ICT SKILLING FOR SCHOOLS

Wireless Networks

By
Nicholas Mugambe
nmugambe@renu.ac.ug
cnimusiima@renu.ac.ug

Outline

May, 2024

Summary

- Introduction
- Wireless networks (Overview)
- Wireless LAN Deployyment
- Troubleshooting
- Lab

Introduction

- As Internet usage increases, users expect reliable access **anytime, anywhere**
- Wired networks offer the basis of user connectivity but are constrained to;
  - **Limited Mobility** – Connected devices are tethered to their physical location
  - **Limited Flexibility and Scalability**- Hard to adapt to changing needs and layouts

How are these challenges addressed?

Wireless Networks

- A wireless network is any type of computer network that uses wireless data connections for connecting network nodes.
- Wireless networks offer;
  - Improved mobility
  - Improved scalability and flexibility

Wireless Networks Terminologies

- Access Point (**AP**)
  - A wireless device that allows wireless-capable devices to connect to a wired network.
- **Wireless Clients**
  - Devices, like laptops, smartphones, that connect to a wireless network
- **SSID** (**S**ervice **S**et **I**dentifier)
  - The "Network Name" Often human readable.

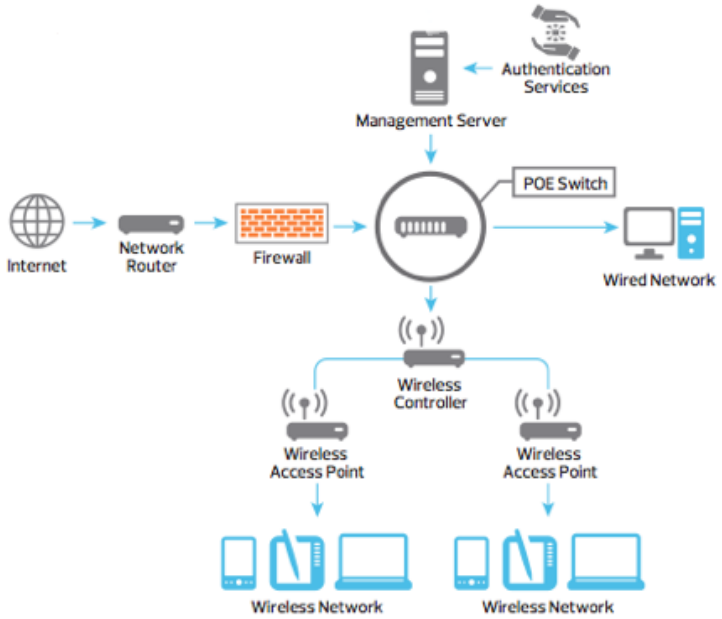
SSID choice has an impact on Roaming

Wireless Networks Terminologies

- **dBm** (decibel milliwatt)
  - Wi-Fi signal strength is measured in dBm. It is provided as a negative value
- **Interference**
  - Disruption of wireless signals caused by overlapping frequencies, physical obstructions, or other electronic devices.

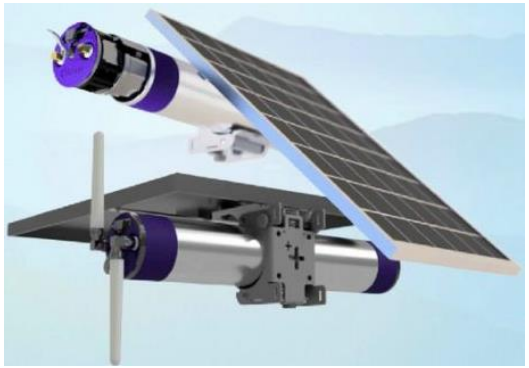
Key Components of a Wireless Network

- Access Point (**AP**)
- Wireless Client devices
- Antenna
- Authentication server
- Wireless Controller



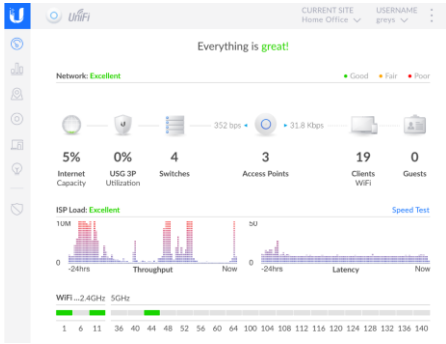
Access Points

- Indoor APs
- Outdoor APs



Wireless Controllers

- Vendor specific
- They can be;
  - **Software-based** (Installed on a physical or Virtual Machine)
  - **Hardware-based**



Wi-Fi

- Wi-Fi is a trademark for an alliance (not a **technical term**)
- Wi-Fi is used to refer to **802.11** family of wireless standards

What are the WiFi Standards?

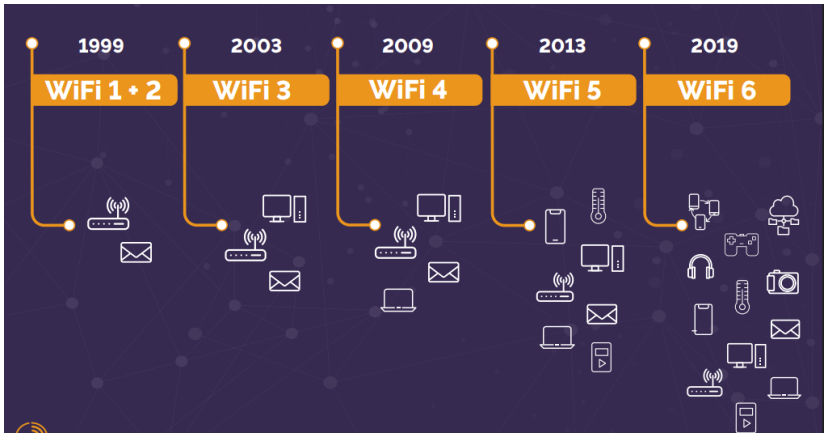
Why do we need standards for WiFi?

Wi-Fi Standards

- Rules and protocols that govern how wireless networks operate
- Developed by **IEEE** and have evolved overtime.
- Ensure compatibility and performance between devices

Wi-Fi Standards

- WiFi standards have evolved to increase;
  - Speed and throughput
  - Range
  - Overall network efficiency



WiFi Standards

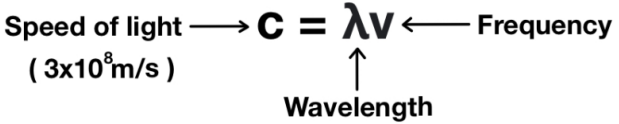
Standard	Frequency (GHz)	Data rate (Mbps)
802.11b (WiFi 1)	2.4	11
802.11a (WiFi 2)	5	54
802.11g (WiFi 3)	2.4	54
802.11n (WiFi 4)	2.4 and 5	300-600
802.11ac (WiFi 5)	5	3500
802.11ax (WiFi 6)	2.4 and 5	9600

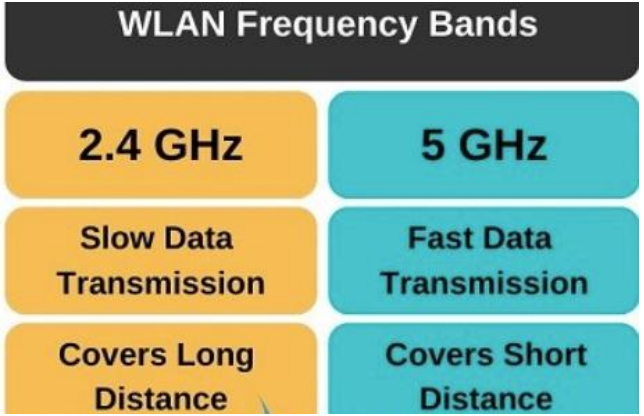
WiFi 7 is predicted to reach a maximum speed of up to **46 Gbps**

2.4 GHz and 5 GHz**?** What is the role frequency?

Frequency Bands

- Frequencies in wireless networks determine;
  - **Coverage and Range**
    - Lower frequencies have a better range and can easily penetrate compared to higher frequencies
  - **Bandwidth**
    - Higher frequencies offer more bandwidth compared to lower frequencies





Roaming

- What happens when wireless clients move:
  - From one AP to another, in the same building?
  - From one building to another?
  - To a different part of campus, or a remote campus
- Is it important to stay on the network, without interruption (for example, to have a video call?
- Is it acceptable to log on again when entering a new network zone?

Wireless Roaming

- Ability of a wireless device to seamlessly switch between different APs within the same network.
- Avoids Interruption
- Avoids re-authentication

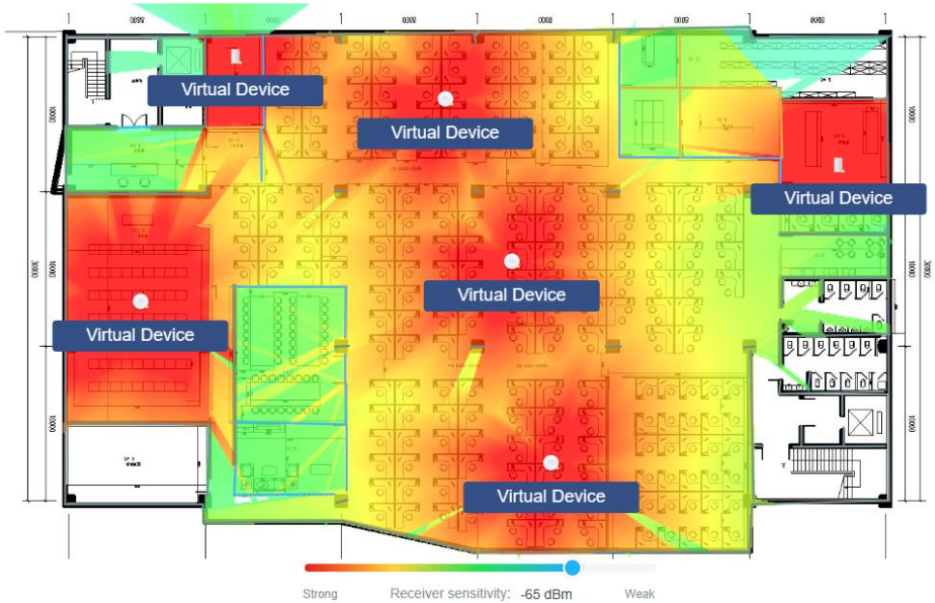
Wireless LAN Deployment

Wireless Network Planning

- **Planning is required;** needed to solve new problems wireless brings
  - Frequency monitoring & management
  - Reach & Power planning: Link budgets, Antennas
  - SSID planning: Names matter!
  - Rogue activity monitoring and management
  - Plan Subnet Sizes
    - Tradeoff between roaming ease & network scalability

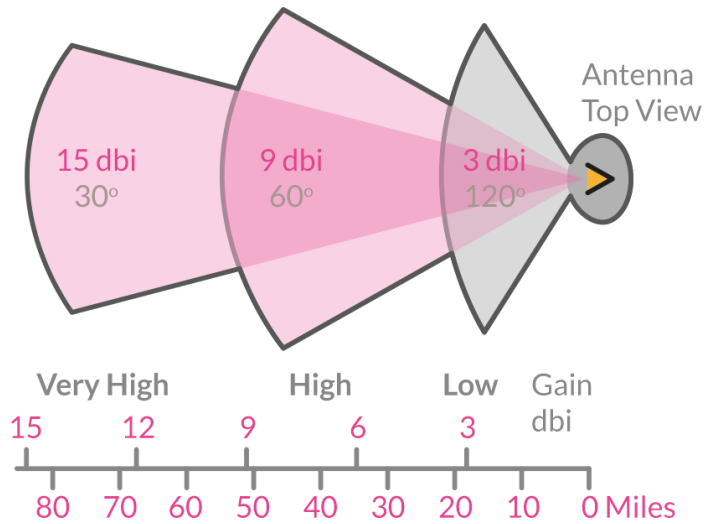
Wireless Network Planning - Tools

- Vendors offer free proprietary design platforms to aid your WLAN planning
  - Unifi Design Center
  - TP-Link Omada Heat Map
  - Cambium Wi-Fi Designer
  - Netspot
    - Limited full feature access
    - Multivendor support



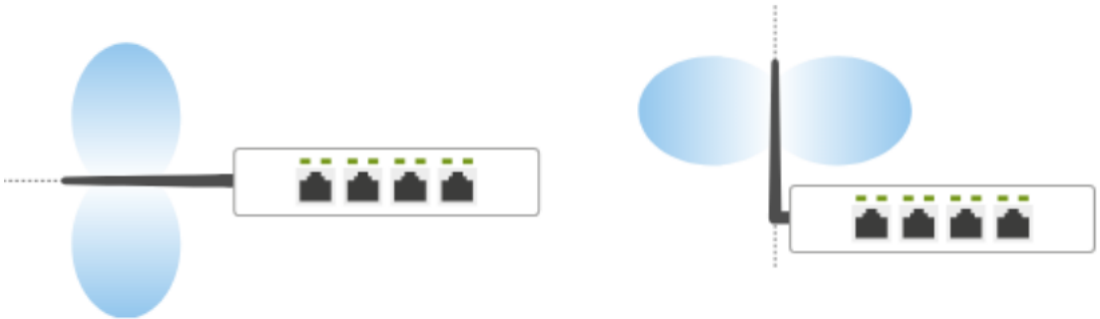
Choosing a wireless access point

- Cloud Management
  - Unifi, TP-Link Omada, D-Link, Cambium, etc
- Wi-Fi Technology
  - MIMO, MESH, PoE, Beam forming
- Antenna Gain
  - The higher the better for long range coverage
- Antenna Type
  - Directional Vs Omni directional antennas
- Speed
- Number of simultaneous connections supported



Wireless AP Placement

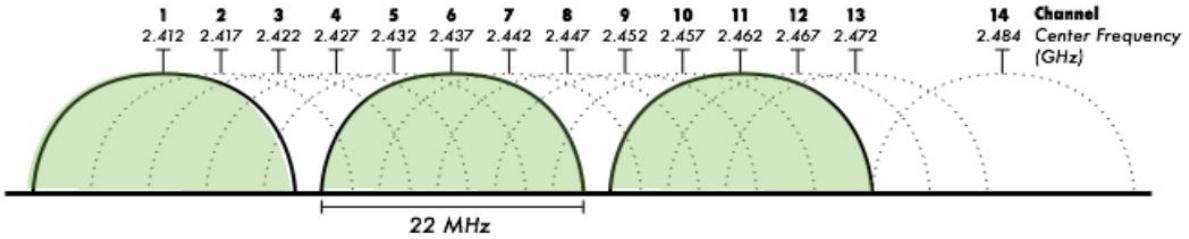
- Access point mounting and location are critical for effective Wi-Fi coverage
- Based on the antenna radiation pattern
- Indoor AP Ceiling mounting vs Wall Mounting



Omni Directional Antenna Radiation Patterns

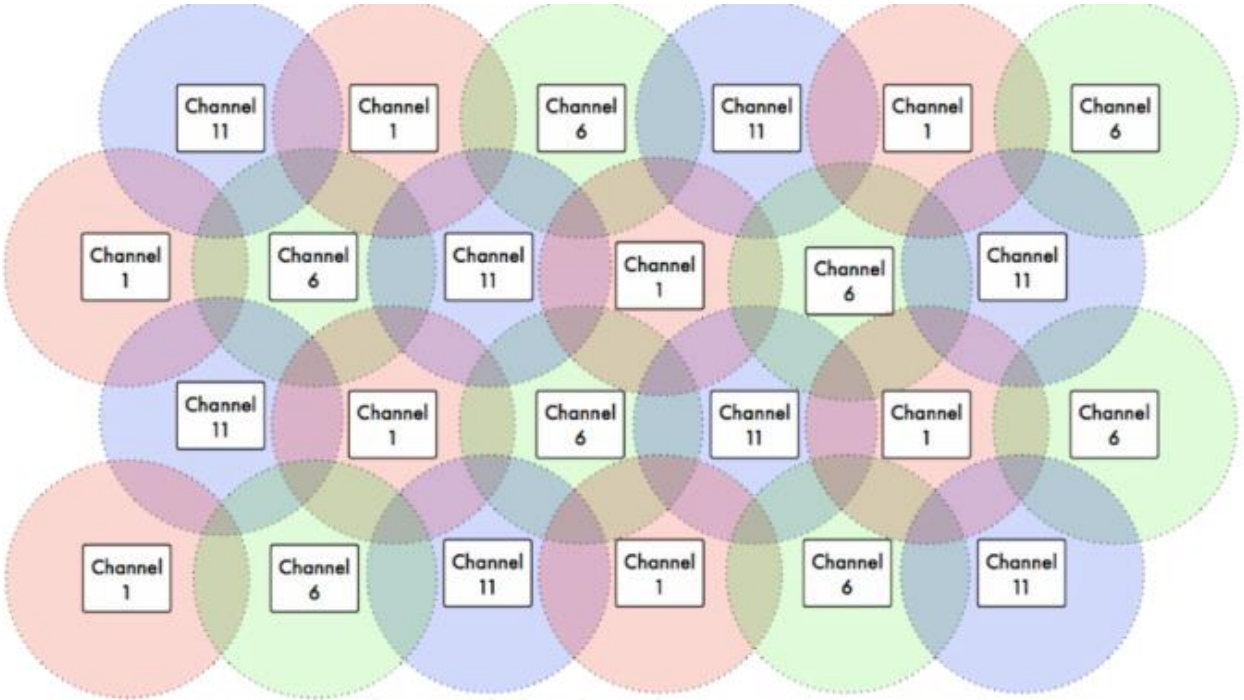
Channel Selection & Optimization

- A physical survey give insights on the available channels with in a specific deployment area.
- Fixed channel optimization Vs Dynamic controller channel optimization
- 2.4GHz band non overlapping channels 1, 6, 11, 14



Channel Selection & Optimization – Cont'd

- Three channel coverage design



Channel Selection & Optimization – Cont'd

- 5Ghz band has 25 non over lapping channels
  - U-NII-1: 5170-5250 has 4 of 20 MHz each
    - 36 ,40, 44, 48
  - U-NII-2A: 5250-5330 has 4 of 20 MHz each
    - 52, 56, 60, 64
  - U-NII-2C: 5490-5730 has 12 of 20 MHz each
    - 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144
  - U-NII-3: 5735-5835 has 5 of 20 MHz each
    - 149, 153, 157, 161, 165

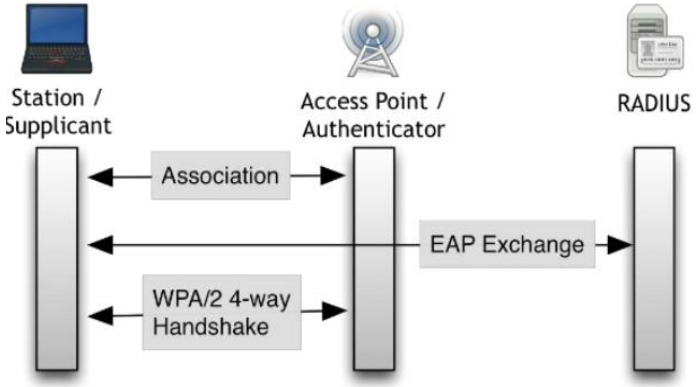
Wireless at Layer 3

- Wi-Fi Routers do many things
  - Routing, NAT, Firewall, DHCP
  - These are Layer 3 functions!
- Keep Layer 3 functions in the wired core
  - You cannot scale a network with Wi-Fi Routers
- An Access Point simply bridges networks
  - This is a layer 2 function: 802.3 <-> 802.11
  - Scalable networks use Access Points, not Wi-Fi Routers

Wireless Router

Wireless Network Authentication

- Authentication can be implemented in many ways:
  - MAC Address Restrictions
  - Pre-Shared Key based Authentication
    - WPA-PSK – insecure, not scalable
  - Captive Portal Authentication
    - Better than a pre-shared key, but not the ideal
  - 802.1x/WPA2 Enterprise Authentication = Ideal!
    - Performed on centralized servers

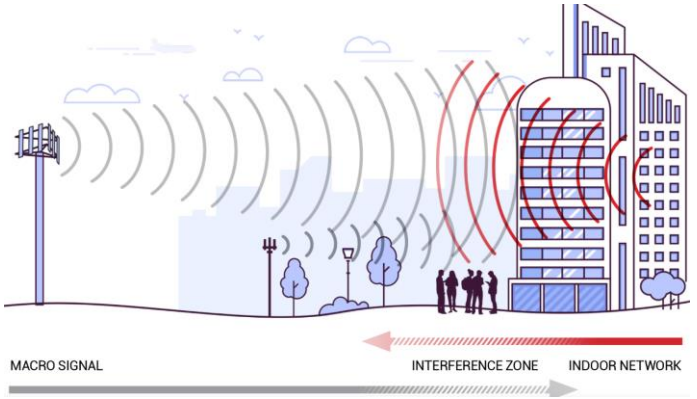


Wireless Network Challenges

- Interference
- Signal coverage and Dead zones
- Bandwidth Congestion
- Device compatibility
- Security Risks

Interference

- Disruption or weakening of a wireless signal
- Caused by
  - Nearby Wi-Fi networks in the same channel
  - Non-Wi-Fi devices like Bluetooth, microwaves
  - Physical obstructions like walls and buildings.



Signal Coverage and Dead Zones

- The extent to which a device can receive and transmit wireless signals
- Places where the signal can't reach.
- Dead zones are caused by;
  - Obstacles
  - Distance from access points

Bandwidth Congestion

- The network has insufficient capacity to handle the amount of data passing through it
- This can be caused by;
  - Too many users connected to an Access Point
  - High bandwidth applications like video streaming, online gaming

I have few users on the network but my network is still slow?

Wireless Network Troubleshooting

What to Look out for??

- **Coverage gaps (Dead zones)**
  - Are you in range of the Wi-Fi signals
  - Are there obstructions like walls, trees
- **Physical and Basic checks**
  - Is the AP or router powered and functioning
  - Are the Ethernet cables securely connected

Wireless Network Troubleshooting

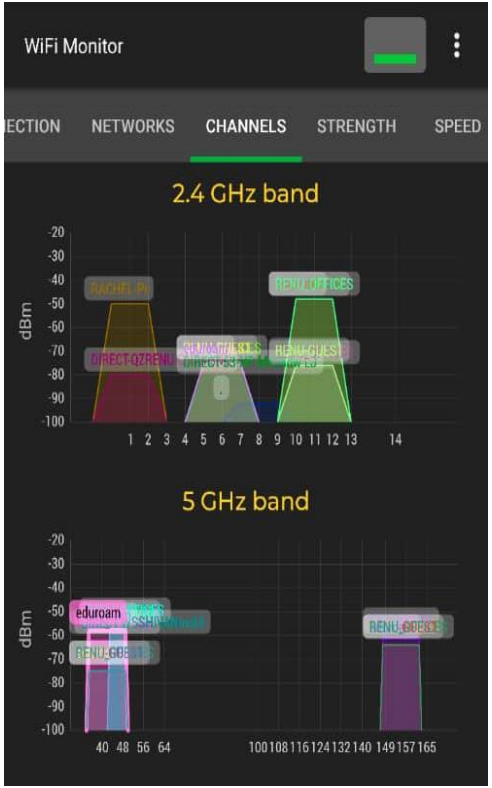
What to Look out for?

- **Channel Interference**
  - Overlapping channels
  - Channel Congestion

Wireless Network Troubleshooting

Troubleshooting tools?

- **WiFi Network Analysers**
  - Detect channel interference
- **WiFi Monitoring Tools**
  - Determine link speed, signal strength, and frequency



Common Fixes to Wireless network Problems

- **Coverage gaps (Dead zones)**
  - Wireless network survey (before and after network setup)
  - Add more APs
  - Strategic AP placement
- **Channel interference**
  - Use non-overlapping channels
- **Device compatibility**
  - Upgrade your device
- **Security**
  - Use secure authentication protocols (**WPA2 Enterprise**)

Enough of the talking, let's make our hands dirty

SETTING UP A WIRELESS NETWORK

Practical session

Setting up a Unifi Controller for Unifi devices

- Form 6 groups
- Each group will have access to a VM
- Follow the documentation provided to install the controller
- Adopt the access points into the controller
- Setup a wireless network

Assignment

Setting up Omada controller for Tp-links

- Find out different ways Omada controller can be setup
- If possible install the controller and adopt the Tp-link wireless devices
- Compare the functionality between the Unifi Controller and Omada Controller

THE END

Thank you for your time