Setup

September 11, 2023 10:07 AM

VLAN 40 - Routing - used for the connection between firewall and layer 3 switch

on firewalls

- by default the firewall has an implicit DENY all rule
- be as restrictive as possible, open when necessary
- set a static route from L3 (routing) to firewall
- firewall needs a route back to the L3 (subnet the whole LAN)
- H-A ports are high availability for connecting 2 firewalls together
  - active-active - both firewalls are acting as primary firewall (not great at load-sharing)
  - active-passive - one firewall acts as primary and the other acts as a standby backup

  backup:
  admin - manual configuration - backup (global will take everything as one file, VDOM is by VDOM)

SDNS - secure DNS uses TCP port 53 rather than normal UDP that uses UDP port 53

Wireless History, Standards, and Protocols

September 13, 2023 1:11 PM

IEEE 802.11 - original wireless standard

Wireless Advantages:

- mobility
- access to network in more areas (public spaces, remote areas)
- connectivity to an organizations infrastructure - point to point antennas (think LTT)
- deployment - network cabling could be difficult / super costly in some places

Wireless Disadvantages:

- security - broadcasting in open air, unauthorized users could get in, rogue APs
- Radio signal interference
- coverage range - low quality for long distances
- slow speed compared to wired

Wireless: all types of devices and tech not connected by wire
Wireless Communications: transmission of digital data without using wires

Wireless Tech used today

- Bluetooth

- low-power, short range wireless data and voice transmissions

- WirelessHD - high frequency

- proprietary standard, used for wireless transmission of HD video and audio on ultra wide band
- theoretically 25Gbps

- Satellite - using satellites

- transmit data over long distance

- Cellular - using cell towers

- High-speed, high-capacity voice and data communication network
- used for cell phones, also used for internet access, or WAN failover

- Fixed broadband wireless communications

- point to point antennas that broadcast signals long distance

- Wi-Fi based wireless LANs

- extension of a wired LAN, connected via wireless AP
- Access Point - network device that allows other wi-fi devices to connect to a wired network
- Wireless network interface card (NIC) - has an antenna built in
- Enterprise WLAN - designed for better security, performance, centralized management/config, and user experience

Standards Organizations
The International Telecommunication Union Radio Communication Sector (ITU-R)

- responsible for **global** management of radio frequency spectrum
- work with regional/local entities (like the Federal Communications Commission or FCC in USA)

Most countries have their own orgs that are like the FCC that regulate **licensed and unlicensed spectrum**.

- Industry Canada regulates the wireless LAN devices use of the RF spectrum in Canada
- There are 5 regions (A-E)

★ **The International Organization for Standardization (ISO)**

- created the OSI model for data communications

★ **The Institute of Electrical and Electronics Engineers (IEEE)**

- creates standards for compatibility and coexistence between networking equipment
- these standards are written documents describing how technical processes and equipment should function
- IEEE 802.11 defines communication mechanisms only at the **Physical layer & MAC sublayer of OSI**

The Internet Engineering Task Force (IEFT)

- responsible for creating internet standards, lots of them are integrated into the wireless networking and security protocols and standards.

★ **The Wi-Fi Alliance**

- responsible for performing certification testing on wireless equipment
- they do the testing and give devices the stamp of approval (they are the WIFI symbol)

Radio Frequency and Antennas Fundamentals

September 19, 2023 10:09 AM

Electromagnetic Spectrum

- the range of all possible electromagnetic radiation, waves that go through matter or space
- radio waves are on the low frequency end so they go farther than x-rays (high frequency) for example

Low Frequency = Long Wavelength

(inverse relationship)

High Frequency = Short Wavelength

What is a radio frequency signal?

- an RF signal starts out as an electrical alternating current (AC) signal generated by a **transmitter**
- sent through copper conductor
- radiated out of an antenna element in form of electromagnetic wave

this is how a wireless signal is made ^

- an antenna is a **transducer** that converts wired electrical signal to EM radiation (and vice versa)

Radio Signal Characteristics z

High-Frequency signals generally attenuate faster than low-frequency signals as they go through walls and other objects.

wavelength

- distance of one cycle of the signal, or distance between two peaks or two valleys in a wave
- measured in meters or centimeters, symbol that it uses is the **lambda**
- dictates optimum size of receiving antenna

frequency

- the number of times per second a signal oscillates
- measured in hertz (Hz) - 1 cycle per second
- signals that oscillate at different frequencies are less likely to interfere with each other
- in WLAN this is done by using slightly different frequencies in different channels

antenna are manufactured to be equal to or a multiple of, a full, half, or quarter wavelength of the signal they are to operate on.

amplitude

- how high/low the wave goes
- more amplitude means more strength
- to increase the amplitude you increase the output power of the transmitter
- more amplitude makes an RF wave easier to detect than one with less, it also increases the RF wave's range.

phase

- the relationship between at least two signals that share the same frequency but different starting points
- two signals that have the same peaks and valleys are **in phase**
- if they don't match they are **out of phase**
- if they are exactly opposite, the first is **in phase** and the second is **180 degrees out of phase**
- in phase is ideal (I believe?)

Radio Frequency Behaviors

RF signal does not just go straight out in a single path to a receiver.

- usually it is many copies of the signal that will reach the receiver (known as multipath)
- signal may bounce off of walls and other objects
- this is called **wave propagation**: how the signal travels

RF signals have behaviors that can be predicted and detected,

Major RF signal behaviors:

gain - amplification of an RF signal (measured in DB)

loss - reduction in signal strength (amplitude)

reflection, refraction, diffraction, scattering - RF propagation behaviours causing RF to travel in a different direction

Radio Antennas Concept:

what is an antenna?

Conductor: a material that allows electrical current to flow through it

Antenna: passive conductor used to transmit EM waves through space

- relies on power source attached
- convert electrical energy into RF waves in the case of **transmitting**
- convert RF waves into electrical energy in the case of **receiving**
- length is directly correlated with frequency that an antenna can transmit or receive propagated waves

Properties of an Antenna

gain: measure of power (in dBi) - the effectiveness of the antenna compared to an isotropic radiator

- isotropic antenna - has a radiation pattern of a perfect sphere (doesn't exist IRL, just theoretical)

active gain: using an amplifier on the wire between transceiver and antenna to increase the inbound and outbound AC voltage - does not change shape of coverage area

passive gain: does not need extra power source; focusing RF signal more powerfully in one direction

beamwidth: - how broad or narrow the focus of an antenna is - measured both horizontally and vertically

- high gain = narrower beamwidth (less chance of interference)
- low gain = broader beamwidth (higher chance of interference)

polarization: orientation of EM wave, direction of oscillation in these waves

Antenna Types:

omni-directional

- most common was dipole antenna (had 2 poles)
- radiated in a sphere-ish shape
- best for being in the center and expanding to an area
- high-gain can be used for connecting buildings

multiple-input multiple-output (MIMO)

- uses multiple antennas with multipath
- combines incoming signals to make them stronger
- **spatial diversity:** MIMO technique that sends the same signal out of multiple antennas - can increase reliability of signal - unlikely that all signals degrade in the same way
- when sensing an RF signal it compares the signal that it is receiving and takes the better one
- **spatial multiplexing:** splits up data and sends different data out of multiple antennas - increases speed without power or bandwidth

semi-directional antennas:

- designed to direct signal in a specific directional
- used for short-to-medium distance
- common for being the network bridge between two buildings in a campus
- examples: patch, panel, yagi

highly-directional:

- emit the narrowest beamwidth

- common types: parabolic dish antenna, grid antenna
- ideal for long-distance point-to-point communications
- coverage may be greater than 50km
- the higher the gain the more precise the aim needs to be

Radio Frequency Math

September 26, 2023 10:07 AM

Why RF Math:

- required to determine whether your RF link is compliant with power limitations set by regulatory bodies (ISED/FCC)
- each rf component affects the output of the transceiver

Components of RF communications:

- transmitter
- intentional radiator (IR)
- equivalent isotropically radiated power (EIRP)
- antenna
- receiver
- isotropic radiator

transmitter:

- initial component in creation of wireless medium
- begins generating AC signal
- AC signal determines frequency of transmission and oscillates accordingly
- takes data and modifies the AC signal using modulation to encode data into signal
- sends modulated signal to antenna directly or through a cable

intentional radiator (IR):

- device specifically designed to generate and radiate RF signals
- includes all hardware from the transmitter up to **but not including** the antenna - (RF device [transmitter/receiver], cabling, connectors)
- FCC/ISED limit the amount of power that is allowed to be generated by the IR

antenna:

- collects modulated AC signal from the transmitter
- directs/radiates RF waves away from the antenna in a pattern specific to the antenna type
- captures the RF waves
- passes the AC signal to the receiver, which converts AC to bits and bytes

- as a reference, RF transmission of an antenna is compared to an isotropic radiator (perfect antenna)

receiver:

- final component in wireless signaling
- converts carrier signal from antenna into 1's and 0's
- receive amplitude (strength) is weaker than transmit amplitude

Basic RF Math:

equivalent isotropically radiated power (EIRP) - the power radiated by the antenna element

- what is regulated by ISED in Canada and FCC in US
- they define maximum power output for IR and maximum EIRP that radiates from antenna
- transmit power of most indoor WLAN radios varies in a range between 1mW and 100mW
- transmit power of 4 watts is allowed to be radiated from an antenna in a point to multipoint application (outside)

RF units of power and units of comparison

units of power (absolute) - used to measure transmission and received amplitude

- **Watts (W) - 1A*1V (one amp at one volt)**
- **Milliwatts (mW) - 1/1000 of a watt | 1mW=0.001W**

most 802.11 devices use between 1mW-100mW

APs are generally 30-100mW

- **decibels relative to 1 milliwatt (dBm)**

units of comparison (relative) - often used to measure how much gain or loss occurs because of cabling or antennas, or a difference in power.

- **decibel (dB) - specifically designed to measure power gain or loss | 1dB = 1/10 of a bell**

often used to compare power to 2 transmitter or more, or difference/loss between EIRP output of a transmitter's antenna and amount of power received by receiver's antenna

- **decibels relative to an isotropic radiator (dBi)**
- **decibels relative to a half-wave dipole antenna (dBd)**

Calculating gain and loss:

- rules of 10s and 3s (dBm and mW)

3 dB of gain (relative) = 2x the absolute power (mW)

3 dB of loss (relative) = /2 the absolute power (mW)

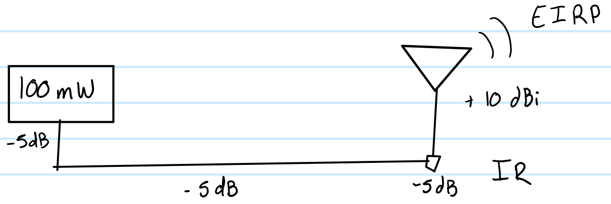
10 dB of gain (relative) = 10x the absolute power (mW)

10 dB of loss (relative) = /10 the absolute power (mW)

ICA 3

September 26, 2023 1:27 PM

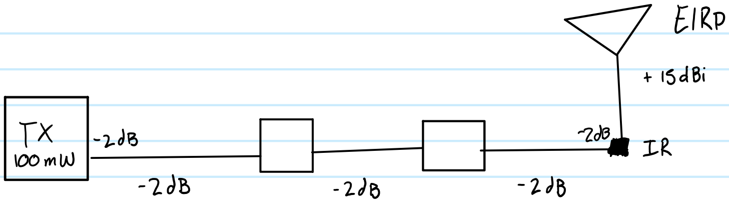
Q5



10 dBm	10 mW	
20 dBm	100 mW	
5 dBm	3.2mW	IR
15 dBm	32mW	EIRP

3 dBm	2 mW
6 dBm	4 mW
9 dBm	8 mW
12 dBm	16 mW
15dBm	32mW
5dBm	3.2mW

Q6



10dBm	10mW	
20dBm	100mW	
10dBm	10mW	IR

	10dBm	10mW	
	13dBm	20mW	
	16dBm	40mW	
+15dB	19dBm	80mW	
	22dBm	160mW	
	25dBm	320mW	EIRP

Study for unit 1 exam

October 3, 2023 7:42 PM

What is the role of IEEE & WiFi Alliance in WLANS?

IEEE acts as the standard maker for all 802.11 standards,
Wifi alliance acts as the checker to make sure products follow IEEE standards

Terminology

passive gain:

creating a stronger signal by narrowing the beamwidth and FOCUSing RF signal

active gain:

amplifying a signal by increasing the transmitter's output power
↳ done by increasing AC voltage

loss:

a decrease in signal strength, usually through interference from objects

IR:

Intentional Radiator - the parts of a transceiver before the antenna.
→ cabling, connections | it is what radiates RF signal to the antenna.

EIRP:

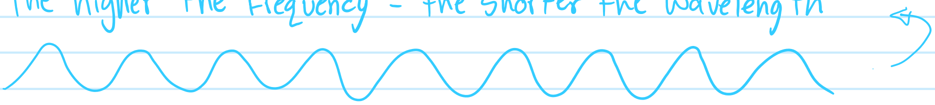
equivalent isotropically radiated power - the power sent out by the antenna

Isotropic Radiator:

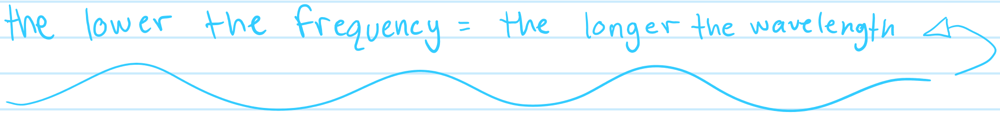
a "Perfect antenna" - the theoretical antenna used for calculations
↳ radiates in a perfect sphere

Relationship between Wavelength & Frequency

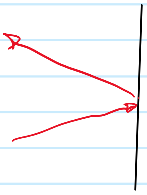
the higher the Frequency = the shorter the wavelength



the lower the frequency = the longer the wavelength



RF Behaviors

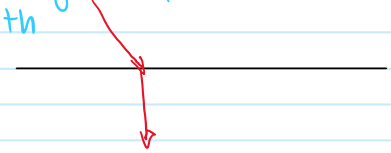


reflection

when RF signal bounces off of an object

refraction

when RF signal comes into an object w/ a different angle than it leaves with



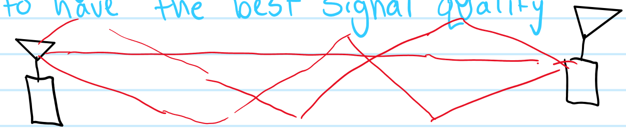
absorption

when RF signal gets absorbed / lost in an object that absorption

when RF signal gets absorbed / lost in an object that is in its path

multipath

sending out multiple RF signals @ the same time in order to have the best signal quality



MIMO - multiple - input multiple-output

a device that uses multiple receivers along with multipath
- can select stronger signal - spatial diversity
- or combine multiple signals - spatial multiplexing

MU-MIMO - multiple user multiple-input multiple-output

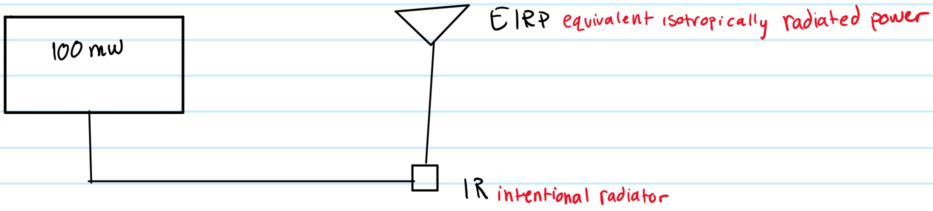
a mimo device that allows multiple users to be using it at the same time.

Calculating power

	dBm	mW
+	3	x 2
+	10	x 10
-	3	÷ 2
-	10	÷ 10

ex.

	dBm	mW	
+3	0	1	x2
+3	3	2	x2
+3	6	4	x2
+10	9	8	x10
	19	80	



Wireless LAN topologies and architecture

October 11, 2023 1:09 PM

wireless topology - the physical and logical layout of wireless hardware

4 major wireless topologies:

- wireless wide area network (WWAN)

ex. EDUROAM - uses RADIUS

- wireless metropolitan area network (WMAN)

ex. New York City / Edmonton Rec Centers

- wireless personal area network (WPAN)

ex. Bluetooth, peer-to-peer (ad hoc)

- wireless local area network (WLAN)

ex. home Wi-Fi

components of WLAN:
main component is **radio**, or the **station service (STA)**

- **client station** - non-AP station (tablet, phone, laptop, etc.)
- when a client station establishes a layer two connection with an AP, they are **associated**

- **access point station** - radio that functions as the wireless portal from which other client stations can communicate
- the AP manages client associations - maintains an **association table** of connected WLAN clients and **directs traffic**

AP acts as a bridge from wireless to wired, or wireless to wireless

- all devices that are associated with an 802.11 WLAN are part of a **service set**
- **service set identifier (SSID)** is a logical name used to identify a wireless network
- 32 characters, is case sensitive

802.11-2016 standard defines 4 topologies (SERVICE SETS)

- basic service set (BSS) - 1 WLAN - 1 unique SSID and 1 unique BSSID

a group of wireless devices served by a single AP

- basic service set identifier (BSSID) - media access control (MAC) address of AP | BSSIDs are incremental off the original MAC address of the AP's radio

- **basic service area (BSA)** - physical area of coverage provided by an AP in a BSS

- extended service set (ESS)

group of two or more identically configured BSS networks, connected via common distribution system
typically multiple APs and their associated clients
extended service area is coverage area of the ESS in which all clients can communicate and roam

- independent basic service set (IBSS)

a group of two or more clients that communicate without an AP (ad hoc or peer-to-peer)
when no connection to internet or external network is needed
for IBSS to work all stations must be transmitting on the same frequency channel, share the same SSID

- mesh basic service set (MBSS)

mesh topology where wired network access is not possible
used to provide wireless distribution of network traffic between a set of APs (bridging traffic)
mesh APs usually have multiple radios - one for traffic of network, the other to maintain BSS for wireless clients
one or more APs are connected to a wired infrastructure **- mesh portals (gateways)**
APs not connected to the upstream wired infrastructure are called **mesh points**

WLAN Architecture:

Autonomous WLAN Architecture

- most common with a "standalone" AP | AKA **autonomous access points or fat access points**
- all configs are in the AP itself
- at **least** two physical interfaces, PLUS one for management
- RF radio, ethernet port, BVI (bridge between the two, for management)
- typically POE and deployed at access layer

Centralized WLAN Architecture

- requires **wireless controller** - this allows you to manage and configure APs | AKA **lightweight APs or thin APs**
- lightweight APs do not contain the management and configuration functions
- WLC can be centrally configured, settings auto distributed to all APs | can be placed at the core, distribution, or access la yer

- wireless controller features:
- AP Management
- WLAN Management
- User Management
- Device Monitoring
- VLANs
- Layer 2 security support
- Captive portal - have to sign in on a website before data can flow

Controller Data-Forwarding Models:

- centralized data forwarding

where all data is forwarded from AP to the WLAN controller for processing.
usually used, especially when WLAN controller manages encryption / QOS

- distributed data forwarding

where AP performs data forwarding locally
maybe used where it is better to perform forwarding at the edge, rather than the central server

Wireless Security

October 31, 2023 10:09 AM

The main function of an 802.11 WLAN is to provide a portal into a wired network.

- if this portal is not protected, unauthorized users could gain access which can lead up to many different wireless attacks.

Wireless Attacks

Rogue Wireless Devices

- potential open and unsecured portal into network infrastructure
- usually installed by employee who didn't realize what they did
- ad hoc wireless can also provide access

Peer-to-peer attacks

- 802.11 client stations can be configured as infrastructure mode or ad hoc mode (peer-to-peer)
- people hacking users that are associated to the same access point

Eavesdropping

- casual or malicious
- casual eavesdropping is finding open WLAN networks and discovering layer 2 information about the WLAN
    - this can be through passive scanning - where the client radio listens for AP beacons
    - or through active scanning - where the client radio transmits probe requests
- malicious eavesdropping is using protocol analyzers to capture wireless communications, this is typically considered illegal
- if there is no encryption, cleartext communications can be captured. layer 3-7 can be captured if WPA2 (or better) is not in place.
- unencrypted 802.11 frames can be reassembled at the upper layers (VoIP can be turned to a WAV file for example.)

Encryption Cracking

- WEP (wired equivalent privacy) is an old 802.11 encryption method that has been cracked for a while.

- WPA (Wi-Fi protected access) replaced WEP, still vulnerable today as it was based on WEP - introduced TKIP (temporary key integrity protocol) and MIC (message integrity check)

- WPA2 (Wi-Fi protected access 2) provides stronger data protection and network access control, replaced WPA in 2004. Introduction of AES (2 types): **WPA2 - Personal** - (implements PSK) - still weak and susceptible to dictionary attack & **WPA2 - Enterprise** (implements RADIUS) - based on 802.1x

- WPA3 (wi-fi protected access 3) latest wireless security protocol - adds new features for WPA3 Personal. Mandatory certification for Wi-Fi certified devices.
    - **WPA3 Personal** - enhances security through replacing the PSK with simultaneous authentication of equals (SAE). Key is generated with each authentication - 128 bit encryption plus forward secrecy (PFS) - prevents compromising session keys.
    - **WPA3 Enterprise** - requires a server certificate validation for confirming the identity of the server to which the device is connecting

Wireless Hijacking (evil twin attack)

- hacker makes a device that pretends to be an AP in a WLAN.
- AP uses the same SSID and users can connect to it.

Social Engineering Attacks

- talking to people and either getting their password from the things they say or from phishing or something

Wireless intrusion monitoring

Wireless Intrusion Prevention System (WIPS)

- software/hardware that is a central point of monitoring security and performance data collection
- sensors can use 802.11 radios to collect information in securing analyzing WLAN traffic
- most vendors have fully integrated WIPS capabilities

Wireless Network Security Architecture

at least 5 major components should be covered when securing a wireless 802.11 network:

- **Data privacy and integrity** - using strong encryption
- **AAA (authentication, authorization, accounting)**
    - ★ authentication - verifying identity credentials
    - authorization - determines if they are allowed to have access to the resources
    - accounting - tracking the use of network resources by users and devices
- ★ **traffic segmentation** - separating user traffic within a network
- **monitoring** - watching the network
- **policies** - making sure the users are following the rules and not doing things that are not allowed

MDM - mobile device management - system used for onboarding personal mobile devices or company-issued ones, also monitors and secures them-
company mobile device - purchased by the company with the intent of enhancing employee performance - in-depth security and monitoring since they have corp info on them
personal device - your own device that requires a different method of management

Guest WLAN access - separate SSID used for guests so they don't have to go through your network and possibly have access to sensitive information

- firewall is important here - prevents them from getting near company network
- captive portals - making a guest sign in before having access to the internet
  - one of the most important things is telling them the appropriate use of the network
- client isolation is important so guest WLAN users can't do peer-to-peer attacks
- often have bandwidth reserved for employees

Wireless Security Policies

Remote-Access WLAN policy - used for when users take their devices off site

- should include the required use of IPsec or SSL VPN solutions & user authentication, strong encryption

Rogue AP Policy - no one should be able to install their own wireless devices on the corp network, or set up ad hoc / peer-to-peer networks

WLAN Proper Usage Policy - should outline the proper use and implementation of the main corp wireless network