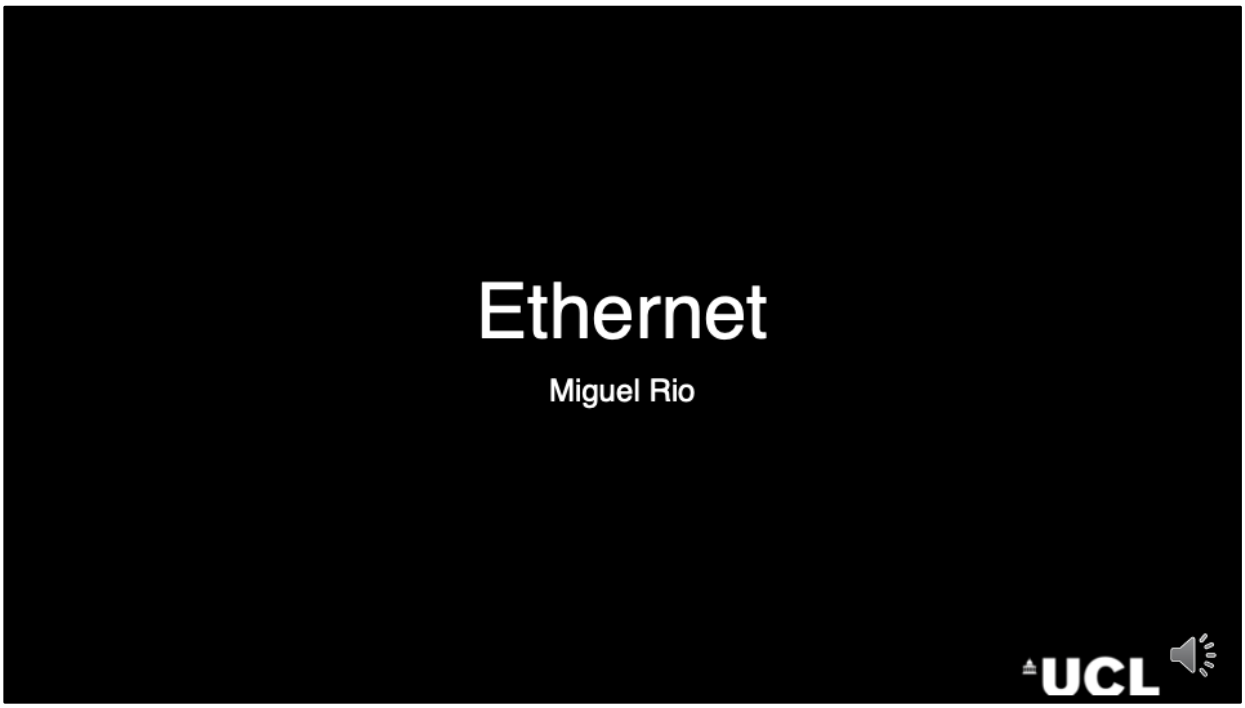
Ethernet

Miguel Rio

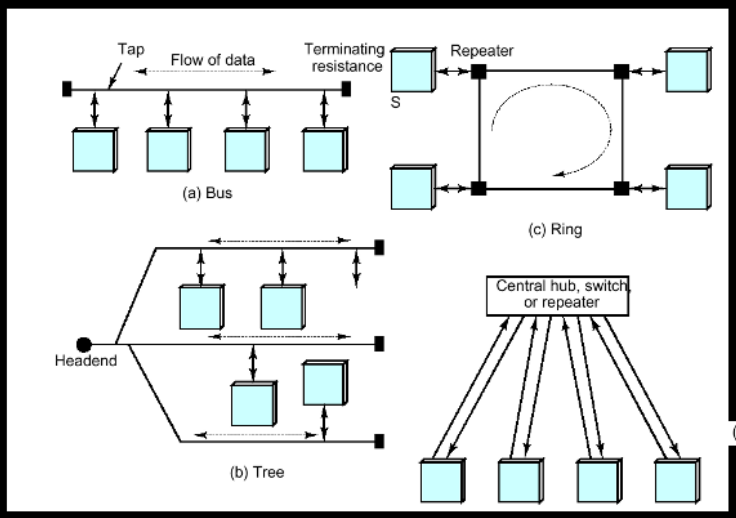


Why is there a need for a LAN?

- The basic reasons why computers are networked are :
- To share resources e.g. files, printers, scanners, internet connections, WAN links
- To share data and applications e.g. common database, help desk software
- To increase productivity by making it easier to share data among users
- To facilitate network management by making the networked computers accessible to the administrator from a centralised site

UCL

LAN Topologies

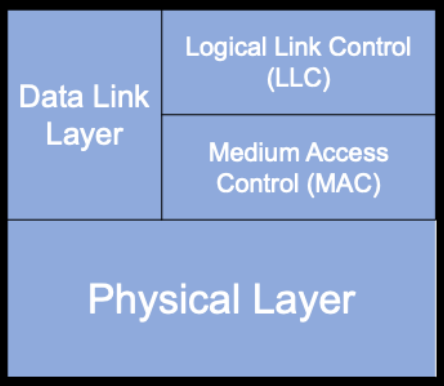


LAN transmission methods

- Unicast transmission
  - a frame is sent from the source to the destination on a network
- Multicast transmission
  - a frame is sent from a source to a subset of nodes on the network
- Broadcast transmission
  - a frame is sent to all nodes on the network

UCL

LAN Protocols and the OSI model



UCL

LAN media access methods

- CSMA/CD – where network devices contend for access to the physical network medium (e.g. Ethernet)
- Token passing – where network devices access the physical network medium based on the possession of a token (Token ring and FDDI)

UCL

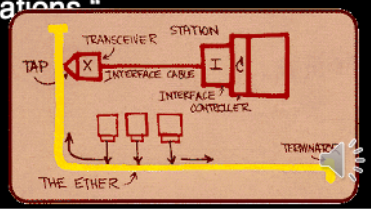
Ethernet

- Ethernet has survived as a LAN technology because of its:-
  - Flexibility
  - Relative simplicity
  - Innovation
    - 10Mbps half duplex and full duplex
    - 100Mbps, 1Gbps, 10Gbps Ethernet
  - Cost
  - Although critics claim that Ethernet cannot scale it continues to dominate the desktop market

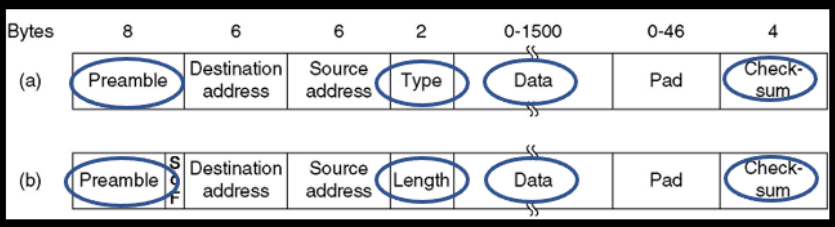
UCL

Ethernet Development Overview

- Originally developed at the Xerox Palo Alto Research Centre in the 1973, patented in 1976.
- In 1980, the first formal Ethernet standard was published when DEC, Intel, and Xerox (DIX) joined together to publish a 10 Mbps Ethernet specification known as Ethernet Version 1.0. In 1982, the DIX alliance updated the standard to include additional media types known as Ethernet Version 2.0.
- In 1983, the IEEE 802 LAN/MAN Standards Committee published a specification for Ethernet -- "IEEE 802.3 Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Access Method and Physical Layer Specifications"
- Thus there are two types of "Ethernet": DIX Ethernet (you can think of it as "the original" Ethernet) and IEEE 802.3 (you can think of it as "the standard" Ethernet).



IEEE 802.3 & DIX Ethernet Frame Formats



- Ethernet type II Frame Format (DIX): (a)
  - Uses a Type field after source address
- 802.3 Ethernet Frame Format: (b)
  - Length field for length of data

Preamble – An alternating pattern of ones and zeros used to tell receiving stations that an Ethernet frame is about to start

Type – Specifies the upper layer protocol to receive the data after Ethernet processing is completed. (Only used in DIX Ethernet)

Length – Indicates the number of bytes if data that follow this field

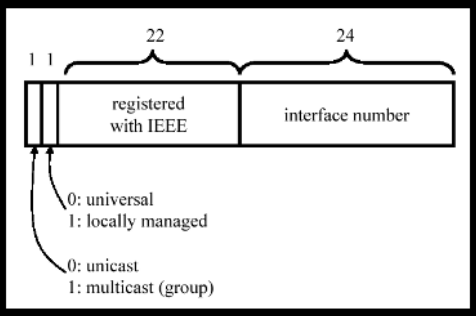
Data - Ethernet expects at least 46 bytes of data

Frame Check Sequence (FCS) – This sequence contains a 4 byte cyclic redundancy check value, used to check for the presence of errors in the frame

UCL

MAC address

- Destination and Source addresses also known as MAC addresses
- MAC addresses identify network entities in Ethernet LANs
- Unique for each LAN interface
- 48 bits in length
  - 22 bits identify the organisational unique identifier (OUI) and it is administered by the IEEE
  - The last 24 bits are vendor assigned
- The MAC address is burned in the ROM of a network interface card (NIC)
- The destination address may be unicast, multicast or broadcast



UCL

Summary

- Local Area Networks
- Ethernet
  - Frame Structure
  - MAC addresses


UCL

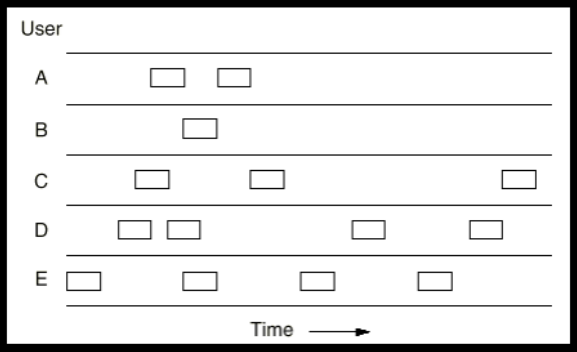

Medium Access Control
UCL

What is MAC?

It is the sublayer that controls the hardware responsible for interaction with the wired, optical or wireless transmission medium

UCL

Pure Aloha

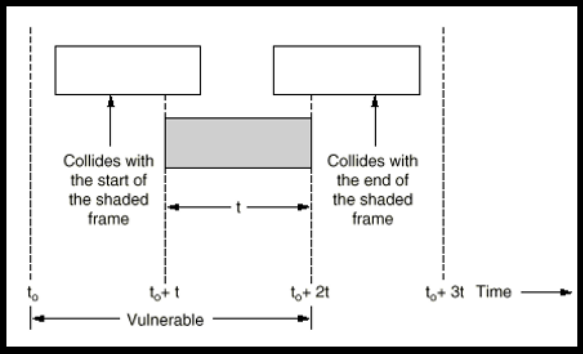


- Transmit when you want to, regardless of others.

Figure 1. ALOHA TCU 1971

UCL

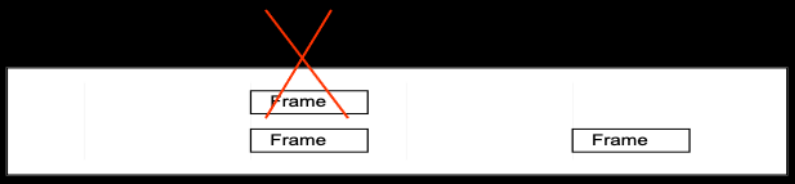
Pure Aloha Collisions



- Extremely inefficient, since the worst-case period of vulnerability is the time to transmit two frames.

UCL

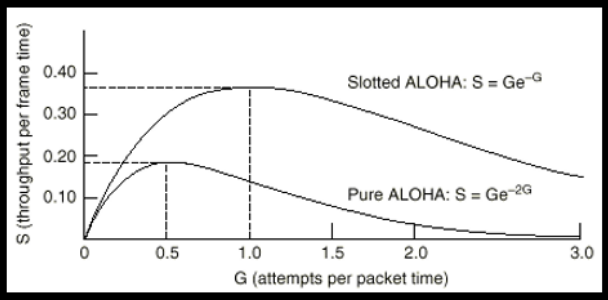
Slotted Aloha



- Transmit only at the beginning of synchronized “slot times”
- Collision inefficiency limited to one frame transmission time

UCL

Aloha vs. Slotted Aloha



- Throughput efficiency increases dramatically for Slotted Aloha.

UCL

CSMA/CD Defined

CS - Carrier Sense (Is someone already talking?)

MA - Multiple Access (I hear what you hear!)

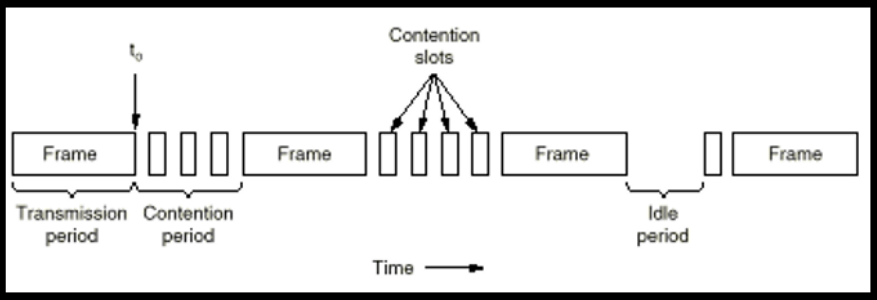
CD - Collision Detection (Hey, we're both talking!)

1. If the medium is idle, transmit anytime.
2. If the medium is busy, wait and transmit right after.
3. If a collision occurs, backoff for a random period, then go back to 1.

We use CSMA/CD in normal group conversation.

UCL

CSMA/CD

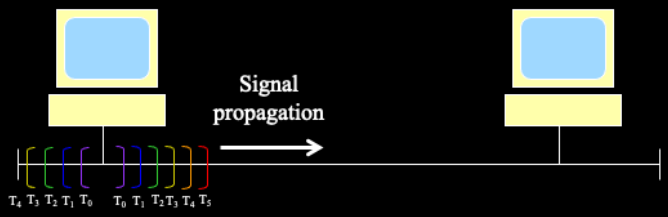


- CSMA/CD can be in one of three states: contention, transmission, or idle.

UCL

CSMA/CD on Ethernet Physical Layer

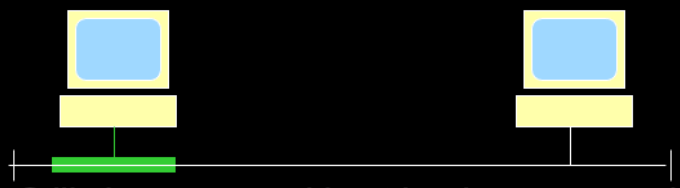
- TIME is proportional to distance over the wire



UCL

Carrier Sense Multiple Access

- Clear wire - host begins transmission



- Still clear - second host begins to transmit

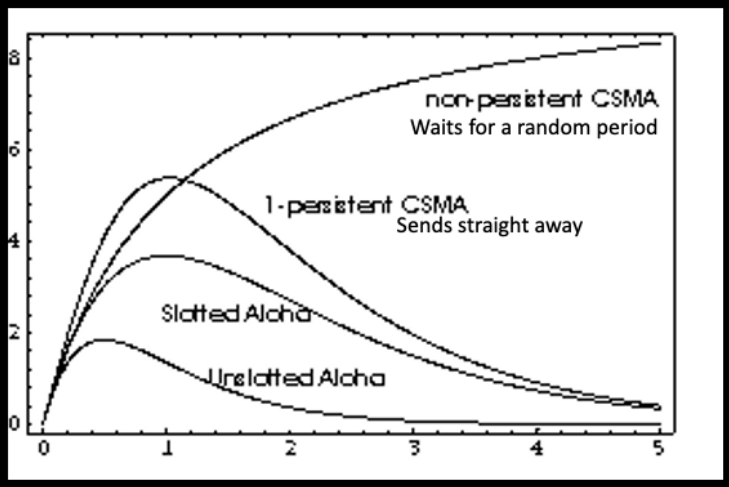
UCL

With Collision Detection

UCL

Performance

Throughput



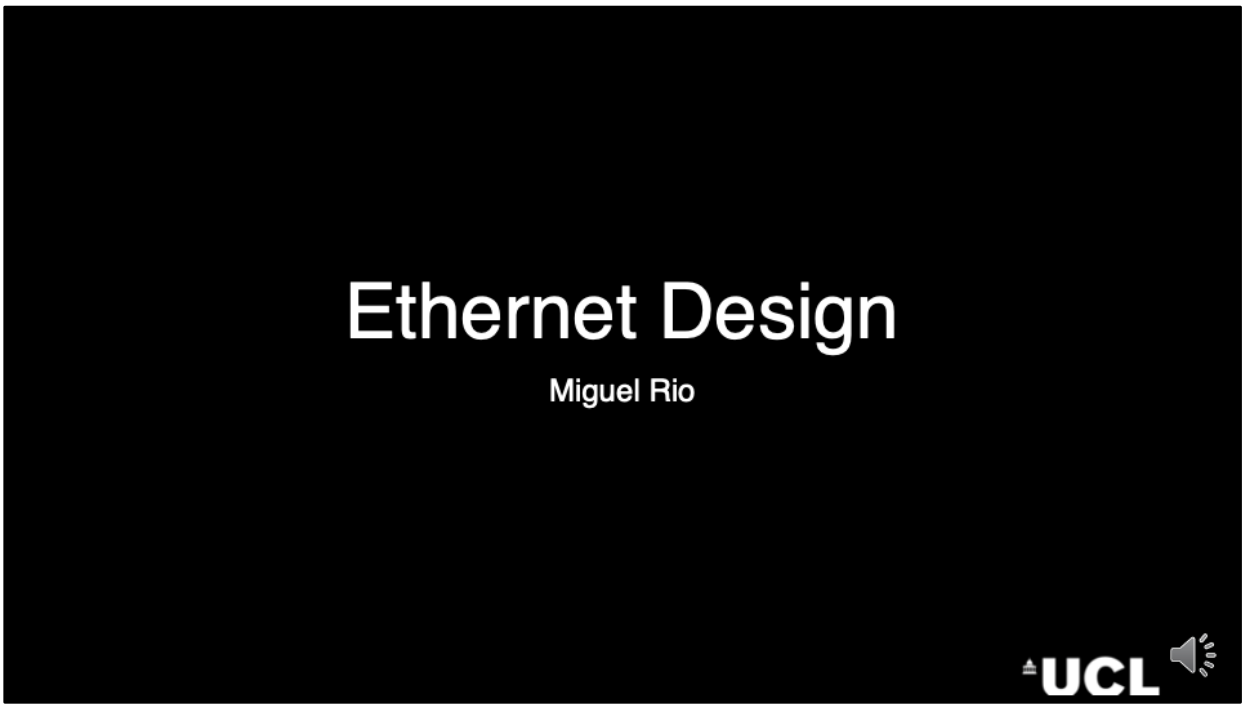
Offered Load

UCL

Summary

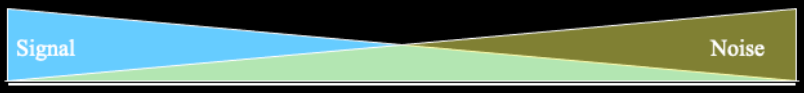
- Medium Access Control Protocols
- CSMA/CD
  - Protocol
  - Performance

UCL


Ethernet Design
Miguel Rio
UCL

Factors Limiting the Length of Ethernet

- Collision Detection - timing
- Attenuation - the signal gets weaker as it propagates along the wire
- Noise - longer wires pick up more noise, which masks the signal



UCL

Ethernet Performance

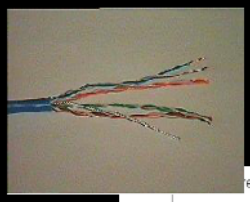
- An Ethernet with less than 20% utilization and less than 0.1% collisions is on **cruise control**
- An Ethernet with more than 40% utilization and greater than 5% collisions **is in trouble**
- If the same frame collides more than 16 times, the network interface card (NIC) will discard it.

UCL

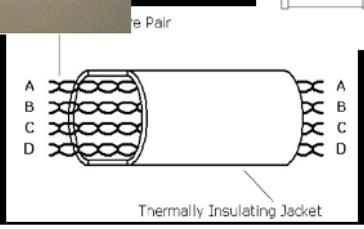
Cable Types

Coaxial Cables
- ThickNet
- ThinNet

Unshielded Twisted Pair (UTP), CAT 5, CAT 6, CAT 7

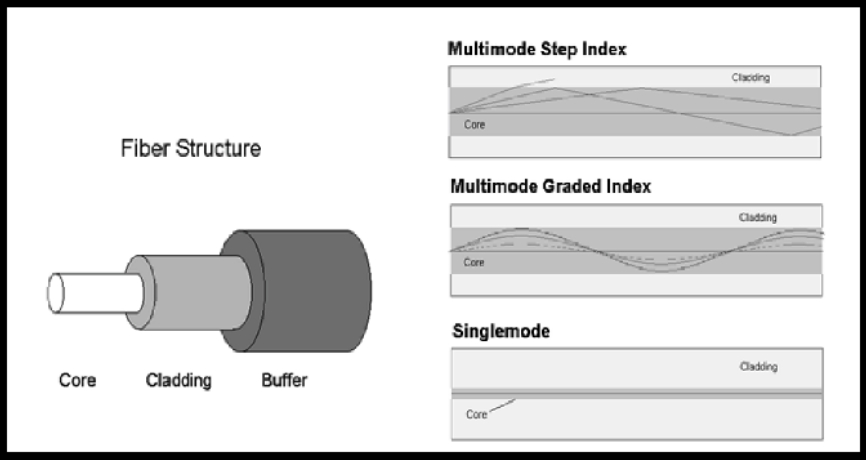


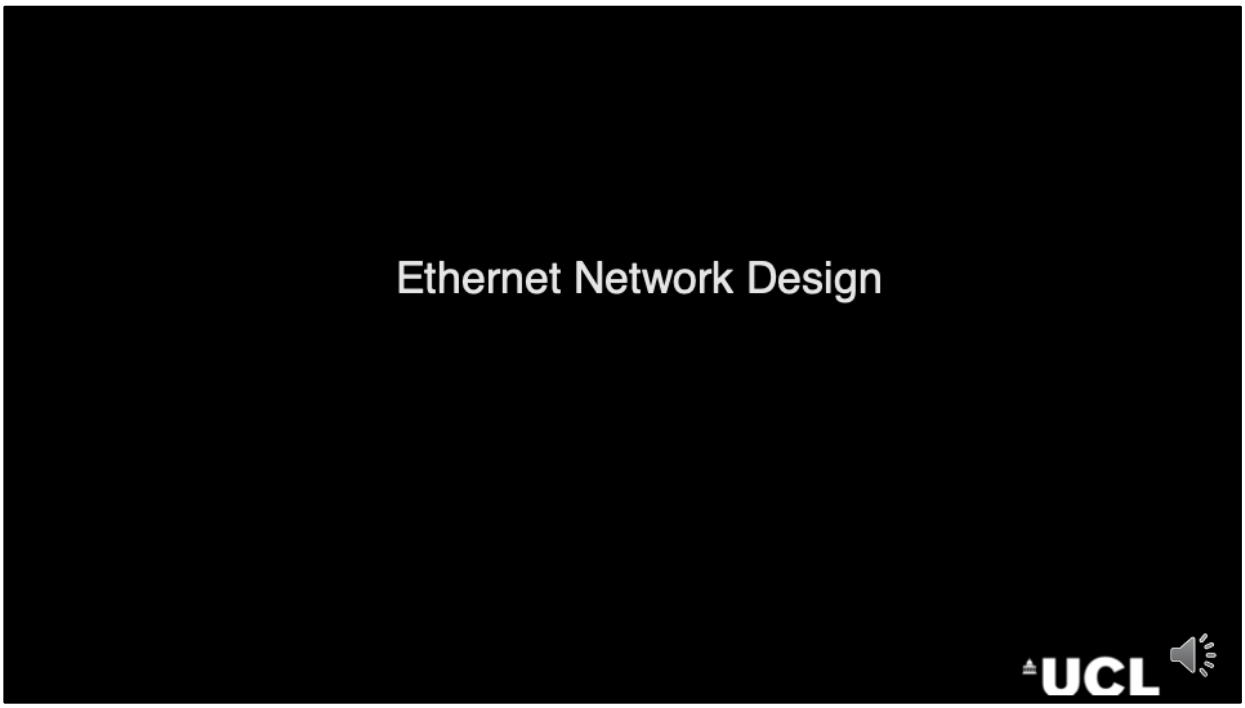
1	2	3	4	5	6	7	8
Solid White, Orange Stripe	Solid Orange, White Stripe	Solid White, Green Stripe	Solid Blue, White Stripe	Solid White, Blue Stripe	Solid Green, White Stripe	Solid White, Brown Stripe	Solid Brown, White Stripe



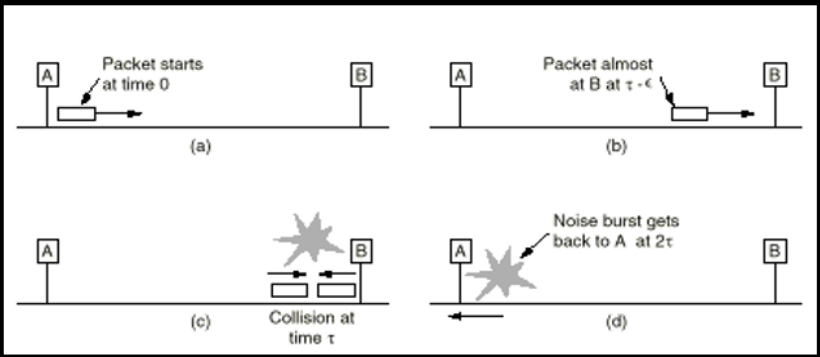
UCL

Fibre Types


Fiber Structure
Core
Cladding
Buffer
Multimode Step Index
Cladding
Core
Multimode Graded Index
Cladding
Core
Singlemode
Cladding
Core


Ethernet Network Design
UCL

The Collision Domain



- A collision domain is defined as an area within which frames that have collided are propagated.
- Collision detection can take as long as 2τ, worst case.
- This "round-trip" delay defines the max Ethernet network diameter, or collision domain.
- Round-trip delay = 512 bit times for all Ethernets.

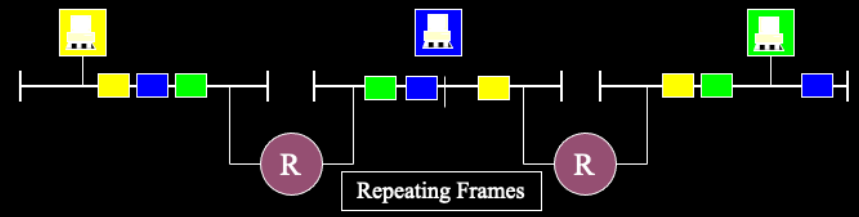
UCL

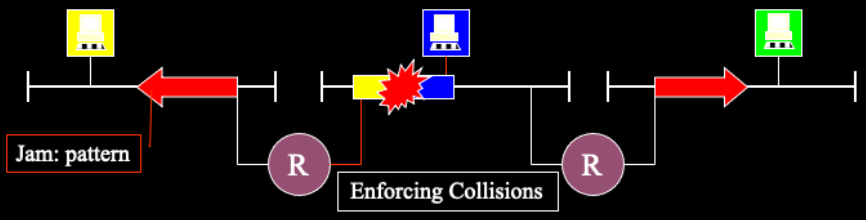
Repeaters

- Works at layer 1 (PHY layer) ONLY
  - Repeaters don't understand frames they only understand BITS
- Repeat incoming signal from a port to all other ports with, restored timing, restored waveform shape, very little delay
- If 2 or more simultaneous receptions, transmit jam
- Class I repeaters may be used to repeat between media segments that use different signalling techniques (timing delays upto 140 bit times)
- Class II repeaters can only connect segments using the same signalling technique (timing delays up to 92 bit times)

UCL

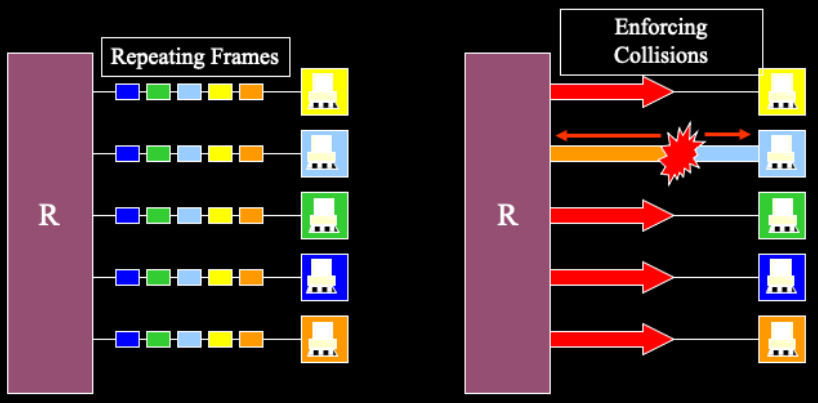
Repeater Action





UCL

HUBs are Multi-port Repeaters

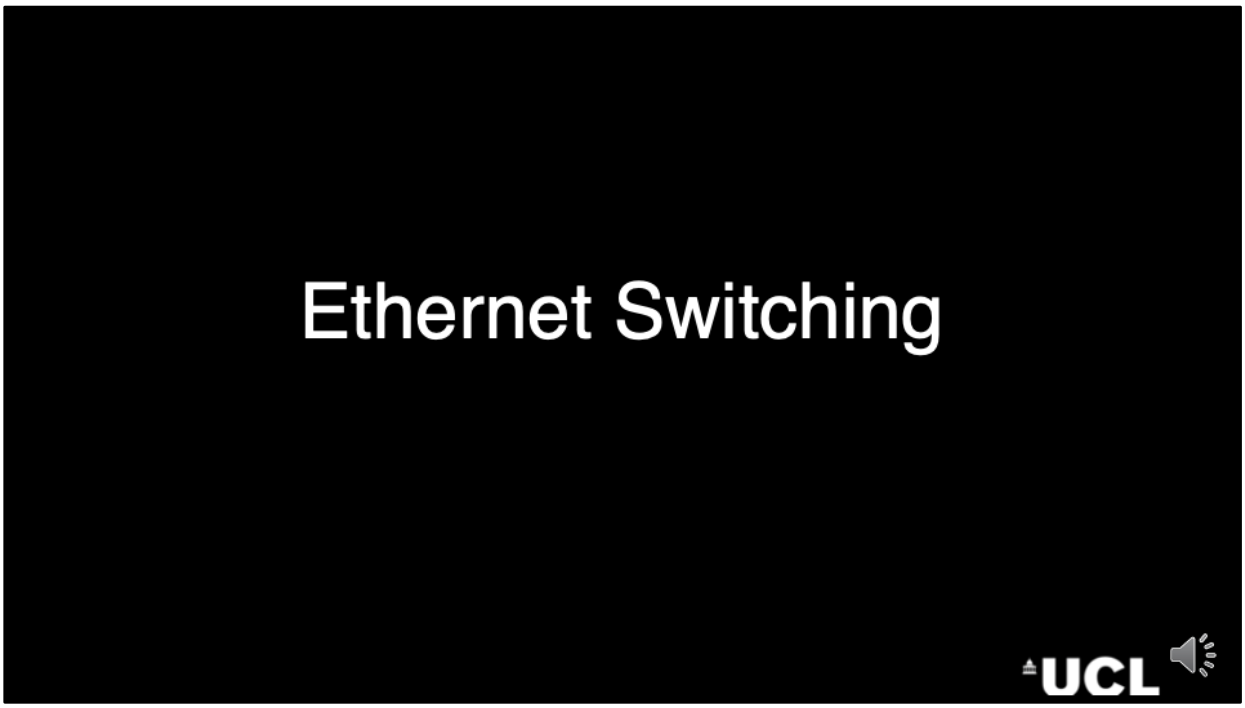


- All share the 10Mb ethernet bandwidth; Frames appear everywhere;
- Comprise a single COLLISION DOMAIN
- Everyone's frames collide with everyone else's; Every collision appears throughout the domain

UCL

Summary

- Ethernet Performance
- The Collision Domain
- Repeaters
- Hubs


Ethernet Switching
UCL

BRIDGES

- Bridges separate collision domains
  - Collision domains do not extend across the bridge
  - Timing rules “restart” at a bridge port
  - Bridge is a store and forward device
- Bridge Properties
  - Frame Forwarding
  - Learning
  - Filtering
  - Spanning Tree

UCL

Bridge Properties – Forwarding

- The bridge receives a frame on one port and transmits it on another port
- The bridge stores (buffers) the frame
  - The other port checks that the wire is clear
  - The other port transmits the frame
  - If a collision occurs, back off and retransmit
- Collisions don't propagate across bridges
- Bridges can connect dissimilar networks

UCL

Bridge Properties – Learning & Filtering

- Learning
  - The bridge examines the layer 2 source addresses of every frame on the attached networks (promiscuous listening)
  - The bridge maintains a table, or cache, of which MAC addresses are attached to each of its ports
- Filtering
  - The bridge examines the destination MAC address of each frame on its attached networks
  - If the destination is on the same port as the source, the frame is not forwarded
  - The frame is forwarded ONLY to the port the destination is attached to
  - Eliminates unnecessary traffic on the attached networks

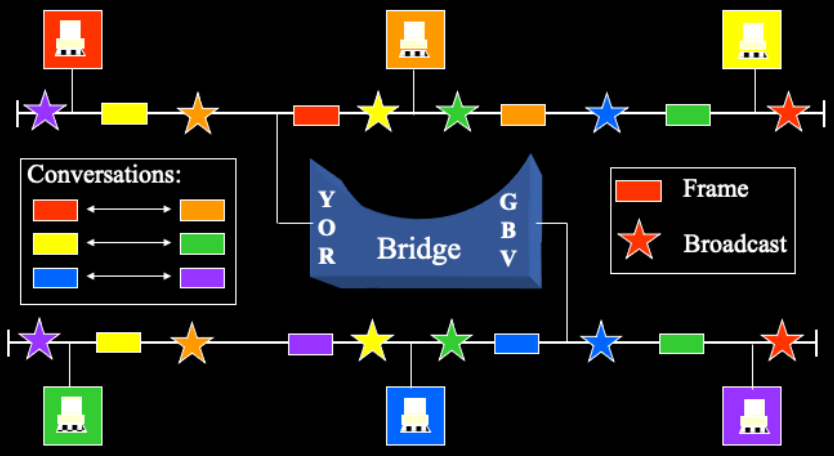
UCL

More Forwarding & Filtering

- A broadcast is a frame destined for every host on the network. Bridges forward broadcasts to every one of their ports – Called “Flooding”
- If a bridge sees a destination address it has not yet learned, it also floods that frame
- Bridges are called layer 2 devices because they examine layer 2 information and modify their behavior accordingly

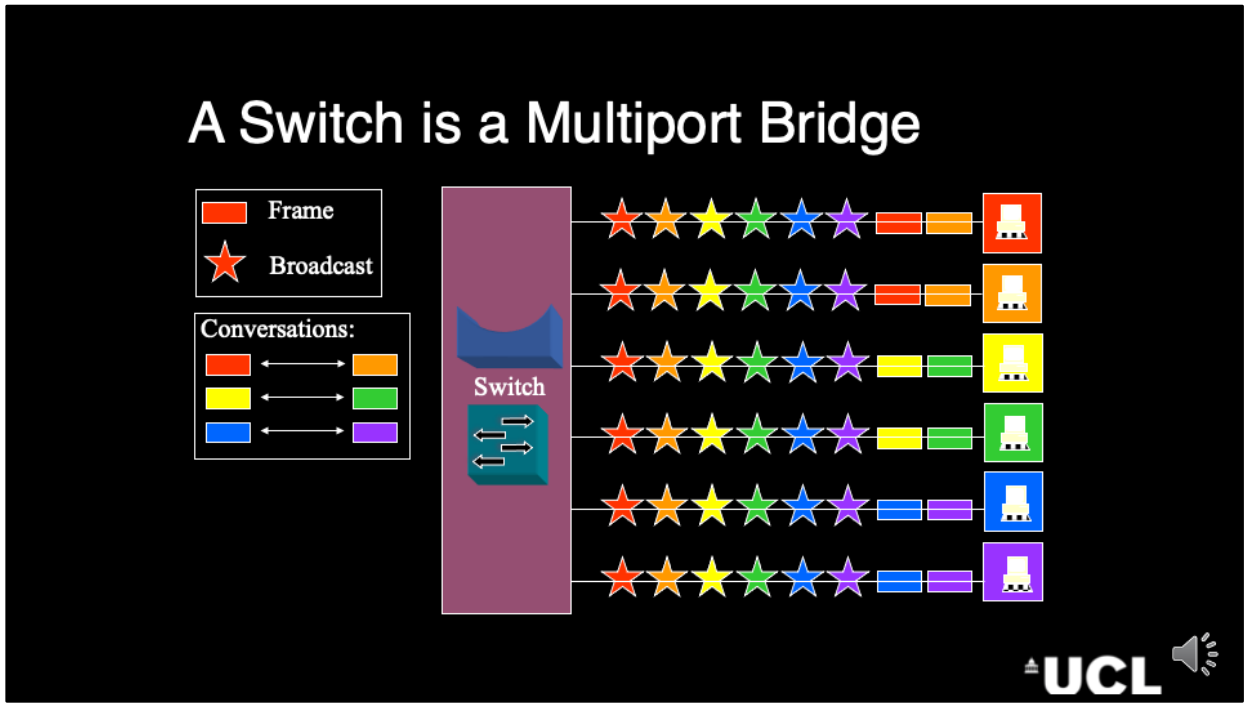
UCL

Forwarding, Learning, Filtering

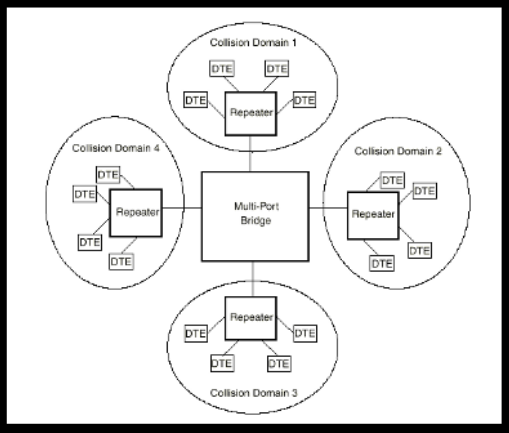


UCL

A Switch is a Multiport Bridge



Breaking up Collision Domains

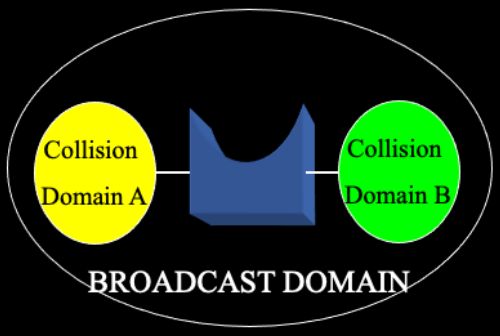


- Repeaters are inside the collision domain, since they propagate collisions
- Bridges/Switches break up the domains, since they operate at layer 2 and buffer packets before sending them

UCL

Broadcast Domain

- A Network Interconnected by Bridges Comprises a BROADCAST DOMAIN
- Broadcasts from one host are seen by every other host on the bridged network
- If a NIC receives a frame not addressed to it, the NIC ignores the frame. This decision is made without interrupting the CPU.
- BUT, broadcasts contain higher-layer information. Processor interrupt required.



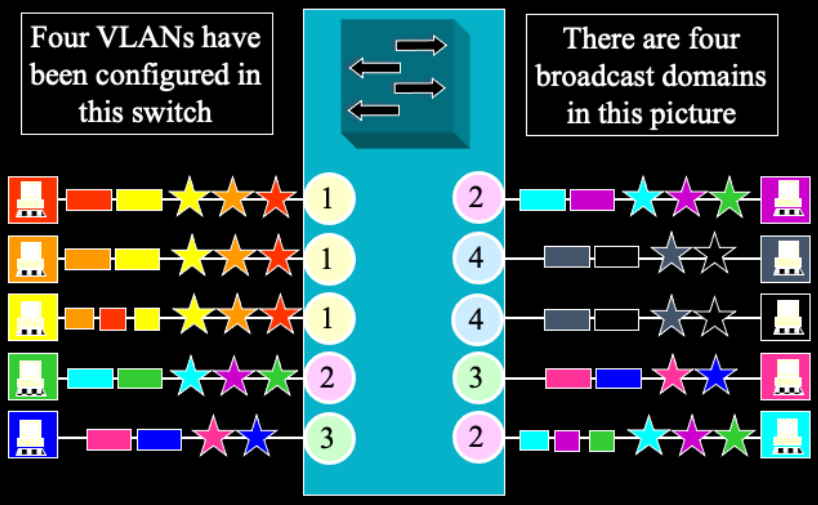
UCL

Managing Broadcast Domains: VLANs

- In a bridged network, broadcast and multicast traffic is sent everywhere
- 100mbps traffic could thus congest 10mbps networks
- It is therefore necessary to isolate broadcast domains
- This may be done using multiple virtual local area networks VLANs within the switches or network

UCL

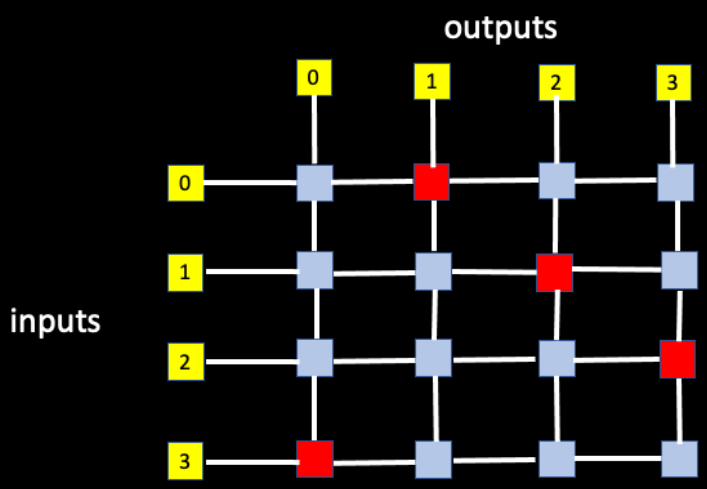
VLANs



Each VLAN is one broadcast domain

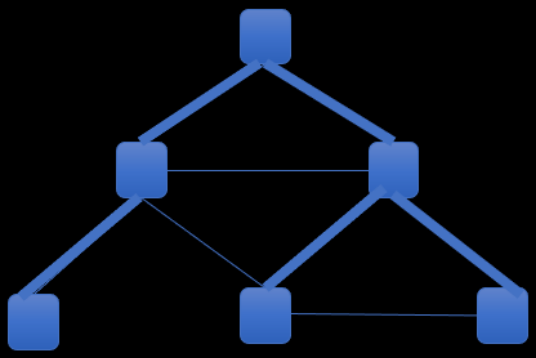
UCL

Switching implementation: Crossbar



UCL

Spanning Tree Protocol



- In many scenarios ethernet switches are connected in network with redundancy
- Broadcasts would be retransmitted forever
- STP builds a spanning tree with a root
- Broadcasts are never repeated

UCL

A Poem

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

UCL

Summary

- Bridges
- Switches
- VLANs
- Crossbar
- Spanning Trees

802.11

Miguel Rio

UCL

WIFI stats

- By 2021, 63 percent of global mobile data traffic
- By 2021, 29 percent of the global IP traffic will be carried by Wi-Fi networks
- Typically 3:1 compared with cellular.

Cisco Visual Networking Index

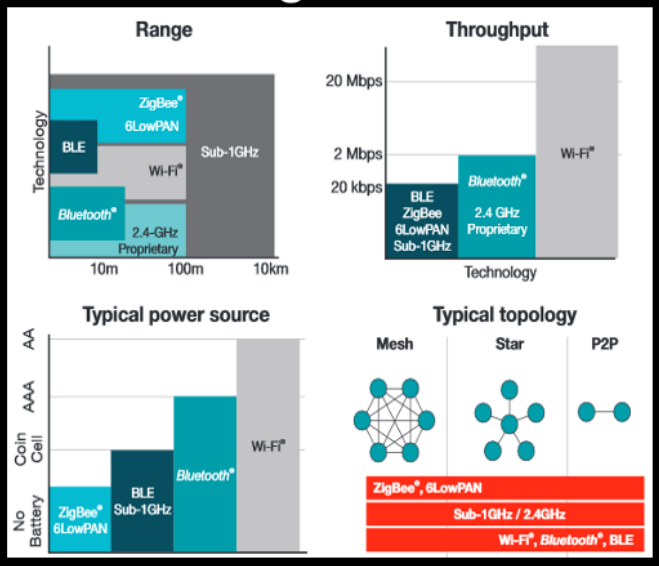
UCL

Challenges of wireless networking

- In wireless networks have a more limited range as the signal strength decreases more rapidly with distance (inverse square law), and is attenuated as it passes through different media.
- Wireless links have a higher Bit Error Rate due to noise, interference and multipath.

UCL

Wireless Technologies – Summary



UCL

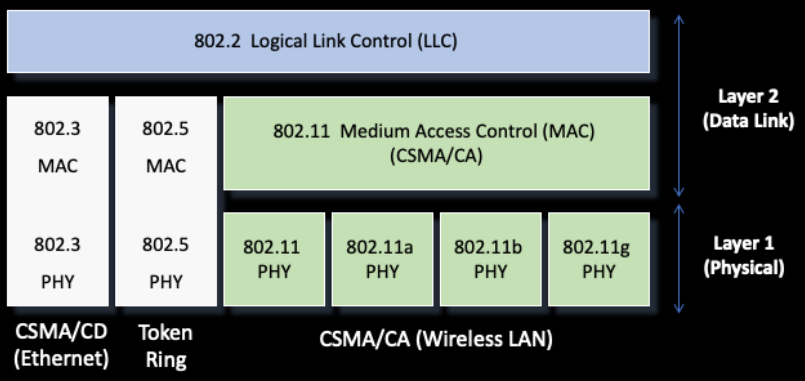
Relevant IEEE Standards

The big picture:

Standard	Description
802.3	CSMA/CD ("Ethernet")
802.5	Token Ring
802.11	Wireless LAN ("WiFi" family of standards)
802.15	Wireless personal area networks (WPAN) – Bluetooth, Zigbee etc.
802.16	Fixed Broadband Wireless Access System ("WiMax")

UCL

IEEE 802 standardisation framework



Multiple air interface options, one common MAC layer based on CSMA/CA

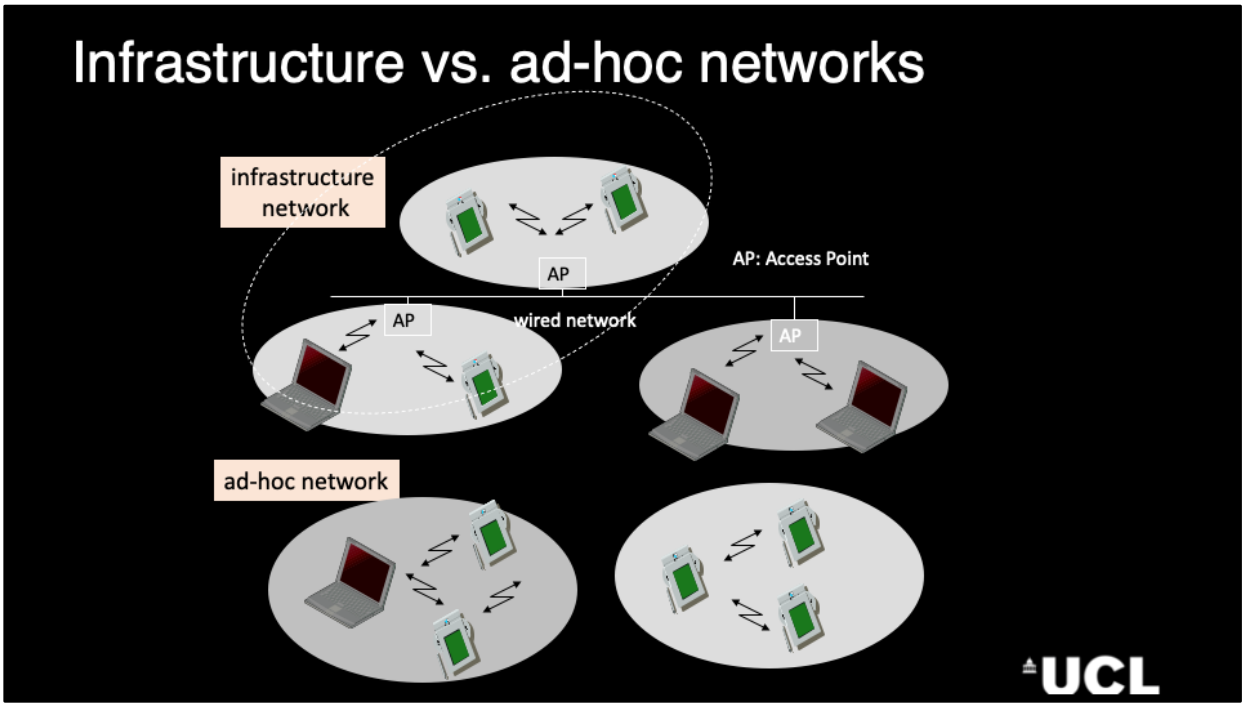
UCL

IEEE 802.11

- Presented as the first true industry standard WLAN (released 1997)
  - The very first “WiFi” standard.
  - Provided data rates of 1Mbps or 2Mbps with range of 20 to 30m.
- 802.11 standard covers two aspects of the protocol stack
  - Physical transport (PHY)
  - Media access control (MAC)
- Two network configurations are supported
  - ad-hoc - no structure and no fixed points (IBSS)
  - infrastructure - fixed network access point, can bridge to fixed networks. (ESS)

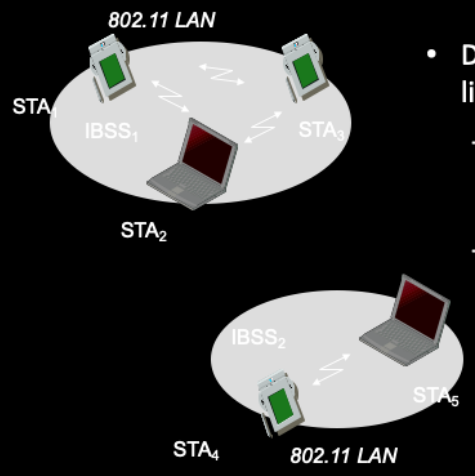
UCL

Infrastructure vs. ad-hoc networks



UCL

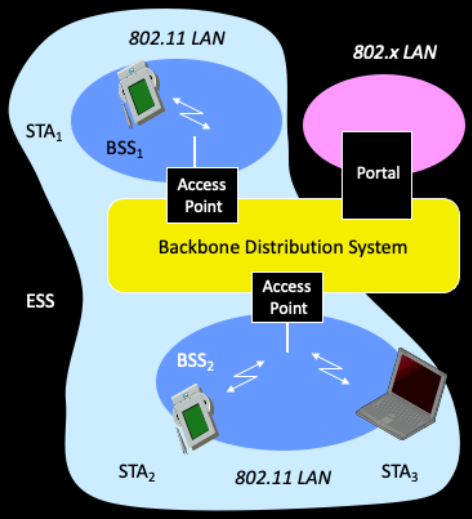
Architecture of an ad-hoc network (802.11)



- Direct communication within a limited range
  - **Station (STA):** terminal with access mechanisms to the wireless medium
  - **Independent Basic Service Set (IBSS):** group of stations using the same radio frequency

UCL

Architecture of an infrastructure network (802.11)



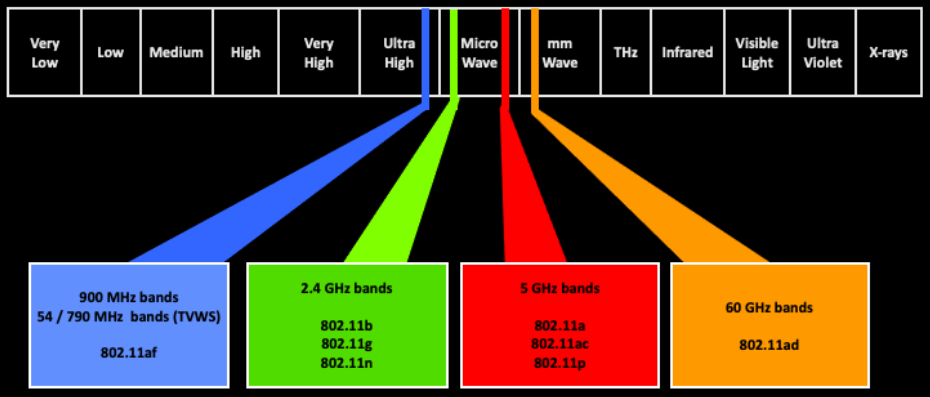
- **Station (STA)**
  - terminal with access mechanisms to the wireless medium and radio contact to the access point
- **Basic Service Set (BSS)**
  - group of stations using the same radio frequency
- **Access Point (AP)**
  - station integrated into the wireless LAN and the distribution system
- **Portal**
  - bridge to other (wired) networks
- **Distribution System**
  - interconnection network to form one logical network (EES: Extended Service Set) based on several BSS

Ref : Schiller , p208

UCL

WLAN frequency bands - ISM

WLAN systems make use of the "Industrial, Scientific, and Medical" (ISM) bands. These are unlicensed frequencies available for free use in most countries, subject to power limitations.



900 MHz bands
54 / 790 MHz bands (TVWS)

802.11af

2.4 GHz bands

802.11b
802.11g
802.11n

5 GHz bands

802.11a
802.11ac
802.11p

60 GHz bands

802.11ad

https://commons.wikimedia.org/

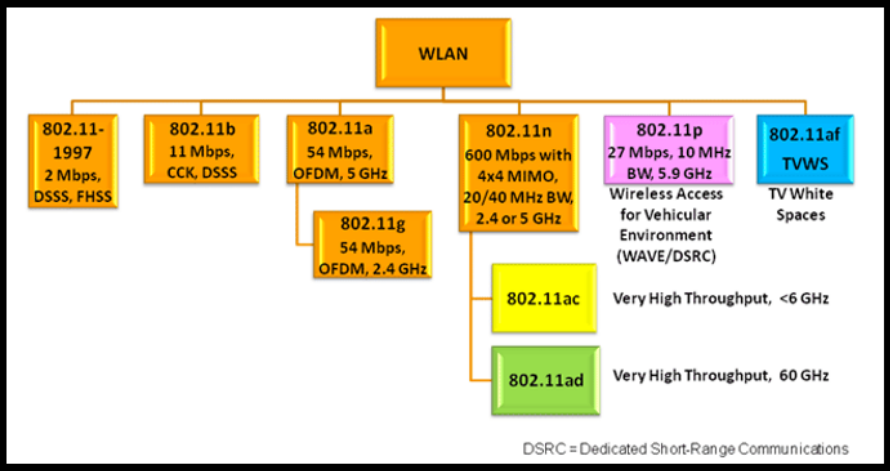
UCL

Summary of 802.11 standards

802.11 Version	Release Date	Operating Frequency	Bandwidth (MHz)	Speed	Modulation
Original	Jun-97	2.4 GHz	20	1Mbps or 2Mbps	DSSS, FHSS
a	Sep-99	5 GHz	20	Up to 54Mbps	OFDM
b	Sep-99	2.4 GHz	20	Up to 11Mbps	DSSS
g	Jun-03	2.4 GHz	20	Up to 54Mbps	OFDM, DSSS
n	Oct-09	2.4 / 5 GHz	20 / 40	Up to 600Mbps	OFDM, 64-QAM
ac	Dec-13	5 GHz	80/160	Up to 1.6Gbps	OFDMA, 256-QAM
ad	May-09	60 GHz	2.16 / 8.64 GHz	Up to **7 Gbps**	OFDM, 64-QAM
p	Jul-10	5.9 GHz	5/10/20	3Mbps to 27Mbps	OFDM, 64-QAM
af	Feb-14	54 / 790 MHz (TVWS)	6MHz	Up to 40Mbps	OFDMA, 256-QAM

UCL

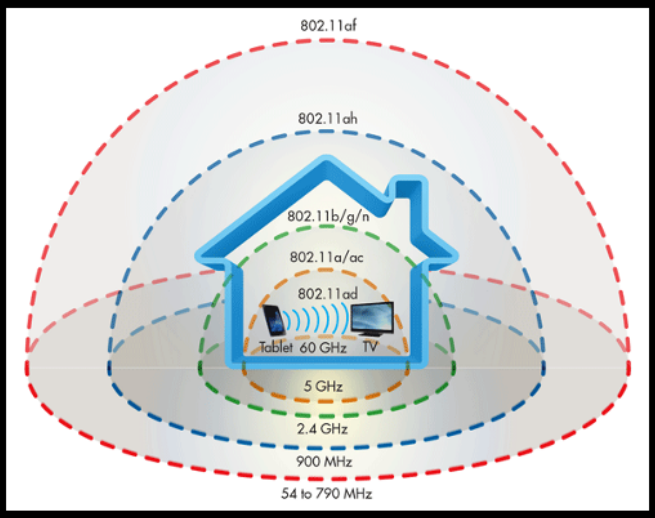
802.11 standards family tree



UCL

Range of 802.11 standards

Standard	Range
802.11ad	~10m
802.11a/ac	~35m
802.11b/g/n	~70m
802.11ah	~ 1km
802.11af	~ 1km



UCL

802.11a

- Confusingly, 802.11a is a more advanced system than 802.11b. Both standards were ratified at around the same time.
- 802.11a specification operates at radio frequencies between 5.15 and 5.825 GHz, i.e. 802.11a utilizes 300 MHz bandwidth in Unlicensed National Information Infrastructure (U-NII) band.
- The FCC has divided total 300 MHz in this band into three distinct 100 MHz bands: low, middle, and high, each with different legal maximum power.

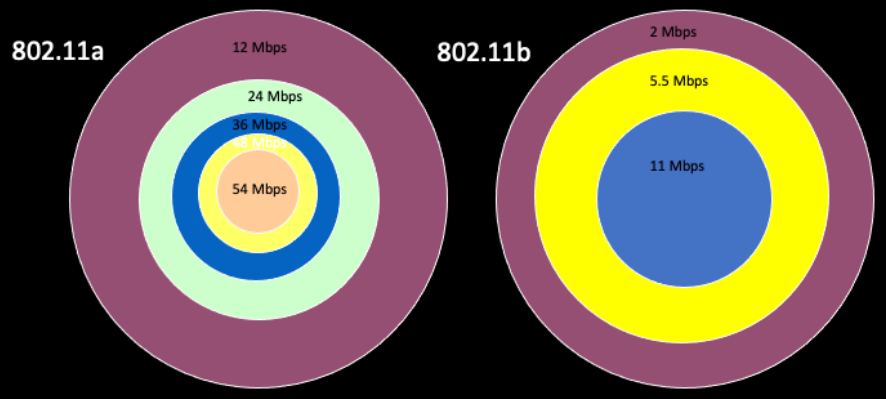
	Band	Channel	Max Power
High band	5.725-5.825 GHz	9-12	1000 mW
Middle band	5.25-5.35 GHz	5-8	250 mW
Low band	5.15-5.25 GHz	1-4	50 mW

UCL

Data rates vary with distance

The 802.11 standards support various data rates that are implemented by varying the number of subcarriers, the modulation scheme, etc. There is a rate fall back mechanism, i.e., as the distance between the transmitter and receiver increases, the supported data rate decreases.

For example, the cases of 802.11a and 802.11b are shown here.



UCL

802.11g

- 802.11g offers throughput of 802.11a with backward compatibility of 802.11b.
- 802.11g operates over 3 non-overlapping channels.
- 802.11g operates in 2.4 GHz band but it delivers data rates from 6 Mbps to 54 Mbps.
- 802.11g also uses OFDM but supports spread-spectrum capabilities if any one component of the system has older equipment, i.e., 802.11b equipment.
- 802.11g's "backward compatibility" with 802.11b means that when a mobile 802.11b device joins an 802.11g access point, all connections on that access point slow down to 802.11b speeds.

UCL

Comparing 802.11a and 802.11g

- 802.11a operates in underused 5 GHz band; 802.11g operates in heavily used 2.4 GHz band.
- 802.11g systems experience interference from other 2.4 GHz devices such as cordless phones, microwave ovens, satellites, etc.
- Both 802.11a and 802.11g offers up to 54Mbps speeds in the lab.
- In the field, 802.11a delivers about 20Mbps.
- 802.11b's 11Mpbs theoretical speed is more often 4Mbps in practice.
- The realistic data rates quoted for 802.11g thus far range from 6 Mbps to 20 Mbps.
- 802.11g has to contend with more interference in the 2.4 GHz range as compared to 11a in the 5 GHz band.

UCL

802.11 frame format

FC = Frame control
D/I = Duration/connection ID
SC = Sequence control

Figure 1: IEEE 802.11 MAC frame format. Image from William Stallings "Data and Computer Communications".

- Very similar to Ethernet
- Duration of connections
- Several addresses, depending if we are using IBSS or BSS

UCL

Summary

- 802.11
- Ad-Hoc vs Infrastructure
- Evolution of 802.11 standards
- Frame format

UCL


CSMA/CA
Miguel Rio
UCL

IEEE 802.11 MAC

As in non-switched Ethernet, a Multiple Access scheme is required to allow multiple users to all transmit within the allotted spectrum without interfering with each other.

UCL

Why not CSMA-CD?

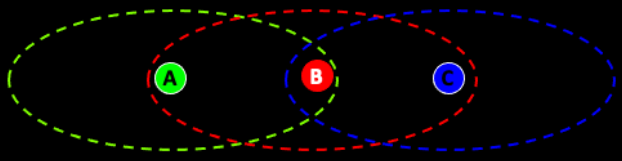
Collision detection (CD), as used in wired LAN, will not work in a wireless LAN because:

- It is not possible to detect a collision: the power of a radio transmission decreases rapidly with distance, listening while transmitting only results in hearing yourself.
- On a wireless network it's not always possible for a station to hear all the other stations, so a sending station that is free to transmit has no way of knowing if the receiving station is free as well. This gives rise to the Hidden Terminal Problem and the Exposed Terminal Problem.

UCL

The Hidden Terminal Problem

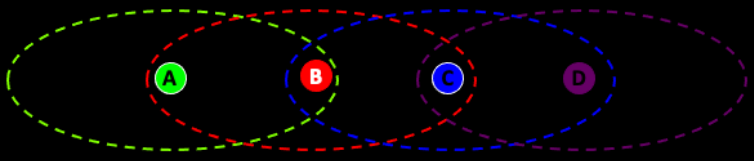
- Station A can communicate with Station B, because they are in range.
- Station C can also communicate with Station B, because they are in range.
- Stations A and C cannot communicate with each other since they are out of range and cannot sense each other.
- Nodes A and C may start to send packets simultaneously to B and there will be a collision at the B receiver. This is unavoidable because A and C cannot detect each other's transmissions as they are out of range of each other.
- This problem cannot be solved using conventional CSMA-CD



UCL

The Exposed Terminal Problem

- Station B wants to transmit to Station A. At the same time, Station C wants to transmit to Station D
- Both transmissions could happen simultaneously without interference, since since A is out of range of C and D is out of range of B. There would only be interference in the path between B and C but this doesn't matter as B and C are not trying to communicate with each other in this instance.
- If B starts transmitting, C will sense the channel and falsely think it cannot transmit, so it will remain silent even though it could have transmitted to D without causing any interference to A.
- This problem cannot be solved using conventional CSMA-CD either.



UCL

Multiple Access in 802.11

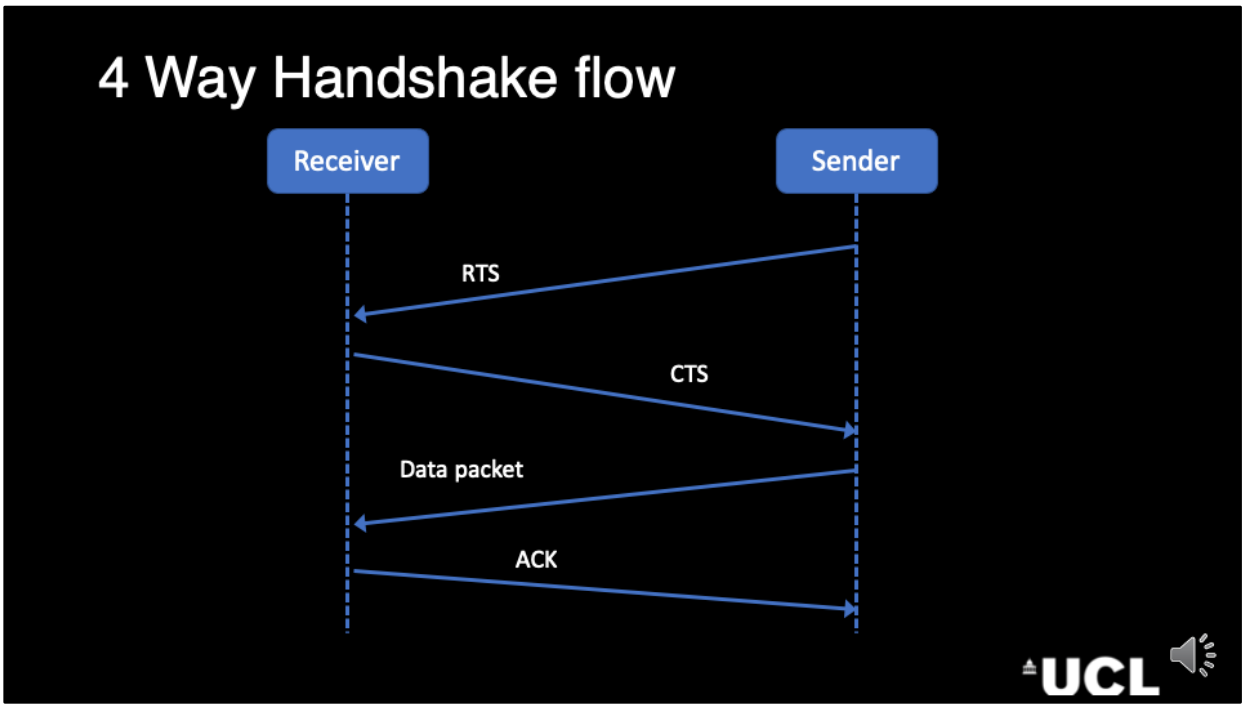
- Multiple Access in 802.11 is handled by means of the Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism.
- The first rules of CSMA/CA are :
  - Only one person talks at a time, the others listen
  - Nobody interrupts or talks over someone else
- If you have something you wish to say, you first listen to ensure that nobody else is talking. If the channel is clear, then you can talk. This is the carrier sense part of CSMA

UCL

Collision Avoidance

- What happens if two dinner guests sense a lull in the conversation and both start talking at the same time? This is a collision.
- In 802.11 terminology, a collision occurs when two (or more) transmitters detect a quiet channel and both start transmitting at the same time.
- The collision will result in an undecipherable message to the intended receivers (listeners).
- But in the wirless word one cannot detect these collisions
- 802.11 handles collisions with a 4 way handshake.

UCL

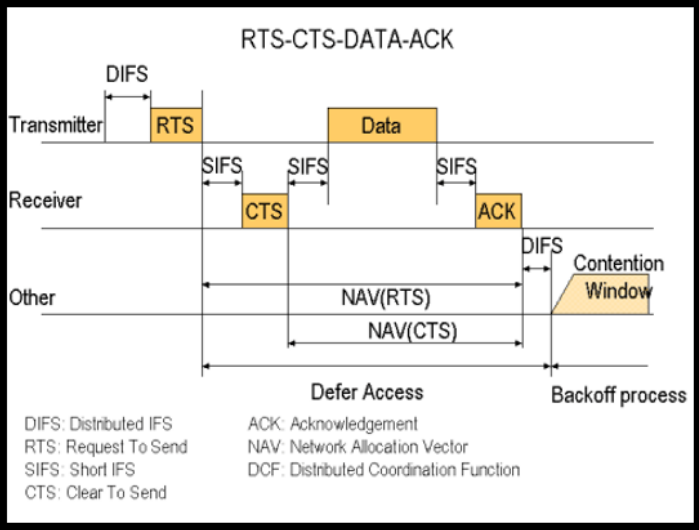

4 Way Handshake flow
Receiver
Sender
RTS
CTS
Data packet
ACK
UCL

Collision Management : 4 Way Handshake

1. "Listen before you talk" : If the channel is busy, node backs-off for a random amount of time after waiting DIFS, just as before.
2. But now, instead of packet, sends a short message: Ready to Send (RTS) which lets the other nodes know that a message packet is coming.
3. RTS contains destination address and duration of message. The RTS tells everyone else to back-off for the duration.
4. If RTS reaches the destination successfully, the destination sends a Clear to Send (CTS) message after waiting a prescribed amount of time, called Short Inter Frame Space (SIFS).
5. After receiving the CTS, the original transmitter transmits the information packet.
6. Other nodes in range of the receiver detect the CTS signal and refrain from transmitting for a time known as the Network Allocation Vector (NAV).
7. The receiver uses the CRC to determine if the packet has been received correctly. If so, the receiver sends out an ACK packet.
8. If the information packet is not ACKed, then the source starts again and tries to retransmit the packet.

UCL

Collision Management : 4 Way Handshake



UCL

Summary

- CSMA/CA
- Hidden Terminal Problem
- The exposed Terminal Problem
- 4-way handshake

UCL

802.11 Protocol

Miguel Rio

802.11 Frame Types

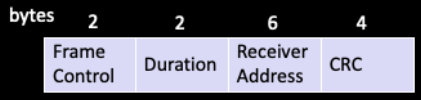
- Management Frames
- Control Frames
- Data Frames

Management Frames

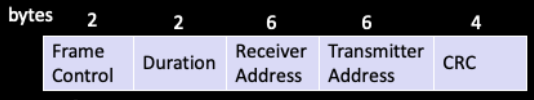
- Beacon
- Probe Req/Res
- Association Req/Res
- Reassociation Req/Res
- Authentication Frame
- Deauthentication & Disassociation
- Action Frames
- Channel Switch Announcement

802.11 Control Frames: ACK, RTS, CTS

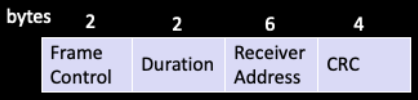
RTS (Request To Send)



CTS (Clear To Send)



ACK (Acknowledgement)



UCL

802.11 control frames (contd)

- PS-Polling
  - Some devices may want to go to sleep mode to save power
  - Node indicates to AP that it's going into power save mode
  - AP buffers the frames for the node
  - When node wakes up sends a PS-POLLING request to AP and gets all the frames.

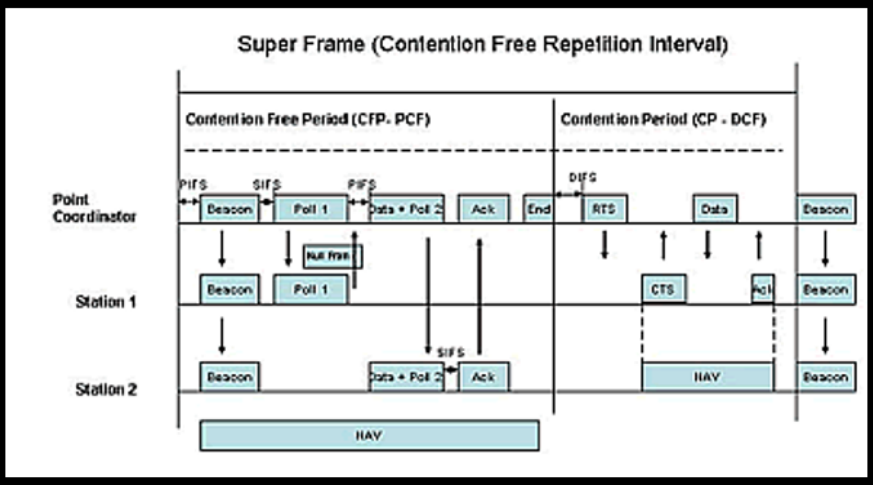
UCL

IEEE 802.11 MAC (cont.)

- The CSMA/CA protocol also includes an optional point coordination function (PCF)
- Access point becomes a point coordinator (providing a contention free service).
- The point coordinator polls each client at a given time
- No other station may transmit at that time.
- This provides a bounded delay service useful for voice, voice over IP (VoIP), and other multimedia traffic.
  - However, this option is very rarely implemented.
- The MAC layer also supports authentication, network management and privacy.

UCL

PCF:Point coordination function



UCL

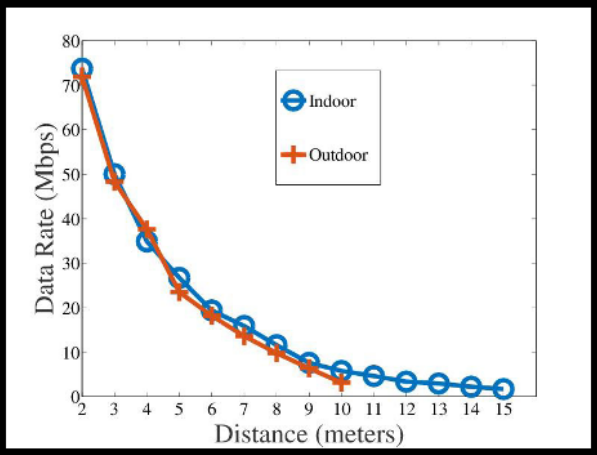
TWT – Target wake up time (802.11ax)

- New feature for IoT
- AP tells devices to go to sleep and wake up at a specific time
- This not only saves power in devices but reduces congestion

- https://arxiv.org/pdf/1804.07717.pdf

UCL

Performance example



UCL

Outline

- 802.11 types of frames
  - Management
  - Control
  - Data
- PCF
- TWT


Other Wireless Technologies
Miguel Rio
UCL

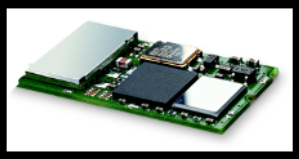
Bluetooth

- Bluetooth was originally aimed at small form factor, low-cost, short-range radio links between mobile PCs, mobile phones and other portable devices.
- Often used for cordless computer peripherals (mouse, keyboard, trackpad etc.)
- Very low cost hardware designed to be widely embedded in industrial and consumer equipment.

UCL

Bluetooth

- The basic idea
  - Universal radio interface for ad-hoc wireless connectivity (no infrastructure)
  - Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
  - Embedded in other devices
  - Short range (10 m), low power consumption, license-free 2.45 GHz ISM
  - Voice and data transmission, approx. 1 Mbit/s gross data rate



One of the first Bluetooth modules (Ericsson) – 1990s

Contemporary Bluetooth LE module - 2015

UCL

Bluetooth History

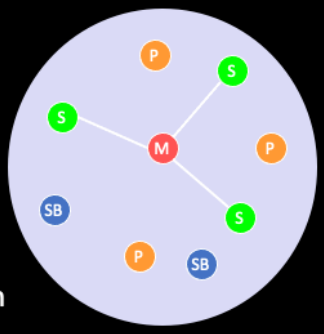
- History
  - 1994: Ericsson (Mattison/Haartsen), "MC-link" project
  - Renaming of the project: Bluetooth according to Harald "Blåtand" Gormsen [son of Gorm], King of Denmark in the 10th century
  - 1998: foundation of Bluetooth SIG, www.bluetooth.org
  - 2001: first consumer products for mass market, spec. version 1.1 released
- Special Interest Group
  - Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
  - Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
  - > 10000 members
  - Common specification and certification of products

Bluetooth Link Types

1. **SCO (Synchronous Connection Oriented)**
   - FEC (forward error correction), no retransmission
   - point-to-point
   - 64 kbit/s duplex
   - circuit switched
   - Intended for voice transmission
2. **ACL (Asynchronous ConnectionLess)**
   - Asynchronous, fast acknowledge
   - point-to-multipoint
   - up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric
   - packet switched
   - Intended for data transmission

Piconet

- Collection of devices connected in an ad hoc fashion
- One unit acts as master and the others as slaves for the lifetime of the piconet
- **Master determines hopping pattern, slaves have to synchronize: This is the MAC layer**
- Each piconet has a unique hopping pattern
- Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)



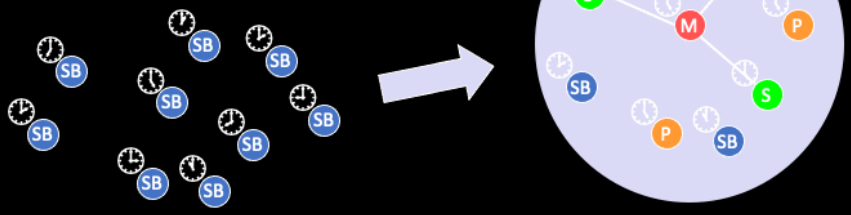
M=Master
S=Slave

P=Parked
SB=Standby

UCL

Forming a piconet

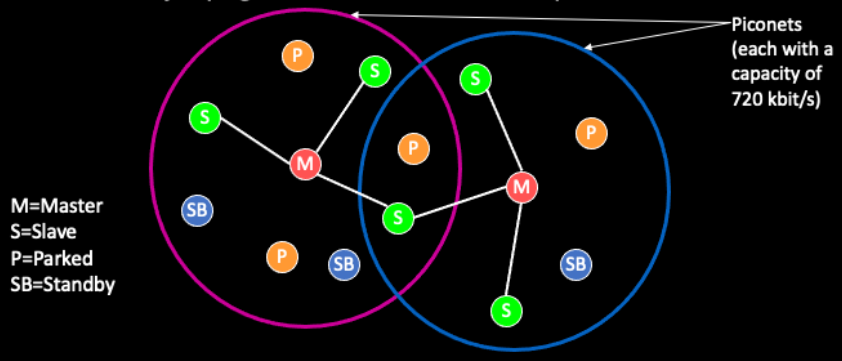
- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
    - Hopping pattern: determined by device ID (48 bit, unique worldwide)
    - Phase in hopping pattern determined by clock
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)



UCL

Scatternet

- Linking of multiple co-located piconets through the sharing of common master or slave devices
  - Devices can be slave in one piconet and master of another
- Communication between piconets
  - Devices jumping back and forth between the piconets



20/10/2020

UCL

Wireless Technologies – Bluetooth LE

- Bluetooth Low-Energy (BLE) - or Bluetooth Smart,- is a significant protocol for IoT applications.
- It offers similar range to Bluetooth it has been designed to offer significantly reduced power consumption.
- Not backward-compatible with the previous “Classic” Bluetooth protocol, but the Bluetooth 4.0 specification permits devices to implement either or both of the LE and Classic systems.
- Most used technology for wearable devices.
- Standard: Bluetooth 4.2 core specification

UCL

Bluetooth LE vs Bluetooth

Parameter	Conventional Bluetooth	Bluetooth Smart technology
Theoretical maximum range	100 m (330 ft)	>100 m (>330 ft)
Over the air data rate	1–3 Mbit/s	1 Mbit/s
Application throughput	0.7–2.1 Mbit/s	0.27 Mbit/s
Modulation scheme	GFSK	GFSK
Active slaves	7	Not defined; implementation dependent
Latency (from a non-connected state)	Typically 100 ms	6 ms
Voice capable	Yes	No
Power consumption	1 W as the reference	0.01 to 0.5 W (depending on use case)
Peak current consumption	<30 mA	<15 mA

UCL

Adhoc networks: MANET (Mobile Ad-hoc Networks)

- Vehicular ad hoc networks
- Military/Rescue networks
- UAV Ad hoc networks
- Wireless sensor networks

- Challenges:
  - Decentralized routing algorithms
  - Power

UCL

Summary

- Bluetooth
- Bluetooth Low energy
- MANETs