



# Week2 Review Notes

ELEC0099: Introduce to Internet Protocol Networks 21/22  
RUFENG DING

## Contents

<b>1 Ethernet</b>	<b>2</b>
1.1 LAN . . . . .	2
1.2 Ethernet details . . . . .	4
<b>2 Medium Access Control</b>	<b>6</b>
2.1 Methods of Medium Access Control . . . . .	6
 2.2 CSMA/CD . . . . .	7
<b>3 Ethernet Design</b>	<b>8</b>
3.1 The Collision Domain . . . . .	9
3.2 Repeaters . . . . .	9
3.3 HUBs . . . . .	10
<b>4 Ethernet Switch</b>	<b>10</b>
4.1 Bridges . . . . .	10
4.2 Switch . . . . .	11
4.3 spanning tree protocol . . . . .	11
<b>5 Wi-Fi 802.11</b>	<b>11</b>
5.1 ad-hoc architecture 802.11 . . . . .	13
5.2 infrastructure architecture 802.11 . . . . .	13
5.3 802.11 frame format . . . . .	14
<b>6 802.11 Protocol</b>	<b>14</b>

6.1	802.11 Frame type . . . . .	14
6.2	802.11 MAC . . . . .	15
6.3	PCF Point coordination function . . . . .	16
6.4	TWT Target wake up time (802.11ax) . . . . .	16
 7	<b>CSMA/CA</b>	<b>16</b>
7.1	Hidden Terminal Problem . . . . .	17
7.2	Exposed Terminal Problem . . . . .	17
7.3	CSMA/CA . . . . .	17
7.3.1	Multiple Access . . . . .	17
7.3.2	Collision Avoidance(4 way handshake) . . . . .	17
8	<b>Other wireless technologies</b>	<b>19</b>
8.1	Bluetooth . . . . .	19
8.1.1	History . . . . .	20
8.1.2	Link Types . . . . .	20
8.2	Piconet . . . . .	20
8.3	Scartternet . . . . .	21
8.4	Bluetooth LE . . . . .	21
8.5	MANET . . . . .	21

## 1 Ethernet

Why there is a need for a LAN?

- to share resources like files, printers, scanners, internet connections, WAN links.
- To share data and applications like 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.

## 1.1 LAN

### LAN topologies

- Bus

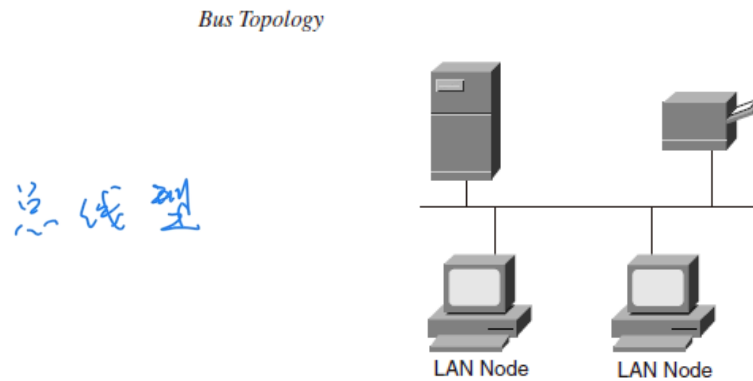


Figure 1: Star topology

- Tree

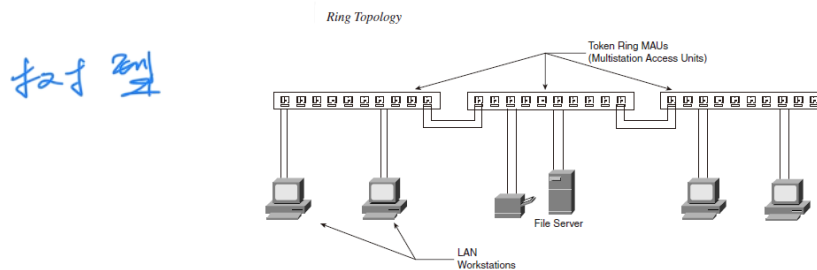


Figure 2: Star topology

- Ring
- Star

### LAN transmission methods

- **Unicast** transmission a frame is sent from the source to the destination on a network

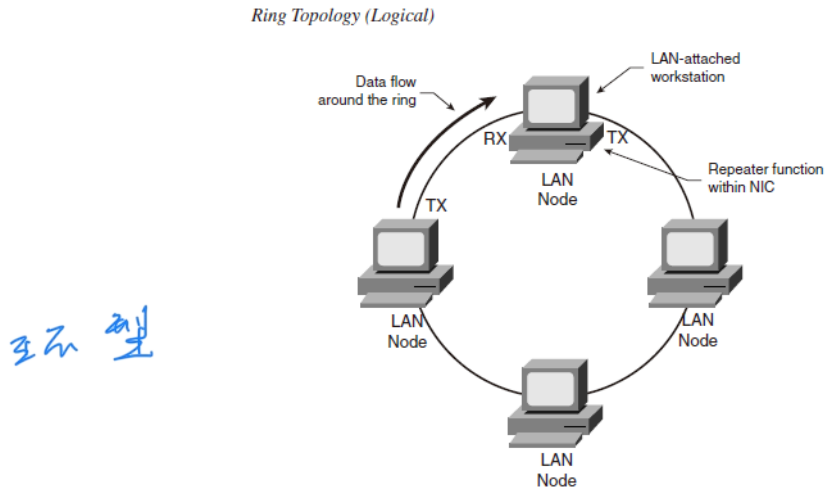


Figure 3: Star topology

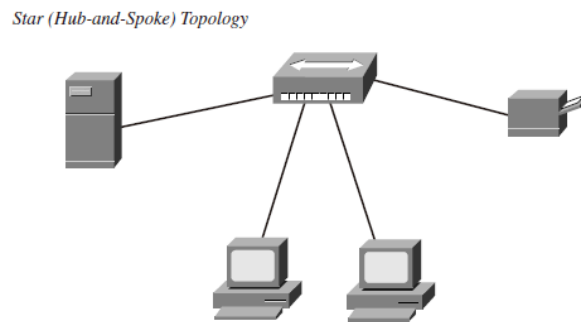


Figure 4: Star topology

- **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

## LAN protocols and OSI model

Table 1: LAN protocols and OSI model

Data Link layer	Logical Link Control (LLC)
	Medium Access Control (MAC)
Physical Layer	

## LAN media access methods

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

## 1.2 Ethernet details

**Ethernet** has survived as a LAN technology because:

- Flexibility
- Relative simplicity
- Innovation
  - 100Mbps half duplex and full duplex
  - 100Mbps, 1Gbps, 10Gbps Ethernet
- costs
- Although critics claim that Ethernet cannot scale it continues to dominate the desktop market

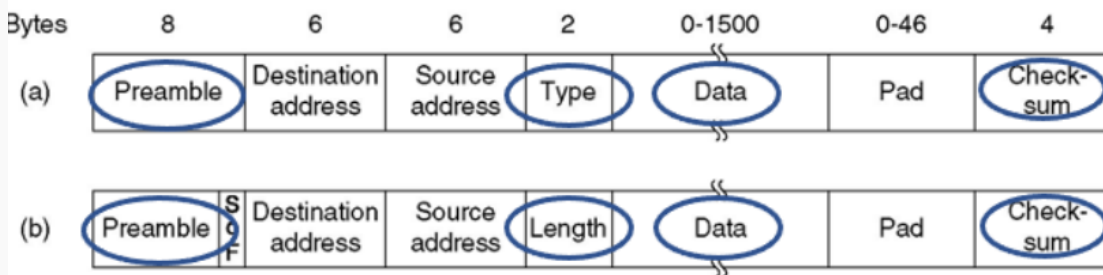
**History** Originally developed at the Xerox Palo Alto Research Centre in 1973 patented in 1976.

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 (original version of Ethernet) and IEEE 802.3 (standard Ethernet).

### Note 1. IEEE 802.3 and DIX Ethernet Frame Formats



Ethernet type 2 uses a Type field after source address while 802.3 Ethernet use Length field (for the 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 of data that follow this field.

Data - Ethernet expects at least 46 bytes of data.

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

**MAC address** Destination and source addresses are called the MAC address. MAC addresses identify network entities in Ethernet LANs.

Characters:

- 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.

## 2 Medium Access Control

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

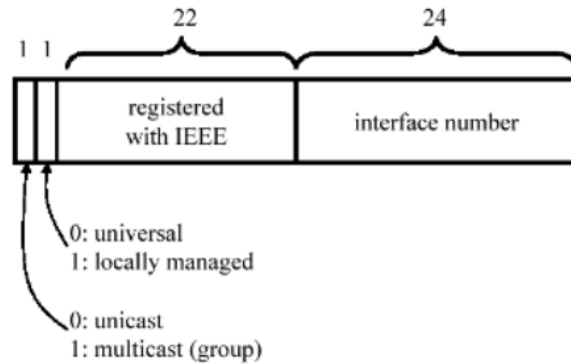


Figure 5: MAC address

## 2.1 Methods of Medium Access Control

**Pure Aloha** Transmit when you want regardless of others.

**Pure Aloha Collision** is extremely inefficient, since the worst-case period of vulnerability is the time to transmit two frames.

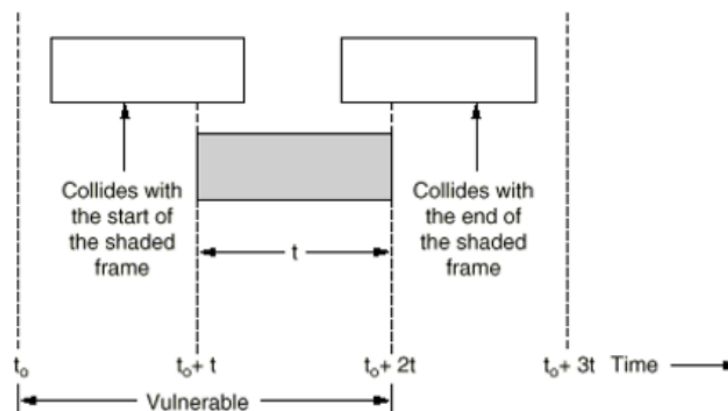


Figure 6: Pure Aloha Collision Control

**Slotted Aloha** Transmission only at the beginning of each Synchronized "slot times". And it is collision inefficient limited to one frame transmission time.

**Comparison of Pure and Slotted Aloha** Throughput efficiency increases dramatically for Slotted Aloha. (Figure 7)



## 2.2 CSMA/CD

CS - CarrierSensels (someone already talking?)

MA - MultipleAccess(I hear what you hear!)

CD - (CollisionDetectionHywe're both talking!)

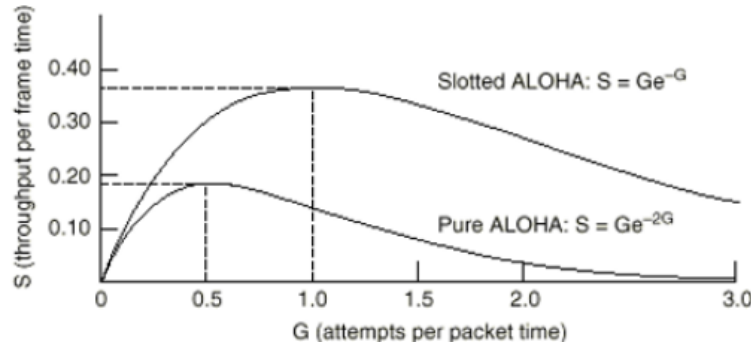


Figure 7: Pure Aloha vs Slotted Aloha

1. If the medium is idle. transmit any time.
2. If the medium is busy, wait and transmit right after.
3. If a collision occurred back off for a random period, then go back to 1.

CSMA/CD can be one of three state : contention, transmission or idle.

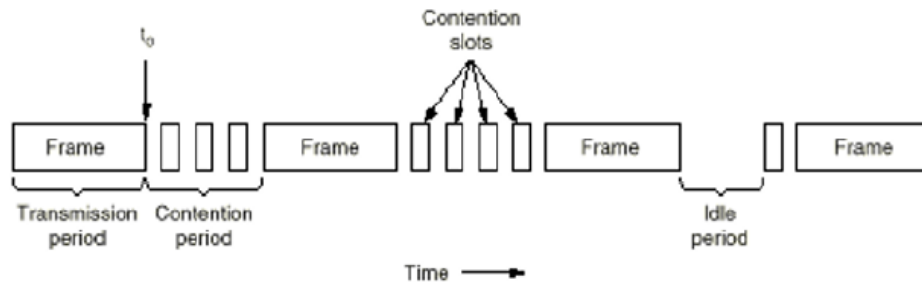


Figure 8: States in CSMA/CD

TIME is proportional to distance over the wire. (CSMA/CD on Ethernet Physical Layer). Host find the wire is clear, it began to transmit. When the packet has not arrived, another host also find the line is still clear so second host begins to transmit. As a result collision detected and the collision propagates and will be detected by both stations.

**Performance** Vertex is Throughput and horizon is Offered Load.

### 3 Ethernet Design

Factors Limiting the Length of Ethernet:

- Collision Detection - timing.



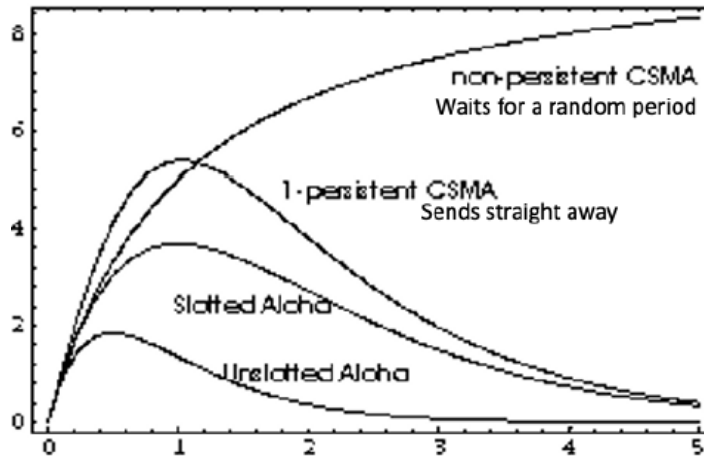


Figure 9: Performance

- Attenuation - the signal gets weaker as it propagates along the wire.
- Noise - longer wires pick up more noise Which masks the signal

**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.

### Cable Types

- Coaxial cables
  - ThickNet
  - ThinNet
- Unshielded Twisted Pair(UTP)
  - CAT5
  - CAT6
  - CAT7

**Fibre Types** Firer contains three parts: Core, Cladding and Buffer. Multimode Step index / Multimode Graded Index / Singlemode.

### 3.1 The Collision Domain

冲突域

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

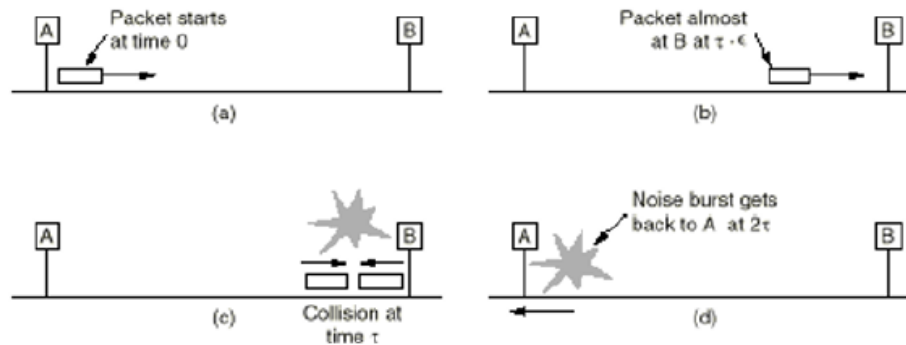


Figure 10: Collision Domain

### 3.2 Repeaters 中继器

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 up to 140 bit times). Class II repeaters can only connect segment using the same signalling technique (timing delays up to 92 bit times).

### 3.3 HUBs 集线器 (物理层)

HUBs are Multi-port Repeaters. All share the 10Mb ethernet bandwidth and Frames appear everywhere. It comprise a single COLLISION DOMAIN and everyone's frames collide with everyone else's/Every collision appears throughout the domain.

## 4 Ethernet Switch

### 4.1 Bridges 网桥

- 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
- Bridges Properties

– Frame Forwarding

The bridge receives a frame on one port and transmit 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

Collision don't propagate across bridges.

Bridges can connect dissimilar networks.

– Learning (学习)

- \* 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.

– Spanning Tree

### More Forwarding and 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 behaviour accordingly.

## 4.2 Switch 交换机

A switch is a multiport bridge.

- Break up collision domain

- 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.

- Broadcast Domain

A Network interconnected by bridges comprises a BROADCAST DOMAIN. Broadcasts from one host are seen by every other host on the bridge 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.

## ( 虚拟局域网 )

- 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.

- Switching implementation: crossbar

### 4.3 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.

## 5 Wi-Fi 802.11

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.

Relevant IEEE standard:

Table 2: IEEE Standards

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

### IEEE 802 standardisation framework

Table 3: IEEE 802

802.2 Logical Link Control (LLC)					
802.3 MAC PHY	802.5 MAC PHY	802.11 Medium Access Control (MAC) (CSMA/CA)			
		802.11 PHY	802.11a PHY	802.11b PHY	802.11g PHY

IEEE 802.11 presented as the first true industry standard WLAN (released in 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 transprot (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)

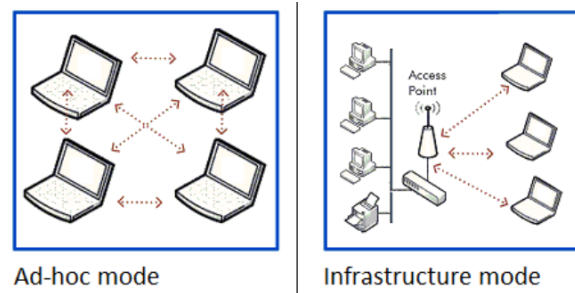


Figure 11: ad hoc model / infrastructure model

## 5.1 ad-hoc architecture 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

## 5.2 infrastructure architecture 802.11

Direct communication within a limited range:

- **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 intergrated into the wireless LAN and the distribution system

- Portal: bridge to other (wired) networks
- Distribution System: interconnection network to form one logical network (ESS:Extended Service Set)based on several BSS

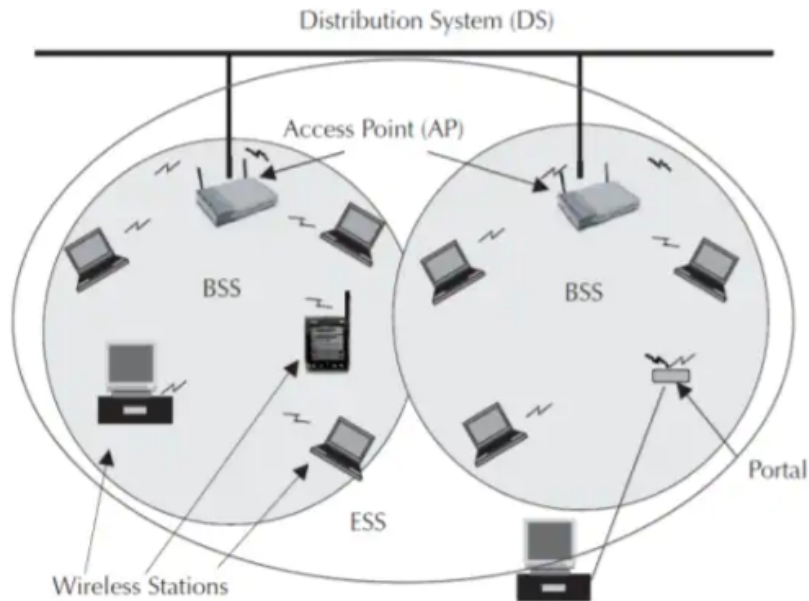


Figure 12: infrastructure architecture

### 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.

### 5.3 802.11 frame format

- very similar to Ethernet.
- Duration of connections.
- serveral addresses, depending if we are using IBSS or BSS.

## 6 802.11 Protocol

### 6.1 802.11 Frame type

- management frames
  - beacon
  - probe Req/Res

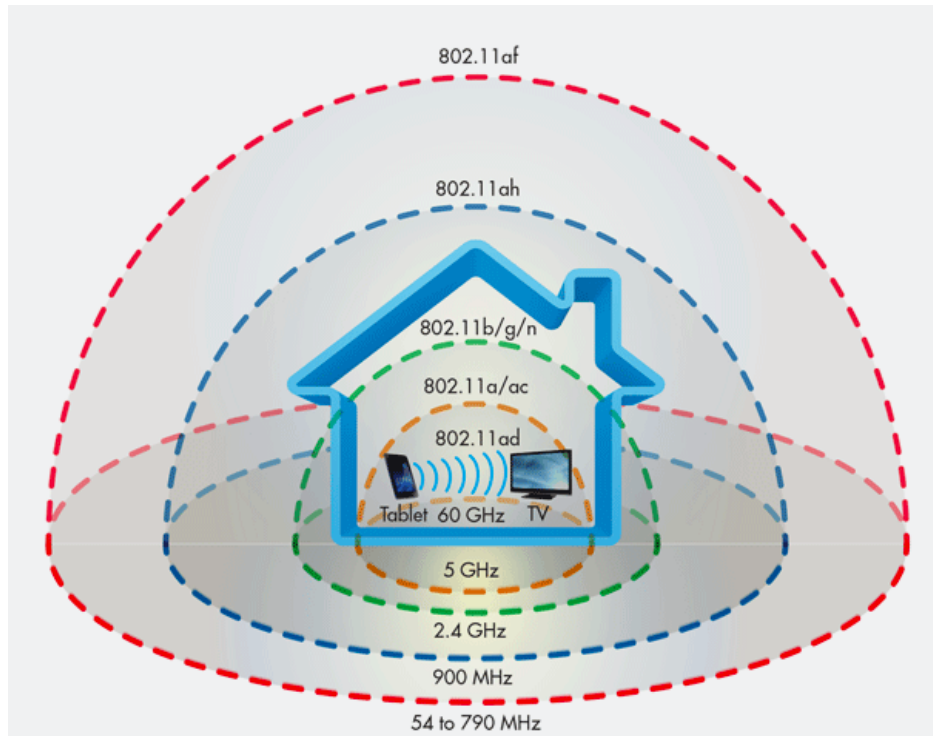


Figure 13: Range of 802.11 Standard

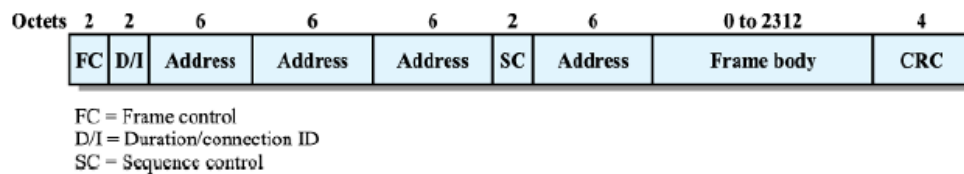


Figure 1: IEEE 802.11 MAC frame format. Image from William Stallings "Data and Computer Communications".

Figure 14: 802.11 frame format

- association Req/Res
- reassociation Req/Res
- Authentication Frame
- Deauthentication and Disassociation
- Action Frames
- Channel Switch Announcement
- control frames
  - RTS(Request To Send)
  - CTS(Clear To Send)
  - ACK(Acknowledgement)
  - 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.

Table 4: RTS

bytes	2	2	6	4
	Frame Control	Duration	Receiver Address	CRC

Table 5: CTS

bytes	2	2	6	6	4
	Frame Control	Duration	Receiver Address	Transmitter Address	CRC

- data frames

## 6.2 802.11 MAC

The CSMA/CA protocol also includes an optional point coordination function (PCF). Access point become 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 support authentication, network management and privacy.

## 6.3 PCF Point coordination function

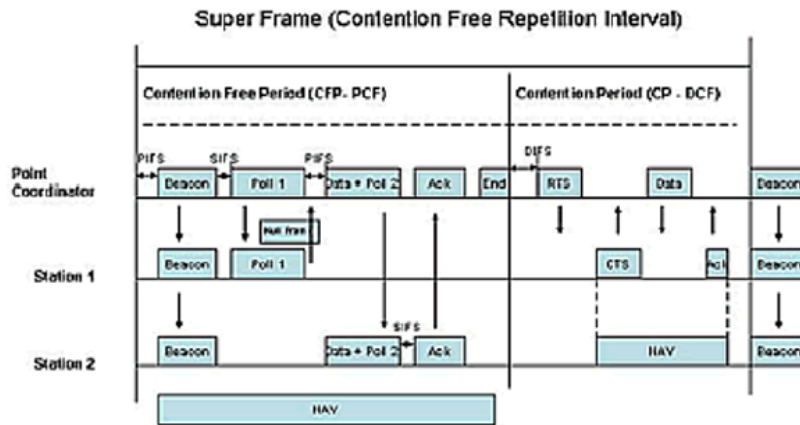


Figure 15: PCF

## 6.4 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.



Table 6: ACK

bytes	2	2	6	4
	Frame Control	Duration	Receiver Address	CRC

## 7 CSMA/CA (Collision Avoidance)

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

Why not CSMA/CD?

- 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**.

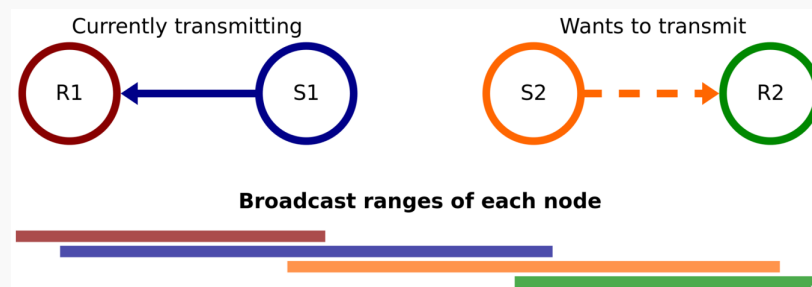
### 7.1 Hidden Terminal Problem (隐蔽站问题)

**Note 2.** In wireless networking, the hidden node problem or hidden terminal problem occurs when a node can communicate with a wireless access point (AP), but cannot directly communicate with other nodes that are communicating with that AP. This leads to difficulties in medium access control sublayer since multiple nodes can send data packets to the AP simultaneously, which creates interference at the AP resulting in no packet getting through.

CSMA/CA 解决

## 7.2 Exposed Terminal Problem

**Note 3.** In wireless networks, the exposed node problem occurs when a node is prevented from sending packets to other nodes because of co-channel interference with a neighboring transmitter. Consider an example of four nodes labeled R1, S1, S2, and R2, where the two receivers (R1, R2) are out of range of each other, yet the two transmitters (S1, S2) in the middle are in range of each other. Here, if a transmission between S1 and R1 is taking place, node S2 is prevented from transmitting to R2 as it concludes after carrier sense that it will interfere with the transmission by its neighbor S1. However note that R2 could still receive the transmission of S2 without interference because it is out of range of S1.



## 7.3 CSMA/CA

### 7.3.1 Multiple Access

The first rule is only one people talk at a time, the other 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.

### 7.3.2 Collision Avoidance(4 way handshake)

What happens if two dinner guests sense a lull 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 wireless world one cannot detect these collisions. 802.11 handles collisions with a **4 way handshake**.

#### 4 way handshake

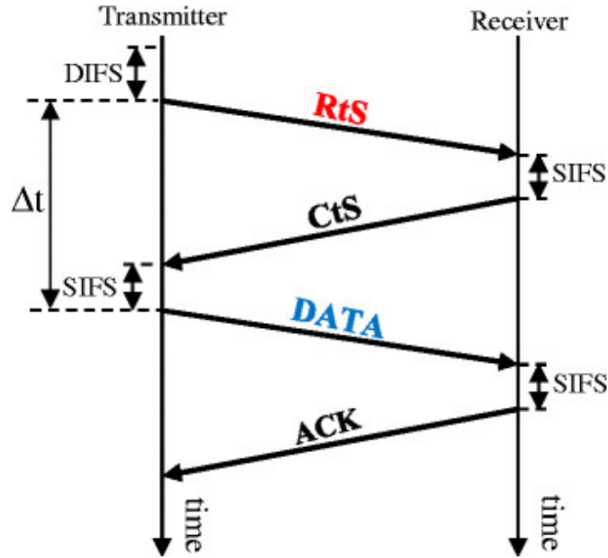


Figure 16: 4 way handshake flow

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. 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).
6. The receiver uses the CRC to determine if the packet has been received correctly. If so, the receiver sends out an ACK packet.
7. If the information packet is not ACKed, then the source starts again and tries to retransmit the packet.

## 8 Other wireless technologies

### 8.1 Bluetooth

- Bluetooth was originally aimed at small form factor, low-cost, short-range radio links between mobile PCs, mobile phones and other portable devices.

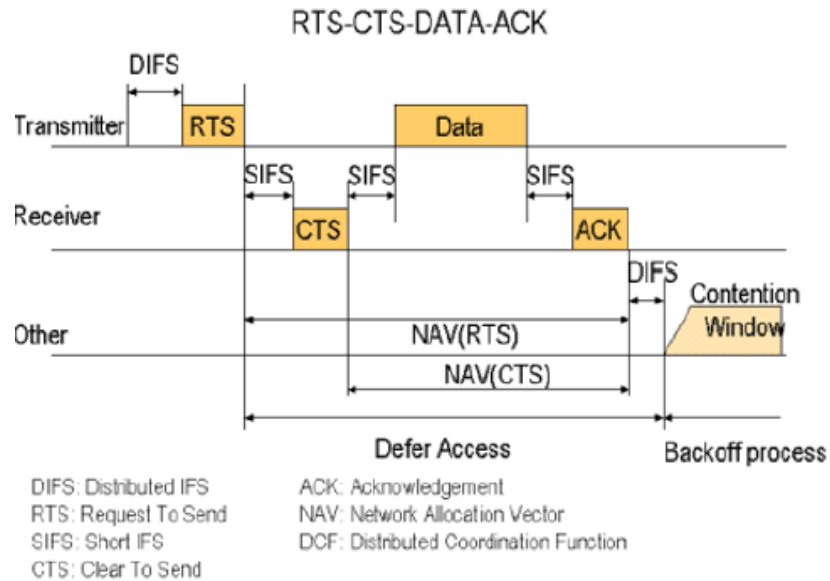


Figure 17: 4 way handshake protocol

- Often used for cordless computer peripherals mouse, keyboard, trackpad etc.
- Very low cost hardware designed to be widely embedded in industrial and consumer equipment.

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

### 8.1.1 History

- 1994: Ericsson (Mattison/Haartsen), "MC-link" project
- Renaming of the project Bluetooth according to Harald Blatand
- Gormsen [son of Gorm], King of Denmark in the 10<sup>th</sup> century
- 1998: foundation of Bluetooth SIG, [www.bluetooth.org](http://www.bluetooth.org)
- 2001: first consumer products for mass market, spec version 1.1 released

### 8.1.2 Link Types

- SCO(Synchronous connection Oriented)
  - FEC (forward error correction,no retransmission)
  - point-to-point
  - 64 kbit/s duplex
  - circuit switched
  - Intended for voice transmission
- 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

## 8.2 Piconet

Collection of devices connected in an ad hoc fashion. One unit acts as master and the others as slaves for the life time 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 and up to 7 simultaneous slaves (> 200 could be parked).

### 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)

## 8.3 Scarttternet

- 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

## 8.4 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.

## 8.5 MANET

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