ITSC 301: Wireless Security

Module 1 – Regulations and Standards

Table of Contents

- Course Introduction
  - Course Structure
  - Evaluation Matrix
  - Wireless Lab
  - Lab/Assignment Grading
- Regulations and Standards
  - Introduction
  - Regulatory and Standard Organizations
  - RF Terminology

Course Introduction

Course Structure

- Course - 14 weeks
- Eight major, equally weighted, sections
  - Module 1 - Regulations and Standards
  - Module 2 - Basic RF theory
  - Module 3 - Layer one technologies
  - Module 4 - Layer two technologies
  - Module 5 - Wireless attack and defense
  - Module 6 - Authentication and encryption
  - Module 7 - Industrial protocols
  - Module 8 - Wireless infrastructure

Evaluation Matrix

Assessment	Weight (%)
Quizzes	10
Labs	15
Midterm Exam	35
Final Exam	40
Total	100

Wireless Labs

- Precautions are necessary
- Any wireless testing that could be malicious should be performed with an isolated industrial location (SAIT Cage).
- Understand the wireless environment/devices present and their operating frequencies, protocols or modulation techniques.

Lab/Assignment Grading

- Assignments are worth 1%
- Lab grades are broken into 7 major, equally weighted sections
- Each lab section consists of:
  - 20% documentation (see ISS standards from your COM 256 course)
  - 70% lab sign-off for successful completion of lab activities
  - 10% homework

RF Terminology

Introduction

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

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.

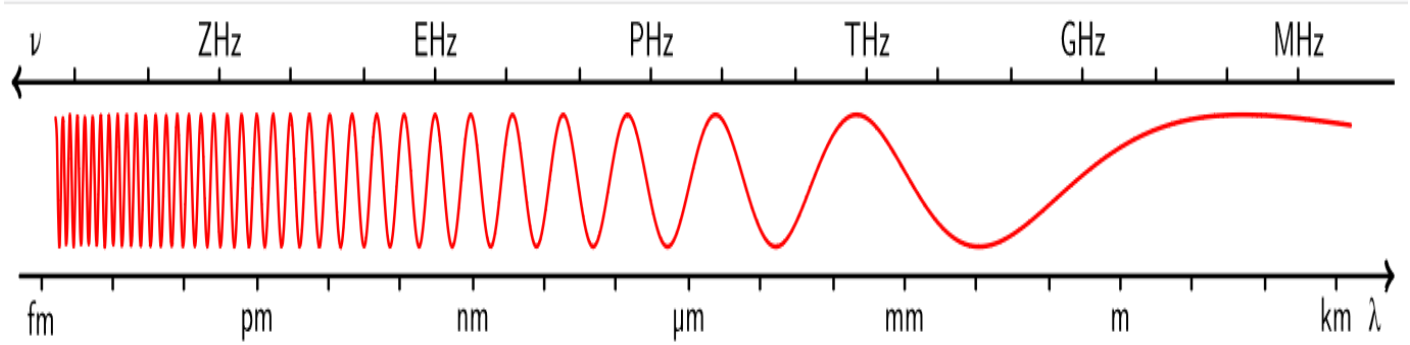


Figure 1: Frequency (v) and wave length (λ) have an inverse relation
© Palosirkka, https://commons.wikimedia.org/wiki/File:Frequency_vs._wave_length.svg (CC-BY-SA 3.0)

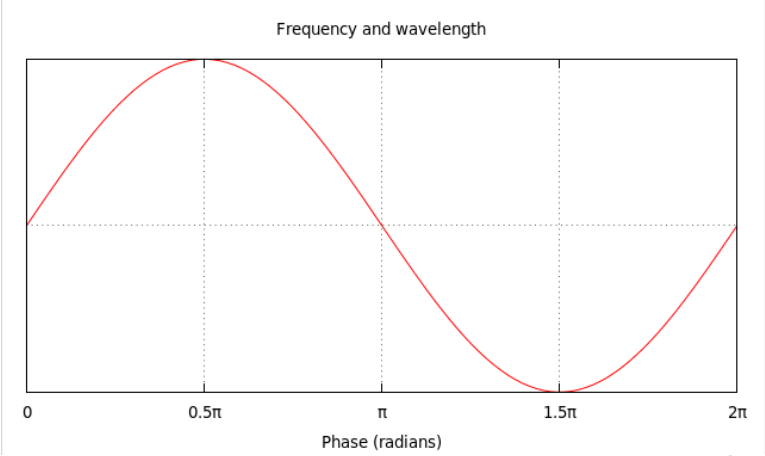


Figure 2:
Source?

RF Conversion

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

$$v = f \lambda$$

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)

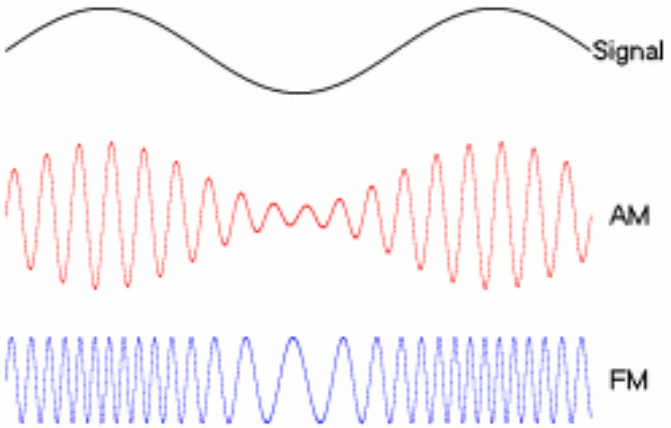
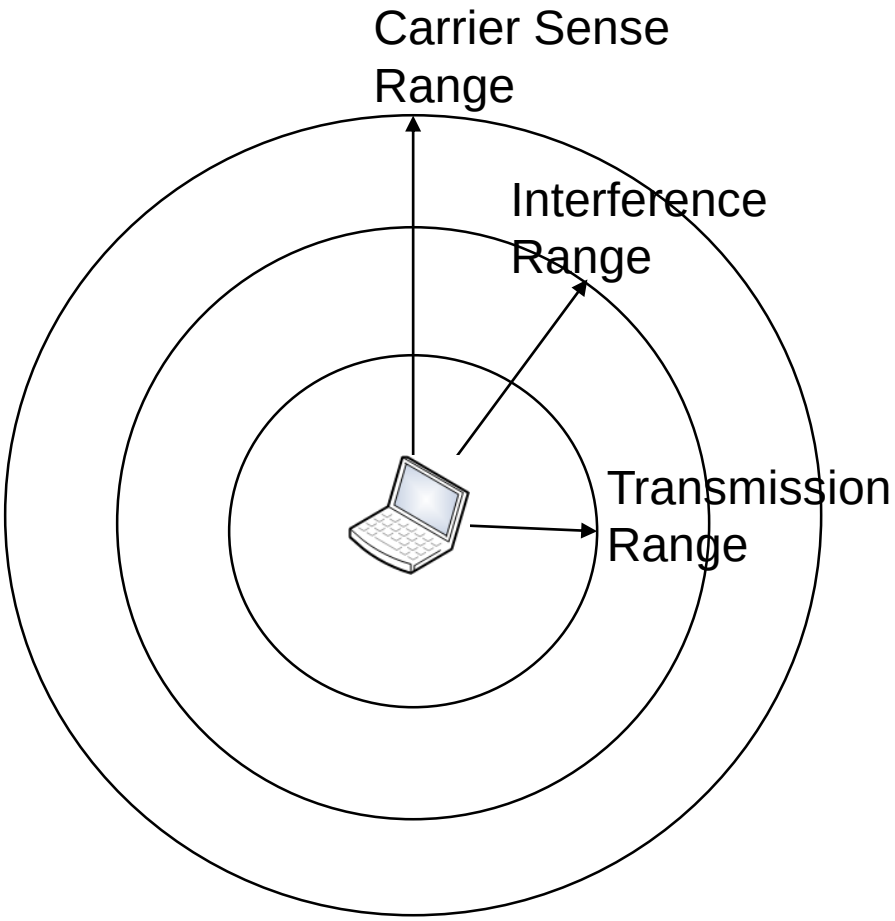


Figure 3: A low-frequency message signal (top) may be carried by an AM or FM radio wave

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



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.

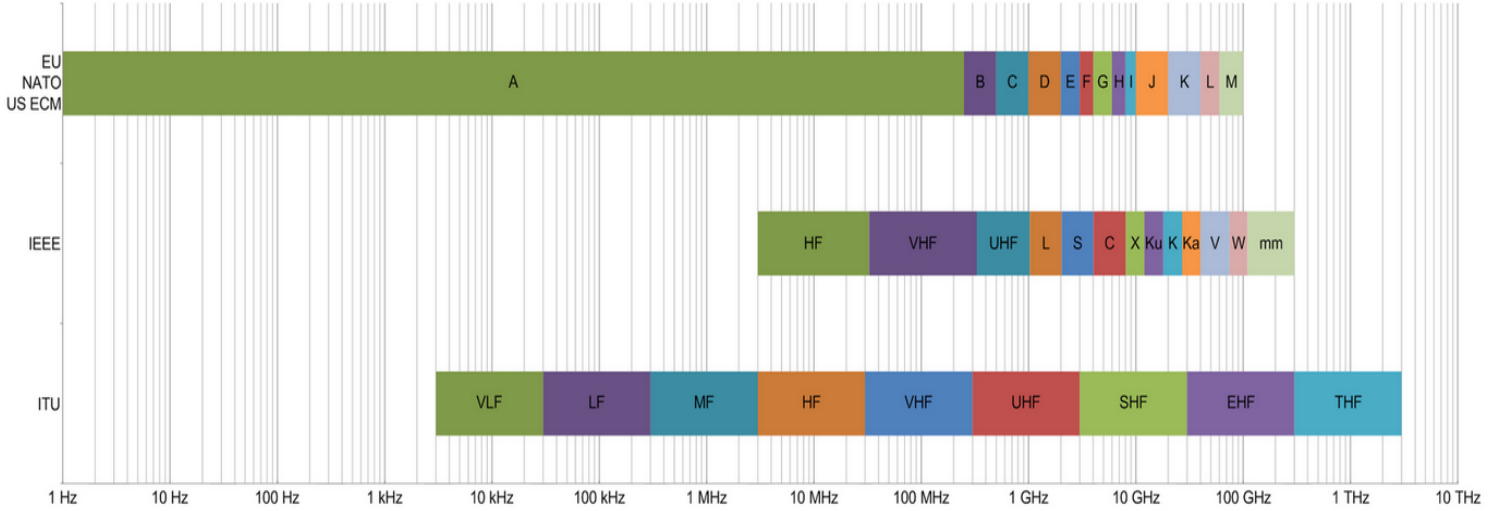


Figure 5: Frequency Band Comparison

RF Spectrum, Regulatory Bodies and Standards

Radio Frequency Spectrum

- Radio spectrum is governed and managed by policies established by Industry Canada
- Considered vital to national interest
- Applications are assigned bands of frequencies
- Rights may be sold to enterprises for sole use of a bands of frequency or spectrum.

Spectrum Chart

- https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/spectallocation-08.pdf/$FILE/spectallocation-08.pdf

Radio Frequency Spectrum

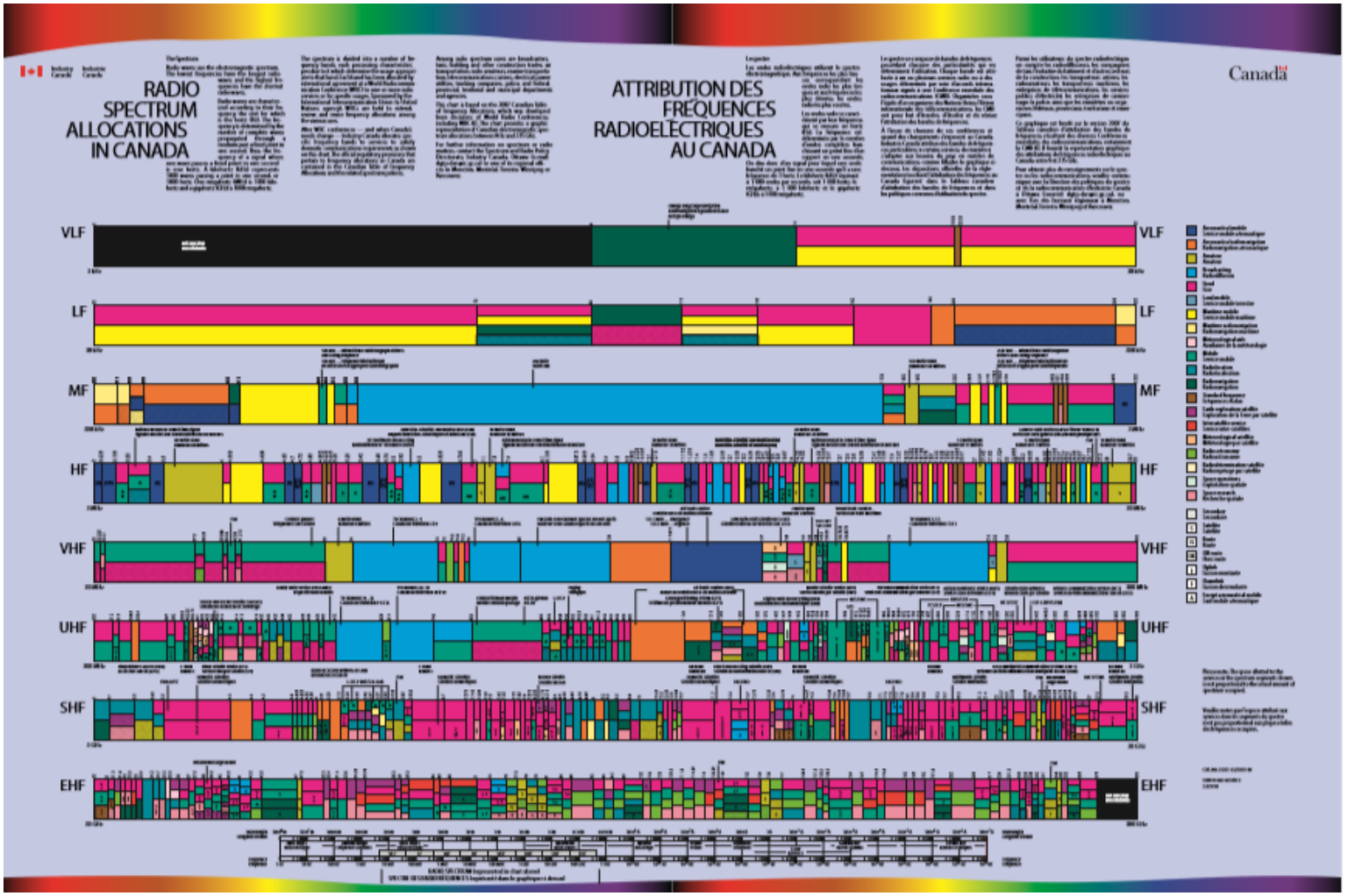


Figure 6: Radio Spectrum Allocations in Canada

Source: Industry Canada, 2006. 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.

Unlicensed Frequency Bands

- Frequency bands and coverage area typically sold by regulatory bodies of each country (e.g., cell phones)
- Industrial, scientific and medical radio bands (ISM)
  - ISM bands first established at the International Telecommunications Conference of the ITU (Atlantic City, 1947)
  - Reserved internationally for the use of radio frequency energy for ISM purposes other than telecommunications.

ISM Frequency Bands

Frequency range		Type	Center frequency	Availability	Licensed users
6.765 MHz	6.795 MHz	**A**	6.78 MHz	Subject to local acceptance	FIXED SERVICE & Mobile service
13.553 MHz	13.567 MHz	**B**	13.56 MHz	Worldwide	FIXED & Mobile services except Aeronautical mobile (R) service
26.957 MHz	27.283 MHz	**B**	27.12 MHz	Worldwide	FIXED & MOBILE SERVICE except Aeronautical mobile service
40.66 MHz	40.7 MHz	**B**	40.68 MHz	Worldwide	Fixed, Mobile services & Earth exploration-satellite service
433.05 MHz	434.79 MHz	**A**	433.92 MHz	only in Region 1, subject to local acceptance	AMATEUR SERVICE & RADIOLOCATION SERVICE, additional apply the provisions of footnote 5.280
902 MHz	928 MHz	**B**	915 MHz	Region 2 only (with some exceptions)	FIXED, Mobile except aeronautical mobile & Radiolocation service; in Region 2 additional Amateur service
2.4 GHz	2.5 GHz	**B**	2.45 GHz	Worldwide	FIXED, MOBILE, RADIOLOCATION, Amateur & Amateur-satellite service
5.725 GHz	5.875 GHz	**B**	5.8 GHz	Worldwide	FIXED-SATELLITE, RADIOLOCATION, MOBILE, Amateur & Amateur-satellite service
24 GHz	24.25 GHz	**B**	24.125 GHz	Worldwide	AMATEUR, AMATEUR-SATELLITE, RADIOLOCATION & Earth exploration-satellite service (active)
61 GHz	61.5 GHz	**A**	61.25 GHz	Subject to local acceptance	FIXED, INTER-SATELLITE, MOBILE & RADIOLOCATION SERVICE
122 GHz	123 GHz	**A**	122.5 GHz	Subject to local acceptance	EARTH EXPLORATION-SATELLITE (passive), FIXED, INTER-SATELLITE, MOBILE, SPACE RESEARCH (passive) & Amateur service
244 GHz	246 GHz	**A**	245 GHz	Subject to local acceptance	RADIOLOCATION, RADIO ASTRONOMY, Amateur & Amateur-satellite service

Type A (footnote 5.138) = frequency bands are designated for *ISM applications*. The use of these frequency bands for ISM applications shall be subject to special authorization by the administration concerned, in agreement with other administrations whose radiocommunication services might be affected. In applying this provision, administrations shall have due regard to the latest relevant ITU-R Recommendations.

Type B (footnote 5.150) = frequency bands are also designated for ISM applications. Radiocommunication services operating within these bands must accept harmful interference which may be caused by these applications.

ITU RR, Footnote 5.280 = In Germany, Austria, Bosnia and Herzegovina, Croatia, Macedonia, Liechtenstein, Montenegro, Portugal, Serbia, Slovenia and Switzerland, the band 433.05-434.79 MHz (center frequency 433.92 MHz) is designated for *ISM applications*. Radiocommunication services of these countries operating within this band must accept harmful interference which may be caused by these applications.

Figure 7: ISM Frequency Bands
Source: Wikipedia, 2018. https://en.wikipedia.org/wiki/ISM_band (CC-BY-SA 3.0)

Application of ISM Frequency Bands

- Citizen band radio (CB)
- Garage door opener and remote keyless entry systems, wireless doorbells, radio control channels for UAVs (drones), wireless surveillance systems,
- Cordless phone, Line of sight microware communication, SCADA and RFID systems for merchandise, and wild animal tracking systems
- Wifi, Bluetooth, baby monitor, Microwave Oven

Advantages & Disadvantages of ISM

Advantages	Disadvantages
• Free for commercial and consumer use	• Crowded
• Allow many different applications	• Limited bands available for use

Regulatory Organizations in Canada

- Department of Innovation, Science and Economics Canada (formerly Industry Canada)
  - Legislation

    http://laws-lois.justice.gc.ca/eng/regulations/SOR-96-484/

International Regulatory Organizations

- Japan: Ministry of Internal Affairs and Communications (MIC)
- Europe: Euro Std Org – European Telecommunications Standards Institute (ETSI)
- USA:
  - Federal Communications Commission (FCC) (https://en.wikipedia.org/wiki/Spectrum_management)

- Describe the concept of "spectrum auction"
  - Who owns the spectrum?
  - What is the maximum number of phone channels (between 61 and __)?

IEEE 802 Standard

- The IEEE 802 LAN/MAN Standards Committee, under the IEEE Computer Society, encompasses the following topics and study groups.
  - 802.1 Higher Layer LAN Protocols Working Group
  - 802.3 Ethernet Working Group
  - 802.11 Wireless LAN Working Group
  - 802.15 Wireless Personal Area Network (WPAN) Working Group
  - 802.16 Broadband Wireless Access Working Group
  - 802.18 Radio Regulatory TAG
  - 802.19 Wireless Coexistence Working Group
  - 802.21 Media Independent Handover Services Working Group
  - 802.22 Wireless Regional Area Networks
  - 802.24 Vertical Applications TAG
  - 802 5G/IMT-2020 Standing Committee

IEEE 802.11 Frequency Bands

V·T·E

802.11 network PHY standards

802.11 protocol	Release date[6]	Frequency (GHz)	Bandwidth (MHz)	Stream data rate[7] (Mbit/s)	Allowable MIMO streams	Modulation	Approximate range[citation needed] Indoor	Approximate range[citation needed] Outdoor
802.11-1997	Jun 1997	2.4	22	1, 2	N/A	DSSS, FHSS	20 m (66 ft)	100 m (330 ft)
a	Sep 1999	5	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	35 m (115 ft)	120 m (390 ft)
		3.7[A]						5,000 m (16,000 ft)[A]
b	Sep 1999	2.4	22	1, 2, 5.5, 11	N/A	DSSS	35 m (115 ft)	140 m (460 ft)
g	Jun 2003	2.4	20	6, 9, 12, 18, 24, 36, 48, 54	N/A	OFDM	38 m (125 ft)	140 m (460 ft)
n	Oct 2009	2.4/5	20	Up to 288.8[B]	4	MIMO-OFDM	70 m (230 ft)	250 m (820 ft)[8]
			40	Up to 600[B]				
ac	Dec 2013	5	20	Up to 346.8[B]	8		35 m (115 ft)[9]	
			40	Up to 800[B]				
			80	Up to 1733.2[B]				
			160	Up to 3466.8[B]				
		0.054-0.79[C]	6-8	Up to 568.9[10]	4			
ad	Dec 2012	60	2,160	Up to 6,757[11] (6.7 Gbit/s)	N/A	OFDM, single carrier, low-power single carrier	3.3 m (11 ft)[12]	
ah	Dec 2016	0.9	1-16	Up to 347 [13]	4	MIMO-OFDM		
aj	Est. Jul 2017	45/60						
ax	Est. Dec 2018	2.4/5		Up to 10.53 Gbit/s		MIMO-OFDM		
ay	Est. Nov 2019	60	8000	Up to 20,000 (20 Gbit/s) [14]	4	OFDM, single carrier,	10 m (33 ft)	100 m (328 ft)
az	Est. Mar 2021	60						
802.11 Standard rollups								
802.11-2007	Mar 2007	2.4, 5		Up to 54		DSSS, OFDM		
802.11-2012	Mar 2012	2.4, 5		Up to 150[B]		DSSS, OFDM		
802.11-2016	Dec 2016	2.4, 5, 60		Up to 866.7 or 6,757[B]		DSSS, OFDM		

- A1 A2 IEEE 802.11y-2008 extended operation of 802.11a to the licensed 3.7 GHz band. Increased power limits allow a range up to 5,000 m. As of 2009, it is only being licensed in the United States by the FCC.
- B1 B2 B3 B4 B5 B6 Based on short guard interval; standard guard interval is ~10% slower. Rates vary widely based on distance, obstructions, and interference.
- C1 IEEE 802.11af about using white space spectrum for WiFi based on the PHY layer of 802.11ac

Figure 8: IEEE 802.11 Frequency Bands
Source: Wikipedia, 2018. https://en.wikipedia.org/wiki/IEEE_802.11 (CC-BY-SA 3.0)

802.3 vs. 802.11 Technologies

- 802.3 wired
  https://en.wikipedia.org/wiki/IEEE_802.3

- 802.11
  https://en.wikipedia.org/wiki/IEEE_802.11

Evolution of 802.11 Technology

Protocol	Date	Data Rate (Mb/s)	Freq (GHz)	Distance (m) (Indoor/Outdoor)
802.11	1997	2	2.4	20/100
802.11a	1999	6-54	3.7/5	35/15000
802.11b	1999	1-11	2.4	35/140
802.11g	2003	6-54	2.4	38/140
802.11n	2009	Up to 600	2.4/5	70/250
Multi 802.11ac, ad,	2013-2017	Up to 6700	2.4-60	3.3-35/-
802.11ah, aj, ax, ay, az	2017-2021	Up to 20000	2.4-60	10/100

802.3 vs. 802.11 Technologies

Protocol	Date	Data Rate (Mb/s)	Medium	Distance (m)
802.3exp	1972	2	Coax	30
802.3	1983	10	Coax	30
802.3u	1995	100	UTP	100
802.3ab	1998	1000	UTP	100
802.3ae	2002	10000	Fiber	100
802.3an	2006	10000	STP	10
802.3ba	2010	40000	UTP	10
802.3bj	2014	100000	Twinax	5
802.3bs	2017	200000	Fiber	
802.3cd	2018	200000	UTP	

References

Industry Canada. (n.d.) Radio spectrum allocations in Canada. Retrieved from https://www.ic.gc.ca/eic/site/smt-gst.nsf/vwapj/spectallocation-08.pdf/$FILE/spectallocation-08.pdf

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