LAN Technology

Wireless LAN Protocols

Arash Habibi Lashkari
PHD of Computer Science - Information Security
July 2010

Wireless LAN Protocols

Outlines:

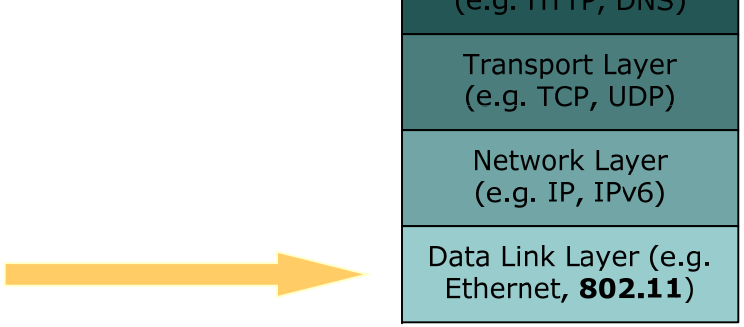
- WLAN: Wireless LAN by IEEE 802.11 Protocols
- IEEE 802.1X: EAP over LAN (EAPOL) for LAN/WAN Authentication and key Management
- IEEE 802.15 and Bluetooth: WPAN Communications
- WiMAX: IEEE 802.16

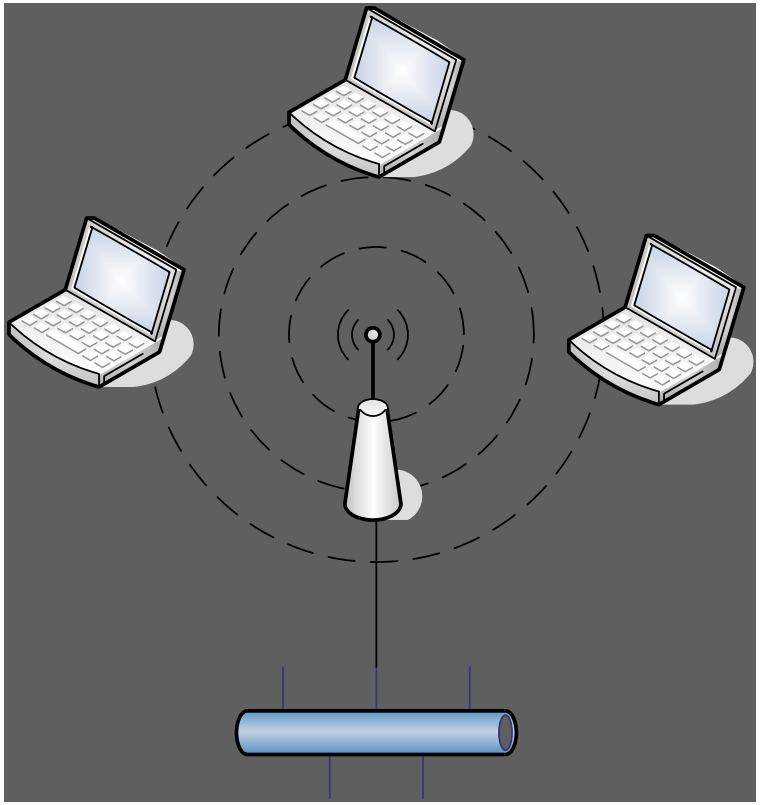
Wireless Networking (Wi-Fi)

Data Link Layer (Layer 2) over radio frequencies

Many standards

Notably IEEE 802.11





IEEE 802.11

IEEE 802 – committee on LAN/MAN standards

IEEE 802.11 – WG on Wireless LAN

Network protocols

- 802.11a, 802.11b, 802.11g

Enhancements

- 802.11i, 802.11e

New work

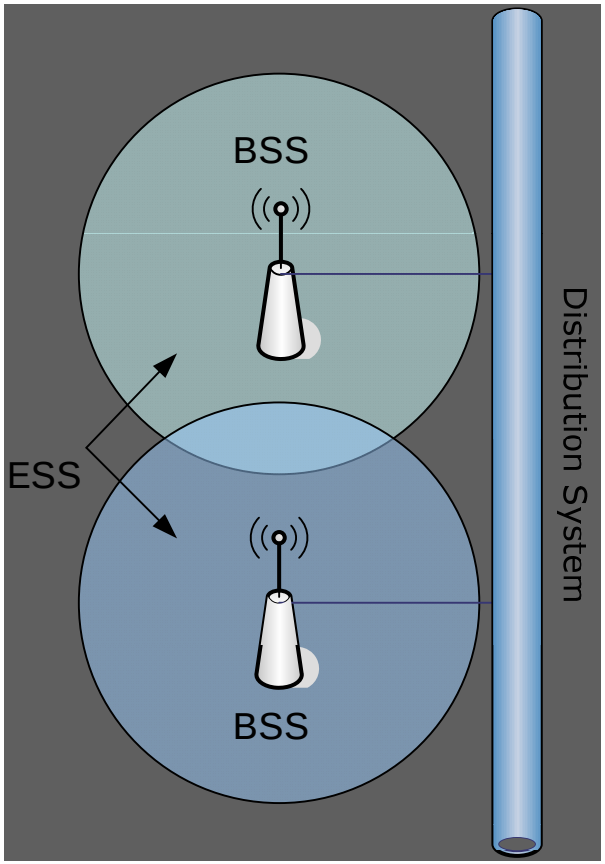
- 802.11n, …

802.11b Key Features

- Speeds up to 11Mb/s
  - Scales down to 5.5Mb/s, 2Mb/s, 1Mb/s
  - About half speed taken with overhead
- Uses 13 × 22MHz channels within the IMS (2.4GHz) band in UK
- Omnidirectional range of ~50m
  - Directional, high-gain antennas can transmit over several km
- DSSS, CSMA/CA

802.11 Architecture

- BSS – Base Service Set
  - One cell from one access point
- ESS – Extended Service Set
  - Network of cells
  - Common ESSID
  - Cells linked by DS: Ethernet or wireless (WDS)

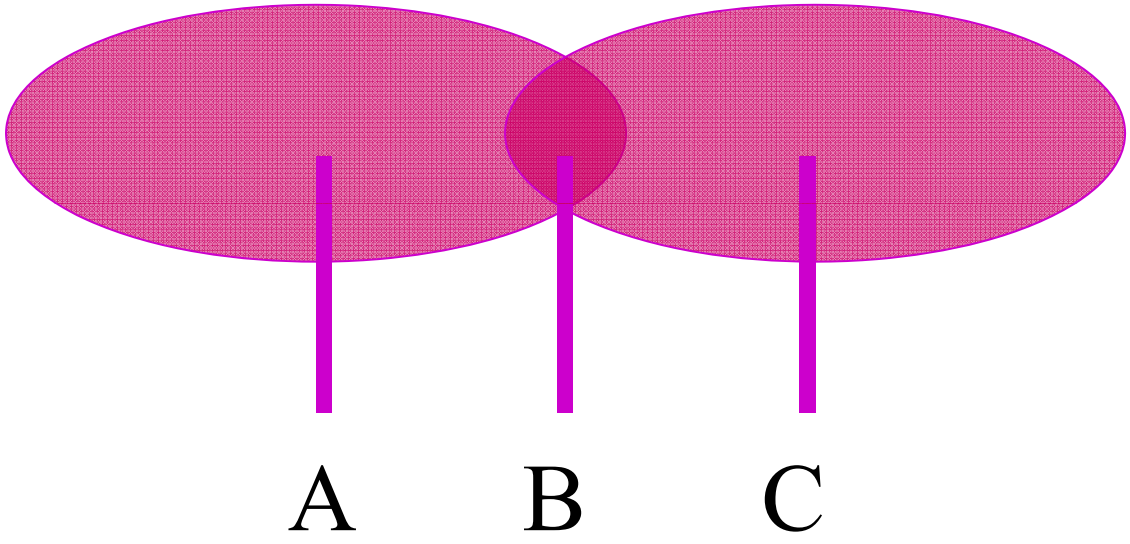


802.11b Layers

- Physical Layer
  - e.g DSSS for 802.11b
- Data Link Layer
  - Media Access Control – CSMA/CA
  - Logical Link Control – 802.2 standard

e.g. HTTP, DNS, SMTP	*Application Layer*
e.g. TCP, UDP	*Transport Layer*
e.g. IP, IPv6	*Network Layer*
802.2 LLC	*Data Link Layer*
802.11 MAC	
DSSS over RF	*Physical Layer*

Hidden Node Problem



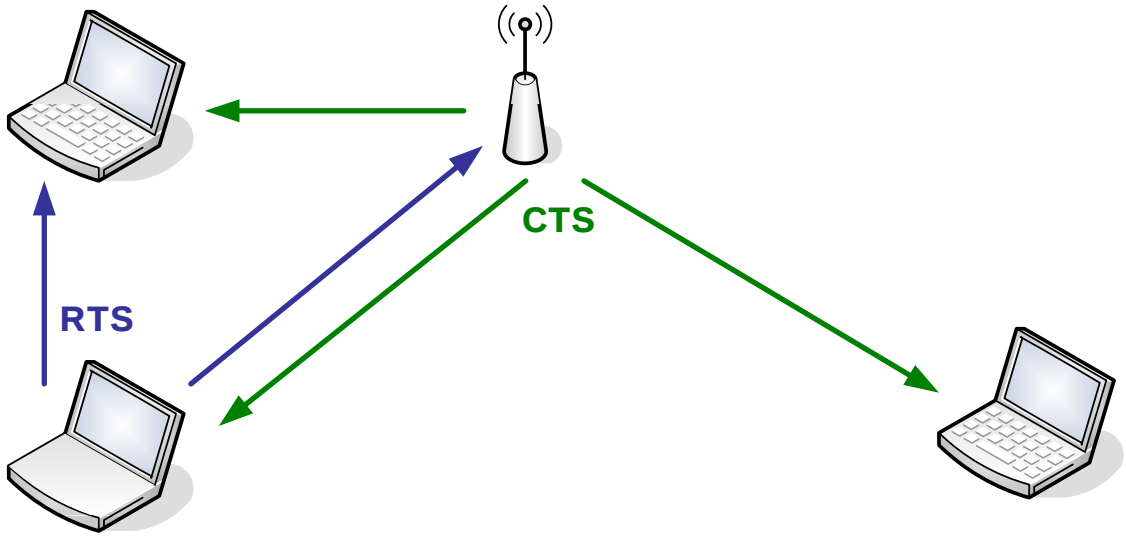
A and C cannot see each other, B can see both

CSMA/CA

Sender sends *Request to Send* (RTS)

Receiver sends *Clear to Send* (CTS)

Sender transmits for required time



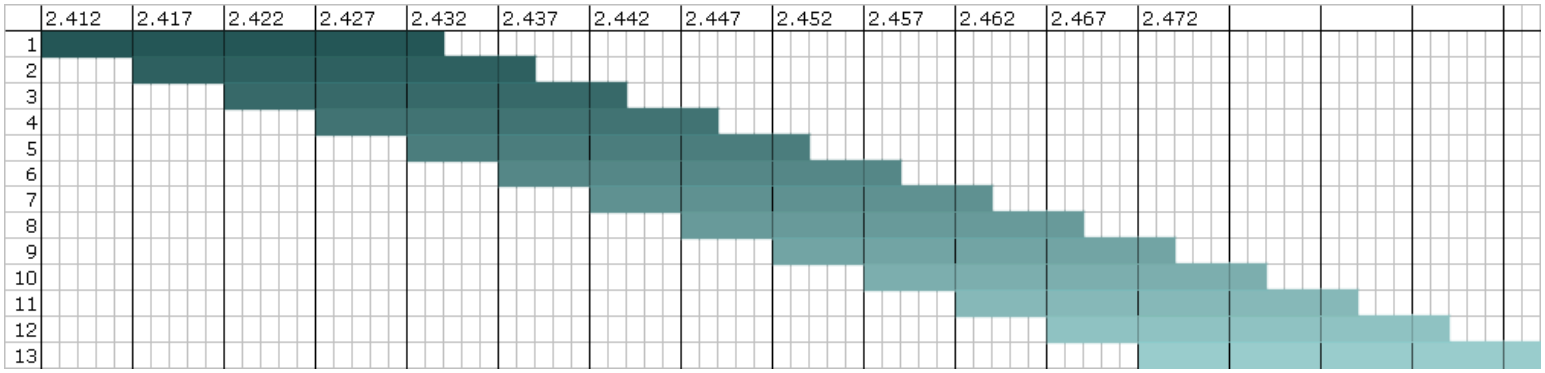
802.11b Channels

In the UK and most of EU: 13 channels, 5MHz apart, 2.412 – 2.472 GHz

Each channel is 22MHz

Significant overlap

Best channels are 1, 6 and 11



TCP Over Wireless

- Wireless unreliable, prone to errors
- TCP will begin a slow start on errors
  - Designed to find optimum window size
  - Inefficient for wireless
- Improvements
  - Adding a threshold
  - TCP Reno – fall back to threshold
- Retransmission Timer
  - Doubles on every retransmission

Security in 802.11b

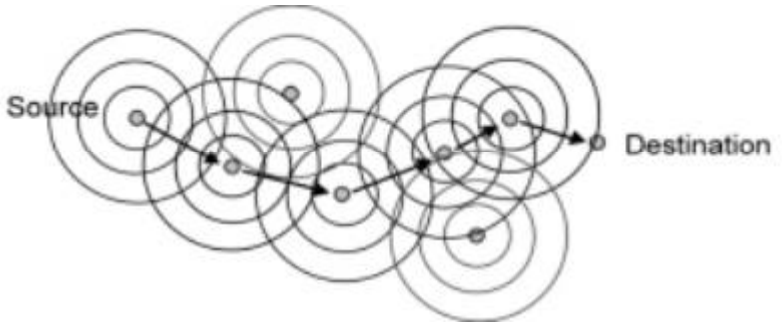
- WEP
  - *Wired Equivalent Privacy*
  - RC4 and CRC32
  - Known vulnerabilities
- WPA
  - *Wi-fi Protected Access*
  - Larger, dynamically changed keys
- 802.1x
  - Port-based authentication
- 802.11i (WPA2)
  - Builds on WPA
  - AES (Rijndael)

Meshed Networking

Decentralised infrastructure

Network of interconnected access points

Peer-to-peer routing, often redundant



Source: Wi-fi technology forum

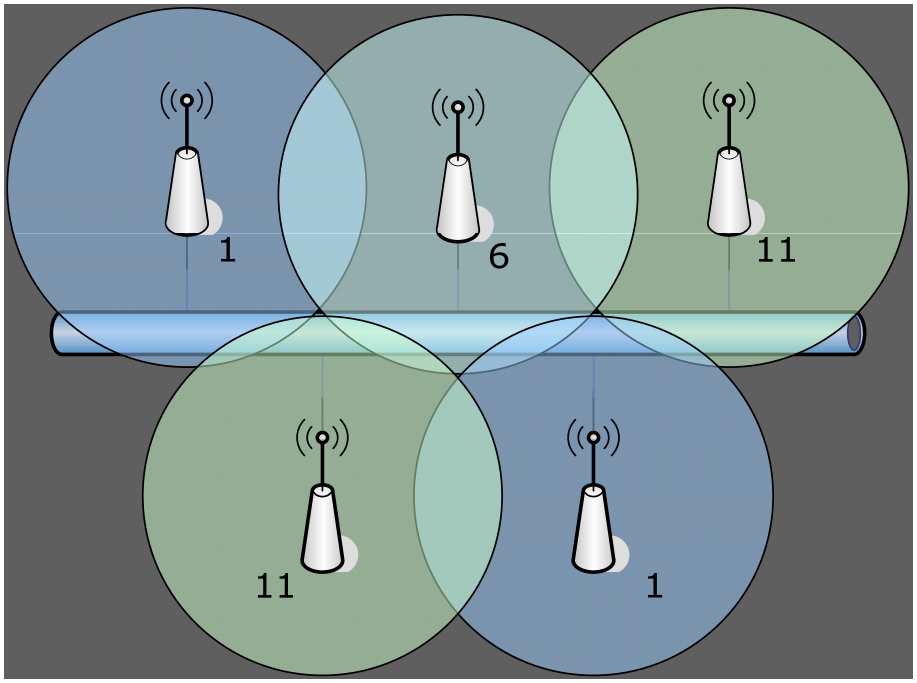
What's not a Mesh?

The ECS Wireless LAN

Multiple APs

Different channels

Same wired subnet



Mesh Approaches

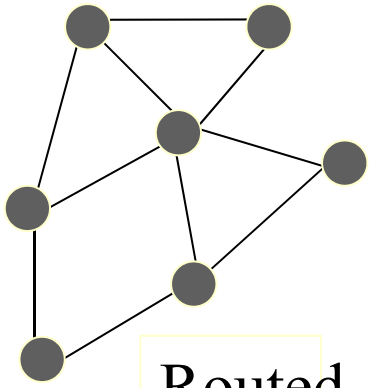
- Ad-Hoc
  - No base station, all hosts are APs
  - Link-local between devices
- Bridging
  - Multiple APs, same subnet
- Routing
  - Multiple APs, multiple subnets
  - WDS links between nodes

Bridging vs Routing

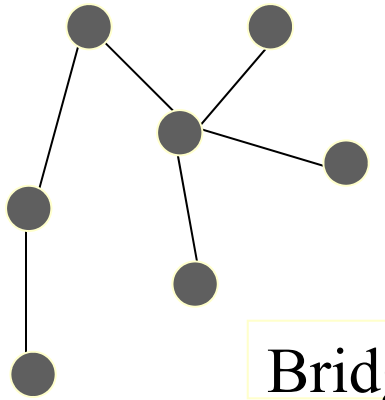
Bridging gives one large subnet

Routing permits multiple paths and external links, reduces bottlenecks

Bridging permits easy mobility



Routed



Bridged

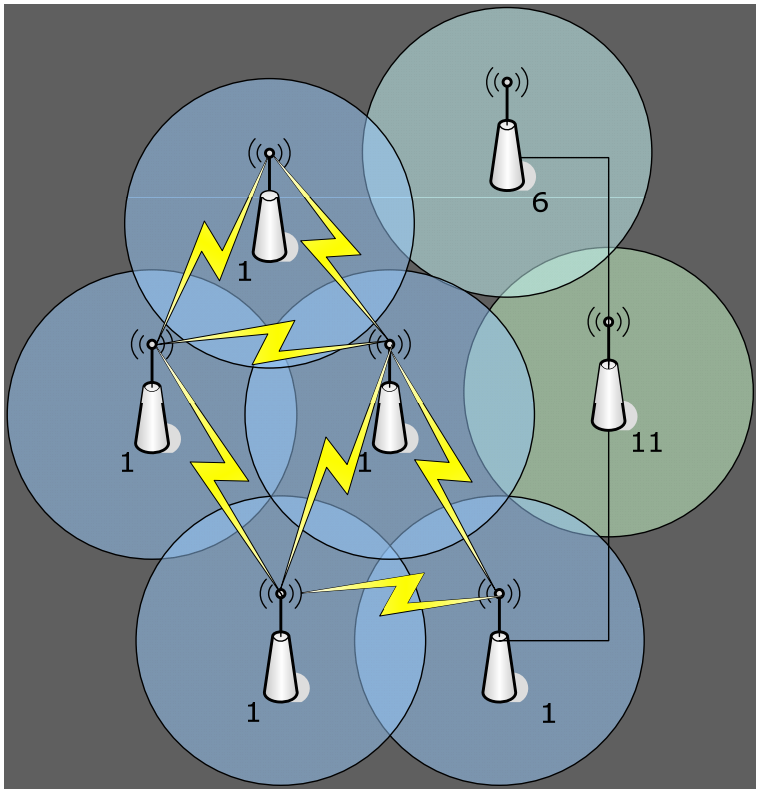
Routed Mesh Networks

WDS

- Wireless Distribution System
- Wireless links between APs, as opposed to wired.
- All are on same channel.

OSPF

- Shortest path routing protocol



Source: Proxim WDS Intro

Mesh Issues

- Scale
  - Bridging does not scale well
  - Single-channel WDS does not scale well
- Distances
  - 1km+ distances are possible…
  - …signal degrades, more users
- Congestion
  - Leads to decreasing performance
  - Colliding channels, hidden node

Mesh Throughput Degradation

All meshed APs on same channel

Data sent from A to G

A – B, full throughput

B – C, ½ throughput

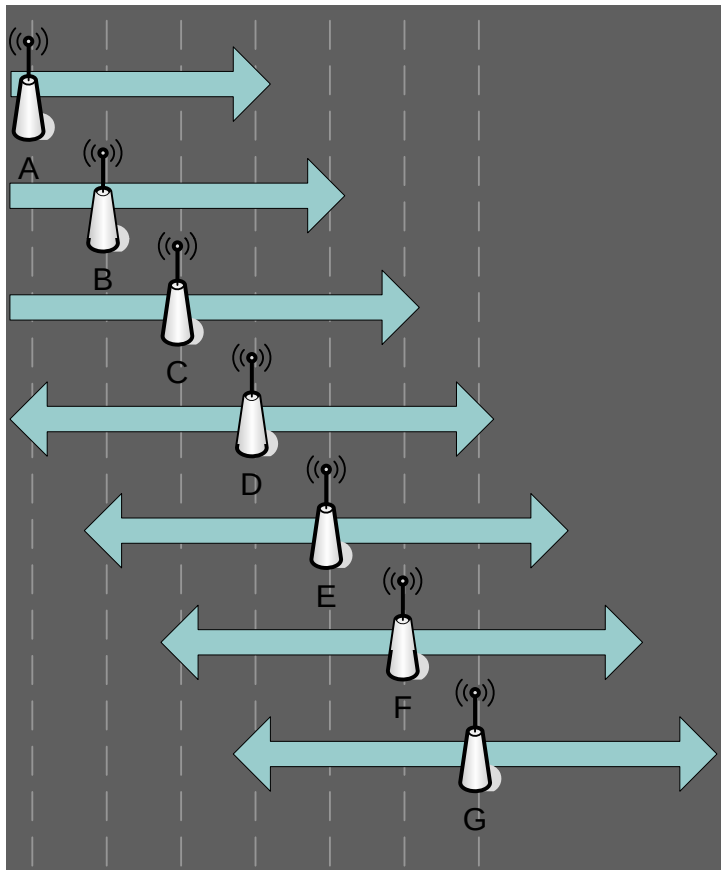
C – D, ¼ throughput

D – E, ⅛ throughput

A now out of range…

E – F, ⅛ throughput

F – G, ⅛ throughput



Source: Wi-fi net news posting

SOWN – A Real Mesh Network?

For a time was a small mesh

- Oakhurst Road to ECS via SUSU

OSPF routing using Linux nodes

Performance degrades very quickly

Hidden node problems

Backbone as a possible future solution

Now just using point-to-point links

Now going infrastructure-based

Security implications

Questions