Wireless Networking

- Motivations
  - mobility
    - » connect from anywhere, anytime, on the move
    - » wi-fi *hotspots* beginning to proliferate
      - coffee shops, airports, hotels etc.
  - flexibility
    - » *ad hoc* networks whenever and wherever required
      - meetings, multi-user networked games
    - » home networks
      - homes increasingly have multiple PCs with one Internet connection
  - costs
    - » no fixed wiring
      - may be difficult and expensive unless buildings designed for the purpose
    - » cheap wireless interface cards and access points

- Challenges
  - radio and infra-red transmissions susceptible to noise and interference
    - » microwave ovens, fluorescent lights etc.
    - » not as reliable as wired transmission
  - strength of radio transmission varies in time and space
    - » fading effects from multipath propagation
    - » uneven propagation due to physical barriers and geographic topography
    - » coverage inconsistent and unpredictable
  - radio transmissions can be intercepted by eavesdroppers
    - » difficult to restrict transmissions to a specific area
  - radio spectrum is finite and must be shared with other users
    - » your neighbour's home wi-fi network
    - » competing WLAN standards e.g. Bluetooth v. 802.11, in 2.5GHz range
  - difficult to provide the high transmission speeds that are easy with wires
    - » e.g. Gigabit wired ethernet
  - allocation of spectrum by national and international authorities – ITU, FCC etc.
    - » agreement often difficult; designing products for a global market difficult

- Network Types
  - – Wireless Wide Area Networks (WWANs)
    - » connections maintained over large geographical areas
      - multiple antenna sites and cells or satellite systems
      - automatic *hand-off* between adjacent cells for mobility
      - international *roaming* between compatible systems
    - » generations of systems
      - 1G systems (analogue) : TACS (UK), AMPS (USA)
      - 2G systems (digital) : GSM (Europe), TDMA (USA)
      - 2½G systems : GPRS (Europe), EDGE
      - 3G systems : UMTS (Europe), CDMA 2000 (USA), TD-SCDMA (China)
        - ¤ aiming for a global standard to allow worldwide roaming but unlikely to happen
    - » private as well as public networks
      - E.g. GSM-R for railways – signalling, control & communications

– Wireless Metropolitan Area Networks (WMANs)

» to establish connections between multiple locations within a metro. area

- e.g. multiple office buildings, a University campus etc.

» backups for wired networks

» radio or infra-red transmission

» technologies:

- Multichannel Multipoint Distribution Service (MMDS)
  - ¤ 2-way voice, data and video streaming
  - ¤ 2 – 10GHz range, 30 miles radius, line-of-sight
- Local Multipoint Distribution Services (LMDS)
  - ¤ 49 TV channels
  - ¤ 24 - 40GHz range, 2 - 3 miles radius, line-of-sight
- IEEE 802.16
  - ¤ working group set up to establish standards for broadband wireless access
  - ¤ 10 – 66GHz range
  - ¤ Demand Assignment Multiple Access-Time Division Multiple Access (DAMA-TDMA)
  - ¤ capacity assignment that adapts to demand

– Wireless Local Area Networks (WLANs)

» communications within a local area

- within a corporate or campus building, public spaces – coffee shops, airports etc.
- 25m – 250m, farther outside than inside, speed decreasing with distance

» where wiring would be difficult or expensive

- to supplement an existing LAN

» to create possibly temporary *ad hoc* networks

- in a meeting room

» to facilitate mobility

- laptops ubiquitous for `road warriers'

» IEEE standardisation

- original 802.11 : 1 or 2 Mbs
- 802.11a : up to 54Mbps in 5GHz band
- 802.11b : up to 11Mbps in 2.4GHz band depending on range from access point
- 802.11e : Quality of Service standards e.g. for Voice over Wireless
- 802.11g : 6Mbs to 54Mbps in 2.4GHz band
- 802.11h : European version with dynamic power and frequency band control
- 802.11i : supplemental draft standard for improved security

– Wireless Personal Area Networks (WPANs)

» *ad hoc* communications within a *personal operating space*

- e.g. PDAs, mobile phones, laptops, headsets, GPS navigators, printers etc.

» a cable replacement technology

» Infra-Red

- Infra-Red Data Association (IrDA) standard
- 9.2kbps to 4Mbps
- short range – 1m to 2m

» Bluetooth (IEEE 802.15.1)

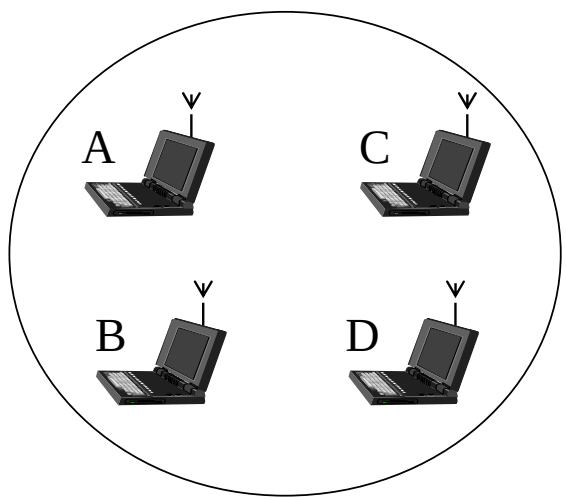
- spread-spectrum frequency-hopping in 2.4GHz band
- low power, low cost
- up to 721kbps data rate
- range 10m
  - ¤ 100m possible with more powerful antenna but not licensed

» ZigBee (IEEE 802.15.4)

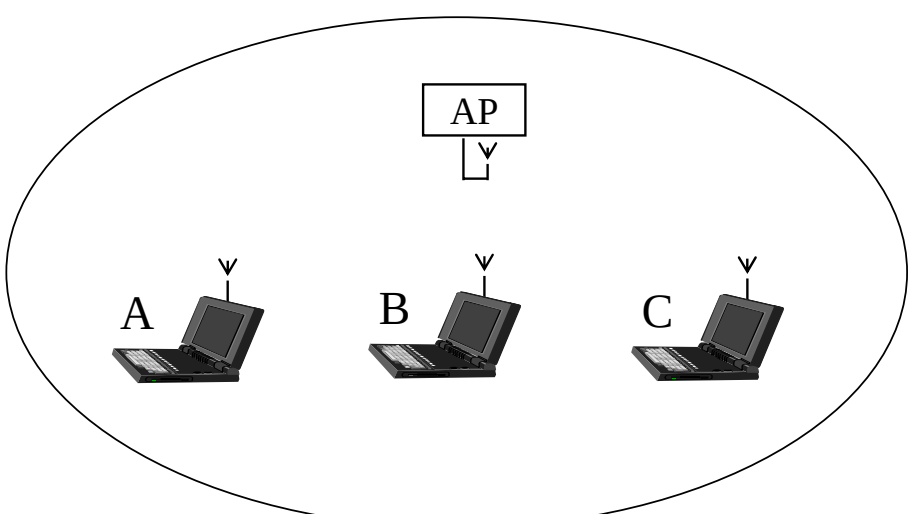
- industrial alliance formed to produce a Bluetooth competitor
- low data rates : 20kbps, 40kbps and 250kbps depending on frequency band used
- range 10m to 75m

IEEE 802.11

- Building blocks :
  - the Basic Service Set (BSS)
    - » a group of stations that coordinate their access to the medium
    - » co-located and unrelated BSS's can co-exist simultaneously
      - via different *channels*
    - » stations intercommunicate within a Basic Service Area (BSA)
      - analogous to a mobile phone *cell*
      - size depending on situation and conditions e.g. indoors v. outdoors
  - an Independent Basic Service Set (Peer to Peer)
    - » a single BSS can form an *ad hoc* network
    - » no access point
    - » typically temporary
      - can be formed spontaneously and disbanded after a limited period of time
      - even just two stations
    - » stations need to be in range of each other to communicate



– Basic Service Set in *infrastructure mode*
  » has an *Access Point* (AP) or *Base Station*
    - to provide a local bridge between stations
  » stations communicate via the Access Point in PCF mode
    - all frames go via the access point
    - stations do not all need to be in range of each other
      ¤ just in range of the access point
  » communicate directly with each other in DCF mode



– Extended Service Set (ESS)

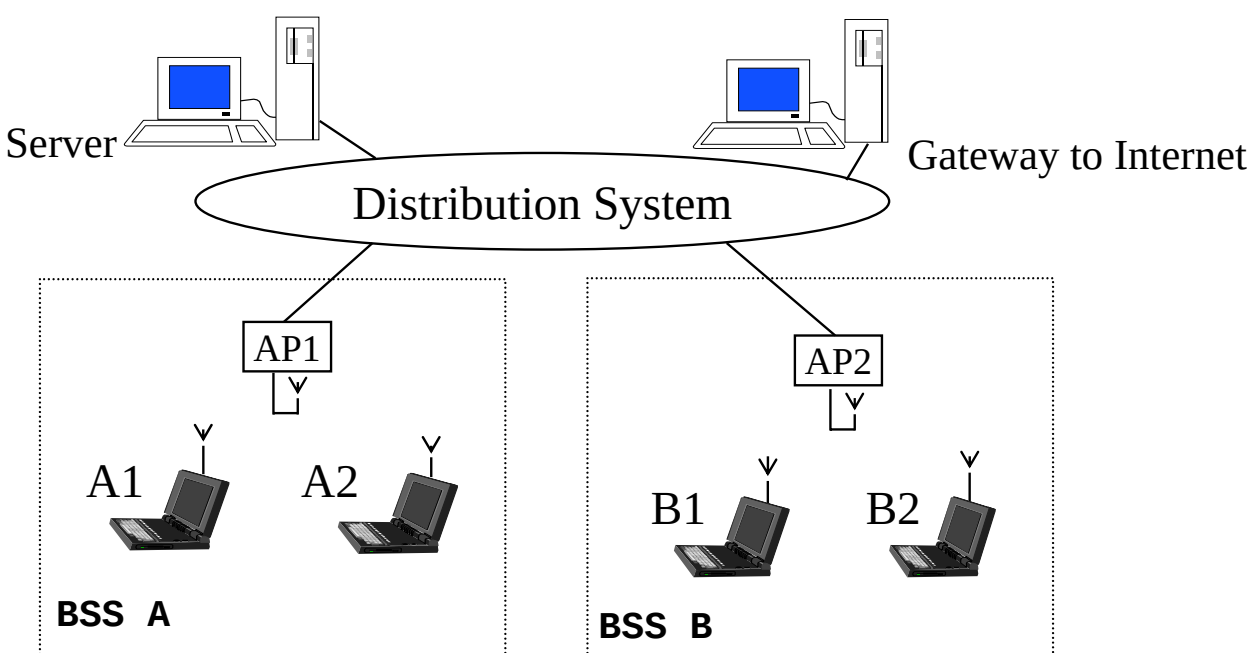
» a set of infrastructure Basic Service Sets

» Access Points communicate amongst themselves to forward traffic from one BSS to another

» allows movement of stations between BSSs

» allows access to network services

- Internet, file & mail servers etc.

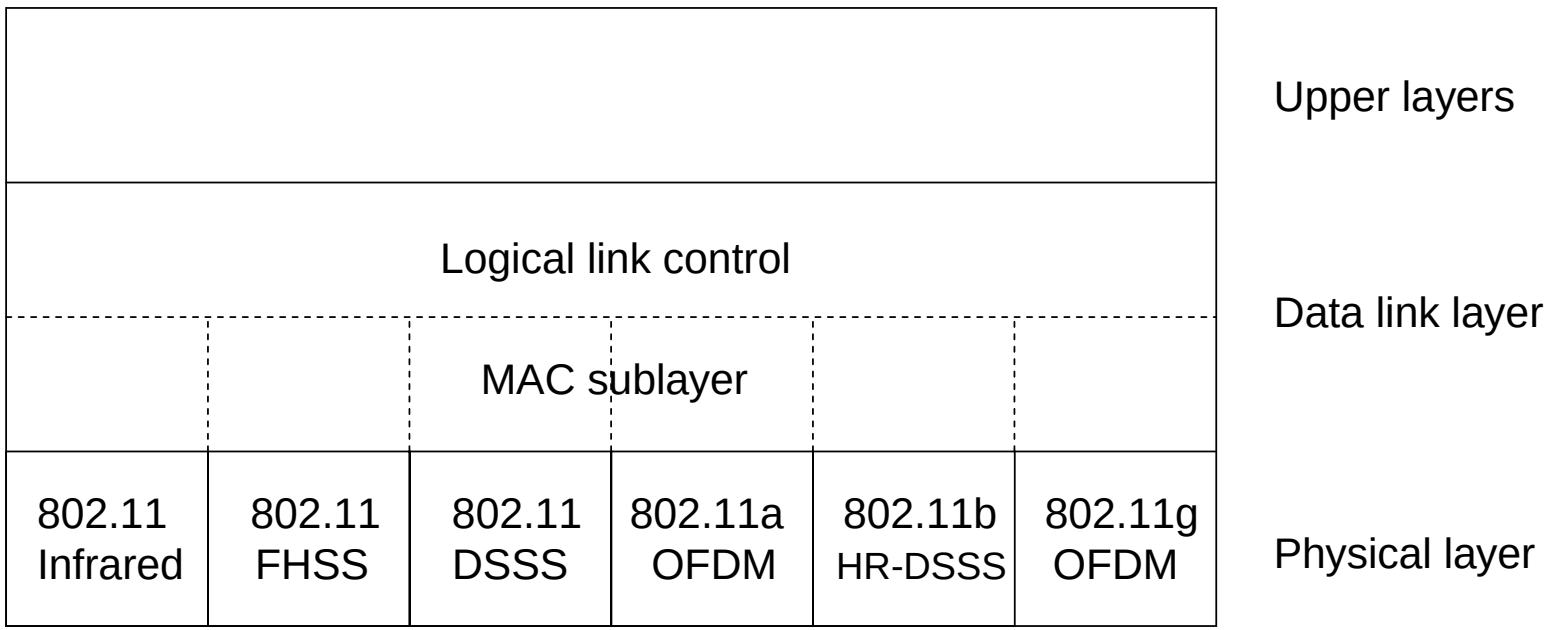


- Distribution services :
  - *Association*
    - » used by mobile stations to connect themselves to base stations
    - » announces its identity and capabilities
      - e.g. data rates supported, power management requirements etc.
    - » base station may accept or reject the request
      - mobile station must authenticate itself if accepted
  - *Disassociation*
    - » either the base station or the mobile may break the association
      - when shutting down or leaving
  - *Reassociation*
    - » station may change its preferred base station
    - » useful for mobile stations moving from one cell to another
      - no data should be lost as a consequence of the handover
  - *Distribution*
    - » to determine how frames are to be routed
    - » destinations local to the BSS can be broadcast over the air
      - otherwise forwarded over the wired network

- *Integration*
  - » handles translation to the format required
    - if frame needs to be sent through a non-802.11 network
    - using a different addressing scheme or frame format

- Station services :
  - *Authentication*
    - » to prove a new station is who he purports to be
    - » a *challenge* and *response* system
      - if successful, mobile station is fully enrolled into the cell
  - *Deauthentication*
    - » when the station wants to leave the cell
  - *Privacy*
    - » to be kept confidential, broadcast information must be encrypted
      - Wired Equivalent Privacy (WEP)
  - *Data Delivery*
    - » modelled on ethernet
    - » not guaranteed to be reliable
      - higher protocol layers must deal with detection and correction of errors

- Protocol Stack
  - follows OSI model, but Data link layer split into two sublayers



  - MAC sublayer determines how the channel is allocated
    - » who gets to transmit next
  - Logical link control hides the differences between 802.11 variants

- Physical layer
  - – each transmission technique allows a MAC frame to be transmitted
  - – Infra-red
    - » 0.85μ or 0.95μ wavelength, diffused
    - » Pulse Position Modulation (PPM)
      - 1Mbps : 4 bit group encoded to 16 bits – 15 zeroes and 1 one
      - 2Mbps : 2 bit group encoded to 4 bits – 3 zeroes and 1 one
    - » low bandwidth makes this an unpopular option
  - – FHSS : Frequency Hopping Spread Spectrum
    - » uses 79 channels, each 1MHz wide in the unlicensed 2.4GHz band
    - » restricted to 1Mbps and 2Mbps
    - » hops between frequencies in pseudorandom sequence
      - all stations need to use same *seed* for random number generator
    - » time spent at each frequency – the *dwell time* – an adjustable parameter
      - must be less than 400ms
    - » some security – eavesdropper needs to know hop sequence and dwell time
    - » FHSS offers fairly good resistance to multi-path fading and interference

– DSSS : Direct Sequence Spread Spectrum
  » similar to Code Division Multiple Access (CDMA)
  » each bit spread using an 11-bit *Barker* sequence
    - 10110111000
    - gives greater immunity to RF interference
    - disperses signal over a 30MHz band
  » 1Mbps uses Binary Phase Shift Keying modulation (BPSK)
    - one phase shift per bit
  » 2Mbps uses Quadrature Phase Shift Keying modulation (QPSK)
    - four rotations : 0, 90, 180 and 270 degrees
– OFDM : Orthogonal Frequency Division Multiplexing
  » 802.11a : 54Mbps in 5GHz band
  » 52 frequencies : 48 for data and 4 for synchronisation
    - used simultaneously
  » encoding based on phase-shift and quadrature amplitude modulation
  » at 54Mbps, 216 bits encoded in 288-bit symbols

– HR-DSSS : High Rate Direct Sequence Spread Spectrum
  » 802.11b : 1Mbps, 2Mbps, 5.5Mbps and 11Mbps rates supported
    - 1Mbps & 2Mbps rates compatible with original 802.11 DSSS scheme
  » 5.2Mbps & 11Mbps run at 1.375 Mbaud (*baud* = *symbols per second*)
    - with 4 bits & 8 bits per baud
    - using Complementary Code Keying (CCK) with Walsh/Hadamard codes
  » dynamic rate shifting
    - automatically adjusts for noisy conditions
    - in practice, operating speed nearly always 11Mbps
  » range usually much greater than 802.11a
  » up to 14 separate independent channels in 2.4GHz band
    - 2.412GHz up to 2.484GHz
    - only 13 allowed in UK, 11 in USA
– OFDM for 802.11g
  » same modulation as for 802.11a
  » using 2.4GHz band
  » not clear yet whether the claimed 54Mbps will be realised in practice

– physical layer adds its own protocol sublayers and headers to MAC frames

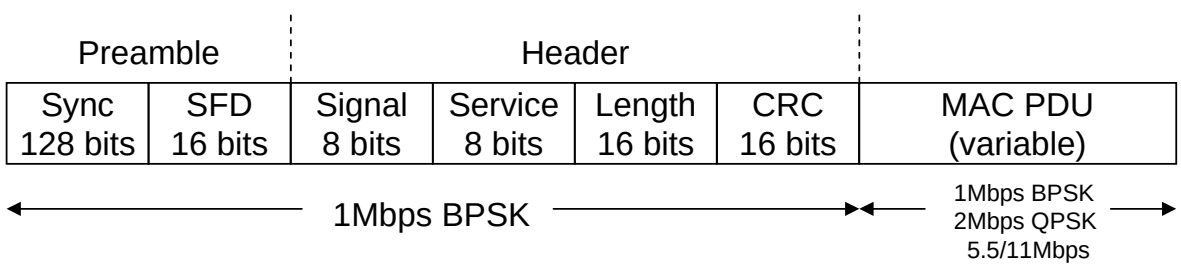
» PLCP : Physical Layer Convergence Protocol

- prepares frames for transmission

» PMD : Physical Medium Dependent

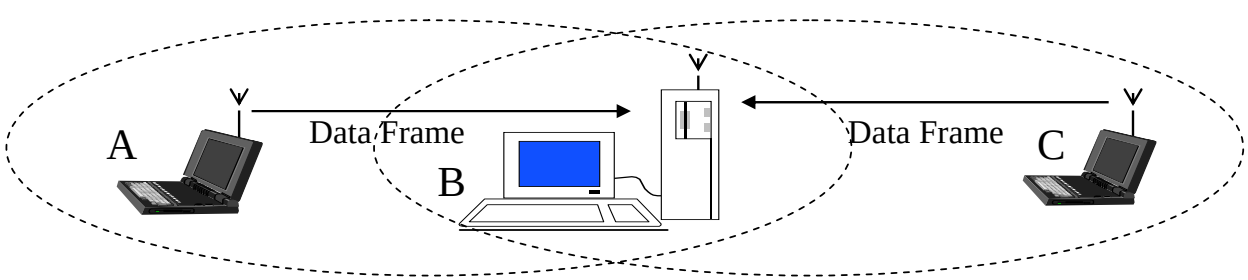
- actually transmits signals, change radio channels, receive signals etc.

– PLCP frame format :



- sync : alternating 0s and 1s to alert receiver
- start frame delimiter : 1111001110100000
- signal : data rate of MAC frame
- service : not used
- length : of following MAC PDU

- MAC sublayer
  - why not just Wireless Ethernet?
    - » designed for broadcast networks (original ALOHA network was radio based)!
  - difficult to detect collisions in a radio environment
    - » therefore not possible to abort transmissions that collide
    - » radios normally half-duplex : either transmit or receive – not both simultaneously
    - » transmit power orders of magnitude greater than receive power
  - radio environment not well controlled
    - » other LAN users e.g. Bluetooth, ZigBee, can interfere with collision detection
  - the *hidden station* problem :
    - » two stations both within range of an intermediate station but not of each other
    - » either one cannot hear the transmissions of the other
      - so think the channel is idle when the other station is using it
      - signals may collide at the intermediate station



– DCF mode : Distributed Coordination Function
  » no central control, like ethernet
  » uses CSMA/CA : CSMA with Collision Avoidance
– PCF mode : Point Coordination Function
  » uses a base station to control all activity in the cell
– CSMA/CA
  » *physical* channel sensing method :
  » a station wishing to transmit senses the medium
  » if the medium is busy, the station defers its transmission
    - waits a random time using ethernet exponential back-off algorithm and try again
  » if the medium is free for a specified time DIFS (Distributed Inter Frame Space),
  the station is allowed to transmit
    - transmits the whole frame because it cannot sense collisions while transmitting
  » receiving station checks CRC
  » sends acknowledge packet (ACK)
  » ACK received by transmitter indicates that no collision occurred
  » if no ACK received, sender will retransmit packet until ACKed
    - or until a given number of retransmissions fail

» *virtual* channel sensing :

» to reduce the probability of collisions in a cell which has two stations which cannot hear each other

» used in the MAC sublayer to tell other stations how long channel will be used

» station wanting to transmit a frame sends a short control packet called RTS

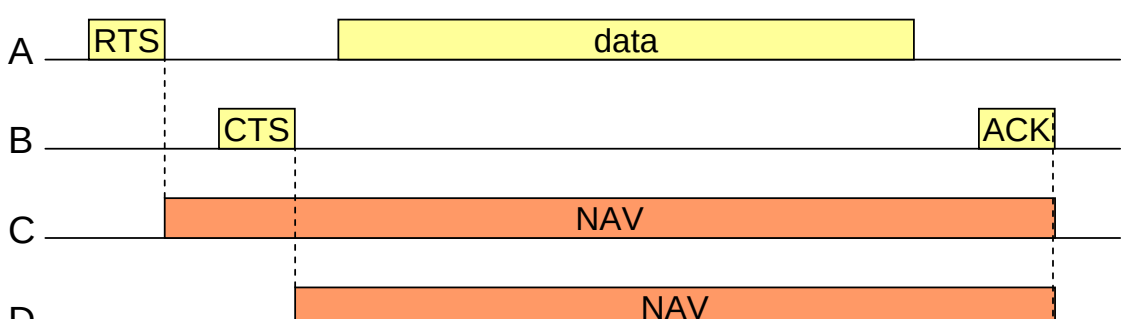
- Request To Send
- includes source, destination and duration of following transaction (packet + ACK)

» destination station responds, if medium free, with a CTS control packet

- Clear To Send
- includes the same duration information

» all other stations receiving either the RTS or the CTS set their *Virtual Carrier Sense* indicator (called NAV or *Network Allocation Vector*) for the given duration

- use this information with physical carrier sense when sensing the medium



» reduces probability of a collision on a receiver `hidden' from transmitter

- to the short duration of the RTS/CTS transmission period

» also reduces the overhead of collisions

- since short control frames are recognised faster than if the whole packet was transmitted
- a mechanism allows short packets to be transmitted without RTS/CTS
  - ¤ controlled per station by an *RTS Threshold* parameter

– Fragmentation and Reassembly

» transmit smaller packets each with their own checksum

- to help deal with noisy channels
- and long ethernet packets (1518 bytes)

» fragments individually numbered and acknowledged

- using a *stop-and-wait* protocol
  - ¤ i.e. fragment k must be acknowledged before fragment *k+1* is sent

» fragment size not fixed by the 802.11 standard

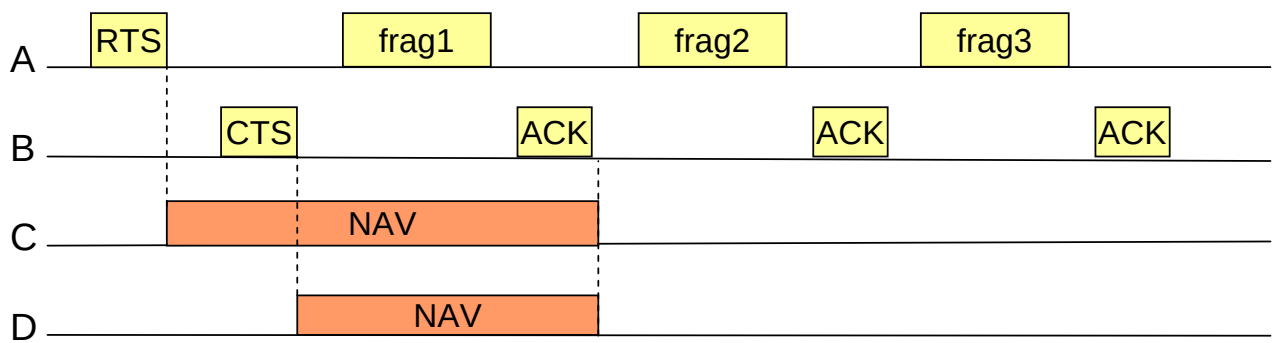
- a parameter of each cell
- can be adjusted by the base station

» multiple fragments can be sent one after another

- once the channel has been acquired using RTS/CTS

» NAV mechanism only keeps other stations quiet until the next acknowledgement :

- SIFS mechanism allows whole burst to be sent without interference

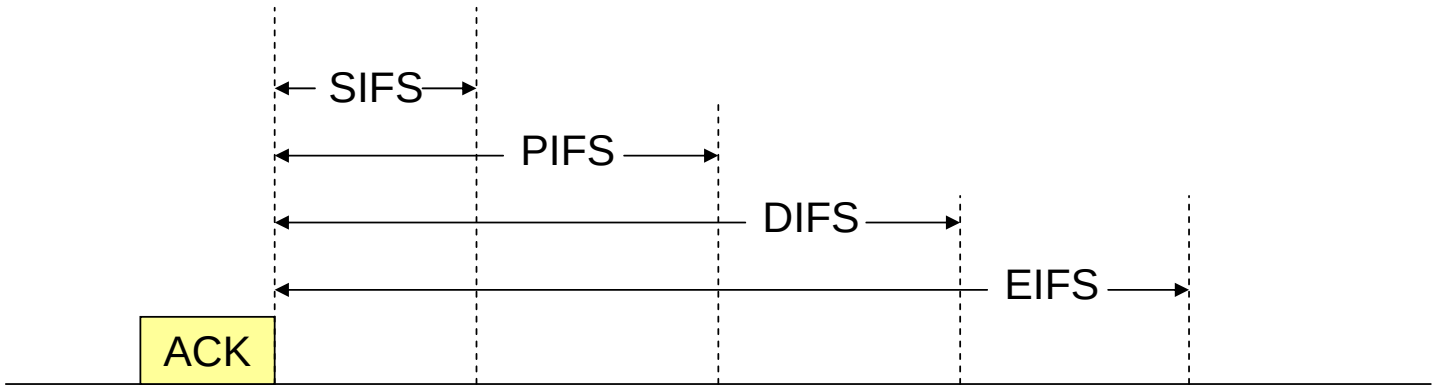


- standard allows the station to transmit to a different address between retransmissions of a given fragment
  - ¤ useful when there are several outstanding packets to be sent to different stations and one does not respond

- PCF : Point Coordination Function
  - – base station (access point) polls other stations
    - » asking if they any frames to send
  - – no collisions occur because under central control
  - – standard prescribes the polling mechanism
    - » but not polling frequency, polling order or priority of service
  - – base station periodically (10 – 100 times per second) sends a *Beacon* frame
    - » contains parameters : hopping sequences, dwell times, clock synchronisation
      - allows stations to keep in synch with the base station's clock
    - » this also invites new stations to sign up for polling service
      - once signed up, station guaranteed a certain fraction of the bandwidth
      - can thus give quality of service guarantees
  - – a CF-Poll frame starts a *Contention Free Period* (CFP) frame
    - » during which data is transferred between one or more stations
  - – a CF-End frame terminates the CFP
    - » CFPs alternate with Contention Periods
  - – allows PCF to coexist with DCF !

- Power Saving
  - – wireless LANs typically related to mobile stations with limited battery power
  - – a mechanism defined by the standard to allow stations to go to *sleep mode*
    - » for long periods of time
    - » without losing information
  - – base station keeps track of stations in sleep mode
    - » and buffers packets addressed to those stations
    - » until they poll for them or change their operation mode
  - – Beacon frames contain information about which stations have packets buffered for them
    - » these stations should wake up
      - still listening even in sleep mode
    - » and send a poll message to the base station to get these frames
  - – multicasts and broadcasts are stored by the base station
    - » transmitted at pre-known times (DTIM parameter) at which all power saving stations who wish to receive these frames should be awake

- Inter-Frame Spaces (IFS)



  - SIFS : Short Inter-Frame Spacing
    - » used to separate transmissions belonging to a single dialogue
      - e.g. fragment – ACK, RTS - CTS
    - » the minimum inter-frame space
    - » at most one station to transmit at this time
      - giving it priority over all other stations
    - » calculated to give time for transmitter to switch back to receive mode
      - and be capable of decoding an incoming frame
      - physical layer dependent e.g. 10µs for 802.11b

– PIFS : Point Coordination Function IFS

» used by the base station to gain access to the medium

- after a SIFS station has had a chance
- before any other stations get a chance

» can send a beacon frame or a PCF poll frame

» = SIFS + slot-time

– DIFS : Distributed Coordination Function IFS

» used if base station does not wish to use the channel

» any station may attempt to acquire the channel and send a new frame

» = PIFS + slot-time

» exponential back-off if a collision occurs

– EIFS : Extended IFS

» used by a station that has received a frame it could not understand

» a longer IFS needed to prevent a collision with a future frame belonging to the current dialogue

- since it could not understand the duration information for the Virtual Carrier Sense

– Exponential Back-Off

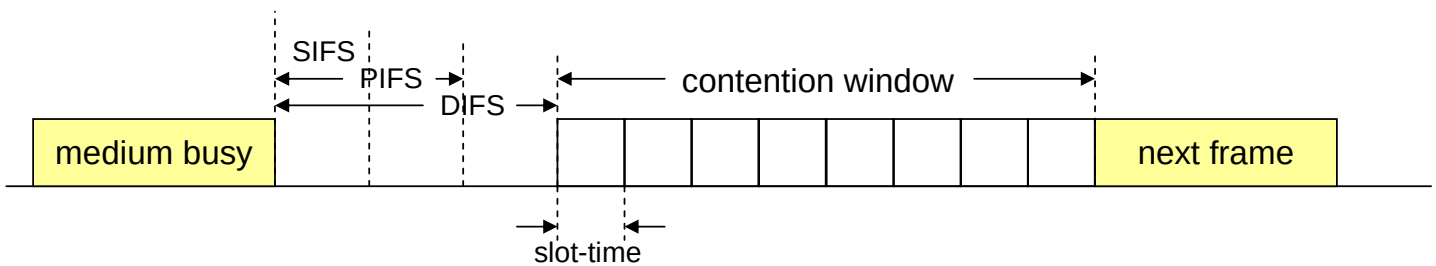
» wait a number of time-slots before accessing the medium

- a random number between *0* and *n*
- the number *n* doubled after each failure

» must be executed :

- when a station senses the medium before transmission of a frame and the medium is busy
- after each retransmission
- after a successful transmission

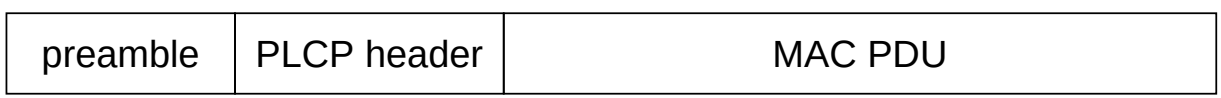
» not used when medium has been free for more than DIFS



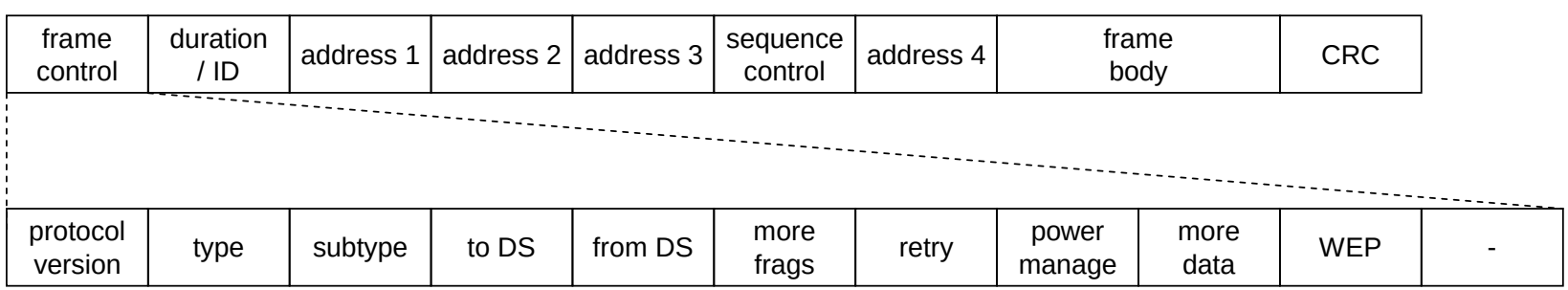
» *slot-time* defined so that a station can always determine if another station has access the medium at the beginning of the previous slot

- reduces the collision probability by half
- = 20µs for 802.11b, = 9µs for 802.11a etc.

- Frame types and structure
  - data frames used for data transmission
  - control frames used to control access to the medium
    - » e.g. RTS, CTS, ACK
  - management frames
    - » transmitted as data frames to exchange management information
    - » not forwarded to upper protocol layers
  - all frames have the structure :



  - MAC PDU :



» types and subtypes e.g. type = `control', subtype = 'ACK'

» to DS : set for frames destined for the Distribution System

» from DS : for frames coming from the Distribution System

» more frags : more fragments yet to follow

» retry : retransmissions of previous failed transmissions

» more data : data has been buffered for station in power save mode

» WEP (Wired Equivalent Privacy) : set when information has been encrypted

» duration/ID : duration to adjust the NAV period
or ID for stations trying to poll

» addresses : 48 bits : BSS identifier, source/destination addresses,
transmitter/receiver addresses

- depending on values of `to DS/from DS'

» sequence : 16 bit sequence number of a fragment

- 12 bits to identify the frame
- 4 bits to identify the fragment

- Joining an existing BSS :
  - a station needs to know the SSID of the network it wants to join
    - » SSID : Service Set Identifier – the network's name
    - » keeping this private is the first level of security
      - often set by default on delivery e.g. always `tsunami' for CISCO interface cards!
      - SSID also broadcast by default in beacon frames and these can be intercepted
  - a station needs to get synchronisation information from the base station
    - » or from other stations in an *ad hoc* network
  - by *passive scanning :*
    - » waits to receive a beacon frame from the base station
  - by *active scanning* :
    - » to find which access points are within range
    - » transmits a *probe request* frame and waits for a *probe response* frame
    - » response contains capability information e.g. supported data rates
  - choice of active or passive up to the station itself
  - joining process goes through two stages :
    - » *Authentication*
    - » *Association*

– Authentication

» station sends an *authentication frame*

- containing its identity (MAC address)

» *MAC address filtering* :

- if the facility is enabled, the Access Point checks that the MAC address is valid
- i.e. the station is permitted to join this network
- maintains a list of allowed MAC addresses

» *Open Authentication* :

- AP checks MAC address, if enabled, and responds with acceptance or rejection
- minimal authentication - essentially *null*
  - ¤ MAC addresses can be *spoofed*

» *Shared Key Authentication* :

- AP creates an authentication frame containing 128 bytes of random *challenge text*
  - ¤ and sends it to the joining station
- joining station encrypts the frame with its pre-shared WEP key
  - ¤ and sends it back to the AP
- AP decrypts the frame and checks that the text is correct
  - ¤ and again responds with acceptance or rejection

» *deauthentication* frames also available

– Association

» station sends an *association request* frame to the access point

- containing the Service Set Identifier (SSID) of the network to associate with
- and information about its interface card e.g. supported data rates

» Access Point sends an *association response* frame

- contains an acceptance or rejection notice
- if accepted, access point reserves memory space
- and returns an ID for the association and data rates available

» allows station to use the access point to communicate with other stations

- and systems on the Distribution System

» *deassociation* frames also available

– Reassociation

» needed if a station roams away from the currently associated access point

- and finds another access point having a stronger beacon signal

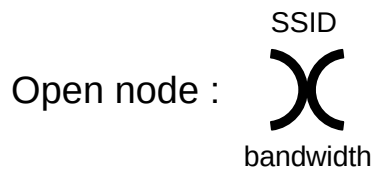
» station sends a *reassociation request* frame to the new access point

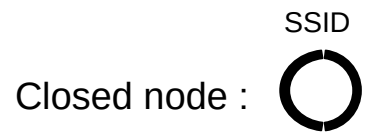
» new AP sends a *reassociation response* frame with acceptance or rejection

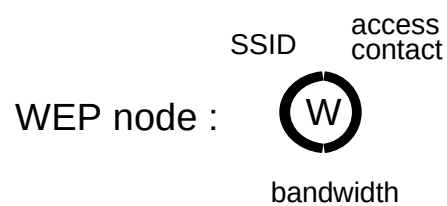
- contains an association ID and supported data rates etc.

» if accepted, new access point coordinates forwarding of data frames that may still be buffered in the old access point

- Security
  - – radio waves at 2.4GHz easily penetrate building walls
    - » may be received at ranges beyond the control of the host organisation
    - » passive eavesdropping very easy
      - warchalking – part of Wi-Fi urban mythology :
  - – also potentially a problem for wired networks
    - » electromagnetic radiation can be picked up
  - – LAN adapters offer a *promiscuous* mode
    - » both wired and wireless
    - » every packet can be captured and analysed
  - – same security issues face wired LANs as wireless LANs
    - » data on a wired LAN is often incorrectly assumed to be protected
      - because wires only run inside buildings
      - corporate Internet-accessible networks invalidate this presumption
    - » threats to physical security of network e.g. denial of service attacks, sabotage
    - » attacks from within an organisations authorised user community
      - e.g. disgruntled current and former employees







- WEP : Wired Equivalent Privacy
  - – designed to meet criteria :
    - » reasonably strong
      - to meet customer privacy, cost and convenience needs
    - » self-synchronising
      - for when stations go in and out of coverage
    - » computationally efficient
      - can be implemented either in hardware or software
      - if efficient enough, software on slow machines still sufficient
    - » exportable
      - USA regards encryption as an armament and tries to control its export
      - (inevitably doomed to failure in practice e.g. PGP)
    - » optional
      - 802.11 does not require encryption always to be enabled
        - ¤ or even implemented in an interface card
        - ¤ can still be 802.11 standard compliant
      - default is usually *off* as interface cards are delivered

– Encryption of plain text :
  » a 40-bit secret key is pre-agreed and pre-shared by the network stations
    - not defined how this happens!
  » a 24-bit *Initialisation Vector* (IV) is concatenated with secret key
    - to produce a 64-bit total key size
    - normally a random value but sometimes just successive integer values from zero
    - *chosen by sender*
  » resulting key is input into the Pseudo-Random Number Generator
    - using the RC4 algorithm
  » outputs a pseudo-random key sequence based on the input key
  » key sequence used to encrypt data by doing a *bitwise XOR*
  » results in the number of encrypted bytes as data bytes + 4
  » extra 4 bytes Integrity Check Value (ICV)
    - ICV computed using CRC-32 over the message plaintext
    - concatenated to end of plain text
    - and also encrypted by the key sequence
  » IV communicated to the peer by placing it, *in clear*, before the cipher text
  » only data frames encrypted, not management frames

- RC4 Encryption Algorithm
  - invented by Ronald Rivest in 1987 (RC4 = Ron's Code version 4)
  - a *symmetric* algorithm
    - » same key used to encrypt and to decrypt
  - kept as a trade secret until 1994, then anonymously posted on the Internet
  - a somewhat complex scheme based on a state table initialised by the key
  - strengths :
    - » difficulty of knowing where any value is in the state table
    - » difficulty of knowing which location in the table is used to select the next key sequence value
    - » about 10 x faster than DES encryption (Data Encryption Standard)
  - weaknesses :
    - » vulnerable to analytic attacks on the state table
    - » 1 in every 256 keys can be a weak key
      - cryptanalysis can identify which generated bytes are correlated with key bytes
  - also used in the SSL Internet protocol and other cryptography products

– Decryption of cipher text :

» the IV of the incoming message used to generate the key sequence

- together with the secret key

» bitwise XOR with the cipher text regenerates the plain text and ICV

» decryption verified by performing the integrity check algorithm on the recovered plain text

» and comparing the computed value with the transmitted value

- an error indication sent back to the transmitting station if not equal

– the IV extends the useful life of the secret key

» a different key sequence for every different IV

– secret key remains constant while IV changes periodically

» usually changes for every frame transmitted

» so that every packet is encrypted with a different key stream

- to increase the degree of privacy

– WEP can be used with or without shared key authentication

- Security Weaknesses of WEP
  - – Key Management
    - » not specified in the WEP standard
      - poor quality keys may be used
        - ¤ e.g. guessable text strings to generate the key
    - » synchronising change of keys is tedious and difficult
      - keys therefore will tend to be long-lived
      - probably one single key shared between every station on the network
  - – Key Size
    - » 40-bit key size was considered reasonable when standard specified in 1997
      - probably sufficient against casual eavesdropping then
        - ¤ export of 40-bit key encryption systems not controlled by US government
    - » 40-bit keys now considered vulnerable to brute-force attack
      - probably even in 1997 by NSA !
    - » most interface card manufacturers have now implemented a 104-bit key
      - a *de facto* standard
      - 104 bit key + 24 bit IV = 128 bits
    - » not considered the primary weakness of WEP

– Initialisation Vector (IV) too small

» 24 bits provides 16777216 different RC4 key sequences

- for a given WEP key

» IV re-use is the problem

» if the RC4 cipher stream for a given IV is found, an attacker can decrypt subsequent packets that were encrypted with the same IV

- don’t need to know the WEP key – just the key sequence
- in practice, much easier to discover the key sequence anyway

» WEP does not specify how the IV is chosen or how often it is changed

- start at zero, increment and roll over back to zero after 16 million packets sent
- or choose at random

» random choice sounds better but isn’t !

- a 50% chance of re-use after 5000 packets

» many methods for finding the key sequence for a particular IV

» e.g. given two encrypted packets with the same IV, the XOR of the encrypted packets gives the XOR of the original packets

- $(p1 \oplus ks) \oplus (p2 \oplus ks) = p1 \oplus (ks \oplus ks) \oplus p2 = p1 \oplus 0 \oplus p2 = p1 \oplus p2$

» if victim is on the Internet, attacker can simply *ping* the victim
- or send an email message
- packets will be sent to the victim by the AP he is using
- AP will encrypt the packets on behalf of the attacker
- and observe and analyse these encrypted packets
  - ¤ just need to wait for the same IV to be reused

» from p1 ⊕ p2, if the attacker knows p2, he can deduce p1
- and hence deduce the key sequence
- to decrypt subsequent packets

» intricate low-level capabilities required
- but straightforward in principle
- hardware/software systems to do this readily available via the Internet

» even without these *active* methods, *passive* methods also possible
- data in frames from higher level protocols e.g. IP is highly predictable
- an attacker can readily determine portions of the key sequence in the same way
  - ¤ just as the German Enigma machine was cracked in WWII – using plain text hints

» over a period of time, all the key sequences could be determined
- and saved up in a database for later re-use

» a much large IV is needed to obviate this weakness

– the Integrity Check Value (ICV) is not appropriate

» based on CRC-32 : $x^{32}+x^{26}+x^{23}+x^{22}+x^{16}+x^{12}+x^{11}+x^{10}+x^8+x^7+x^5+x^4+x^2+x^1+1$

» good checksum for error detection but *awful* choice for a cryptographic hash

- better encryption systems use MD5 (RFC 1321)
- or SHA-1 (Secure Hashing Algorithm) from NIST (US National Institute of Standards and Technology)

» CRC-32 ICV is a *linear* function of the message

- an attacker can modify an encrypted packet
- and easily fix the ICV so that the message appears authentic
  - ¤ without knowing the contents of the message

» many possible attacks based on this approach

» e.g. attacker can make the victim's wireless AP decrypt the packets for him

- simply capture an encrypted packet stream
- modify the destination address of each packet to be the attacker's IP address
- fix up the ICV
- retransmit the packets over the air to the AP
- AP happily decrypts the packets and forwards them to the attacker!

» biggest weakness is that ICV-based attacks are independent of key size

– WEP’s use of RC4

» RC4 has been found to have some weak keys

- more correlation between key and output than there should be for good security

» possible weak keys can be identified by examining the IV

- first three bytes of key, sent in plain text in each packet

» about 9000 out of 16 million IV values `interesting’ to cracker tools

» if attacker captures enough interesting packets, only necessary to try a small number of possible keys to gain access to the network

» because all the original IP packets start with known values, easy to know when you have found the right key

» for a 104 bit WEP key, only have to capture between 2000 and 4000 interesting packets

» on a busy network

- 1000000 packets a day common
- a few hundred interesting packets might be captured

» best approach is not to use these weak keys

- most vendors now offer algorithms which avoid them
- but only need one station using weak keys for the attack to succeed

– Authentication messages can be forged

» open system versus shared key authentication

» shared key should be better than open system

» in practice, the reverse is true!

» monitoring attacker can observe both the challenge and the encrypted response

» can therefore determine the key sequence used to encrypt the response

- and use that stream to encrypt any challenge he receives in future
- i.e. can later forge an authentication

» shared key authentication also allows a station quickly to determine if they know the correct WEP key

- allows a malicious client station to try a `dictionary' attack on the network
- since keys usually generated from text strings

» best for network managers to turn shared key authentication *off*

- and depend on other protocols e.g. 802.1X
- or use VPNs (Virtual Private Networks) on top of Wi-Fi
  - ¤ through a *firewall*

– Denial of Service attacks

» client stations must be authenticated

» 802.11 standard includes facility for *deauthentication*

- via deauthentication frames

» clients and access points can request deauthentication from one another

» unfortunately, this request message is *not* itself authenticated!

» an attacker can therefore *spoof* such a message

» access point or client will refuse all further packets until authentication is reestablished

- how long depends on how aggressively the client retries and on any higher-level time-outs or back-offs

» by repeated attacks, a client can be denied access to the network indefinitely

» a very flexible form of attack

- can target individual clients or whole network, limit rates of access etc.
- can also prevent a client from switching to an overlapping network
  - ¤ by monitoring other channels also

» similar vulnerability applies to association/disassociation

» possible power saving vulnerability might allow buffered packets to be lost

- Improving 802.11 Security
  - Working Group 802.11i set up to define a better standard than WEP
    - » should report late 2003
  - two main developments :
    - » Wi-Fi Protected Access (WPA)
    - » Robust Security Network (RSN)
  - WPA :
    - » to plug holes in legacy devices
      - by firmware or driver upgrades
    - » uses Temporal Key Integrity Protocol (TKIP)
      - changes ways keys are derived and how they are rotated
      - adds a message-integrity-check to prevent packet forgeries
    - » but may not be backward-compatible with all legacy devices
      - will probably degrade performance
      - unless acceleration hardware incorporated

– RSN :

» dynamic negotiation of authentication and encryption algorithms

- lets algorithms evolve with the state of the art in security and algorithms

» authentication scheme proposed based on 802.1X and the Extensible Authentication Protocol (EAP) (RFC 2284)

» encryption algorithm is the Advanced Encryption Standard (AES)

- *Rijndael* selected by NIST after open competition
- invented by Daemen and Rijmen in Belgium
- a block cipher with variable block length and key length
- can be very efficiently implemented on a wide variety of hardware

» should be significantly stronger than WEP and WPA

- but will run very poorly on legacy devices
- seen to be the future of wireless security