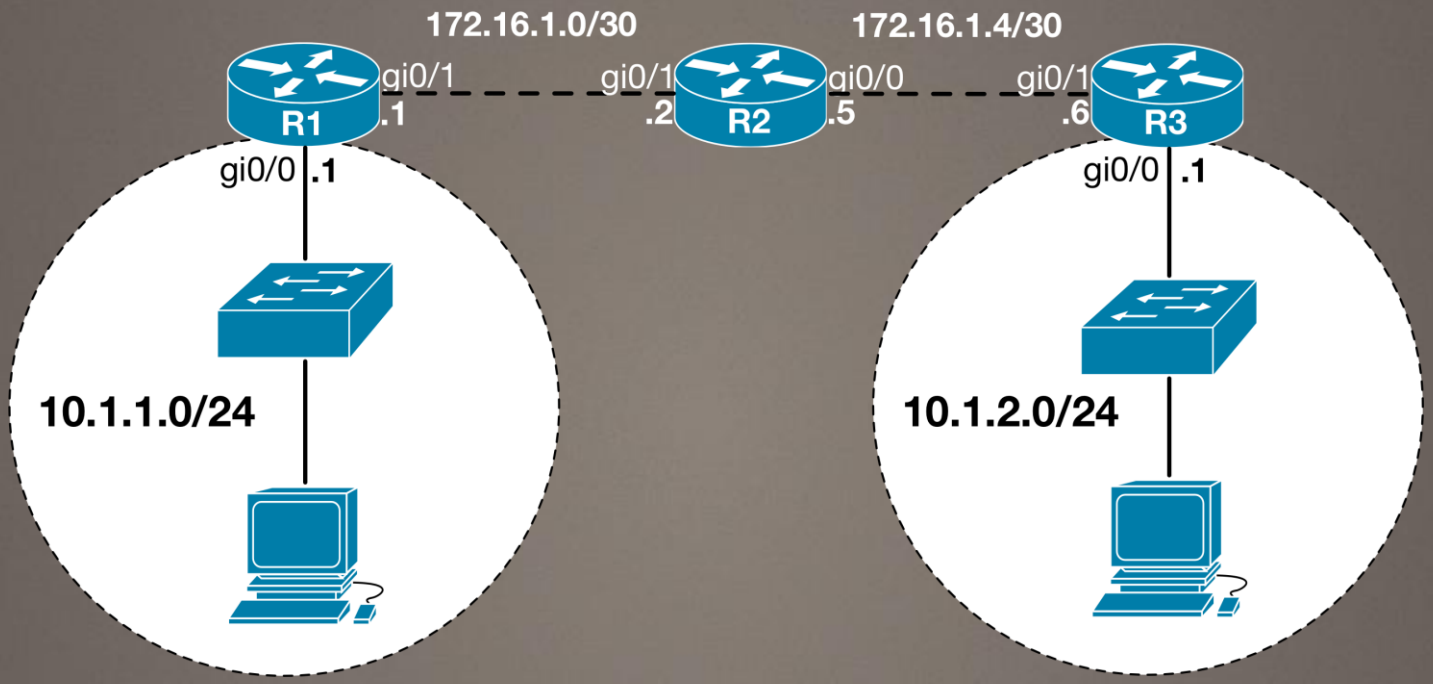
Review Question

Consider the topology below

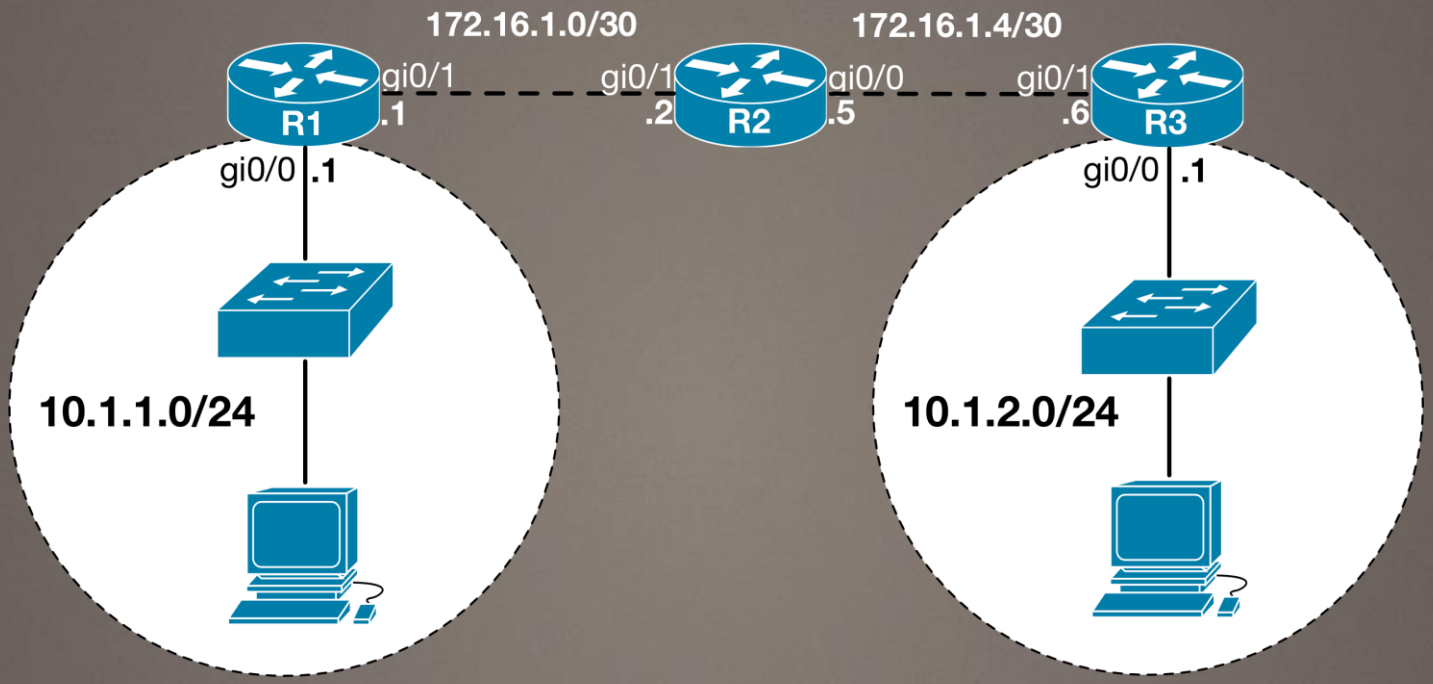


- What OSPF network statements will be required for R1?
- What would be the consequence if R2 only had a network statement for 172.16.1.5?

Murdoch UNIVERSITY

Review Question

Consider the topology below



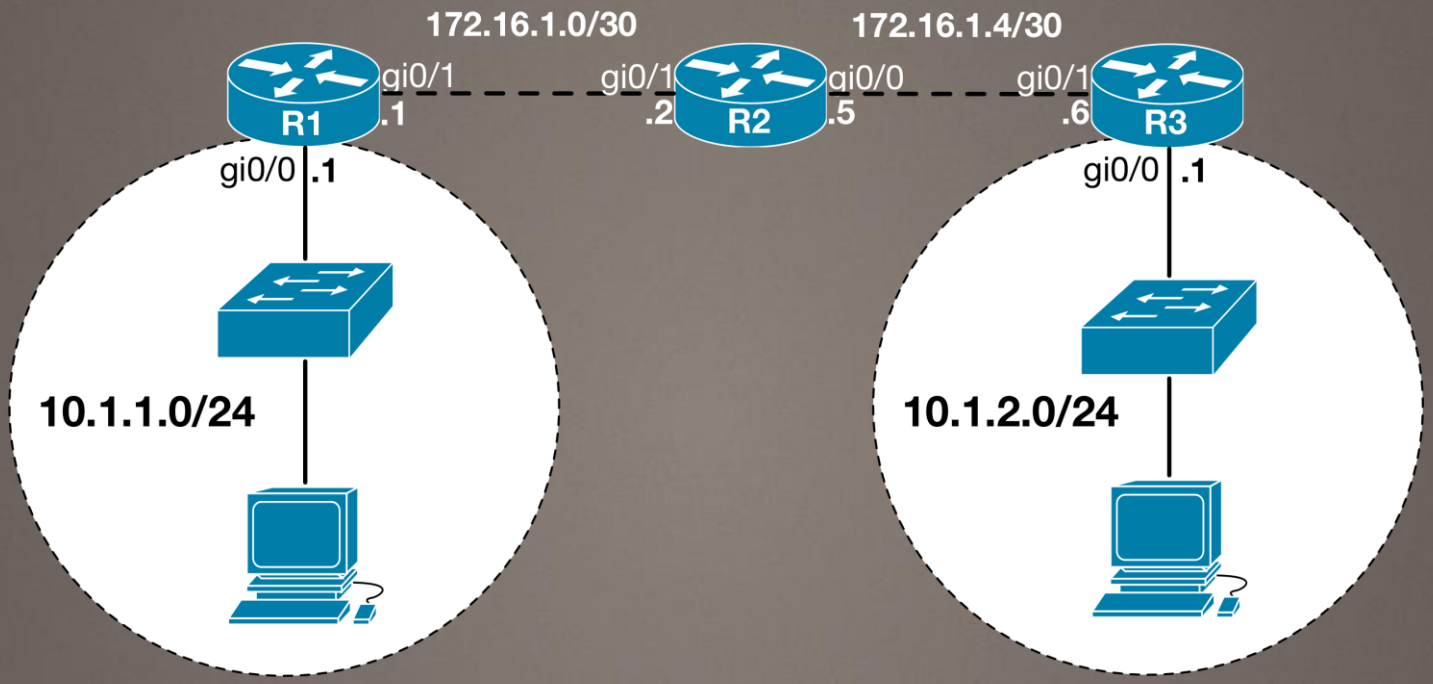
- What OSPF network statements will be required for R1?

```
network 10.1.1.1 0.0.0.0 area 0
network 172.16.1.1 0.0.0.0 area 0
```

Murdoch UNIVERSITY

Review Question

Consider the topology below



- What would be the consequence if R2 only had a network statement for 172.16.1.5?

R2 would not form a neighbor adjacency with, and would therefore not accept LSAs from, R1. The end result would be that no routes would propagate between R1 and R2.

Murdoch UNIVERSITY

Murdoch
UNIVERSITY

Wireless Networks

ICT169

Foundations of Data Communications

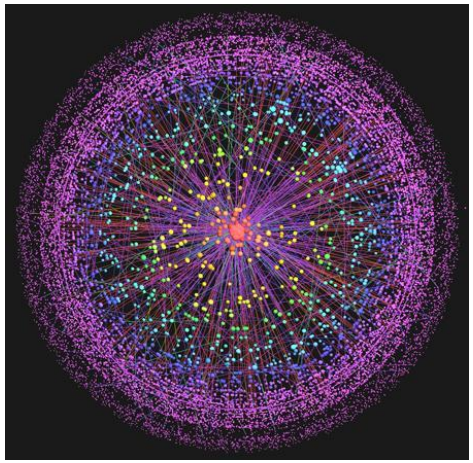
Admin

- Lecture recording for Topic 8 missing audio
  - First half of the lecture missing audio due to LCS failure
  - Lecture recording from 2017 available
- Access to the data centre outside of lab time
  - Available until 8:00PM on weeknights
  - Unavailable on weekends

Murdoch UNIVERSITY

Last Week

- A look at OSPF and the OSPF convergence process
- Exterior gateway routing with BGP
- The structure of the Internet
- Content Distribution Networks and Net Neutrality



Murdoch UNIVERSITY

Lecture Overview

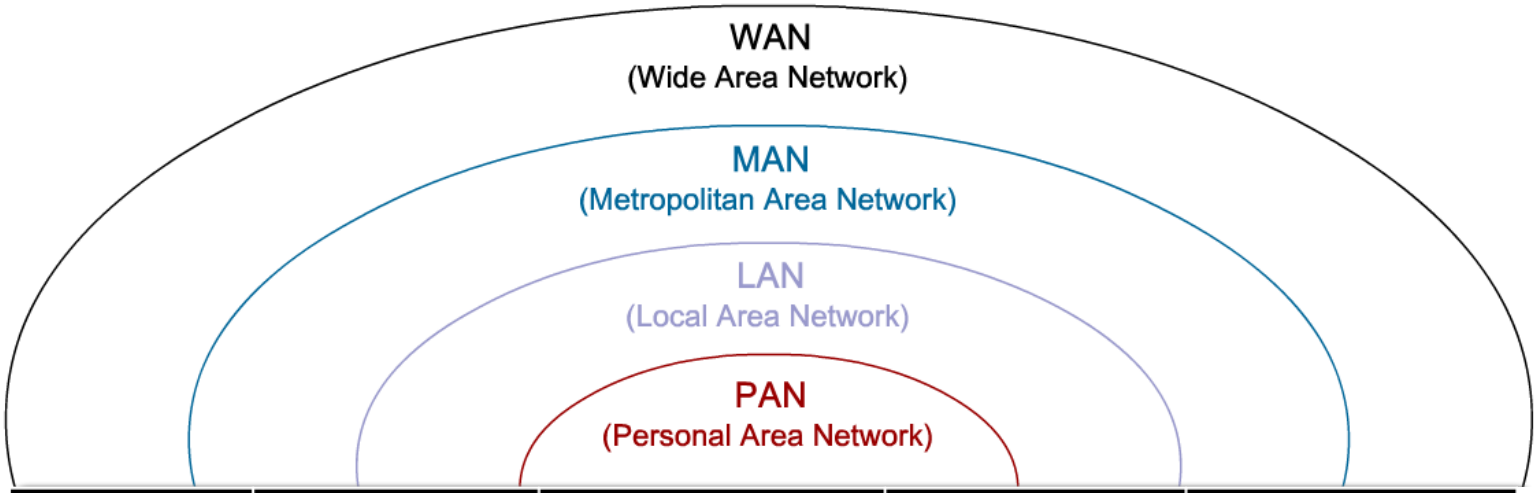
- All about wireless networks:
  - Different wireless technologies
  - Properties of wireless networking as a communications medium
  - 802.11 (WiFi standards)
  - Overheads in wireless
  - WiFi security

The Motivation for Wireless Networks

- Historically, networked devices needed to be connected by a cable (Ethernet or otherwise)
- This approach is no longer practical as we now expect:
    - Mobility – the ability to move freely while using our devices
    - Flexibility – the ability to use our devices anywhere within the coverage area

Categories of Wireless Technologies

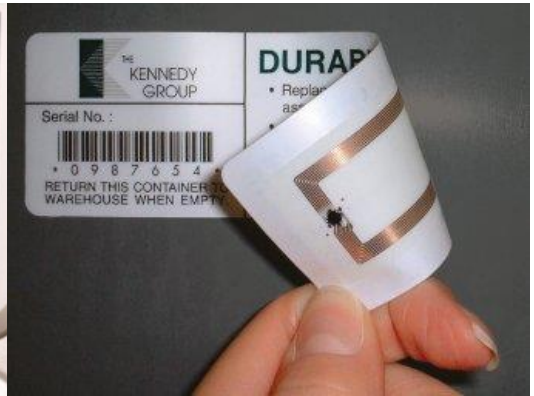
- Wireless technologies can be classified into three categories based on range



	PAN	LAN	MAN	WAN
Standards	Bluetooth, 802.11ad	802.11	802.11 802.16	GSM, CDMA, LTE, … Satellite
Speed	Up to 7 Gbps	11 Mbps to 1+ Gbps	10 - 100+ Mbps	10 kbps – 50 Mbps
Range	Short	Medium	Medium-Long	Long
Applications	Peer-to-Peer	Enterprise nets	Last mile access	Mobile data

Radio Frequency Identification (RFID)

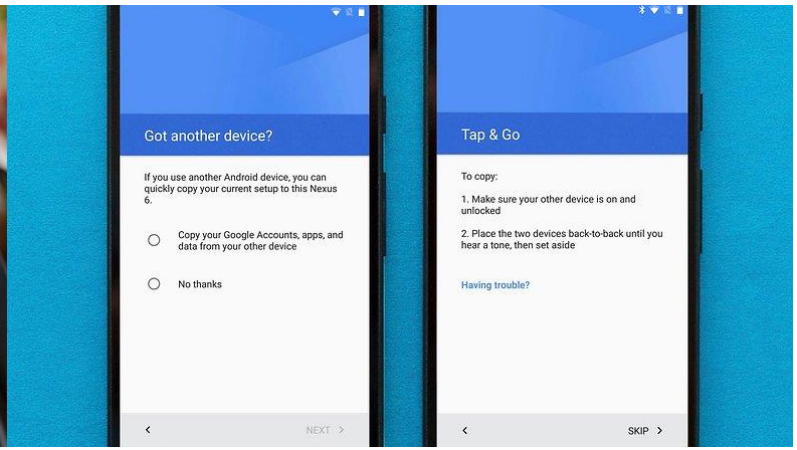
- Wireless technology used for identification and tracking
- Utilises the 13.56MHz and 125MHz spectrum
- Passive and active versions, depending on range required
- Used for:
  - Animal microchips
  - Building access
  - Inventory tracking and asset management
  - Public transport payments (eg. SmartRider)



Murdoch UNIVERSITY

Near-Field Communication (NFC)

- Short range wireless technology, closely related to RFID
- Incorporated into most smartphones
- Used for:
  - Contactless payments (eg. PayPass, PayWave)
  - Initialising WiFi / Bluetooth connections
  - Small file transfer (eg. Contact details)
  - Smartphone automation



https://www.androidpit.com/how-to-set-up-an-android-smartphone

Murdoch UNIVERSITY

Bluetooth

- Formally known as IEEE 802.15.1
- Used to replace cables over short distances (< 10m)
- Theoretical range of 240m (for Bluetooth 5.0)
- Used for:
  - Headphones, microphones, and speakers
  - Keyboards and Mice
  - Game controllers (Nintendo Wii, PlayStation 3/4)
  - Wearable devices (fitness trackers and smartwatches)

Murdoch UNIVERSITY

Zigbee

- Formally known as 802.15.4
- Used to support sensor networks and in many Internet of Things / Smart Home connected appliances (eg. light bulbs, thermostats)

Murdoch UNIVERSITY

WiGig (802.11ad)

- Designed to replace cables over short distances in high speed applications (eg. laptop docks, wireless display)
- Maximum data rate of 7Gbps over 60GHz

WiFi (802.11)

- The most common wireless LAN technology in use
- Designed to provide network access around homes or offices
- Operates on the 2.4GHz and 5GHz frequency ranges
- Incorporated into many consumer electronics including smartphones, tablets, printers, TVs, game consoles, cameras, and even fridges

Murdoch UNIVERSITY

3G and HSDPA

- Wireless WAN (WWAN) technology used for mobile networks usually operated by telecommunications providers
- Data rates between 384Kbps and 42.3Mbps
- Frequencies used vary by country
- Used for mobile Internet access (by smartphones or mobile broadband modems)

Long Term Evolution (LTE)

- Successor to HSDPA, often referred to as '4G'
- Maximum download speed of 300Mbps
- Frequencies in use vary by country
- Superseded by LTE Advanced (max download speed of 1Gbps)
- Used for mobile Internet access (by smartphones or mobile broadband modems)

Murdoch UNIVERSITY

5G

- Successor to LTE / LTE Advanced
- Download speeds of 100Mbps—20Gbps (average 1Gbps)
- Emphasis on reducing latency (target 1ms)
- Improve network density without increasing congestion
- Commercial availability beginning 2019

Murdoch UNIVERSITY

Worldwide Interoperability for Microwave Access (WiMAX)

- **W**orldwide **I**nteroperability for **M**icrowave **A**ccess
- Provides downlink speeds of 30Mbps—40Mbps
- Initially envisaged to be the successor to 3G / HSDPA
- Now used for some fixed-wireless services

From: http://www.broadbandtips.in/what-is-wi-max/

Licensed Microwave

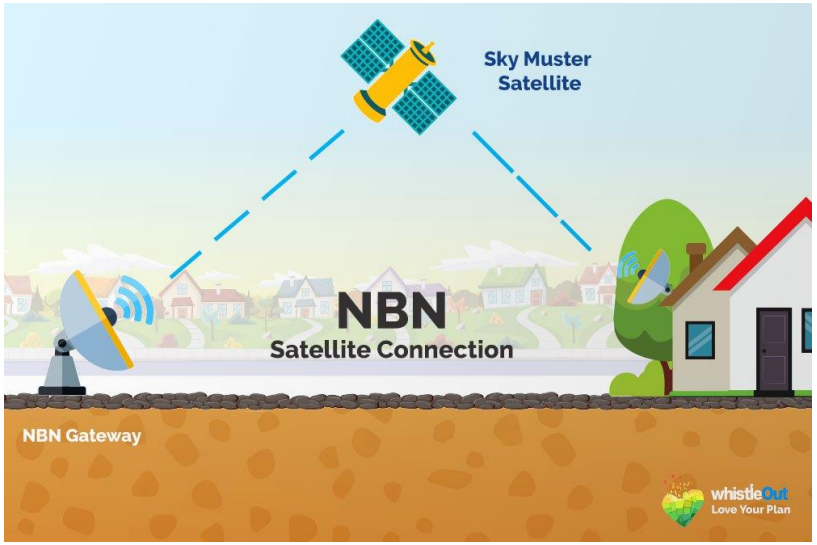
- Proprietary point-to-point links designed to be an alternative to deploying fibre
- Usually requires line of sight
- Operates over 2.4GHz or 5.8GHz bands

http://www.hsecommunications.com/about_hse.htm

Murdoch UNIVERSITY

Satellite

- Used to provide Internet connectivity to very remote areas, aircraft, and ships
- Much slower and higher latency than other wireless technologies (typical speeds <= 20Mbps)
- Two types of satellites, Geosynchronous Orbit (GEO) and Low Earth Orbit (LEO)

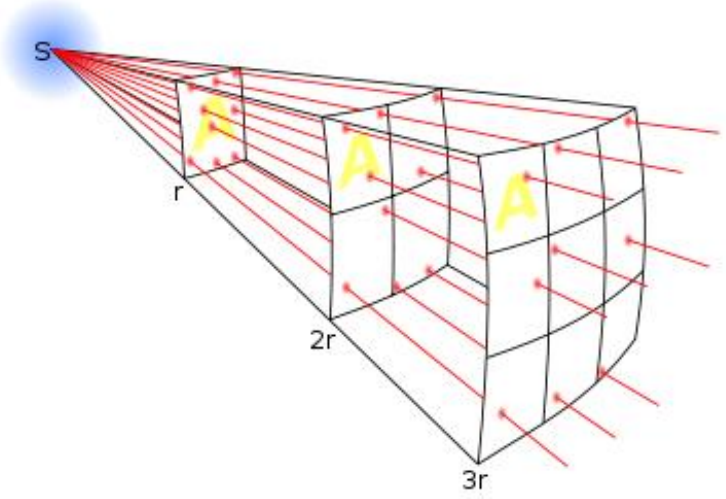


https://www.whistleout.com.au/Broadband/Guides/nbn-satellite-everything-you-need-to-know

Murdoch UNIVERSITY

Wireless Range

- Wireless technologies suffer the most attenuation of any transmission media
- Every time the distance doubles, the energy from a wireless transmission is spread over four times the area; this is known as the **inverse square law**
- The result is that the signal strength is reduced to ¼

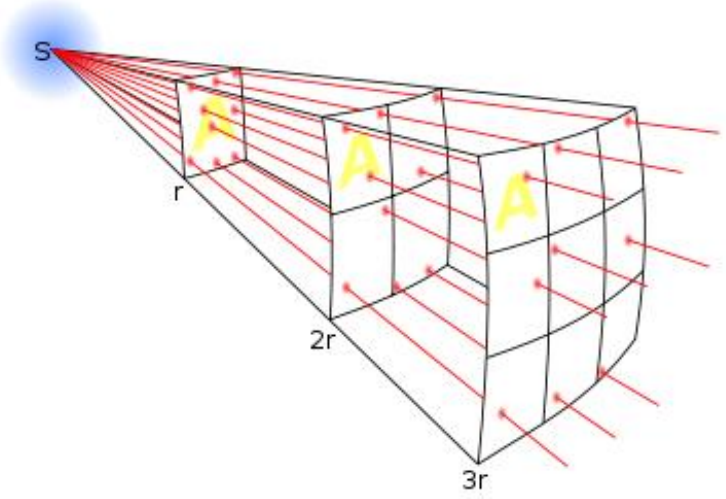


http://en.wikipedia.org/wiki/Inverse-square_law

Murdoch UNIVERSITY

Wireless Range (cont.)

- Given the same parameters (eg. antennas, transmission power), short range technologies will always be faster than long range ones
- But use cases for each technology will vary



http://en.wikipedia.org/wiki/Inverse-square_law

Murdoch UNIVERSITY

Increasing Range through Transmission Power

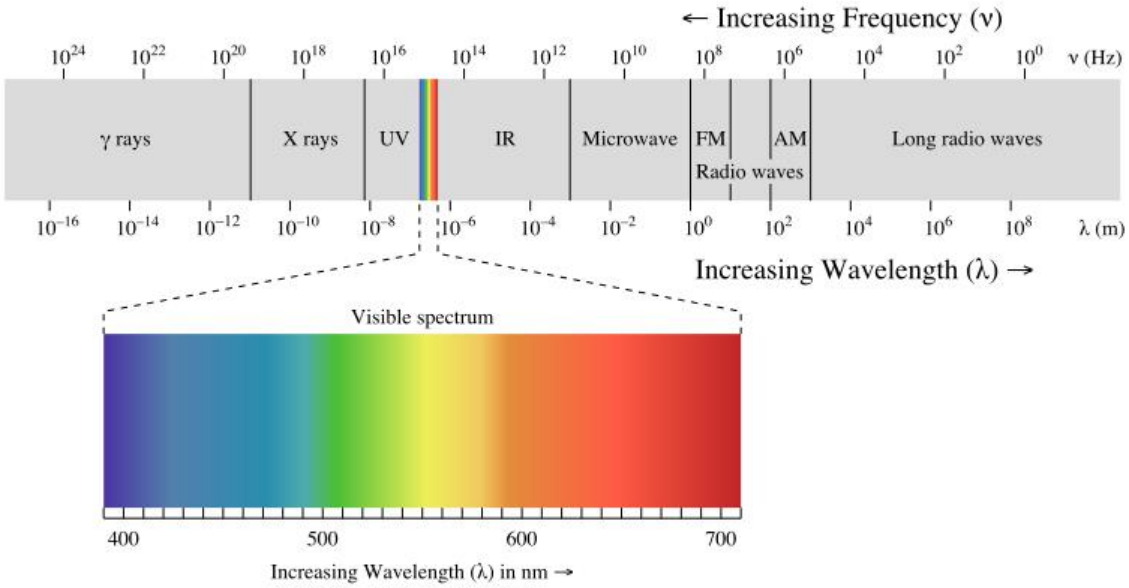
- Range of a wireless transmission can be increased by increasing the transmission power
- Not always feasible to use this approach
    - Power requirements and constraints
    - Licensing restrictions

http://picsdigger.com/keyword/communication%20link/

Murdoch UNIVERSITY

Frequency

- Wireless transmissions are transmitted using electromagnetic spectrum
- Radio communications operate at frequencies between 30KHz and 300GHz
- Lower frequencies propagate further (and usually penetrate solid objects better) than higher ones



http://en.wikipedia.org/wiki/File:EM_spectrum.svg

Murdoch UNIVERSITY

Frequency (cont.)

- Every country has a government body that regulates the use of these frequencies
  - US Federal Communications Commission (FCC)
  - Australian Communications and Media Authority (ACMA)
- These bodies allocate available spectrum for different uses (eg. military, civil aviation, mobile networks, etc)
  - Three bands reserved for unlicensed use
  - 900MHz, 2.4GHz, 5GHz
- These licenses also stipulate other rules (such as maximum transmission power) for use of these frequencies

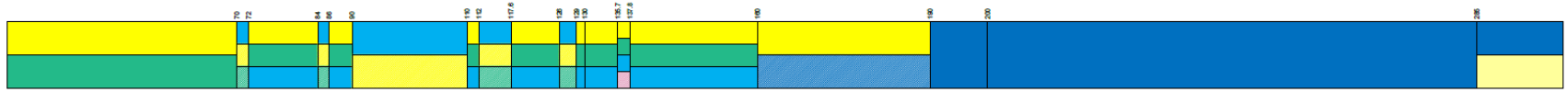
Australian radiofrequency spectrum

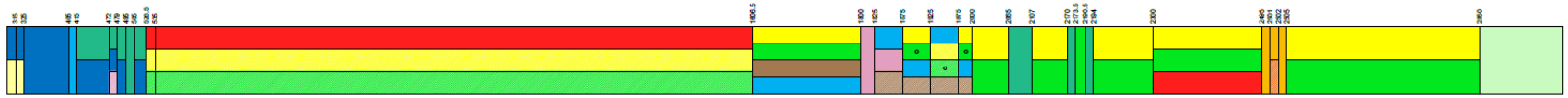
allocations chart

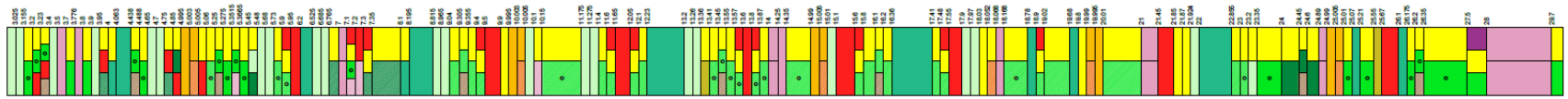
Australian Government

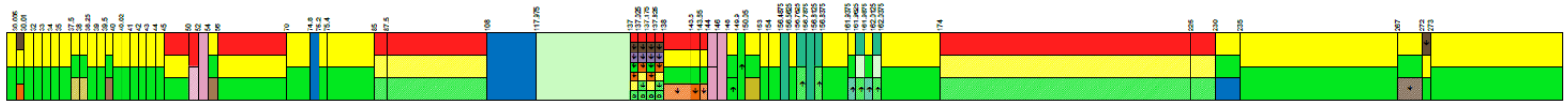
acma

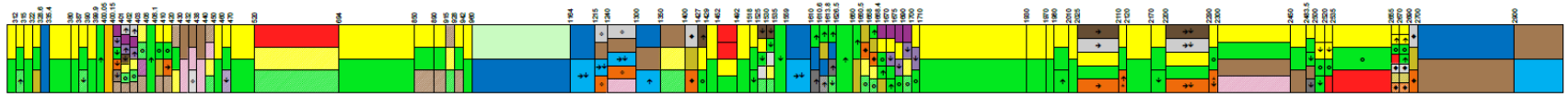
Australian Communications and Media Authority

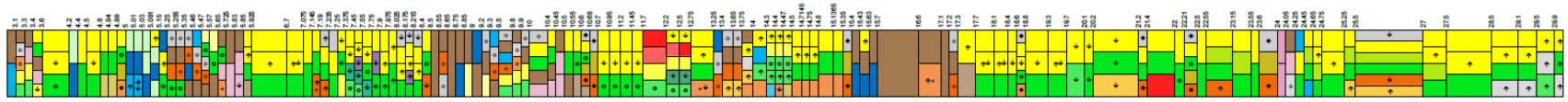


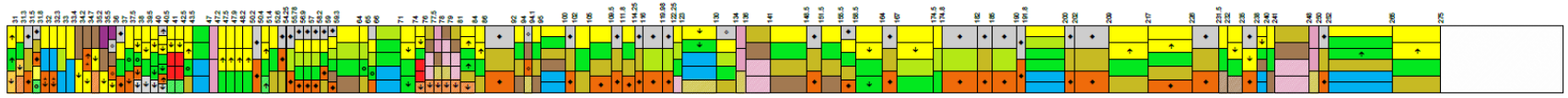












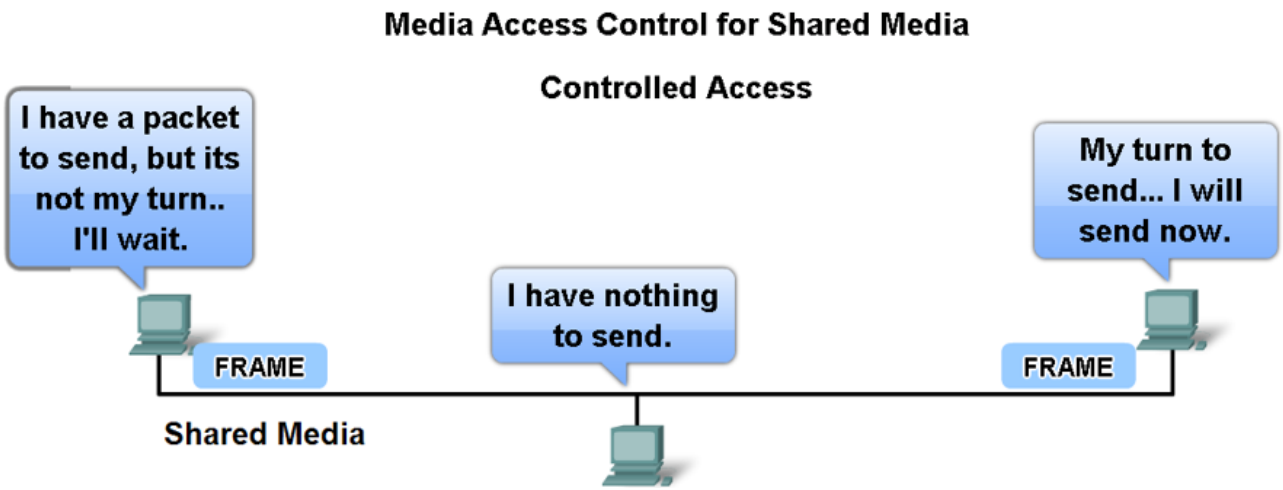
https://www.acma.gov.au/-/media/Spectrum-Engineering/Information/pdf/Spectrum-Chart-2017-pdf.pdf

Media Access Control Revisited

- Two devices transmitting at the same time causes a collision, requiring the message to be re-sent
- There are two common approaches to controlling transmissions over a multi-access network:
- Controlled access
    - Token-based (Token Ring, FDDI)
    - Time Division Multiple Access (GPON, DOCSIS, 3G, HSDPA, LTE)
- Contention-based access
    - Carrier Sense Multiple Access (Ethernet / WiFi)

Controlled Access Revisited

- Controlled Access MAC avoids collisions entirely by ensuring that only one device can transmit at any given time
- This is usually achieved by having devices pass a **token** or sharing time slices



Murdoch UNIVERSITY

Time Division Multiple Access (TDMA)

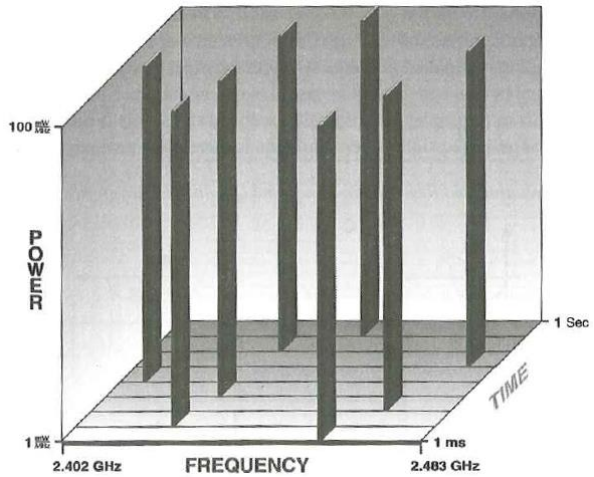
- Transmission time is divided into slots controlled by a central node
    - Usually handled by a point coordinator or cellular tower
- Devices may only transmit in their allocated time slots
- Used by HSDPA, LTE, WiMAX

Frequency Division Multiple Access (FDMA)

- Available spectrum is sub-divided amongst all devices in range
- Each device must only transmit on its allocated frequency
- If the frequencies are not widely spaced, they can still interfere with one another
- FDMA is often used for satellite communications, but can be used to enable full duplex communications

Frequency Hopping Spread Spectrum (FHSS)

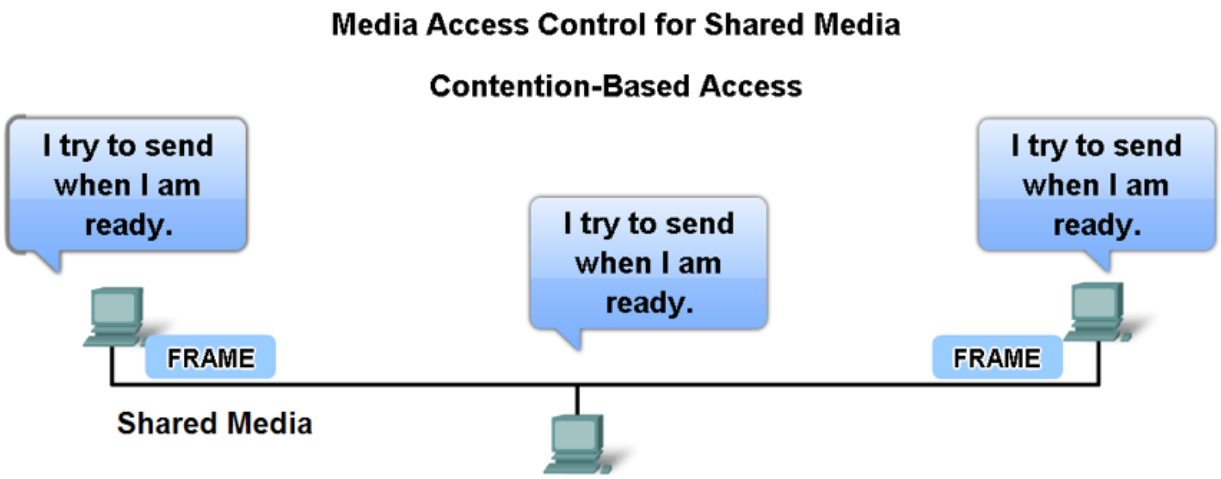
- Used by Bluetooth for medium access
- Technique designed for use in military applications
  - Resistant to jamming
- Divides usable frequency space into 79 channels
- Communicating devices establish random hopping pattern between channels
  - Different devices share medium by using different patterns



Murdoch UNIVERSITY

Contention-based MAC Revisited

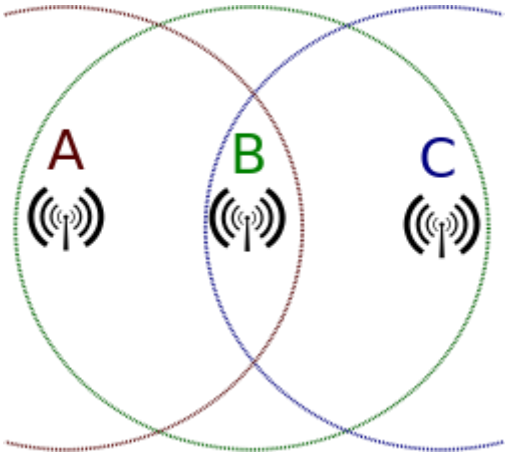
- In contention-based media access control, devices can transmit at (almost) any time
- Usually requires that devices listen for other transmissions before transmitting
- If a device hears an ongoing transmission, it should wait until that transmission is complete before transmitting



Murdoch UNIVERSITY

Carrier Sense Multiple Access with Collision Avoidance

- Wireless devices are unable to reliably detect collisions
  - Difficult to listen and transmit simultaneously
  - Hidden node problem – may not be in range of all devices on the network
- CSMA/CA takes a more conservative approach by attempting to prevent collisions from occurring at all



https://en.wikipedia.org/wiki/Hidden_node_problem

Murdoch UNIVERSITY

Carrier Sense Multiple Access with Collision Avoidance (cont.)

- Waits a random amount of time before sending (preemptive back-off)
- Devices can transmit a notification that they are about to begin a transmission (known as a Request to Send)
    - Prevents other devices from transmitting until the transmission is complete
    - Awaits permission to transmit (Clear to Send)
    - Not active by default due to performance overheads
- Devices also wait for an acknowledgement that the receiver has the frame

Break

When we return: More on WiFi

Murdoch UNIVERSITY

802.11 (WiFi) Standards

Since its introduction in 1997, the 802.11 standard has undergone significant changes.

The original version of 802.11 provided data rates of 1Mbps—2Mbps.

802.11ac allows for speeds up to 1.3Gbps.

802.11

- Original WiFi standard, ratified in 1997
- Provided data rates of between 1Mbps and 2Mbps
- Operated over 2.4GHz spectrum

802.11a

- Ratified by the IEEE in 1999
- Operates on 5GHz spectrum
- Provides data rate of up to 54Mbps
- Introduced Orthogonal Frequency Division Multiplexing (OFDM)
- Never reached widespread adoption

802.11b

- Ratified by IEEE in 1999
- Operates on 2.4GHz spectrum
- Provides data rates up to 11Mbps
- First commonly used WiFi standard

802.11g

- Ratified by IEEE in 2003
- Operated over 2.4GHz spectrum
- Provides data rates up to 54Mbps
- First 2.4GHz 802.11 standard to implement OFDM
- Backwards compatible with 802.11b

802.11n (Wi-Fi 4)

- Ratified by IEEE in 2009
- Operates over 2.4GHz or 5GHz spectrum
- Provides data rates up to 600Mbps
- Introduced Multiple-Input Multiple-Output (MIMO), channel bonding and frame aggregation

802.11ac (Wi-Fi 5)

- Ratified by IEEE in 2014
- Operates over 5GHz spectrum only
- Provides data rates up to 6.9Gbps; current maximum 2.34Gbps (with Wave 2 products only)
- Introduces Multi-User MIMO, wider channels (80Mhz—160Mhz)

802.11ax (Wi-Fi 6)

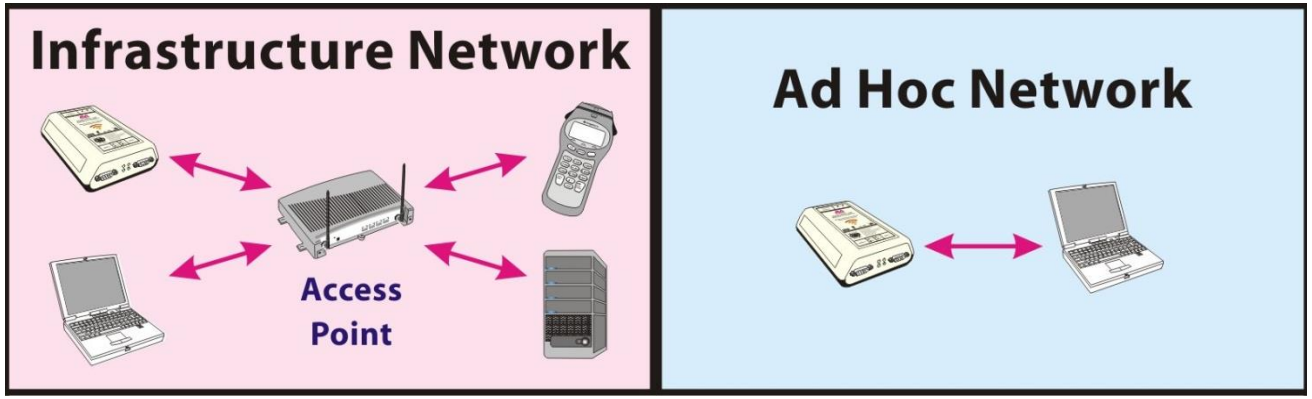
- Currently in development (expected to be ratified in late 2019)
- Operates over 2.4GHz and 5GHz spectrum
- Maximum throughput of 10Gbps
- Improved support for high density environments (numerous clients)

Implementing WiFi Networks

- The exact configuration process for WiFi networks varies from vendor to vendor
- The 802.11 standards specify some standard attributes that must (or should) be set:
    - Network type
    - Service Set Identifier (SSID)
    - Frequency Channel
    - Security

Network Types

- 802.11 networks can operate in two modes: Infrastructure and Ad-Hoc
- **Infrastructure mode** describes networks that have a dedicated wireless access point through which all devices communicate
- In **ad-hoc networks**, devices communicate directly without the need for an access point



Murdoch UNIVERSITY

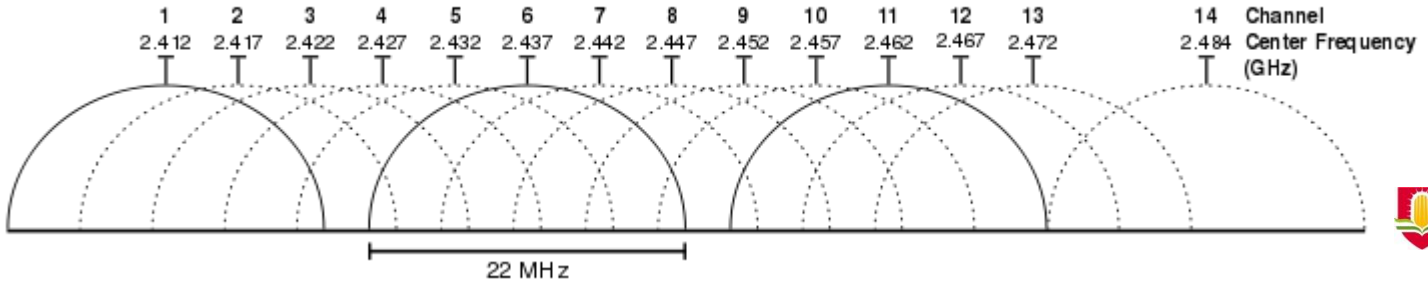
Service Set Identifier (SSID)

- Unique identifier used to distinguish between different WiFi networks
- Usually a string of text (eg. “eduroam”)
- Only needs to be unique among the networks within range

Murdoch UNIVERSITY

2.4GHz 802.11 Channels

- 802.11bgn subdivides the available spectrum to allow multiple WiFi networks to co-exist
- 14 channels available, each 20MHz wide
  - Only 3 of these channels do not overlap
  - Alternate between these channels to avoid overlap in large deployments
- Better propagation and object penetration properties

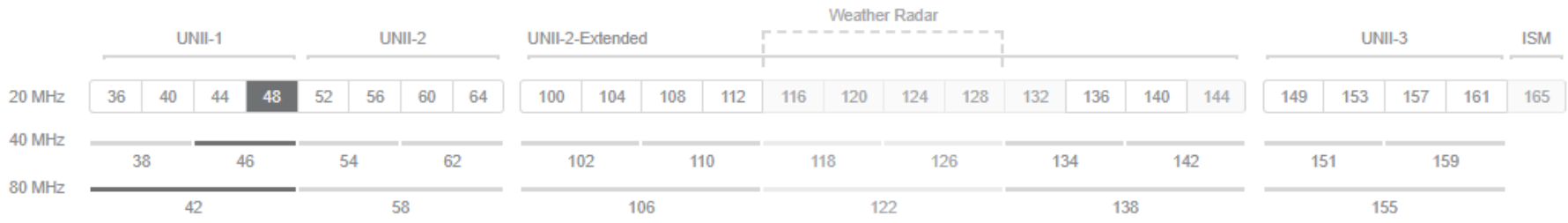


http://en.wikipedia.org/wiki/File:2.4_GHz_Wi-Fi_channels_(802.11b,g_WLAN).svg

Murdoch UNIVERSITY

5GHz 802.11 Channels

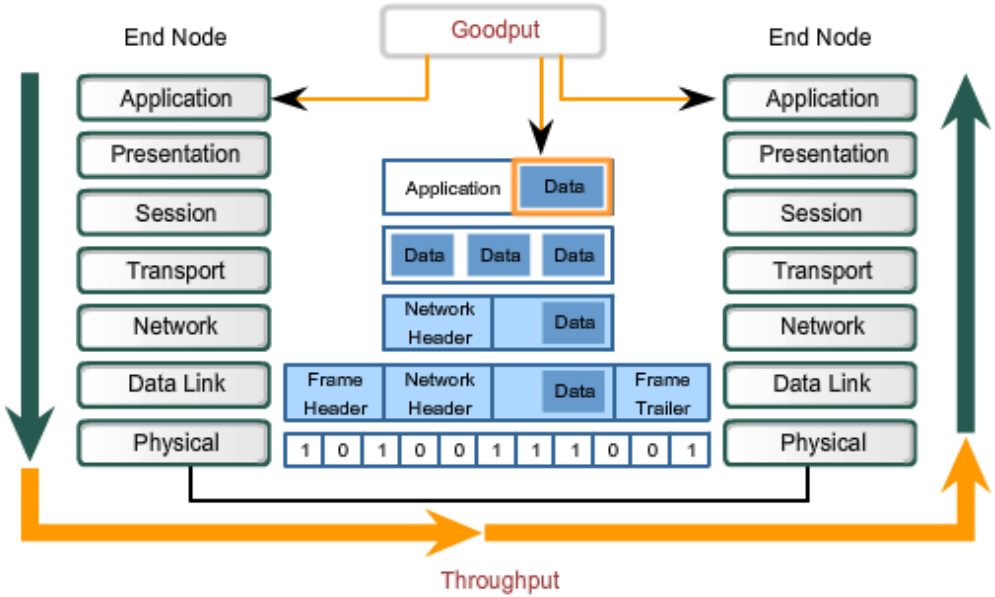
- Used by 802.11an and 802.11ac
- More spectrum available than at 2.4GHz, so up to 24 channels
    - Availability depends on country
    - Channels don’t overlap
- Less crowded than 2.4GHz but range is lower (and worse object penetration)



Murdoch UNIVERSITY

802.11 Performance

- **Link rate** is maximum speed at which data can be sent over link
  - 802.11g has a link rate of 54Mbps
- **Throughput** is total amount of data transferred per second
- **Goodput** is amount of application data transferred per second (without any lower-layer protocol overheads)



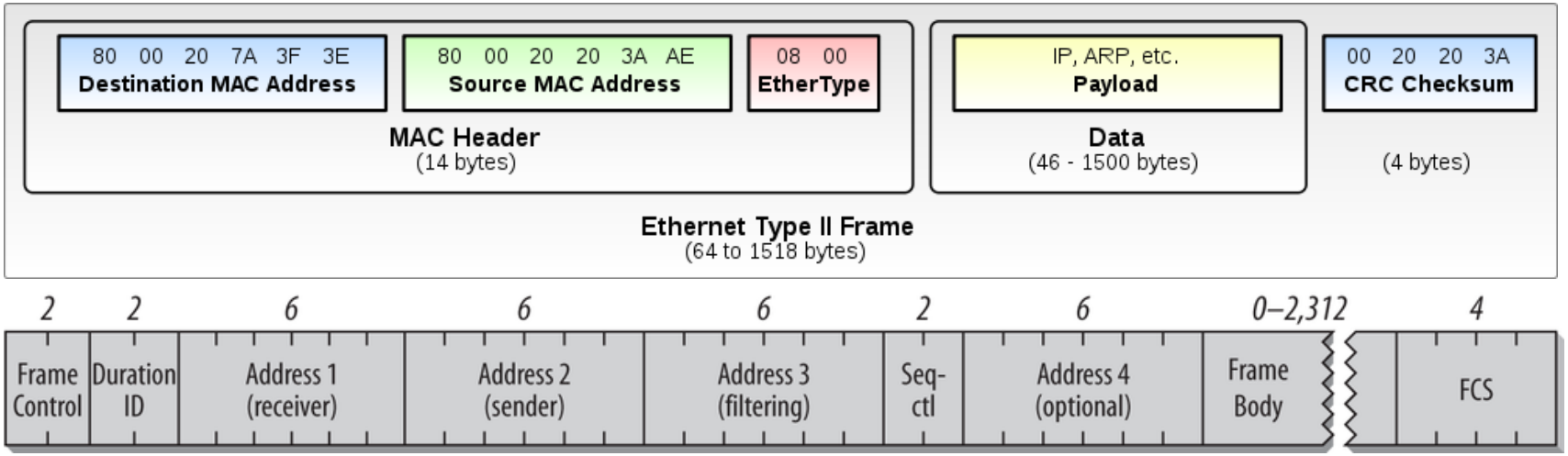
Murdoch UNIVERSITY

802.11 Performance (cont.)

- Throughput and goodput over wireless networks are usually substantially lower than the link rate
- Overheads associated with 802.11 will reduce throughput
  - Link layer acknowledgements
  - Larger packet headers
  - CSMA/CA
- Also easily influenced by channel conditions like
  - Distance from access point
  - Contention from other nearby devices
  - External interference

802.11 Frame Headers

- Additional header fields are needed for wireless
  - Frame control has control information for the Wi-Fi network
  - Duration is described in the standard
  - Address 3 can be used for filtering
  - Address 4 is optional and rarely used
  - Sequence-Control (Seq-ctl) specifies sequence numbering (similar to TCP)



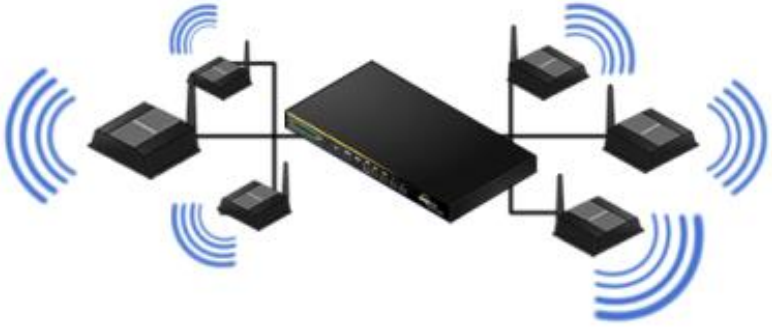
https://www.oreilly.com/library/view/80211-wireless-networks/0596100523/ch04.html

802.11 Security

- WiFi signals can be intercepted more easily than transmissions over wired media
- Two major types of security measures exist:
    - Security through Obscurity (SSID Hiding, MAC Address Filtering).
    - Encryption (WEP, WPA, WPA2, WPA3)
- WPA supports personal (shared password) and enterprise (individual login)

802.11 in the Enterprise

- The configuration options we've discussed must be set on each access point
- Numerous access points are needed to provide coverage over a larger area
- Most Enterprise deployments use a controller-based system
  - Lightweight access points
  - Centralised controller to provide configuration and monitoring
- Controllers can be hardware-based, software-based or cloud managed



Murdoch UNIVERSITY

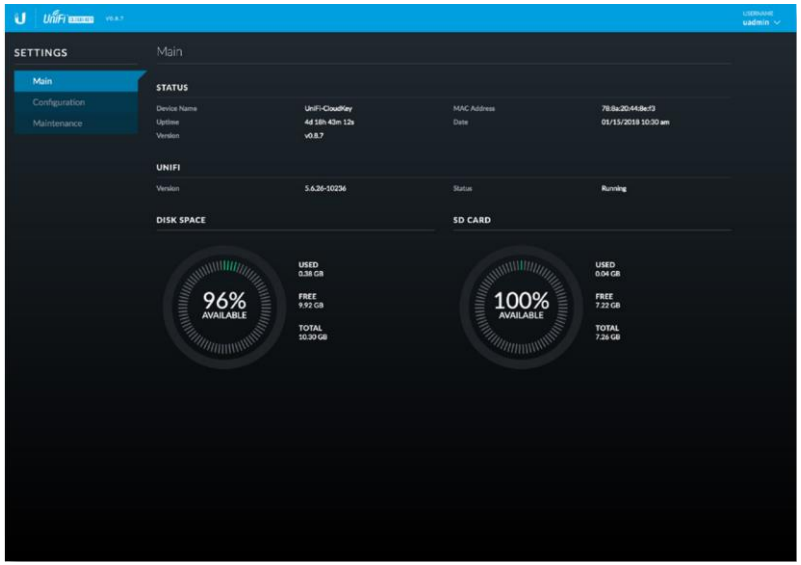
802.11 Hardware Controllers

- Hardware controllers are dedicated pieces of hardware (or hardware modules) that provide management functions
  - High upfront cost
  - Single point of failure
- Cisco and HPE Aruba use this approach

Murdoch UNIVERSITY

802.11 Software Controllers

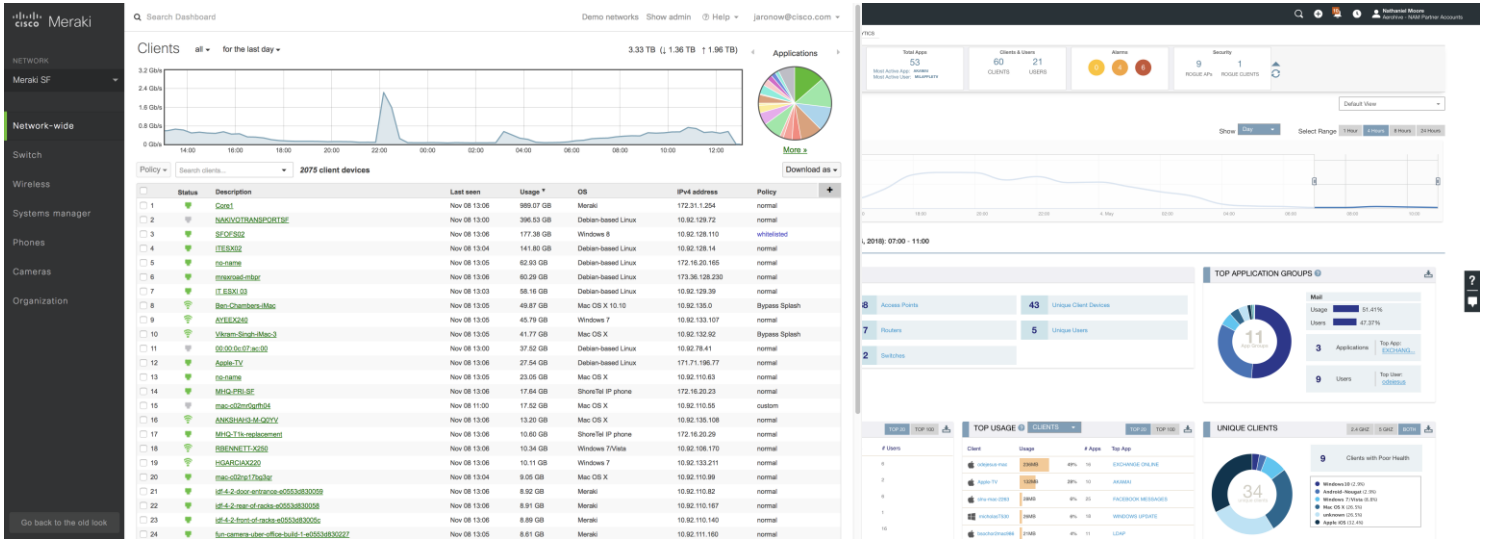
- Software-based controllers are a piece of software that runs on an existing server or workstation
  - Low (or no) additional costs; likely already have hardware
  - Single point of failure still exists
- Ubiquiti Networks uses a software-based controller



Murdoch UNIVERSITY

802.11 Cloud-based Controllers

- Software-based controllers can also be hosted in the cloud
  - Low (or no) upfront costs, but usually involves a subscription fee
  - Hardware may cease to function without a subscription
  - Removes single point of failure
  - Requires Internet connection for management
- Meraki and Aerohive use this approach



Murdoch UNIVERSITY

Lecture Objectives

You should now be able to:

- Describe the motivation for using wireless technologies
- Describe common wireless technologies and their applications
- Differentiate between Personal Area, Local Area and Wide Area wireless networks
- Differentiate between different wireless media access control techniques
- Differentiate between CSMA/CA and CSMA/CD
- Describe the relationship between spectrum use, transmission power and range in relation to wireless networks
- Differentiate between different 802.11 standards
- Describe the limitations of 802.11 performance
- Differentiate between infrastructure and ad-hoc networking in relation to 802.11
- Describe the purpose of the Service Set Identifier in relation to 802.11 networks
- Differentiate between the security mechanisms available to protect 802.11 networks

Lecture Summary and the Week Ahead

- We’ve looked at wireless technologies and applications at length, with a specific focus on 802.11
- Implementation options of 802.11 wireless networks
- Readings for this week are listed on LMS
- In the labs: configuring wireless networking and NAT

Murdoch UNIVERSITY

Next Week

- An introduction to network security and notable security breaches
    - The CIA triangle
    - Categories of attacks
    - Securing your devices

https://hackaday.com/2017/04/01/ask-hackaday-which-balaclava-is-best-for-hacking/

Murdoch UNIVERSITY