Wireless LANs: 802.11

Sridhar Iyer

Leena Chandran-Wadia

K R School of Information Technology

IIT Bombay

Revised by Quan Le-Trung, *Dr.techn.*

http://sites.google.com/site/quanletrung/

Outline

- Challenges of wireless communications
- IEEE 802.11
  - spread spectrum and physical layer specification
  - MAC functional specification: DCF mode
    - role in WLANs – infrastructure networks
    - role in MANETs
  - MAC functional specification: PCF mode

References

- http://standards.ieee.org/getieee802/802.11.html
  IEEE Computer Society 1999, Wireless LAN MAC and PHY layer specification

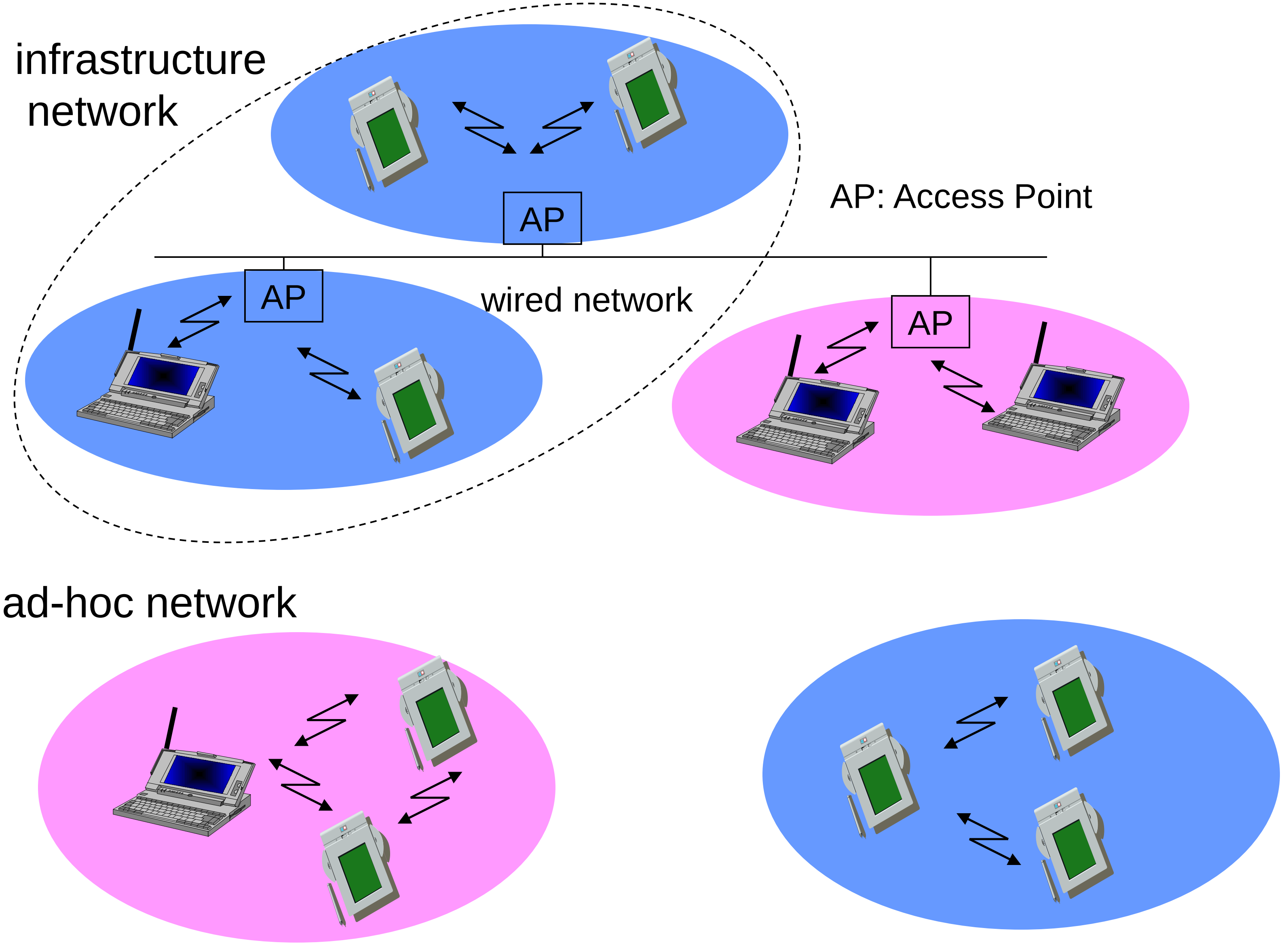
Wireless LANs

- Infrared (IrDA) or radio links (Wavelan)
- Advantages
  - very flexible within the reception area
  - Ad-hoc networks possible
  - (almost) no wiring difficulties
- Disadvantages
  - low bandwidth compared to wired networks
  - many proprietary solutions
    - Bluetooth, HiperLAN and IEEE 802.11

Wireless LANs vs. Wired LANs

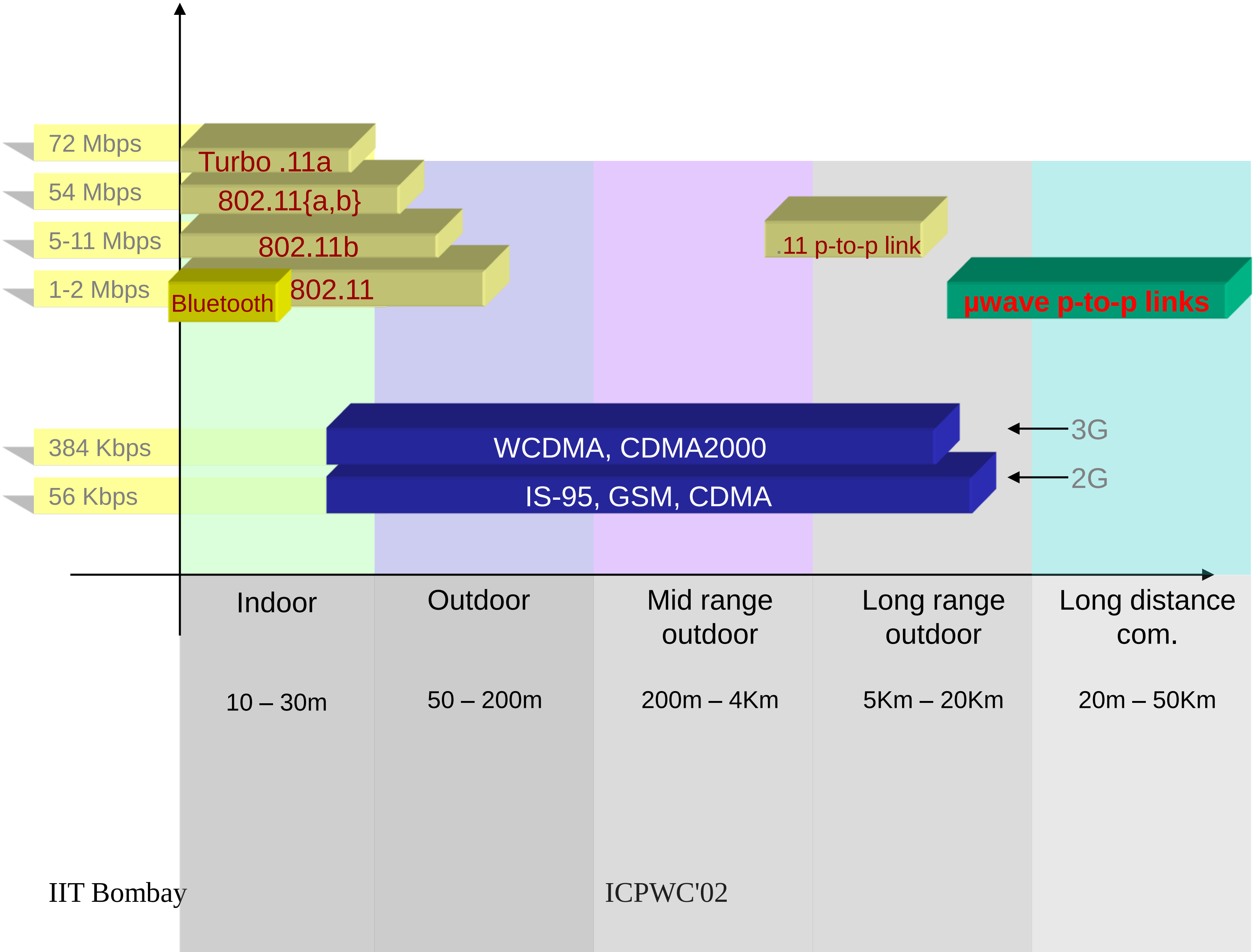
- Destination address does not equal destination location
- The media impact the design
  - wireless LANs intended to cover reasonable geographic distances must be built from basic coverage blocks
- Impact of handling mobile (and portable) stations
  - Propagation effects
  - Mobility management
  - Power management

Infrastructure vs. Ad hoc WLANs



Source: Schiller

Wireless Technology Landscape



Challenges of
Wireless Communications

Wireless Media

- Physical layers used in wireless networks
  - have neither absolute nor readily observable boundaries outside which stations are unable to receive frames
  - are unprotected from outside signals
  - communicate over a medium significantly less reliable than the cable of a wired network
  - have dynamic topologies
  - lack full connectivity and therefore the assumption normally made that every station can hear every other station in a LAN is invalid (i.e., STAs may be "hidden" from each other)
  - have time varying and asymmetric propagation properties

Limitations of the mobile environment

- Limitations of the Wireless Network
  - limited communication bandwidth
  - frequent disconnections
  - heterogeneity of fragmented networks

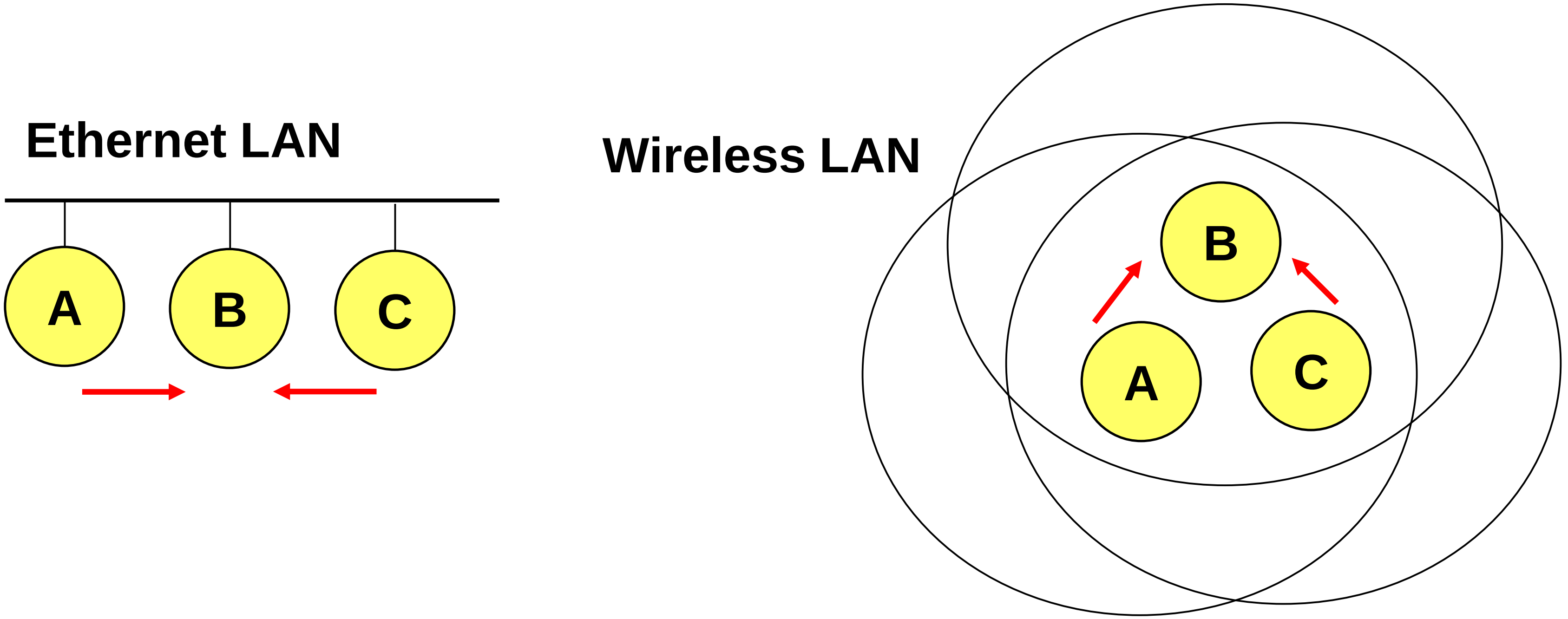
- Limitations Imposed by Mobility
  - route breakages
  - lack of mobility awareness by system/applications

- Limitations of the Mobile Device
  - short battery lifetime
  - limited capacities

Wireless v/s Wired networks

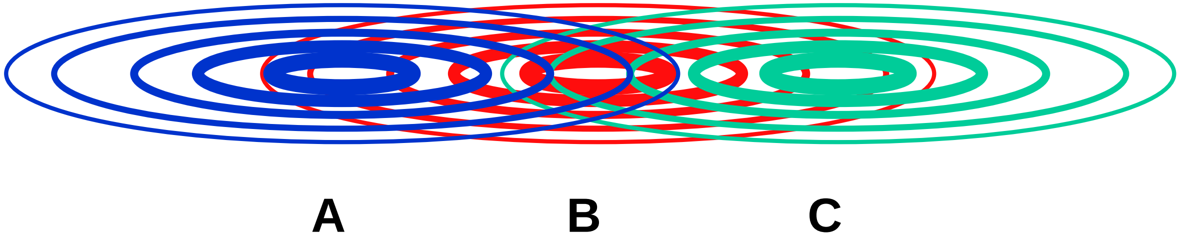
- Regulations of frequencies
  - Limited availability, coordination is required
  - useful frequencies are almost all occupied
- Bandwidth and delays
  - Low transmission rates
    - few Kbps to some Mbps
  - Higher delays
    - several hundred milliseconds
  - Higher loss rates
    - susceptible to interference, e.g., engines, lightning
- Always shared medium
  - Lower security, simpler active attacking
  - radio interface accessible for everyone
  - Fake base stations can attract calls from mobile phones
  - secure access mechanisms important

Difference Between Wired and Wireless



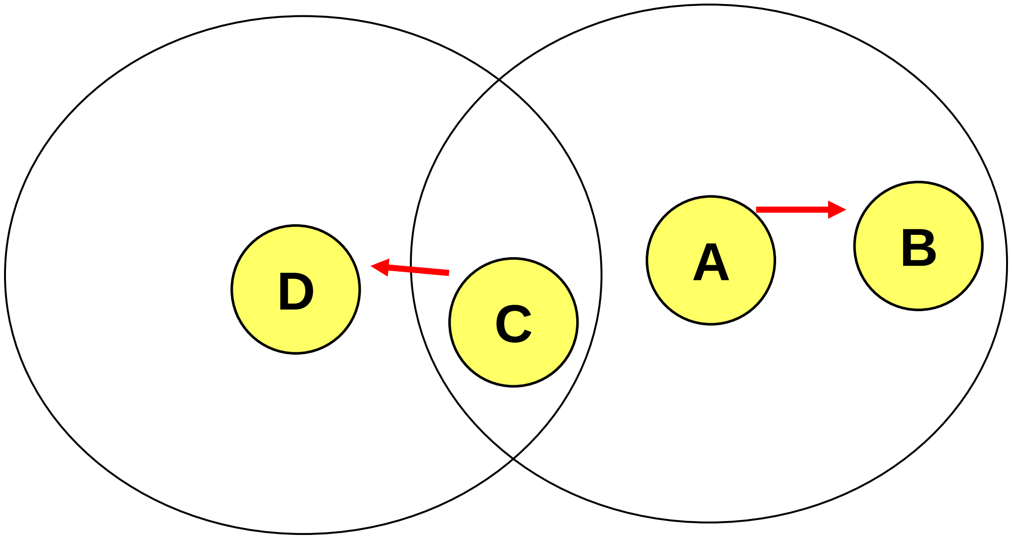
- If both A and C sense the channel to be idle at the same time, they send at the same time.
- Collision can be detected at sender in Ethernet.
- Half-duplex radios in wireless cannot detect collision at sender.

Hidden Terminal Problem



- A and C cannot hear each other
- A sends to B, C cannot receive A
- C wants to send to B, C senses a “free” medium (Carrier Sense fails)
- Collision occurs at B
- A cannot receive the collision (Collision Detection fails)
- A is “hidden” for C

Exposed Terminal Problem



- A starts sending to B
- C senses carrier, finds medium in use and has to wait for A->B to end
- D is outside the range of A, therefore waiting is not necessary
- A and C are “exposed” terminals

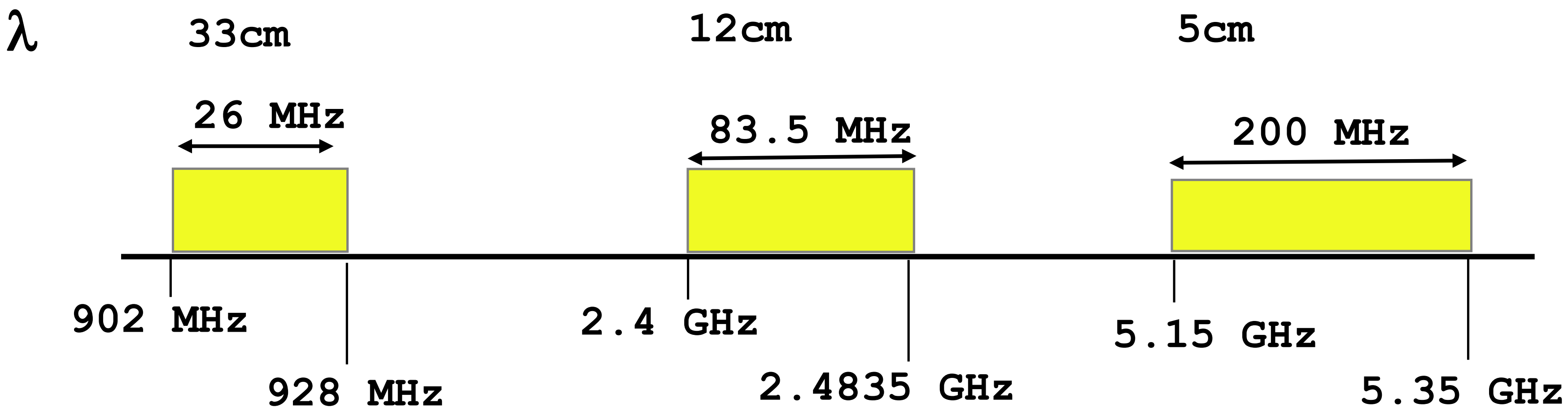
Effect of mobility on protocol stack

- Application
  - new applications and adaptations
- Transport
  - congestion and flow control
- Network
  - addressing and routing
- Link
  - media access and handoff
- Physical
  - transmission errors and interference

802.11-based Wireless LANs
Architecture and Physical Layer

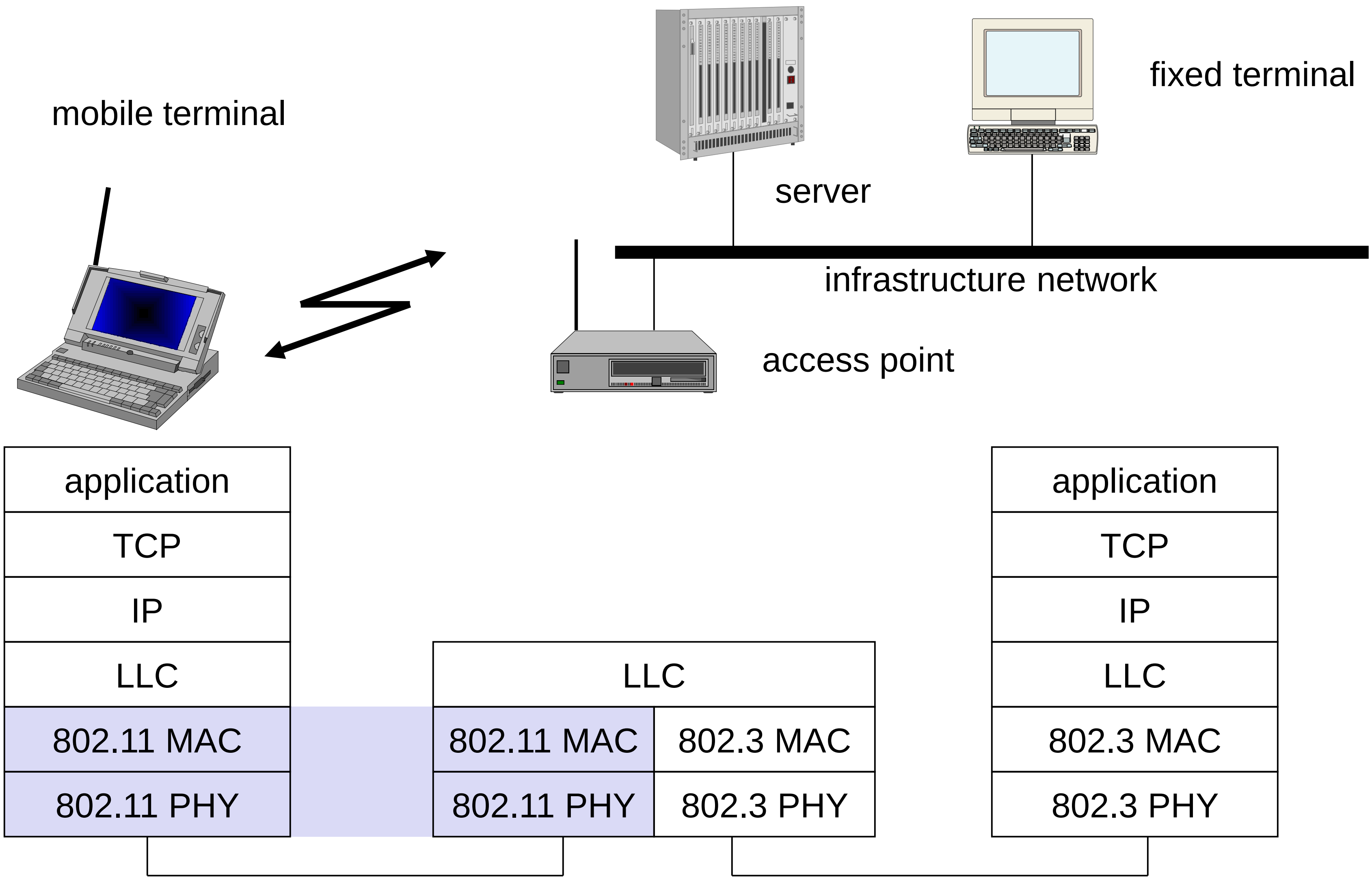
IEEE 802.11

- Wireless LAN standard defined in the unlicensed spectrum (2.4 GHz and 5 GHz U-NII bands)



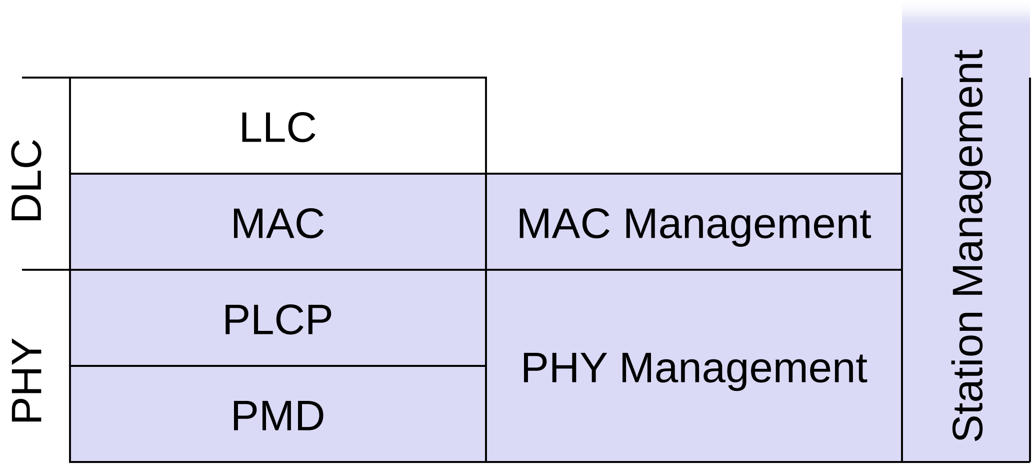
- Standards covers the MAC sub-layer and PHY layers
- Three different physical layers in the 2.4 GHz band
  – FHSS, DSSS and IR
- OFDM based Phys layer in the 5 GHz band (802.11a)

802.11- in the TCP/IP stack



802.11 - Layers and functions

- MAC
  - access mechanisms, fragmentation, encryption
- MAC Management
  - synchronization, roaming, MIB, power management



- PLCP Physical Layer Convergence Protocol
  - clear channel assessment signal (carrier sense)
- PMD Physical Medium Dependent
  - modulation, coding

PHY Management
  - channel selection, MIB

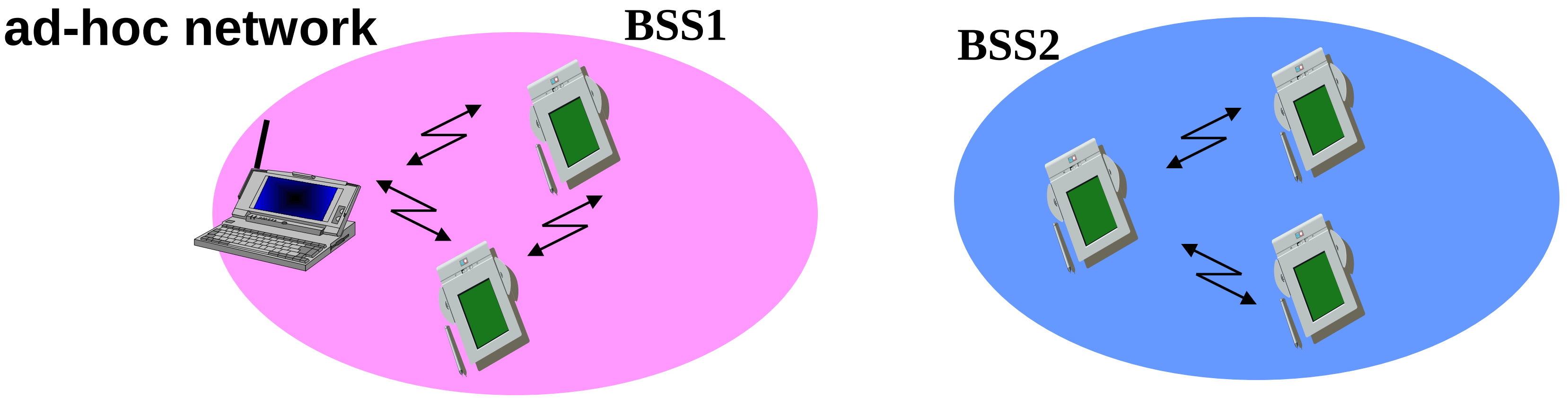
Station Management
  - coordination of all management functions

Clear Channel Assessment

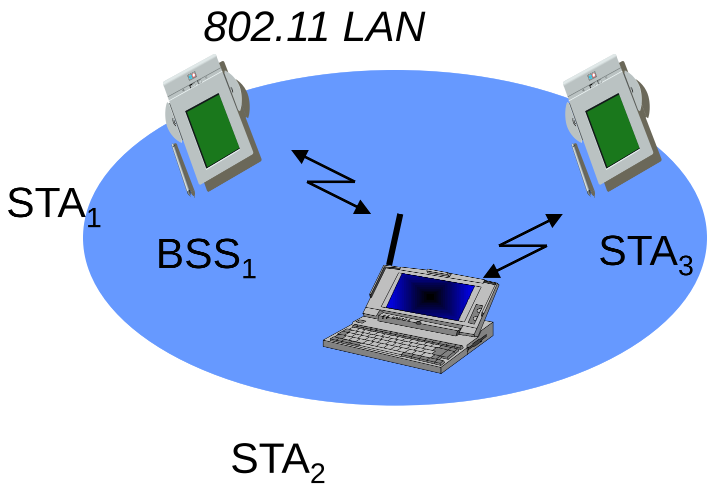
- Determine if the channel is open for transmission by checking the signal energy on the channel before transmitting
- A packet being transmitted will carry a signal intensity (called a received signal strength indication or RSSI) high enough to exceed a specified threshold and that all extraneous noise will fall below the threshold and be ignored
- If the channel detects an RSSI value above the clear channel assessment threshold (CCAT), it assumes the channel is in use by traffic and will postpone packet transmission

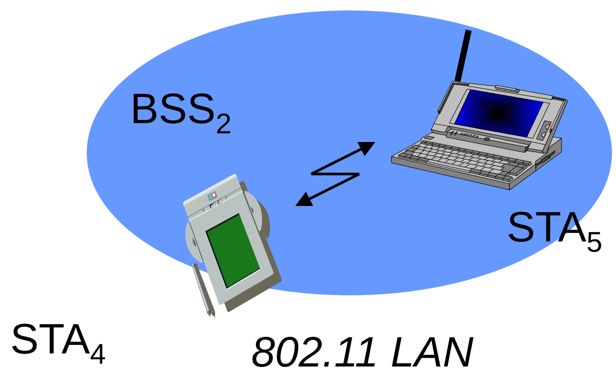
Components of IEEE 802.11 architecture

- The basic service set (BSS) is the basic building block of an IEEE 802.11 LAN
- The ovals can be thought of as the coverage area within which member stations can directly communicate
- The Independent BSS (IBSS) is the simplest LAN. It may consist of as few as two stations



802.11 - ad-hoc network

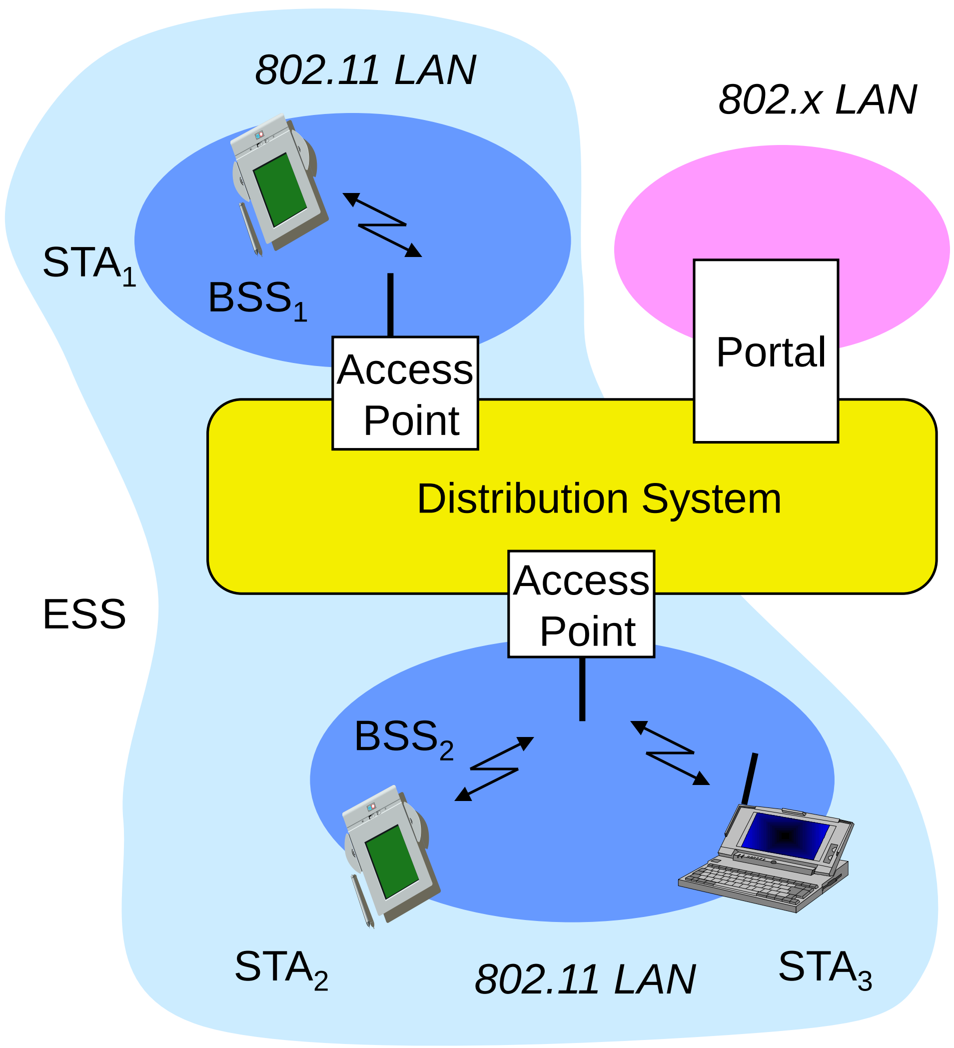




- Direct communication within a limited range
  - Station (STA): terminal with access mechanisms to the wireless medium
  - Basic Service Set (BSS): group of stations using the same radio frequency

Source: Schiller

802.11 - infrastructure network



- 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
  - 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

Source: Schiller

Distribution System (DS) concepts

- The Distribution system interconnects multiple BSSs
- 802.11 standard logically separates the wireless medium from the distribution system – it does not preclude, nor demand, that the multiple media be same or different
- An Access Point (AP) is a STA that provides access to the DS by providing DS services in addition to acting as a STA.
- Data moves between BSS and the DS via an AP
- The DS and BSSs allow 802.11 to create a wireless network of arbitrary size and complexity called the Extended Service Set network (ESS)

Extended Service Set network

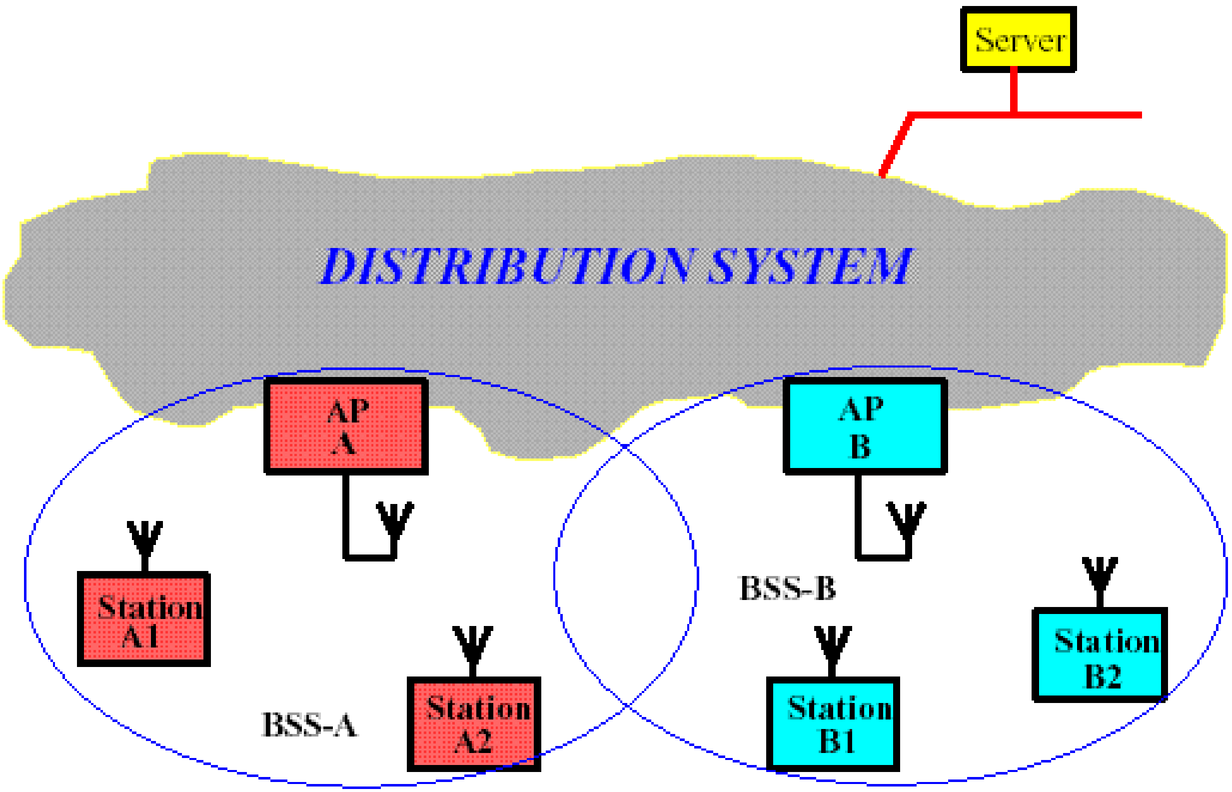


Figure 2 ESS Provides Campus-Wide Coverage

Source: Intersil

802.11 - Physical layer

- 3 versions of spread spectrum: 2 radio (typ. 2.4 GHz), 1 IR
  - data rates 1 or 2 Mbps
- FHSS (Frequency Hopping Spread Spectrum)
  - spreading, despreading, signal strength, typically 1 Mbps
  - min. 2.5 frequency hops/s (USA), two-level GFSK modulation
- DSSS (Direct Sequence Spread Spectrum)
  - DBPSK modulation for 1 Mbps (Differential Binary Phase Shift Keying), DQPSK for 2 Mbps (Differential Quadrature PSK)
  - preamble and header of a frame is always transmitted with 1 Mbps, rest of transmission 1 or 2 Mbps
  - chipping sequence: +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
  - max. radiated power 1 W (USA), 100 mW (EU), min. 1mW
- Infrared
  - 850-950 nm, diffuse light, typ. 10 m range
  - carrier detection, energy detection, synchronization

Spread-spectrum communications

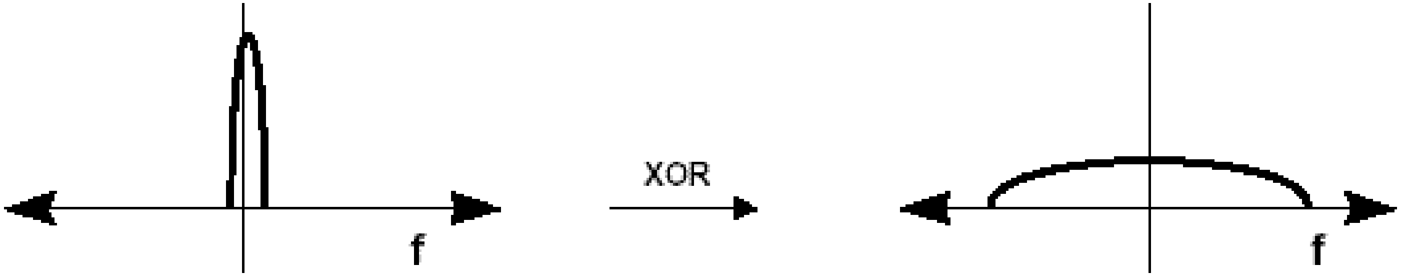


Figure 5a Effect of PN Sequence on Transmit Spectrum

pseudonoise (PN)

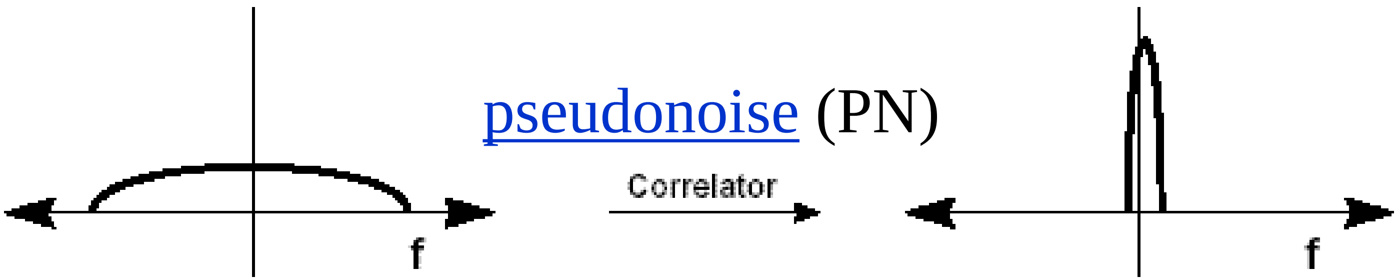
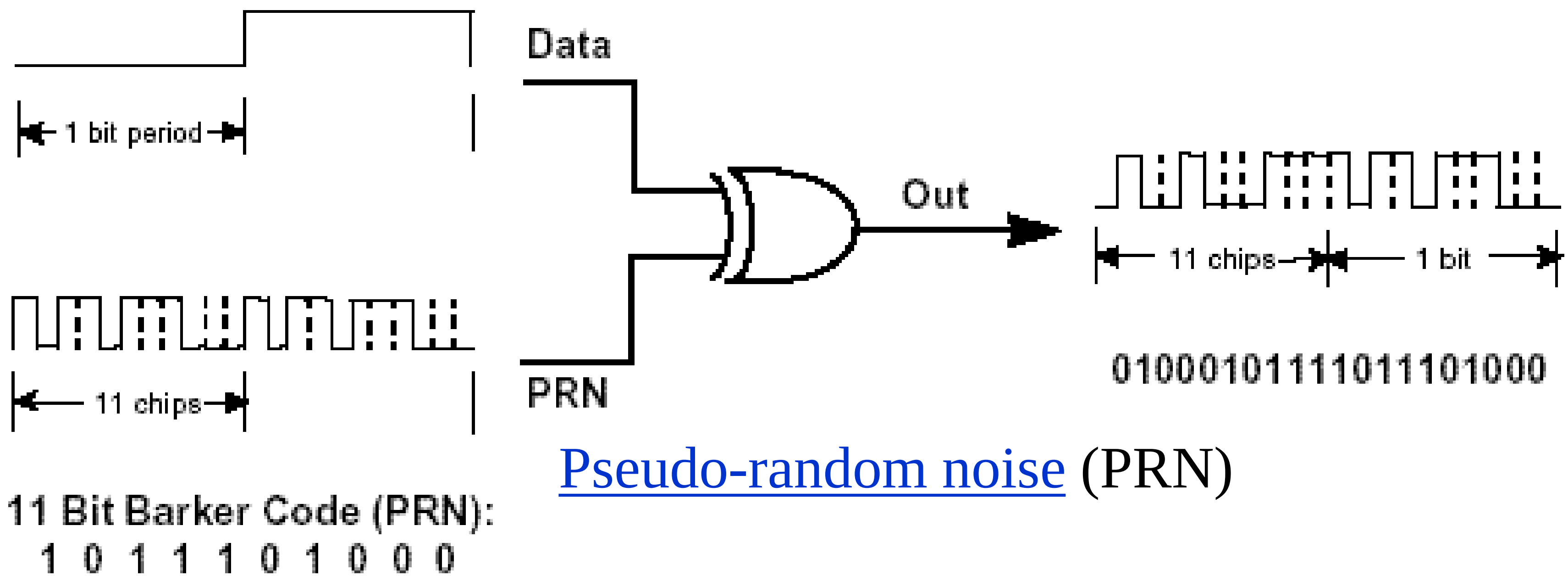


Figure 5b Received Signal is Correlated with PN to Recover Data and Reject Interference

Ref. APPLICATION NOTE 1890, "An Introduction to Spread-Spectrum Communications"
www.maxim-ic.com/an1890

Source: Intersil

DSSS Barker Code modulation



Pseudo-random noise (PRN)

Figure 3 Digital Modulation of Data with PRN Sequence

Source: Intersil

DSSS properties

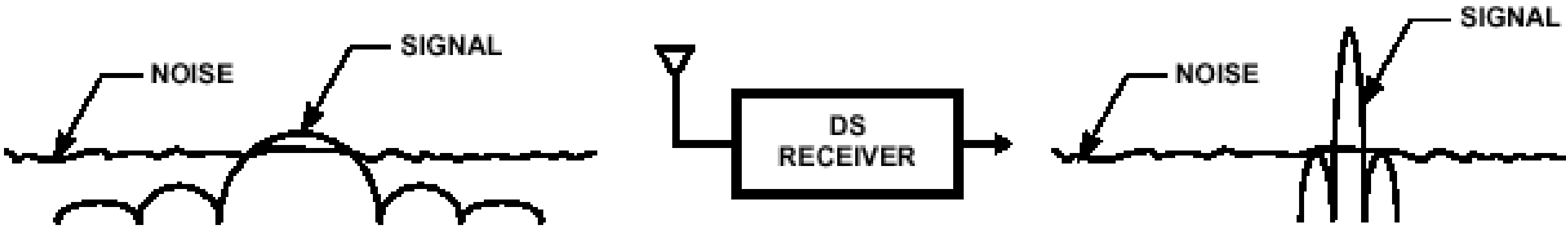


FIGURE 2A. LOW POWER DENSITY

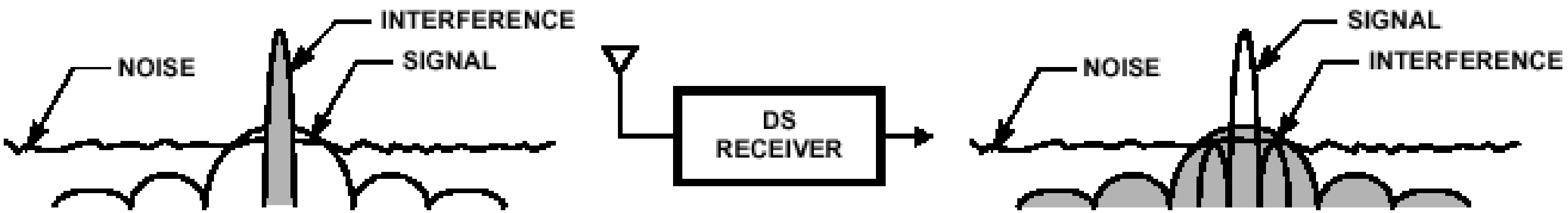


FIGURE 2B. INTERFERENCE REJECTION

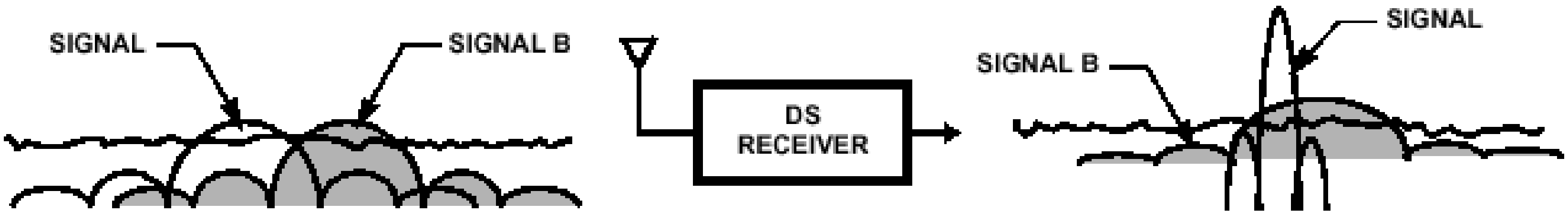


FIGURE 2C. MULTIPLE ACCESS

FIGURE 2. DIRECT SEQUENCE SPREAD SPECTRUM PROPERTIES

Source: Intersil

Hardware

- Original WaveLAN card (NCR)
  - 914 MHz Radio Frequency
  - Transmit power 281.8 mW
  - Transmission Range ~250 m (outdoors) at 2Mbps
  - SNRT 10 dB (capture)
- WaveLAN II (Lucent)
  - 2.4 GHz radio frequency range
  - Transmit Power 30mW
  - Transmission range 376 m (outdoors) at 2 Mbps (60m indoors)
  - Receive Threshold = - 81dBm
  - Carrier Sense Threshold = -111dBm
- Many others….Agere, Cisco,………

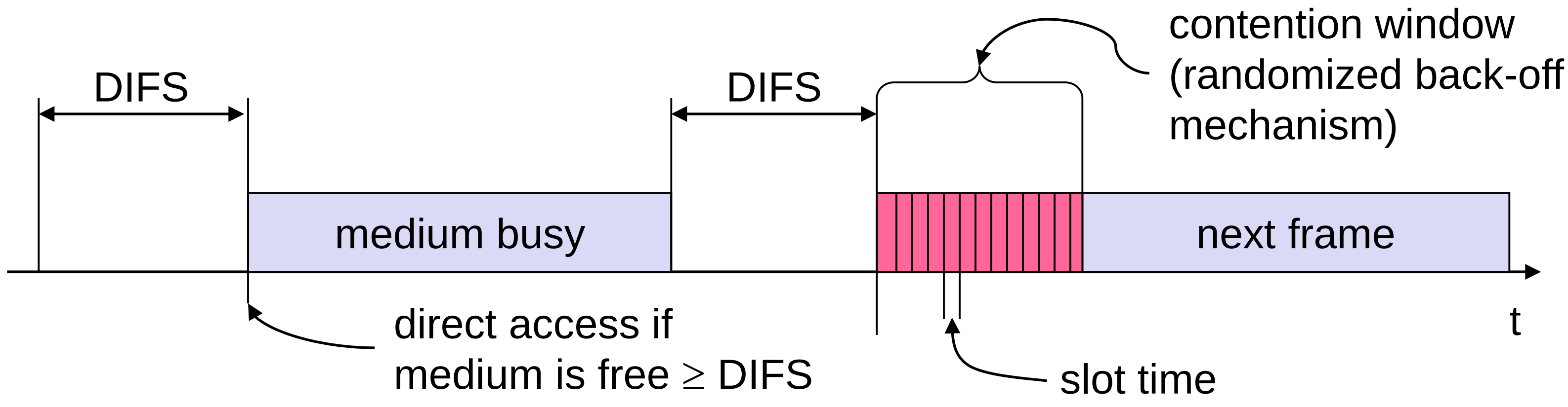
802.11-based Wireless LANs
MAC functional spec - DCF

802.11 - MAC layer

- Traffic services
  - Asynchronous Data Service (mandatory) – DCF
  - Time-Bounded Service (optional) - PCF

- Access methods
  - DCF CSMA/CA (mandatory)
    - collision avoidance via randomized back-off mechanism
    - ACK packet for acknowledgements (not for broadcasts)
  - DCF w/ RTS/CTS (optional)
    - avoids hidden/exposed terminal problem, provides reliability
  - PCF (optional)
    - access point polls terminals according to a list

802.11 - CSMA/CA

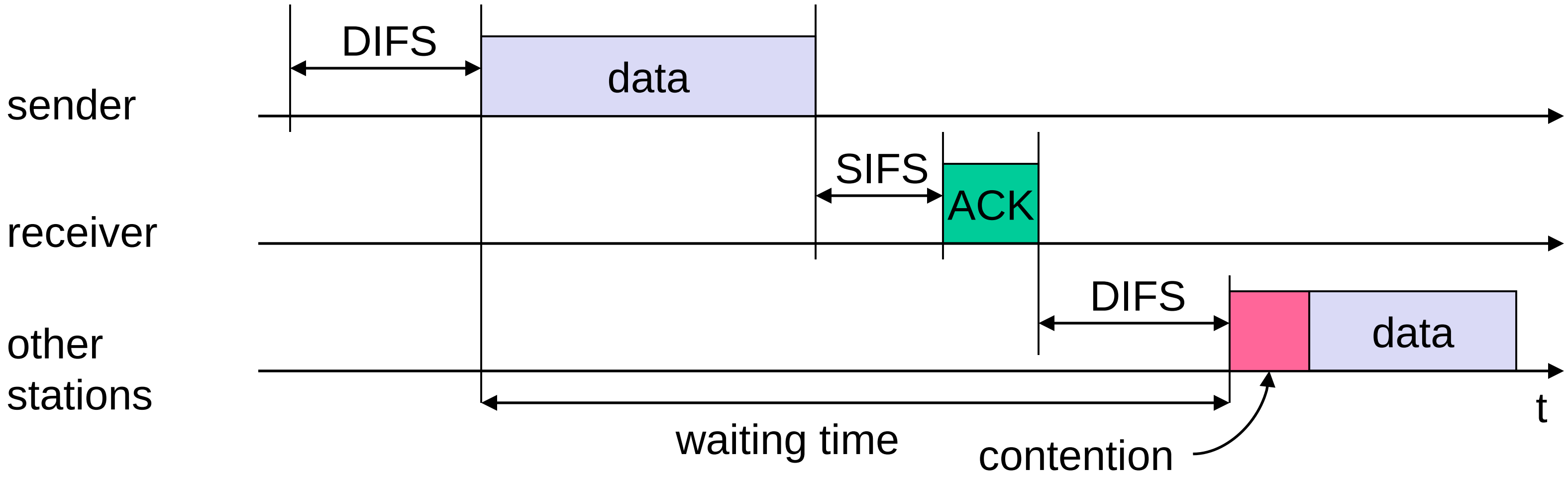


DCF Inter-Frame Space

- station which has data to send starts sensing the medium (Carrier Sense based on CCA, Clear Channel Assessment)
- if the medium is free for the duration of an Inter-Frame Space (IFS), the station can start sending (IFS depends on service type)
- if the medium is busy, the station has to wait for a free IFS plus an additional random back-off time (multiple of slot-time)
- if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

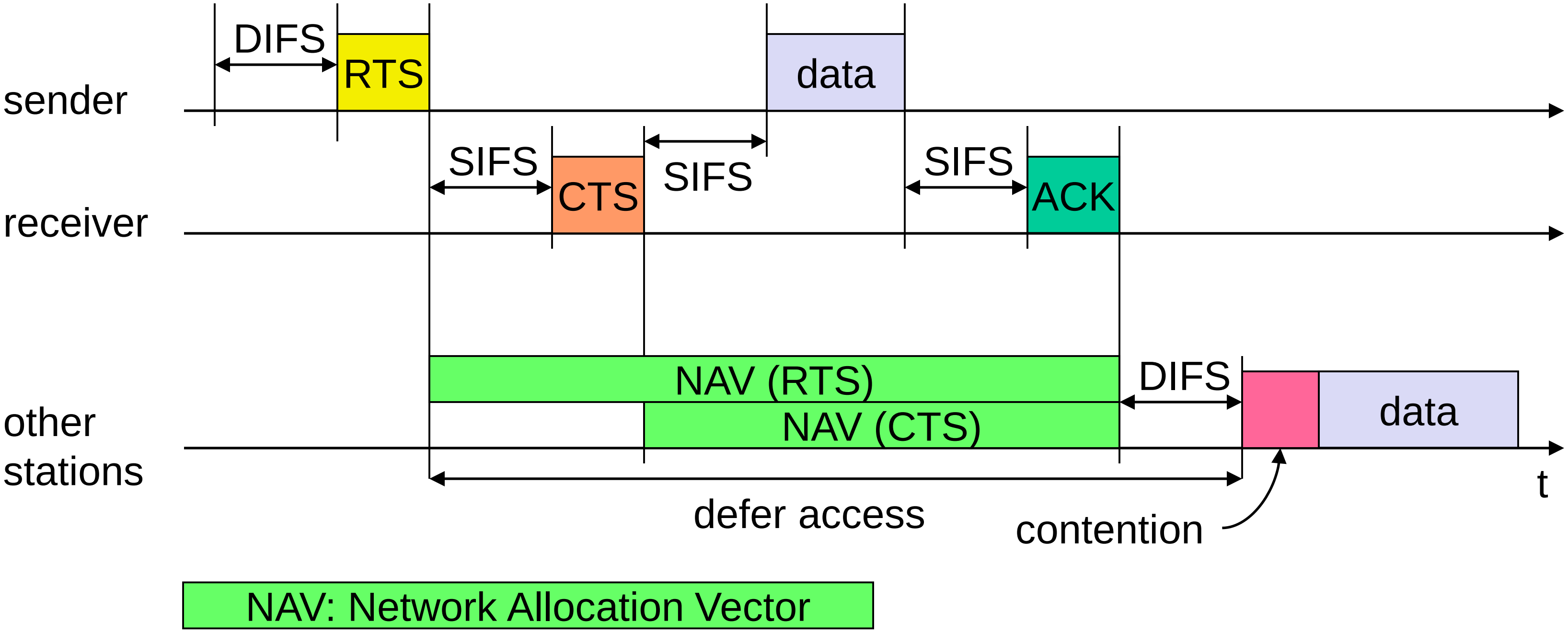
802.11 DCF – basic access

- If medium is free for DIFS time, station sends data
- receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly (CRC)
- automatic retransmission of data packets in case of transmission errors



802.11 –RTS/CTS

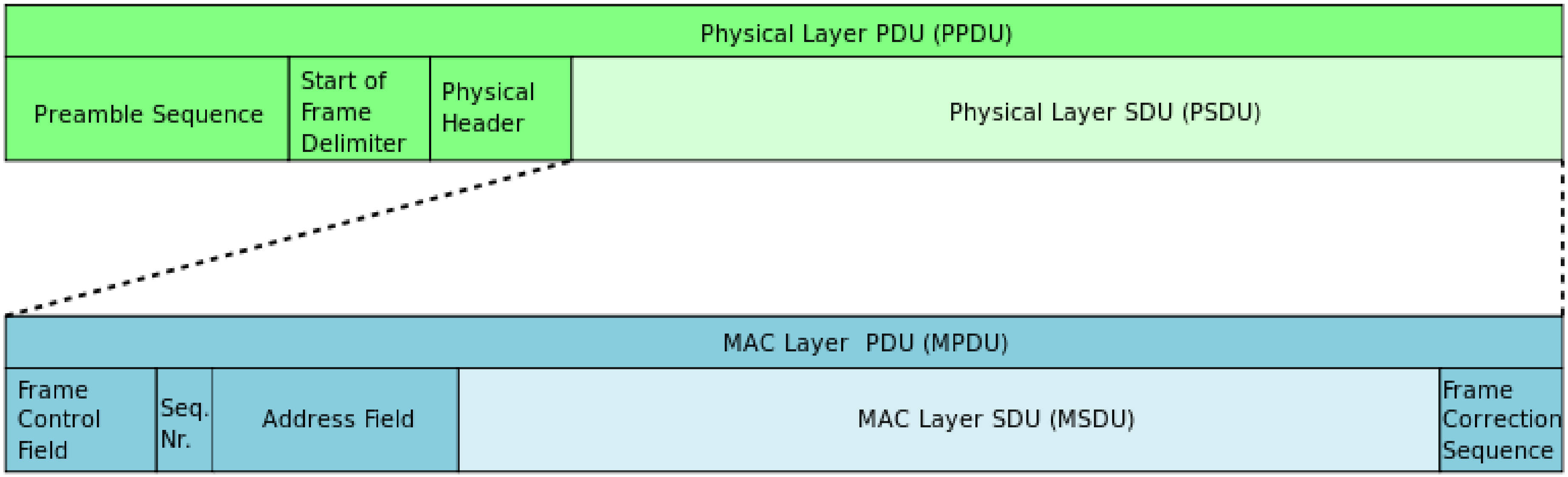
- If medium is free for DIFS, station can send RTS with reservation parameter (reservation determines amount of time the data packet needs the medium)
- acknowledgement via CTS after SIFS by receiver (if ready to receive)
- sender can now send data at once, acknowledgement via ACK
- other stations store medium reservations distributed via RTS and CTS



802.11 - Carrier Sensing

- **In IEEE 802.11, carrier sensing is performed**
  - at the air interface (*physical carrier sensing*), and
  - at the MAC layer (*virtual carrier sensing*)
- **Physical carrier sensing**
  - detects presence of other users by analyzing all detected packets
  - Detects activity in the channel via relative signal strength from other sources
- **Virtual carrier sensing** is done by sending MAC Protocol Data Unit (MPDU) duration information in the header of RTS/CTS and data frames
- Channel is busy if **either** mechanisms indicate it to be
- Duration field indicates the amount of time (in microseconds) required to complete frame transmission
- Stations in the BSS use the information in the duration field to adjust their network allocation vector (NAV)

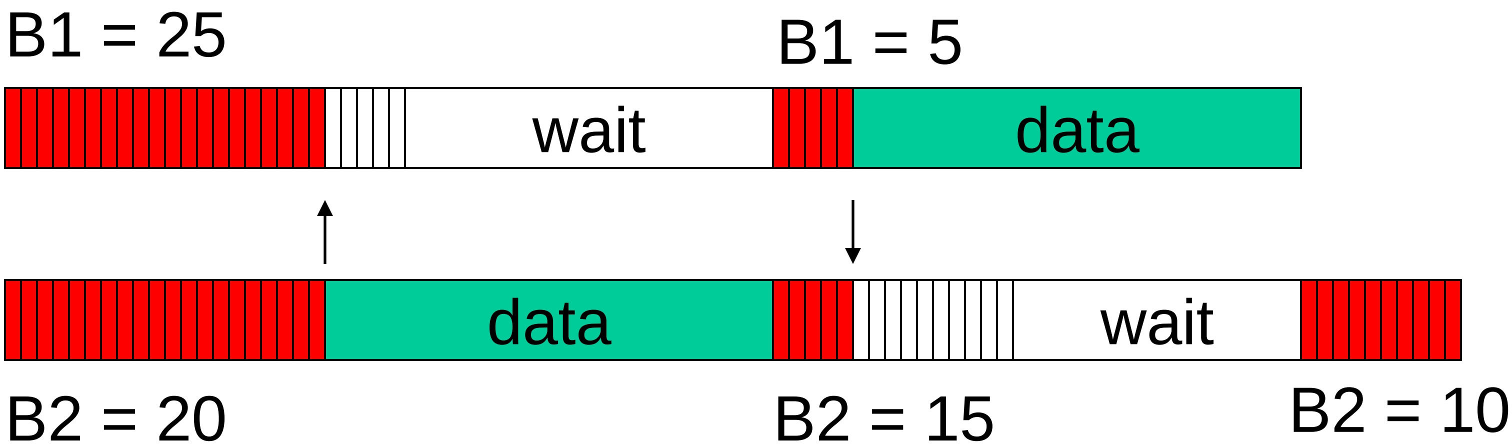
Mac Protocol Data Unit (MPDU)



802.11 - Collision Avoidance

- If medium is not free during DIFS time..
- Go into Collision Avoidance: Once channel becomes idle, wait for DIFS time plus a randomly chosen backoff time before attempting to transmit
- For DCF the backoff is chosen as follows:
  - When first transmitting a packet, choose a backoff interval in the range [0,cw]; cw is contention window, nominally 31
  - Count down the backoff interval when medium is idle
  - Count-down is suspended if medium becomes busy
  - When backoff interval reaches 0, transmit RTS
  - If collision, then double the cw up to a maximum of 1024
- Time spent counting down backoff intervals is part of MAC overhead

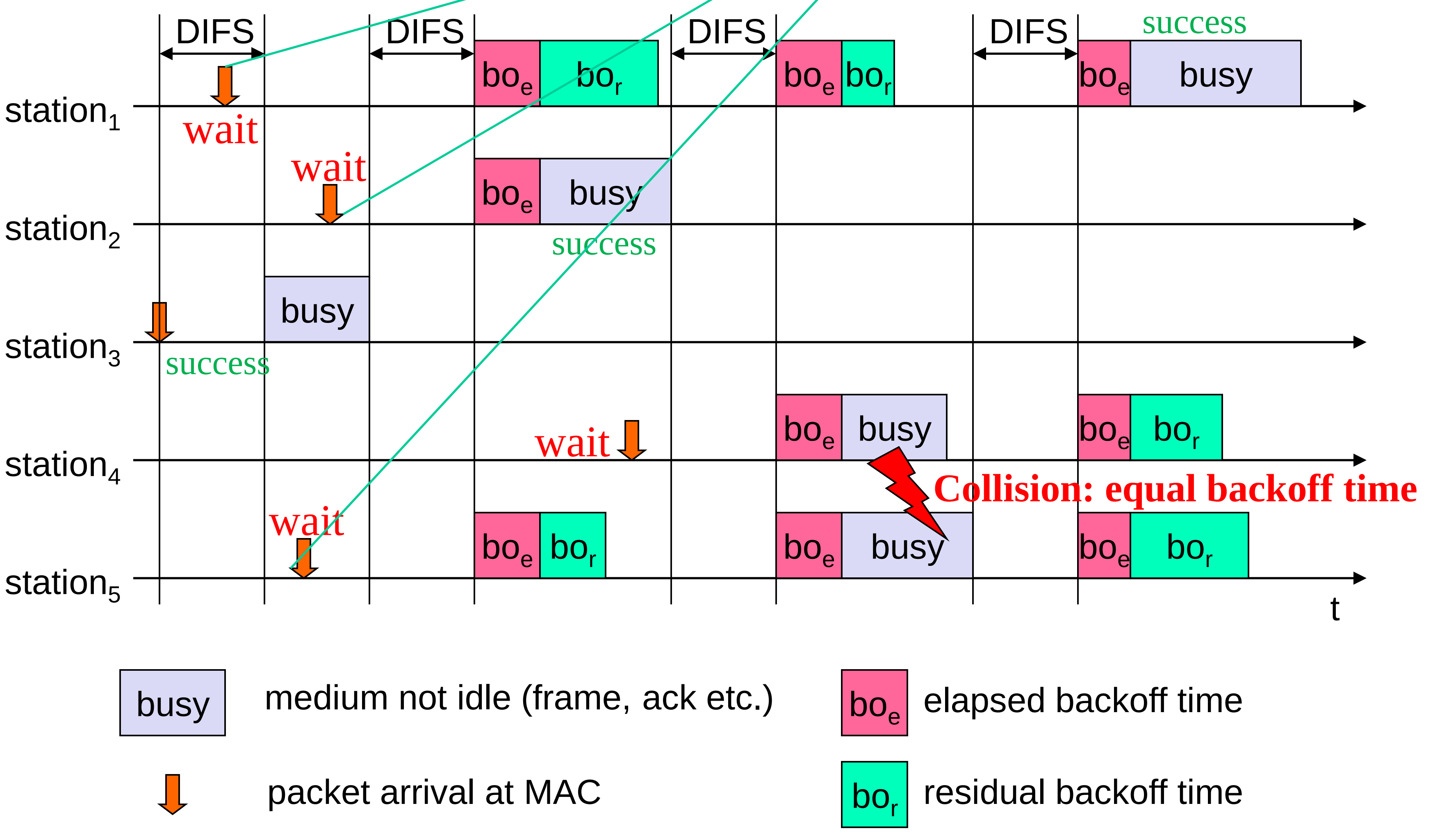
Example - backoff



cw = 31

B1 and B2 are backoff intervals at nodes 1 and 2

If medium is not free during DIFS time.. Go into Collision Avoidance: Once channel becomes idle, wait for DIFS time plus a randomly chosen backoff time before attempting to transmit



Backoff - more complex example

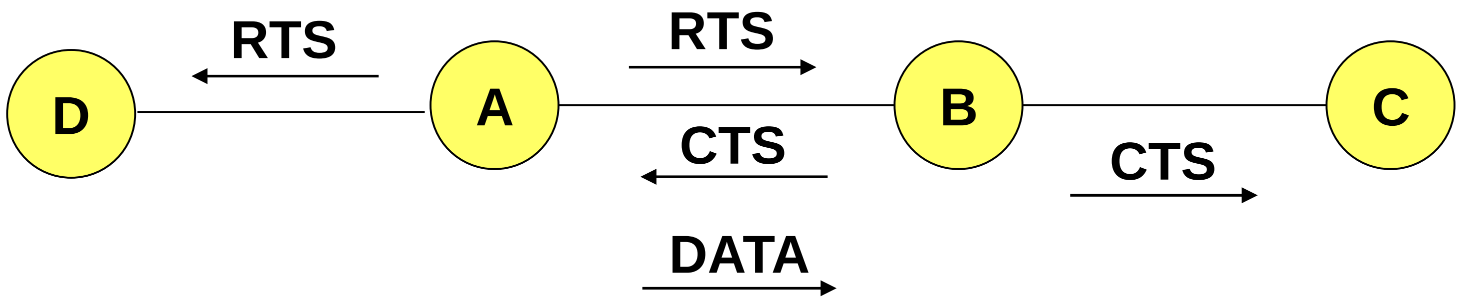
Source: Schiller

802.11 - Priorities

- defined through different inter frame spaces – mandatory idle time intervals between the transmission of frames
- SIFS (Short Inter Frame Spacing)
  - highest priority, for ACK, CTS, polling response
  - SIFSTime and SlotTime are fixed per PHY layer (10 μs and 20 μs respectively in DSSS)
- PIFS (PCF IFS)
  - medium priority, for time-bounded service using PCF
  - PIFSTime = SIFSTime + SlotTime
- DIFS (DCF IFS)
  - lowest priority, for asynchronous data service
  - DCF-IFS: DIFSTime = SIFSTime + 2xSlotTime

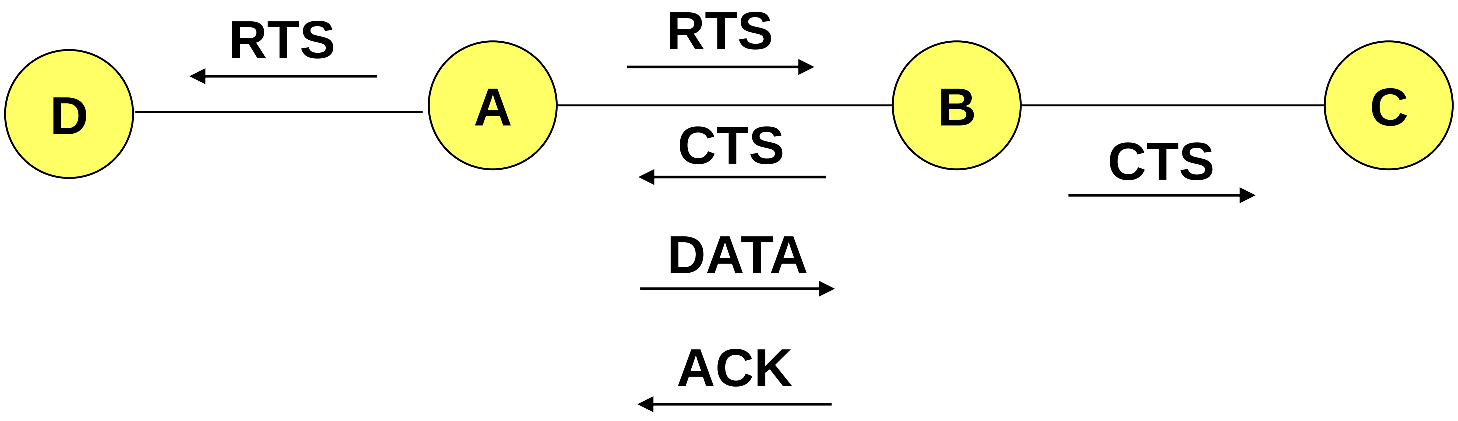
Solution to Hidden/Exposed Terminals

- A first sends a *Request-to-Send (RTS)* to B
- On receiving RTS, B responds *Clear-to-Send (CTS)*
- Hidden node C overhears CTS and keeps quiet
  – Transfer duration is included in both RTS and CTS
- Exposed node overhears a RTS but not the CTS
  – D's transmission cannot interfere at B



802.11 - Reliability

- Use acknowledgements
  - When B receives DATA from A, B sends an ACK
  - If A fails to receive an ACK, A retransmits the DATA
  - Both C and D remain quiet until ACK (to prevent collision of ACK)
  - Expected duration of transmission+ACK is included in RTS/CTS packets

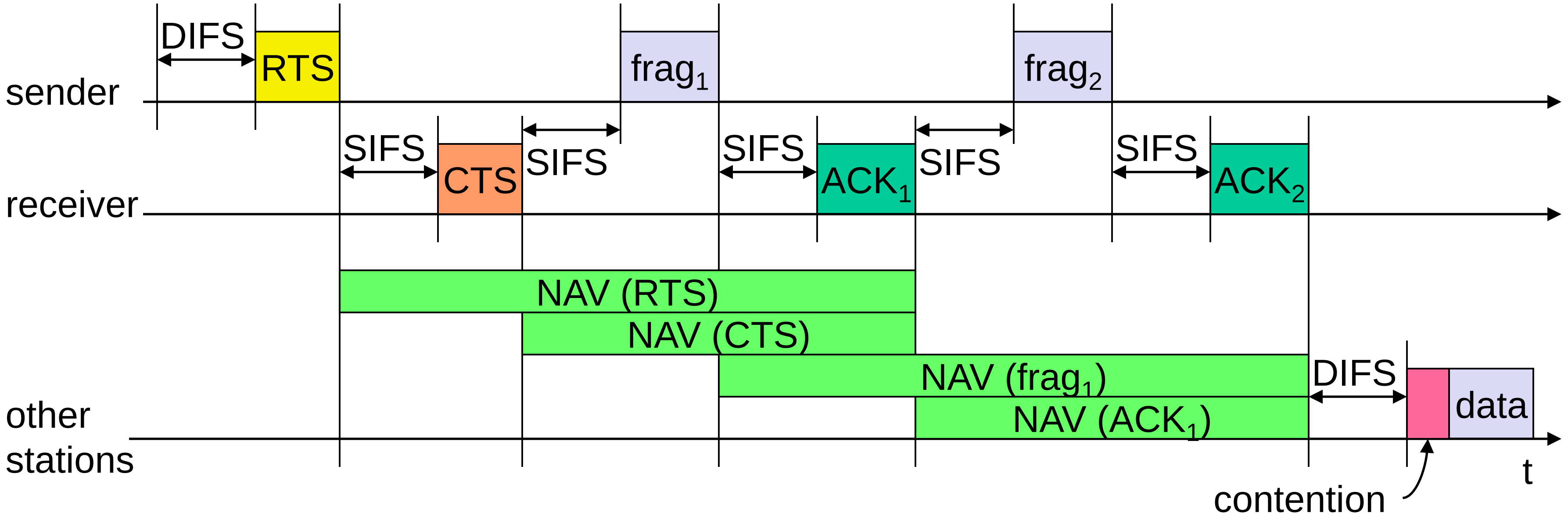


802.11 - Congestion Control

- Contention window (cw) in DCF: Congestion control achieved by dynamically choosing cw
- *large* cw leads to larger backoff intervals
- *small* cw leads to larger number of collisions

- Binary Exponential Backoff in DCF:
  - When a node fails to receive CTS in response to its RTS, it increases the contention window
    - cw is doubled (up to a bound cwmax =1023)
  - Upon successful completion data transfer, restore cw to cwmin=31

Fragmentation



802.11 - MAC management

- Synchronization
  - try to find a LAN, try to stay within a LAN
  - timer etc.
- Power management
  - sleep-mode without missing a message
  - periodic sleep, frame buffering, traffic measurements
- Association/Reassociation
  - integration into a LAN
  - roaming, i.e. change networks by changing access points
  - scanning, i.e. active search for a network
- MIB - Management Information Base
  - managing, read, write

802.11 - Power management

- Idea: switch the transceiver off if not needed
- States of a station: sleep and awake
- Timing Synchronization Function (TSF)
  - stations wake up at the same time
- Infrastructure
  - Traffic Indication Map (TIM)
    - list of unicast receivers transmitted by AP
  - Delivery Traffic Indication Map (DTIM)
    - list of broadcast/multicast receivers transmitted by AP
- Ad-hoc
  - Ad-hoc Traffic Indication Map (ATIM)
    - announcement of receivers by stations buffering frames
    - more complicated - no central AP
    - collision of ATIMs possible (scalability?)

802.11 - Energy Conservation

- Power Saving in infrastructure mode
  - Nodes can go into sleep or standby mode
  - An Access Point periodically transmits a beacon indicating which nodes have packets waiting for them
  - Each power saving (PS) node wakes up periodically to receive the beacon
  - If a node has a packet waiting, then it sends a PS-Poll
    - After waiting for a backoff interval in [0,CWmin]
  - Access Point sends the data in response to PS-poll

802.11 - Frame format

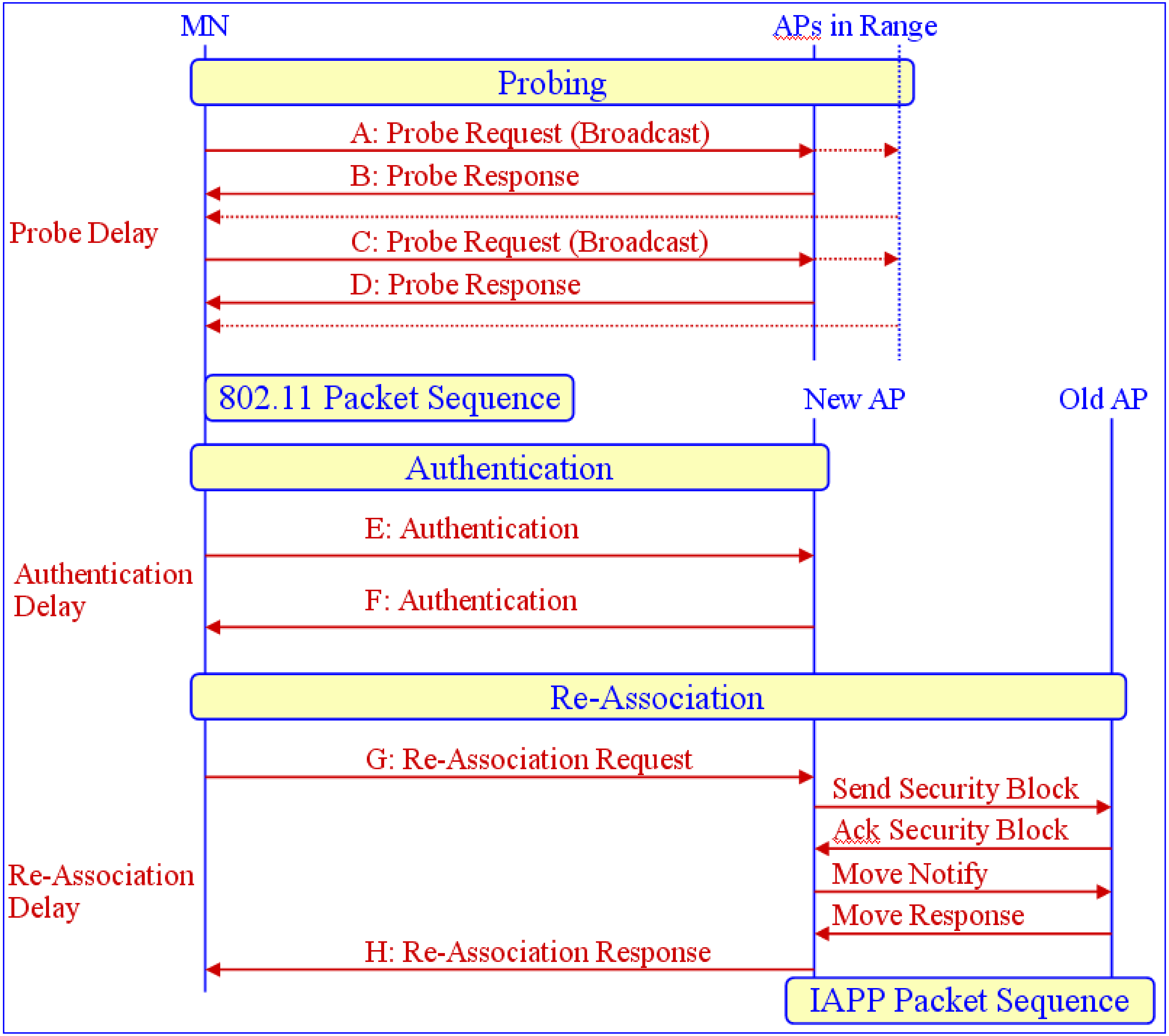
- Types
  – control frames, management frames, data frames
- Sequence numbers
  – important against duplicated frames due to lost ACKs
- Addresses
  – receiver, transmitter (physical), BSS identifier, sender (logical)
- Miscellaneous
  – sending time, checksum, frame control, data

bytes	2	2	6	6	6	2	6	0-2312	4
	Frame Control	Duration ID	Address 1	Address 2	Address 3	Sequence Control	Address 4	Data	CRC

version, type, fragmentation, security, ...

Types of Frames

- Control Frames
  - RTS/CTS/ACK
  - CF-Poll/CF-End
- Management Frames
  - Beacons
  - Probe Request/Response
  - Association Request/Response
  - Dissociation/Reassociation
  - Authentication/Deauthentication
  - ATIM
- Data Frames


MN
APs in Range
Probing
A: Probe Request (Broadcast)
B: Probe Response
Probe Delay
C: Probe Request (Broadcast)
D: Probe Response
802.11 Packet Sequence
New AP
Old AP
Authentication
E: Authentication
Authentication Delay
F: Authentication
Re-Association
G: Re-Association Request
Send Security Block
Ack Security Block
Re-Association Delay
Move Notify
Move Response
H: Re-Association Response
IAPP Packet Sequence

802.11 - Roaming

- Bad connection in Infrastructure mode? Perform:
- scanning of environment
  - listen into the medium for beacon signals or send probes into the medium and wait for an answer
- send Reassociation Request
  - station sends a request to a new AP(s)
- receive Reassociation Response
  - success: AP has answered, station can now participate
  - failure: continue scanning
- AP accepts Reassociation Request and
  - signals the new station to the distribution system
  - the distribution system updates its data base (i.e., location information)
  - typically, the distribution system now informs the old AP so it can release resources

802.11-based Wireless LANs
Point Coordination Function (PCF)

802.11 - Point Coordination Function

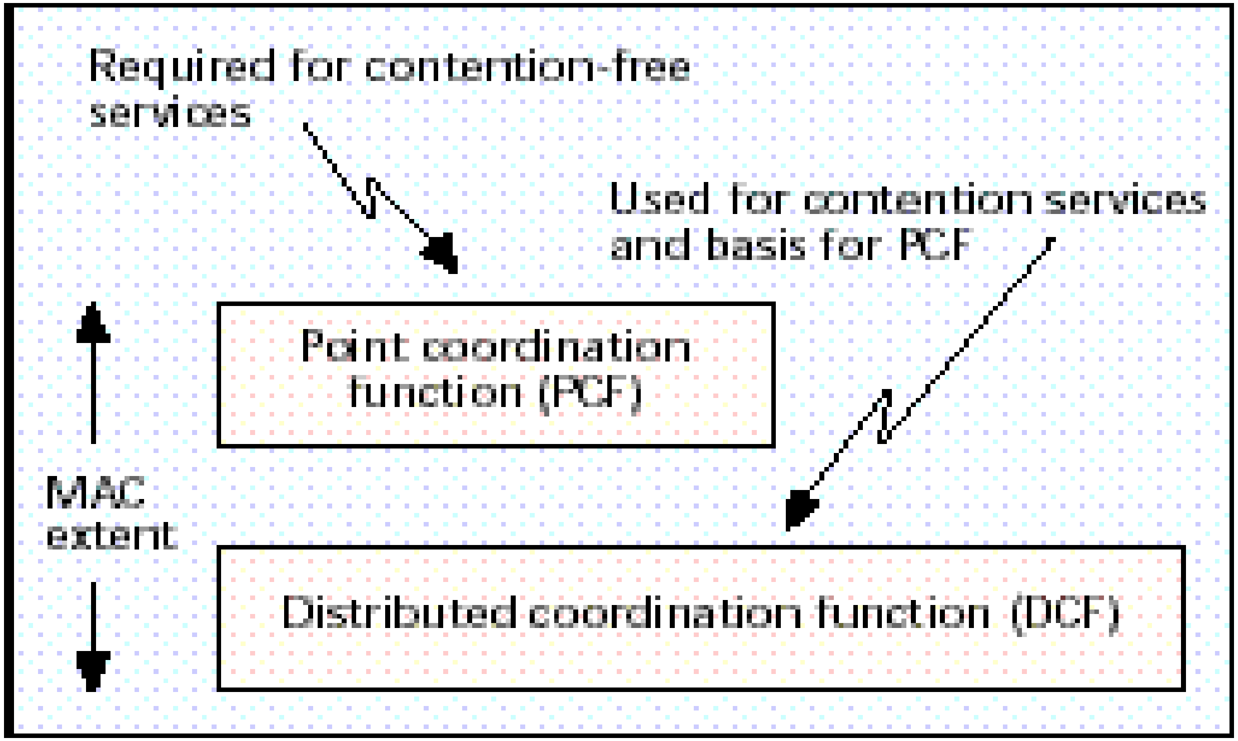
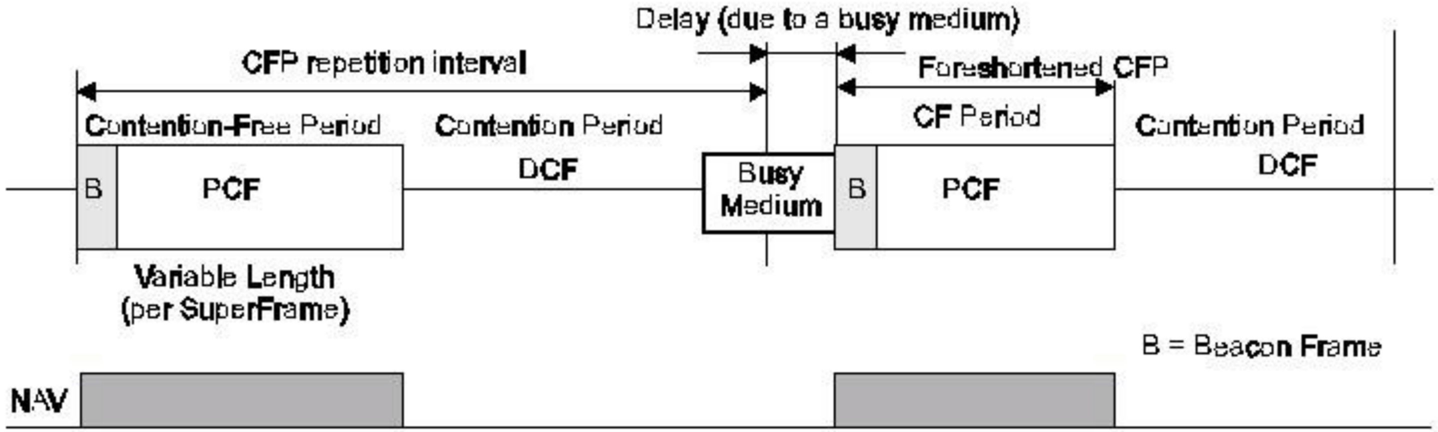


Figure 4. *MAC architecture.*

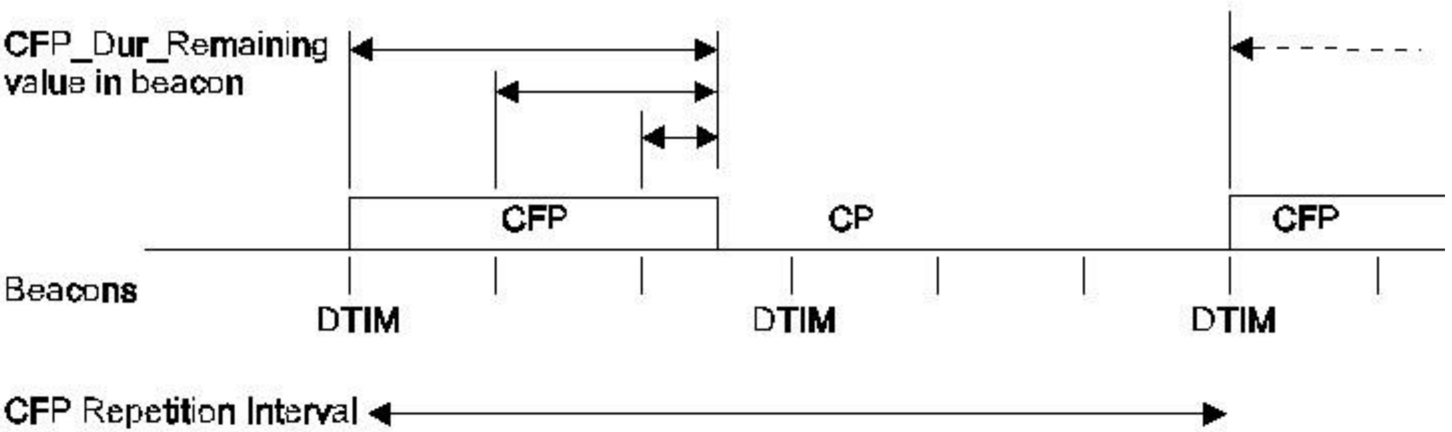
Coexistence of PCF and DCF

- A Point Coordinator (PC) resides in the Access Point and controls frame transfers during a Contention Free Period (CFP)
- A CF-Poll frame is used by the PC to invite a station to send data. Stations are polled from a list maintained by the PC
- The CFP alternates with a Contention Period (CP) in which data transfers happen as per the rules of DCF
- This CP must be large enough to send at least one maximum-sized packet including RTS/CTS/ACK
- CFPs are generated at the CFP repetition rate
- The PC sends Beacons at regular intervals and at the start of each CFP
- The CF-End frame signals the end of the CFP

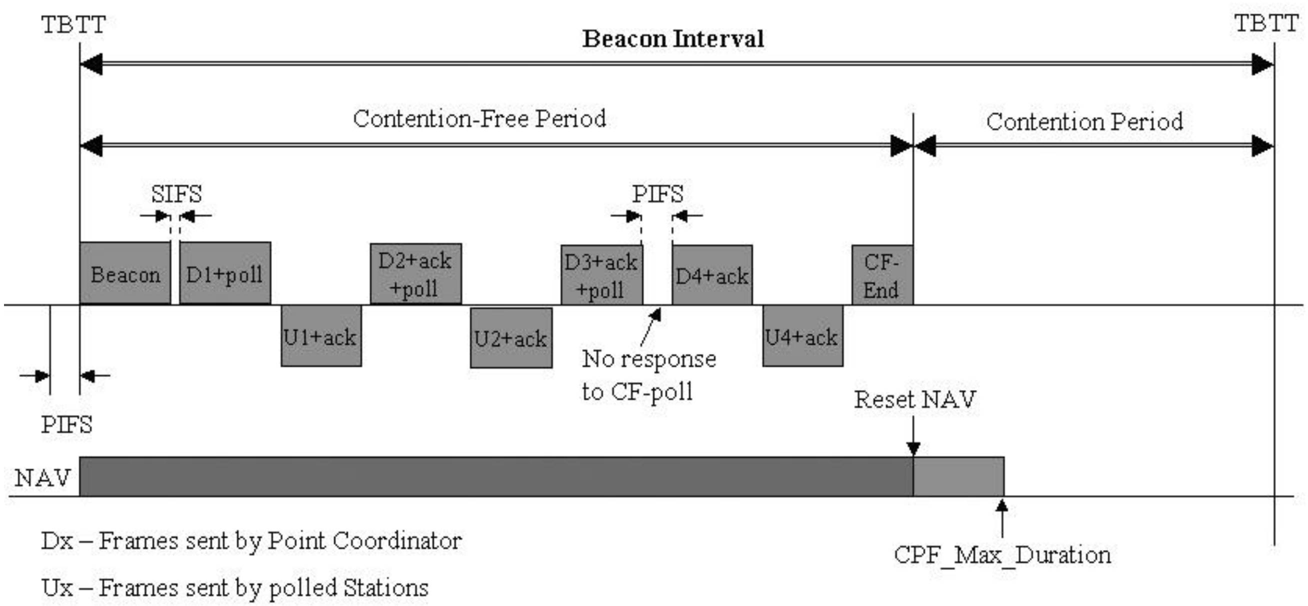
CFP structure and Timing



CFP/CP Alternation and Beacon Periods



Point Coordination Function



Time slot is divided in to two parts:

- CFP
- CP

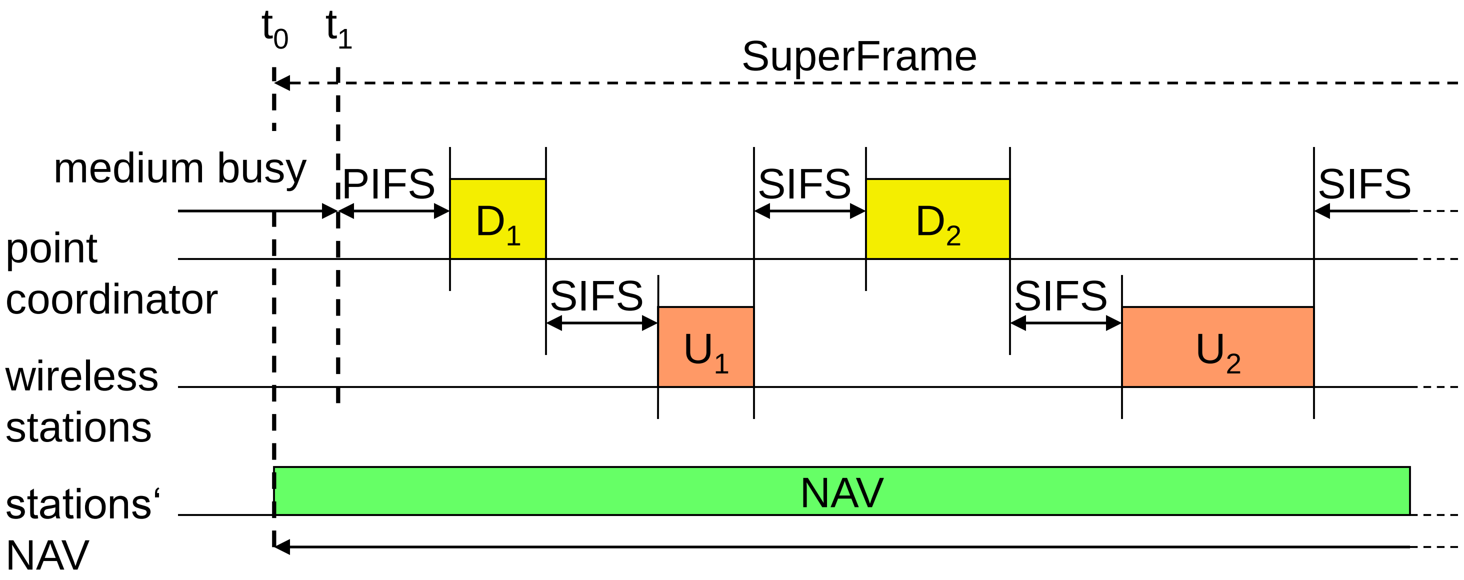
- In Contention free Period the AP polls the registered stations

- PC waits for PIFS.
- Sends a Beacon Frame to start the polling sequence

- All other STAs set their NAVs to the value of CPF_Max_Duration
- After SIFS, PC Sends Data + Polled STA

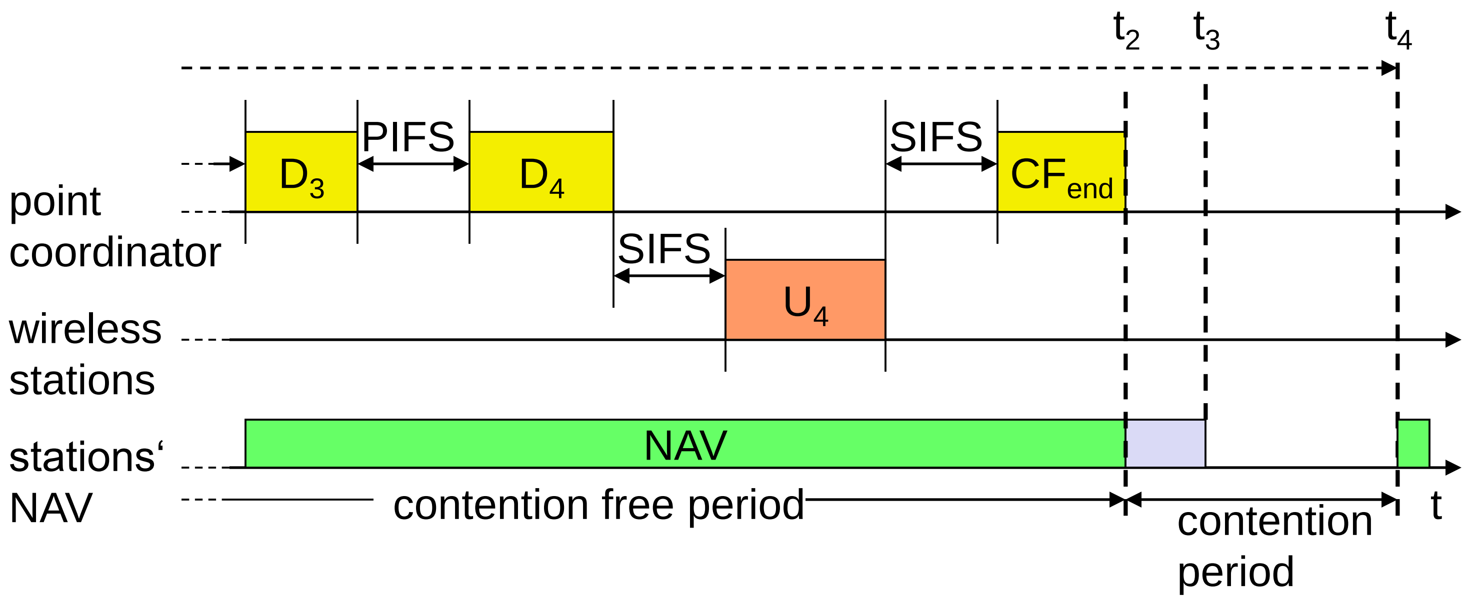
- STA1,Sends the Data + Ack
- PC Data + Polled STA + Ack

802.11 - PCF I



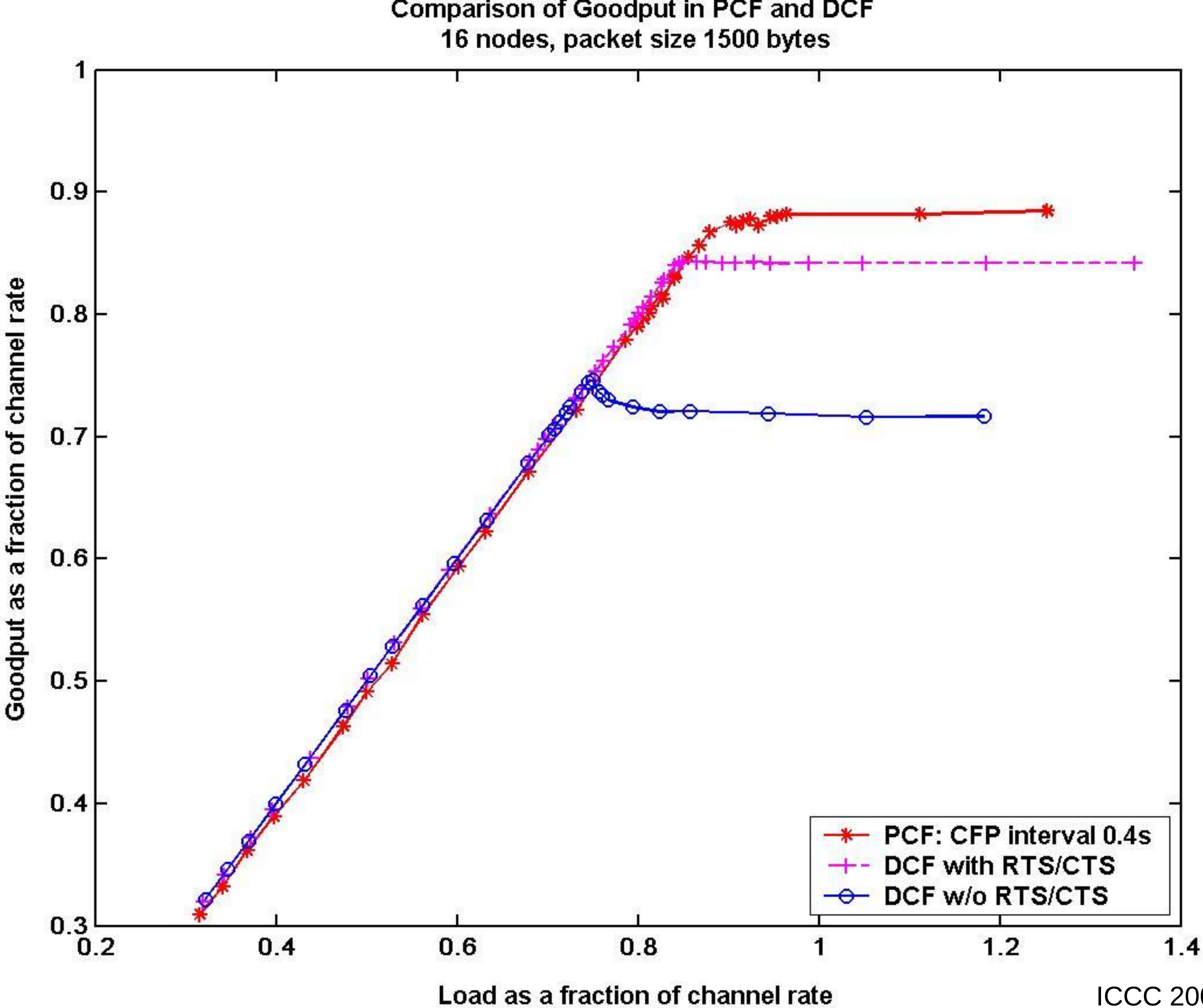
Source: Schiller

802.11 - PCF II


t2
t3
t4
PIFS
SIFS
SIFS
D3
D4
CFend
U4
point coordinator
wireless stations
stations' NAV
NAV
contention free period
contention period
t

Throughput – DCF vs. PCF

- Overheads to throughput and delay in DCF mode come from losses due to collisions and backoff
- These increase when number of nodes in the network increases
- RTS/CTS frames cost bandwidth but large data packets (>RTS threshold) suffer fewer collisions
- RTC/CTS threshold must depend on number of nodes
- Overhead in PCF modes comes from wasted polls
- Polling mechanisms have large influence on throughput
- Throughput in PCF mode shows up to 20% variation with other configuration parameters – CFP repetition rate
- Saturation throughput of DCF less than PCF in all studies presented here (‘heavy load’ conditions)



Comparison of Goodput in PCF and DCF
16 nodes, packet size 1500 bytes
Goodput as a fraction of channel rate
Load as a fraction of channel rate
0.3
0.4
0.5
0.6
0.7
0.8
0.9
1
0.2
0.4
0.6
0.8
1
1.2
1.4
PCF: CFP interval 0.4s
DCF with RTS/CTS
DCF w/o RTS/CTS

ICCC 2002

IEEE 802.11 Summary

- Infrastructure and ad hoc modes using DCF
- Carrier Sense Multiple Access
- Binary exponential backoff for collision avoidance and congestion control
- Acknowledgements for reliability
- Power save mode for energy conservation
- Time-bound service using PCF
- Signaling packets for avoiding Exposed/Hidden terminal problems, and for reservation
  - Medium is reserved for the duration of the transmission
  - RTS-CTS in DCF
  - Polls in PCF

802.11 DCF Implementation in ns-2, propagation model

- **Radio Propagation Model**
  - Friss-space attenuation($1/d^2$) at near distance

$$P_r(d) = \frac{P_t G_t G_r \lambda^2}{(4\pi)^2 d^2 L}$$

  - Two-ray Ground ($1/d^4$) at far distance

$$P_r(d) = \frac{P_t G_t G_r h_t^2 h_r^2}{d^4 L}$$

  - Cross-distance

$$d_c = \frac{(4\pi h_t h_r)}{\lambda}$$

- **Antenna (Omni-directional, unity-gain)**
  - $G_t = G_r = 1.0$
  - Transmission range : 250m
  - Carrier sense range : 550m
- **Determine Collision**

$$SIR = \frac{P_s}{P_i} = \left(\frac{d_i}{d_s}\right)^{\alpha} \geq CPThresh$$

•MAC 802.11 DCF

```
# IEEE 802.11 MAC settings
if [TclObject is-class Mac/802_11] {
        Mac/802_11 set delay_ 64us
        Mac/802_11 set ifs_ 16us
        Mac/802_11 set slotTime_ 16us
        Mac/802_11 set cwmin_ 16
        Mac/802_11 set cwmax_ 1024
        Mac/802_11 set rtxLimit_ 16
        Mac/802_11 set bssId_ -1
        Mac/802_11 set sifs_ 8us
        Mac/802_11 set pifs_ 12us
        Mac/802_11 set difs_ 16us
        Mac/802_11 set rtxAckLimit_ 1
        Mac/802_11 set rtxRtsLimit_ 3
        Mac/802_11 set basicRate_ 1Mb
        Mac/802_11 set dataRate_ 1Mb
}
```

•Network Interface

```
# Initialize the SharedMedia interface with parameters to make
# it work like the 914MHz Lucent WaveLAN DSSS radio interface
Phy/WirelessPhy set CPThresh_ 10.0
Phy/WirelessPhy set CSThresh_ 1.559e-11
Phy/WirelessPhy set RXThresh_ 3.652e-10
Phy/WirelessPhy set bandwidth_ 2e6
Phy/WirelessPhy set Pt_ 0.28183815
Phy/WirelessPhy set freq_ 914e+6
Phy/WirelessPhy set L_ 1.0
Phy/WirelessPhy set debug_ false
```

Source: "The ns-2 Manual and Source Codes," http://www.isi.edu/nsnam/ns/.

802.11 current status