**UNIT 3**

**Objectives :**

* To understand the different IEEE networks such as WLANs, Bluetooth
* To understand about the each layers of these two networks

**WLAN advantages**

* **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere .Sometimes wiring is difﬁcult if ﬁrewalls separate buildings. Penetration of a ﬁrewall is only permitted at certain points to prevent ﬁre from spreading too fast.
* **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans. As long as devices follow the same standard, they can communicate. For wired networks, additional cabling with the right plugs and probably interworking units (such as switches) have to be provided.
* **Design:** Wireless networks allow for the design of small, independent devices which can for example be put into a pocket. Cables not only restrict users but also designers of small PDAs, notepads etc.
* **Robustness:** Wireless networks can survive disasters, e.g., earthquakes or users pulling a plug. If the wireless devices survive, people can still communicate. Networks requiring a wired infrastructure will usually break down completely.
* **Cost:** After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a wireless network will not increase the cost. This is, important for e.g., lecture halls, hotel lobbies or gate areas in airports where the numbers using the network may vary significantly. Using a ﬁxed network, each seat in a lecture hall should have a plug for the network although many of them might not be used permanently.

**WLAN Disadvantages**

• **QoS:** WLANs offer typically lower QoS. Lower bandwidth due to limitations in radio transmission (1- 10 Mbit/s) and higher error rates due to interference

• **Proprietary solutions**: slow standardization procedures lead to many proprietary solutions only working in an homogeneous environment

• **Safety and security:** using radio waves for data transmission might interfere with other high-tech equipment

• **Restrictions:** All wireless products have to comply with national regulations. Several government and non-government institutions worldwide regulate the operation and restrict frequencies to minimize interference. Consequently, it takes a very long time to establish global solutions like, e.g., IMT-2000, which comprises many individual standards .WLANs are limited to low-power senders and certain license-free frequency bands, which are not the same worldwide.

**WLAN Design Goals:**

• **Global operation:** LAN equipment may be carried from one country to another and this operation should be legal (frequency regulations national and international).

• **Low power:** take into account that devices communicating via WLAN are typically running on battery power. The LAN design should take this into account and implement special power-saving modes and power management functions.

● **License-free operation:** LAN operators do not want to apply for a special license to be able to use the product. The equipment must operate in a license-free band, such as the 2.4 GHz ISM band.

● **Robust transmission technology:** Compared to their wired counterparts, WLANs operate under difficult conditions. If they use radio transmission, many other electrical devices can interfere with them (vacuum cleaners, hairdryers, train engines etc.).

• **Simplified spontaneous co-operation:** no complicated setup routines but operate spontaneously after power-up.

**• Easy to use:** WLANs are made for simple users, they should not require complex management but rather work on a plug-and-play basis.

• **Protection of investment:** a lot of money has been invested for wired LANs, WLANs should be able to interoperate with existing network (same data type and services).

• **Safety and security:** safe to operate. Encryption mechanism, do not allow roaming profiles for tracking people (privacy)

• **Transparency for applications:** existing applications should continue to work.

**Basic transmission technologies for WLANs**

**Infrared (lR) LANs :**.

Optical wireless communication in the infrared portion of the spectrum is in most of homes, where it is used for a variety of remote control devices. Version 1.0 of this industry standard implements data rates of up to 115 kbit/s, while IrDA 1.1 deﬁnes higher data rates of 1.152 and 4 Mbit/s.

Strengths:

* Spectrum virtually unlimited & Extremely high data rates
* Infrared shares some properties of visible light
* Diffusely reflected by light-colored objects
* Use ceiling reflection to cover entire room
* Does not penetrate walls or other opaque objects
* More easily secured against eavesdropping than microwave
* Separate installation in every room without interference
* Inexpensive and simple
* Uses intensity modulation, so receivers need to detect only amplitude

Weaknesses:

Many consumption indoor environments experience background radiation, from sunlight and indoor lighting. This ambient radiation appears as noise in an infrared receiver requiring higher power and limiting range. Power limited by concerns of eye safety and power .

**Radio Transmisssion**

• The main advantages of radio transmission:

– Long-term experience for wide area networks and mobile cellular phones

– Can cover larger area and can penetrate walls, furniture..

– Does not need LOS

– Current radio-based products offer higher transmission rates (e.g., 54 Mbit/s)

• The main disadvantages of radio transmission:

– Shielding is not simple(this is also the main advantage), radio transmission can interfere with other senders or electrical devices can destroy data transmitted

– It is only permitted in certain frequency bands

– Very limited ranges of license-free bands are available but they are not the same in all countries

**Wireless network structures**

**Infrastructure-based wireless network**

• Communication typically takes place only between the wireless nodes and the access point. Not directly between the wireless nodes.

• Access point: acts as a bridge

• Access points with a fixed network can connect several wireless networks to form a larger network beyond the actual radio coverage

• Design is simpler because most of the network functionality lays within the access point

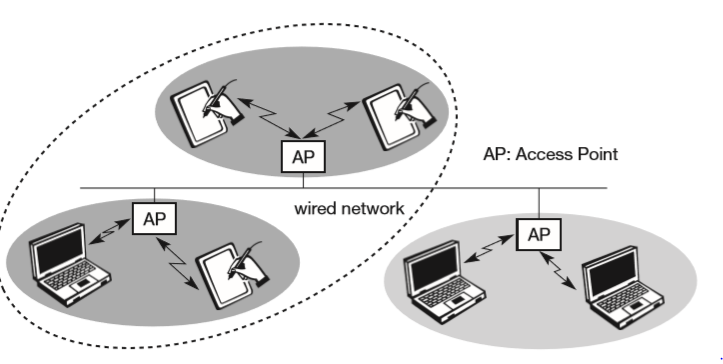
• Collision may occur if medium access of the wireless node and the access point is not coordinated

• Useful for Qos garantees such as minimum bandwidth for certain nodes

• Lose some of the flexibility wireless networks can offer, they cannot be used for disaster relief

• Cellular phone are typically infrastructure-based networks for wide area

• Also satellite-based cellular phone have an infrastructure (the satellites)



**Ad hoc wireless networks**

• Do not need any infrastructure to work

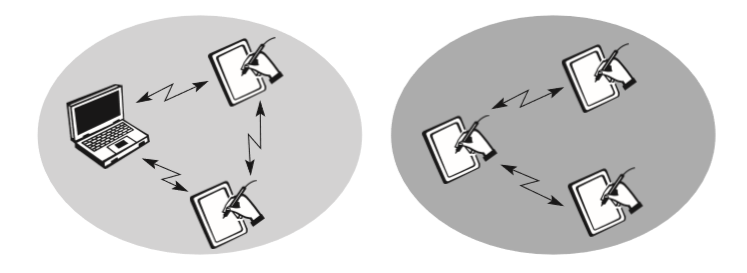
• Each node can directly communicate with another node

• Nodes can only communicate if they reach each other physically (if they are within each other’s radio range) or if other nodes can forward the message.

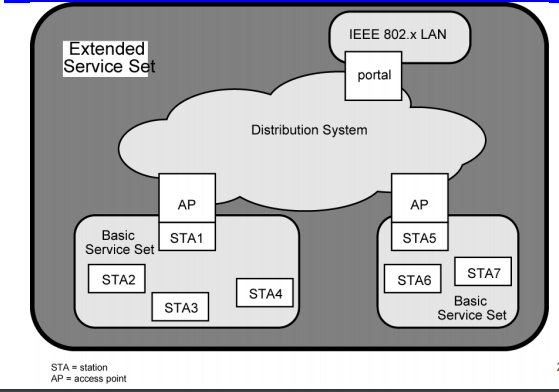
• The complexity of each node is higher: medium access mechanisms, priority mechanisms to provide a certain QoS

• Exhibits the greatest possible flexibility (unexpected meetings, communication scenario far away from any infrastructure)

• Ad hoc networks might only have selected nodes with the capabilities of forwarding data. Most of the node have to connect first to a special node in order to transmit data to the receiver if it is out of their range

****

**IEEE 802.11 Architecture**



• Defines the characteristics of the physical layer (PHY) and medium access control layer (MAC) for wireless LAN

• Provide the same interface to higher layers as the others in order to maintain interoperability

• The 2.4 GHz ISM band was chosen for the standard, which is available in most countries around the world

• The original standard sets the access rate of 1 and 2 Mbps. The extension 802.11b define the access rate of 5.5 and 11 Mbps Network configuration

**Network configurations:**

– Ad-Hoc (peer to peer)

– Infrastructure

• Cell = Base Service Set (BSS): 1 Base station required

– Extended

• multi-cell service = Extended Service Set (ESS): Base station is connected to wired backbones, or support the bridge function to other BSS

• requires handoff management

**Basic Service Set (BSS)**

**•** The basic building block of WLAN is the **BSS**

• BSS represents the coverage area where two or more stations (called **STAi)** communicate through a set of functions via the wireless connection

• A synonim of BSS is Ad Hoc Network

**Extended Service Set (ESS)**

• A **BSS** may be part of a extended network that is build connecting multiple AdHoc networks with a named **Distribution System (DS)**

• The **DS** may consist of wired and/or wireless connections

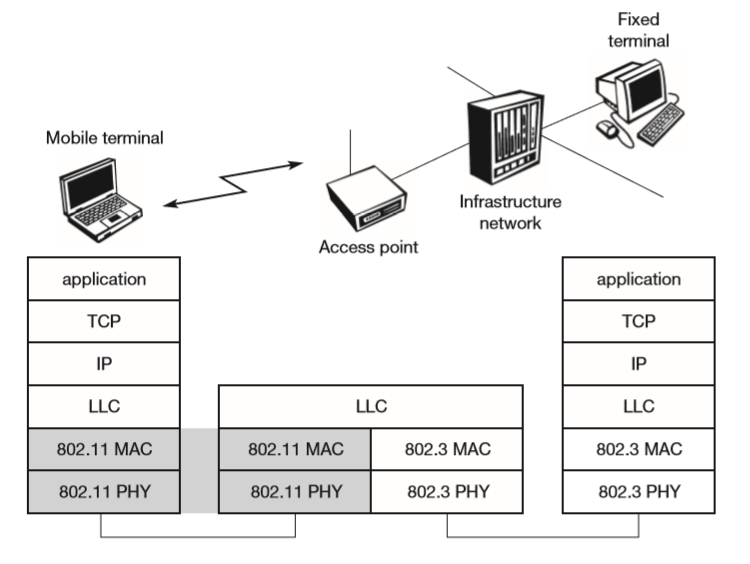
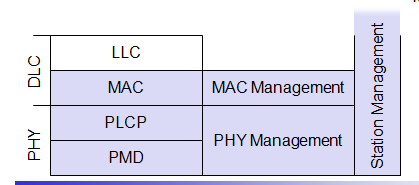
• Inside each BSS, the station Adapter connecting the BSS to the DS is named **Access Point (AP).**

• The DS and BSSs allow to create a wireless network of arbitrary size and complexity: **ESS**

• To access a wired network from the wireless one, the communication has to go through a portal which provides the integration between the two communication systems

• The **portal** (that could be integrated in the functionality of an AP) forms the internetworking unit to other LANs

**Protocol architecture**

• The IEEE 802.11 fits into other standards for wired LANs

• The most common scenario is that of a IEEE 802.11 wireless LAN connected to an IEEE 802.3 Ethernet via a bridge

• Applications should not notice any differences. The higher layers (application, TCP, IP) look the same for the wireless node as for the wired node

• The upper part of the data link control layer, the Logical Link Control (LCC) covers the differences of the Medium Access Control (MAC) layers needed for the different media IEEE 802.

• The standard only covers the PHY layer and the MAC layer

• The PHY is subdivided into a physical layer convergence protocol (PLCP) and the physical medium dependent sub-layer (PMD)

• PLCP provides a carrier sense signal called clear channel signal (CCA) and a common PHY service access point (SAP) independent of the transmission technology

• PMD handles modulation and encoding/decoding of signals

• The MAC management supports the association and re-association of a STA to an AP and roaming between different AP

• controls authentication mechanisms, encryption, synchronization of a STA with regard to an AP

• Controls power management to save battery power

**Physical layer**

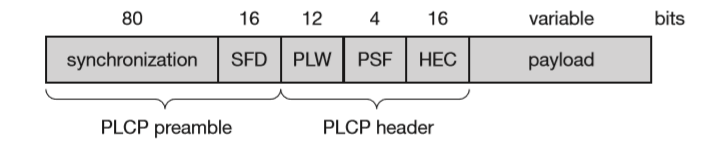
• Three different physical layers: one layer based on infrared and two layers based on radio transmission

• All layers including the provision of the clear channel assessment (CCA) signal and a service acess provider (SAP)

• The CCA signal is needed for the MAC mechanism controlling medium access and indicates if the medium is currently idle

• The SAP give to the MAC layer a transfer rate of 1 or 2 Mbps

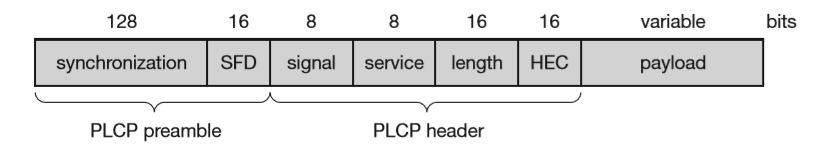
1. **FHSS (Frequency Hopping Spread Spectrum)**
   * spreading, de-spreading, signal strength, typ. 1 Mbit/s
   * 79 hopping channels for North America and Europe, and 23 hopping channels for Japan (each with a bandwidth of 1 MHz
   * A 2 level GFSK for 1 Mbit/s(i.e., 1 bits) , a 4 level GFSK for 2 Mbit/s (i.e., 2 bits are mapped to one frequency).
   * min. 2.5 frequency hops/s (USA)



* **Synchronization:** The PLCP preamble starts with 80 bit synchronization, which is a 010101... bit pattern. This pattern is used for synchronization of potential receivers and signal detection by the CCA.
* SFD (Start Frame Delimiter): The following 16 bits indicate the start of the frame and provide frame synchronization. The SFD pattern is 0000110010111101.
* PLW (PLCP\_PDU Length Word): This first field of the PLCP header indicates the length of the payload in bytes including the 32 bit CRC at the end of the payload. PLW can range between 0 and 4,095.
* PSF (PLCP Signaling Field): All bits set to zero (0000) indicates the lowest data rate of 1 Mbit/s. The granularity is 500 kbit/s, thus 2 Mbit/s is indicated by 0010 and the maximum is 8.5 Mbit/s (1111). This system obviously does not accommodate today’s higher data rates
* HEC (Header Error Check) : CRC with x16+x12+x5+1

**DSSS (Direct Sequence Spread Spectrum)**

* + DBPSK modulation for 1 Mbit/s (Differential Binary Phase Shift Keying), DQPSK for 2 Mbit/s (Differential Quadrature PSK)
  + preamble and header of a frame is always transmitted with 1 Mbit/s, rest of transmission 1 or 2 Mbit/s
  + chip sequence (11 symbols) : +1, -1, +1, +1, -1, +1, +1, +1, -1, -1, -1 (Barker code)
  + max. radiated power 1 W (USA), 100 mW (EU), min. 1mW nfrared
  + carrier detection, energy detection, synchronization



* Synchronization:
  + synch., gain setting, energy detection, frequency offset compensation
* SFD (Start Frame Delimiter): This 16 bit ﬁeld is used for synchronization at the beginning of a frame and consists of the pattern 1111001110100000.
* Signal: data rate of the payload (0x0A: 1 Mbit/s DBPSK; 0x14: 2 Mbit/s DQPSK)
* Service : future use, 00: 802.11 compliant
* Length : length of the payload
* HEC (Header Error Check): protection of signal, service and length, x16+x12+x5+1

**802.11 Medium Access Control**

Traffic services

* + Asynchronous Data Service (mandatory)
    - exchange of data packets based on “best-effort”
    - support of broadcast and multicast
  + Time-Bounded Service (optional)
    - implemented using PCF (Point Coordination Function)

Access methods

* + DFWMAC-DCF CSMA/CA (mandatory)
    - collision avoidance via randomized „back-off“ mechanism
    - minimum distance between consecutive packets
    - ACK packet for acknowledgements (not for broadcasts)
  + DFWMAC-DCF w/ RTS/CTS (optional)
    - Distributed Foundation Wireless MAC
    - avoids hidden terminal problem
  + DFWMAC- PCF (optional)
    - access point polls terminals according to a list

**Priorities**

**Inter-Frame Spacing (IFS)** Inter-Frame Spacing refers to the time interval between the transmission of successive frames by any station. There are four types of IFS: SIFS, PIFS, DIFS, and EIFS, in order from shortest to longest. They denote priority levels of access to the medium. Shorter IFS denotes a higher priority to access the medium, because the wait time to access the medium is lower. The exact values of the IFS are obtained from the attributes specified in the Physical Layer Management Information Base (PHYMIB) and are independent of the station bit rate.

**• Short Inter-Frame Spacing (SIFS)** is the shortest of all the IFSs and denotes highest priority to access the medium. It is defined for short control messages such as acknowledgments for data packets and polling responses. The transmission of any packet should begin only after the channel is sensed to be idle for a minimum time period of at least SIFS.

• **PCF Inter-Frame Spacing (PIFS)** is the waiting time whose value lies between SIFS and DIFS. This is used for real-time services.

• **DCF Inter-Frame Spacing (DIFS)** is used by stations that are operating under the DCF mode to transmit packets. This is for asynchronous data transfer within the contention period.

**• Extended Inter-Frame Spacing (EIFS)** is the longest of all the IFSs and denotes the least priority to access the medium. EIFS is used for resynchronization whenever physical layer detects incorrect MAC frame reception.

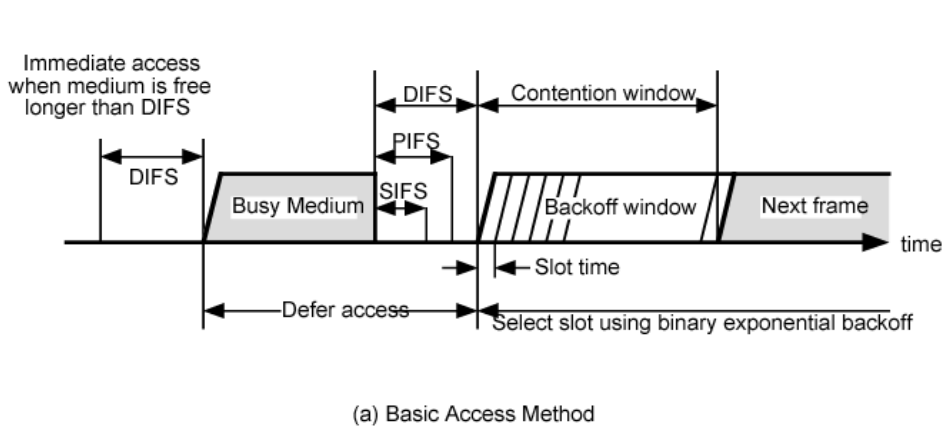
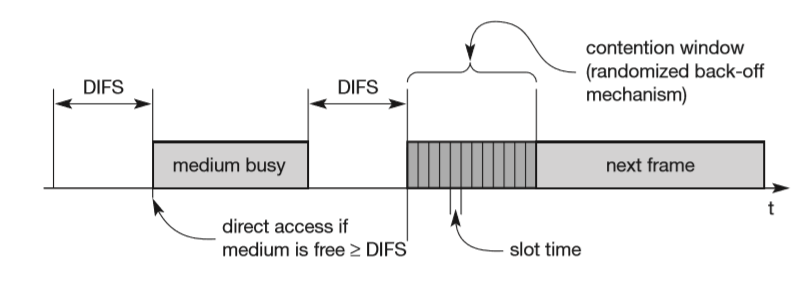


Fig: IEEE 802.11 MAC Timing Basic Access Method

1. **Basic DFWMAC-DCF using CSMA/CA**

****

* + If the medium is idle for at least the duration of DIFS (with the help of the CCA signal of the physical layer), a node can access the medium at once. This allows for short access delay under light load. But as more and more nodes try to access the medium, additional mechanisms are needed. station ready 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, then the station must additionally wait a random back-off time (collision avoidance, multiple of slot-time) CW = 7, 15, 31, 63, 127
  + if another station occupies the medium during the back-off time of the station, the back-off timer stops (fairness)

**Binary Exponential Backoff**

* Stations choose their backoff time randomly from contention Window
* Ideal contention window size is trade-off between acceptable load and experienced delay
* Initial contention window size (CWmin) is 7 slots (backoff time between 0 and 7)
* After collision (no ack), contention window is “doubled” until Cwmax = 255 is reached: 7 -> 15 -> 31 -> 63 -> 127 -> 255

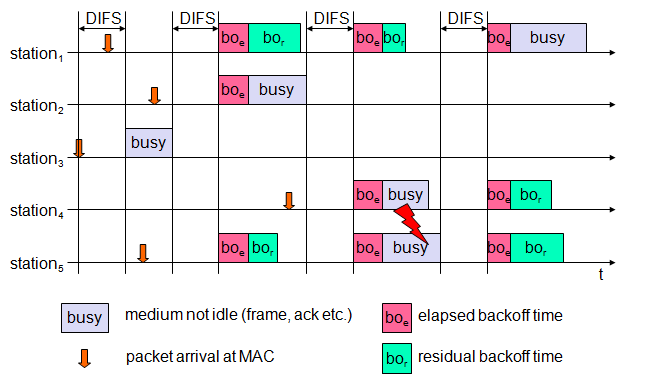
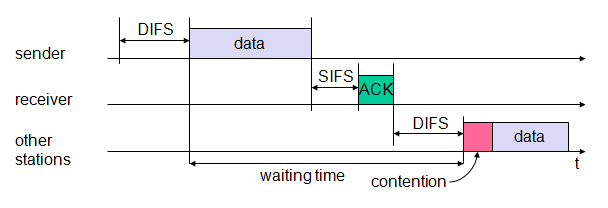
****

Fig: 802.11 - competing stations - simple version (no RTS/CTS)

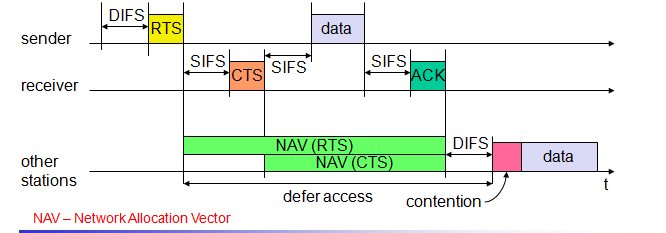
* Figure explains the basic access mechanism of IEEE 802.11 for five stations trying to send a packet at the marked points in time.
* Station3 has the ﬁrst request from a higher layer to send a packet. The station senses the medium, waits for DIFS and accesses the medium, i.e., sends the packet.
* Station1, station2, and station5 have to wait at least until the medium is idle for DIFS again after station3 has stopped sending. Now all three stations choose a backoff time within the contention window and start counting down their backoff timers.
* The random backoff time of station1 as sum of boe (the elapsed backoff time) and bor (the residual backoff time). The same is shown for station5. Station2 has a total backoff time of only boe and gets access to the medium ﬁrst. No residual backoff time for station2 is shown.
* The backoff timers of station1 and station5 stop, and the stations store their residual backoff times.
* While a new station has to choose its backoff time from the whole contention window, the two old stations have statistically smaller backoff values. The older values are on average lower than the new ones.
* Now station4 wants to send a packet as well, so after DIFS waiting time, three stations try to get access. It can now happen, that two stations accidentally have the same backoff time, no matter whether remaining or newly chosen. This results in a collision on the medium as shown, i.e., the transmitted frames are destroyed. Station1 stores its residual backoff time again. In the last cycle shown station1 finally gets access to the medium, while station4 and station5 have to wait. A collision triggers a retransmission with a new random selection of the backoff time.

Sending unicast packets

* + station has to wait for DIFS before sending data
  + receivers acknowledge at once (after waiting for SIFS) if the packet was received correctly
  + automatic retransmission of data packets in case of transmission errors

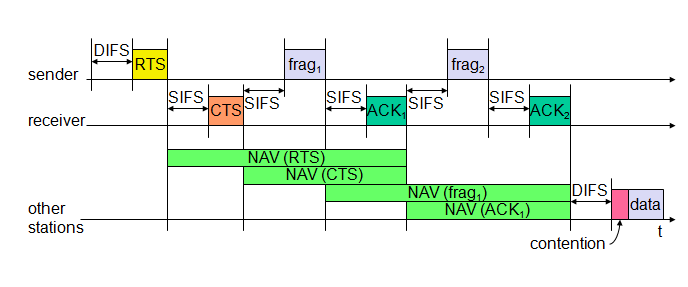


1. **DFWMAC-DCF with RTS/CTS extension**

****

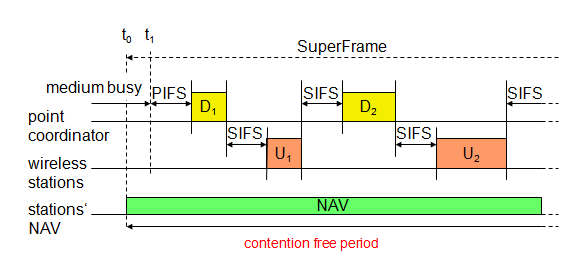
* Figure illustrates the use of RTS and CTS. After waiting for DIFS (plus a random backoff time if the medium was busy), the sender can issue a request to send (RTS) control packet. The RTS packet includes the receiver of the data transmission to come and the duration of the whole data transmission. This duration specifies the time interval necessary to transmit the whole data frame and the acknowledgement related to it. Every node receiving this RTS now has to set its net allocation vector (NAV) in accordance with the duration field
* If the receiver of the data transmission receives the RTS, it answers with a clear to send (CTS) message after waiting for SIFS. This CTS packet contains the duration ﬁeld again and all stations receiving this packet from the receiver of the intended data transmission have to adjust their NAV.
* Now all nodes within receiving distance around sender and receiver are informed that they have to wait more time before accessing the medium. Basically, this mechanism reserves the medium for one sender exclusively (this is why it is sometimes called a virtual reservation scheme).
* Finally, the sender can send the data after SIFS. The receiver waits for SIFS after receiving the data packet and then acknowledges whether the transfer was correct. The transmission has now been completed, the NAV in each node marks the medium as free and the standard cycle can start again.

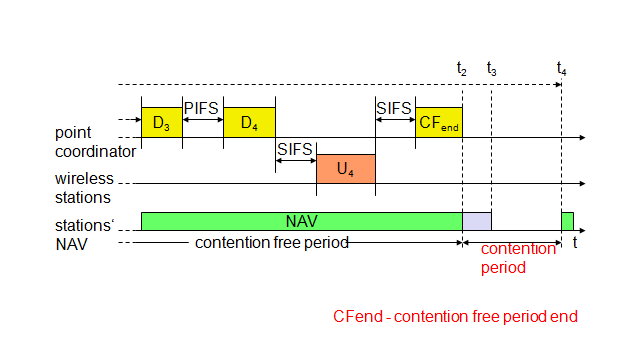
When frames are fragmented into small frames



* Again, a sender can send an RTS control packet to reserve the medium after a waiting time of DIFS. This RTS packet now includes the duration for the transmission of the ﬁrst fragment and the corresponding acknowledgement. A certain set of nodes may receive this RTS and set their NAV according to the duration ﬁeld.
* The receiver answers with a CTS, again including the duration of the transmission up to the acknowledgement. A set of receivers gets this CTS message and sets the NAV.
* The sender can now send the ﬁrst data frame, frag1, after waiting only for SIFS. The new aspect of this fragmentation mode is that it includes duration ﬁeld reserves the medium for the duration of the transmission following, comprising the second fragment and its acknowledgement.
* Again, several nodes may receive this reservation and adjust their NAV.
* The receiver of frag1 answers directly after SIFS with the acknowledgement packet ACK1 including the reservation for the next transmission as shown. Again, a set of nodes may receive this reservation and adjust their NAV (If frag2 was not the last frame of this transmission, it would also include a new duration for the third consecutive transmission. (In the example shown, frag2 is the last fragment of this transmission so the sender does not reserve the medium any longer.) The receiver acknowledges this second fragment, not reserving the medium again. After ACK2, all nodes can compete for the medium again after having waited for DIFS.

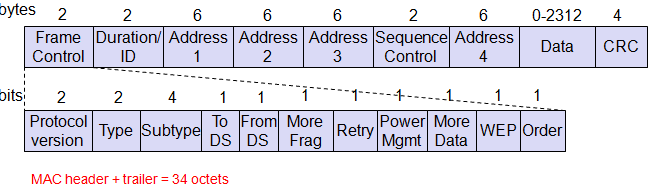
1. **Point Coordination Function (PCF) with polling :**

****

****

* The two access mechanisms presented so far cannot guarantee a maximum access delay or minimum transmission bandwidth. To provide a time-bounded service, the standard specifies a point coordination function (PCF) on top of the standard DCF mechanisms. Using PCF requires an access point that controls medium access and polls the single nodes. The point co-ordinator in the access point splits the access time into super frame periods
* A super frame comprises a contention-free period and a contention period. The contention period can be used for the two access mechanisms presented above. At time t0 the contention-free period of the super frame should theoretically start, but another station is still transmitting data (i.e., the medium is busy).
* After the medium has been idle until t1, the point coordinator has to wait for PIFS before accessing the medium. As PIFS is smaller than DIFS, no other station can start sending earlier.
* The point coordinator now sends data D1 downstream to the first wireless station. This station can answer at once after SIFS .
* After waiting for SIFS again, the point coordinator can poll the second station by sending D2. This station may answer upstream to the coordinator with data U2. Polling continues with the third node.
* This time the node has nothing to answer and the point coordinator will not receive a packet after SIFS. After waiting for PIFS, the coordinator can resume polling the stations.
* Finally, the point coordinator can issue an end marker (CFend), indicating that the contention period may start again. Using PCF automatically sets the NAV, preventing other stations from sending.
* In the example, the contention-free period planned initially would have been from t0 to t3. However, the point coordinator ﬁnished polling earlier, shifting the end of the contention-free period to t2. At t4, the cycle starts again with the next super frame.

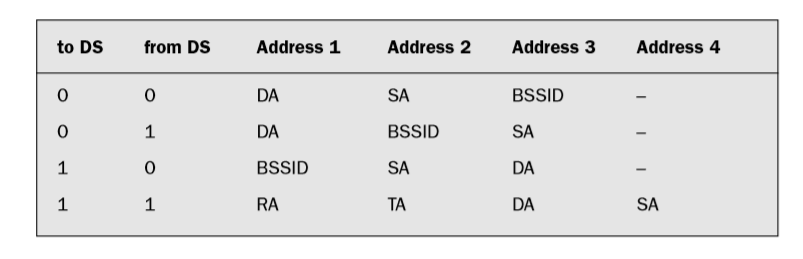
**IEEE 802.11 MAC Frame Format**

****

* **Duration/ID**: the duration field contains the value indicating the period of time in which the medium is occupied (in µs).
* **Address 1 to 4:** The four address fields contain standard IEEE 802 MAC addresses (48 bit each),
* **Sequence control:** Due to the acknowledgement mechanism frames may be duplicated. Therefore a sequence number is used to ﬁlter duplicates.
* **Data:** The MAC frame may contain arbitrary data (max. 2,312 byte), which is transferred transparently from a sender to the receiver(s).
* **Checksum (CRC):** Finally, a 32 bit checksum is used to protect the frame as it is common practice in all 802.x networks.

The frame control ﬁeld shown in Figure 7.16 contains the following ﬁelds:

* **Protocol version**: This 2 bit ﬁeld indicates the current protocol version and is ﬁxed to 0 by now
* **Type:** The type field determines the function of a frame: management (=00), control (=01), or data (=10). The value 11 is reserved.
* **Subtype:** Example subtypes for management frames are: 0000 for association request, 1000 for beacon. RTS is a control frame with subtype 1011, CTS is coded as 1100. User data is transmitted as data frame with subtype 0000.
* **More fragments:** This field is set to 1 in all data or management frames that have another fragment of the current MSDU to follow.
* **Retry:** If the current frame is a retransmission of an earlier frame, this bit is set to 1.
* **Power management:** This field indicates the mode of a station after successful transmission of a frame. Set to 1 the ﬁeld indicates that the station goes into power-save mode. If the ﬁeld is set to 0, the station stays active.
* **More data:** In general, this ﬁeld is used to indicate a receiver that a sender has more data to send than the current frame.
* **Wired equivalent privacy (WEP**): This field indicates that the standard security mechanism of 802.11 is applied. However, due to many weaknesses found in the WEP algorithm higher layer security should be used to secure an 802.11 network
* **Order:** If this bit is set to 1 the received frames must be processed in strict order.



DS: Distribution System

AP: Access Point

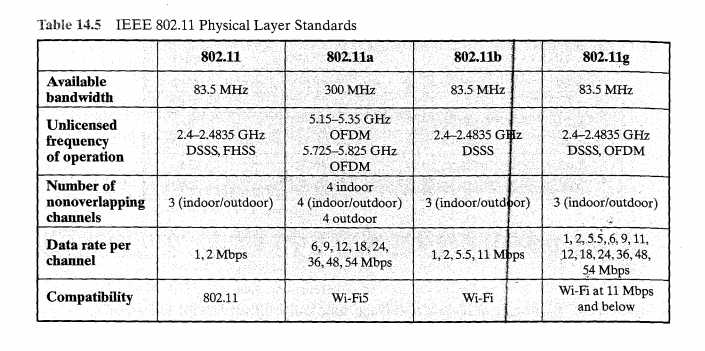
DA: Destination Address

SA: Source Address

BSSID: Basic Service Set Identifier

RA: Receiver Address (AP)

TA: Transmitter Address (AP)

****

**Bluetooth Overview:**

2.4 GHz ISM band, 79 (23) RF channels, 1 MHz carrier spacing

* + Channel 0: 2402 MHz … channel 78: 2480 MHz
  + G-FSK modulation, 1-100 mW transmit power

FHSS and TDD

* + Frequency hopping with 1600 hops/s
  + Hopping sequence in a pseudo random fashion, determined by a master
  + Time division duplex for send/receive separation

Voice link – SCO (Synchronous Connection Oriented)

* + FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched

Data link – ACL (Asynchronous ConnectionLess)

* + Asynchronous, fast acknowledge, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched

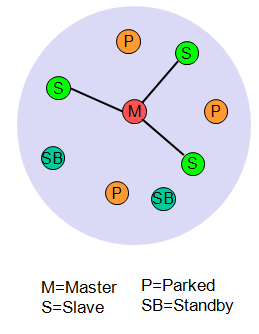
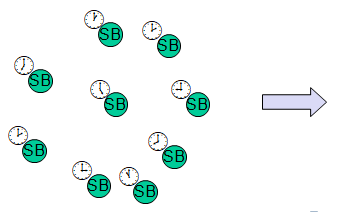
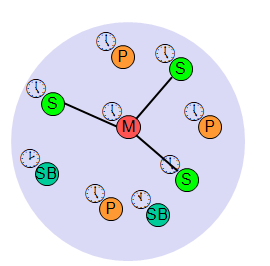
Topology: Overlapping piconets (stars) forming a scatternet

**Piconet**

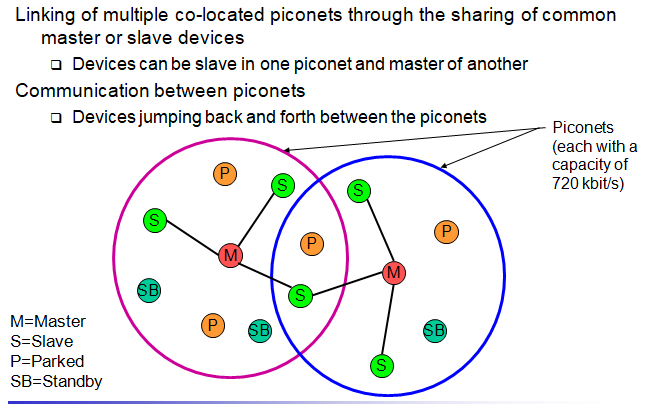
* Collection of devices connected in an ad hoc fashion
* One unit acts as master and the others as slaves for the lifetime of the piconet
* Master determines hopping pattern, slaves have to synchronize
* Each piconet has a unique hopping pattern
* Participation in a piconet = synchronization to hopping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

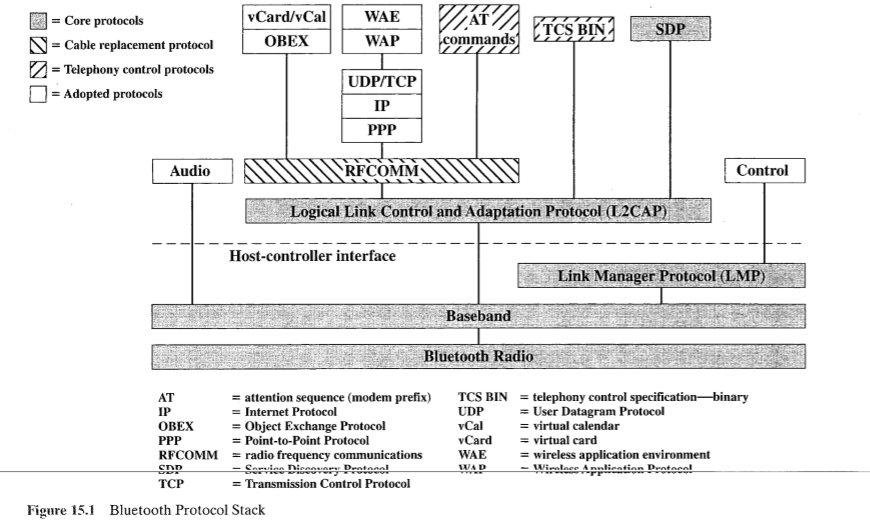
**FORMING A PICONET**

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

* Scatternet
* Device in one piconet may exist as master or slave in another piconet
* Allows many devices to share same area
* Makes efficient use of bandwidth
* Devices jumping back and forth between the piconets

****



* **Bluetooth is a layered protocol architecture**
  + **Core protocols**
  + **Cable replacement Protocol**
  + **Telephony control protocols**
  + **Adopted protocols**
* **Core protocols**
  + Radio
  + Baseband
  + Link manager protocol (LMP)
  + Logical link control and adaptation protocol (L2CAP)
  + Service discovery protocol (SDP)
* **Cable replacement protocol**
* RFCOMM=radio frequency communications which is a replacement of RS232 cable
* **Telephony control protocol**
* Telephony control specification – binary (TCS BIN)
* AT commands
* **Adopted protocols**
* PPP =Point-to-Point Protocol
* TCP/UDP/IP
* OBEX= Object Exchange Protocol
* WAE/WAP= wireless application environment/ wireless application Protocol

**Radio Specification:**

**Class 1:** Outputs 100 mW for maximum range, In this class, power control is mandatory This mode provides the greatest distance.

**Class 2:** Outputs 2.4 mW at maximum. Power control is optional.

**Class 3**: Lowest power. Nominal output is 1 mW.

**Base Band Specifications:**

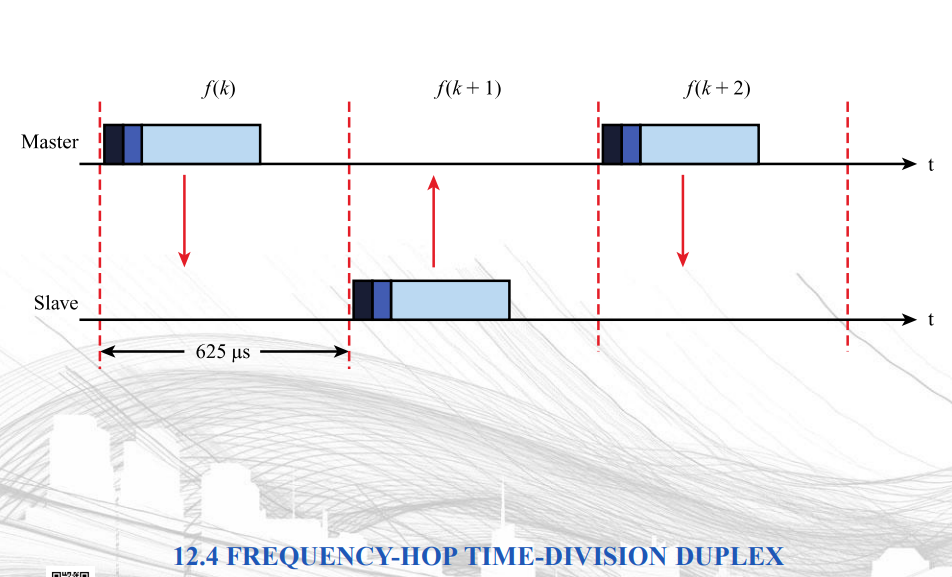
FREQUENCY HOPPING

* Total bandwidth divided into 1MHz physical channels
* FH occurs by jumping from one channel to another in pseudorandom sequence
* Hopping sequence shared with all devices on piconet
* Piconet access:

– Bluetooth devices use time division duplex (TDD)

– Access technique is TDMA

– FH-TDD-TDMA



PHYSICAL LINKS BETWEEN MASTER AND SLAVE

* Synchronous connection oriented (SCO)

– Allocates fixed bandwidth between point-to-point connection of master and slave

– Master maintains link using reserved slots

– Master can support three simultaneous links

* Asynchronous connectionless (ACL)

– Point-to-multipoint link between master and all slaves

– Only single ACL link can exist

* Extended Synchronous connection oriented (eSCO)

– Reserves slots just like SCO , But these can be asymmetric

– Retransmissions are supported

**LINK MANAGER**

* Manages various aspects of the radio link between a master and a slave
* Involves the exchange LMP PDUs (protocol data units)
* Procedures defined for LMP are grouped into 24 functional areas, which include

– Authentication

– Pairing

– Encryption

– Clock offset request

– Switch master/slave

– Name request

– Hold or park or sniff mode

* **Sniff state:** The sniff state has the highest power consumption of the low power states. Here, the device listens to the piconet at a reduced rate
* **Hold state:** The device does not release its AMA but stops ACL transmission. A slave may still exchange SCO packets. If there is no activity in the piconet, the slave may either reduce power consumption or participate in another piconet.
* **Park state:** In this state the device has the lowest duty cycle and the lowest power consumption. The device releases its AMA and receives a parked member address (PMA). The device is still a member of the piconet, but gives room for another device to become active (AMA is only 3 bit, PMA 8 bit).
* **standby State**: Every device, which is currently not participating in a piconet (and not switched off), is in standby mode.
* **Active state**: Devices which are actively participating in a piconet

**LOGICAL LINK CONTROL AND ADAPTATION PROTOCOL (L2CAP)**

* Provides a link-layer protocol between entities with a number of services
* Relies on lower layer for flow and error control
* Makes use of ACL links, does not support SCO links
* Provides two alternative services to upper-layer protocols

– Connection service

– Connection-mode service

**L2CAP LOGICAL CHANNELS**

* Connectionless

– Supports connectionless service

– Each channel is unidirectional

– Used from master to multiple slaves

* Connection-oriented

– Supports connection-oriented service

– Each channel is bidirectional

* Signalling – Provides for exchange of signalling messages between L2CAP entities