THE UNIVERSITY OF
MELBOURNE

COMP30023 – Computer Systems
2019 – Semester 1 - Week 9 – Lecture 2

Medium acess control (MAC)

Dr Lachlan Andrew

Recap

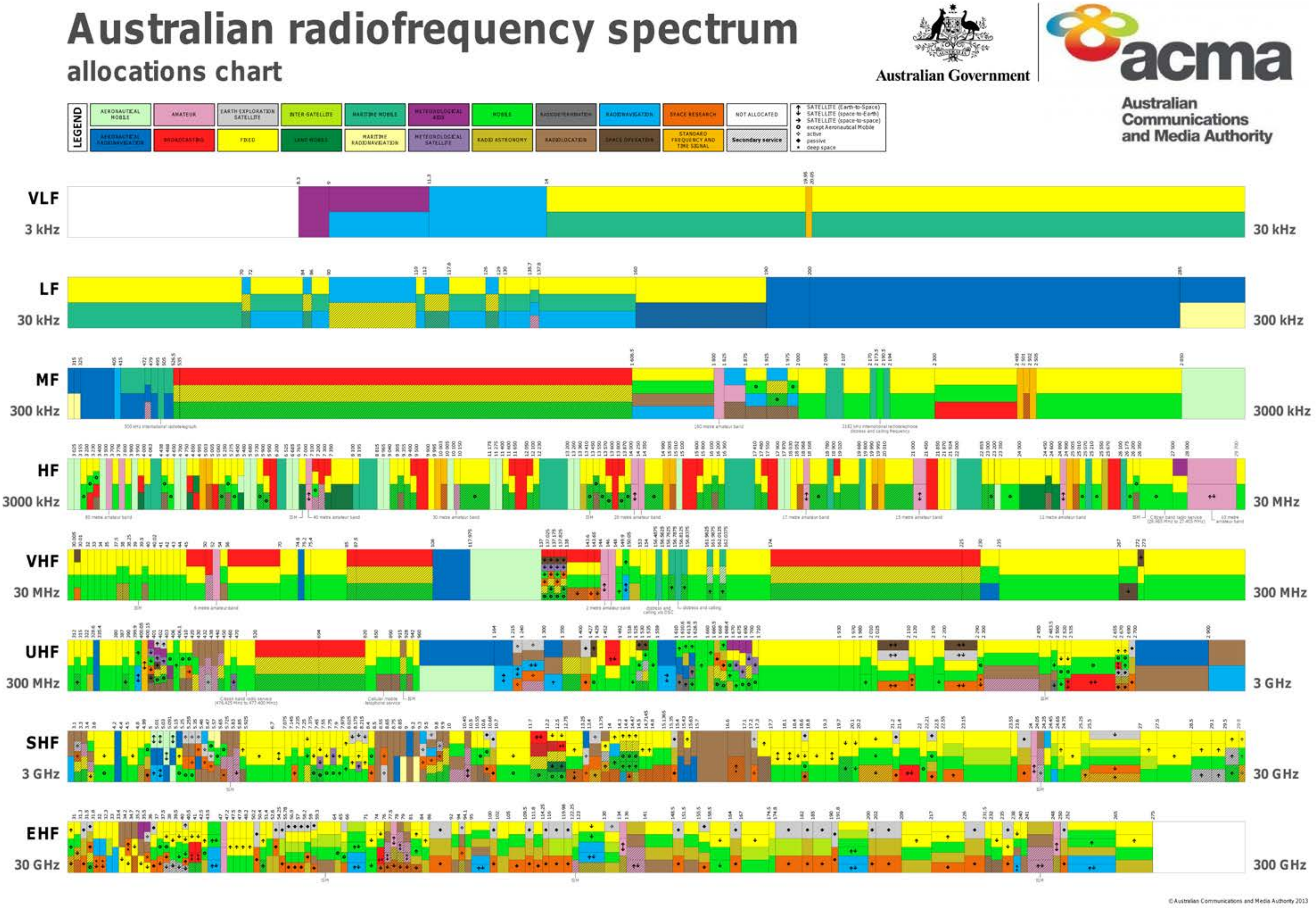
- Network address translation (NAT)
- Fragmentation

Medium Access Control

- We now consider a special type of network
- No point-to-point links
- Broadcast, and everyone hears
  - “Shared medium” networks
- Main challenge: Who gets to broadcast when?

Example: Wireless Communication

- Wireless uses radio waves to communicate
  - Such waves operate at a specific frequency
  - Different frequencies are reserved for different purposes, some are open and some are restricted
  - Within a frequency band (think of it as a block) there could be a number of channels operating, each with a subdivision of the frequency band as whole
  - Adjacent channels and frequencies tend to interfere with each other, careful channel and frequency selection is sometimes necessary



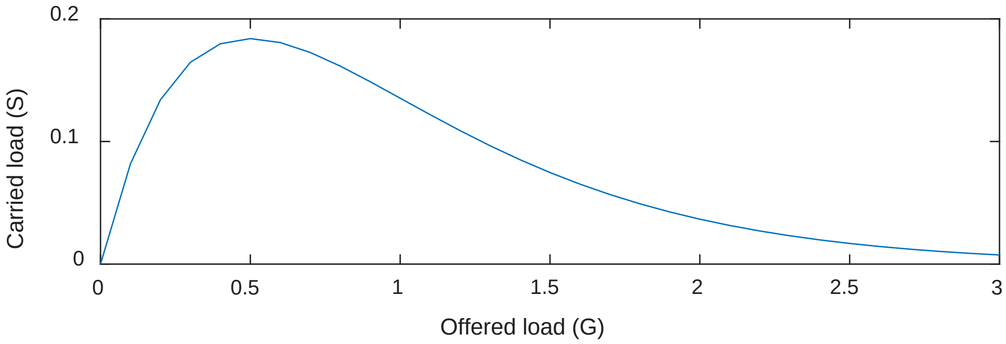
https://www.acma.gov.au/-/media/Spectrum-Transformation-and-Government/Publication/pdf/spectrum_chart2013-pdf.pdf

Aloha

- 1960s, University of Hawai'i needed a network
- Wireless
- Just transmit whenever you have data

  → Collisions
- Acknowledge packets, resend those not acknowledged
- "Offered traffic" (G) vs "carried traffic" (S)
  - "Offered" includes collisions
  - Simple model

    $S = Ge^{-2G}$



Aloha

- Maximum link utilization 18%
  - On average, collide with one other packet
  - Offered load G=1/2
- Must wait for a timeout before retransmitting
- Transmission can take many attempts
- Simple!
- Repeaters extend the range
  - Device that receives, amplifies and retransmits signals

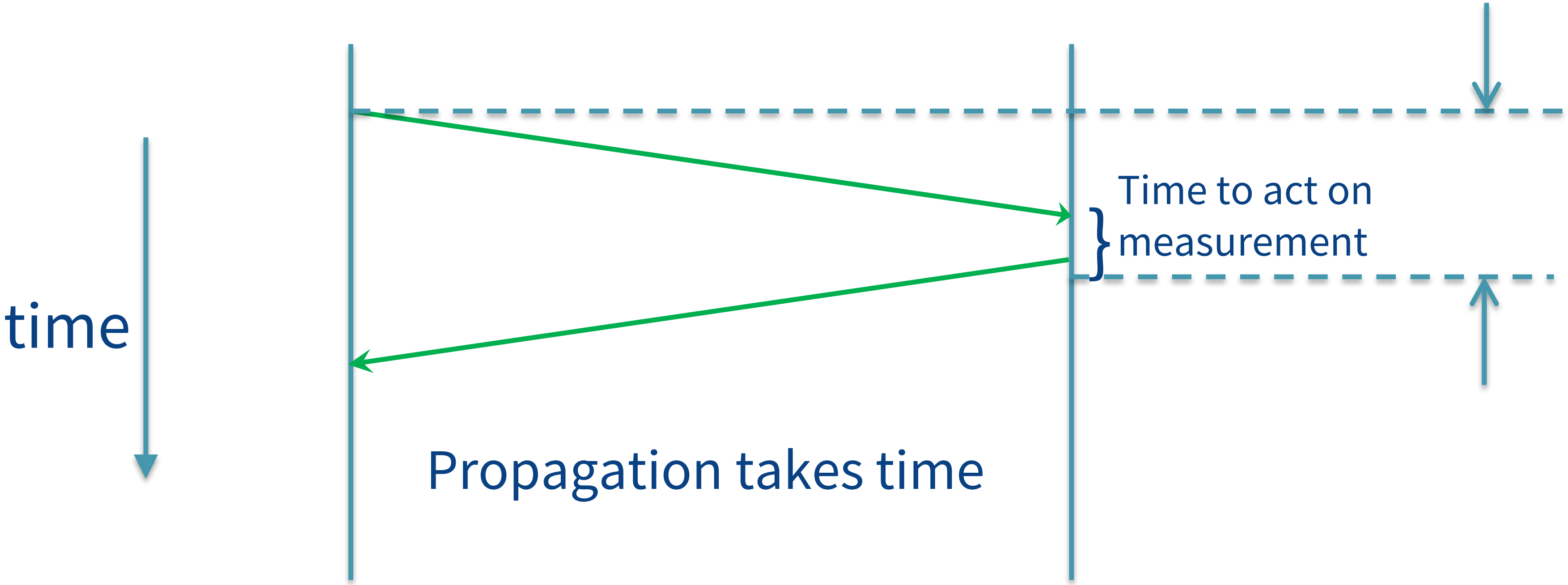
CSMA

- Obvious way to reduce collisions:
  - Don’t start transmitting if someone else is already
- “Carrier-sense multiple access” (CSMA)
- “Listen-before-talk”

- More complicated electronics was a problem back then
- Used in today’s descendants of Aloha

Still some collisions

- Even with CSMA, collisions occur if two nodes start transmitting at “the same” time
- How similar do the times have to be?



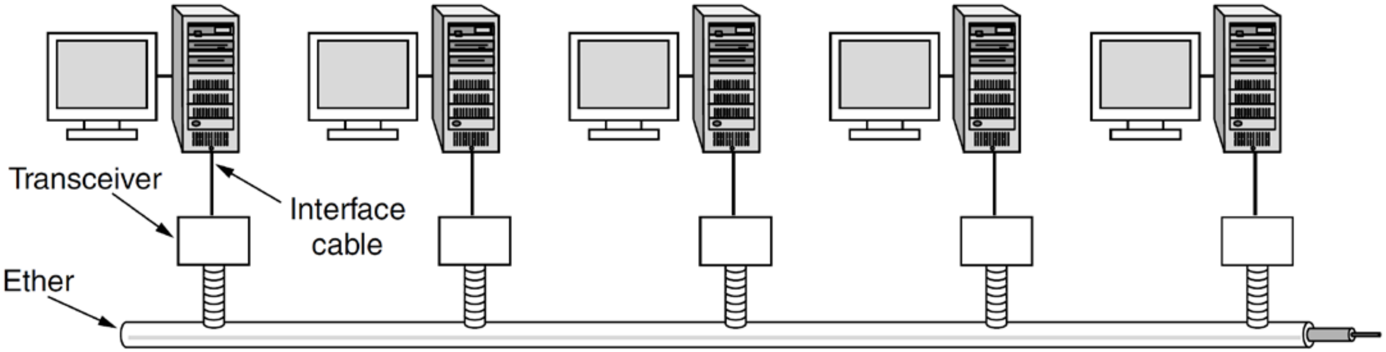
Collision detection

- If collisions can’t be avoided, what else can we do?
- Minimise the cost of collisions
  - Stop the collision before the whole packet is sent
  - Retransmit without waiting for a timeout

- Carrier sense multiple access with collision detection
  - CSMA/CD

Classic Ethernet

- First created in 1976 – Metcalfe and Boggs at Xerox PARC
  - 3 Mbps using a single coaxial cable
- Standardised in 1978 by DEC, Intel and Xerox (DIX) eventually becoming the 802.3 standard in 1983
- Xerox showed no interest in commercialising it, so Metcalfe formed his own company, 3Com

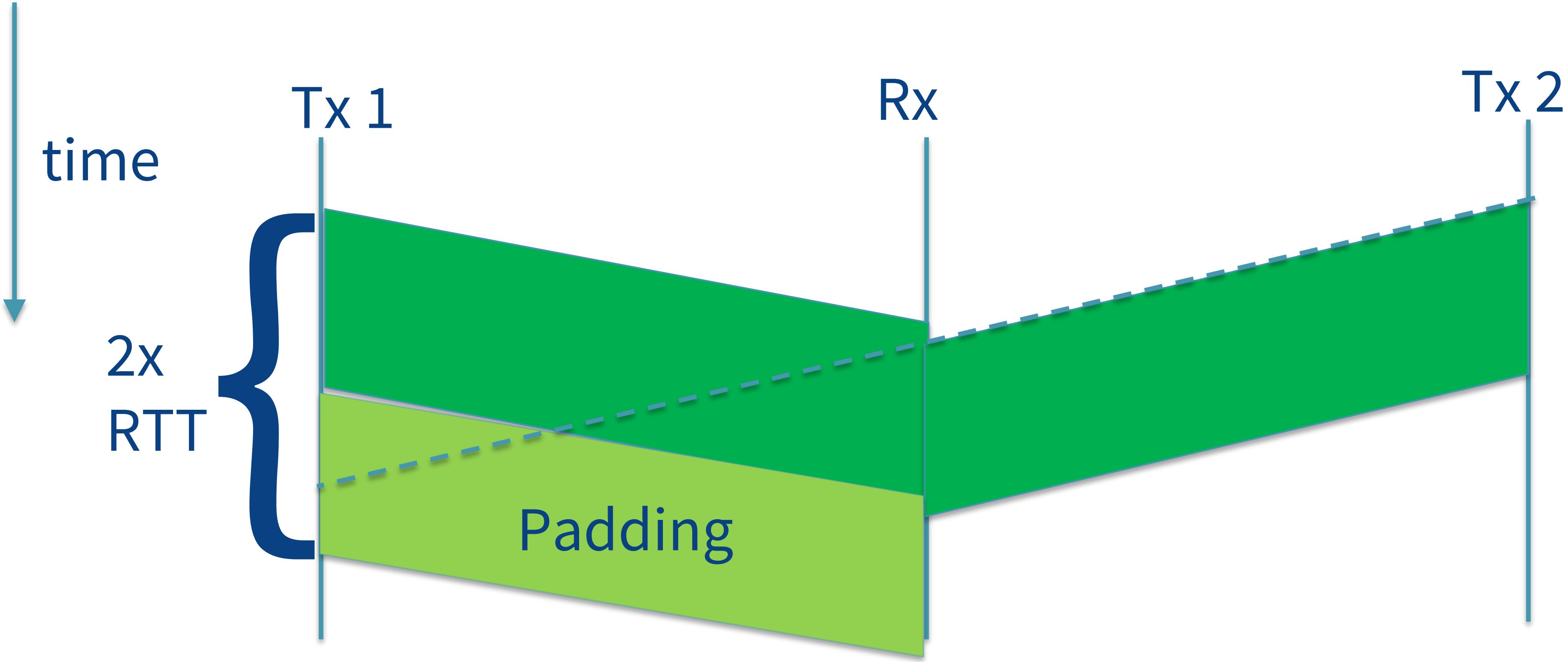


Early Ethernet

- In 1973, Bob Metcalf at Xerox PARC described Ethernet
  - PARC invented many great things that others commercialized
  - Notable example: the windows/icons/menus/pointer GUI
- Used CSMA/CD to connect Alto computers to laser printers
- Standardised in 1980s as IEEE 802.3

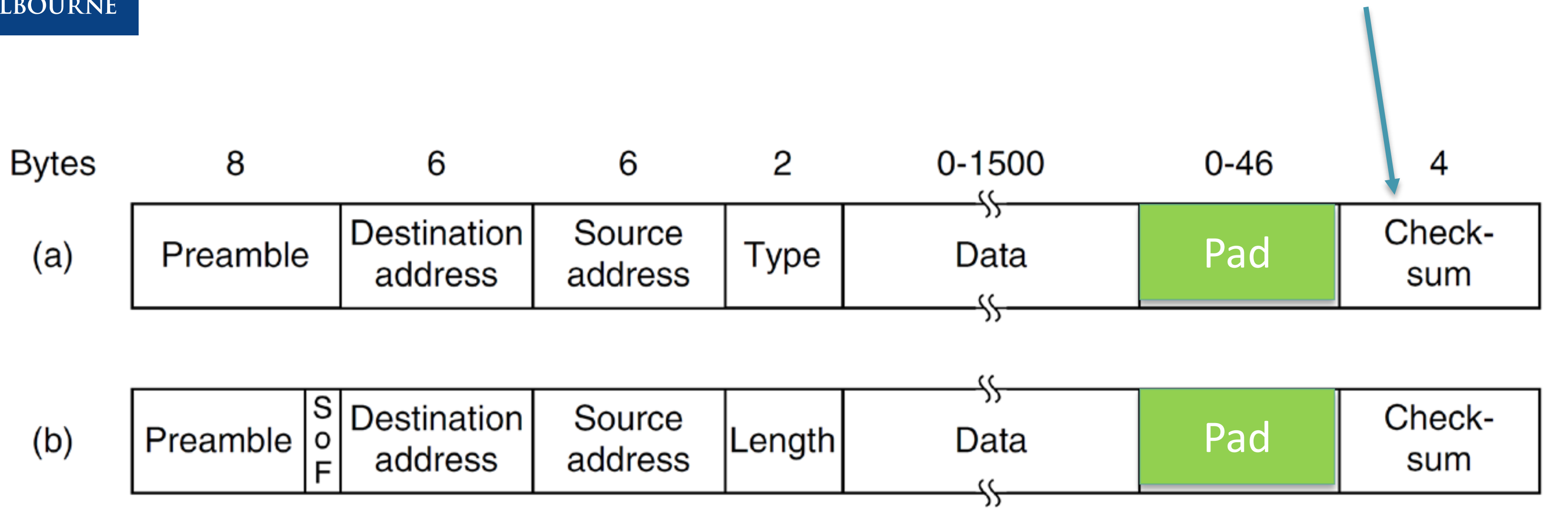
How collision detection works

- What matters is collisions at the *receiver*, not transmitter



Ethernet Frames

Vital: Link layer frames are often corrupted, especially by collisions



Bytes	8	6	6	2	0-1500	0-46	4
(a)	Preamble	Destination address	Source address	Type	Data	Pad	Check-sum
(b)	Preamble SoF	Destination address	Source address	Length	Data	Pad	Check-sum

a) Ethernet (DIX), b) IEEE 802.3

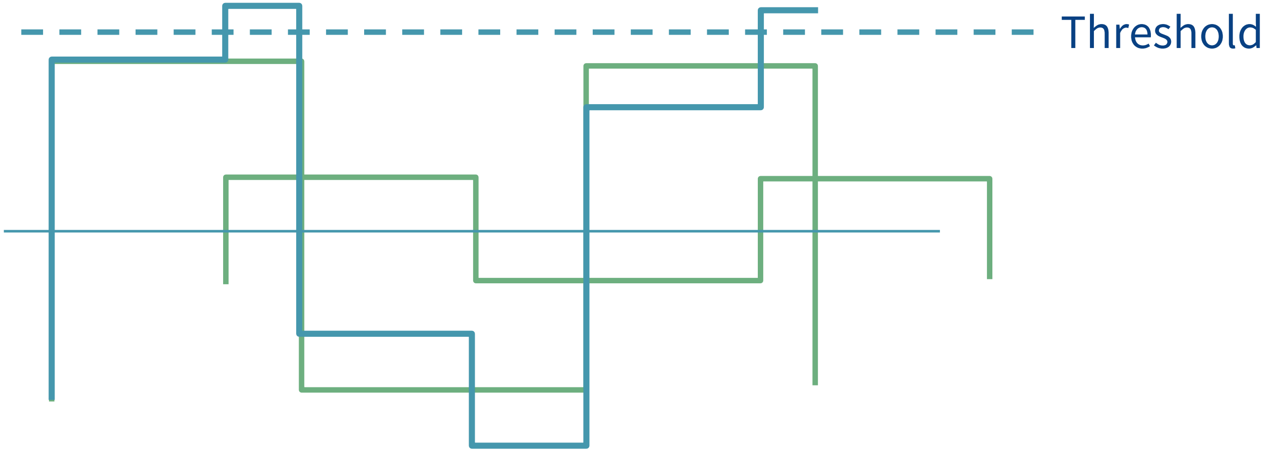
Higher bit rates don’t reduce minimum packet duration.

High-speed or long distance CSMA/CD doesn’t work

Modern “ethernet” is totally different

How are collisions detected?

- Must be detected at the *transmitter*
- Measure sum of my signal + theirs, attenuated
- If that exceeds a threshold, a collision occurred
- Need a clear gap between receive strength and noise

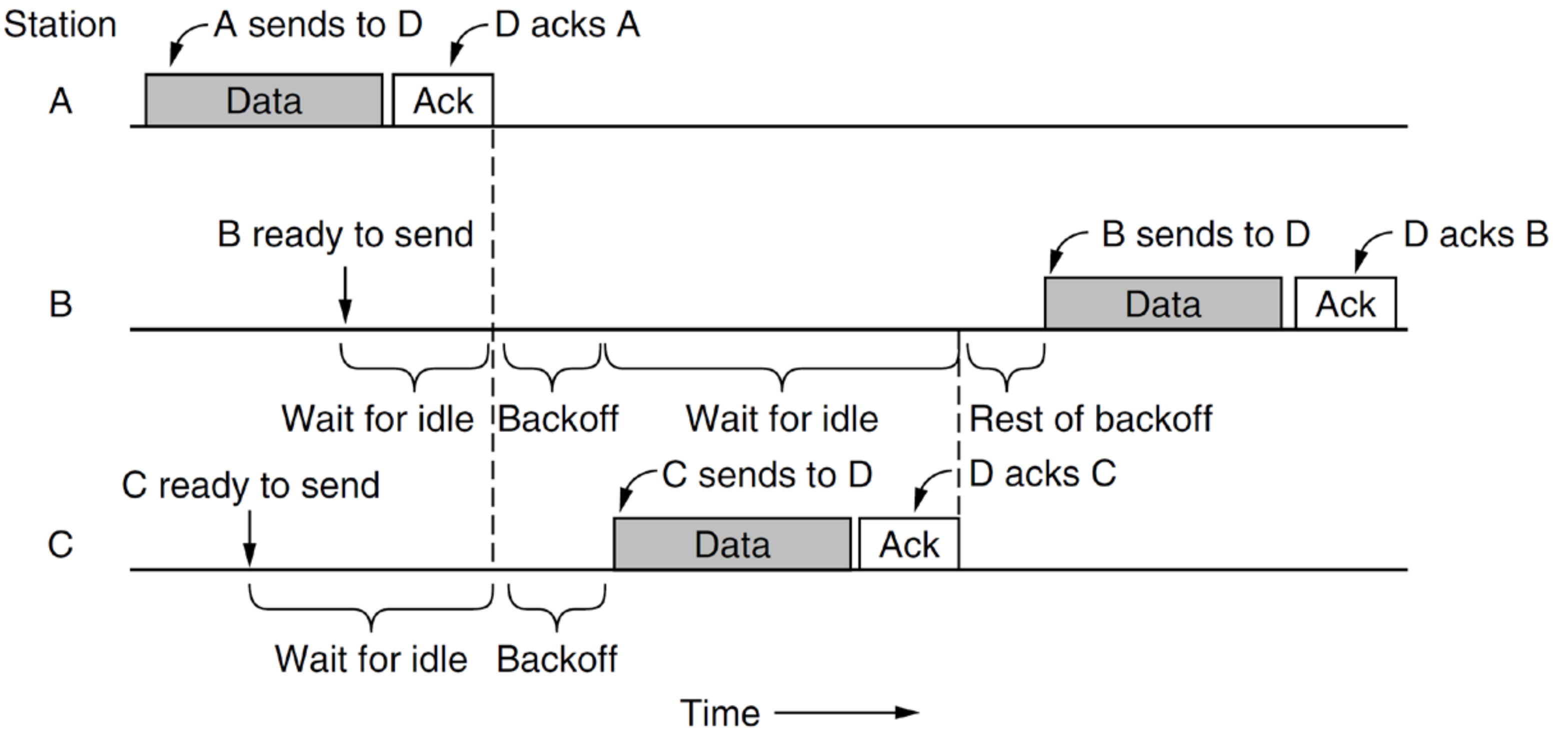


Wireless collisions

- Could this have been used in Aloha?
- No
  - Transmit power up to 100 mW
  - Receive power as low as 10^{-8} W – 10,000,000 times smaller

- WiFi (IEEE 802.11) cannot use CSMA/CD

CSMA/CA – WiFi MAC



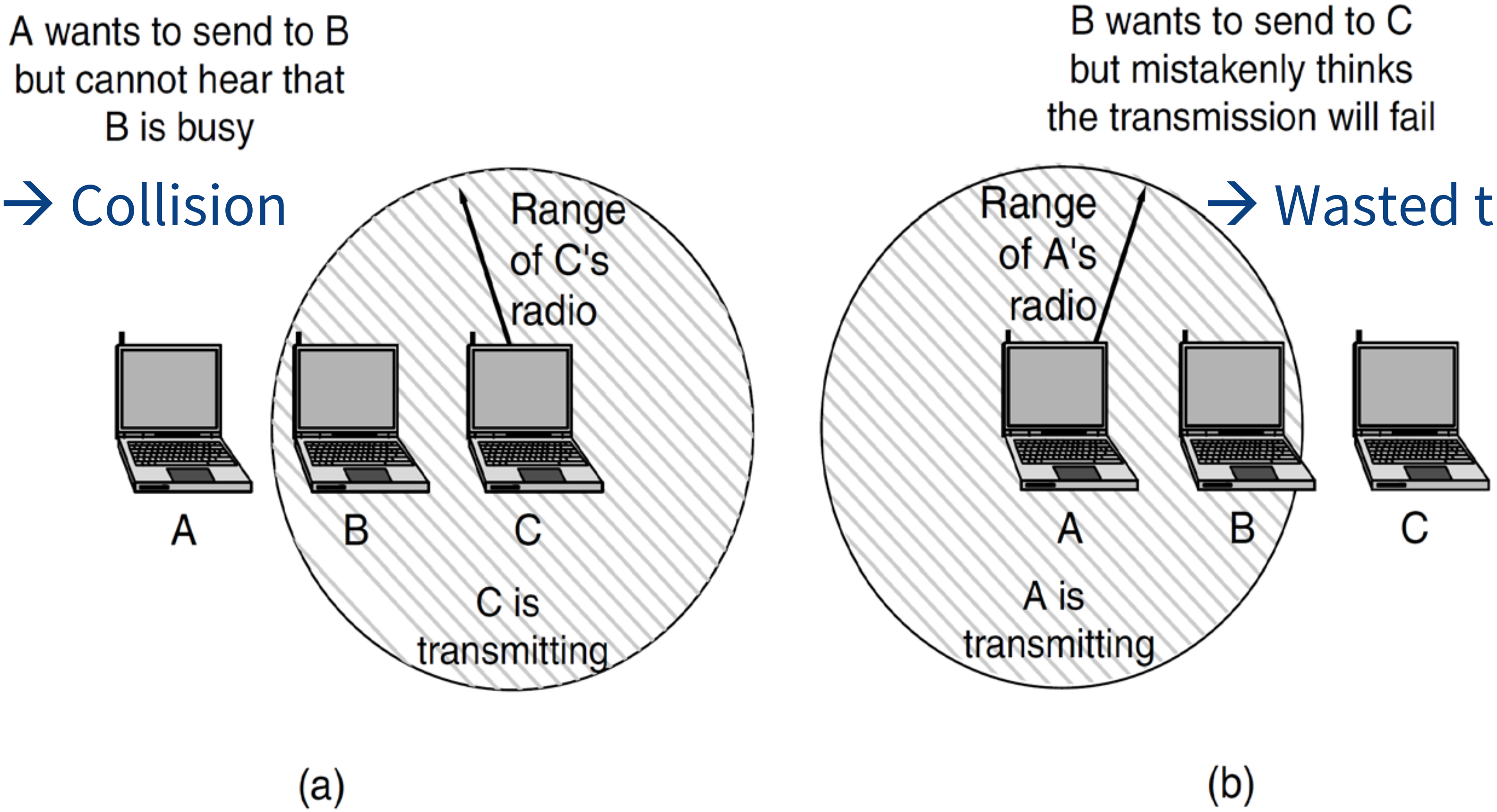
CSMA/CA – WiFi MAC

- A station wanting to transmit chooses a value uniformly at random from its initial “contention window”, CWmin
- While the channel is idle, it counts down from this value
- When the counter reaches 0, the station transmits
- If the packet is received correctlythe receiver sends an ACK
- If the sender does not receive an ACK, then
  - It doubles it CWs (“binary backoff”)
  - Repeats the process
  - Eventually gives up, and packet is lost

CSMA/CA vs CSMA/CD

- CSMA/CA requires ACKs – CDMA/CD did not use them
- Ethernet assumed most collisions could be detected
  - Can limit maximum segment length (attenuation, time)
  - Transport layer recovers the rest
  - Slow (timeout, 3 dup ACK), causes TCP CWND reduction
- Wireless CSMA/CA cannot detect collisions
  - Dynamic range problem mentioned earlier
  - Can’t limit segment size
    - Nodes scattered over entire suburbs
      - Networks with different SSIDs (names) still share the same channel
    - Can’t even guarantee CSMA works, giving…

...Hidden / exposed terminals

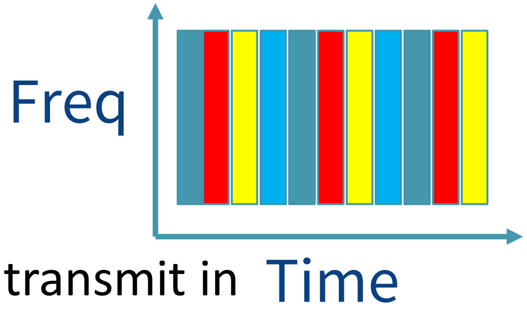


→ Collision

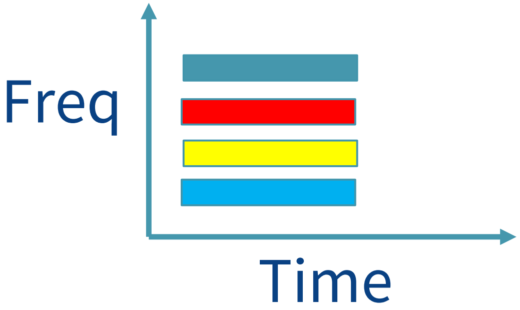
→ Wasted time

Alternatives: “circuit” switching

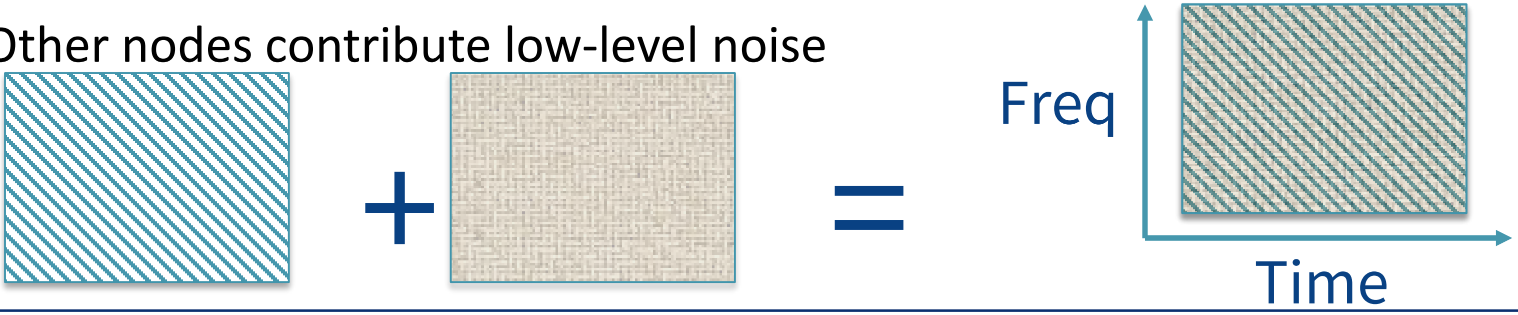
- Time division
  - Time is divided into slotted frames
  - Each node has a fixed slot within the frame to transmit in



- Frequency division
  - Frequency band is divided into channels
  - Each node has a fixed channel to transmit in



- Code division / spread spectrum
  - Each node smears data over time and frequency in a different way
  - Other nodes contribute low-level noise



There even if nothing to send

Alternatives

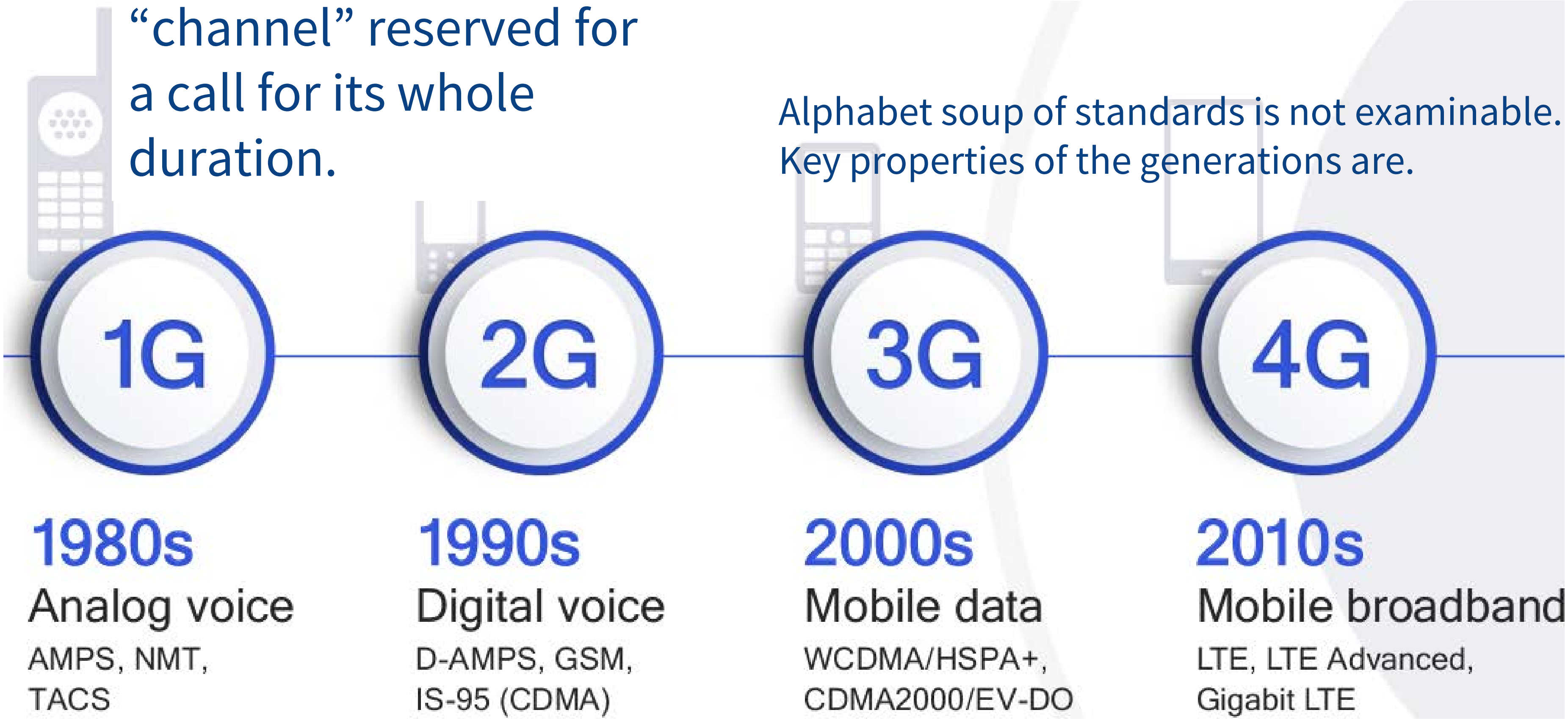
- Reservation
  - Dynamic time division
  - Still need a way to make reservations
- Polling
  - Central controller asks each slave “do you have data”
- Token passing
  - One node at a time has permission to transmit (802.5, 802.4, 802.12)
  - After transmission, the permission (“token”) is passed to the next node

Mobile phone protocols

Circuit switched: "channel" reserved for a call for its whole duration.

Packet switched

Alphabet soup of standards is not examinable.
Key properties of the generations are.



1G
1980s
Analog voice
AMPS, NMT, TACS

2G
1990s
Digital voice
D-AMPS, GSM, IS-95 (CDMA)

3G
2000s
Mobile data
WCDMA/HSPA+, CDMA2000/EV-DO

4G
2010s
Mobile broadband
LTE, LTE Advanced, Gigabit LTE

Figure © Qualcomm

5G MAC

- Specified by 3GPP ("Third Generation Partnership Project")
  - ITU-T specified 1G to 3G
  - Their processes are slow, so industry took over
- Contention (CSMA) used to make an association
- Once associated, *short* slot is used to make reservations

Link Layer – Wireless LANs

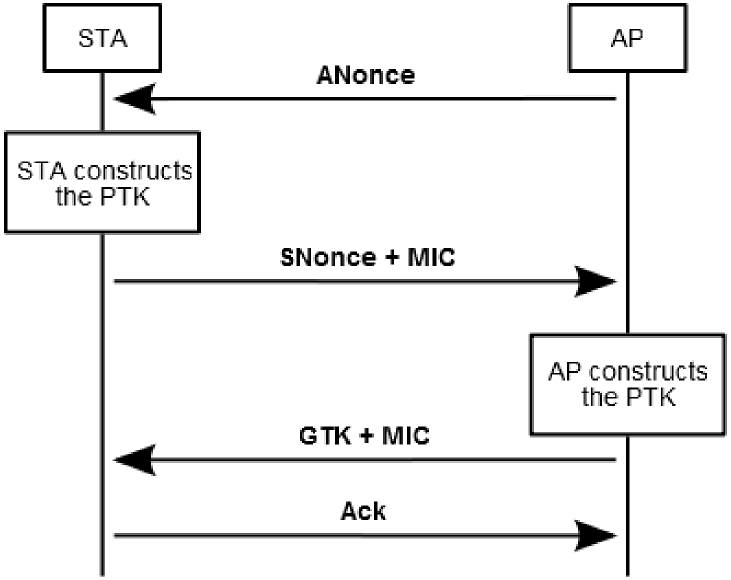
- 802.11b – 11Mbps running in the 2.4-Ghz band
- 802.11g – 54Mbps running in the 2.4-Ghz band
- 802.11a – 54Mbps running in the 5-Ghz band
- 802.11n – multiple antennas – 4 antennas gives up to 600Mbps
- 802.11ac – multiple antennas – 8 antennas gives up to 1300Mbps
- The 2.4-Ghz and 5-Ghz bands are unlicensed (unlike mobile frequencies, which are very expensive to buy) and free to use with certain power limits (1 W)
  - This means many devices other than WiFi networks use the bands – including cordless phones, garage door openers, microwave ovens, etc.

802.11 Security

- Authentication and Security tied together
  - In the same way as a wired connection frames can be blocked and spoofed – requires being able to overpower the original signal
- Open – no authentication or encryption
  - All traffic is visible
- WEP – Wired Equivalent Privacy
  - Key is 40 – 100 bits – RC4 encryption
  - Easy to crack by capturing packets
    - (40,000 packets – 3 mins to capture – 3 seconds to crack key)
- WPA – WiFi Protected Access
  - Temporal Key Integrity Protocol (TKIP) – each packet has a unique key
  - Attacks focused on recovery of small amounts of data – not access
  - Best access attacks were directed at brute forcing weak passwords

802.11 Security

- WPA2 – Updated version of WPA
  - Uses AES to counter the weakness in WPA1
  - Was considered secure until KRACK attack in 2017: https://www.krackattacks.com/
- KRACK attack was against the WPA2 protocol, not a specific implementation
  - Key reinstallation attack – keys should only be used once, otherwise they are susceptible to attack
  - The attack was against the 4-way handshake used in WPA2 to negotiate a key. The third message may be resent in case of loss, each time the client received message 3 it would reinstall the key, causing a reuse of key material



Acknowledgement

- The slides were prepared by Lachlan Andrew based on material developed previously by: Chris Culnane Michael Kirley, Zoltan Somogyi, Rao Kotagiri, James Bailey and Chris Leckie.
- Some of the images included in the notes were supplied as part of the teaching resources accompanying the text books listed in lecture 1.