1

802.15.4 and Zigbee

What is ZigBee?

- Technological Standard Created for Control and Sensor Networks
  - Based on the IEEE 802.15.4 Standard
  - Centered in small radios
- Created by the ZigBee Alliance
  - 200+ members
- History
  - *May 2003: IEEE 802.15.4 completed*
  - December 2004: ZigBee specification ratified
  - June 2005: public availability

What Does ZigBee Do?

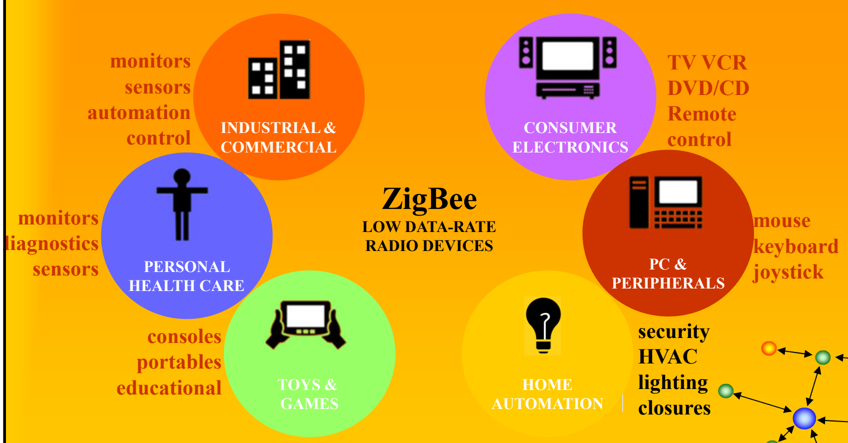
- **Designed for wireless controls and sensors**
  - Operates in Personal Area Networks (PAN's) and device-to-device networks
  - Connectivity between small packet devices
  - Examples: control of lights, switches, thermostats, appliances, etc.

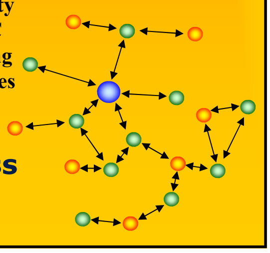
Zigbee?

- Named for erratic, zig-zagging patterns of bees between flowers
- Symbolizes communication between nodes in a mesh network
- Network components "seen as analogous" to queen bee, drones, worker bees

4

ZigBee network applications





- **Just everything you can imagine for wireless sensor nodes or in general short range communications**

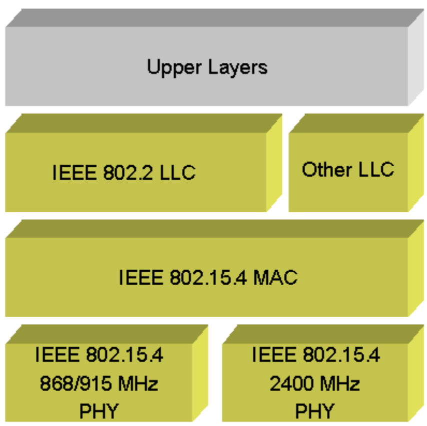
ZigBee and Other Wireless Technologies @early start

Market Name Standard	ZigBee™ 802.15.4	--- GSM/GPRS CDMA/1xRTT	Wi-Fi™ 802.11b	Bluetooth™ 802.15.1
Application Focus	Monitoring & Control	Wide Area Voice & Data	Web, Email, Video	Cable Replacement
System Resources	4KB - 32KB	16MB+	1MB+	250KB+
Battery Life (days)	100 - 1,000+	1-7	.5 - 5	1 - 7
Network Size	Unlimited (2^{64})	1	32	7
Bandwidth (KB/s)	20 - 250	64 - 128+	11,000+	720
Transmission Range (meters)	1 - 100+	1,000+	1 - 100	1 - 10+
Success Metrics	Reliability, Power, Cost	Reach, Quality	Speed, Flexibility	Cost, Convenience

Source: http://www.zigbee.org/en/about/faq.asp

IEEE 802.15.4 - Overview

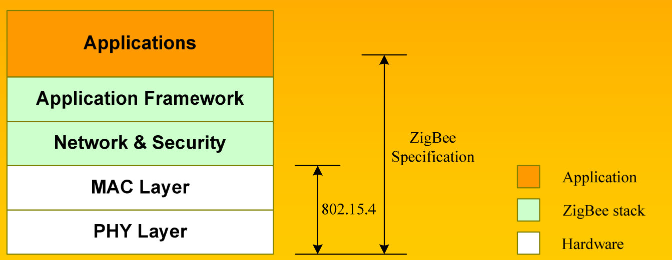
- Low Rate WPAN (LR-WPAN)
  - E.g. Sensor networks
- Simple and low cost
  - Fully handshake protocol
- Low power consumption
  - Years on lifetime using standard batteries
- Different topologies
  - Star, peer-to-peer, combined
- Data rates: 20-250 kbps
  - Low latency support
- Operates at different frequencies
  - 868 Mhz, 915 Mhz, 2.4 GHz



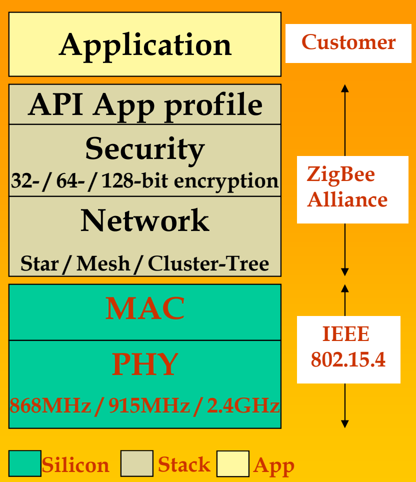
7

ZigBee/802.15.4 architecture

- **ZigBee Alliance**
  - 45+ companies: semiconductor mfrs, IP providers, OEMs, etc.
  - Defining upper layers of protocol stack: from network to application, including application profiles
  - First profiles published mid 2003
- **IEEE 802.15.4 Working Group**
  - Defining lower layers of protocol stack: MAC and PHY



IEEE 802.15.4 & ZigBee In Context



ZigBee Alliance

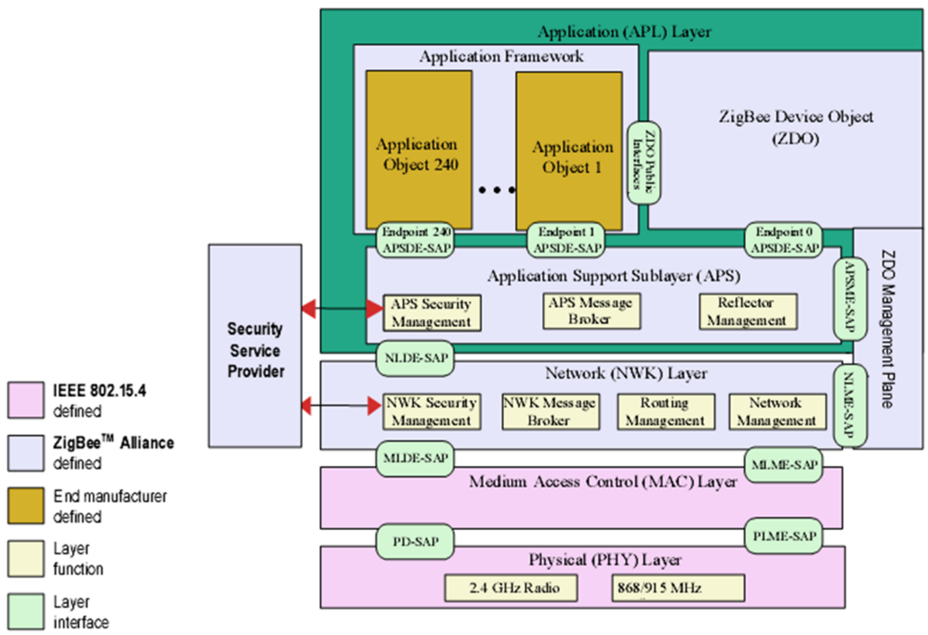
- "the software"
- Network, Security & Application layers
- Brand management

IEEE 802.15.4

- "the hardware"
- Physical & Media Access Control layers

Source: http://www.zigbee.org/resources/documents/IWAS_presentation_Mar04_Designing_with_802154_and_zigbee.ppt

Protocol Stack



How ZigBee Works

- **Topology**
  - **Star**
  - **Cluster Tree**
  - **Mesh**
- **Network coordinator, routers, end devices**
- **2 or more devices form a PAN/WSN**

How ZigBee Works

- States of operation
  - Active
  - Sleep
- Devices
  - Full Function Devices (FFD's)
  - Reduced Function Devices (RFD's)
- Modes of operation
  - Beacon
  - Non-beacon
- Traffic types
  - Intermittent
  - Repetitive
  - Periodic

ZigBee Node-Types

ZigBee Coordinator (ZBC) (IEEE 802.15.4 FFD)

- only one in a network
- initiates network
- stores information about the network
- all devices communicate with the ZBC
- routing functionality
- bridge to other networks

ZigBee Router (ZBR) (IEEE 802.15.4 FFD)

- optional component
- routes between nodes, network backbone
- extends network coverage
- manages local address allocation/de-allocation

ZigBee End Device (ZBE) (IEEE 802.15.4 RFD)

- optimized for low power consumption
- cheapest device type
  - sensor would be deployed here

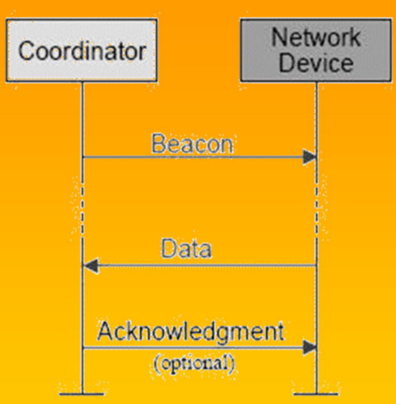
IEEE 802.15.4: Traffic-Types

- **Data is periodic**
  - application dictates rate (e.g. sensors)
- **Data is intermittent**
  - application or stimulus dictates rate (optimum power savings), e.g. light switch
- **Data is repetitive (fixed rate a priori)**
  - device gets guaranteed time slot (e.g. heart monitor)

IEEE 802.15.4: Traffic-Modes

Beacon mode:

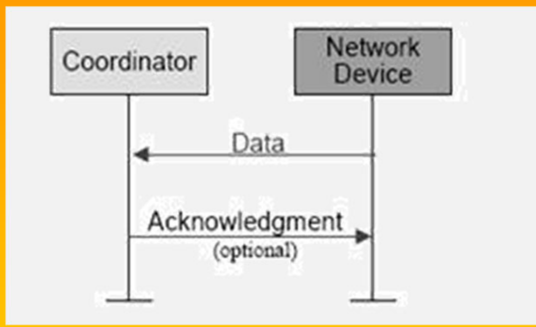
- beacon sent periodically
- Coordinator and end device can go to power save
- Lowest energy consumption
- Precise timing needed
- Beacon period (ms-m)



IEEE 802.15.4: Traffic-Modes

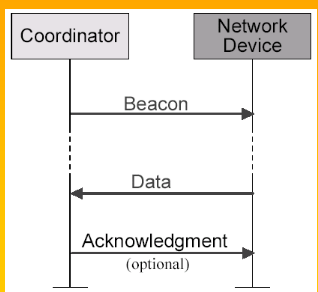
Non-Beacon mode:

- **coordinator/routers have to stay awake (robust power supply needed)**
- **heterogeneous network**
- **asymmetric power**

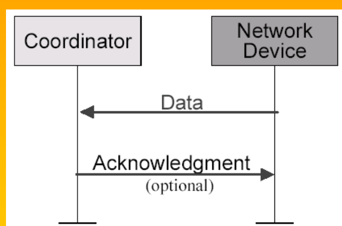


Data transfer model (device to coordinator)

- **Data transferred from device to coordinator**
  - **In a beacon-enable network, device finds the beacon to synchronize to the superframe structure. Then using slotted CSMA/CA to transmit its data.**
  - **In a non beacon-enable network, device simply transmits its data using unslotted CSMA/CA**



Communication to a coordinator
In a beacon-enabled network



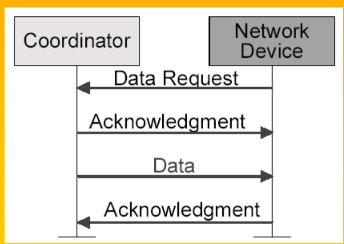
Communication to a coordinator
In a non beacon-enabled network

16

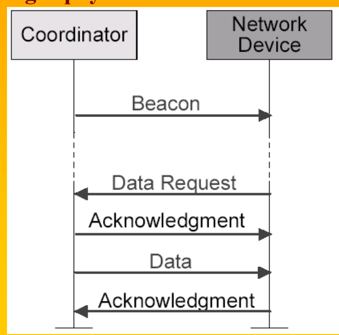
17

Data transfer model (coordinator to device)

- **Data transferred from coordinator to device**
  - **In a beacon-enable network, the coordinator indicates in the beacon that the data is pending. Device periodically listens to the beacon and transmits a MAC command request using slotted CSMA/CA if necessary.**
  - **In a non-beacon-enable network, a device transmits a MAC command request using unslotted CSMA/CA. If the coordinator has its pending data, the coordinator transmits data frame using unslotted CSMA/CA. Otherwise, coordinator transmits a data frame with zero length payload.**

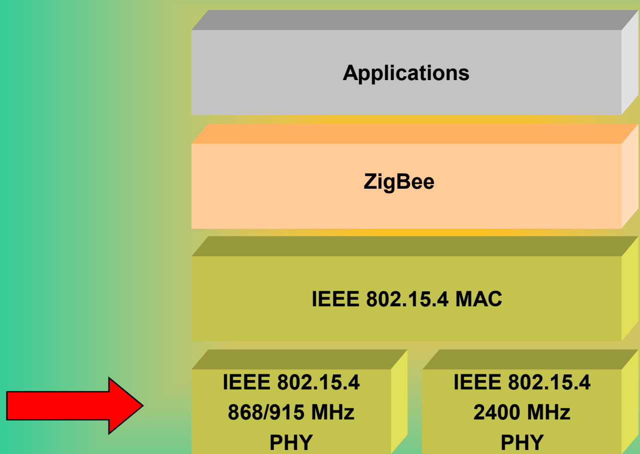


Communication from a coordinator in a non beacon-enabled network



Communication from a coordinator In a beacon-enabled network

802.15.4 / ZigBee Architecture



- Packet generation
- Packet reception
- Data transparency
- Power Management

19

IEEE 802.15.4 basics

- 802.15.4 is a simple packet data protocol for lightweight wireless networks
  - Channel Access is via Carrier Sense Multiple Access with collision avoidance and optional time slotting
  - Message acknowledgement and an optional beacon structure
  - Multi-level security
  - Works well for
    - Long battery life, selectable latency for controllers, sensors, remote monitoring and portable electronics
  - Configured for maximum battery life, has the potential to last as long as the shelf life of most batteries

20

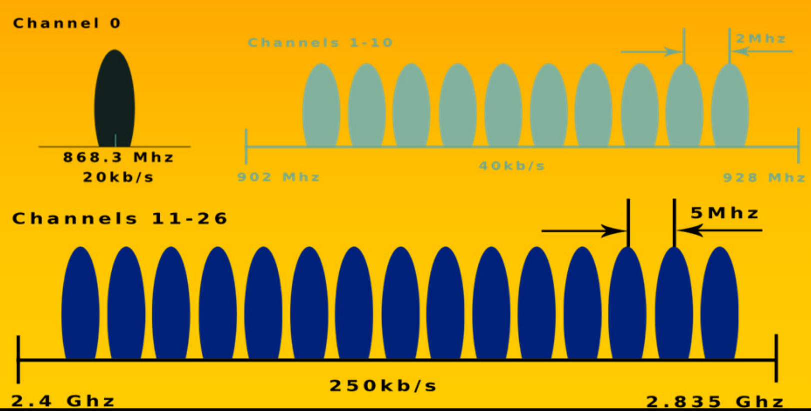
802.15.4 General characteristics

- Data rates of 250 kbps , 20 kbps and 40kpbs.
- Star or Peer-to-Peer operation.
- Support for low latency devices.
- CSMA-CA channel access, with CCA detection
- Dynamic device addressing.
- Fully handshaked protocol for transfer reliability.
- Low power consumption.
- 16 channels in the 2.4GHz ISM band, 10 channels in the 915MHz ISM band and one channel in the European 868MHz band.
- Extremely low duty-cycle (<0.1%)

802.15.4 frequency bands

Operates in Unlicensed Bands

- ISM 2.4 GHz Global Band at 250kbps
- 868 MHz European Band at 20kbps
- 915 MHz North American Band at 40kbps



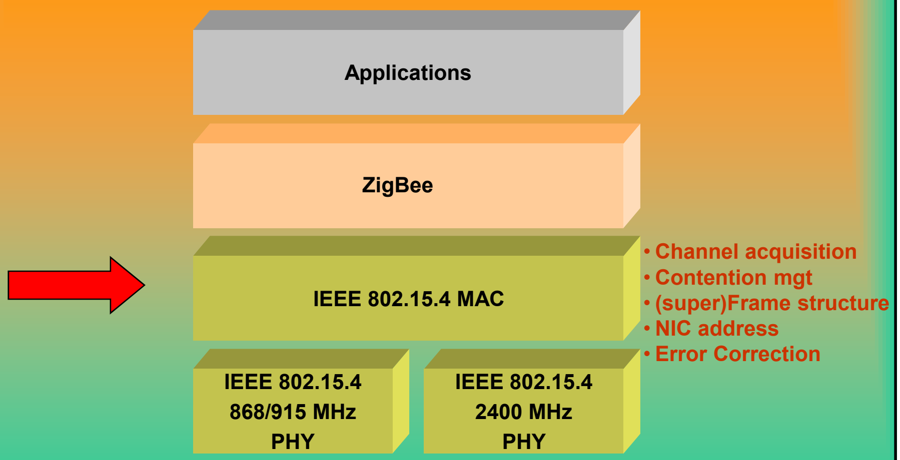
22

PHY frame structure

- **PHY packet fields**
  - Preamble (32 bits) – synchronization
  - Start of packet delimiter (8 bits) – shall be formatted as “11100101”
  - PHY header (8 bits) –PSDU length
  - PSDU (0 to 127 bytes) – data field

Sync Header		PHY Header		PHY Payload
Preamble	Start of Packet Delimiter	Frame Length (7 bit)	Reserve (1 bit)	PHY Service Data Unit (PSDU)
4 Octets	1 Octets	1 Octets		0-127 Bytes

802.15.4 Architecture (MAC)

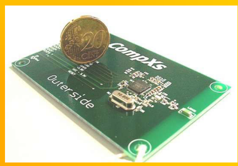


IEEE 802.15.4 MAC Design Drivers

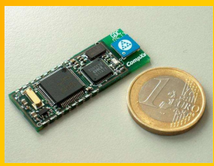
- Extremely low cost
- Ease of implementation
- Reliable data transfer
- Short range operation
- Very low power consumption

Simple but flexible protocol

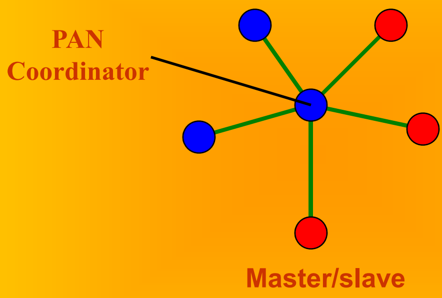
IEEE 802.15.4 MAC Overview
Device Classes



- **Full function device (FFD)**
  - **Any topology**
  - **Network coordinator capable**
  - **Talks to any other device**
  - **The FFD can operate in three modes serving**
    - Device
    - Coordinator
    - PAN coordinator
- **Reduced function device (RFD)**
  - **Limited to star topology**
  - **Talks only to a network coordinator**
    - Cannot become a network coordinator
  - **Very simple implementation**



IEEE 802.15.4 MAC Overview
Star Topology



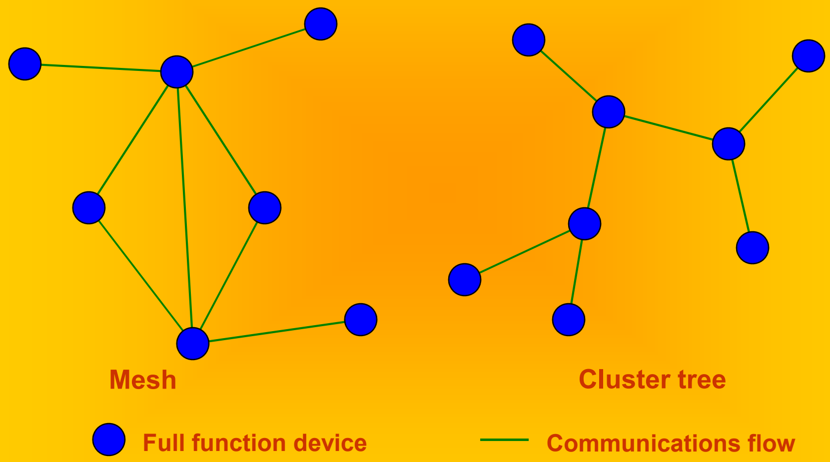
Full function device

Reduced function device

Communications flow

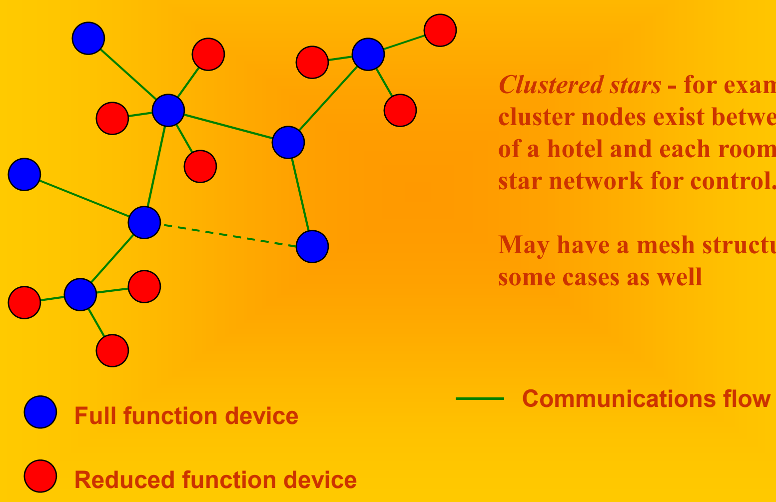
IEEE 802.15.4 MAC Overview

Mesh (Peer-Peer) and cluster tree topologies



IEEE 802.15.4 MAC Overview

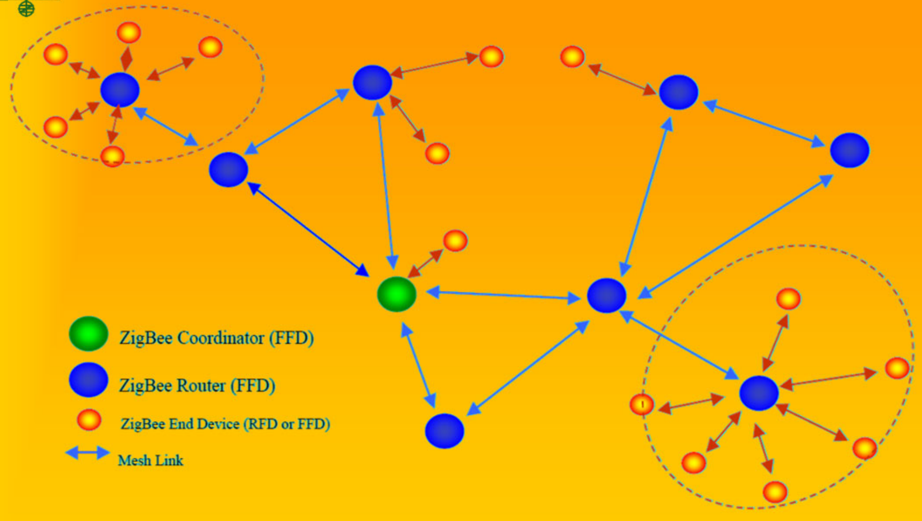
Combined Topology



Clustered stars - for example, cluster nodes exist between rooms of a hotel and each room has a star network for control.

May have a mesh structure in some cases as well

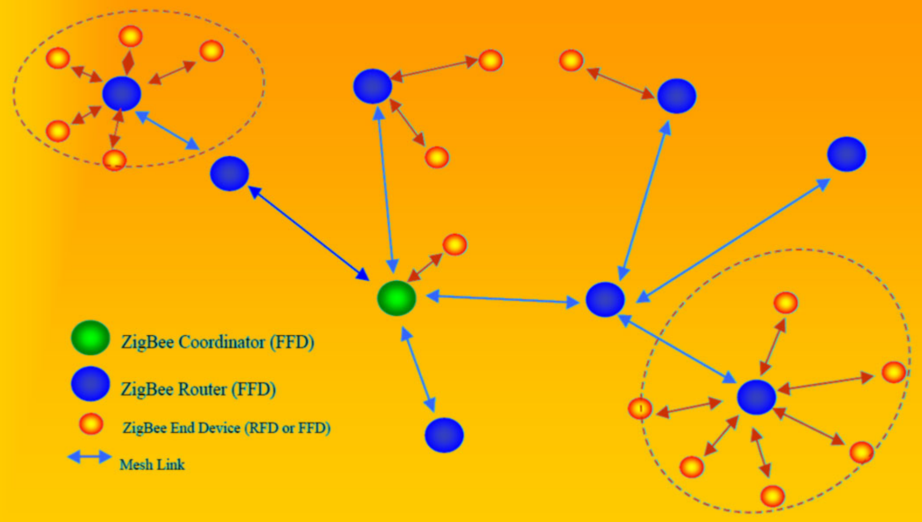
Combined topologies: Mesh Topologies



In a mesh network, regular beacons are not allowed.

Devices in a mesh network can only communicate with each other by peer-to-peer transmissions

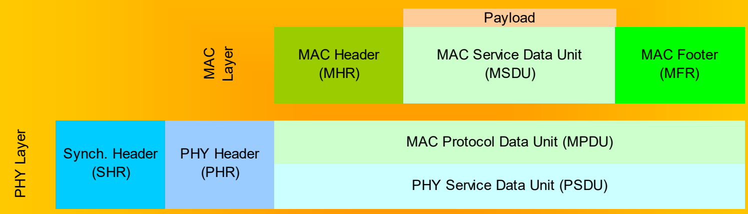
Combined Topologies: Tree



In a tree network, the coordinator and routers can announce beacons.

IEEE 802.15.4 MAC Overview

General Frame Structure



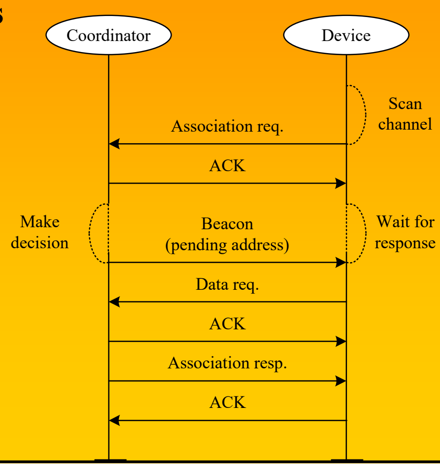
4 Types of MAC Frames:

- Data Frame
- Beacon Frame
- Acknowledgment Frame
- MAC Command Frame

32

Association procedures

- A device becomes a member of a WSN by associating with its coordinator
- Procedures



33

Association procedures

- In IEEE 802.15.4, association results are announced in an indirect fashion
- A coordinator responds to association requests by appending devices' long addresses in beacon frames
- Devices need to send a data request to the coordinator to acquire the association result
- After associating to a coordinator, a device will be assigned a 16-bit *short address*.

MAC layer

Managing PANs
- Channel scanning (ED, active, passive, orphan)
- PAN ID conflict detection and resolution
- Starting a PAN
- Sending beacons
- Device discovery, association/disassociation
- Synchronization (beacon/nonbeacon)
- Orphaned device realignment

Transfer handling
- Transaction based (indirect transmission)
  - Beacon indication
  - Polling
- Transmission, Reception, Rejection, Retransmission
  - Acknowledged / Not acknowledged
- GTS management
  - Allocation/deallocation/Reallocation
  - Usage

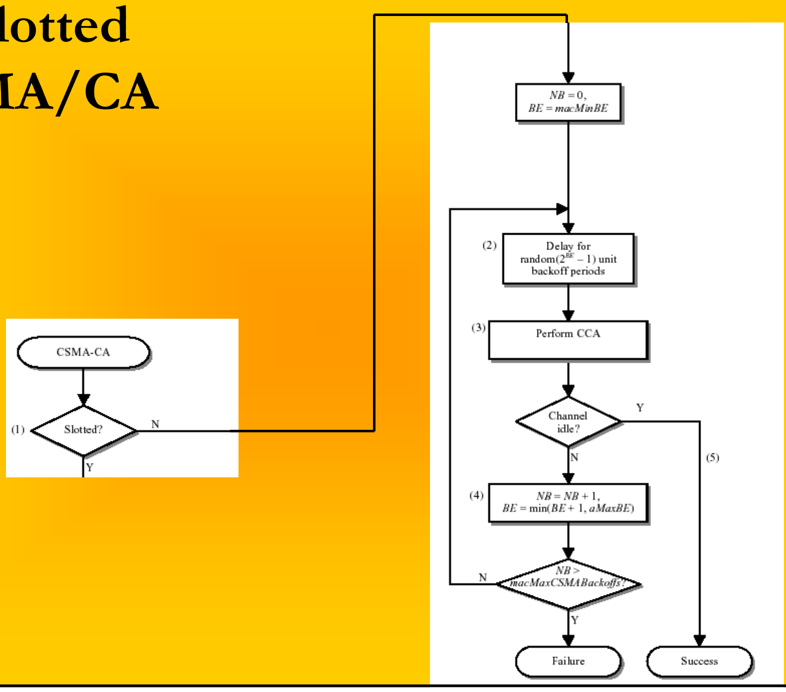
35

Channel access mechanism

- **Two type channel access mechanism:**
  - **In non-beacon-enabled networks → unslotted CSMA/CA channel access mechanism**
  - **In beacon-enabled networks → slotted CSMA/CA channel access mechanism**

36

Unslotted CSMA/CA



37

CSMA/CA algorithm

- **In slotted CSMA/CA**
  - **The backoff period boundaries of every device in the PAN shall be aligned with the superframe slot boundaries of the PAN coordinator**
    - i.e. the start of first backoff period of each device is aligned with the start of the beacon transmission
  - **The MAC sublayer shall ensure that the PHY layer commences all of its transmissions on the boundary of a backoff period**

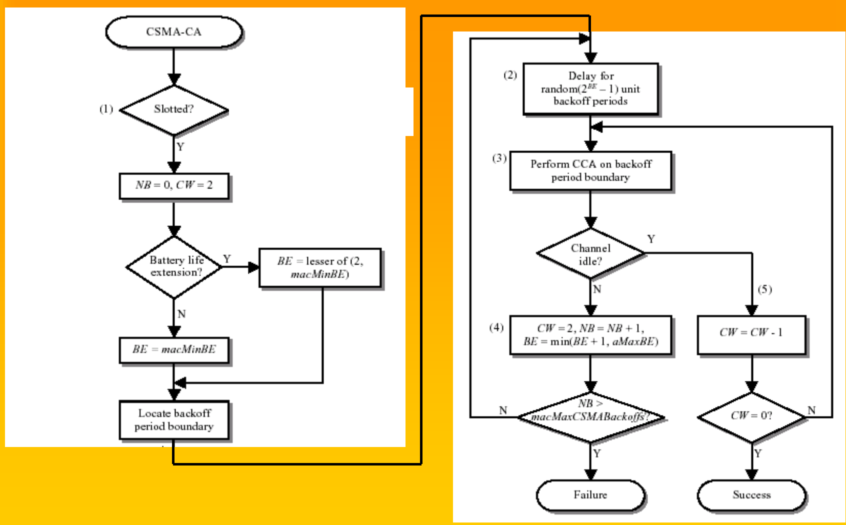
38

CSMA/CA algorithm

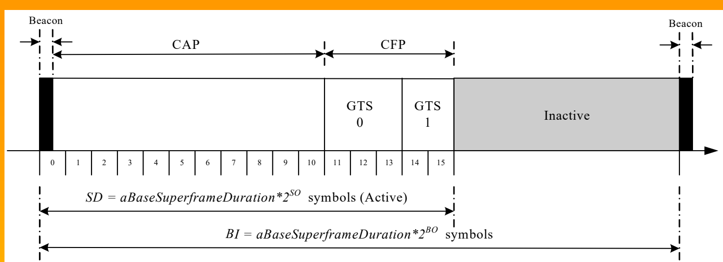
- **Each device shall maintain three variables for each transmission attempt**
  - **NB: number of time the CSMA/CA algorithm was required to backoff while attempting the current transmission**
  - **CW: contention window length, the number of backoff periods that needs to be clear of channel activity before transmission can commence (initial to 2 and reset to 2 if sensed channel to be busy)**
  - **BE: the backoff exponent which is related to how many backoff periods a device shall wait before attempting to assess a channel**

39

Slotted CSMA/CA



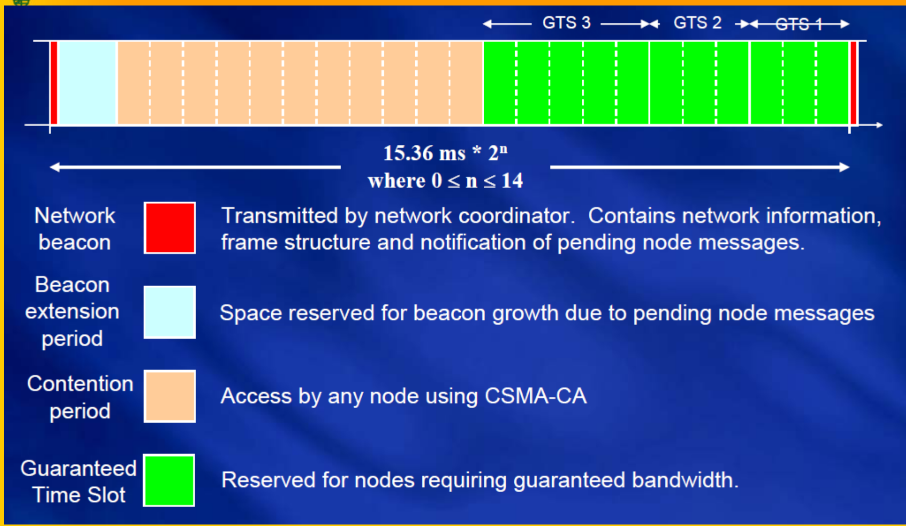
Superframe



- **A superframe is divided into two parts**
  - **Inactive: all devices sleep**
  - **Active:**
    - Active period will be divided into 16 slots
    - 16 slots can further divided into two parts
      - » Contention access period
      - » Contention free period

40

Beacon Mode



42

Superframe

- **Beacons are used for**
  - **starting superframes**
  - **synchronizing with associated devices**
  - **announcing the existence of a PAN**
  - **informing pending data in coordinators**
- **In a beacon enabled network,**
  - **Devices use the slotted CAMA/CA mechanism to contend for the usage of channels**
  - **FFDs which require fixed rates of transmissions can ask for *guarantee time slots (GTS)* from the coordinator**

43

Superframe

- The structure of superframes is controlled by two parameters: *beacon order (BO)* and *superframe order (SO)*
  - BO decides the length of a superframe
  - SO decides the length of the active potion in a superframe
- For a beacon-enabled network, the setting of BO and SO should satisfy the relationship 0≦SO≦BO≦14
  - Each device will be active for $2^{-(BO-SO)}$ portion of the time, and sleep for $1-2^{-(BO-SO)}$ portion of the time
- For channels 11 to 26, the length of a superframe can range from 15.36 *msec* to 215.7 *sec*.
  - which means very low duty cycle

BO-SO	0	1	2	3	4	5	6	7	8	9	≧10
Duty cycle (%)	100	50	25	12	6.25	3.125	1.56	0.78	0.39	0.195	< 0.1

44

GTS concepts

- A guaranteed time slot (GTS) allows a device to operate on the channel within a portion of the superframe
- A GTS shall only be allocated by the PAN coordinator
- The PAN coordinator can allocated up to seven GTSs at the same time
- The PAN coordinator decides whether to allocate GTS based on:
  - Requirements of the GTS request
  - The current available capacity in the superframe

45

GTS concepts

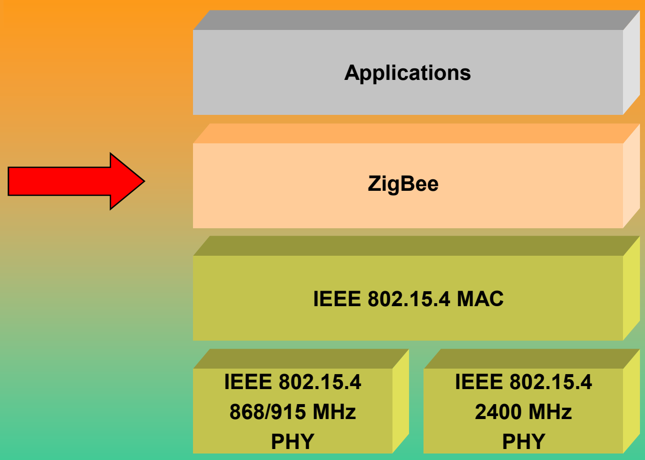
- A GTS can be deallocated
  - At any time at the discretion of the PAN coordinator or
  - By the device that originally requested the GTS
- A device that has been allocated a GTS may also operate in the CAP
- A data frame transmitted in an allocated GTS shall use only short addressing
- The PAN coordinator shall be able to store the info of devices that necessary for GTS, including starting slot, length, direction and associated device address

46

GTS concepts

- Before GTS starts, the GTS direction shall be specified as either transmit or receive
- Each device may request one transmit GTS and/or one receive GTS
- A device shall only attempt to allocate and use a GTS if it is currently tracking the beacon
- If a device loses synchronization with the PAN coordinator, all its GTS allocations shall be lost
- The use of GTSs be an RFD is optional

802.15.4 Architecture



- Network Routing
- Address translation
- Packet Segmentation
- Profiles

48

Device addressing

- **Two or more devices communicating on the same physical channel constitute a WPAN which includes <u>at least one FFD (PAN coordinator)</u>**
- **Each independent PAN will select a unique PAN identifier**
- **All devices operating on a network shall have unique 64-bit extended address (IEEE 802.15.4). This address can be used for direct communication in the PAN**
- **The network address can use a 16-bit short address, which is allocated to the child routers by the PAN coordinator when the device associates**
- **256 sub addresses may be allocated for subunits**

49

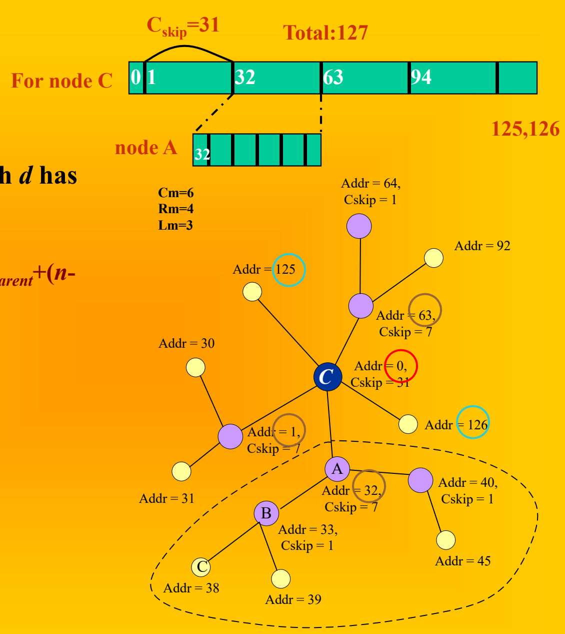
Address assignment in a ZigBee network

- **In ZigBee, network addresses are assigned to devices by a distributed address assignment scheme**
- **ZigBee coordinator determines three network parameters to set the allocations**
  - **the maximum number of children (C_m) of a ZigBee router**
  - **the maximum number of child routers (R_m) of a parent node**
  - **the depth of the network (L_m)**
- **A parent device utilizes C_m, R_m, and L_m to compute a parameter called C_{skip}**
  - **which is used to compute the size of its children's address pools**

$$Cskip(d) = \begin{cases} 1 + Cm \cdot (Lm - d - 1), & \text{if } Rm = 1 \quad \cdots\cdots\cdots\cdots(a) \\ \dfrac{1 + Cm - Rm - Cm \cdot Rm^{Lm-d-1}}{1 - Rm}, & \text{Otherwise} \quad \cdots\cdots\cdots\cdots(b) \end{cases}$$

50

- **If a parent node at depth d has an address A_{parent},**
  - **the nth child router is assigned to address $A_{parent}+(n-1)\times C_{skip}(d)+1$**
  - **nth child end device is assigned to address $A_{parent}+R_m\times C_{skip}(d)+n$**



51

ZigBee routing protocols

- **In a tree network**
  - **Utilize the address assignment to obtain the routing paths**
- **In a mesh network**
  - **Two options**
    - Reactive routing: if having routing capacity
    - Use tree routing: if do not have routing capacity
- **Note:**
  - **ZigBee coordinators and routers are said to have *routing capacity* if they have routing table capacities and route discovery table capacities**

52

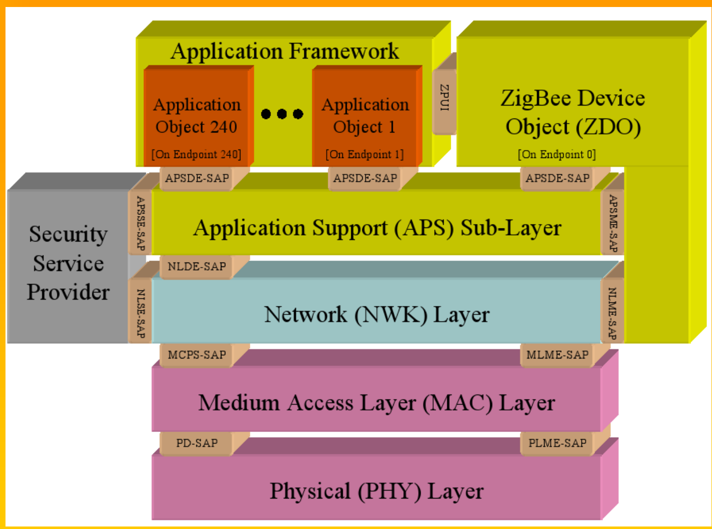
Summary of ZigBee network layer

- **Pros and cons of different kinds of ZigBee network topologies**

	Pros	Cons
Star	1. Easy to synchronize 2. Support low power operation 3. Low latency	1. Small scale
Tree	1. Low routing cost 2. Can form superframes to support sleep mode 3. Allow multihop communication	1. Route reconstruction is costly 2. Latency may be quite long
Mesh	1. Robust multihop communication 2. Network is more flexible 3. Lower latency	1. Cannot form superframes (and thus cannot support sleep mode) 2. Route discovery is costly 3. Needs storage for routing table

Application Level

ZigBee – Short range comunication



ZigBee Profiles

Profiles:

Definition of ZigBee-Profiles

- **describes a common language for exchanging data**
- **defines the offered services**
- **device interoperatbility across different manufacturers**
- **Standard profiles available from the ZigBee Alliance**
- **profiles contain device descriptions**
- **unique identifier (licensed by the ZigBee Alliance)**

57

ZigBee and BLE

- Business comparison:
  - ZigBee is older. It has gone through some iterations
  - Market barriers: connectivity – ZigBee is not in PCs or mobile phones yet.
- Technical comparison:
  - Zigbee is low power; Bluetooth LE is even lower. Detailed analysis depends on specific applications and design detail, no to mention chip geometry.
  - ZigBee stack is light; the Bluetooth LE/GATT stack is even simpler
- Going forward:
  - ZigBee has a lead on developing applications and presence
  - Bluetooth low energy has improved technology, and a commanding presence in several existing markets: mobile phones, automobiles, consumer electronics, PC industry
  - Replacing "classic Bluetooth " with "dual mode" devices bootstraped market quickly

802.11

We all live with it

59

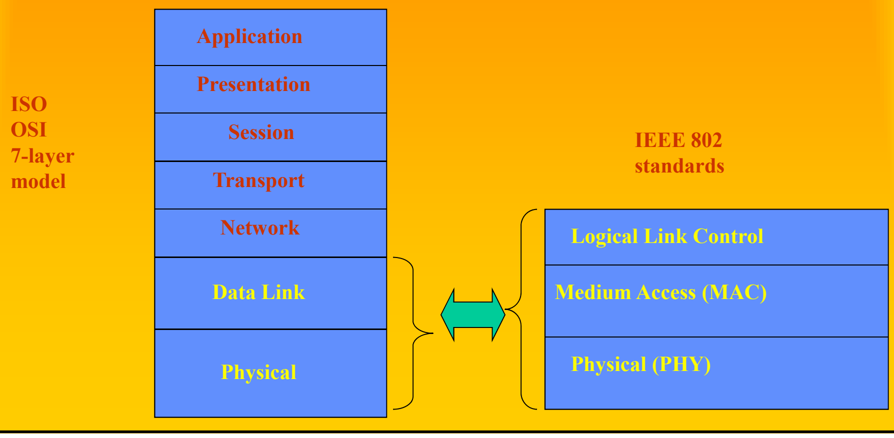
© Rui L. Aguiar (ruilaa@det.ua.pt)

Outline

- 802.11 standard
- ➢ Physical layer
- MAC
  – DCF
  – PCF
- Advanced MAC functions

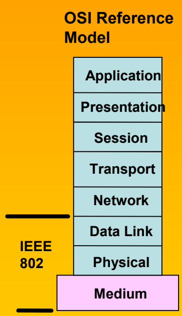
Standardization of Wireless Networks

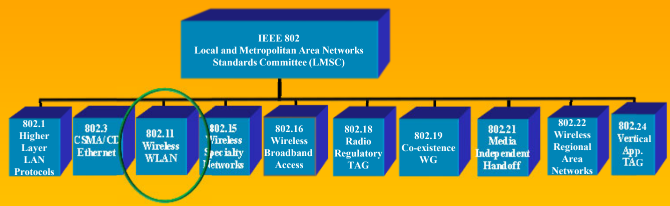
- Wireless networks are standardized by IEEE.
- Under 802 LAN MAN standards committee.



The IEEE 802.11 Working Group

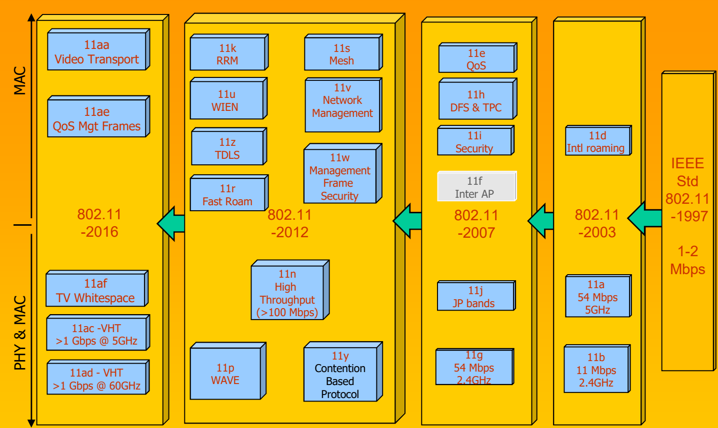
- Focus on link and physical layers of the network stack
- Leverage IETF protocols for upper layers





IEEE 802.11 WG Voting Members: 300+

Development of the IEEE 802.11 Standard is ongoing since 1997



62

Old versions are being deprecated by new versions, and new features are added as time goes by.

63

Historic IEEE 802.11 standard

- Local Wireless Network (WLAN)
- Includes Medium Access Control (MAC)
- Includes(d) five physical layers (PHY)
  - Frequency Hopping Spread Spectrum
  - Direct Sequence Spread Spectrum
  - infrared
  - 11 Mbps - 2.4 GHz
  - 54 Mbps - 5 GHz
- Early efforts divided in three standards:
  - 802.11
  - 802.11a
  - 802.11b

Historic IEEE 802.11 Family

Protocol	Release Data	Freq.	Rate (typical)	Rate (max)	Range (indoor)
Legacy	1997	2.4 GHz	1 Mbps	2Mbps	?
802.11a	1999	5 GHz	25 Mbps	54 Mbps	~30 m
802.11b	1999	2.4 GHz	6.5 Mbps	11 Mbps	~30 m
802.11g	2003	2.4 GHz	25 Mbps	54 Mbps	~30 m
802.11n	2008	2.4/5 GHz	200 Mbps	600 Mbps	~50 m

IEEE 802.11 innovation

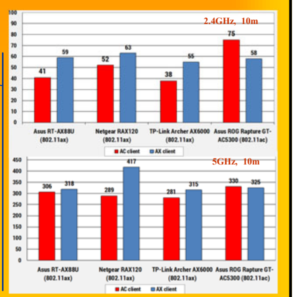
- Market demands and new technology push for new 802.11 standards
- Demand for throughput
  - Continuing exponential demand for throughput (802.11ax and 802.11ay, 802.11be)
  - Most (50-80%, depending on the country) of the world's mobile data is carried on 802.11 (Wi-Fi) devices
- New usage models / features
  - Dense deployments (802.11ax), Indoor Location (802.11az),
  - Automotive (IEEE Std 802.11p, Next Gen V2X), Internet of Things (802.11ah)
  - Low Power applications (802.11ba)
  - WLAN Sensing (802.11bf – pending approval)
- Technical capabilities
  - MIMO (IEEE Std 802.11n, 802.11ac, 802.11ay) and OFDMA (802.11ax)
  - 60 GHz radios (802.11ay)
- Changes to regulation
  - TV whitespaces (IEEE Std 802.11af), Radar detection (IEEE Std 802.11h), 6GHz (802.11ax, 802.11be)
  - Coexistence and radio performance rules (e.g., ETSI BRAN, ITU-R)

65

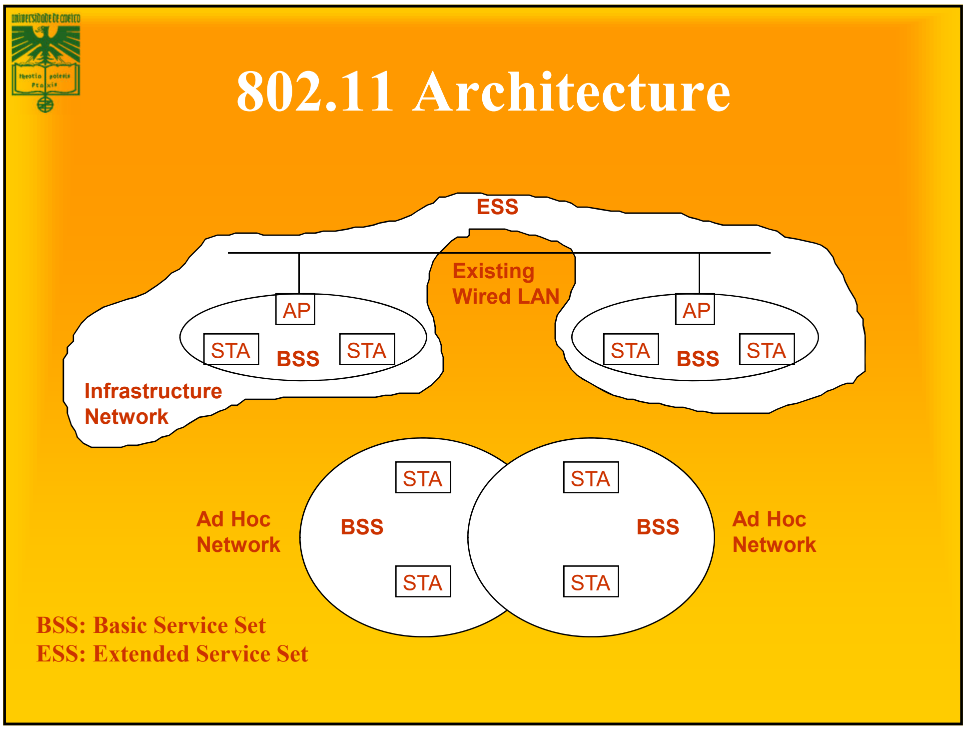
New 802.11 Radio technologies

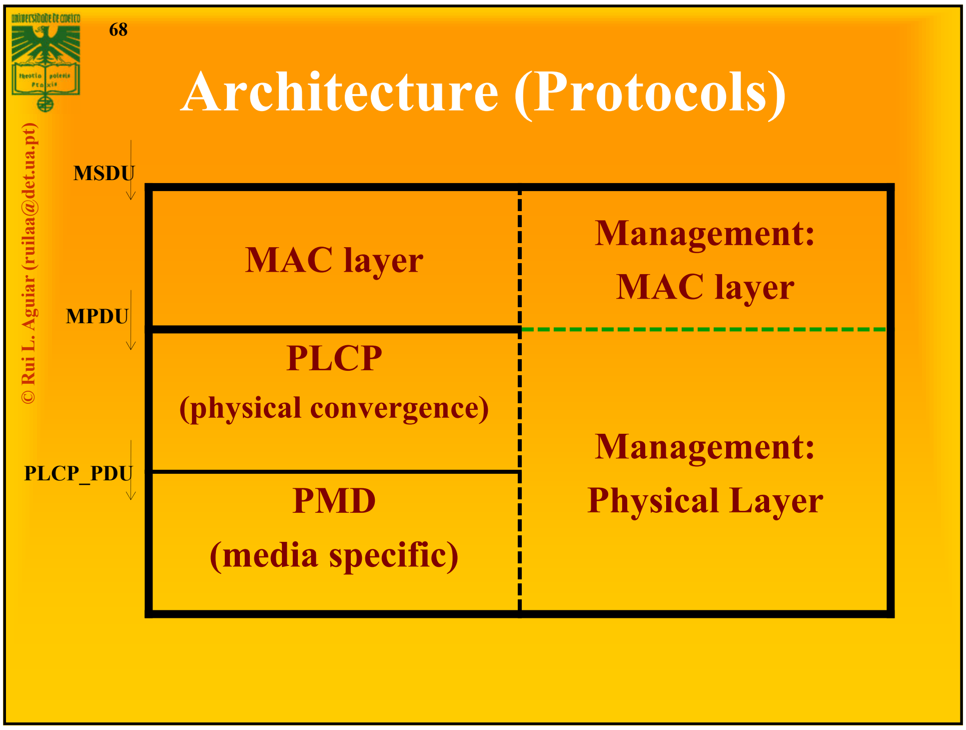
Current recent innovations being deployed:

- 802.11ax – Increased throughput in 2.4, 5 (and 6) GHz bands. Increased efficiency. WiFi6
- 802.11ay – Support for 20 Gbps in 60 GHz band.
- 802.11az – 2nd generation positioning features.
- 802.11ba – Wake up radio. Low power IoT applications.
- 802.11bb – Light Communications
- 802.11bc – Enhanced Broadcast Service
- 802.11bd – Enhancements for Next Generation V2X
- 802.11be – Extremely High Throughput
- 802.11bf – WLAN Sensing [pending approval]



66


802.11 Architecture
ESS
Existing
Wired LAN
AP
STA
BSS
STA
AP
STA
BSS
STA
Infrastructure
Network
STA
STA
Ad Hoc
Network
BSS
BSS
Ad Hoc
Network
STA
STA
BSS: Basic Service Set
ESS: Extended Service Set


68
Architecture (Protocols)
© Rui L. Aguiar (ruilaa@det.ua.pt)
MSDU
MAC layer
Management:
MAC layer
MPDU
PLCP
(physical convergence)
PLCP_PDU
PMD
(media specific)
Management:
Physical Layer

69

Components

- **Station (STA) –** Mobile Terminal
- **Access Point (AP) -** STA are connected to Access Points (infrastructured networks)
- **Basic Service Set (BSS) –** STA and AP with the same coverage and connectivity area create a BSS.
- **Extended Service Set (ESS) –** Multiple BSSs connected via the APs create an ESS.

802.11 Wireless Glossary

- **Clear Channel Assessment (CCA):**
  - A station function used to determine when it is OK to transmit.
- **Association:**
  - A function that maps a station to an Access Point.
- **MAC Service Data Unit (MSDU):**
  - Data Frame passed between user & MAC.
- **MAC Protocol Data Unit (MPDU):**
  - Data Frame passed between MAC & PHY.
- **PLCP Packet (PLCP_PDU):**
  - Data Packet passed from PHY to PHY over the Wireless Medium.

Terminology for infrastructure mode

- Stations and access points
- BSS - Basic Service Set
  - One access point that provides access to wired infrastructure
  - Infrastructure BSS
- ESS - Extended Service Set
  - A set of infrastructure BSSs that work together
  - APs are connected to the same infrastructure
  - Tracking of mobility
- DS – Distribution System
  - AP communicates with another
  - Thin layer between LLC and MAC sublayers

Infrastructure vs Ad Hoc Mode

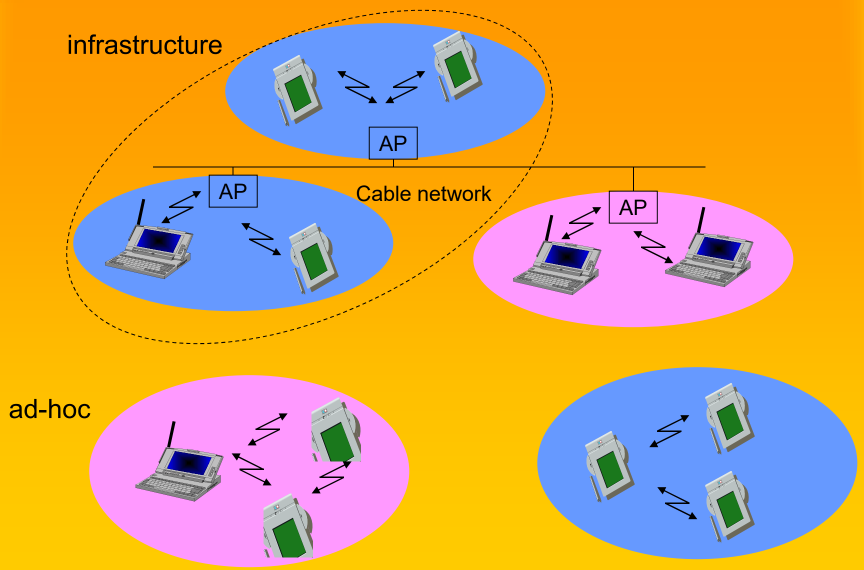
- Infrastructure mode: stations communicate with one or more access points which are connected to the wired infrastructure
  - What is deployed in practice
- Two modes of operation:
  - Distributed Control Functions - DCF ← Industry Focus
  - Point Control Functions – PCF
  - PCF is rarely used - inefficient
- Alternative is “ad hoc” mode: multi-hop, assumes no infrastructure
  - Rarely used, e.g. military
  - Hot research topic!

What about Ad Hoc?

- **Ad-hoc mode: no fixed network infrastructure**
  - **Based on an Independent BSS**
  - **A wireless endpoint sends and all nodes within range can pick up signal**
  - **Each packet carries destination and source address**
  - **Effectively need to implement a "network layer"**
    - How do know who is in the network?
    - Routing?
    - Security?
  - **Research area**
    - discussed elsewhere

74

Infrastructure vs. Adhoc



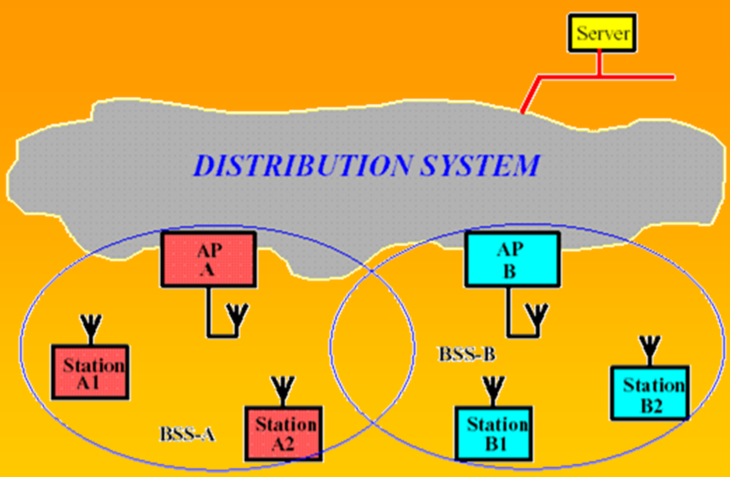
75

Distribution System (DS)

- 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)

76

Extended Service Set network

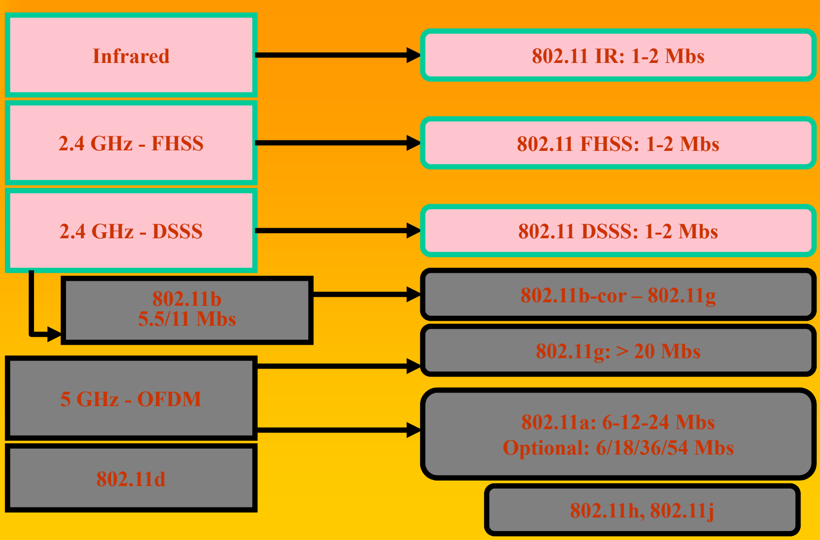


77

Outline

- 802.11 standard
- ➢Physical layer
- MAC
  - DCF
  - PCF
- Advanced MAC functions

Physical Layer



79

802.11: Physical Layer FH-SS

- **Spread-spectrum (frequency hopping)**
- **79 channels, hop rate > 2.5 hops/sec.**
- **Band: 2.4 GHz ISM**
- **Transference rate: 1 or 2 Mbps**
- **Modulation: 2 or 4 levels in FSK**
- **Data Whitening for Bias Suppression**
  - 32/33 bit stuffing and block inversion
  - 7-bit LFSR scrambler
- **80-bit Preamble Sync pattern**
- **32-bit Header**
- **1 Watt maximum (100 - 500 mw typical)**

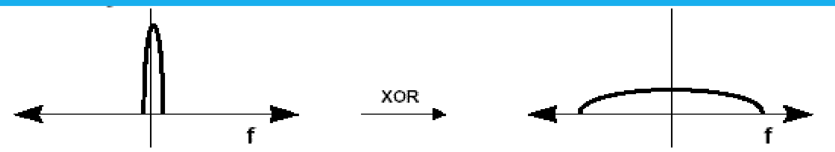
80

802.11: Physical Layer DS-SS

- **Spread spectrum, direct sequence**
- **Spread factor: 11 chips per bit.**
- **Band 2.4 GHz ISM**
- **Three channels of ~20 MHz**
- **Transmission rate: 1 or 2 Mbps**
- **Modulation: DQPSK or differential binary**
- **Data Scrambling using 8-bit LFSR**
- **128-bit Preamble Sync pattern**
- **48-bit Header**
- **1 Watt maximum (100 - 500 mw typical)**

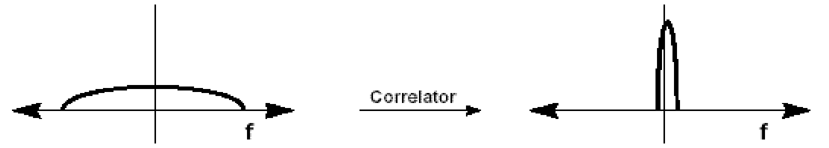
81

Spread-spectrum communications



Transmit – Signal through PRN sequence

Receive – Sginal correlated with the PRN sequence



82

DSSS properties

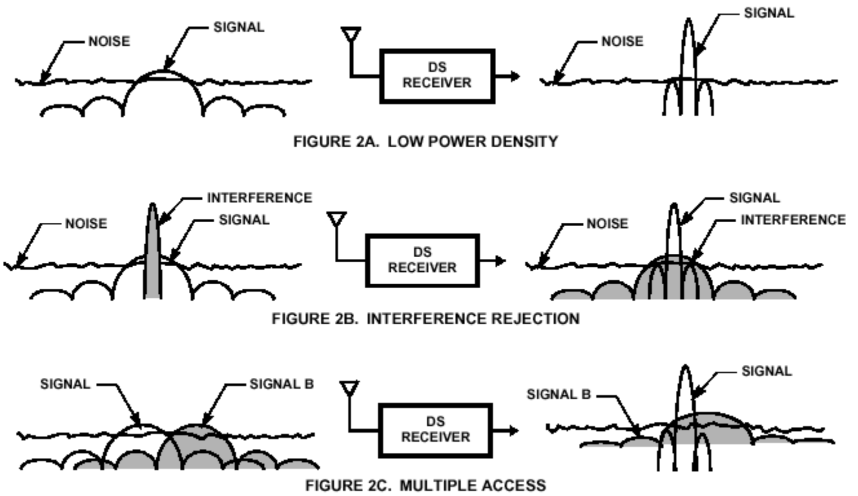


FIGURE 2. DIRECT SEQUENCE SPREAD SPECTRUM PROPERTIES

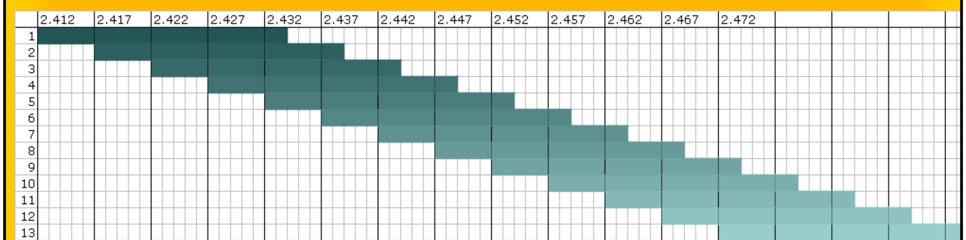
83

802.11b

- Extension to original DS-SS mode
- Added transmission at 5.5 and 11 Mbps
  - And bitrate adjustment
- Compatible with original 802.11 DS-SS
  - Can use the same three channels on the 2.4 GHz band
- Modulation: Complementary Code Keying (CCK)
- Uses the original MAC

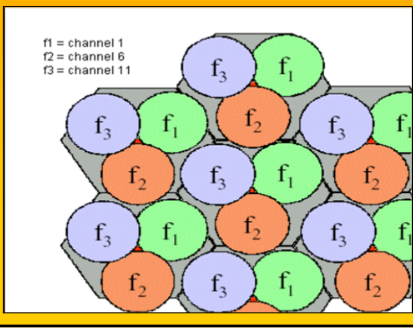
802.11b Channels

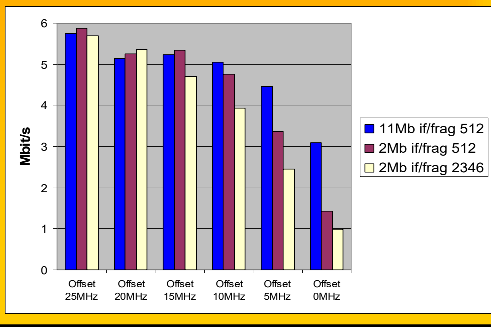
- In the UK and most of EU: 13 channels, 5MHz apart, 2.412 – 2.472 GHz
- In the US: only 11 channels
- Each channel is 22 MHz
- Significant overlap
- Best channels are 1, 6 and 11



Frequency planning

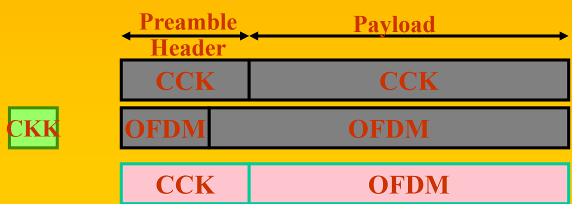
- Interference from other WLAN systems or cells
- IEEE 802.11 operates at uncontrolled ISM band
- 14 channels of 802.11 are overlapping, only 3 channels are disjointed. For example Ch1, 6, 11
- Throughput decreases with less channel spacing
- A example of frequency allocation in multi-cell network





Going Faster: 802.11g

- 802.11g basically extends 802.11b
  - Use the same technology DS-SS/CCK for lower rates
  - Uses OFDM technology for rates > 20 Mbs
- Using OFDM makes it easier to build 802.11a/g cards
  - Since 802.11a uses OFDM
- But it creates an interoperability problem since 802.11b cards cannot interpret OFDM signals
  - Solutions: send CTS using CCK before OFDM packets in hybrid environments, or use (optional) hybrid packet format



802.11a

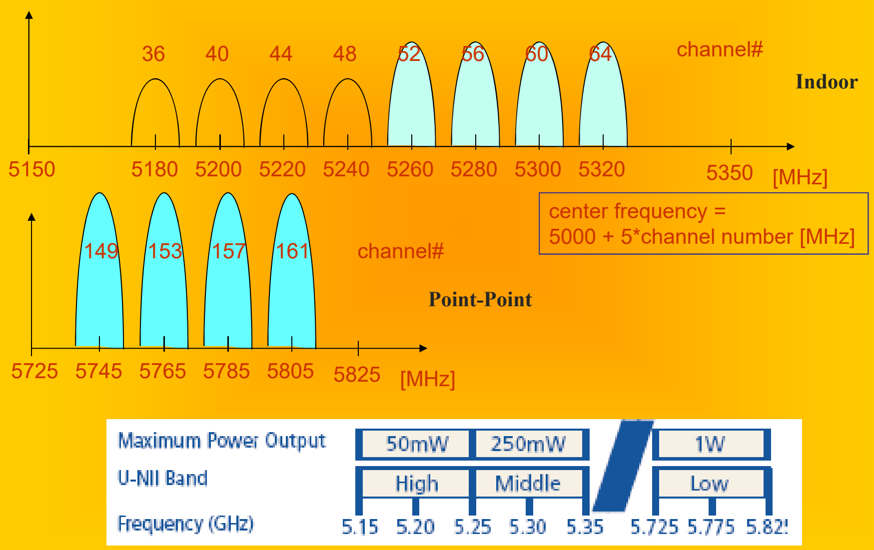
- Uses OFDM in the 5.2 and 5.7 GHz bands (U-NII)
  - Information transmitted in multiple sub-carriers
- Uses same MAC than 802.11
- What are the benefits of 802.11a compared with 802.11b?
  - Greater bandwidth (up to 54Mb), according with sub-carrier modulation and FEC
    - 54, 48, 36, 24, 18, 12, 9 and 6 Mbs
  - Less potential interference (5GHz)
  - More non-overlapping channels
- But does not provide interoperability with 802.11b, as 802.11g does
  - Interoperability at chipset level

802.11a Modulation

- Use OFDM to divide each physical channel (20 MHz) into 52 subcarriers (20M/64=312.5 KHz each)
  - 48 data, 4 pilot

- Adaptive modulation
  - BPSK: 6, 9 Mbps
  - QPSK: 12, 18 Mbps
  - 16-QAM: 24, 36 Mbps
  - 64-QAM: 48, 54 Mbps

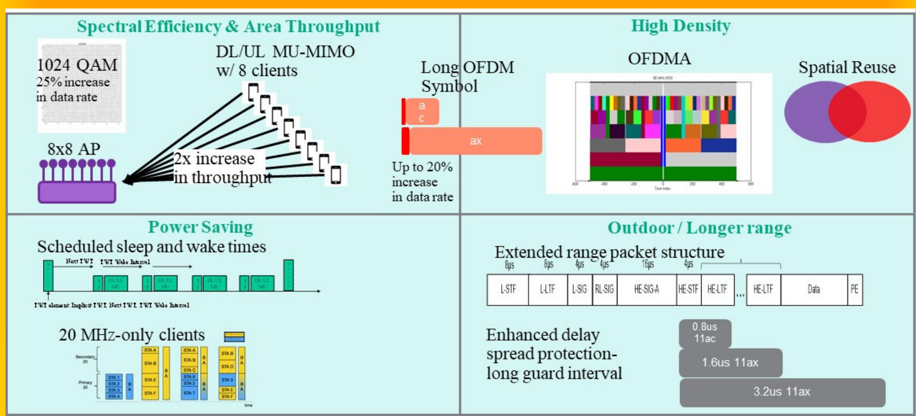
802.11a Physical Channels



WiFi6

Currently under acceptance:

- **802.11ax – Increased throughput in 2.4, 5 (and 6) GHz bands. Increased efficiency.**



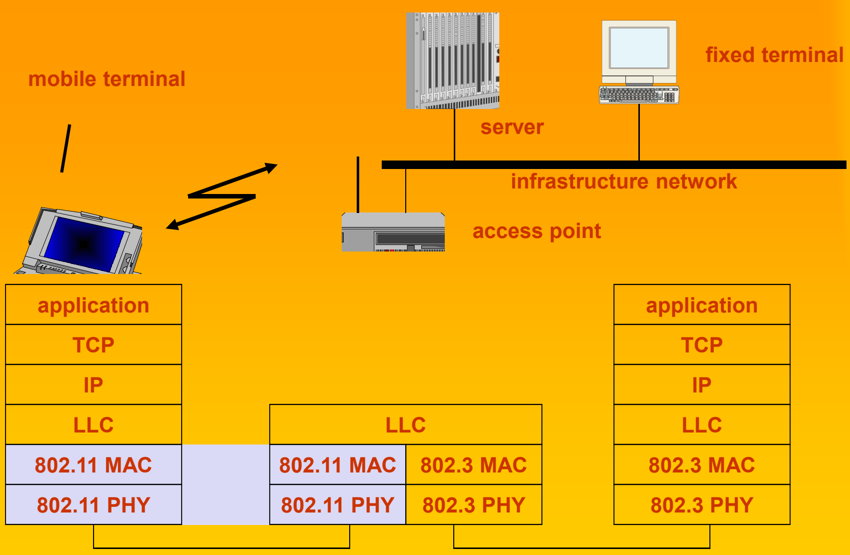
91

Outline

- 802.11 standard
- Physical layer
- ➢ MAC
  - DCF
  - PCF
- Advanced MAC functions

92

802.11- in the TCP/IP stack



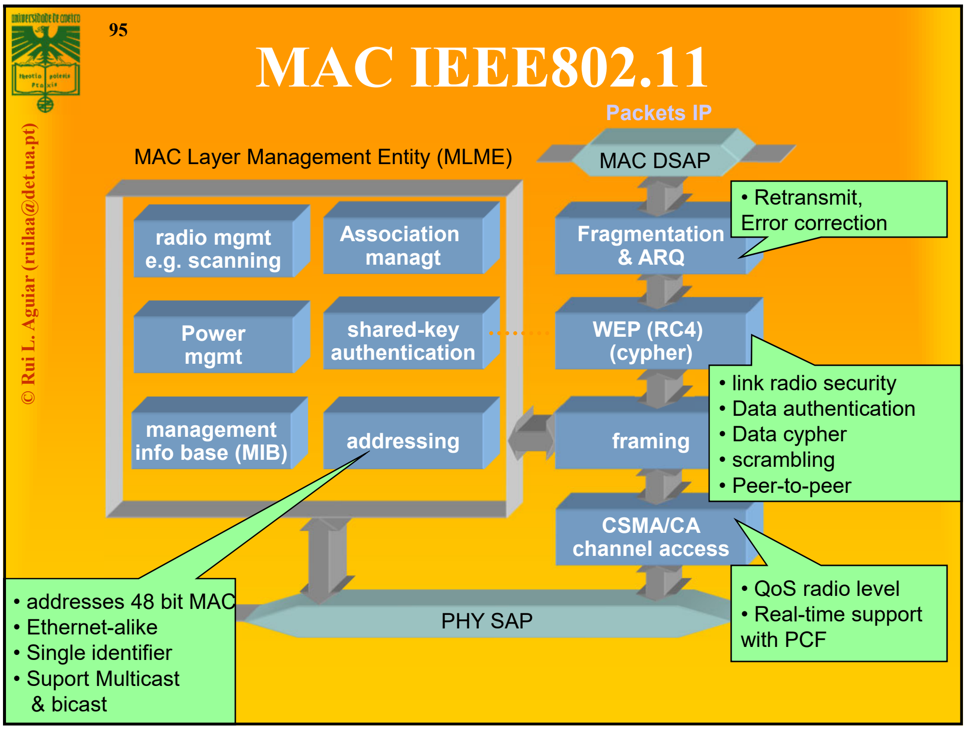
93

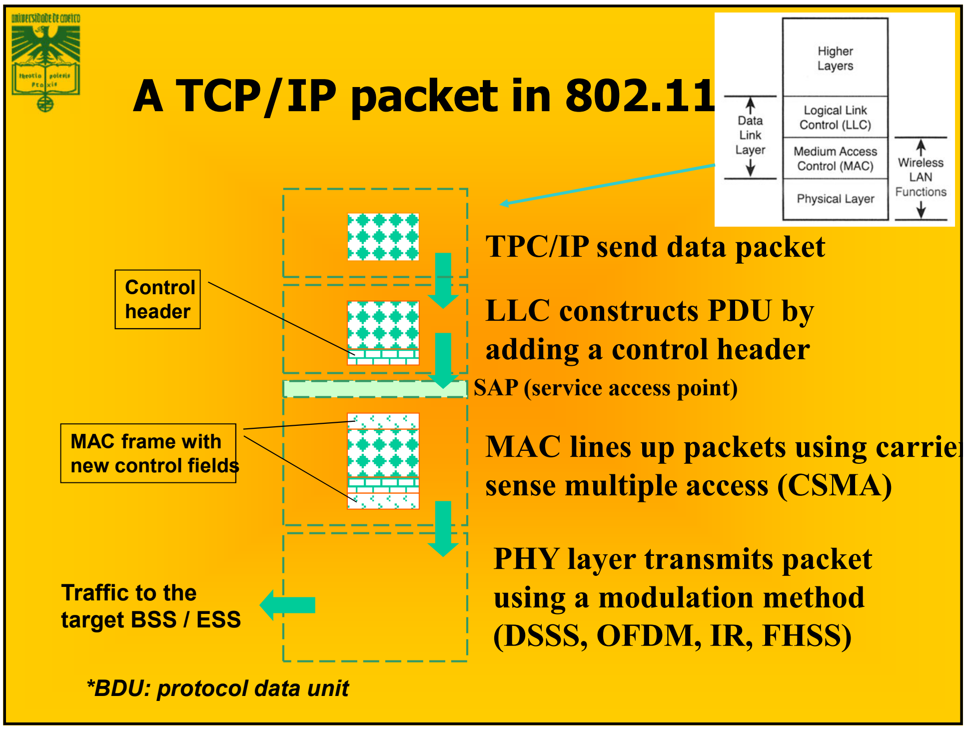
802.11 MAC Overview

- Uses variant of Carrier Sense Multiple Access with Collision Avoidance (CS/MACA)
  - RTS/CTS used for addressing hidden-nodes
- Automatic Repeat Request (ARQ)
  - All frames have to be properly ACK.
- Two operating modes:
  - Infra-structured network (Access point)
  - Ad-Hoc networks (without access point)
- Power saving support
- Wired Equivalent Privacy (WEP)
- MAC management
- Independent of the physical layer or of operating mode

Features of 802.11 MAC protocol

- Fair control access
  - Supports Media Access Control functionalities
    - Addressing
    - CSMA/CA
- Protection of date
  - Error detection (FCS)
  - Error correction (ACK frame)
- Reliable data delivery
  - Flow control: stop-and-wait
  - Fragmentation (More Frag)

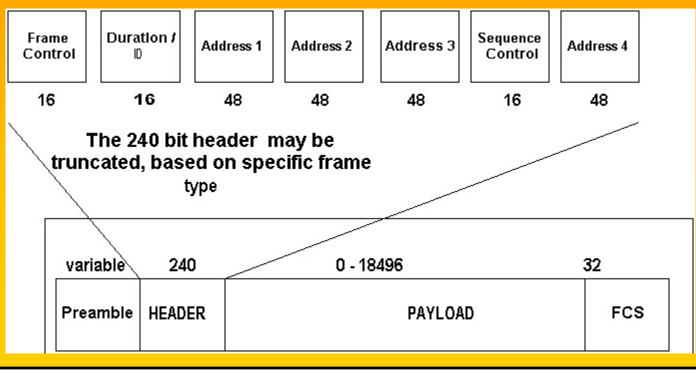

95
MAC IEEE802.11
© Rui L. Aguiar (ruilaa@det.ua.pt)
Packets IP
MAC Layer Management Entity (MLME)
MAC DSAP
radio mgmt
e.g. scanning
Association
managt
Power
mgmt
shared-key
authentication
management
info base (MIB)
addressing
Fragmentation
& ARQ
WEP (RC4)
(cypher)
framing
CSMA/CA
channel access
• Retransmit,
Error correction
• link radio security
• Data authentication
• Data cypher
• scrambling
• Peer-to-peer
• QoS radio level
• Real-time support
with PCF
PHY SAP
• addresses 48 bit MAC
• Ethernet-alike
• Single identifier
• Suport Multicast
& bicast


A TCP/IP packet in 802.11
Higher
Layers
Logical Link
Control (LLC)
Medium Access
Control (MAC)
Physical Layer
Data
Link
Layer
Wireless
LAN
Functions
TPC/IP send data packet
Control
header
LLC constructs PDU by
adding a control header
SAP (service access point)
MAC frame with
new control fields
MAC lines up packets using carrie
sense multiple access (CSMA)
PHY layer transmits packet
using a modulation method
(DSSS, OFDM, IR, FHSS)
Traffic to the
target BSS / ESS
*BDU: protocol data unit

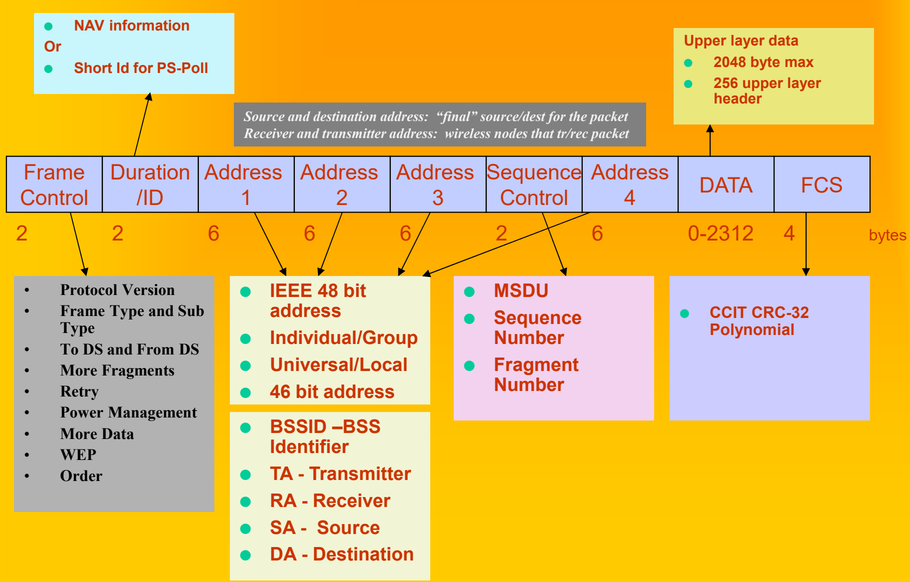
97

802.11 Frames

- Three types of frames
  - control: RTS, CTS, ACK
  - Management
  - Data
- Header depends on the frame type



Frame Format



Packet Types

- Type/sub-type field is used to indicate the type of the frame
- Management:
  - Association/Authentication/Beacon
- Control
  - RTS, CTS, CF-end, ACK
- Data
  - Data only, or Data + CF-ACK, or Data + CF-Poll or Data + CF-Poll + CF-ACK

Some More Fields

- Duration/ID: Duration in DCF mode/ID is used in PCF mode
- More Frag: 802.11 supports fragmentation of data
- More Data: In polling mode, station indicates it has more data to send when replying to CF-POLL
- RETRY is 1 if frame is a retransmission;
- WEP (Wired Equivalent Privacy) is 1 if frame is WEP coded
- Power Mgmt is 1 if in Power Save Mode;
- Order = 1 for strictly ordered service

Multi-bit Rate

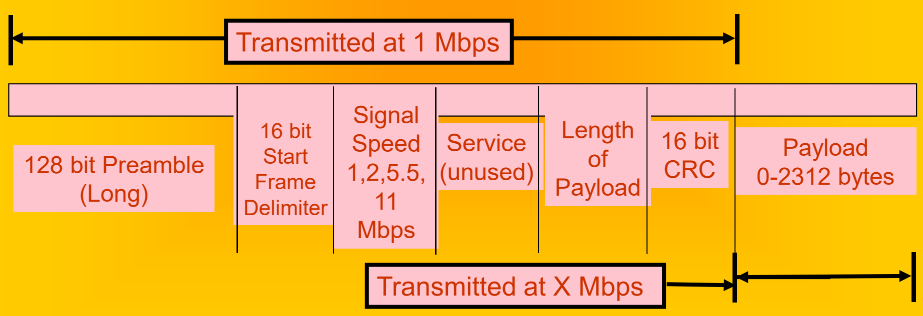
- **802.11 allows for multiple bit rates**
  - **Allows for adaptation to channel conditions**
  - **Specific rates dependent on the version**
- **Algorithm for selecting the rate is not defined by the standard – left to vendors**
- **Packets have multi-rate format**
  - **Different parts of the packet are sent at different rates**

Following examples illustrative (newer versions are different, but problems are similar)

802.11b: Long Preamble

Long Preamble = 144 bits

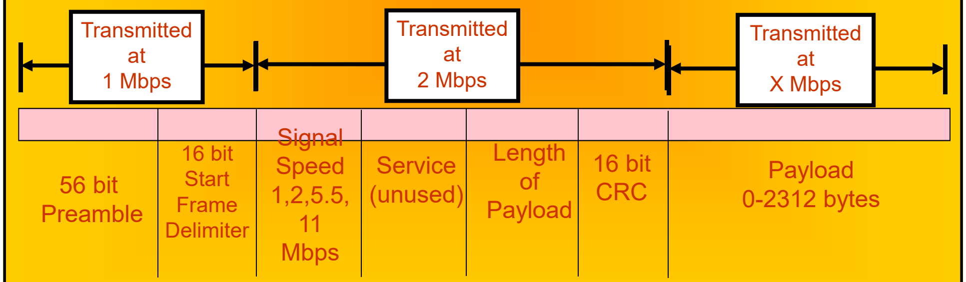
- **Interoperable with older 802.11 devices**
- **Entire Preamble and 48 bit PLCP Header sent at *1 Mbps***



802.11b: Short Preamble

Short Preamble = 72 bits

- Preamble transmitted at 1 Mbps
- PLCP Header transmitted at 2 Mbps
- more efficient than long preamble



Addressing Fields

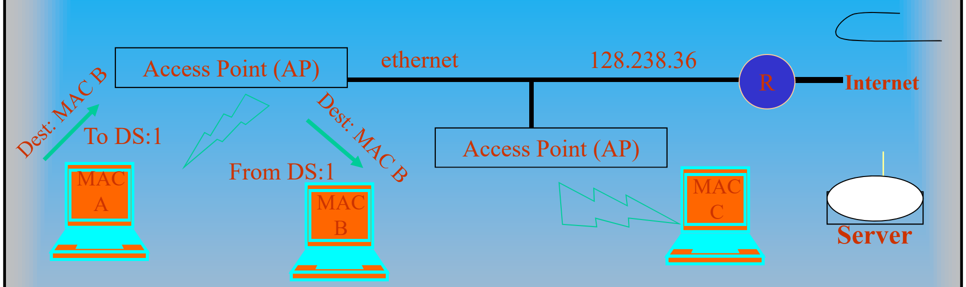
To DS	From DS	Message	Address 1	Address 2	Address 3	Address 4
0	0	station-to-station frames in an IBSS; all mgmt/control frames	DA	SA	BSSID	N/A
0	1	From AP to station	DA	BSSID	SA	N/A
1	0	From station to AP	BSSID	SA	DA	N/A
1	1	From one AP to another in same DS	RA	TA	DA	SA

RA: Receiver Address TA: Transmitter Address
DA: Destination Address SA: Source Address
BSSID: MAC address of AP in an infrastructure BSS

Data Flow Examples

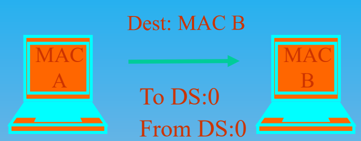
- Case 1: Packet from a station under one AP to another in same AP's coverage area
- Case 2: Packet between stations in an IBSS
- Case 3: Packet from an 802.11 station to a wired server on the Internet
- Case 4: Packet from an Internet server to an 802.11 station

Case 1: Communication Inside BSS



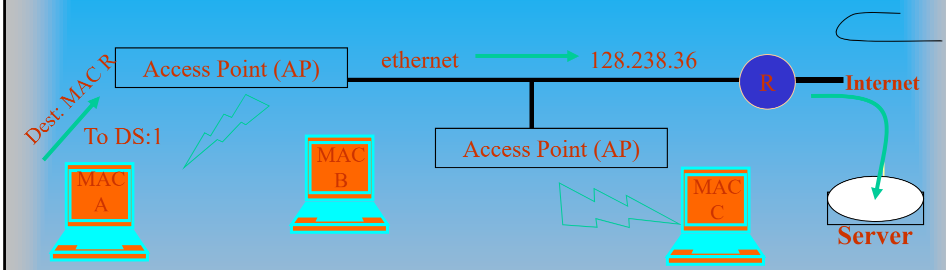
- AP knows which stations are registered with it so it knows when it can send frame directly to the destination

Case 2: Ad Hoc



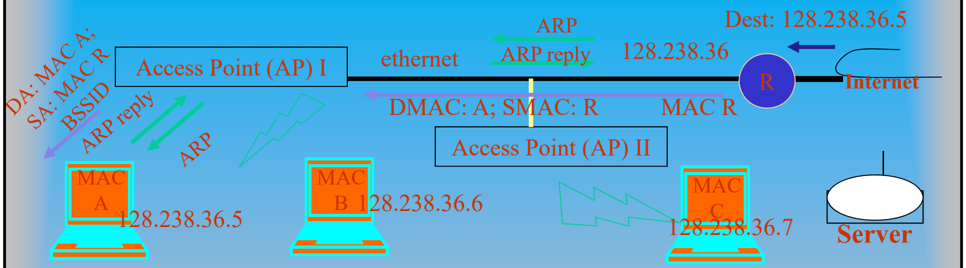
- **Direct transmit only in IBSS (Independent BSS), i.e., without AP**
- **Note:**
  - **in infrastructure mode (i.e., when AP is present), even if B can hear A, A sends the frame to the AP, and AP relays it to B**

Case 3: To the Internet



- **MAC A determines IP address of the server (using DNS)**
- **From the IP address, it determines that server is in a different subnet**
- **Hence it sets MAC R as DA;**
  - **Address 1: BSSID, Address 2: MAC A; Address 3: DA**
- **AP will look at the DA address and send it on the ethernet**
  - **AP is an 802.11 to ethernet bridge**
- **Router R will relay it to server**

Case 4: From Internet to Station



- **Packet arrives at router R – uses ARP to resolve destination IP address**
  - **AP knows nothing about IP addresses, so it will simply broadcast ARP on its wireless link**
  - **DA = all ones – broadcast address on the ARP**
- **MAC A host replies with its MAC address (ARP reply)**
  - **AP passes on reply to router**
- **Router sends data packet, which the AP simply forwards because it knows that MAC A is registered**

110

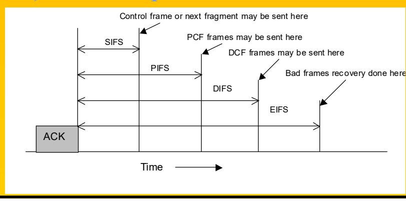
Outline

- **802.11 standard**
- **Physical layer**
- **MAC**
  - ➢**DCF**
  - – **PCF**
- **Advanced MAC functions**

111

MAC Layer

- Asynchronous Data Service (DCF)
  - CSMA/CA
  - RTS/CTS
- Timing-controled service (PCF)
  - Polling
- Inter-frame spacing (IFS)
  - DIFS (distributed), for the node to start transmisting
  - PIFS (point), used by PCF to net access
  - SIFS (short), between packets of the same flow



Carrier Sense Multiple Access

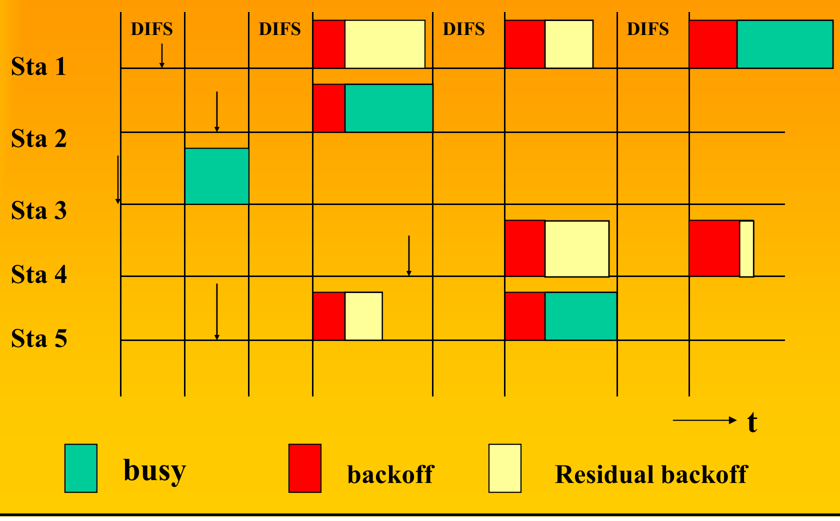
- Before transmitting a packet, sense carrier
- If it is idle, send
  - After waiting for one DCF inter frame spacing (DIFS)
- If it is busy, then
  - Wait for medium to be idle for a DIFS (DCF IFS) period
  - Go through exponential backoff, then send
  - Want to avoid that several stations waiting to transmit automatically collide
- Wait for ack
  - If there is one, you are done
  - If there isn't one, assume there was a collision, retransmit using exponential backoff

Exponential Backoff

- **Force stations to wait for random amount of time to reduce the chance of collision**
  - **Backoff period increases exponential after each collision**
  - **Similar to Ethernet**
- **If the medium is sensed it is busy:**
  - **Wait for medium to be idle for a DIFS (DCF IFS) period**
  - **Pick random number in contention window (CW) = backoff counter**
  - **Decrement backoff timer until it reaches 0**
    - But freeze counter whenever medium becomes busy
  - **When counter reaches 0, transmit frame**
  - **If two stations have their timers reach 0; collision will occur;**
- **After every failed retransmission attempt:**
  - **increase the contention window exponentially**
  - **$2^i - 1$ starting with CW_{min} up to CW_{max} e.g., 7, 15, 31, …**

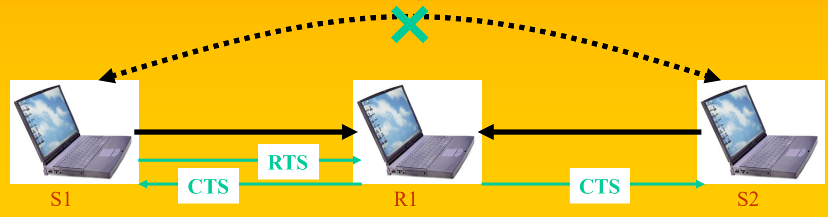
114

CSMA/CA



Collision Avoidance

- **Difficult to detect collisions in a radio environment**
  - **While transmitting, a station cannot distinguish incoming weak signals from noise – its own signal is too strong**
- **Why do collisions happen?**
  - **Near simultaneous transmissions**
    - Period of vulnerability: propagation delay
  - **Hidden node situation: two transmitters cannot hear each other and their transmission overlap at a receiver**



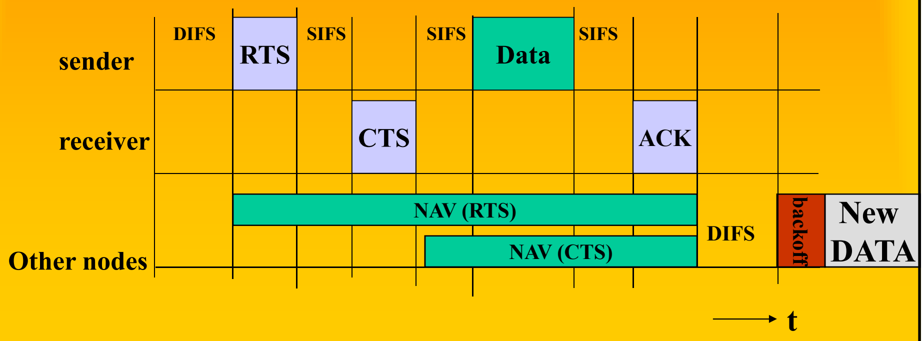
Request-to-Send and Clear-to-Send

- **Before sending a packet, first send a station first sends a RTS.**
- **The receiving station responds with a CTS.**
  - **RTS and CTS are smaller than data packets**
  - **RTS and CTS use shorter IFS to guarantee access**
- **Stations that hear either the RTS or the CTS “remember” that the medium will be busy for the duration of the transmission**
  - **Based on a Duration ID in the RTS and CTS**
- **Virtual Carrier Sensing: stations maintain Network Allocation Vector (NAV)**
  - **Time that must elapse before a station can sample channel for idle status**

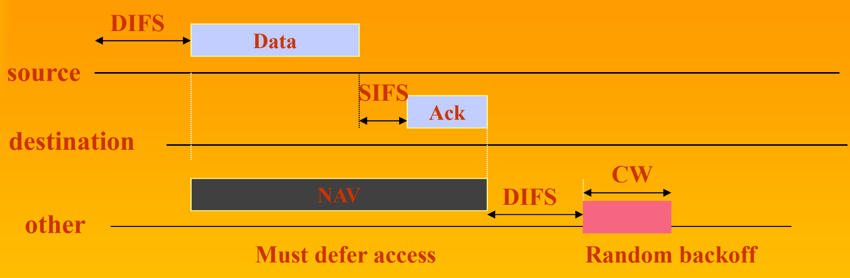
RTS/CTS: NAV

NAV: Network Allocation Vector

NAV acts as a distributed (in each node) resource allocation register



DCF mode transmission without RTS/CTS



RTS/CTS is often not used

Overhead is too high compared with benefit

119

Overal control is time-based!

- **Inter-frame spacing (IFS)**
  - **DIFS (distributed)**
    - **Time before a normal transmission, for contention-based period**
  - **PIFS (point),**
    - **Time used by the PCF, to have priority access during contention-free period**
  - **SIFS (short),**
    - **Time between packets of the same flow, and these should not be interrupted**
    - **High priority transmissions**
  - **EIFS (extended),**
    - **Error periods**

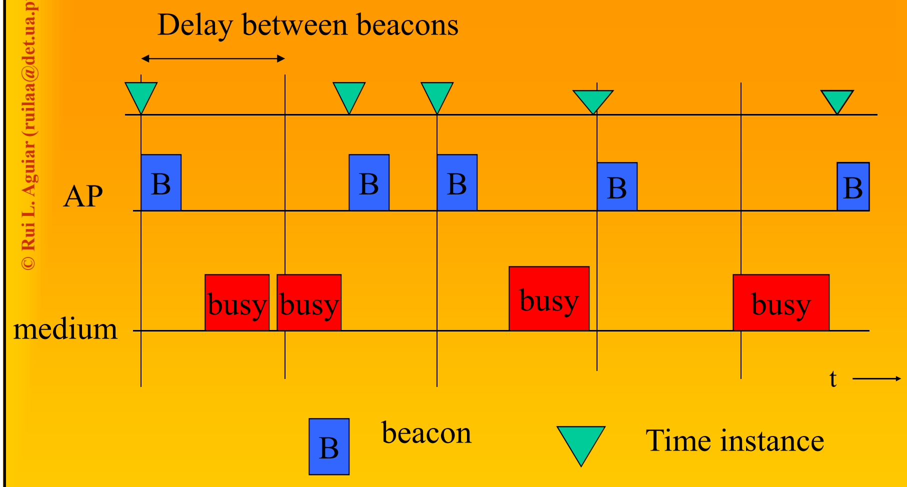
120

Synchronization

- **Timing synchronization function (TSF)**
  - **Beacons of the AP are sent in well-defined instants.**
  - **Content of packet is the exact instant when it goes to the network.**
- **Used also for power management**
  - **All clocks of all stations ins the BSS are synchronized**
    - This allows STA to wake-up to check if packets exist.

121

Synchronization



122

Outline

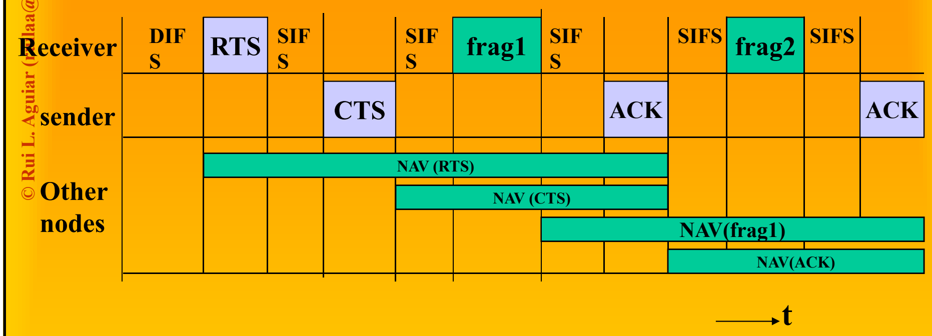
- **802.11 standard**
- **Physical layer**
- **MAC**
  - ➢ **DCF**
  - – **PCF**
- **Advanced MAC functions**

Some More MAC Features

- Use of RTS/CTS is controlled by an RTS threshold
  - RTS/CTS is only used for data packets longer than the RTS threshold
  - Pointless to use RTS/CTS for short data packets – high overhead!
- Number of retries is limited by a Retry Counter
  - Short retry counter: for packets shorter than RTS threshold
  - Long retry counter: for packets longer than RTS threshold
- Packets can be fragmented.
  - Each fragment is acknowledged
  - But all fragments are sent in one sequence
  - Sending shorter frames can reduce impact of bit errors
  - Lifetime timer: maximum time for all fragments of frame

124

Fragmentation



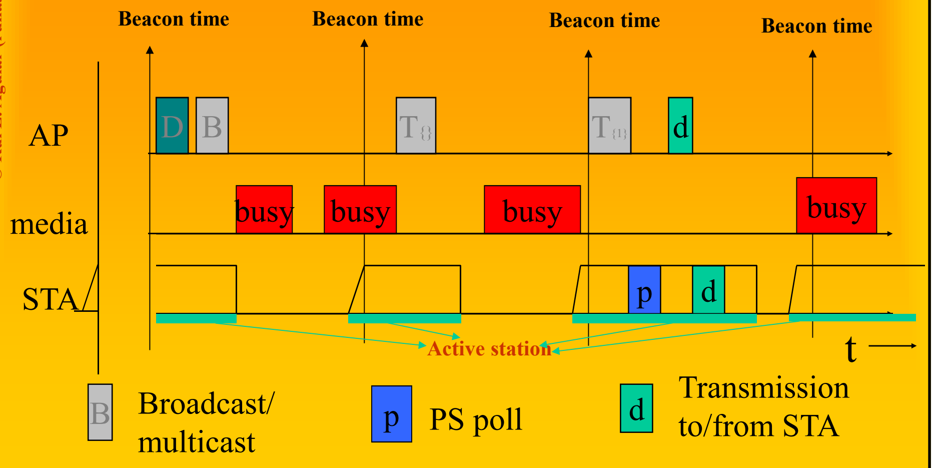
125

Power management (infrastructure)

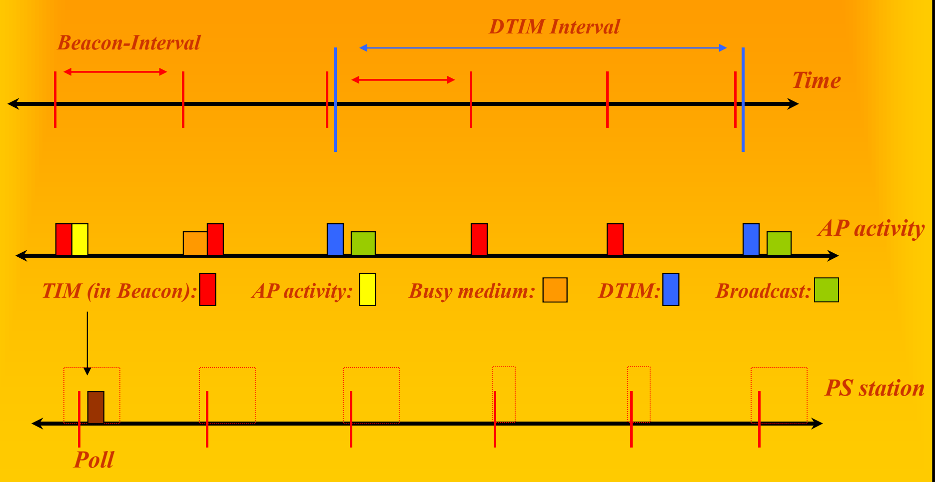
- APs buffer packets to PowerSaving stations
  - APs announce in beacons which packets are waiting with the TIM (traffic indication Map)
  - Broadcast/multicast frames are also buffered at AP
    - Sent after beacons, same common timing period.
    - Uses Delivery Traffic Indication Map (DTIM)
    - AP controls DTIM interval
- STA in power save wake periodically to listen for beacons
  - If it has data pending, send a PS-Poll
  - AP sends buffered data to this PS-poll
- TSF (Timing Synchronization Function) assures AP and stations are synchronized
  - Synchronizes clocks of the nodes in the BSS

126

Power management



Power Management and Broadcast



802.11 MAC discussion

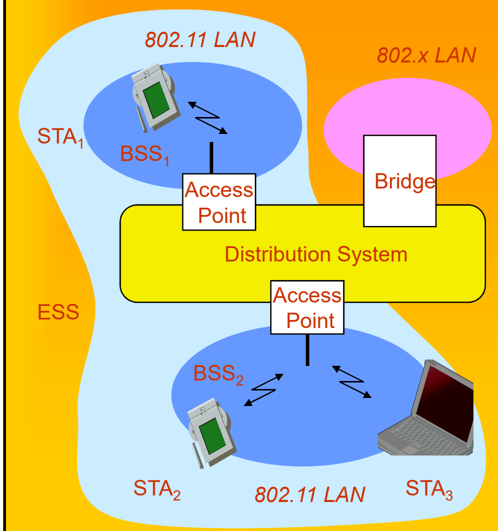
- Antenna diversity is very common
  - Can significantly reduce the effect of multipath
- RTS/CTS is almost never used
  - Overhead is too high compared with benefit
- Two key parameters are the transmit power and the Clear Channel Assessment (CCA) threshold
  - The two parameters have impact on the hidden and exposed terminal problem
  - With default settings, in most deployments, exposed terminals are a more common than hidden terminals

129

Control services at MAC

- **Synchronization, Roaming and Association**
  - Functions to find a network
  - Change APs
  - SearchAPs.
- **Power Management**
  - sleep mode without losing packets
  - Power management functions
- **MIB: Management information base**
- **Security: authentication and cypher**

802.11: Infrastructure Reminder



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

SSID

- **Mechanism used to segment wireless networks**
  - **Multiple independent wireless networks can coexist in the same location**
- **Each AP is programmed with a SSID that corresponds to its network**
- **Client computer presents correct SSID to access AP**
- **Security Compromises**
  - **AP can be configured to "broadcast" its SSID**
  - **Broadcasting can be disabled to improve security**
  - **SSID may be shared among users of the wireless segment**

132

Association Management: Scanning

- Scanning is needed to:
  - Find and connect to a networks
  - Find a new AP during roaming
- Passive Scanning:
  - Station simply listens for Beacon and get info of the BSS. Power is saved.
- Active Scanning:
  - Station transmits Probe Request; elicits Probe Response from AP. Saves time.

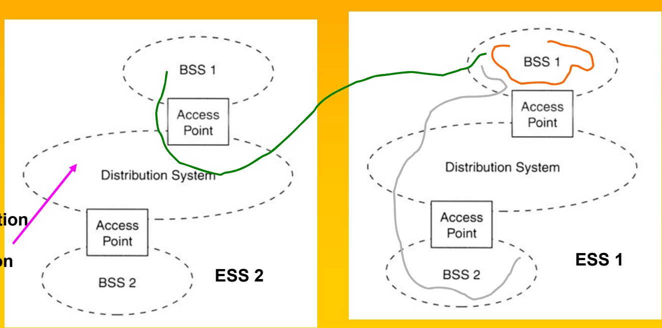
Association Management: Scanning, and Joining

- Station must associate with an AP before they can use the network
  - AP must know about them so it can forward packets
- Reassociation (roaming): association is transferred
  - Supports mobility in the same ESS
- Disassociation: station or AP can terminate association
- Stations can detect AP based by scanning.
- Joining a BSS
  - Synchronization in Timestamp Field and frequency :
  - Adopt PHY parameters
  - Other parameters: BSSID, WEP, Beacon Period, etc.

IEEE 802.11 Mobility

- Standard defines the following mobility types:
  - No-transition: no movement or moving within a local BSS
  - BSS-transition: station movies from one BSS in one ESS to another BSS within the same ESS
  - ESS-transition: station moves from a BSS in one ESS to a BSS in a different ESS (continuos roaming not supported)

- Address to destination mapping
- seamless integration of multiple BSS



135

© Rui L. Aguiar (ruilaa@det.ua.pt)

Roaming

- **Roaming: station changes network (BSS)**
- **STA may go:**
  - **Outside the coverage area of their AP**
  - **But still under the coverage area of another AP**

- **Reassociate the STA with the new AP allows the communication to continue**

136

© Rui L. Aguiar (ruilaa@det.ua.pt)

Roaming

- STA decides that the signal with the current AP is bad.
- STA does scanning (act/pas) to find new AP
- STA reassociate with the new AP (NAP)
  - Includes authorization.
- Without positive answer
  - STA does new scan
- With positive answer:
  - STA changed network to the new NAP
  - AP informs the ESS of the new association
  - Information in the distributed system is always updated.