Virtual Circuit, Wireless, Spanning Tree

11 December 2024
Lecture 6

Some Slides Credits: Steve Zdancewic (UPenn), Kurose and Ross

Topics for Today

- Virtual Circuit Routing
- 802.11 Wireless
- Bridges and Spanning Tree Algorithm

Virtual circuit approach

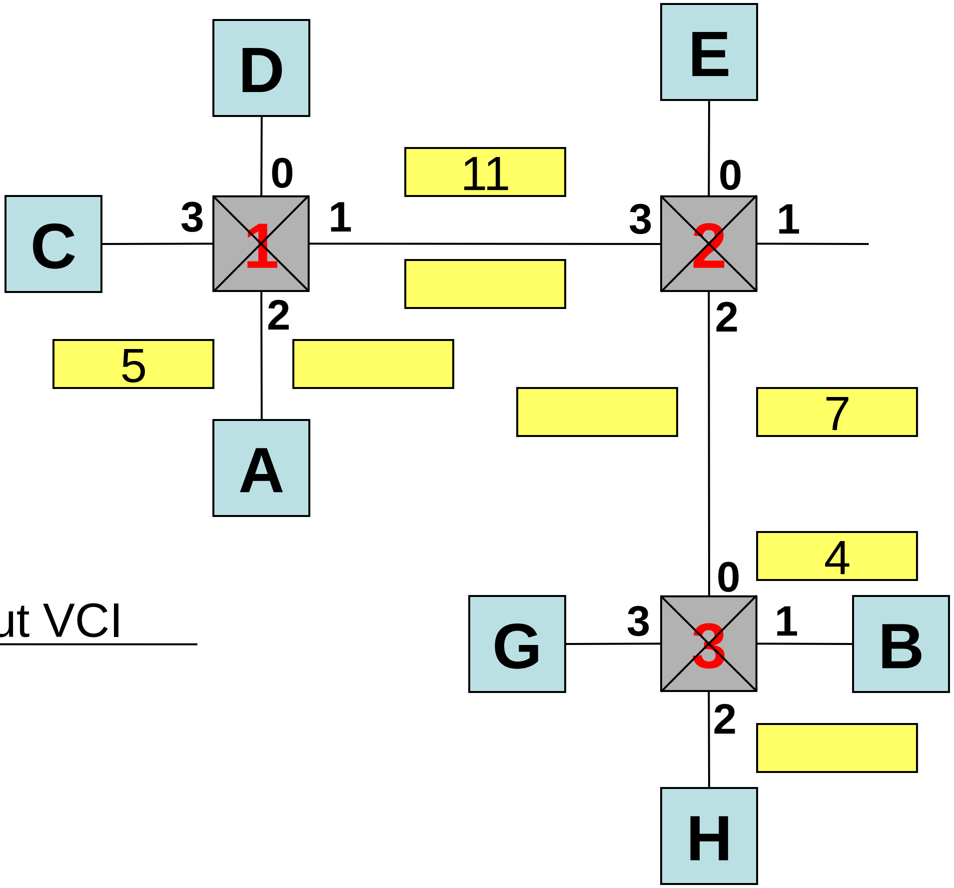
- Set up the connection before data transfer
  - Allocate resources on circuits
  - Set up forwarding tables

- Benefits of virtual circuit approach
  - Performance: per-packet switching cost is low
  - Reliability: predictable latency and throughput
- Drawbacks
  - Setup time is long
    - At least one RTT – why?
  - Fault tolerance
    - What if the circuit fails during the transmission?

Virtual Circuit Switching

- VCI = Virtual Circuit Identifier
- Incoming port + VCI uniquely identify virtual circuit
- Setup phase constructs circuit table entries at each switch

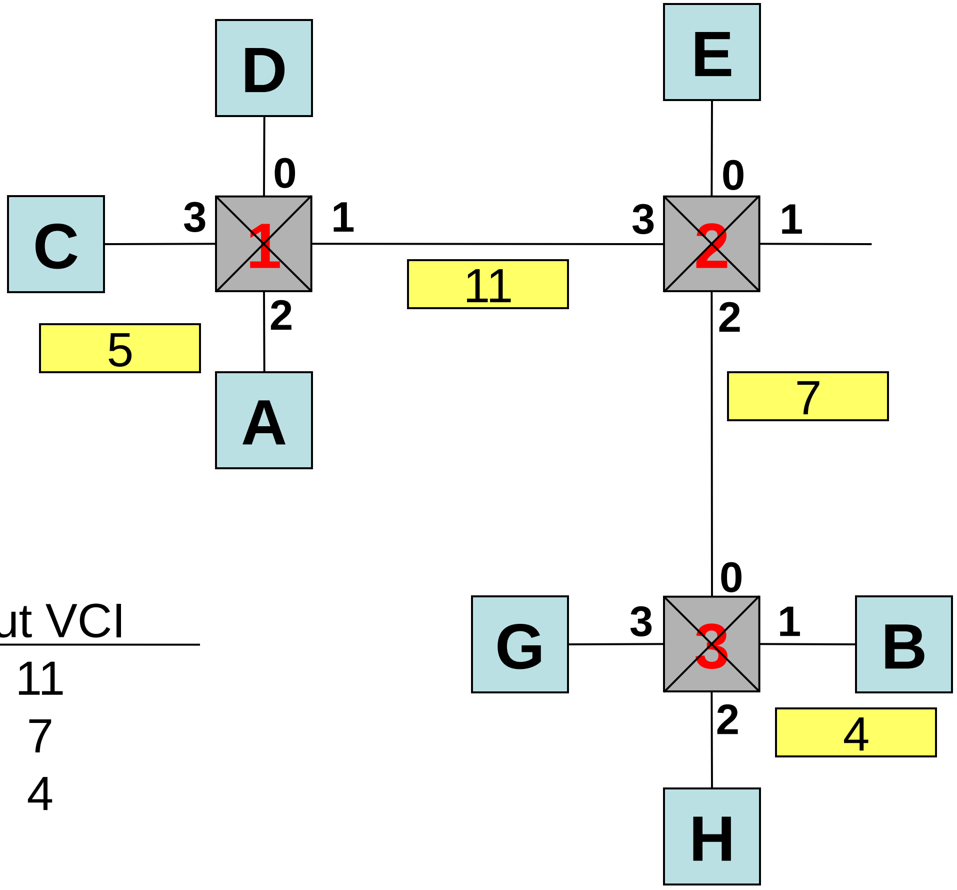
A wants to send to B



Switch	In Port	In VCI	Out port	Out VCI
1				
2				
3				

Virtual Circuit Switching

- VCI = Virtual Circuit Identifier
- Incoming port + VCI uniquely identify virtual circuit
- Setup phase constructs circuit table entries at each switch



Switch	In Port	In VCI	Out port	Out VCI
1	2	5	1	11
2	3	11	2	7
3	0	7	1	4

Datagram versus Virtual Circuit

Datagram

Advantages:

1. Messages have no setup cost.
2. Routing table size depends on the number of nodes, not number of conversations.
3. Faster recovery from network failures.

Disadvantages:

1. Networks with many nodes have slow table lookup.
2. Packet 2 takes just as long to route as packet 1.

Virtual Circuit

Advantages:

1. Routing table size depends on number of conversations.
2. Can configure the circuit once and future messages can route very fast.
3. Save space in packet header.

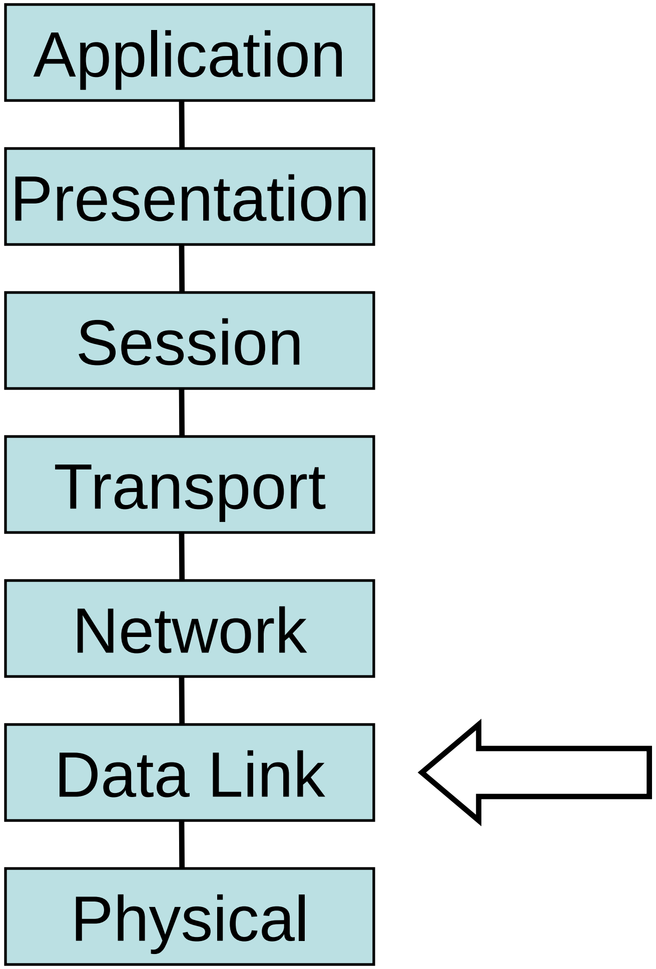
Disadvantages:

1. Dynamic setup is costly (1 round trip).
2. Slower to recover from failures.
3. Can't easily route around problems.
4. Bootstrapping requires existing tables.

So Far

- Virtual Circuit Routing
- 802.11 Wireless
- Bridges and Spanning Tree Algorithm

OSI Reference Model



Next: Wi-Fi

Wireless (802.11)

Like Ethernet, 802.11 has shared medium

- Need MAC
- Uses exponential backoff

Unlike Ethernet, in 802.11

- No support for collision detection
- Not all senders and receivers are directly connected

Background

Number of wireless (mobile) phone subscribers now exceeds the number of wired phone subscribers!

Computer networks

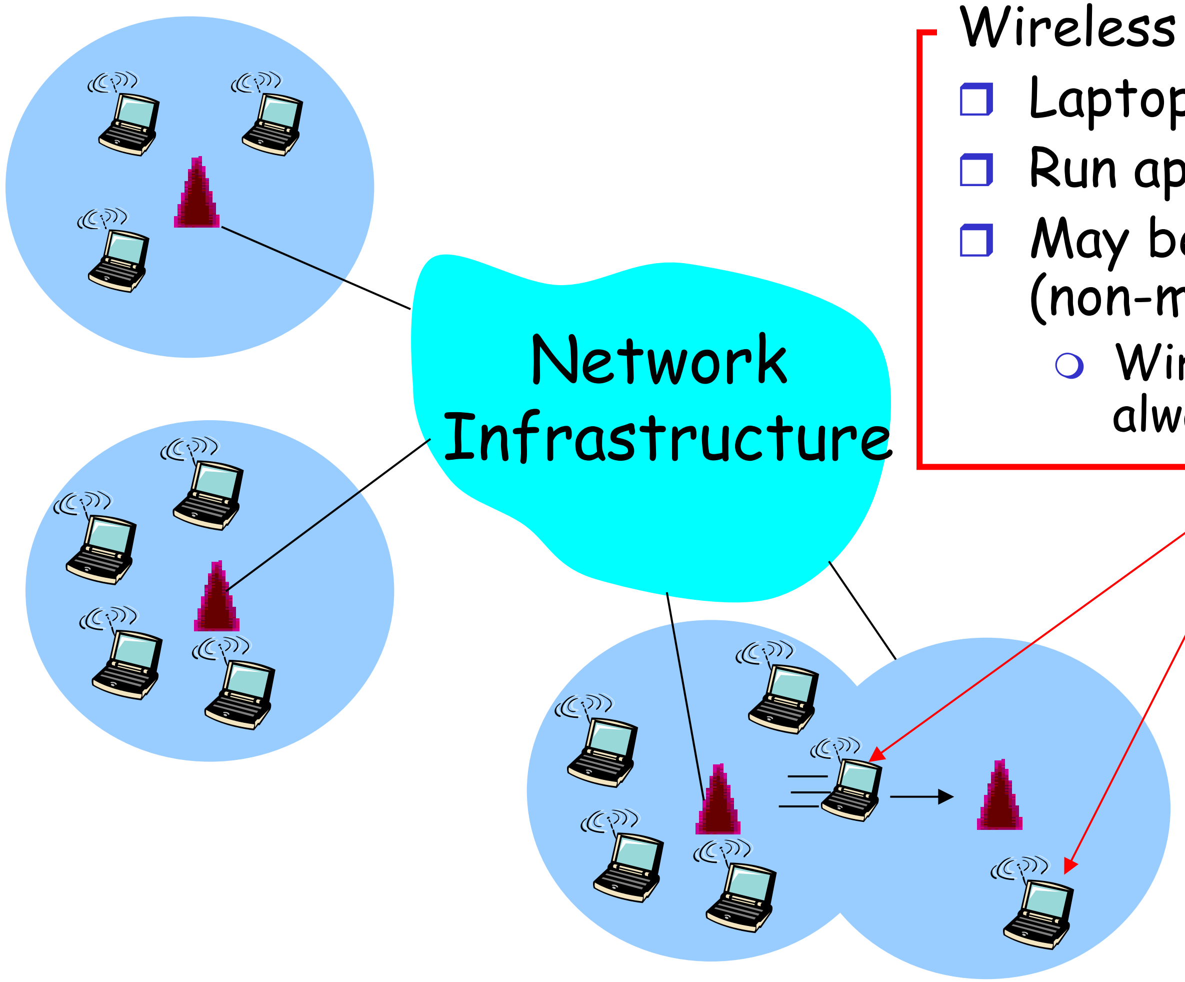
- laptops
- palmtops
- PDAs
- Internet-enabled phones

Promises anytime untethered Internet access

Two important (but different) challenges

- *Wireless:* communication over wireless link
- *Mobility:* handling the mobile user who changes point of attachment to network

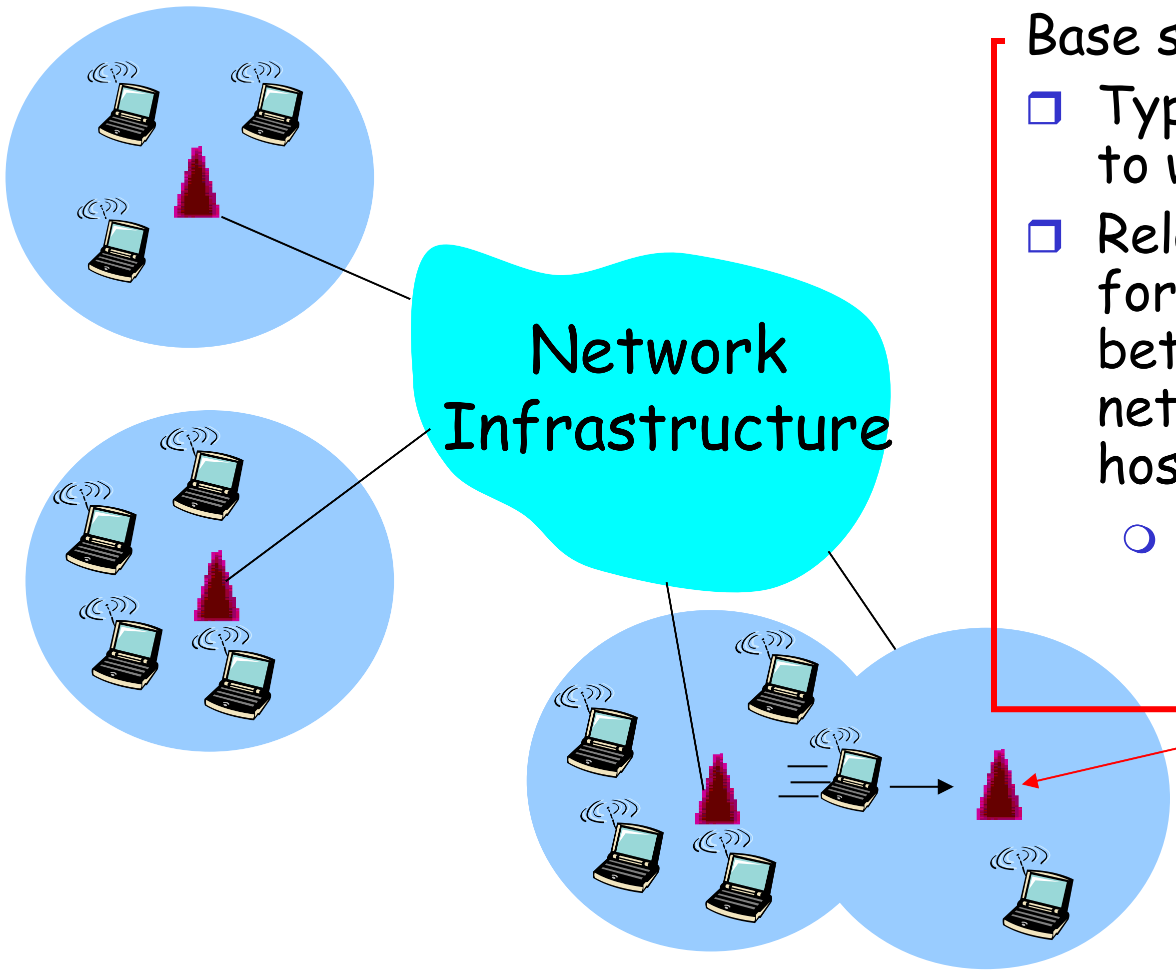
Elements of a Wireless Network



Wireless hosts

- Laptop, PDA, IP phone
- Run applications
- May be stationary (non-mobile) or mobile
  - Wireless does *not* always mean mobility

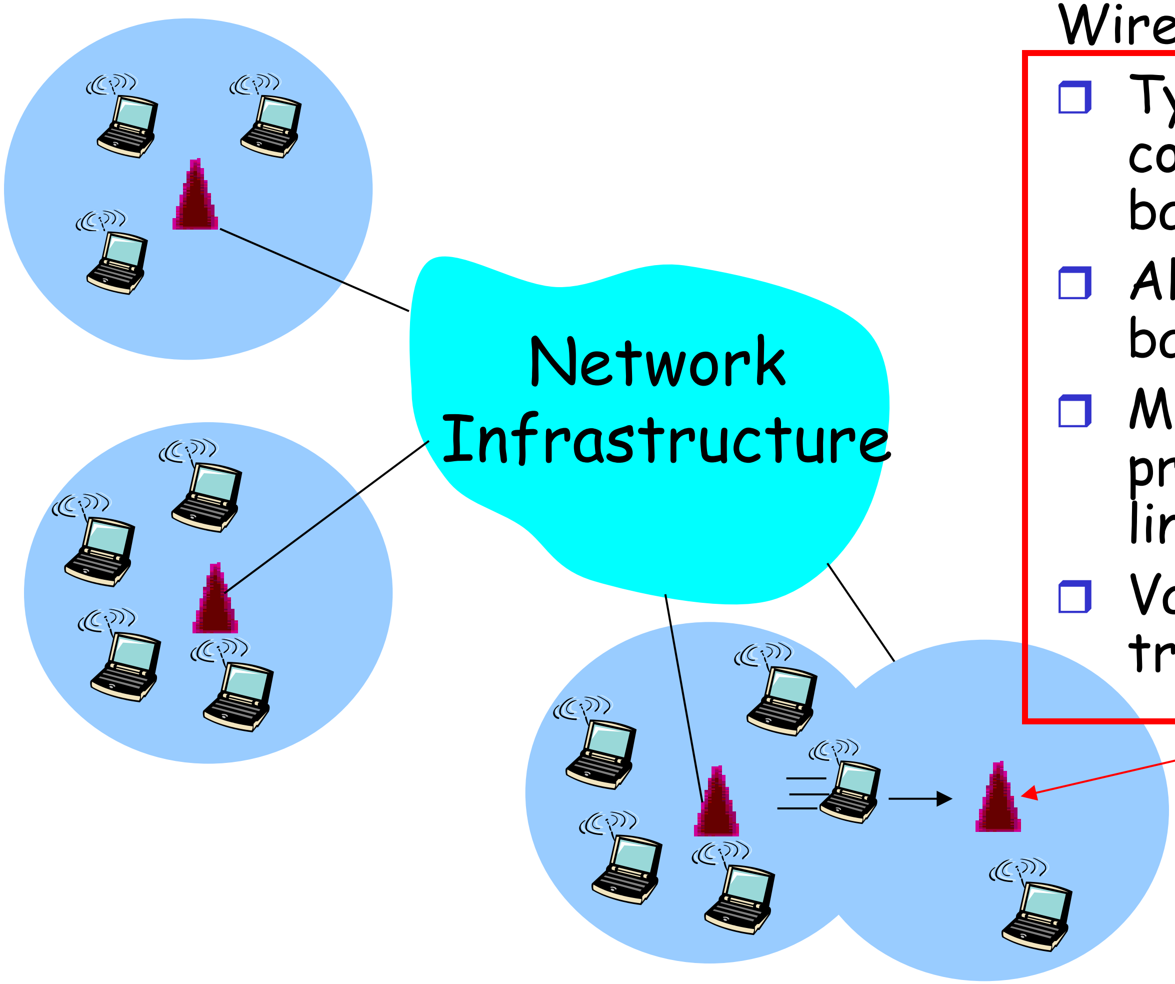
Elements of a Wireless Network



Base station

- Typically connected to wired network
- Relay - responsible for sending packets between wired network and wireless host(s) in its "area"
  - e.g., cell towers, 802.11 access points

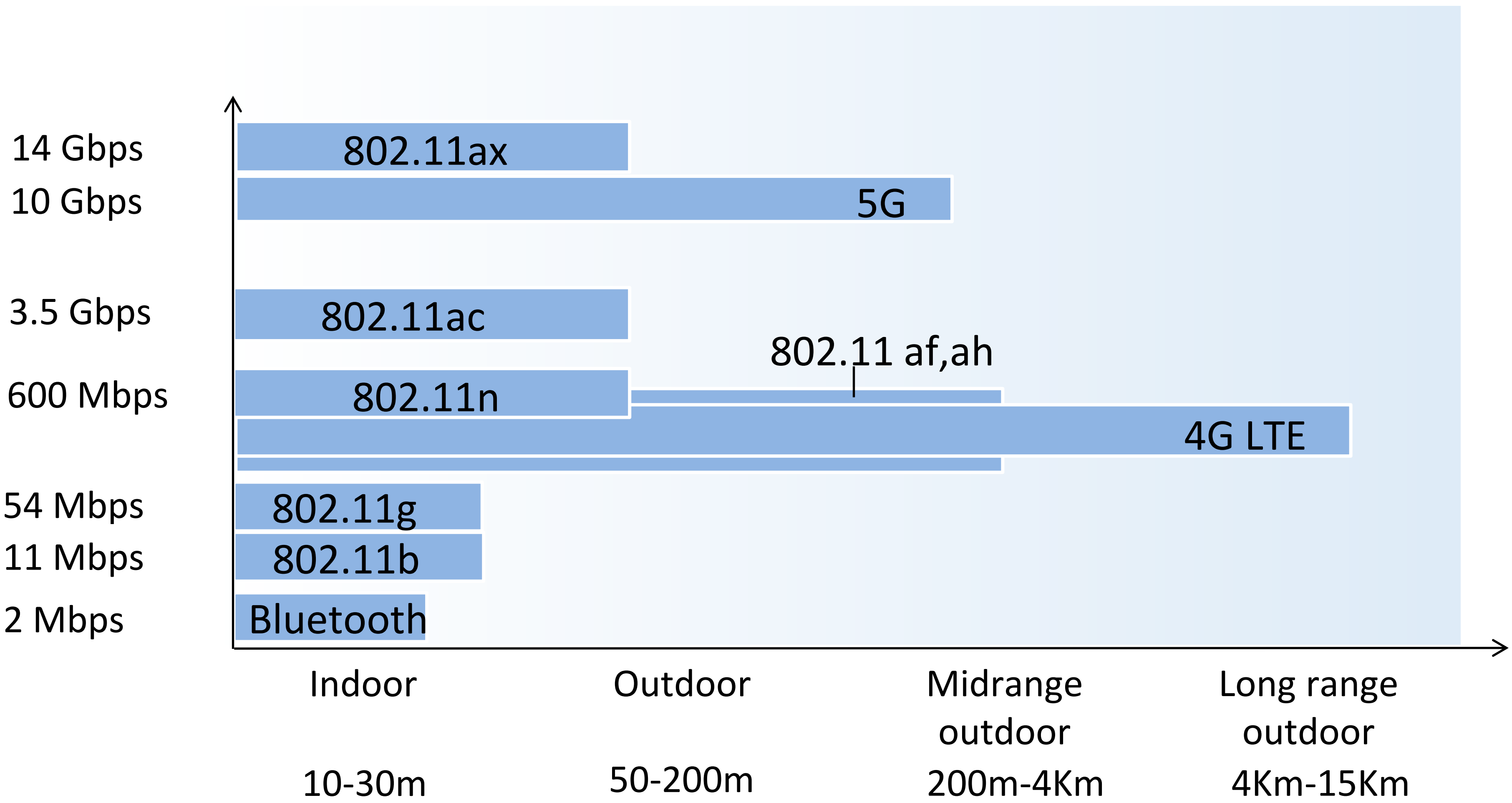
Elements of a Wireless Network



Wireless link

- Typically used to connect mobile(s) to base station
- Also used as backbone link
- Multiple access protocol coordinates link access
- Various data rates, transmission distance

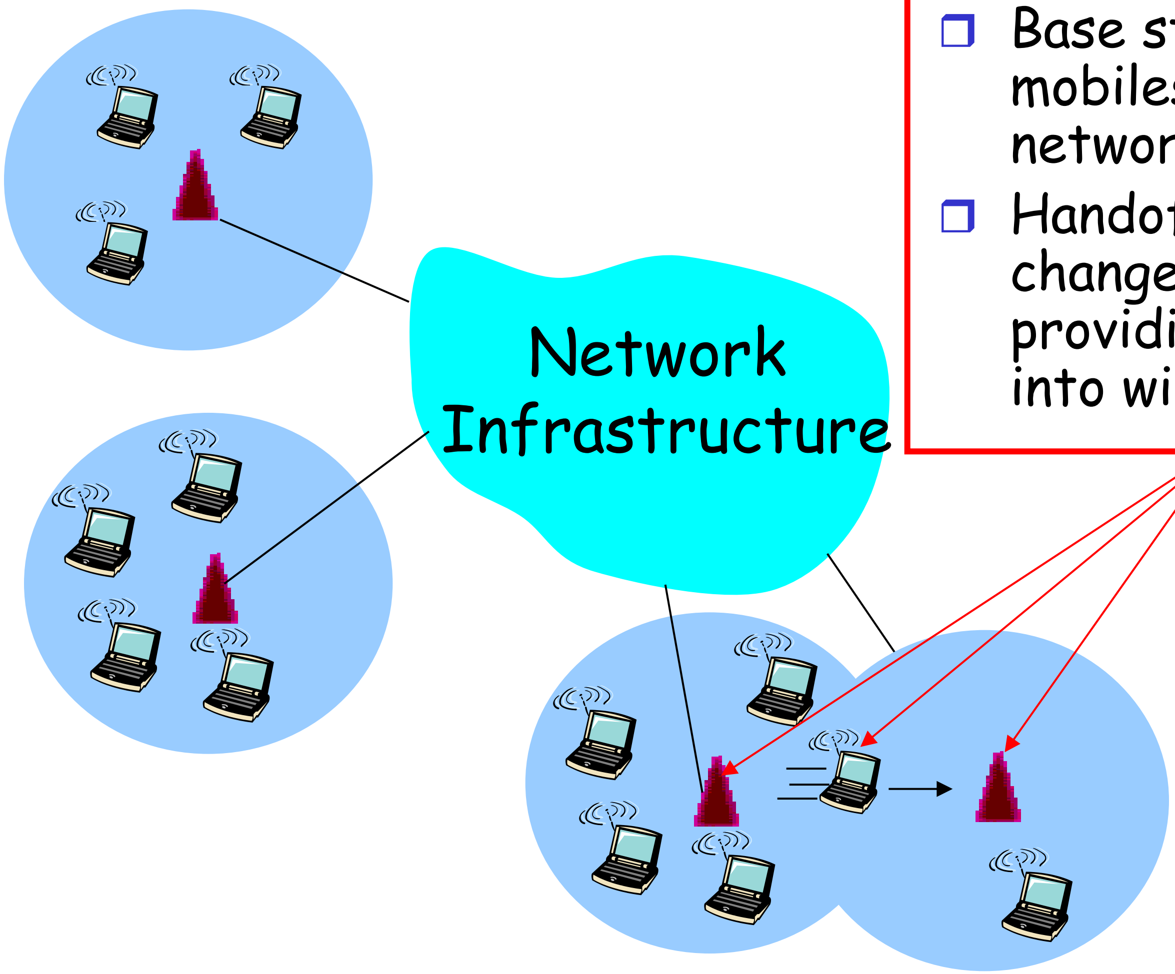
Characteristics of selected wireless link standards



802.11 Wireless LAN Standards

IEEE 802.11 standard	Year	Max data rate	Range	Frequency
802.11b	1999	11 Mbps	30 m	2.4 Ghz
802.11g	2003	54 Mbps	30m	2.4 Ghz
802.11n (WiFi 4)	2009	600	70m	2.4, 5 Ghz
802.11ac (WiFi 5)	2013	3.47 Gpbs	70m	5 Ghz
802.11ax (WiFi 6)	2021	14 Gbps	70m	2.4, 5 Ghz
802.11af	2014	35 – 560 Mbps	1 Km	unused TV bands (54-790 MHz)
802.11ah	2017	347Mbps	1 Km	900 Mhz
802.11be (WiFi 7)	2024 (exp)	0.4-23,059 Mbps	30-120m	2.4, 5, 6

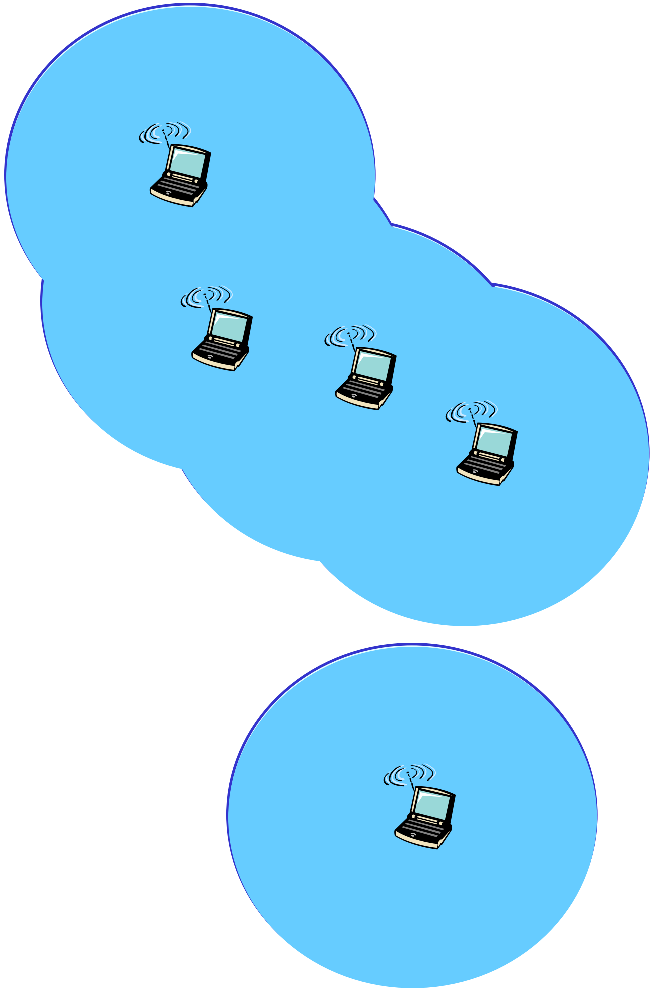
Elements of a Wireless Network



Infrastructure mode

- Base station connects mobiles into wired network
- Handoff: mobile changes base station providing connection into wired network

Elements of a Wireless Network



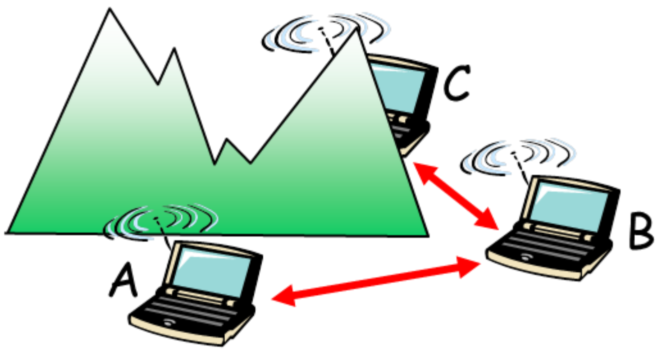
Ad hoc mode

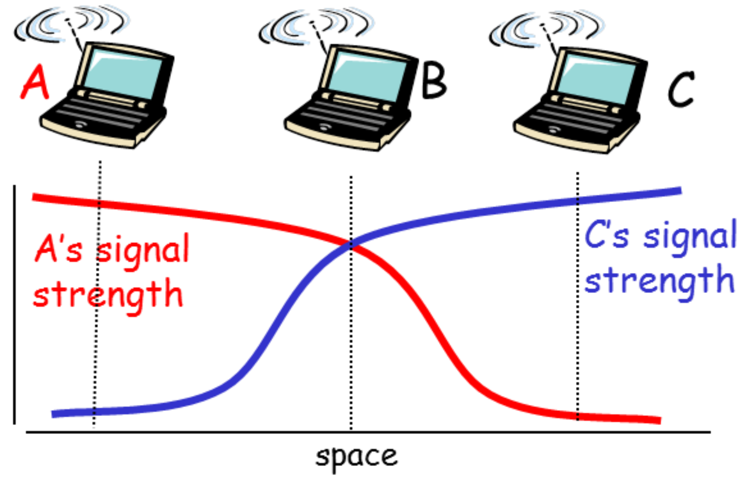
- No base stations
- Nodes can only transmit to other nodes within link coverage
- Nodes organize themselves into a network: route among themselves

Wireless Network Taxonomy

	Single Hop	Multiple Hops
Infrastructure	host connects to base station (WiFi, WiMAX, cellular) which connects to larger Internet	host may have to relay through several wireless nodes to connect to larger Internet: mesh net
No Infrastructure	no base station, no connection to larger Internet (Bluetooth, ad hoc nets)	no base station, no connection to larger Internet. May have to relay to reach other a given wireless node MANET, VANET

Hidden Node Problem





Hidden terminal problem
- B, A hear each other
- B, C hear each other
- A, C can not hear each other

means A, C unaware of their interference at B

Signal attenuation:
- B, A hear each other
- B, C hear each other
- A, C can not hear each other interfering at B

Exposed Node Problem

Exposed terminal problem
- B, C hear each other
- B wants to talk to A
- C wants to talk to D

- B needs to know that D can't hear B and is OK to send

Signal attenuation:
- B, C hear each other
- A, C don't hear each other
- D, B don't hear each other

How 802.11 works

Medium is *shared*

Collision domains are more complex

Method of operation: *CSMA/**CA***

- *Carrier sensing multiple access, with **collision avoidance***

Augmented media access control (MAC) protocol:

- Slot reservation protocol

MAC Protocol: CSMA/CA

<u>802.11 sender</u>

1 if sense channel idle for **DIFS** then

transmit entire frame (no CD)

2 if sense channel busy then

start random backoff time

timer counts down while channel idle

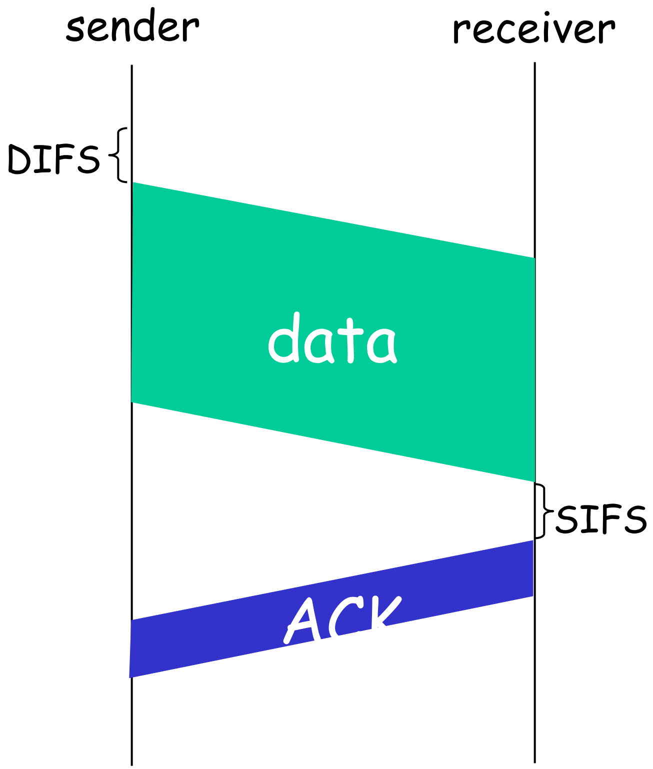
transmit when timer expires

if no ACK, increase random backoff interval, repeat 2

<u>802.11 receiver</u>

- if frame received OK

return ACK after **SIFS** (ACK needed due to hidden terminal problem)



SIFS/DIFS Numbers

Standard	SIFS	Slot Time	DIFS = SIFS+ $2 \times$ Slot Time
IEEE 802.11-1997 (FHSS)	$28\mu s$	$50\mu s$	$128\mu s$
IEEE 802.11-1997 (DSSS)	$10\mu s$	$20\mu s$	$50\mu s$
IEEE 802.11b	$10\mu s$	$20\mu s$	$50\mu s$
IEEE 802.11a	$16\mu s$	$9\mu s$	$34\mu s$
IEEE 802.11g	$10\mu s$	9 or $20\mu s$	28 or $50\mu s$
IEEE 802.11n (2.4 GHz)	$10\mu s$	9 or $20\mu s$	28 or $50\mu s$
IEEE 802.11n (5 GHz)	$16\mu s$	$9\mu s$	$34\mu s$
IEEE 802.11ac	$16\mu s$	$9\mu s$	$34\mu s$

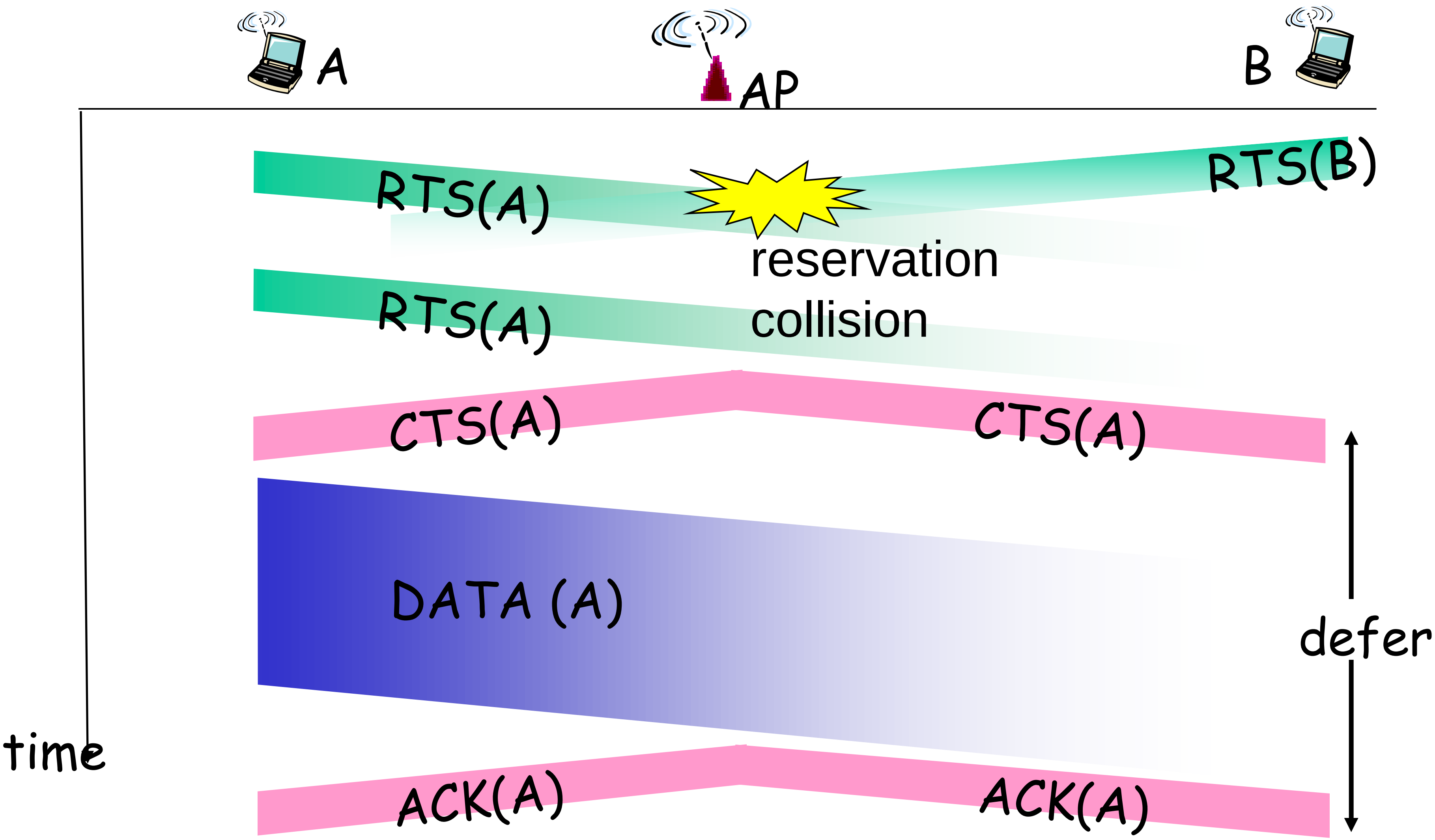
Avoiding Collisions

Idea: Allow sender to “reserve” channel rather than random access of data frames: avoid collisions of long data frames

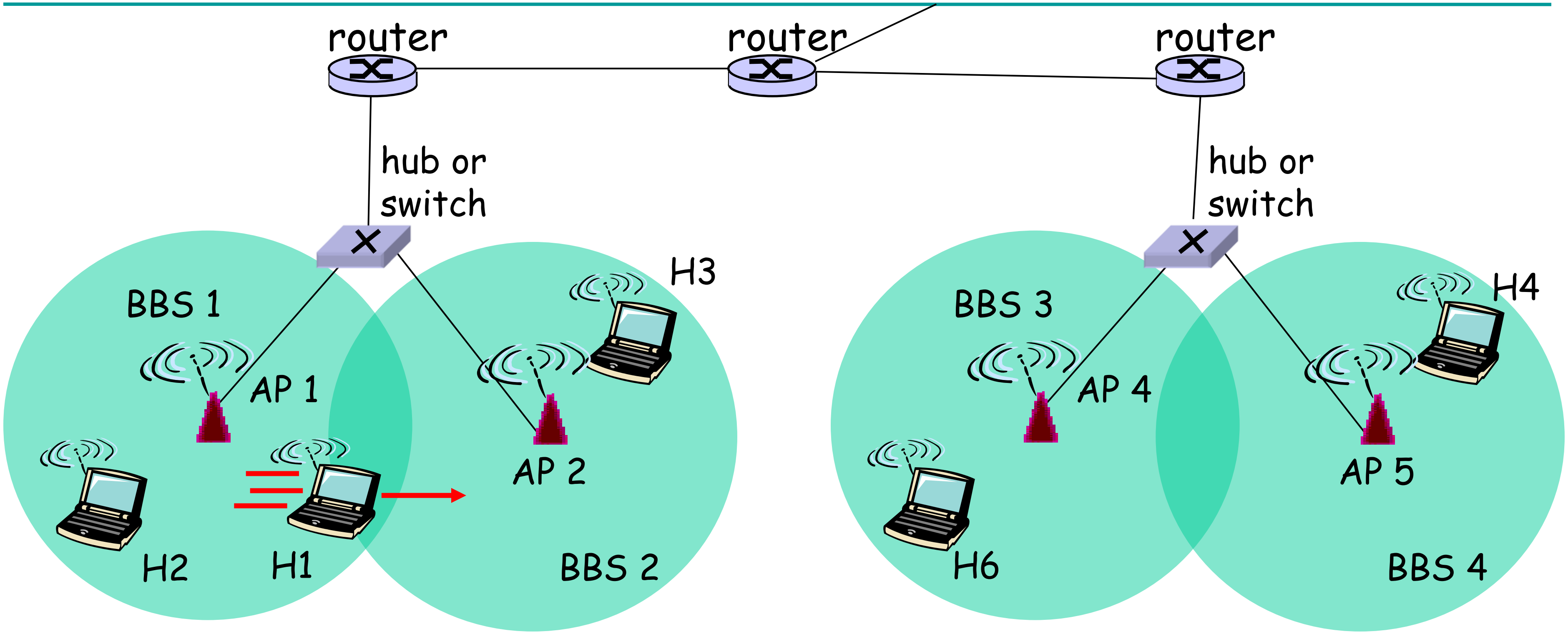
- Sender first transmits *small* request-to-send (RTS) packets to BS using CSMA
  - RTS contains requestor name and length of data to send
  - RTSs may still collide with each other (but they’re short)
- BS broadcasts clear-to-send CTS in response to RTS
  - Echoes approved node and the data length to send
- CTS heard by all nodes
  - sender transmits data frame
  - other stations defer transmissions

avoid data frame collisions completely
using small reservation packets!

Collision Avoidance: RTS-CTS

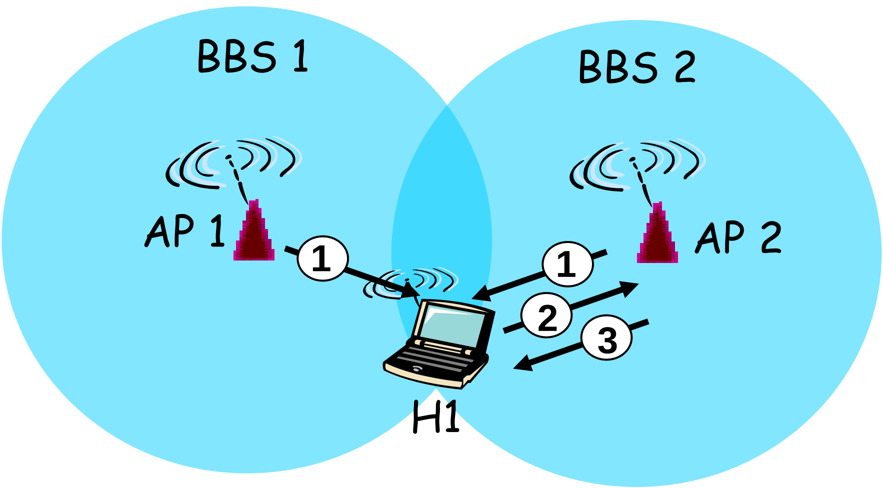


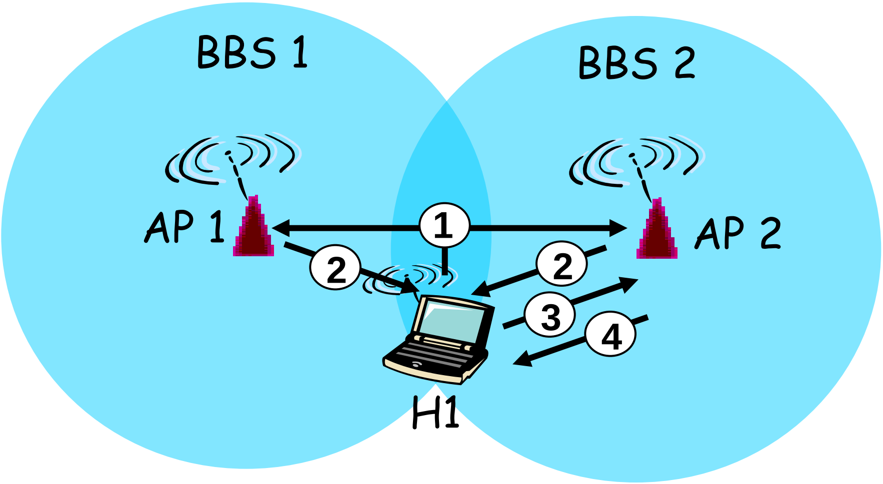
Wireless Access Points



- Distribution System – wired network infrastructure connects routers
- Mobility: H1 moves right, sees AP2 getting stronger than AP1, requests to associate with AP2

Scanning: Active and Passive





Passive Scanning:
1. Beacon frames sent from APs
2. Association Request frame sent: H1 to selected AP
3. Association Response frame sent: H1 to selected AP

Active Scanning:
1. Probe Request frame broadcast from H1
2. Probes response frame sent from APs
3. Association Request frame sent: H1 to selected AP
4. Association Response frame sent: H1 to selected AP

802.11 Security Issues

Packet Sniffing is *worse*

- No physical connection needed
- Long range (6 blocks)
- Old encryption standards (WEP, WEP2) were bad

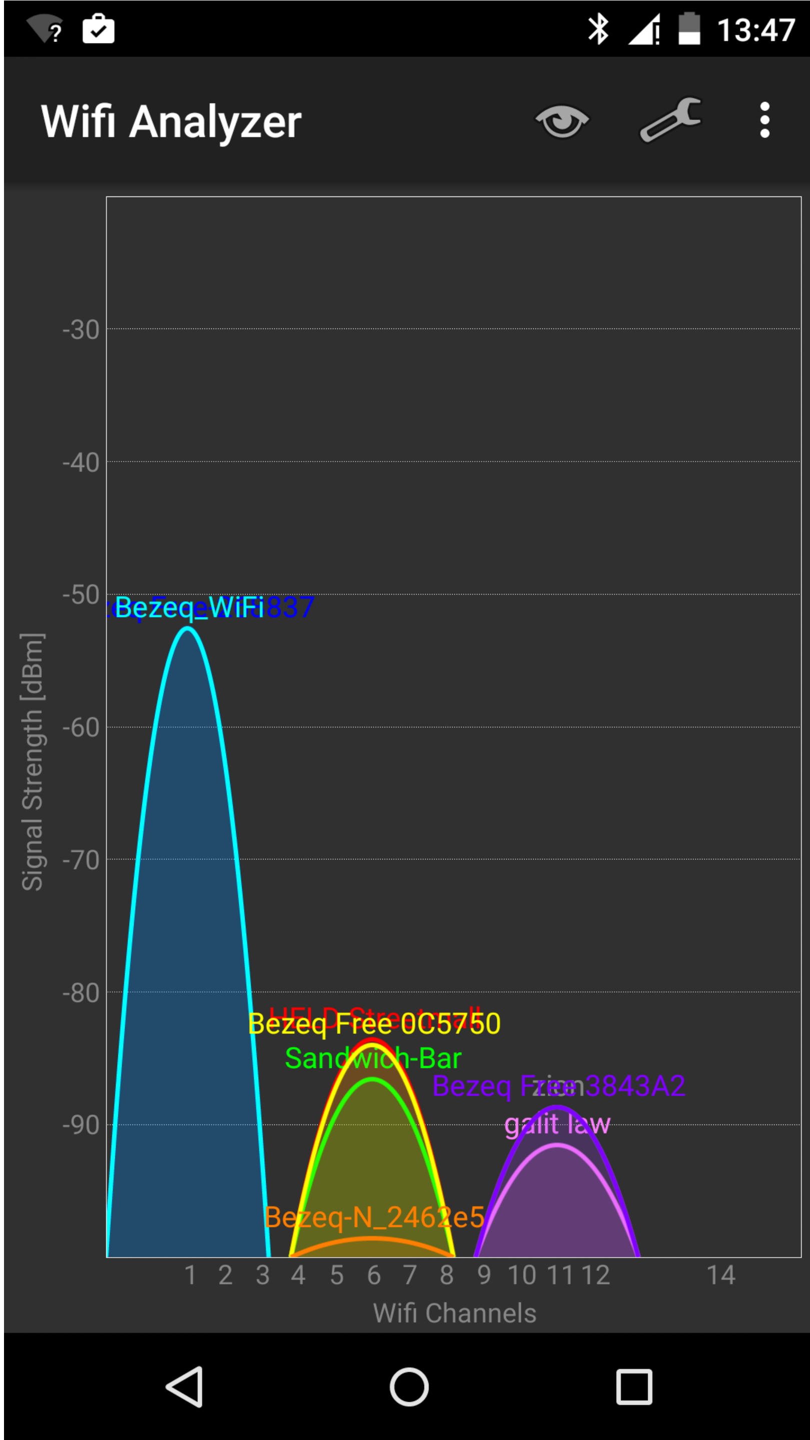
Denial of service

- Association (and Disassociation) Requests are not authenticated

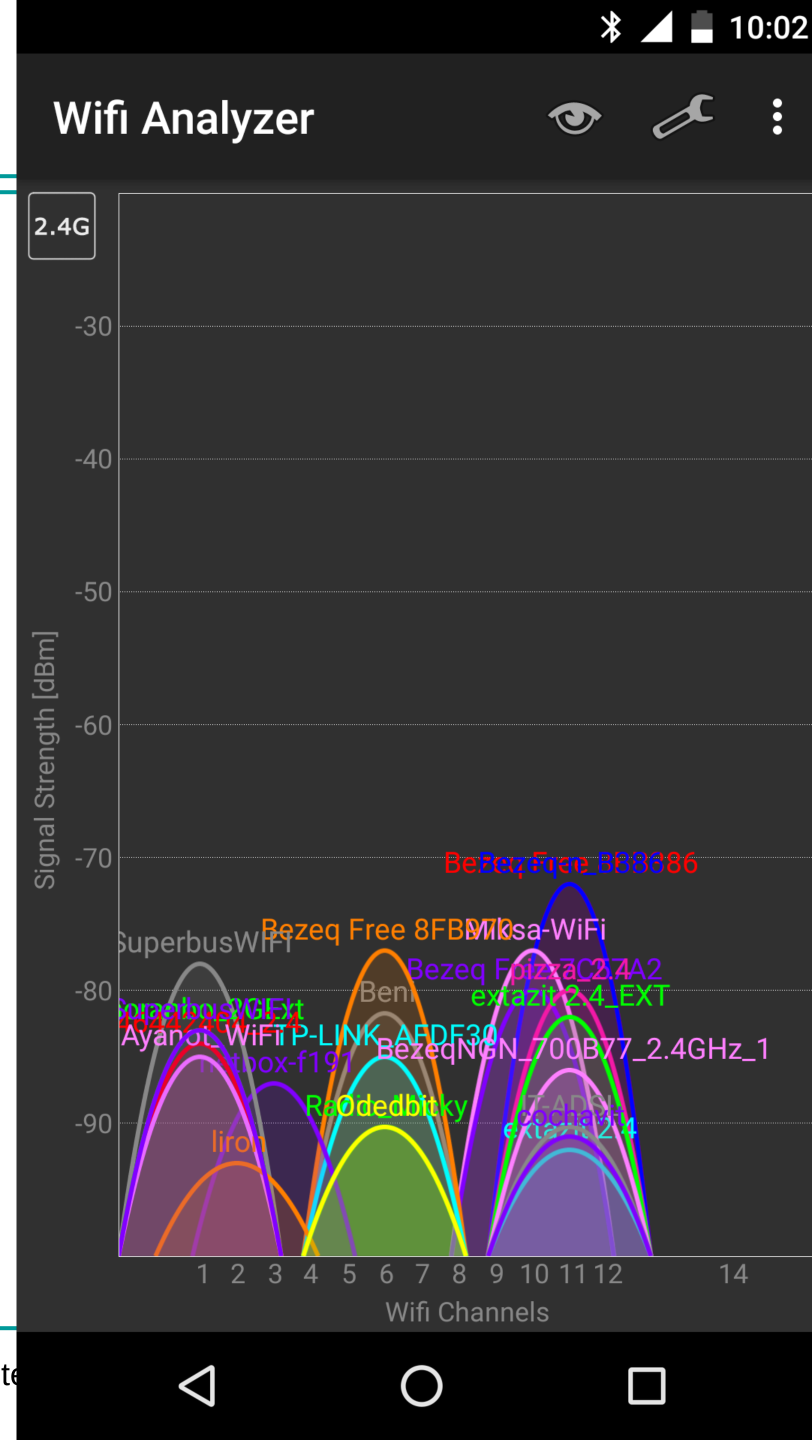
Better: WPA "Wi-Fi Protected Access"

- Introduced in 802.11i
- Uses much stronger cryptology (AES)

More about this in the SE course Communication and Information Security


13:47
Wifi Analyzer
Bezeq_WiFi
Bezeq Free 0C5750
Sandwich-Bar
Bezeq-N_2462e5
galit law
Signal Strength [dBm]
-30
-40
-50
-60
-70
-80
-90
1 2 3 4 5 6 7 8 9 10 11 12 14
Wifi Channels

ks


10:02
Wifi Analyzer
2.4G
SuperbusWiFi
Bezeq Free 8FB
extazit 2.4_EXT
BezeqNGN_700B77_2.4GHz_1
liron
Signal Strength [dBm]
-30
-40
-50
-60
-70
-80
-90
1 2 3 4 5 6 7 8 9 10 11 12 14
Wifi Channels

Wi-Fi Channels

Two main Wi-Fi frequency zones

- 2.4GHz
- 5GHz

Each zone divided into channels

Hosts and AP communicate over selected channel

- If 2 hosts send on overlapping channels, neither one is understandable

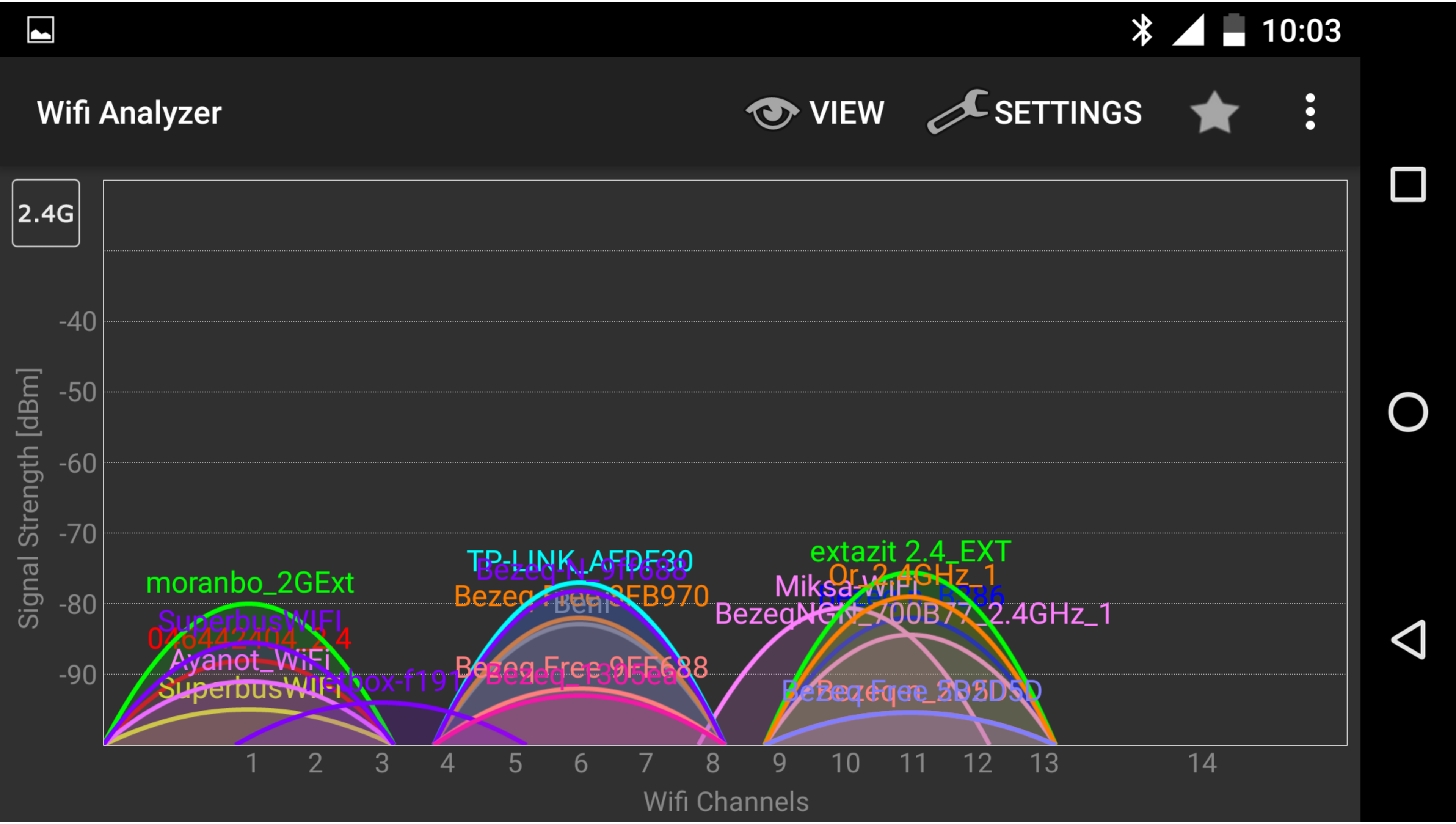
2.4GHz: Lots of overlapping channels

- Can choose multiple non-overlapping ones

5GHz: Less overlap

- Can bond multiple channels for a single message to increase throughput

Wi-Fi 2.4GHz channels



2.4GHz channels

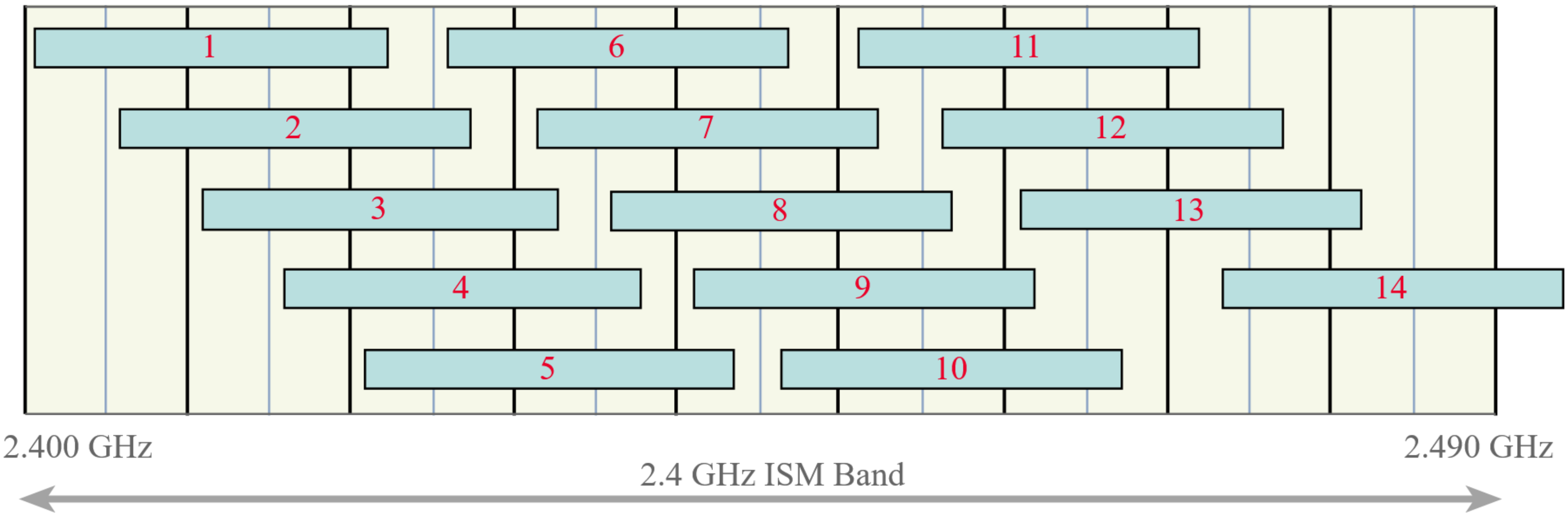
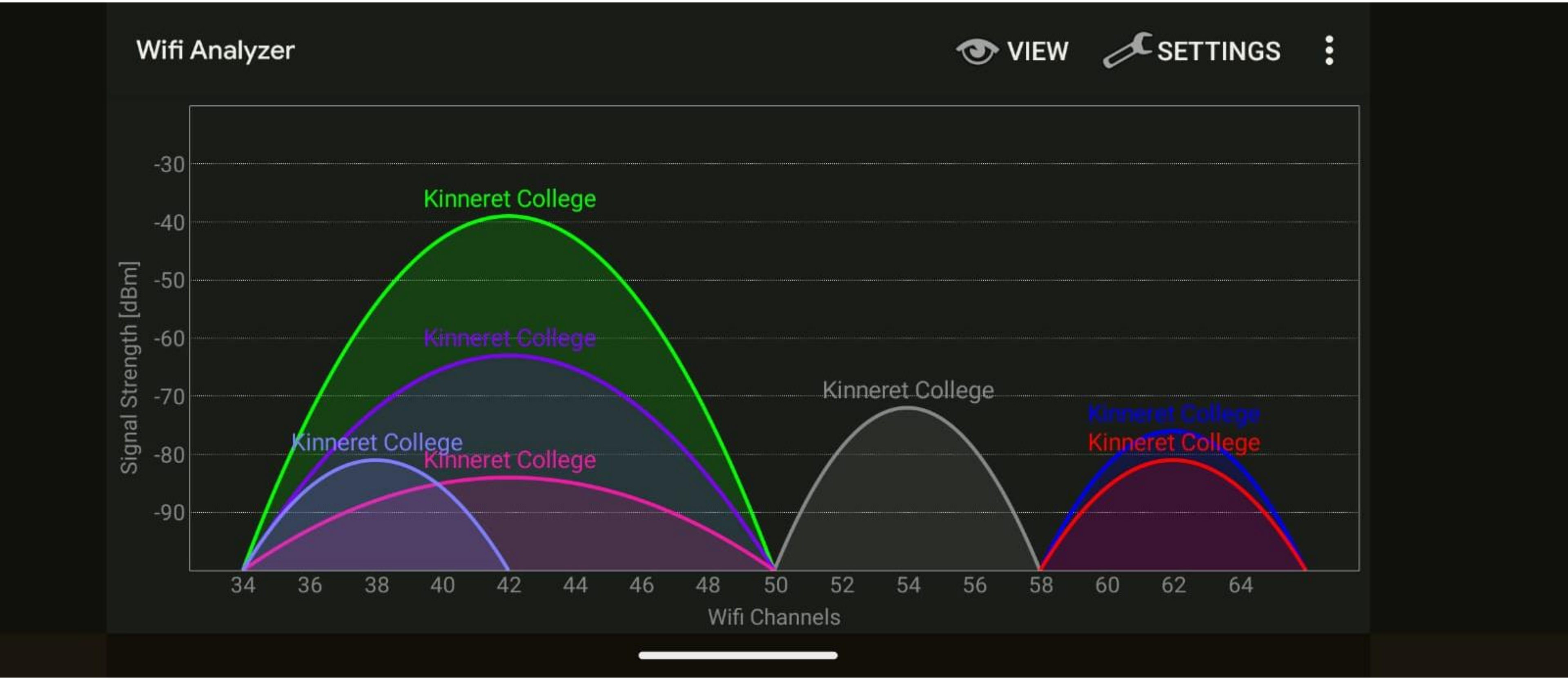


Image source: https://www.electronics-notes.com/articles/connectivity/wifi-ieee-802-11/channels-frequencies-bands-bandwidth.php

Wi-Fi 5GHz channels



5GHz channels at 20MHz wide

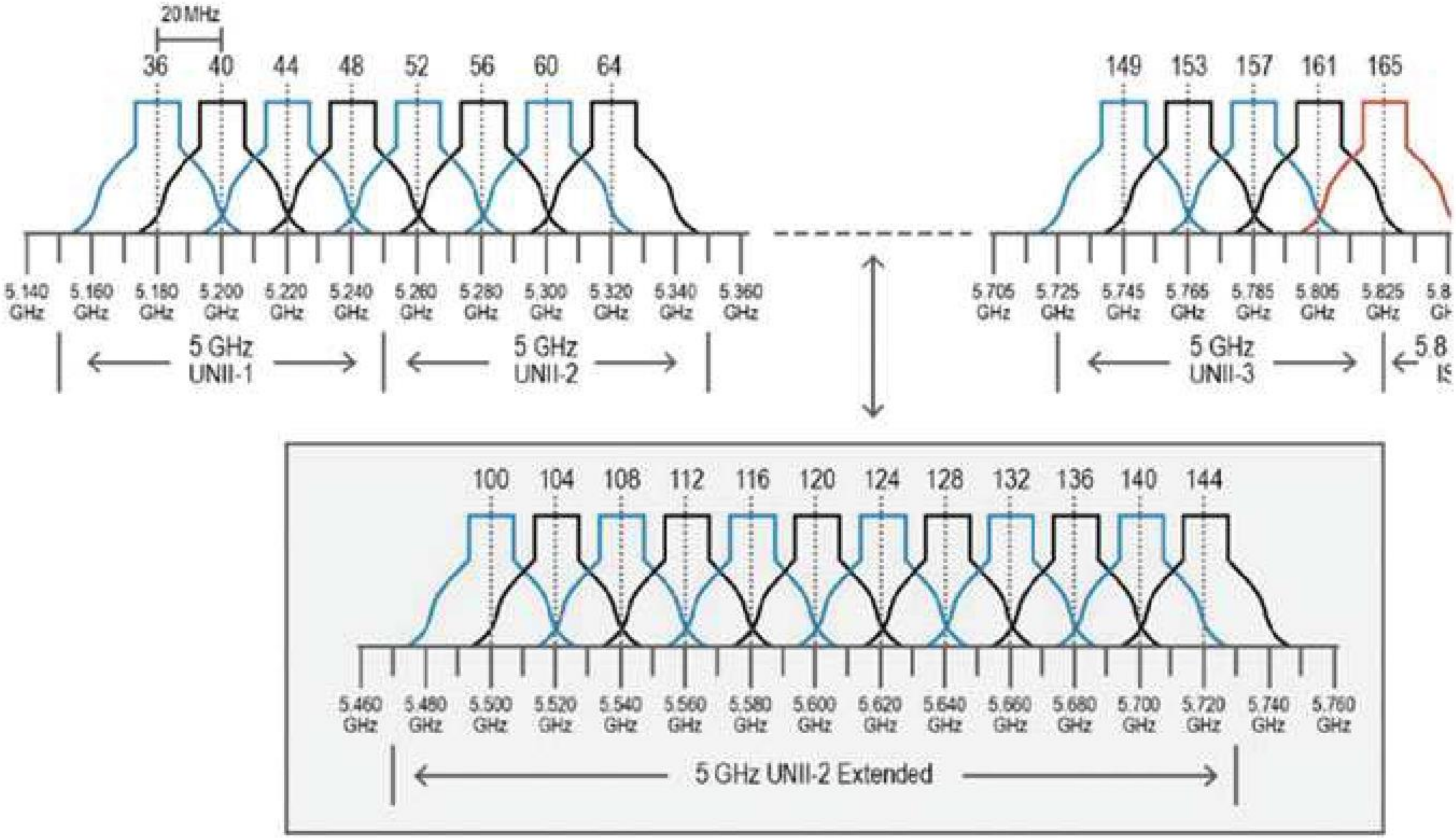
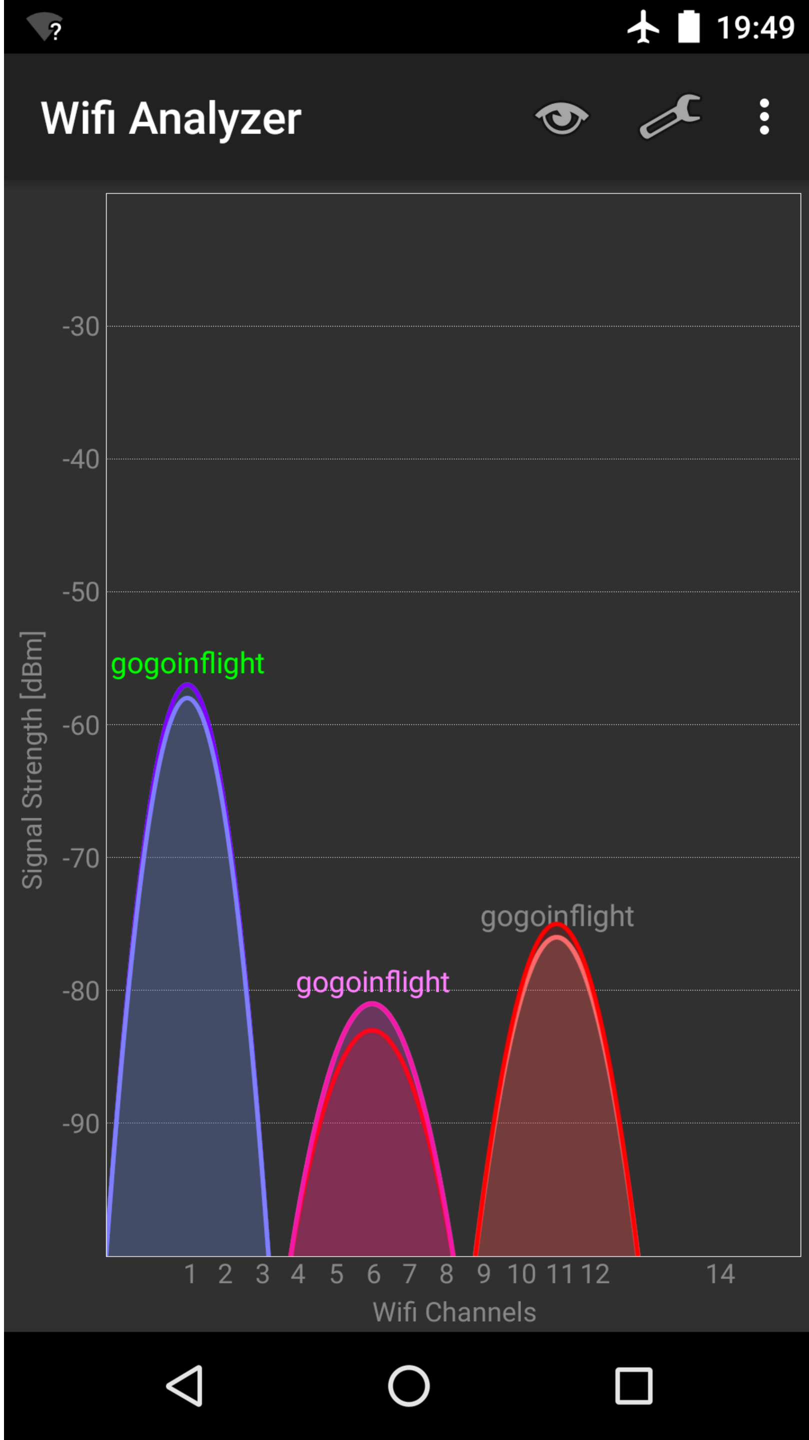
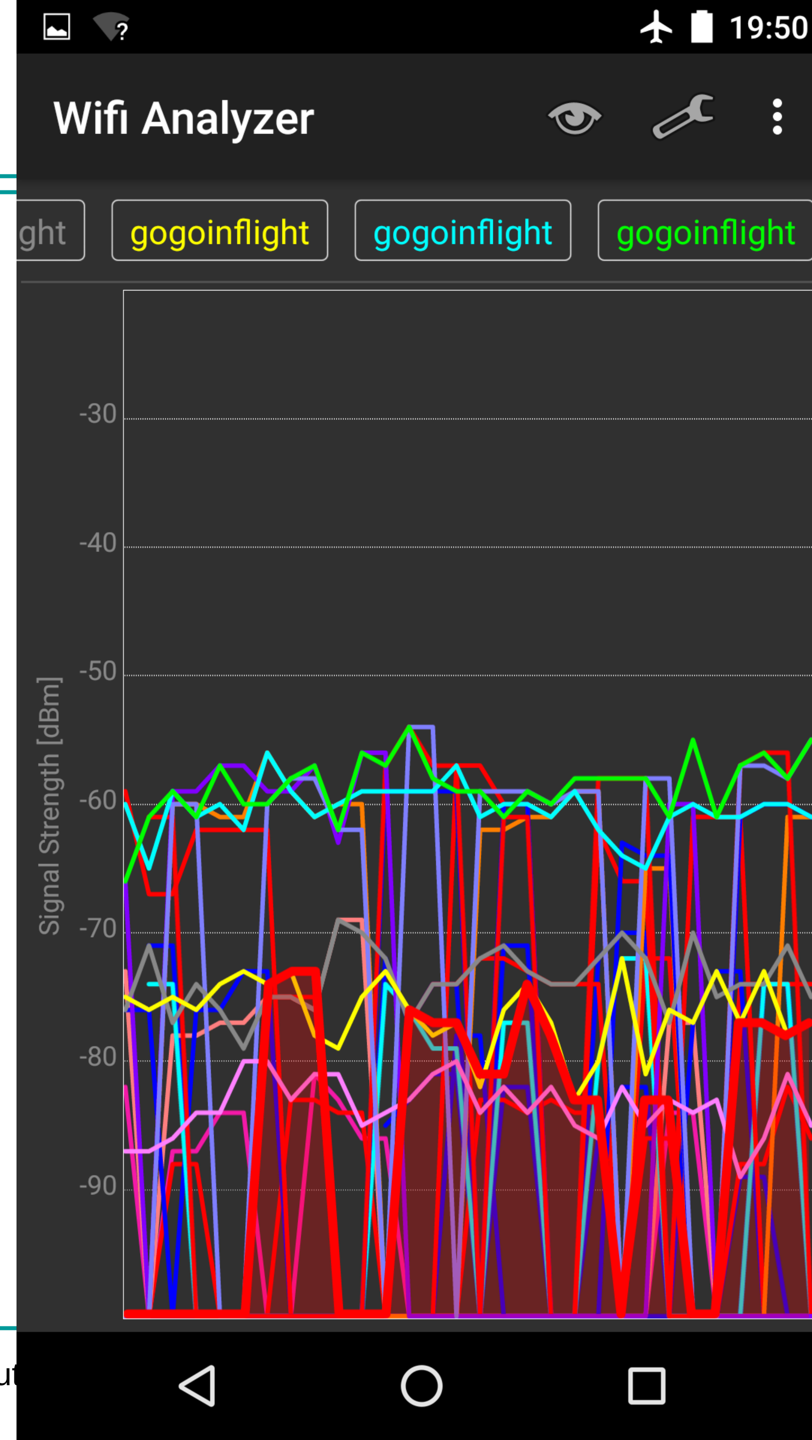


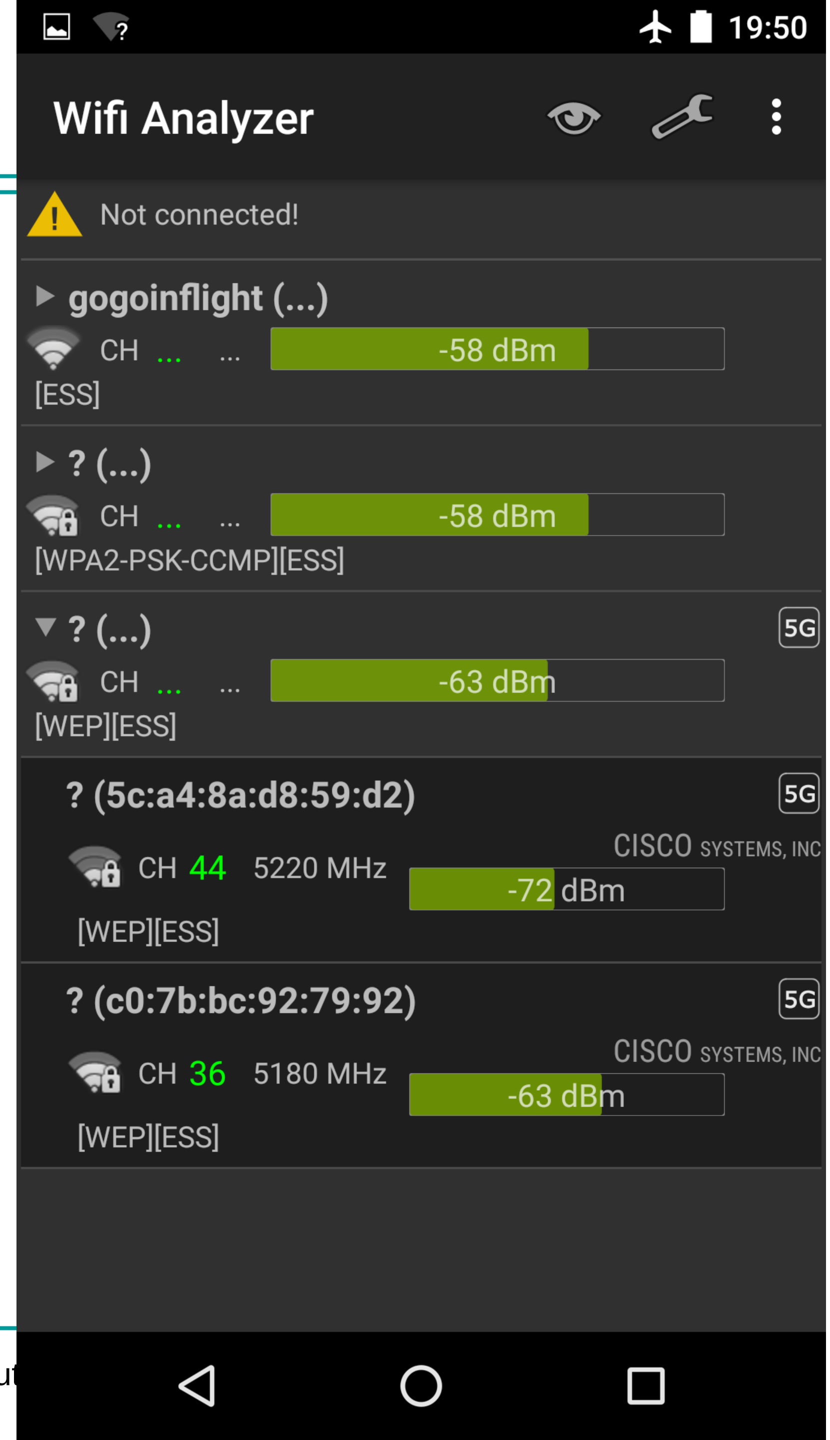
Fig. 3 WLAN channels in 5 GHz band [6]

Lepaja, Salem & Maraj, Arianit & Berzati, Shpat. (2019). WLAN Planning and Performance Evaluation for Commercial Applications: Evolvements in Business Information Processing and Management—Volume 1. 10.1007/978-3-319-94117-2_3.


19:49
Wifi Analyzer
-30
-40
-50
-60
-70
-80
-90
Signal Strength [dBm]
gogoinflight
gogoinflight
gogoinflight
1 2 3 4 5 6 7 8 9 10 11 12 14
Wifi Channels


19:50
Wifi Analyzer
ght
gogoinflight
gogoinflight
gogoinflight
-30
-40
-50
-60
-70
-80
-90
Signal Strength [dBm]

Plane WiFi


19:50
Wifi Analyzer
Not connected!
gogoinflight (...)
CH ... ...
-58 dBm
[ESS]
? (...)
CH ... ...
-58 dBm
[WPA2-PSK-CCMP][ESS]
? (...)
5G
CH ... ...
-63 dBm
[WEP][ESS]
? (5c:a4:8a:d8:59:d2)
5G
CISCO SYSTEMS, INC
CH 44 5220 MHz
-72 dBm
[WEP][ESS]
? (c0:7b:bc:92:79:92)
5G
CISCO SYSTEMS, INC
CH 36 5180 MHz
-63 dBm
[WEP][ESS]

So Far

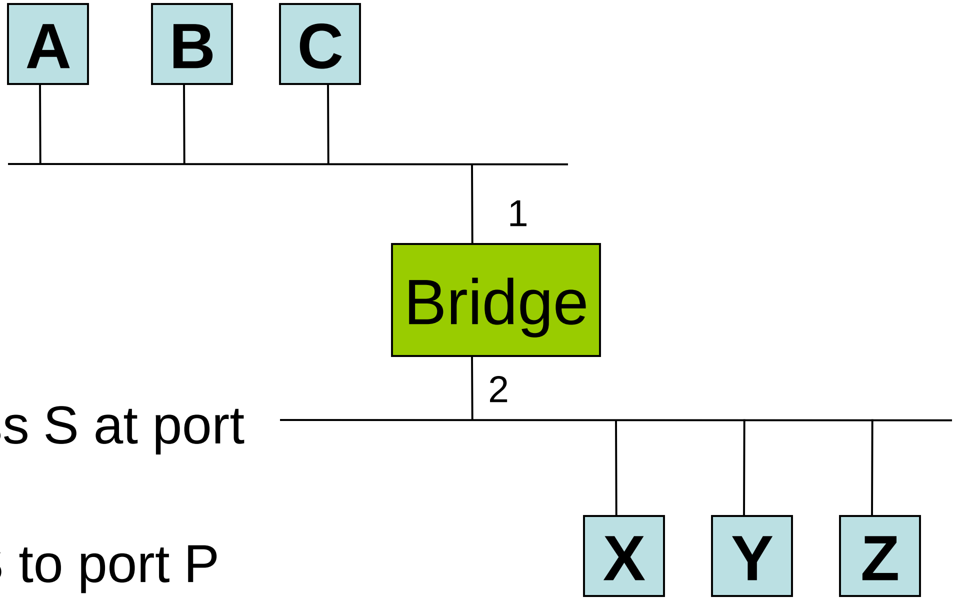
- Virtual Circuit Routing
- 802.11 Wireless
- Bridges and Spanning Tree Algorithm

Bridges and LAN Switches

- Bridge accepts LAN frames Bridge on one port, outputs them on another.

- Optimization: only forward appropriate frames

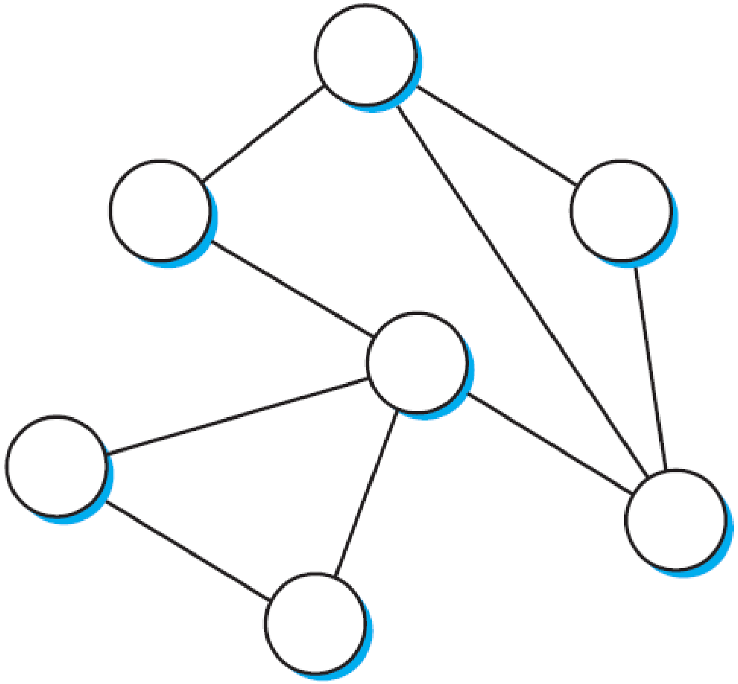
- Learning bridge
  - Watch incoming *source* address S at port number P
  - Add entry to forward address S to port P
  - If no entry, broadcast to all ports



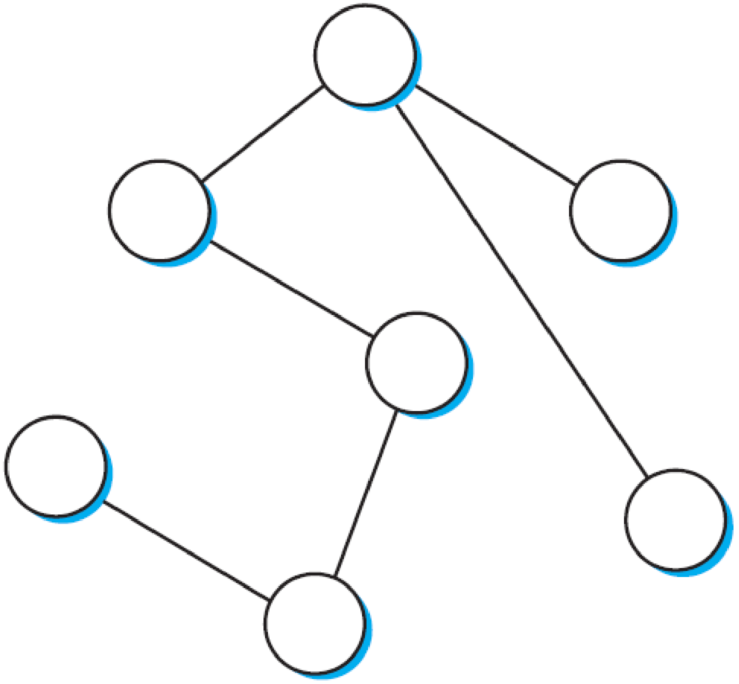
Problem: Cycles (Loops)

- Frame gets rebroadcast forever
- Could avoid by construction, BUT:
  - Hard, especially management
  - Often want redundancy
- Solution:
  - Restrict active ports to a *Spanning Tree*
  - Basic design by Radia Perlman of Digital
  - 802.1 specification of LAN Bridges is based on this algorithm

What is a Spanning Tree?



(a)



(b)

Algorhyme

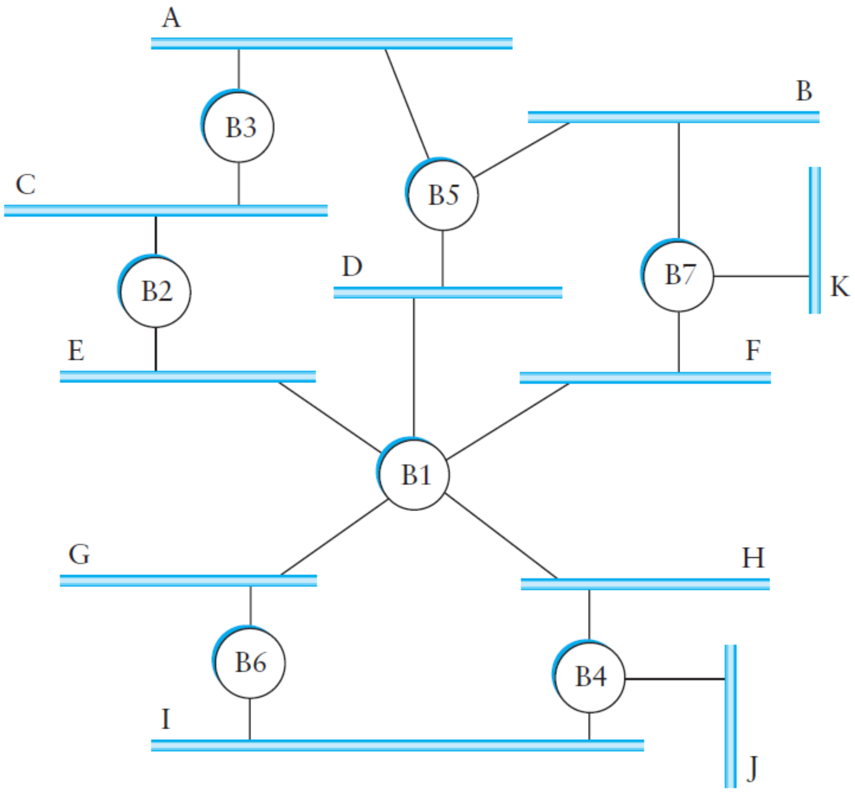
I think that I shall never see
a graph more lovely than a tree.
A tree whose crucial property
is loop-free connectivity.
A tree that must be sure to span
so packets can reach every LAN.
First, the root must be selected.
By ID, it is elected.
Least-cost paths from root are traced.
In the tree, these paths are placed.
A mesh is made by folks like me,
then bridges find a spanning tree.

Radia Perlman

Spanning Tree Concepts

Key concepts:

- A single root bridge is elected
  - Each subnet must have a single path to reach the root bridge
- Each bridge may be connected to (and receive packets from) multiple subnets
  - Only the designated bridge will forward packets toward the root
- Every bridge knows which of its ports is closest to the root bridge
  - Called the root port



Spanning Tree Algorithm

Advertisement
$(ROOT, dist, SENDER)$

- $ROOT$ root node ID
- $dist$ how many hops to the root $ROOT$
- $SENDER$ ID who sent it

Each node begins thinking it's the root and starts advertising that

If a node receives a better advertisement, it stops broadcasting its own messages

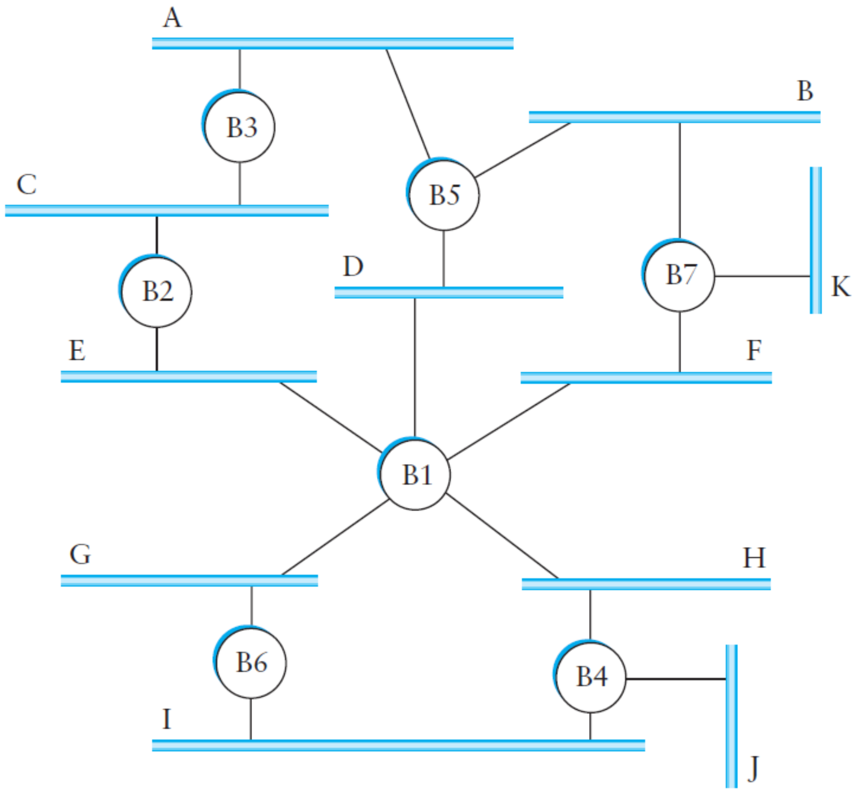
- Better is smaller $ROOT$ ID or same $ROOT$ ID and smaller $dist$
- Last one generating ads wins as root
- Bridge remembers where the shortest, best path – that's the Root Port

Election also for designated bridge (at the same time)

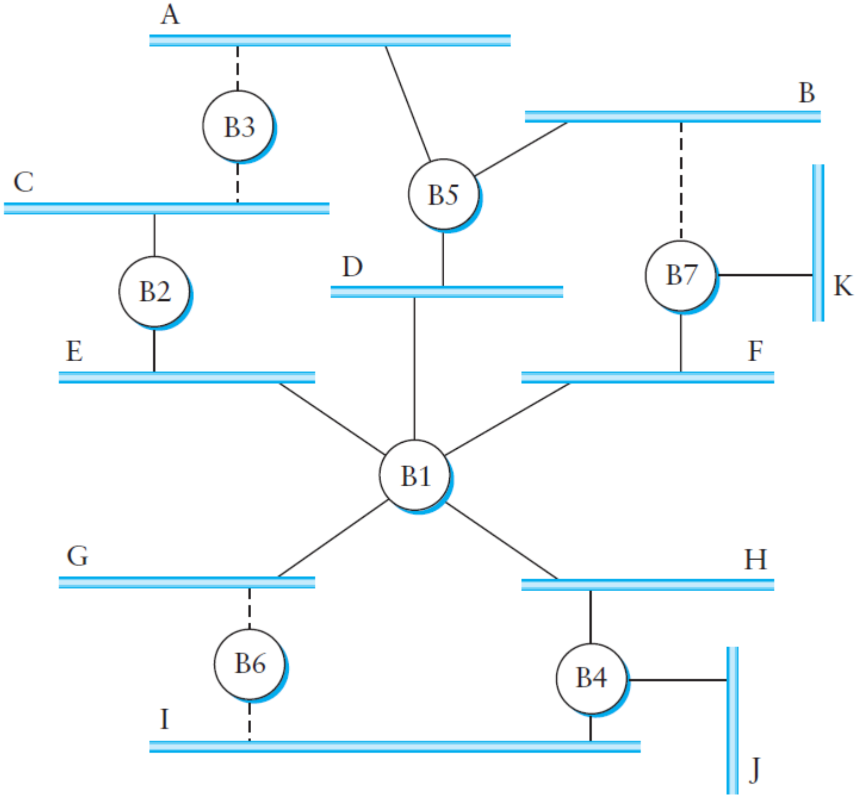
- Smallest $dist$ to $ROOT$ or same $dist$ but smaller ID
- If a bridge hears a shorter, better path on a port, it knows it's not the Designated Bridge for that subnet

Spanning Tree Example

Before



After



Spanning Tree Maintenance

The root bridge is the last one generating advertisements

- It sends out advertisements every so often
- If a bridge notices that it hasn't heard an advertisement in a while (timer), it starts the algorithm again

- Automatic detection of failures and network topology changes

Limitations of Bridges

Scaling

- Connections on order of dozens
- Spanning tree algorithm scales linearly
- Transparency incomplete

Congestion can be visible to higher protocol layers

Latency can be larger and more variable

Heterogeneity

- Limited to compatible (similarly addressed) link layers

Conclusion

- Virtual Circuit Routing
- 802.11 Wireless
- Bridges and Spanning Tree Algorithm