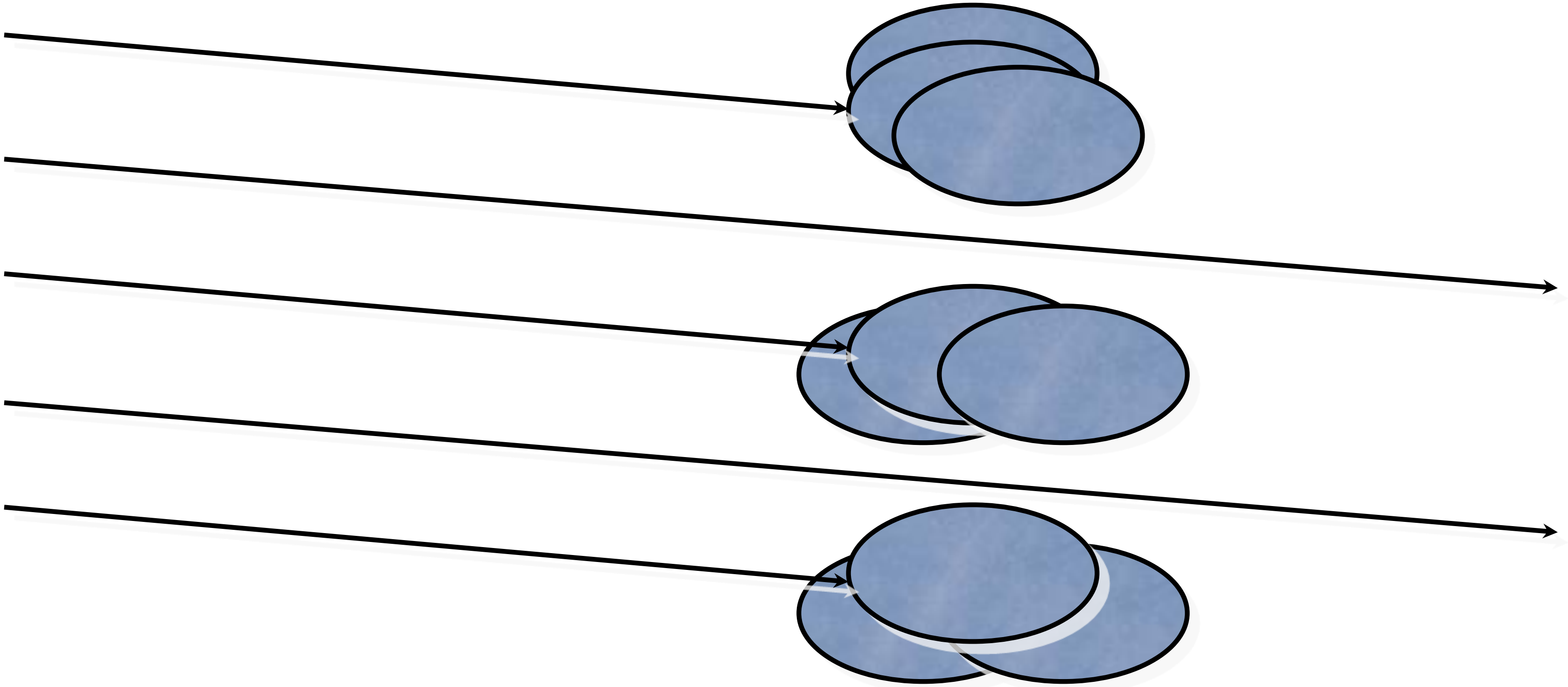


Figure 16: Absorption

Radio Wave Propagation: Scatter

- Non-uniform changes in an electromagnetic wave’s trajectory.

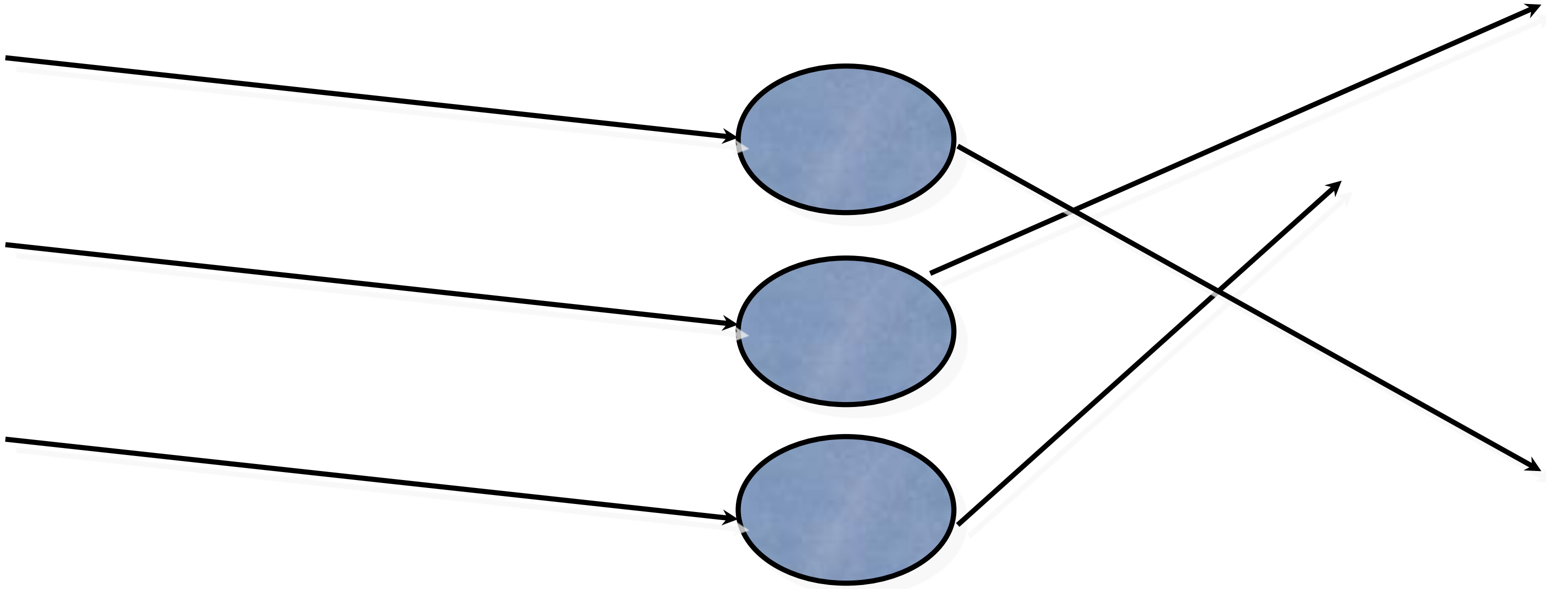


Figure 17: Scatter

Radio Wave Propagation

- To quantify radio line of sight, the *Fresnel Zone theory* is applied.
- Think of the Fresnel Zone as a football-shaped tunnel between the two sites that provides a path for RF signals.
- Obstructions in the Fresnel Zone are generally undesirable.

Radio Wave Propagation

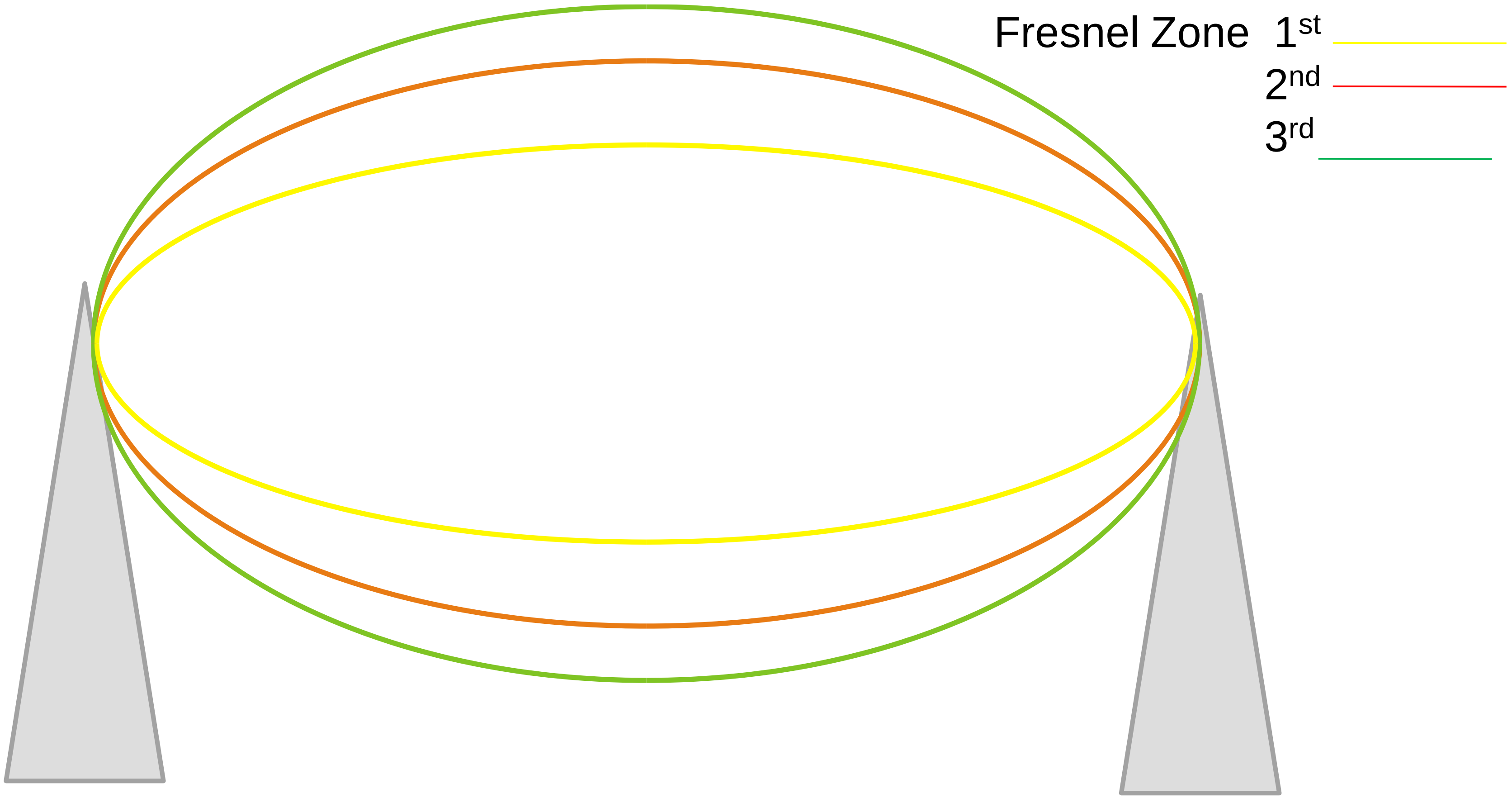
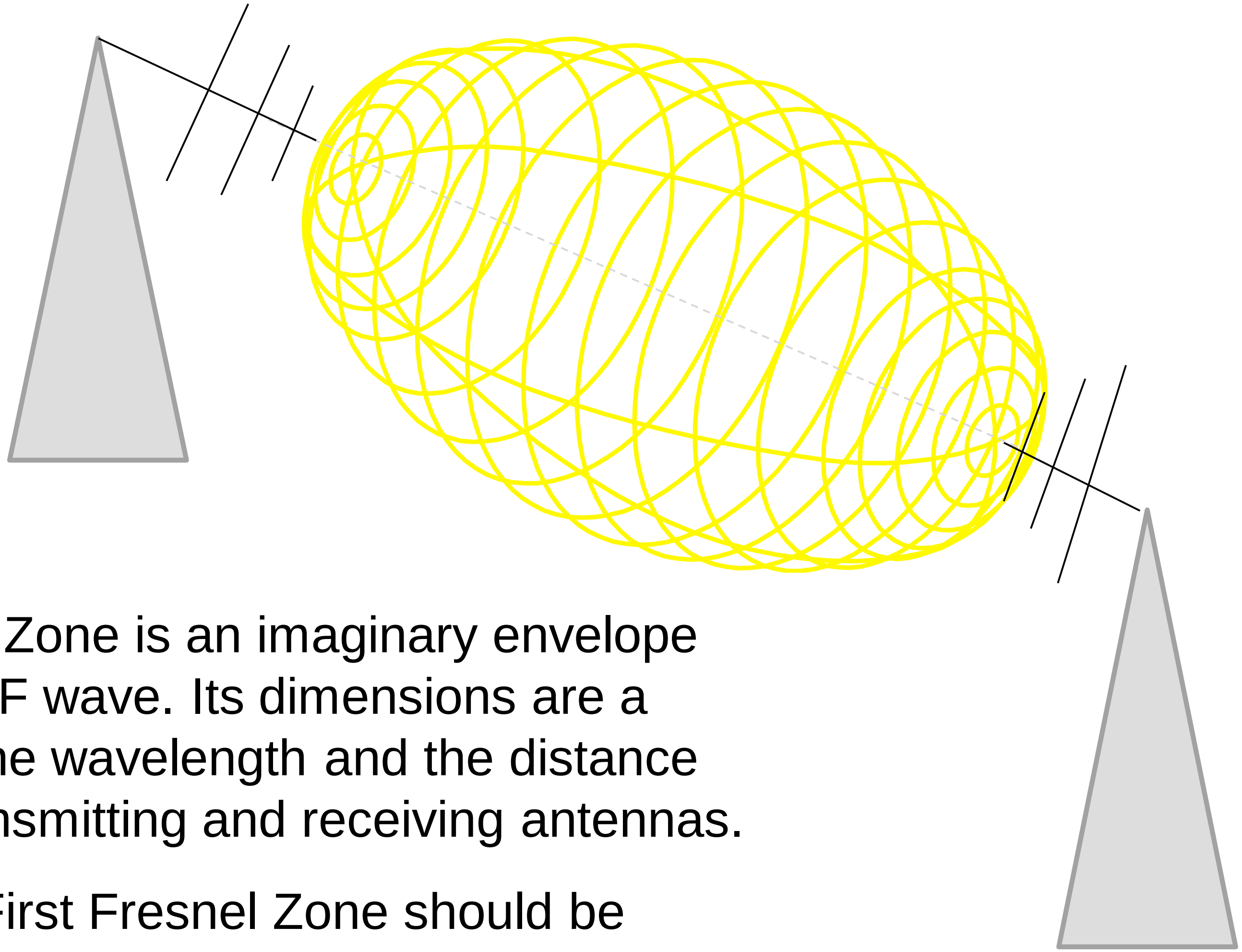


Figure 18: Fresnel Zone
© 2018, Southern Alberta Institute of Technology

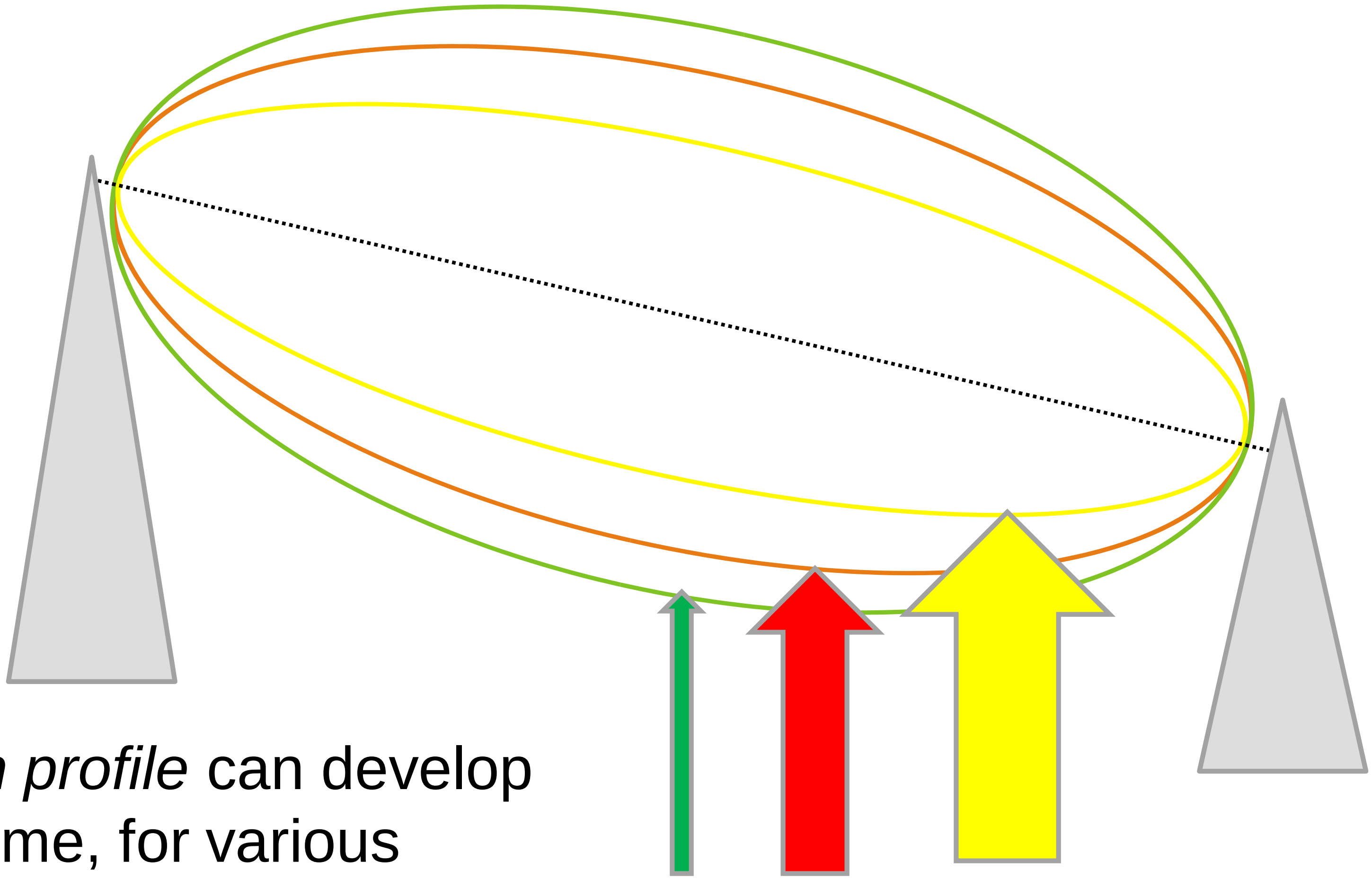
The First Fresnel Zone



- The Fresnel Zone is an imaginary envelope around an RF wave. Its dimensions are a function of the wavelength and the distance between transmitting and receiving antennas.
- 60% of the First Fresnel Zone should be obstruction free

Figure 19: Title
© 2018, Southern Alberta Institute of Technology

The Path Profile



A *path profile* can develop over time, for various reasons (e.g., vegetation, buildings).

Figure 20: Title
© 2018, Southern Alberta Institute of Technology

Ground Waves

- Frequencies up to 3 MHz follow the curvature of earth.
- Ground waves attenuate quickly.
- Ground waves are effective in achieving over-the-horizon applications, but only LF or VLF bands.
- See: http://www.radio-electronics.com/info/propagation/ground_wave/ground_wave.php

Space Waves

- Space waves are also referred to as *direct waves*.

- Tx to RX Line of Sight LOS is required.

Sky Waves

- Sky waves are refracted back to earth by the ionosphere.
- Sky waves are high frequency HF band signals.
- Sky waves must contact the ionosphere at the perfect angle to skip back to earth.

Radio Wave Propagation

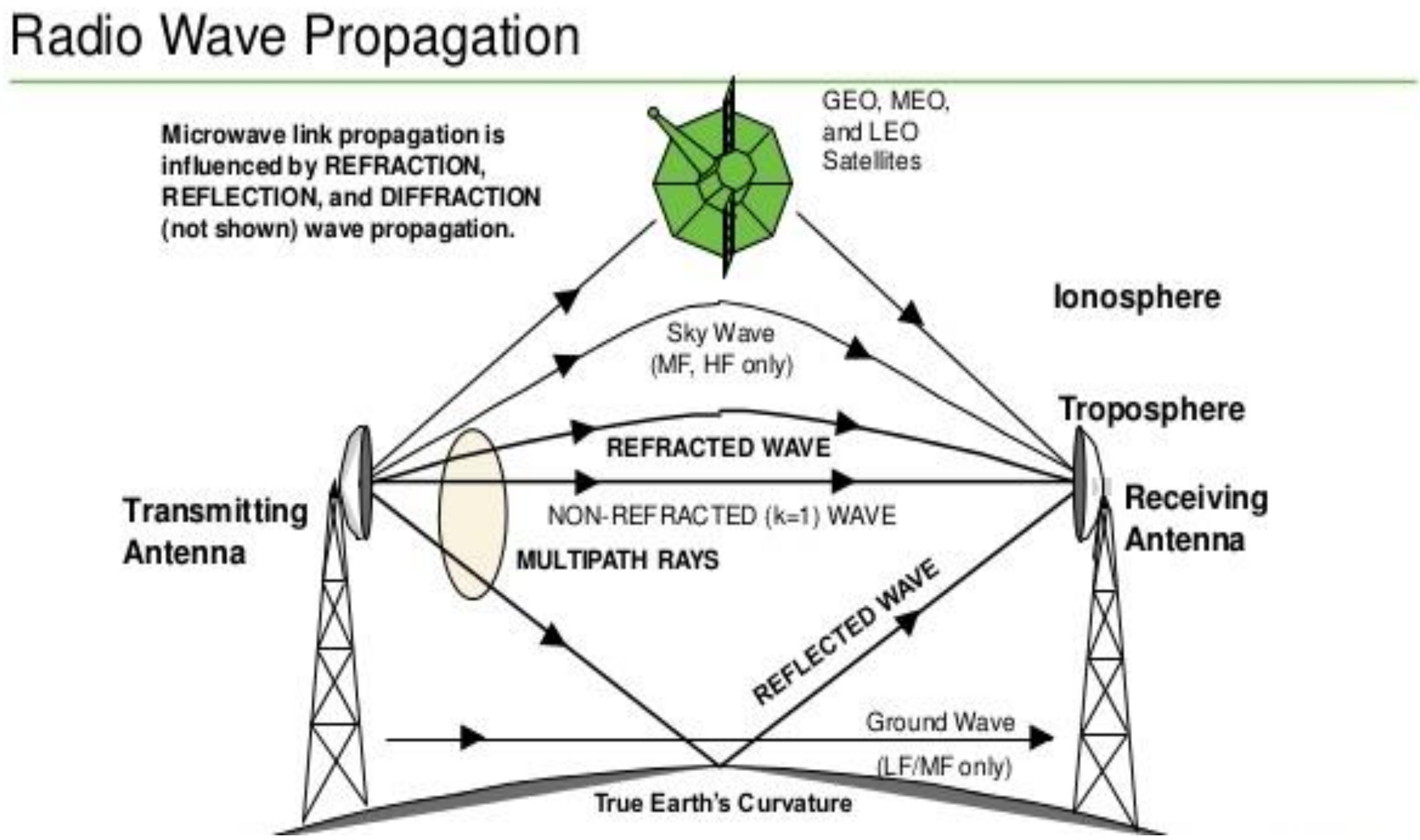


Figure 21: Title
Source: Aviat Networks., 2013. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Radio Wave Propagation

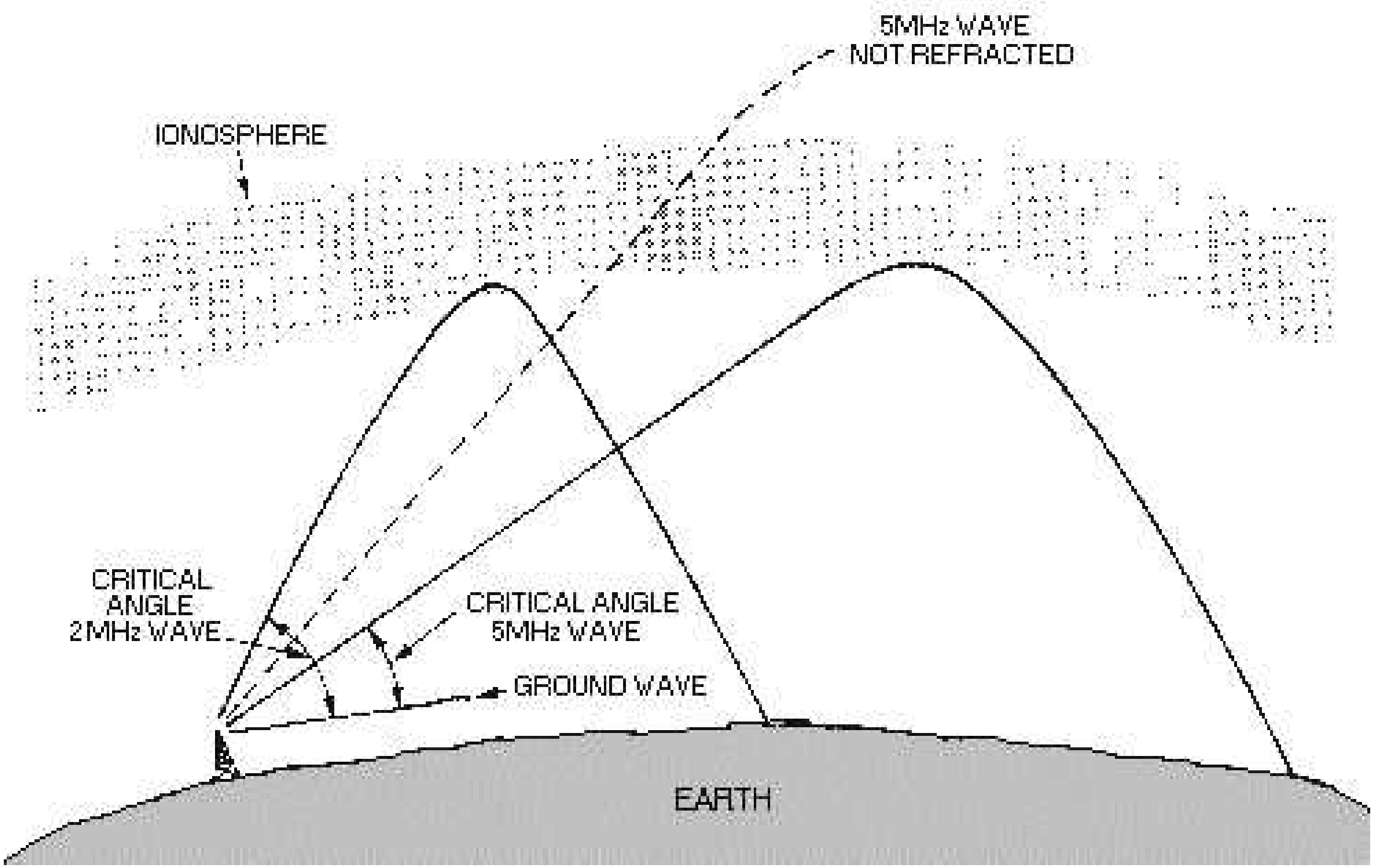


Figure 22: Effects of Frequency on the Critical Angle

Source: Integrated Publishing, Inc., n.d. Reproduced and used in accordance with the fair dealing provisions in section 29 of the Canadian Copyright Act for the purposes of education, research or private study. Further distribution may infringe copyright.

Radio Wave Propagation

- Fixed environment versus mobile environment
- Mobile environment path is dynamic
- Mobile environment can be very cluttered
- Mobile environment attenuation increases more rapidly with distance

Free Space Loss Lfs(dB) = 32.45 + 20Log f (MHz) + 20Log d(km)

Mobile Propagation loss Lp(db) = 68.75 + 26.16 Log f – 13.82 log h + (44.9-6,55 log h) log d

Units & Conversion

Units of Measure

- Watt (W)
- Milliwatt (mW)
- Decibel (dB)
- Decibel milliwatt (dBm)
- Decibel isotropic (dBi)

Milliwatts & Watts

Milliwatts

- 802.11 devices use between 1 and 100 mW
- 1 mW used for small areas
- 15–30 mW for PCMCIA
- 30–100 mW for APs (some companies use up to 250 mW)
- > 250 mW for outdoor use

Watts

- CSA allows up to four watts radiated antenna power on PTMP unlicensed 2.5GHz

Decibels

- RF signal has logarithmic drop-off during propagation
- Signal weakens quickly
- Measures the relative strength between two signals

Power difference (dB) = 10 × log(power A ÷ power B)

Gain & Loss

- Measures in dB
- 10s & 3s RF shortcut

  -3 dB = 1/2 power mW = ÷ 2

  +3 dB = double power mW = × 2

  -10 dB = 1/10 power mW = ÷ 10

  +10 dB = 10 times power mW = × 10

10s and 3s

- 25 mW signal has 3 dB loss:

  25 mW – 3 dB = 25 mW ÷ 2 = 12.5 mW

- 200 mW signal has a 10 dB gain:

  200 mW + 10 dB = 200mW × 10 = 2000 mW = 2W

10s and 3s Combining

- 15 mW signal has a 13 dB gain:

  15 mW + 13 dB

  = 15 mW + 10 dB + 3 dB

  = 15 mW × 10 × 2

  = 300 mW

10s and 3s Table

Gain dB	10s and 3s
1 dB	+ 10 - 9 (+ 10 - 3 - 3 - 3)
2 dB	- 10 + 12 (- 10 + 3 +3 + 3 + 3)
3 dB	+ 3
4 dB	+ 10 - 6 (+10 - 3 - 3)
5 dB	+ 20 - 15 (+ 10 + 10 - 3 - 3 - 3 - 3 - 3)
6 dB	+ 6 (+ 3 + 3)
7 dB	+ 10 - 3
8 dB	+ 20 - 12 (+ 10 + 10 - 3 - 3 - 3 - 3)
9 dB	+ 9 (+ 3 + 3 + 3)
10 dB	+ 10

Gain & Loss

- Remember: it's additive
- Add and subtract all gain or loss for a link, and then calculate the resulting dB from the original signal

dBm

- Normalizing the decibel (using an arbitrary reference point)
- dBm uses 1 mW as the reference point

100mW transmit power

$= 1 \text{ mW} \times 10 \times 10$

$= 1 \text{ mW} + 10 \text{ dB} + 10 \text{ dB}$

$= 1 \text{ mW} + 20 \text{ dB}$

Cumulative dBm

- Add gains and subtract losses
- Calculate total dB gain or loss as normal
- Use 1mW as reference to find total power in mW

45 mW transmitter has a cable loss of 6 dB, then is amplified with a gain of 10 dB

= 45 mW - 6 dB + 10 dB

= 45 mW - 3 dB - 3 dB +10 dB

= 45 mW ÷ 2 ÷ 2 × 10

= 112.5 mW

Or

= 45 mW - 6 dB + 10 dB

= 45 mW + 4 dB

= 45 mW + 10 dB - 3 dB - 3 db

= 45 mW × 10 ÷ 2 ÷ 2

= 112.5 mW

Convert dBm to mW

Convert to dBm first:

1 mW × 9 × 5 = 45 mW

1 mW + 9dB + 5dB = 45 mW

1 mW +14dB = 45 mW

14 dBm = 45 mW

= 14 - 6 + 10 = 18 dBm

Convert back to mW:

1 mW + 10 dB + 8 dB

= 1 mW × 10 × 10 × 10 ÷ 2 ÷ 2 ÷ 2 ÷ 2

= 62.5 mW

Not accurate (other method = 112.5 mW)

Accurate dBm

(wireless calculator)

$$dBm = (10\text{Log}_{10}(\text{milliWatts})) + 30$$

$$10\text{Log}_{10}(45\text{mW}) + 30$$

$$16.5 \text{ dBm}$$

$$16.5 \text{ dBm} - 6 \text{ dB} + 10 \text{ dB} = 20.5 \text{ dBm}$$

$$\text{milliWatts} = 10^{(\text{dBm}/10)}$$

$$10^{(20.5\text{dBm}/10)}$$

$$112.2 \text{ mW}$$

Power Level Chart

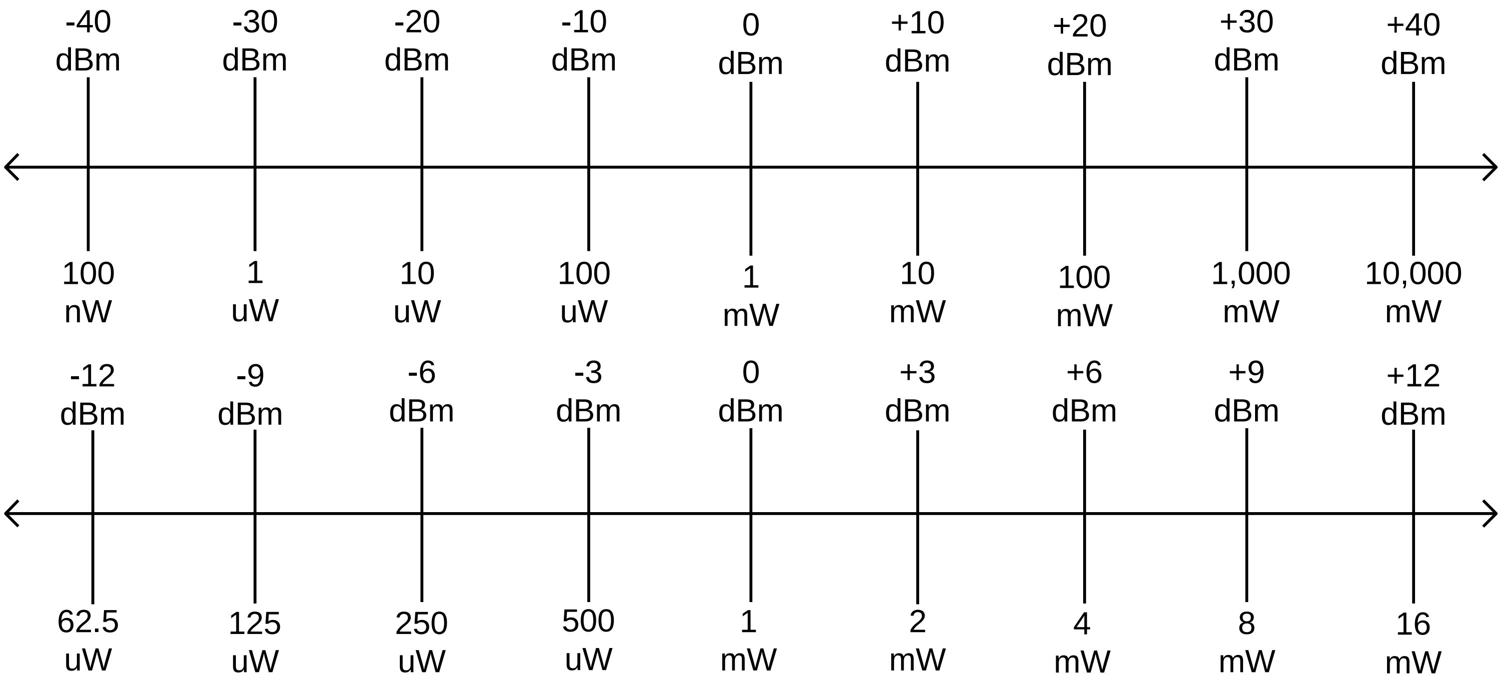


Figure 23: Power Level Chart
© 2018, Southern Alberta Institute of Technology

References

Aviat Networks, 2013. Fundamentals of microwave radio communication for IP and TDM. Retrieved from https://www.slideshare.net/loboalfaleal/uca-uni-july-2013

Integrated Publishing, n.d. The effect of the Earth's atmosphere on radio waves. Retrieved from http://electriciantraining.tpub.com/14182/css/Diffraction-73.htm

Integrated Publishing, n.d. Introduction to wave propagation, transmission lines, and antennas. Retrieved from http://electriciantraining.tpub.com/14182/

Laird Technologies, 2012. Bluetooth and Wi-Fi coexistence. Retrieved from https://home.zhaw.ch/~kunr/NTM1/literatur/laird-wireless-bluetooth-wifi-coexistence.pdf

National Instruments Corporation, 2016. Teach tough concepts: Frequency domain in measurements. Retrieved from http://www.ni.com/tutorial/13042/en/

For more information, contact:
Director, Centre for Instructional Technology and Development
Southern Alberta Institute of Technology
1301 16 Ave. N.W., Calgary, AB T2M 0L4