Lanka Education and Research Network

Wireless LAN Recommendations

Wi-Fi in your Campus

11th March 2019

Campus Network Best Practices workshop

Thilina Pathirana

Based on NSRC, ICTP, WNDW and TRC-SL guidelines

Objectives

- Introduce wireless LAN technologies – basically Wi-Fi
- WLAN implementation techniques
- Best practices in implementing campus wide Wi-Fi
- WPA-2 Enterprise / AES authentication and eduroam
- Why Wireless and FAQ’s

ISM / U-NII bands

- Most commercial wireless devices (mobile phones, television, radio, etc.) use licensed radio frequencies. Large organizations pay licensing fees for the right to use those radio frequencies.

- Wi-Fi uses unlicensed spectrum. License fees are not usually required to operate WiFi equipment.
- The Industrial, Scientific and Medical (ISM) bands allow for unlicensed use of 2.4-2.5 GHz, 5.8 GHz, and many other (non-WiFi) frequencies.
- The Unlicensed National Information Infrastructure (U-NII) 5GHz radio band is part of the radio frequency spectrum used by IEEE 802.11 devices

Wireless networking protocols

The 802.11 family of radio protocols are commonly referred to as Wi-Fi.

- 802.11a supports up to 54 Mbps using the 5 GHz unlicensed bands.
- 802.11b supports up to 11 Mbps using the 2.4 GHz unlicensed band.
- 802.11g supports up to 54 Mbps using the 2.4 GHz unlicensed band.
- 802.11n supports up to 600 Mbps using the 2.4 GHz and 5 GHz unlicensed bands.
- 802.11ac supports up to 1300 Mbps using 5 GHz with MU-MIMO
- 802.11ax (high efficiency wi-fi) supports up to 11 Gbps using the 1 – 7 GHz

- 802.16 (WiMAX) is not 802.11 Wi-Fi ! It is a completely different technology that uses a variety of licensed and unlicensed frequencies.

Data Rates

- Note that the “**data rates**” quoted in the Wi-Fi specifications refer to the raw radio symbol rate, not the actual TCP/IP throughput rate. The difference is called **protocol overhead**, and is needed by the WiFi protocol to manage collisions, retransmissions, and general management of the link.

- A good rule of thumb is to divide the radio symbol rate by two to obtain the maximum practical TCP/IP throughput. For example, a 54 Mbps 802.11a link has a maximum practical throughput of roughly 25 Mbps. An 11 Mbps 802.11b link has a maximum throughput of about 5 Mbps.

MAC layer: CSMA vs. TDMA

- 802.11 WiFi uses **Carrier Sense Multiple Access (CSMA)** to avoid transmission collisions. Before a node may transmit, it must first listen for transmissions from other radios. The node may only transmit when the channel becomes idle.

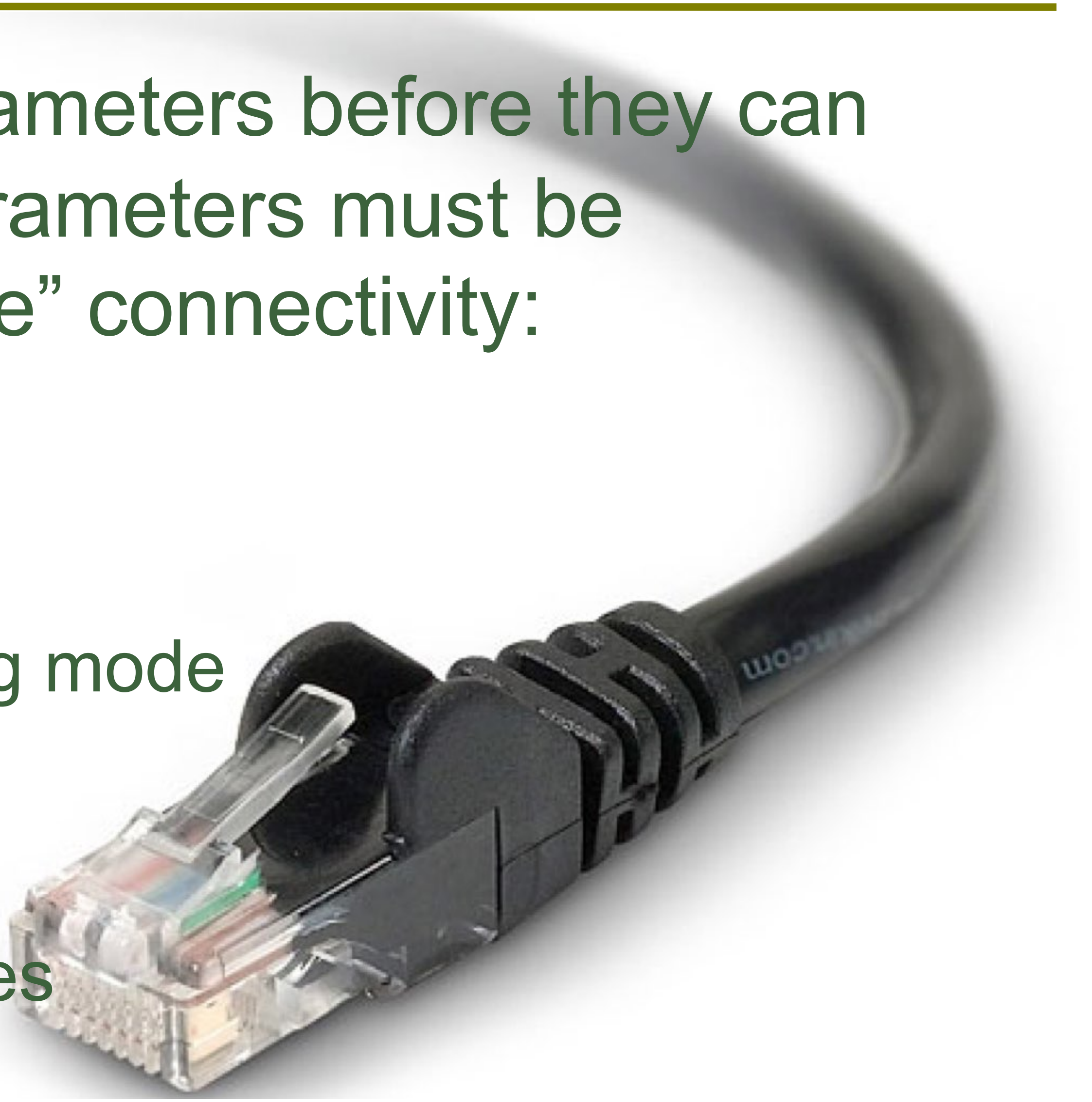
- Other technologies (such as WiMAX, Nstreme, and AirMAX) use **Time Division Multiple Access (TDMA)** instead. TDMA divides access to a given channel into multiple time slots, and assigns these slots to each node on the network. Each mode transmits only in its assigned slot, thereby avoiding collisions.

Layer 1

Wi-Fi devices must agree on several parameters before they can communicate with each other. These parameters must be properly configured to establish "layer one" connectivity:

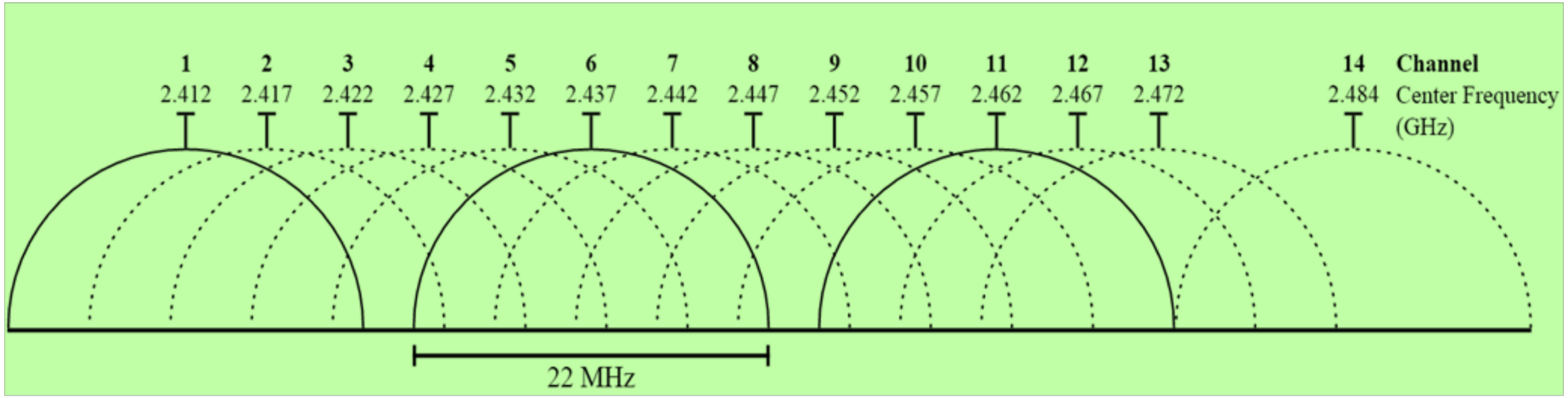
TCP/IP Protocol Stack	
5	Application
4	Transport
3	Internet
2	Data Link
1	Physical

- Radio channel
- Radio operating mode
- Network name
- Security features

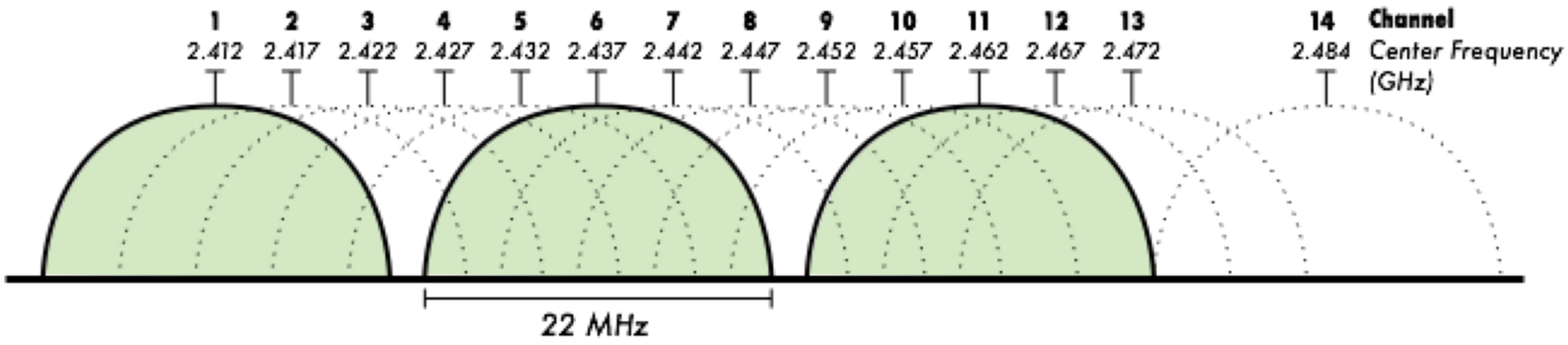


802.11 Wi-Fi Channels

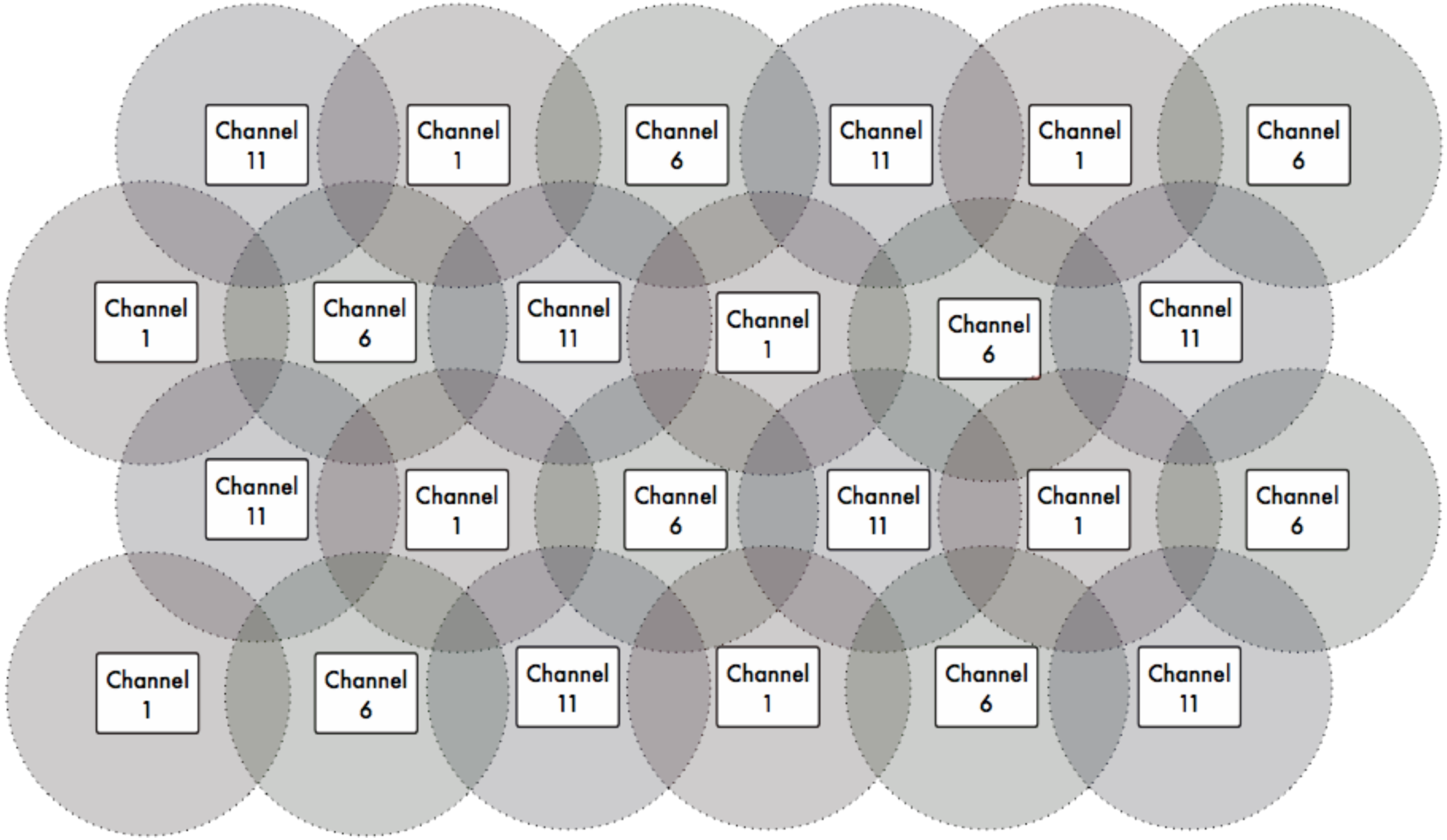
Wi-Fi devices must use the same channel in order to communicate with each other. They send and receive on the same channel, so only one device may transmit at any time. This kind of connection is called **half-duplex**.



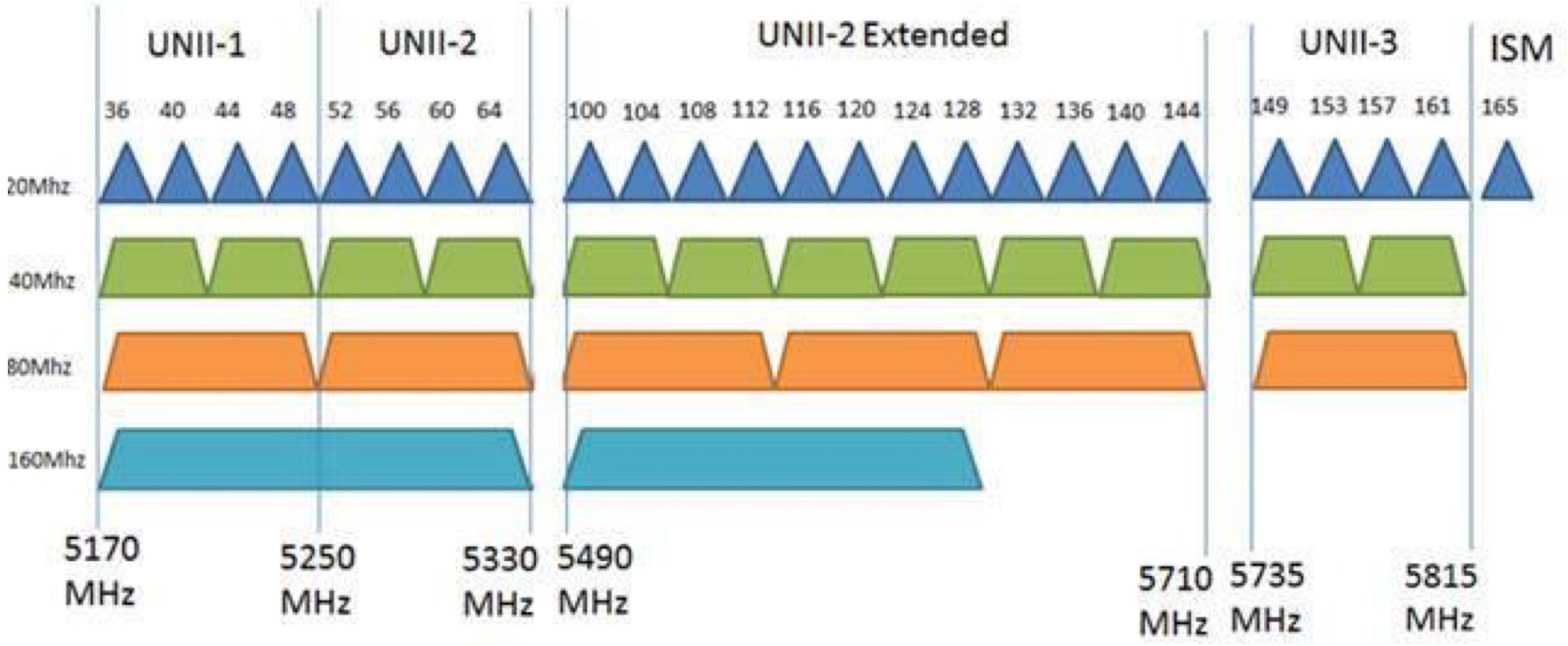
Non-overlapping channels: 1, 6, 11



AP channel re-use



802.11 Wi-Fi Channels



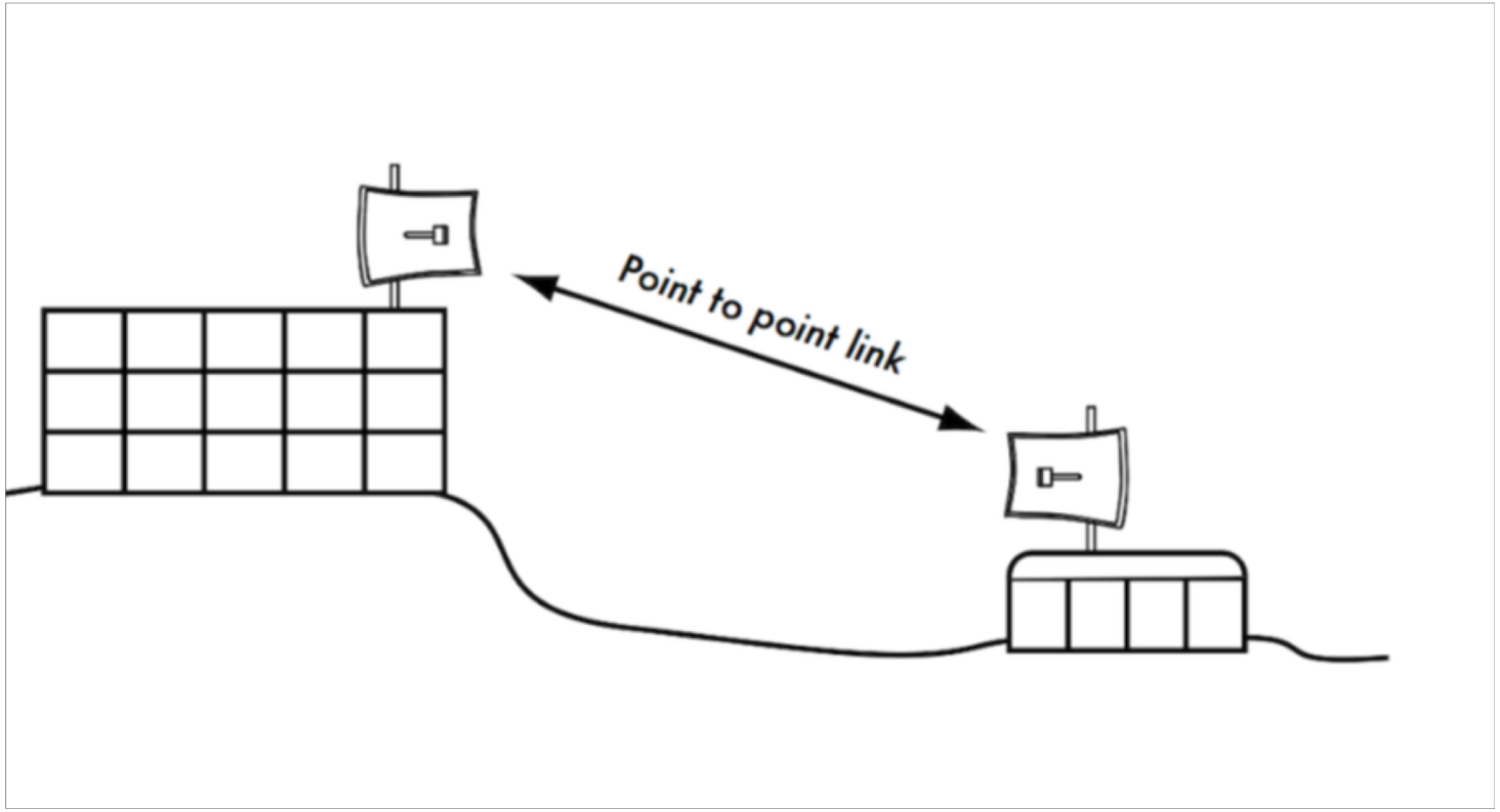
Wireless network topologies

- Any complex wireless network can be thought of as a combination of one or more of these types of connections:

  - Point-to-Point
  - Point-to-Multipoint
  - Multipoint-to-Multipoint

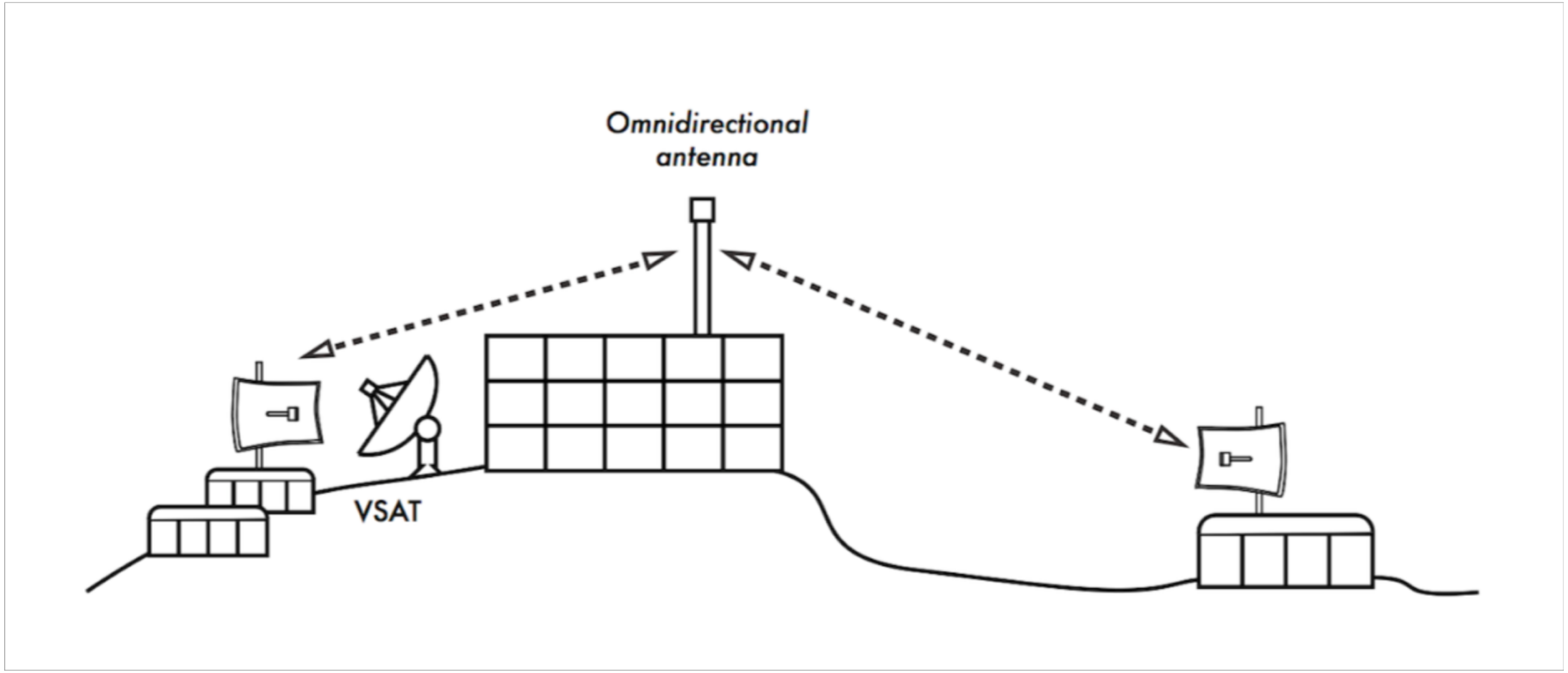
Point-to-Point

- The simplest connection is the point-to-point link.
- These links can be used to extend a network over great distances.



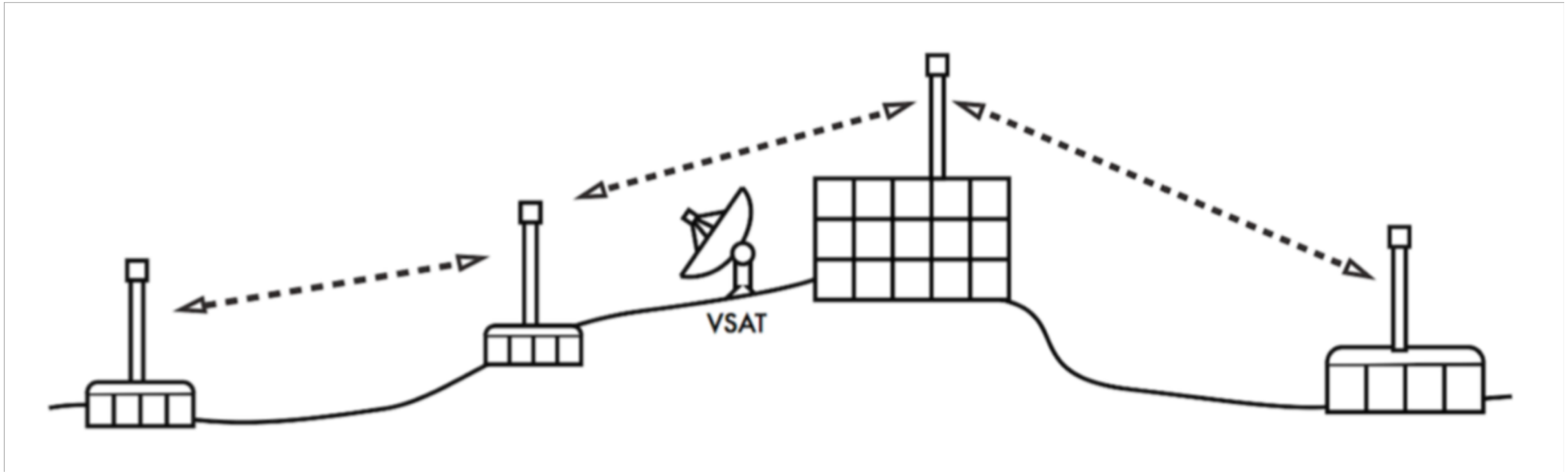
Point-to-Multipoint

- When more than one node communicates with a central point, this is a point-to-multipoint network.



Multipoint-to-Multipoint

- When any node of a network may communicate with any other, this is a multipoint-to-multipoint network
(also known as an **ad-hoc** or **mesh** network).



Wi-Fi Radio Modes

- Wi-Fi devices can be operated in one of these modes:
  - Master (access point)
  - Managed (also known as client or station)
  - Ad-hoc (used for mesh networks)
  - Monitor (not normally used for communications)
  - Other proprietary non-802.11 modes (e.g. Mikrotik Nstreme or Ubiquiti AirMAX)

- Each mode has specific operating constraints, and radios may only operate in one mode at a time.

Master Mode

Master mode (also called AP or infrastructure mode) is used to provide an infrastructure with an access point connecting different clients. The access point creates a network with a specified name (called the SSID) and channel, and offers network services on it. Wi-Fi devices in master mode can only communicate with devices that are associated with it in managed mode.

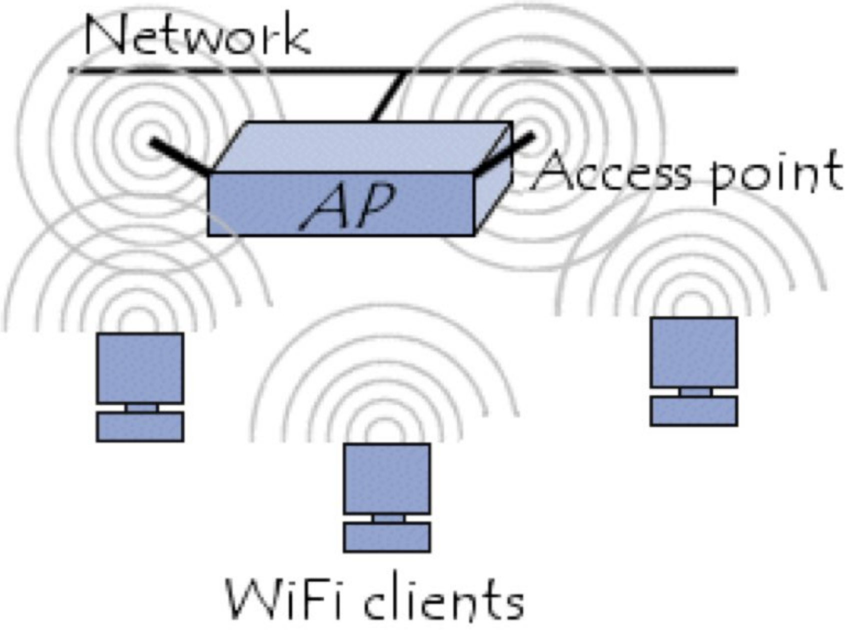


Image: https://ccm.net/

Managed Mode

- Managed mode is sometimes also referred to as **client mode**. Wireless devices in managed mode will join a network created by a master, and will automatically change their channel to match it.

- Clients using a given access point are said to be **associated** with it. Managed mode radios do not communicate with each other directly, and will only communicate with an associated master (and only with one at a time).

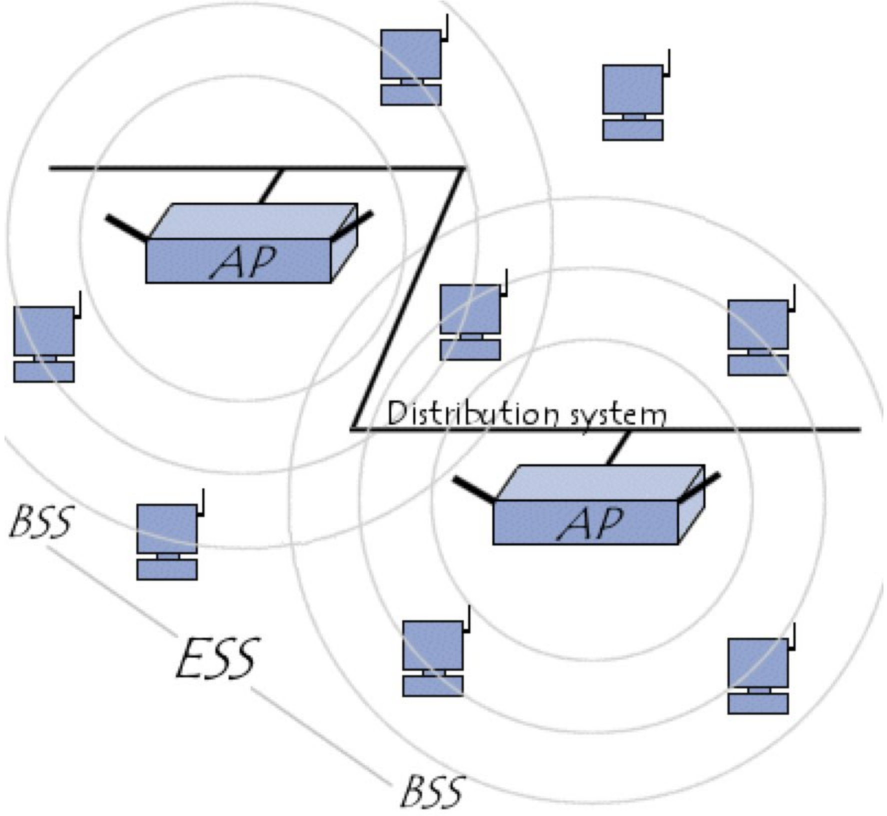


Image: https://ccm.net/

Ad-hoc Mode

- Ad-hoc mode is used to create mesh networks with:
  - No master devices (APs)
  - Direct communication between neighbors
- Devices must be in range of each other to communicate, and they must agree on a network name and channel.

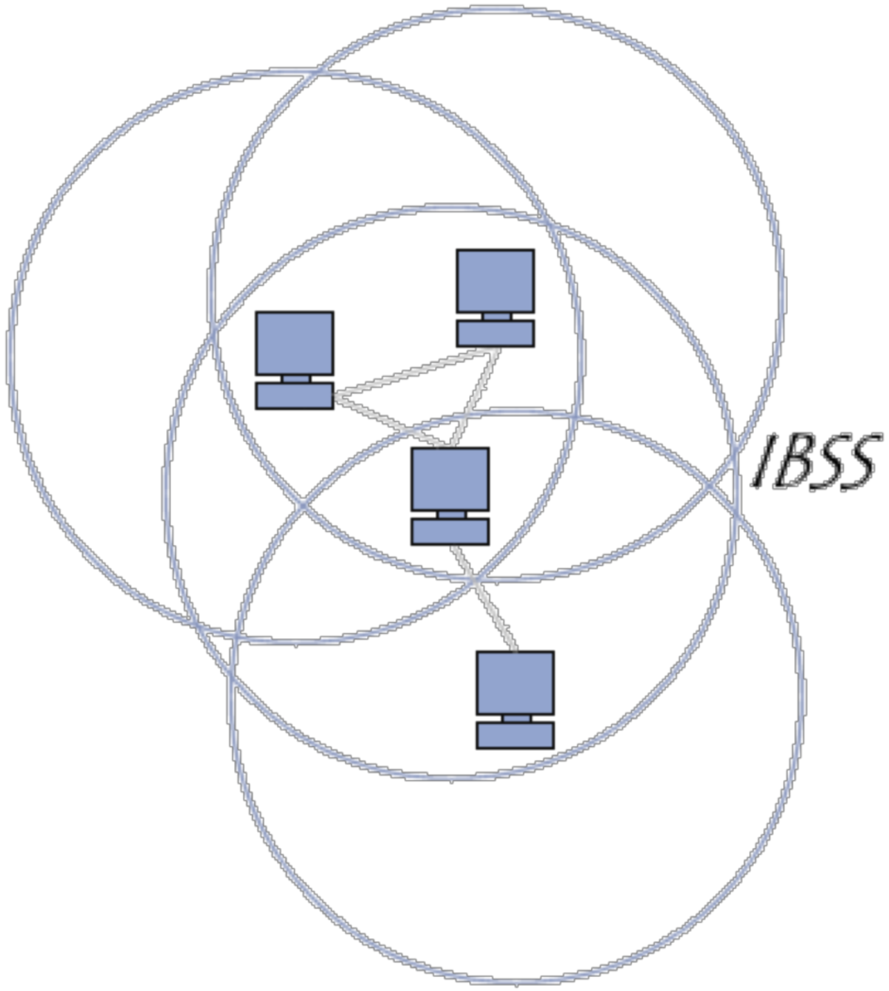
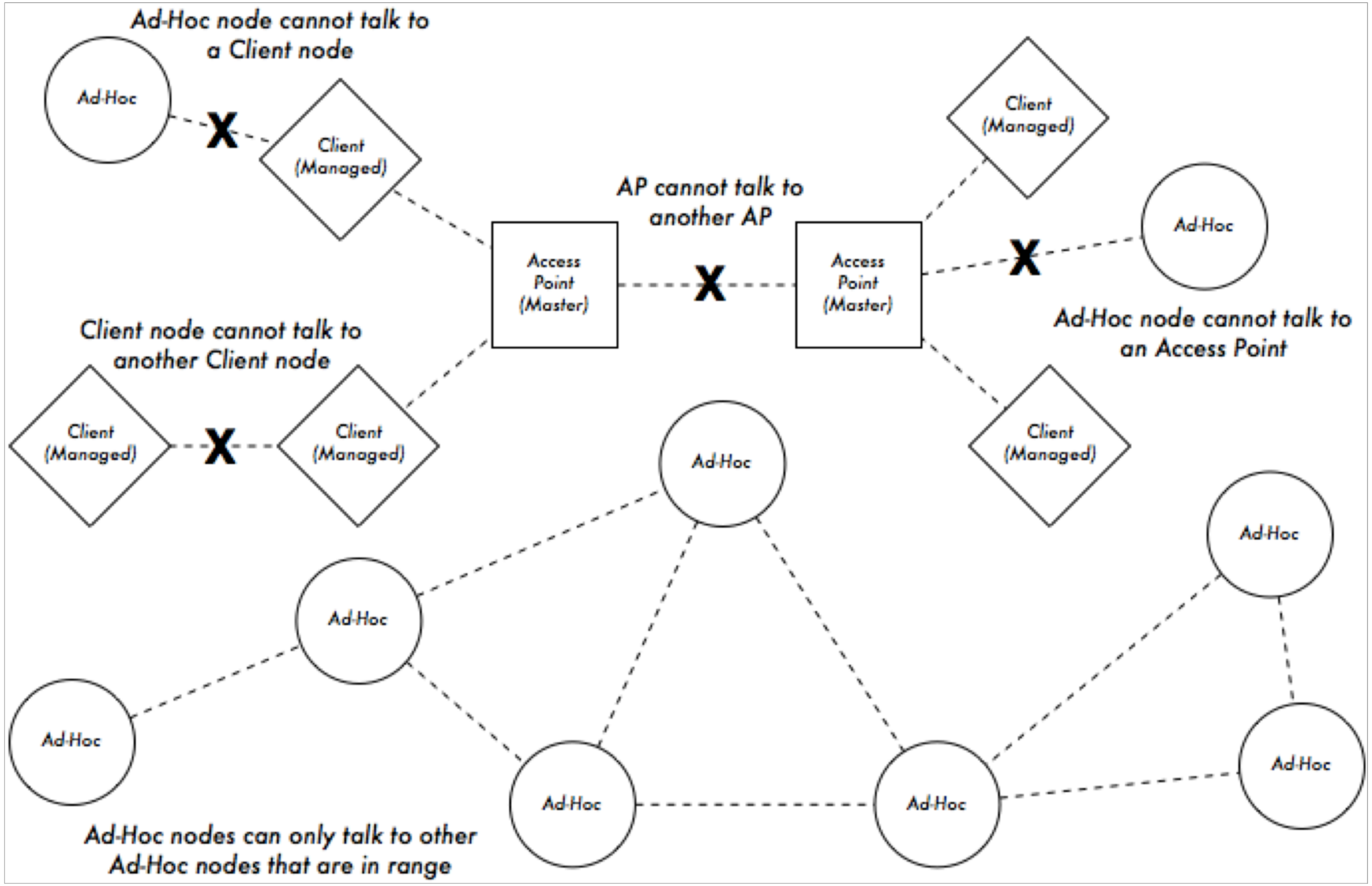


Image: https://ccm.net/

Monitor Mode

- Monitor mode is used to passively listen to all radio traffic on a given channel. This is useful for:
  - Analyzing problems on a wireless link
  - Observing spectrum usage in the local area
  - Performing security maintenance tasks

Wi-Fi Radio Modes in action



Ad-Hoc node cannot talk to a Client node

AP cannot talk to another AP

Client node cannot talk to another Client node

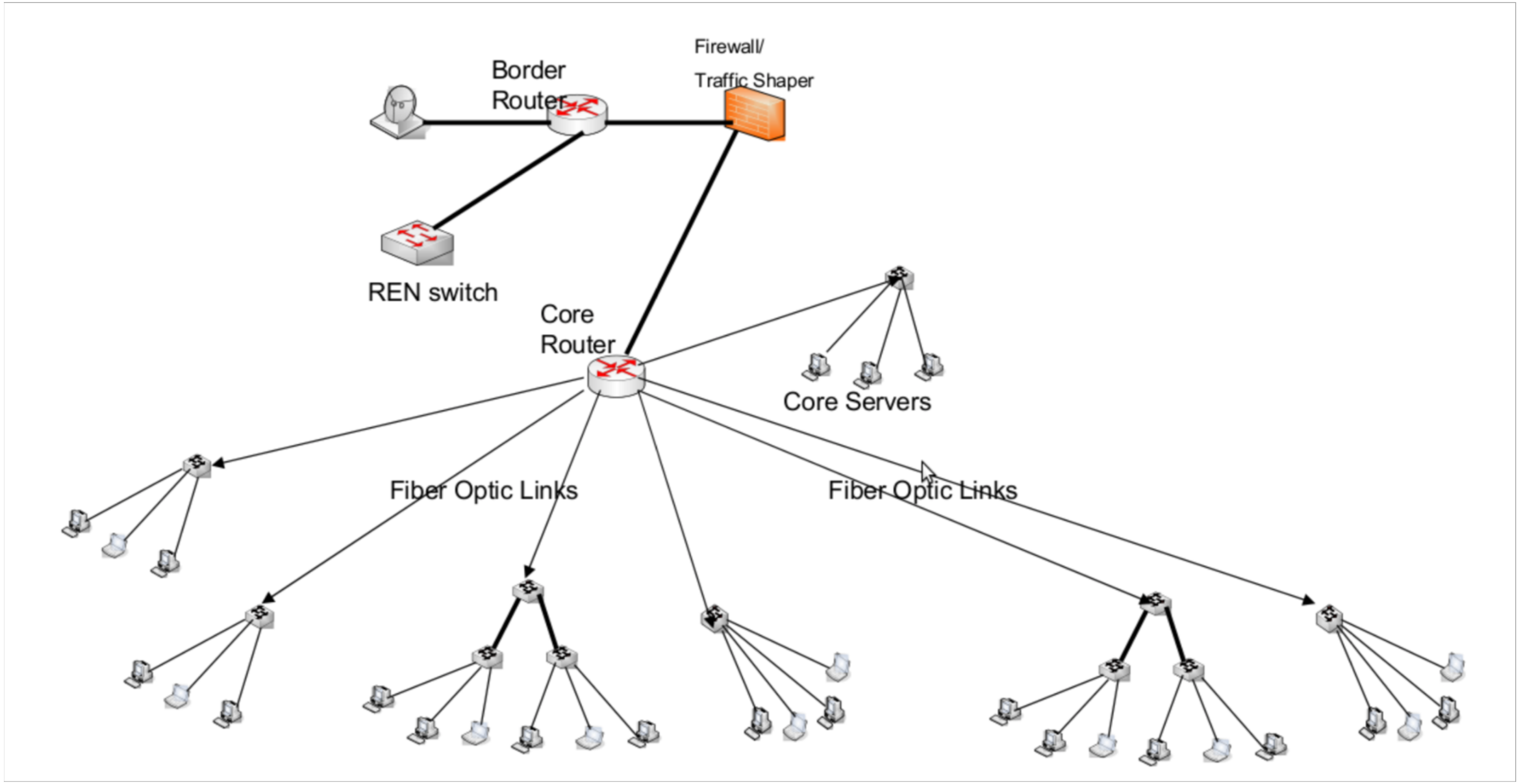
Ad-Hoc node cannot talk to an Access Point

Ad-Hoc nodes can only talk to other Ad-Hoc nodes that are in range

WLAN's in Campus Networks

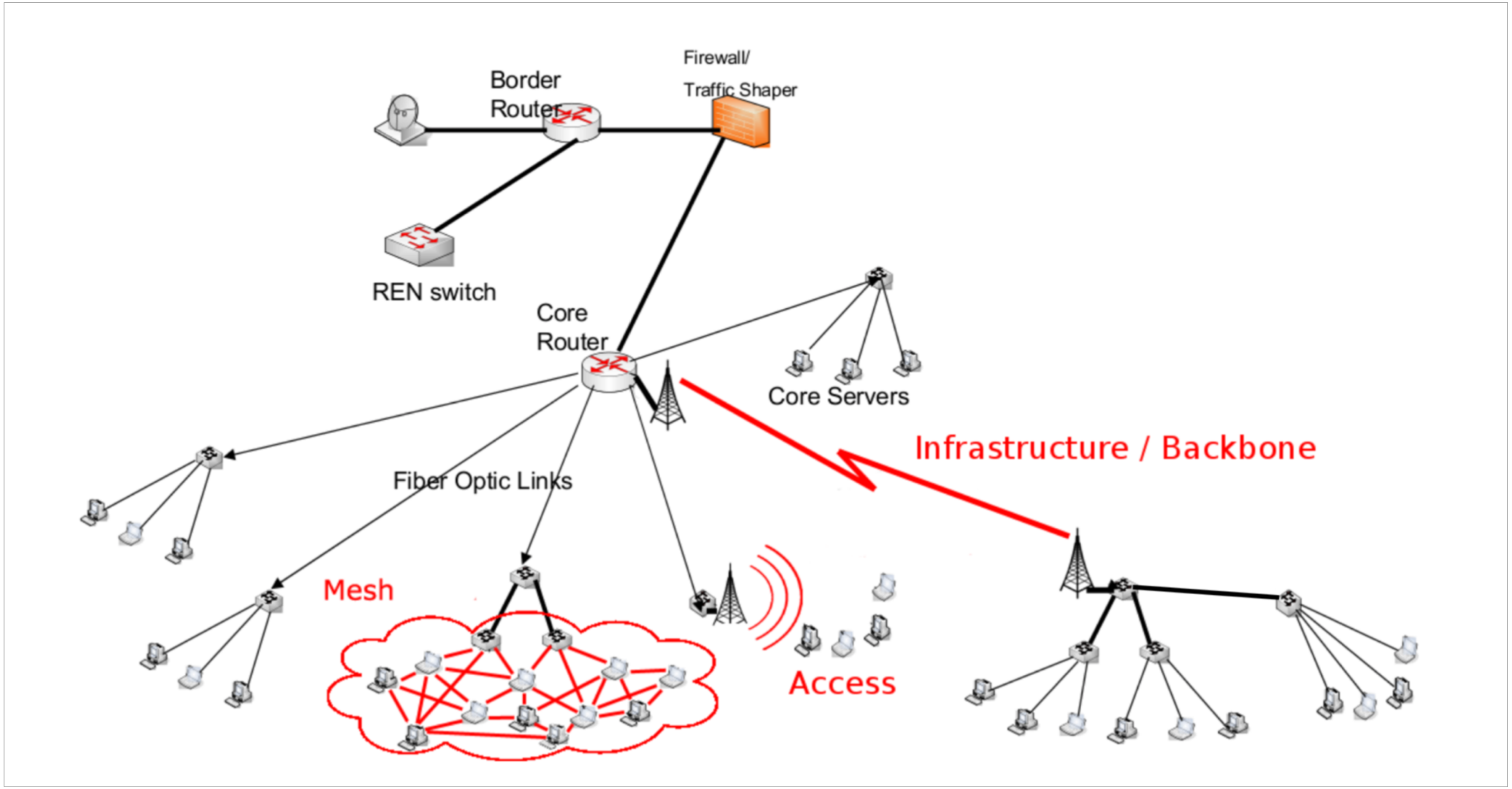
- Edge Access = Access For Users
  - Connect users (laptops, desktops, phones, tablets) to the network, services and Internet
- Infrastructure/Backbone
  - Distance, terrain, or obstacles make fibre too hard?
    - Use wireless point-to-point links
- Mesh
  - Where line of sight is difficult, mesh networks can act both as edge access and infrastructure

Wired Network



Design: NSRC

Wired & Wireless Network



Design: NSRC

Separate Access from Core

- It is important to keep a strict line between access and core networks
- Users should not see infrastructure
  - Do not allow users to see management network
  - Do not advertise SSIDs for backbone links
  - Control access to 802.11 backbone links
    - With security and by MAC address
- Keep user traffic away from your infrastructure!

Wired / Wireless Differences

- Physical location disconnected from network logic
  - A user on the library network might in fact be 10 miles away
- Link quality no longer binary
  - not “working” or “not working”, but something in-between
- New parameters separate networks on Layer 1/2:
  - frequency, protocol, ssid, polarization, ...
- Networks change over time
  - Devices come and go
  - Need to consider roaming
- Clients difficult to control & numbers growing fast

WLAN planning

- Required 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

WLAN planning, Cont…

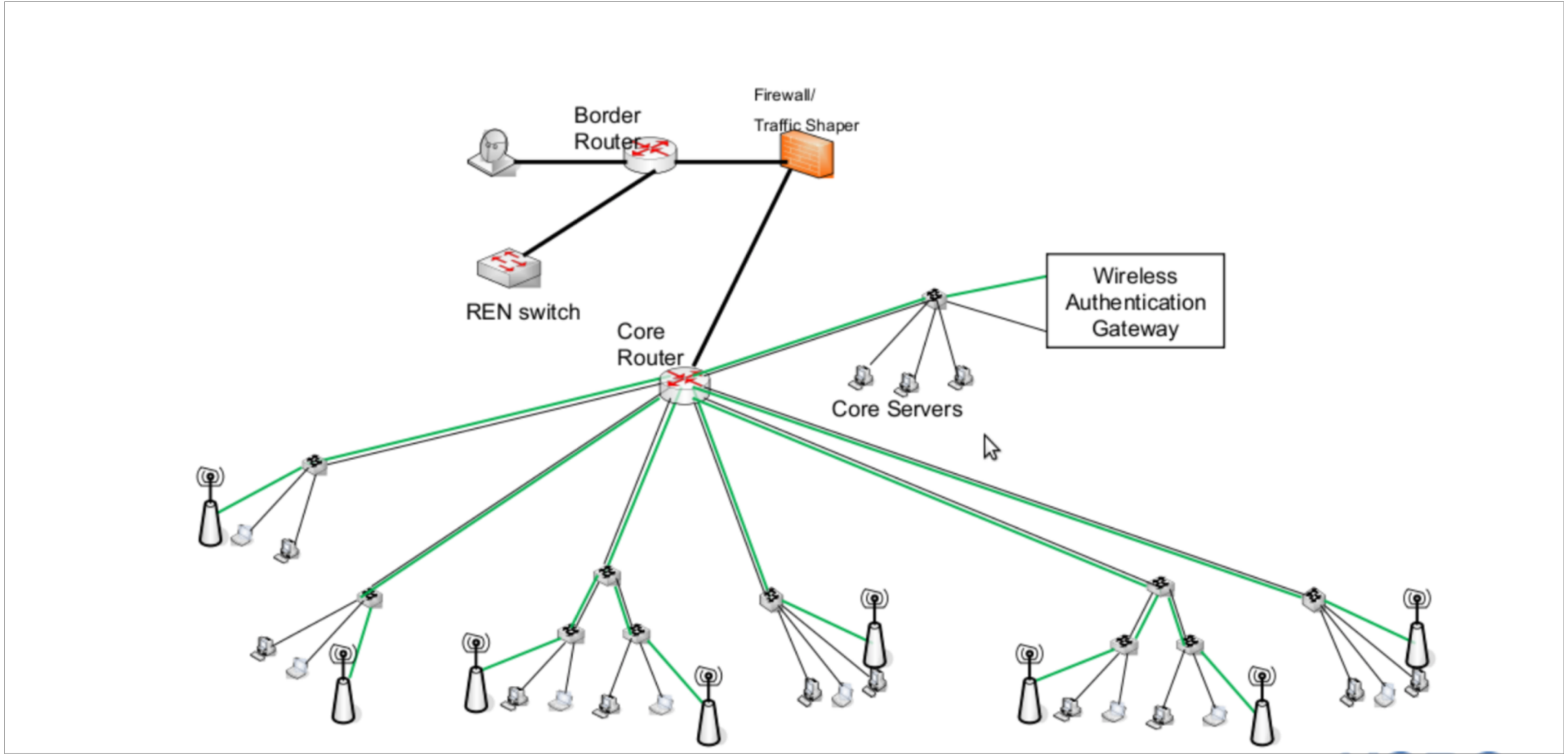
- SSIDs can provide user information:
  - MyUniv-Library
  - MyUniv-Hostel1
  - MyUniv-Adminbld
- Tempting SSIDs are a bad idea
  - Campus-Security
  - Finance-Department
- SSID choice can have an impact on:
  - Roaming & network design

WLAN planning, Cont…

- 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 Voice over IP chat or video chat)?
- Is it acceptable to log on again, when entering a new network zone?
- Ability to move around and stay on the network, Two kinds for roaming:
  - Nomadic: interrupted, yet able to pick up again
  - Seamless: uninterrupted, always on
- Users prefer Seamless Roaming:
  - Avoids interruption
  - Avoids re-authentication – Keeps state and session

Wireless Authentication

- Keep it in the core, not on edge APs



Protecting Wireless networks

Here are a few security measures that can be used to protect your users and your wireless networks.

- "Closed" networks
- MAC filtering
- Captive Portals
- WEP encryption
- WPA encryption
- Strong end-to-end encryption

Closed Networks

By hiding SSID (i.e. not advertising it in beacons), you can prevent your network from being shown in network scan utilities.

- Advantages:
  - Standard security feature supported by virtually all access points.
  - Unwanted users cannot accidentally choose a “closed” network from a network list.
- Disadvantages:
  - Users must know the network name in advance.
  - “Closed” networks are not easily found in a site survey, and yet they are easily found using passive monitoring tools.

MAC Filtering

A MAC filter may be applied to an access point to control which devices may be permitted to connect.

- Advantages:
  - Standard security feature supported by virtually all access points.
  - Only devices with a matching MAC address may connect to your network.

- Disadvantages:
  - MAC tables are inconvenient to maintain.
  - MAC addresses are transmitted in the clear (even when using WEP encryption), and are easily copied and reused.

Captive Portals

A captive portal is an authentication mechanism useful in cafés, hotels, and other settings where casual user access is required.

By using a web browser for authentication, captive portals work with virtually all laptops and operating systems. Captive portals are typically used on open networks with no other

authentication methods (such as WEP or MAC filters).

Since they do not provide strong encryption, captive portals are not a very good choice for networks that need to be locked down to only allow access from trusted users.

WEP Encryption

- Part of the 802.11 standard, Wired Equivalent Privacy provides basic shared encryption at layer two. WEP works with nearly all modern WiFi devices.

- Advantages: Standard security feature supported by virtually all access points.

- Disadvantages: Shared key, numerous security flaws, incompatible key specification methods, long-term maintenance is impossible on large networks.

- In short: Use WPA2-PSK instead.

WPA Encryption

- WPA2 (802.11i) is now the standard for protected Wi-Fi access. It uses 802.1x port authentication with the Advanced Encryption Standard (AES) to provide very strong authentication and encryption.
- Advantages:
  - Significantly stronger protection than WEP
  - Open standard
  - Verification of clients and access points.
  - Good for “campus” or “office” networks
- Disadvantages:
  - Some vendor interoperability problems, complex configuration, protection only at layer two.

Eduroam

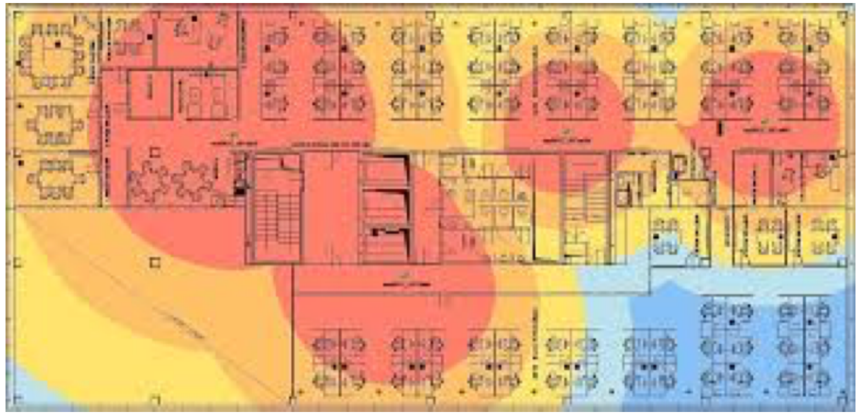
- Single SSID for the whole world
- Centralized authentication
- Local and Foreign users can log in using their own accounts
- Moderate Security encryption using WPA2-Enterprise and AES
- Seamless wireless setup using controller based or single SSID
- Eg:
  - 1 x Freeradius + IDP server
  - 1 x Controller (can be any commercial one or opensource like Unifi)
  - N x AP’s

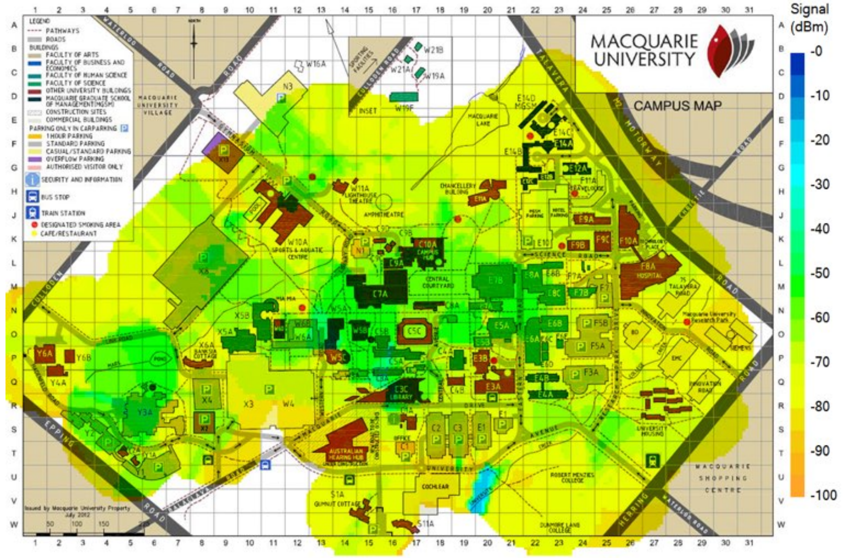
Site Surveys: Understanding Requirements

- Where is coverage needed?
- At what data rates?
- For how many subscribers or devices?
- Are there latency or jitter requirements?
- Will VoIP or AR/VR be supported? Industrial controls?
- Is itinerant connectivity ok, or is seamless mobility required?
- Are there places no coverage is required?
- High density places like entrances/exits, conference halls?
- High demand locations like labs or demonstration spaces?

Site Surveys: Mapping

- Outdoor surveys can rely on Google Maps or Open Street Maps
- Indoor surveys require a site plan
- The site plan must be scaled accurately
- A blueprint is best - both scanned & on paper required





Site Surveys: Assessing Indoor Sites

- With your blue print or map…
- Visit each room and hallway at a site
- Record its layout, walls, construction material
  - Are there attenuation, reflection, diffraction opportunities?
  - Are there places we cannot mount access points?
- How many people will the room hold?
- Are there rooms above or below it?
- Are there adjacent rooms? Windows onto crowded streets?
- Record where coverage is needed and all room attributes.

Site Surveys: Indoor and Outdoor

- Outdoor surveys
  - Rely on a GPS receiver
  - Associate RF measurements with a GPS point
  - Are fast & easy with many tools available

- Indoor surveys
  - Rely on hand-curated location data
  - Associate RF measurements with a location on a map
  - Are not as accurate as outdoor surveys
  - Typically require expensive, proprietary software tools

Site Surveys: Passive Surveys

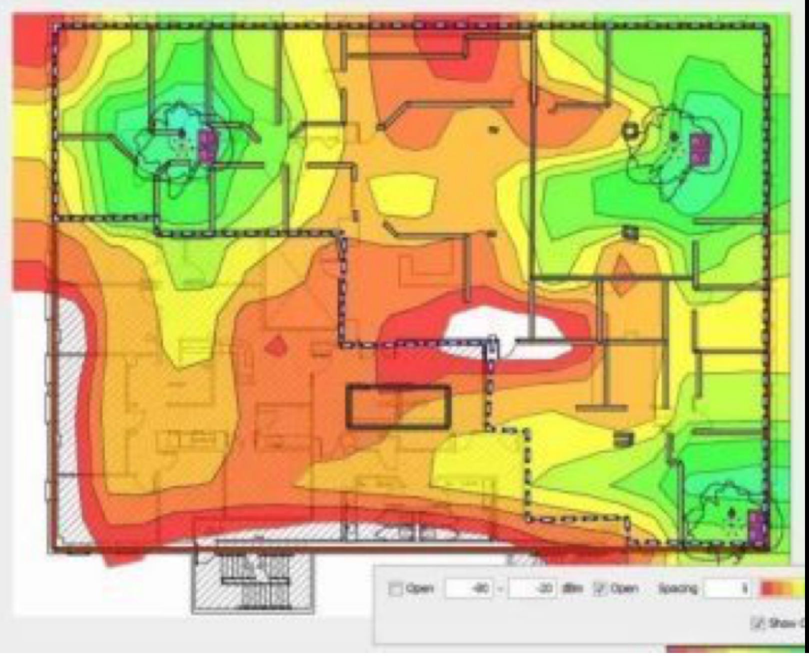
- Listen to APs, record signal strength, interference, & quality
  - At a single point in space and time
- With multiple points recorded
  - Can determine AP coverage and provide data for heat maps
  - Can geolocate Aps
  - Can geolocate interference sources
- Over time can determine how the RF environment changes
- Passive surveys only measure received performance
  - They can't predict how well a terminal will be received at an AP

Site Surveys: Active Surveys

- Are performed while a client is connected to a network
- Can be tied to a single AP, or to a single SSID
- Allow recording of performance at a location & time
    - Typically through bidirectional TCP testing to an on-net test server
    - Can tie performance to signal strength, frequency, and data rate
- Can debug handover issues

Site Surveys: Surveying Tools

- Smartphone based tools:
  - iBWave
  - iMapper WiFi Pro
  - WiFi Analyzer & Surveyor
  - WiTuners
- Laptop based tools:
  - Acrylic WiFi
  - Ekahau Site Survey
  - Netspot
  - Tamograph
- Hardware Wi-Fi Tools



Site Surveys: Reporting for Planning

- Start with listing the requirements
- Show AP placement on a map
    - Including type of AP and antenna
    - Expected frequencies, number of subscribers, peak throughput
- Show unavoidable interference
- Provide a mounting / powering / cabling plan for each

Site Surveys: Reporting for Audit

- Summary of APs, BSSIDs, and networks detected
- Summary BSSIDs by channel & maximum data rate
- Complete device inventory of target network
- Geolocations & times of each measurement taken
- Geolocations of each AP
- Adjacent channel overlap areas & co-channel interference areas
- Heat map of per AP/frequency cover & per network cover
- Usable coverage per AP

What about your campus?

- Do you have Wi-Fi?
- Is it standalone (master mode) or controller based (managed mode) ?
- How your users are Authenticated?
- Are you still using MAC or shared key security?
- If no Wi-Fi try to start small but with complete infra
- Do you need help implementing Wi-Fi / eduroam? -- > Call Me 😉

Thank You

Thilina Pathirana

thilina@learn.ac.lk