1.6 BRAN (BROADBAND RADIO ACCESS NETWORK)

The broadband radio access networks (BRAN), which have been standardized by the European Telecommunications Standards Institute (ETSI).

Many service providers experience problems getting access to customer's because the telephone infrastructure belongs to a few big companies. One possible technology to provide network access for customers is radio. The advantages of radio access are high flexibility and quick installation. Different types of traffic are supported, one can multiplex traffic for higher efficiency, and the connection can be asymmetrical.

Radio access allows for economic growth of access bandwidth. If more bandwidth is needed, additional transceiver systems can be installed easily. For wired transmission this would involve the installation of additional wires. The primary market for BRAN includes private customers and small to medium-sized companies with Internet applications, multi-media conferencing, and virtual private networks. The BRAN standard and IEEE 802.16 (Broadband wireless access, IEEE, 2002b) have similar goals.

BRAN has specified four different network types

- HIPERLAN 1: This high-speed WLAN supports mobility at data rates above 20 Mbit/s. Range is 50 m, connections are multi-point-to-multi-point using ad-hoc or infrastructure networks.
- HIPERLAN/2: This technology can be used for wireless access to ATM or IP networks and supports up to 25 Mbit/s user data rate in a point-to-multi-point configuration. Transmission range is 50 m with support of slow (< 10 m/s) mobility.
- HIPERACCESS: This technology could be used to cover the _last mile'to a customer via a fixed radio link, so could be an alternative to cable modems or xDSL technologies. Transmission range is up to 5 km, data rates of up to 25 Mbit/s are supported. However, many proprietary products already offer 155 Mbit/s and more, plus QoS.
- HIPERLINK: To connect different HIPERLAN access points or HIPER ACCESS nodes with a high-speed link, HIPERLINK technology can be chosen. HIPERLINK provides a fixed point-to-point connection with up to 155 Mbit/s.

BRAN technology is independent from the protocols of the fixed network. BRAN can be used for ATM and TCP/IP networks. Based on possibly different physical layers, the DLC layer of BRAN offers a common interface to higher layers. To cover special characteristics of wireless links and to adapt directly to different higher layer network technologies, BRAN provides a network convergence sublayer. This is the layer which canbe used by a wireless ATM network, Ethernet, Fire wire, or an IP network. In the case of BRAN as the RAL for WATM, the core ATM network would use services of the BRAN network convergence sublayer.

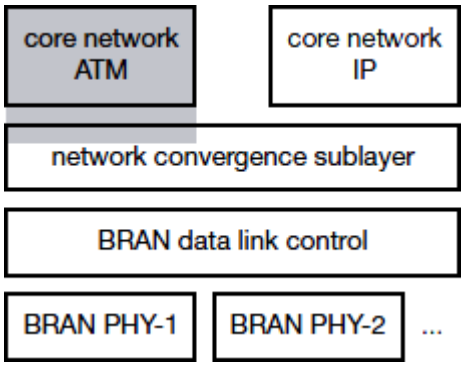


Fig. 1.19 Layered model of BRAN wireless access networks

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.7 HiperLAN2

It is a mobile short-range access network specified in the Broadband Radio Access Networks (BRAN) project chartered by the European Telecommunications Standards Institute (ETSI). Hyperlink/2, a competes directly with IEEE 802.11g/n, aka Wi-Fi.HiperLAN2 supports both asynchronous data and time critical services (e.g. packetized voice and video) that are bounded by specific time delays to achieve an acceptable Quality of Service (QoS) being developed under the auspices of the ETSI's Project BRAN (Broadband Radio Access Networks).

The HiperLAN2 standard is nearly identical to 802.11 in terms of its physical layers – both use OFDM technology to achieve their data rates, for instance – but is very different at the MAC (Media Access Control) level and in the way the data packets are formed and devices are addressed. On a technical level, whereas 802.11 can be viewed as true wireless Ethernet, HiperLAN2 is more akin to wireless Asynchronous Transfer Mode (ATM). It operates by sharing the 20MHz channels in the 5GHz spectrum in time, using Time Division Multiple Access (TDMA) to provide QoS through ATM-like mechanisms.

It supports two basic modes of operation: centralized mode and direct mode. The centralized mode is used in the cellular networking topology where each radio cell is controlled by an access point covering a certain geographical area. In this mode, a mobile terminal communicates with other mobile terminals or with the core network via an access point. It is mainly used in business applications – both indoors and outdoors – where an area much larger than a radio cell has to be covered. The direct mode is used in the ad-hoc networking topology – mainly in typical private home environments – where a radio cell covers the whole serving area.

1.7.1 Features of HiperLAN/2:

- High-speed transmission
- Connection-oriented
- Quality-of-Service (QoS) support ·
- Automatic frequency allocation
- Security support
- Mobility support
- Network & application independent
- Power save

1.7.2 High-speed transmission

HiperLAN/2 has a very high transmission rate, which at the physical layer extends up to 54 Mbit/s and on layer 3 up to 25 Mbit/s. To achieve this, Hyperlink/2 makes use of Orthogonal Frequency Digital Multiplexing (OFDM) to transmit the analogue signals. OFDM is very efficient in time-dispersive environments, e.g. within offices, where the transmitted radio signals are reflected from many points, leading to different propagation times before they eventually reach the receiver. Above the physical layer, the Medium Access Control (MAC) protocol is all new which implements a form of dynamic time-division duplex to allow for most efficient utilization of radio resources.

1.7.3 Connection-oriented

In a Hyperlink/2 network, data is transmitted between the MT and the AP that have been established prior to the transmission using signaling functions of the Hyperlink/2 control plane. Connections are time-division-multiplexed over the air interface. There are two types of connections, point to-point and point-to-multipoint.

Point-to-point connections are bidirectional whereas point-to-multipoint is unidirectional in the direction towards the Mobile Terminal. In addition, there is also a dedicated broadcast channel through which traffic reaches all terminals transmitted from one AP.

1.7.4 Quality of service support:

With the help of connections, support of QoS is much simpler. Each connection has its own set of QoS parameters (bandwidth, delay, jitter, bit error rate etc.). A more simplistic scheme using priorities only is available.

1.7.5Dynamic frequency selection:

In a Hyperlink/2 network, there is no need for manual frequency planning as in cellular networks like GSM. The radio base stations, which are called Access Points in HiperLAN/2, have a built-in support for automatically selecting an appropriate radio channel for transmission within each AP‘s coverage area. An AP listens to neighboring APs as well as to other radio sources in the environment, and selects an appropriate radio channel based on both what radio channels are already in use by those other APs and to minimize interference with the environment.

1.7.6 Security support

The HiperLAN/2 network has support for both authentication and encryption. With authentication both the AP and the MT can authenticate each other to ensure authorized access to the network (from the AP‘s point of view) or to ensure access to a valid network operator (from the MT‘s point of view). Authentication relies on the existence of a supporting function, such as a directory service, but which is outside the scope of HiperLAN/2. The user traffic on established connections can be encrypted to protect against for instance eaves-dropping and man-in-middle attacks.

1.7.7 Mobility support

Mobile terminals can move around while transmission always takes place between the terminal and the access point with the best radio signal. Handover between access points is performed automatically. If enough resources are available, all connections including their QoS parameters will be supported by a new access point after handover. However, some data packets may be lost during handover.

1.7.8 Application and network independence:

HiperLAN2 was not designed with a certain group of applications or networks in mind. Access points can connect to LANs running Ethernet as well as IEEE 1394 (Fire wire) systems used to connect home audio/video devices

1.7.9 Protocol architecture & the layers

In the protocol reference model for the HiperLAN/2 radio interface is depicted. The protocol stack is divided into a control plane part and a user plane part i.e. user plane includes functions for transmission of traffic over established connections, and the control plane includes functions for the control of connection establishment, release, and supervision. The HiperLAN/2 protocol has three basic layers; Physical layer (PHY), Data Link Control layer (DLC), and the Convergence layer (CL). At the moment, there is only control plane functionality defined within DLC.

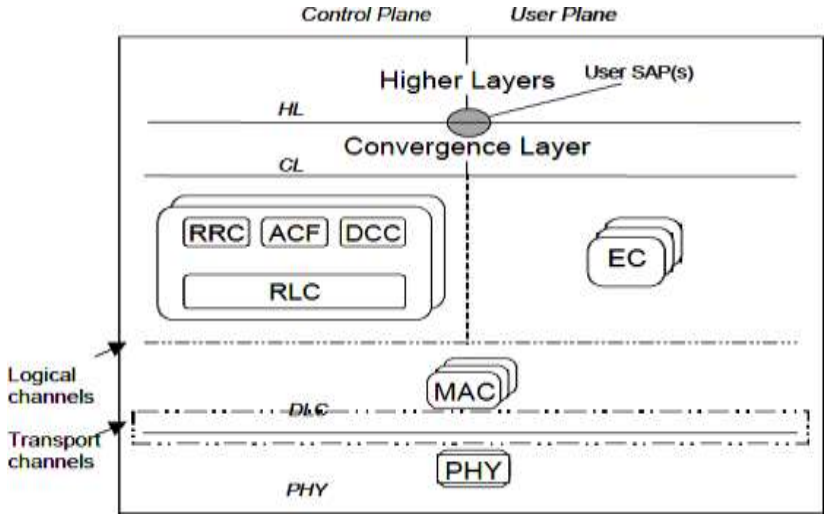


Fig. 1.20 HiperLAN/2 protocol reference model

[Source: Text book -Mobile Communications, Second Edition, Pearson Education bJoSchiller]

1.7.10 Physical Layer

The transmission format on the physical layer is a burst, which consists of a preamble part and a data part, where the latter could originate from each of the transport channels within DLC. The channel spacing is 20 MHz, which allows high bit rates per channel but still has a reasonable number of channels in the allocated spectrum.52 subcarriers are used per channel, where 48 subcarriers carry actual data and 4 subcarriers are pilots which facilitate phase tracking for coherent demodulation. The duration of the guard interval is equal to 800 ns, which is sufficient to enable good performance on channels with delay spread of up to 250 ns.

1.7.11 Data Link Control Layer

The Data Link Control (DLC) layer constitutes the logical link between an AP and the MTs. The DLC includes functions for medium access and transmission (user plane) as well as terminal/user and connection handling (control plane). Thus, the DLC layer consists of a set of sublayers: - Medium Access Control (MAC) protocol. - Error Control (EC) protocol - Radio Link Control (RLC) protocol with the associated signaling entities DLC Connection Control (DCC), the Radio Resource Control (RRC) and the Association Control Function (ACF)

Each MAC frame is further sub-divided into four phases with variable boundaries:

- Broadcast phase: The AP of a cell broadcasts the content of the current frame plus information about the cell (identification, status, resources).
- Downlink phase: Transmission of user data from an AP to the MTs.
- Uplink phase: Transmission of user data from MTs to an AP.
- Random access phase: Capacity requests from already registered MTs and access requests from non-registered MTs (slotted Aloha).

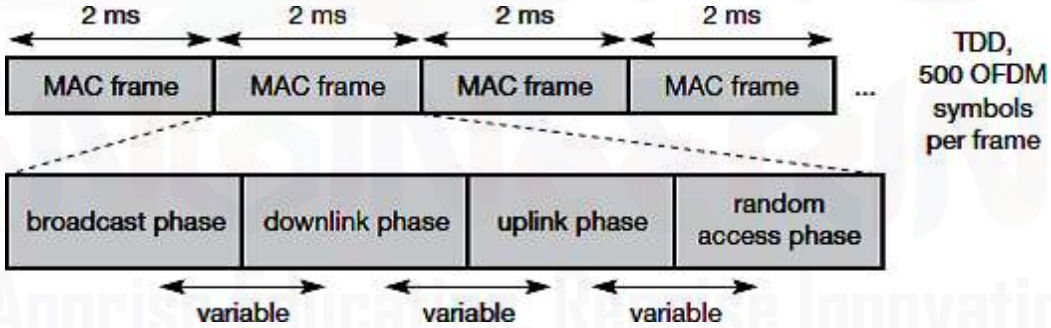


Fig. 1.21 HiperLAN2 MAC Frames

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Convergence Layer

The convergence layer (CL) has two main functions: adapting service request from higher layers to the service offered by the DLC and to convert the higher layer packets (SDUs) with variable or possibly fixed size into a fixed size that is used within the DLC. The padding, segmentation and reassembly function of the fixed size DLC SDUs is one key issue that makes it possible to standardize and implement a DLC and PHY that is independent of the fixed network to which the HiperLAN/2 network is connected. The generic architecture of the CL makes HiperLAN/2 suitable as a radio access network for a diversity of fixed networks, e.g. Ethernet, IP, ATM, UMTS, etc. There are currently two different types of CLs defined; cell-based and packet-based. The former is intended for interconnection to ATM networks, whereas the latter can be used in a variety of configurations depending on fixed network type and how the interworking is specified.

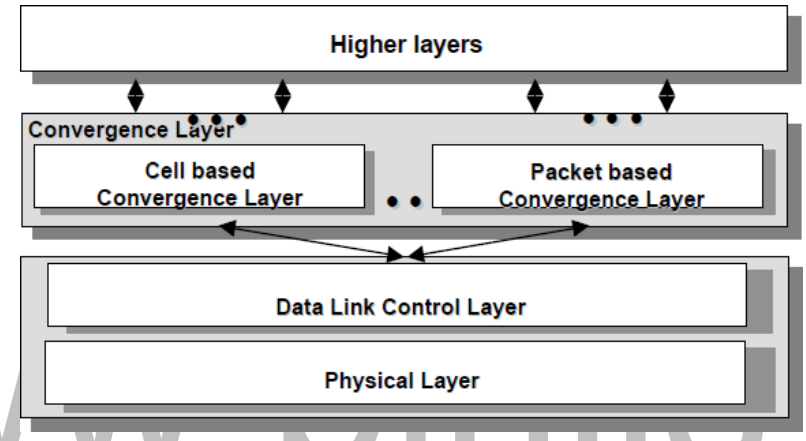


Fig. 1.22 Convergence layer

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.7.12 Modes of Operation

HiperLAN2 networks can operate in two different modes (which may be used simultaneously in the same network).

- Centralized mode (CM): All APs are connected to a core network and MTs are associated with APs. Even if two MTs share the same cell, all data is transferred via the AP. In this mode the AP will takes complete control of everything.
- Direct mode (DM): Data is directly exchanged between MTs if they can receive each other, but the network still has to be controlled. This can be done via an AP that contains a central controller (CC) anyway or via an MT that contains the CC functionality. There is no real difference between an AP and a CC besides the fact that APs are always connected to an infrastructure but here only the CC functionality is needed. This is why the standard coined two different names. IEEE 802.11, too, offers an ad-hoc mode, but not the CC functionality for QoS support.

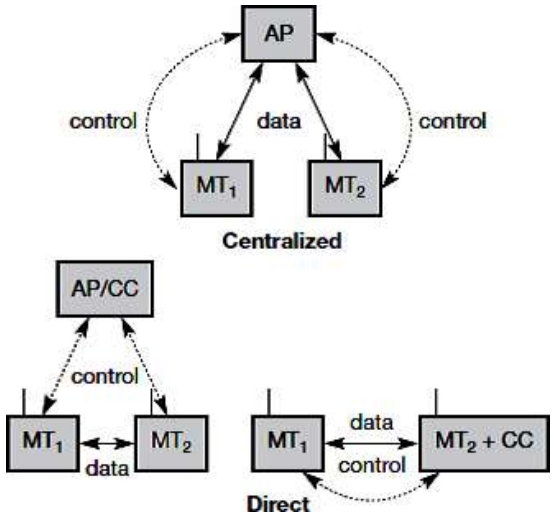


Fig. 1.23 HiperLAN2 Modes

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

HiperLAN2 defines six channels for data transfer.

- Broadcast channel (BCH): This channel conveys basic information for the radio cell to all MTs. This comprises the identification and current transmission power of the AP. Furthermore, the channel contains pointers to the FCH and RCH which allows for a flexible structure of the MAC frame. The length is 15 bytes.
- Frame channel (FCH): This channel contains a directory of the downlink and uplink phases (LCHs, SCHs, and empty parts). The length is a multiple of 27 bytes.
- Access feedback channel (ACH): This channel gives feedback to MTs regarding the random access during the RCH of the previous frame. The length is 9 bytes.
- Long transport channel (LCH): This channel transports user and control data for downlinks and uplinks. The length is 54 bytes.
- Short transport channel (SCH): This channel transports control data for downlinks and uplinks. The length is 9 bytes.
- Random channel (RCH): This channel is needed to give an MT the opportunity to send information to the AP/CC even without a granted SCH.The length is 9 bytes. A maximum number of 31 RCHs is currently supported.

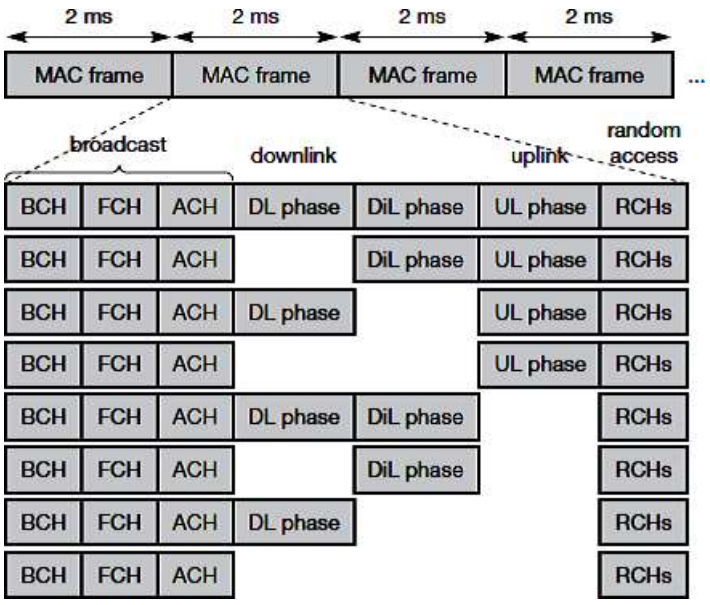


Fig. 1.24 MAC frames Configurations

[Source: Text book -Mobile Communications, Second Edition,earson Education by Jochen Schiller]

Bluetooth

Bluetooth is a standard for short range, low power, low cost wireless communication that uses radio technology. Although originally envisioned as a cable-replacement technology. Bluetooth technology can be used at home, in the office, in the car, etc. This technology allows to the users instantaneous connections of voice and information between several devices in real time. The way of transmission used assures protection against interferences and safety in the sending of information.

The Bluetooth is a small microchip that operates in a band of available frequency throughout the world. Communications can realize point to point and pointmultipoint. The standard Bluetooth operates in the band of 2,4 GHz. Though worldwide, this band is available, the width of the band can differ in different countries. This is the frequency of band of the scientific and medical industries 2.45 GHz (ISM*). The ranges of the bandwidth in The United States and Europe are between 2.400 to 2.483,5 MHz and it covers part of France and Spain. The ranges of the bandwidth in Japan are between 2.471 to 2.497 MHz.

User scenarios

Many different user scenarios can be imagined for wireless piconets or WPANs:

- Connection of peripheral devices: Most of the devices are connected to a desktop computer via wires (e.g., keyboard, mouse, joystick, headset, speakers).This type of connection has several disadvantages: each device has its own type of cable, different plugs are needed, and wires block office space. In a wireless network, no wires are needed for data transmission. However, batteries now have to replace the power supply, as the wires not only transfer data but also supply the peripheral devices with power.
- Support of ad-hoc networking: Imagine several people coming together,

Wireless networks can support interactive exchange of data as a group. Small devices might not have WLAN adapters following the IEEE 802.11 standard, but cheaper Bluetooth chips built in.

- Bridging of networks: Using wireless piconets, a mobile phone can be connected to a PDA or laptop in a simple way. Mobile phones will not have full WLAN adapters built in, but could have a Bluetooth chip. The mobile phone can then act as a bridge between the local piconet and, e.g., the global GSM network.

ARCHITECTURE OVERVIEW

Bluetooth link control hardware, integrated as either one chip or a radio module and a baseband module, implements the RF, baseband, and link manager portions of the Bluetooth specification. This hardware handles radio transmission and reception as well asrequired digital signal processing for the baseband protocol. Its functions include establishing

connections, support for asynchronous (data) and synchronous (voice) links, error correction, and authentication. The link manager firmware provided with the

baseband CPU performs low-level device discovery, link setup, authentication, and link configuration.
Bluetooth operates on 79 channels in the 2.4 GHz band with 1 MHz carrier spacing. Eachdevice performs frequency hopping with1,600 hops/s in a pseudo random fashion. A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence. One device in the piconet can act as master (M), all other devices connected to the master must act as slaves (S).

The master determines the hopping pattern in the piconet and the slaves have to synchronize to this pattern. Each piconet has a unique hopping pattern. If a device wants toparticipate it has to synchronize to this. Two additional types of devices are shown: parked devices (P) cannot actively participate in the piconet (i.e., they do not have a connection), but are known and can be reactivated within some milliseconds.

Devices in stand-by (SB) do not participate in the piconet. Each piconet has exactly one master and up to seven simultaneous slaves. More than 200 devices can be parked. The reason for the upper limit of eight active devices is the 3-bitaddress used in Bluetooth. If a parked device wants to communicate and there are already seven active slaves, one slave has to switch to park mode to allow the parked device to switch to active mode.

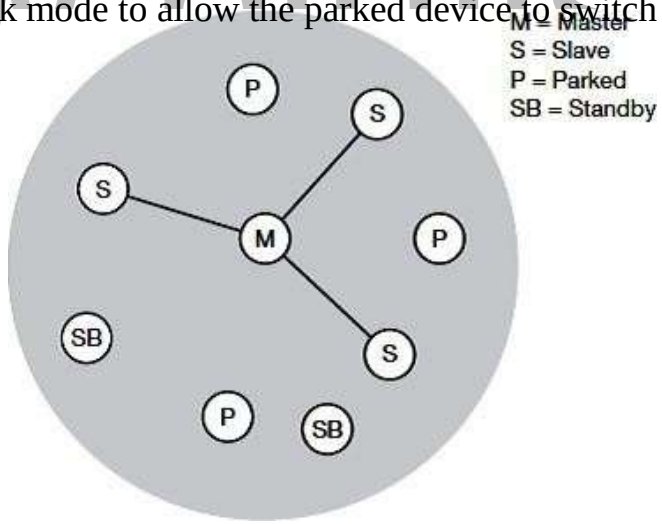


Fig. 1.25 Bluetooth piconet

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The Piconet are several devices that are in the same radio of coverage where they share the same channel and that is constituted between two and eight of these units. Every device has the unique direction of 48 bits, based on the standard IEEE 802.11 for WLAN, whereas the Scatternet formed by the connection of a Piconet to other one, with a maximum of interconnections of ten Piconets.

As all active devices have to use the same hopping sequence they must be synchronized. The first step involves a master sending its clock and device ID. All Bluetooth devices have the same networking capabilities, i.e., they can be master or slave. There is no distinction between terminals and base stations, any two or more devices can forma piconet.

The unit establishing the piconet automatically becomes the master, all other devices will be slaves. The phase in the hopping pattern is determined by the master‘s clock. After adjusting the internal clock according to the master a device may participate in the piconet. All active devices are assigned a3-bit active member address (AMA). All parked devices use an 8-bit parked member address (PMA). Devices in stand-by do not need an address.

\

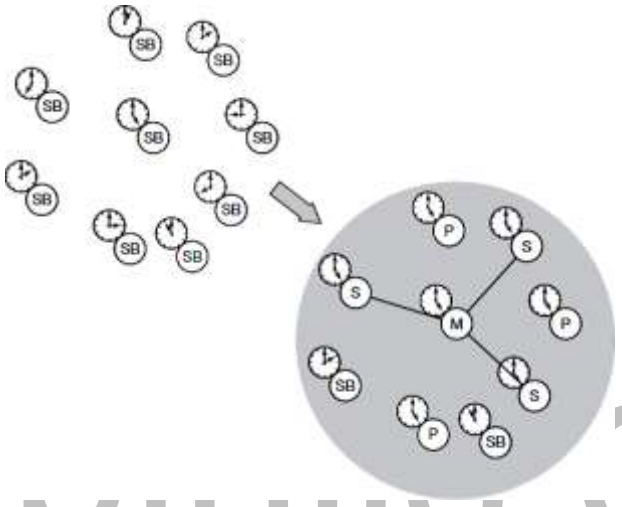


Fig. 1.26 Forming a Bluetooth piconet

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

All users within one piconet have the same hopping sequence and share the same 1 MHz channel. As more users join the piconet, the throughput per user drops quickly (a single piconet offers less than 1 Mbit/s gross data rate).This led to the idea of forming groups of piconets called scatternet. If a device wants to participate in more than one piconet, it has to synchronize to the hopping sequence of the piconet it wants to take part in.

If a device acts as slave in one piconet, it simply starts to synchronize with the hopping sequence of the piconet it wants to join. After synchronization, it acts as a slave in this piconet and no longer participates in its former piconet. To enable synchronization, a slave has to know the identity of the master that determines the hopping sequence of a piconet. Before leaving one piconet, a slave informs the current master that it will be unavailable for a certain amount of time. There maining devices in the piconet continue to communicate as usual.

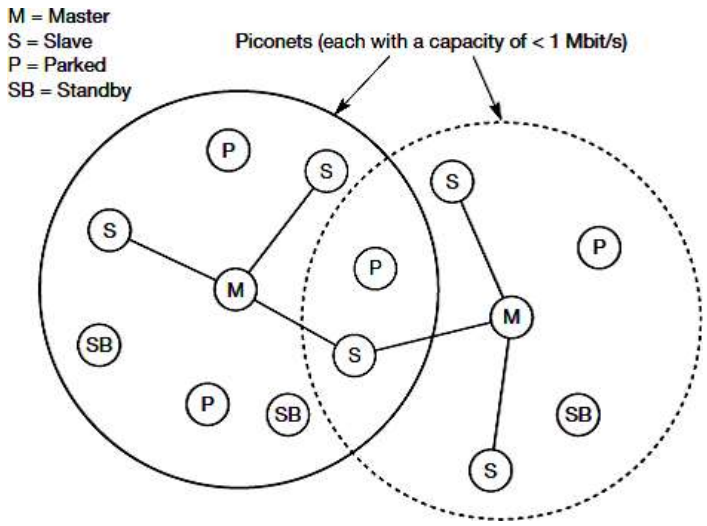


Fig. 1.27 Bluetooth scatter net

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Protocols Stack

The protocol architecture of the Bluetooth consists of following in a Bluetooth protocol stack:

- Core protocols consisting 5 layer protocol stack viz. radio, baseband, link manager protocol, logical link control and adaptation protocol, service discovery protocol.
- Cable replacement protocol, RFCOMM
- Telephony Control Protocols
- Adopted protocols viz. PPP,TCP/UDP/IP,OBEX and WAE/WA Core protocols

Radio: This protocol specification defines air interface, frequency bands, frequency Hopping specifications, modulation technique used and transmits power classes. Baseband: Addressing scheme, packet frame format, timing and power control algorithms required for establishing connection between Bluetooth devices within picante defined in this part of protocol specification.

Link Manager Protocol: It is responsible to establish link between Bluetooth devices and to maintain the link between them. This protocol also includes authentication and encryption specifications. Negotiation of packet sizes between devices can be taken care by this. Logical link control and adaptation protocol: This L2CAP protocol adapts upper layer frame to baseband layer frame format and vice versa. L2CAP take care of both connections oriented and connectionless services.

Service discovery protocol: Service related queries including device information can be Bluetooth devices

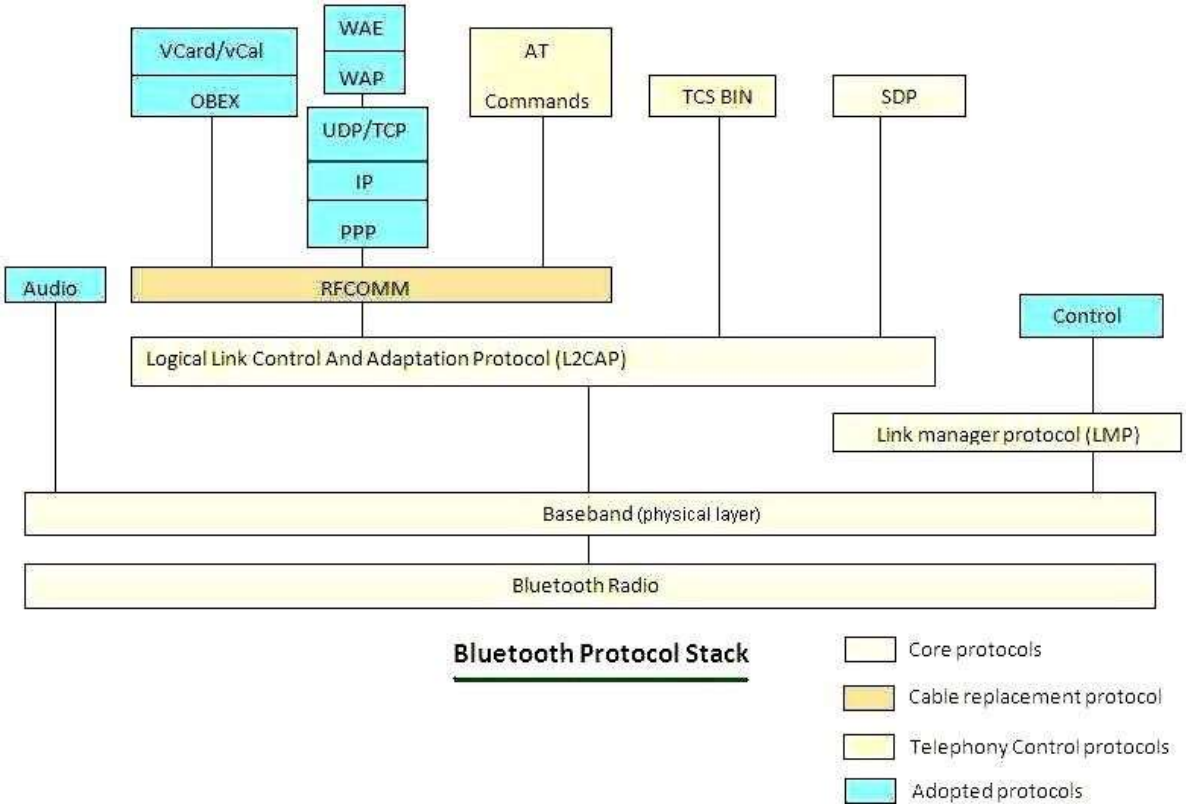


Fig.1.28 Bluetooth Protocol Stack

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Radio Layer

• The Bluetooth radio layer corresponds to the physical layer of OSI model. It deals with radio transmission and modulation. The radio layer moves data from master to slave or vice versa. It is a low power systemthat uses 2.4 GHz ISM band in a range of 10 meters.

• This band is divided into 79 channels of 1MHz each. Bluetooth uses the Frequency Hopping Spread Spectrum (FHSS) method in the physical layer to avoid interference from other devices or networks.

The radio specification defines the carrier frequencies and output power. Bluetooth devices will be integrated into typical mobile devices and rely on battery power. This requires small, low power chips which can be built into handheld devices. The combined use for data and voice transmission has to be reflected in the design, i.e., Bluetooth has to support multi-media data.

Bluetooth uses the license-free frequency band at 2.4 GHz allowing for worldwide operation with some minor adaptations to national restrictions. A frequency-hopping/time- division duplex scheme is used for transmission, with a fast hopping rate of 1,600 hops per second. The time between two hops is called a slot, which is an interval of 625 μs. Each slot uses a different frequency. In order to change bits into a signal, it uses a FSK with Gaussian bandwidth filtering.

Bluetooth transceivers use Gaussian FSK for modulation and are available in three classes:

- Power class 1: Maximum power is 100 m W and minimum is 1 m W (typ. 100 m range without obstacles). Power control is mandatory.
- Power class 2: Maximum power is 2.5 m W, nominal power is 1 m W, and minimum power is 0.25 m W (typ. 10 m range without obstacles). Power control is optional.
- Power class 3: Maximum power is 1 mW.

Baseband Layer

Baseband layer is equivalent to the MAC sublayer in LANs.

The baseband layer controls transmission of frames in association with frequency hopping. Master and slave stations communicate with each other using time slots. The master in a piconet takes the channel to transmit in even-numbered hops, and slaves transmit in odd-numbered hops, reflecting a time-division duplex for all devices in apiconet.

A single frame can be transmitted in the duration of one, three, or five hops. Depending on the nature of the logical link between a slave and the master, two types of links are offered. Bluetooth uses a form of TDMA called TDD-TDMA (time division duplex TDMA).The master in each piconet defines the time slot of 625 μsec.

In TDD- TDMA, communication is half duplex in which receiver can send and receive data but not at the same time. If the piconet has only no slave; the master uses even numbered slots (0, 2, 4, ...) and the slave uses odd-numbered slots (1, 3, 5,). Both master and slave communicate in half duplex mode. In slot 0, master sends & secondary receives; in slot 1, secondary sends and primary receives. If piconet has more than one slave, the master uses even numbered slots. The slave sends in the next odd-numbered slotif the packet in the previous slot was addressed to it.

The baseband layer has defined some types of frames that correspond to various purposes of the baseband frames. Different types of frames can carry different sizes of payload data and error-correction schemes. In particular, the access code field in a baseband frame indicates the purpose of the frame in a special state. For example, a frame with the inquiry access code (IAC) will be sent when a device elects to scan for other devices within the radio range in a series of 32 frequency hops.

Bluetooth devices can be configured to periodically hop according to the inquiry scan hopping sequence to scan inquires. When an inquiry is detected, the device, now the slave, will reply with its address and timing information to the master, and then the master and the slave begin the paging process to determine a common hopping sequence to establish a connection. Eventually, both the master and the slave will hop on the same sequence of channels for the duration of the connection.

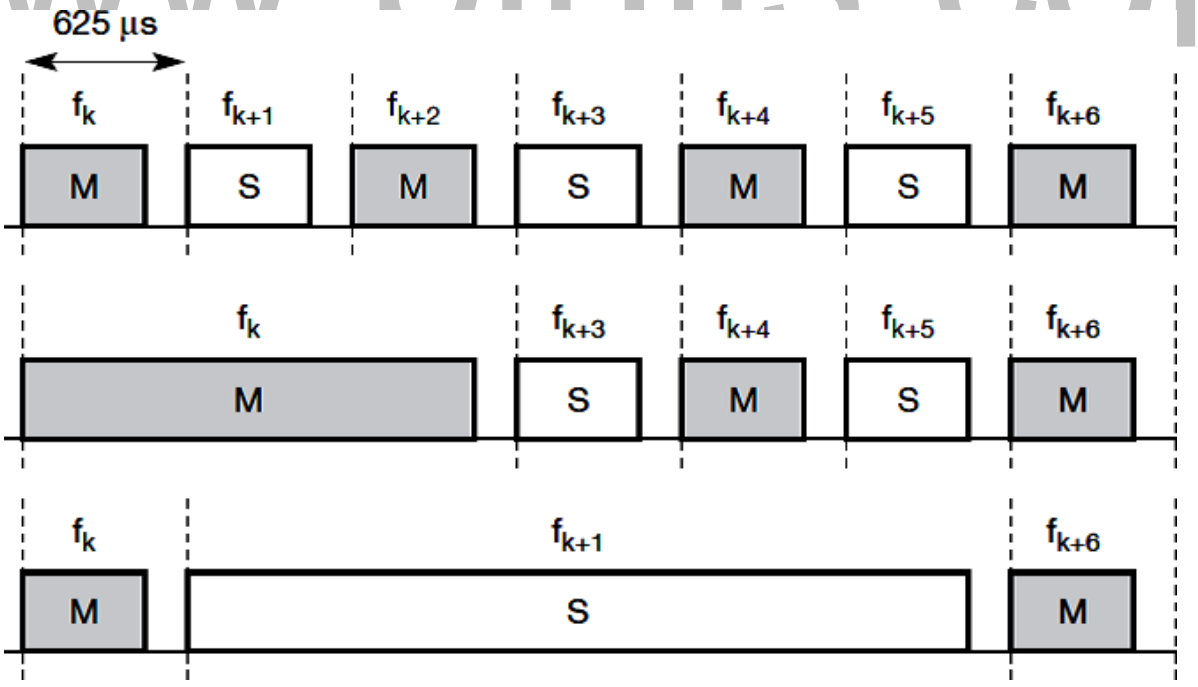


Fig. 1.29 Frequency selection during data transmission using 1, 3, 5 packet slots

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Link manager protocol

The Link Manager (LM) translates the commands into operations at the Baseband level, managing the following operations.

1) Attaching slaves to piconets, and allocating their active member addresses.
2) Breaking connections to detach Slaves from a piconet.
3) Configuring the link including Master/Slave switches
4) Establishing ACL and SCO links.
5) Putting connections into Low Power modes: Hold, Sniff and Park.
6) Controlling test modes.

A Bluetooth Link Manager communicates with Link Managers on other Bluetooth devices using the Link Management protocol (LMP).

The link can be configured at any time, including at mode changes, quality of service changes, packet type changes and any power level changes. Finally, information about an active link can be retrieved at any time. When the connection is no longer required, LMP can cause disconnection.

The link manager protocol (LMP) manages various aspects of the radio link between a master and a slave and the current parameter setting of the devices. LMP enhances baseband functionality, but higher layers can still directly access the baseband. The following groups of functions are covered by the LMP:

• Authentication, pairing, and encryption: Although basic authentication is handled in the baseband, LMP has to control the exchange of random numbers and signed responses. The pairing service is needed to establish an initial trust relationship between two devices that have never communicated before.

The result of pairing is a link key. This may be changed, accepted or rejected. LMP is not directly involved in the encryption process, but sets the encryption mode (no encryption, point-to-point, or broadcast), key size, and random speed.

• Synchronization: Precise synchronization is of major importance within a Bluetooth network. The clock offset is updated each time a packet is received from the master. Additionally, special synchronization packets can be received. Devices can also exchange timing information related to the time differences (slot boundaries) between two adjacent piconets.

• Capability negotiation: Not only the version of the LMP can be exchanged but also information about the supported features. Not all Bluetoothdevices will support all features that are described in the standard, so devices have to agree the usage of, e.g., multi-slot packets, encryption, SCO links, voice encoding, park/sniff/hold mode, HV2/HV3packets etc.

• Quality of service negotiation: Different parameters control the QoS of a Bluetooth device at these lower layers. The poll interval, i.e., the maximum time between transmissions from a master to a particular slave, controls the latency and transfer capacity. Depending on the quality of the channel, DMor DH packets may be used (i.e., 2/3 FEC protection or no protection). The number of repetitions for broadcast packets can be controlled. A master can also limit the number of slots available for slaves 'answers to increase its own bandwidth.
• Power control: A Bluetooth device can measure the received signal strength. Depending on this signal level the device can direct the sender of the measured signal to increase or decrease its transmitting power.

1.6 HIPERLAN

HIPERLAN is a European (ETSI) standardization initiative for a High Performance wireless Local Area Network. Radio waves are used instead of a cable as a transmission medium to connect stations. Either, the radio transceiver is mounted to the movable stationas an add-on and no base station has to be installed separately, or a base station is needed in addition per room. The stations may be moved during operation-pauses or even become mobile. The maximum data rate for the user depends on the distance of the communicating stations. With short distances (<50 m) and asynchronous transmission a data rate of 20 Mbit/s is achieved, with up to 800 m distance a data rate of 1 Mbit/s are provided.

1.6.1 HiperLAN features:

- Range 50 m
- Slow mobility (1.4 m/s)
- Supports asynchronous and synchronous traffic
- Bit rate - 23.2 Mbit/s
- Description- wireless Ethernet
- Frequency range- 5 GHz

1.6.2 HIPERLAN 1

HIPERLAN1 was originally one out of four HIPERLANs envisaged, as ETSI decided to have different types of networks for different purposes. The key feature of all four networks is their integration of time-sensitive data transfer services. Overtime, names have changedAN2, HIPERACCESS, and HIPERLINK. The current focus is onHiperLAN2, a standard that comprises many elements from ETSI‘s BRAN (broadband radio access networks) and wireless ATM activities.

ETSI describes HIPERLAN 1 as a wireless LAN supporting priorities and packet life time for data transfer at 23.5 Mbit/s, including forwarding mechanisms, topology discovery, user data encryption, network identification and power conservation mechanisms.

HIPERLAN 1 should operate at 5.1–5.3 GHz with a range of 50 m in buildings at 1 Transmit power. The service offered by a HIPERLAN 1 is compatible with the standardMAC services known from IEEE 802.x LANs. Addressing is based on standard 48 bit MAC addresses. Confidentiality is ensured by an encryption/decryption algorithm that requires the identical keys and initialization vectors for successful decryption of a DataStream encrypted by a sender. An innovative feature of HIPERLAN 1, which many other wireless networks do not offer, is its ability to forward data packets using

Several relays. Relays can extend the communication on the MAC layer beyond the radio range.

For power conservation, a node may set up a specific wake-up pattern.

This pattern determines at what time the node is ready to receive, so that at other times, the node can turn off its receiver and save energy. These nodes are called p-savers and need so- called p-supporters that contain information about the wake-up patterns of all the p-savers they are responsible for. A p-supporter only forwards data to a p-saver at the moment the p-saver is awake. This action also requires buffering mechanisms for packets on p- supporting forwarders.

Elimination-yield non-preemptive priority multiple access (EY-NPMA) is not only a complex acronym, but also the heart of the channel access providing priorities and different access schemes. EY-NPMA divides the medium access of different competing nodes into three phases:

- Prioritization: Determine the highest priority of a data packet ready to be sent by competing nodes.
- Contention: Eliminate all but one of the contenders, if more than one sender has the highest
- Transmission: Finally, transmit the packet of the remaining node.

The dynamic extension is randomly chosen between 0 and 3 times 200 high bit rate. This extension further minimizes the probability of collisions accessing a free channel if stations are synchronized on higher layers and try to access the free channel at the same time. HIPERLAN 1 also supports _channel access in the hidden elimination condition ‘to handle the problem of hidden terminals as described in ETSI.

The contention phase is further subdivided into an elimination phase and a yield phase. the elimination phase is to eliminate as many contending nodes as possible. The result of the elimination phase is a more or less constant number of remaining nodes, almost independent of the initial number of competing nodes. Finally, the yield phase completes the work of the elimination phase with the goal of only one remaining node.

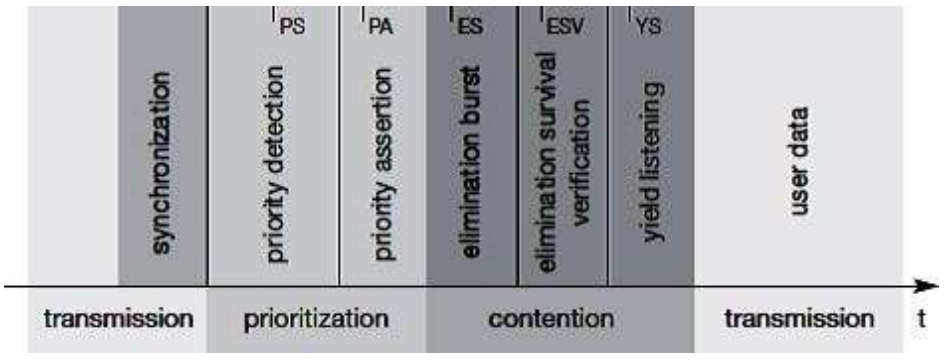


Fig. 1.17 Phases of HIPERLAN1

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The above figure gives an overview of the three main phases and some more details which will be explained in the following sections. For every node ready to send data, the access cycle starts with synchronization to the current sender.
The first phase, prioritization, follows. After that, the elimination and yield part of the contention phase follow. Finally, the remaining node can transmit its data. Every phase has a certain duration which is measured in numbers of slots and is determined by the variable sips, IPA, IES, IESV, and IYS.

1.6.3 Prioritization phase

HIPERLAN 1 offers five different priorities for data packets ready to be sent. After one node has finished sending, many other nodes can compete for the right to send. The first objective of the prioritization phase is to make sure that no node with a lower priority gains access to the medium while packets with higher priority are waiting at other nodes. This mechanism always grants nodes with higher priority access to the medium, no matter how high the load on lower priorities.

In the first step of the prioritization phase, the priority detection, time is divided into five slots, slot 0 (highest priority) to slot 4 (lowest priority). Each slot has a duration of IPS = 168 high rate bit-periods. If a node has the access priority p, it has to listen into the medium for p slots (priority detection).
Consider for example, that there are three nodes with data ready to be sent, the packets of node 1 and node 2 having the priority 2, the packet of node3 having the priority 4.
Then nodes 1, 2 and 3 listen into the medium and sense
Slots 0 and 1 are idle. Nodes 1 and 2 both send a burst in slot 2 as priority assertion.
Node 3 stops its attempt to transmit its packet. In this example, the prioritization phase has taken three slots.

After this first phase at least one of the contending nodes will survive, the surviving nodes being all nodes with the highest priority of this cycle.

1.6.4 Elimination Phase

Several nodes may now enter the elimination phase. Again, time is divided into slots, usingthe elimination slot interval IES = 212 high rate bit periods. The length of an individual elimination burst is 0 to 12 slot intervals long, the probability of bursting within a slot is
0.5. The probability PE(n) of an elimination burst to be in elimination slot intervals long is given by:

- $PE(n) = 0.5n+1$ for $0 \leq n < 12$
- $PE(n) = 0.512$ for $n = 12$

The elimination phase now resolves contention by means of elimination bursting and elimination survival verification. Each contending node sends an elimination burst with length n as determined via the probabilities and then listens to the channel during the survival verification interval IESV = 256 high rate bit periods. The burst sent is the same as for the priority assertion.
A contending node survives this elimination phase if, and only if, it senses the channel is idle during its survival verification period. Otherwise, the node is eliminated and stops its attempt to send data during this transmission cycle.

1.6.5 Yield phase

During the yield phase, the remaining nodes only listen into the medium without sending any additional bursts. Again, time is divided into slots, this time called yield slots with a duration of IYS = 168 high rate bit-periods. The length of an individual yield listening period can be 0 to 9 slots with equal likelihood. The probability PY (n) for a yield listening period

Each node now listens for its yield listening period. If it senses the channel is idle during the whole period, it has survived the yield listening. At least one node will survive this phase and can start to transmit data. This is what the other nodes with longer yield listening period than one surviving node so a collision is still possible.

1.6.6 Transmission phase

A node that has survived the prioritization and contention phase can now send its data, called a low bit-rate high bit-rate HIPERLAN 1 CAC protocol data unit (LBR-HBR HCPDU). This PDU can either be multicast or unicast. In case of a unicast transmission, the sender expects to receive an immediate acknowledgement from the destination, called an acknowledgement HCPDU (AK-HCPDU), which is an LBR HCPDU containing only an LBR part.

1.7 WATM (WIRELESS ATM)

Wireless ATM also called as wireless, mobile ATM, warm. It describes a transmission technology to specify a complete communication system. IEEE WLAN originates from the data communication community whereas WLAN arise from the tale communication industry.

1.7.1 Development of WATM

- The wireless terminals are integrated into an ATM network for supporting different types of traffic streams as ATM does in fixed network.

- ATM network will scale well from LANs to WANs & mobility is needed in local and wide applications.
- WATM offers QOS for adequate support of multimedia data streams.
- For telecommunication service providers, merging of mobile wireless communication & ATM technology will leads to wireless ATM.

1.7.2 Standardization of WATM

WATM is a specific broadband wireless solution which is significantly meets the architectural and performance goals needed. WATM has been driven by the wide acceptance of ATM switching technology as a basis for broadband networks which support integrated services with QoS control. ATM signaling protocol (e.g.,Q2931) for connection establishment and QoS control also provide a suitable basis for mobility extensions such as handover and location management.

1.7.3 Extension of ATM

The following more general extensions of the ATM system also need to be considered fora mobile ATM:

- **Location management:** Similar to other cellular networks, WATM networks must be able to locate a wireless terminal or a mobile user, i.e., to find the current access point of the terminal to the network.
- **Mobile routing:** Even if the location of a terminal is known to the system, it still has to route the traffic through the network to the access point currently responsible for the wireless terminal. Each time a user moves to anew access point, the system must reroute traffic.
- **Handover signaling:** The network must provide mechanisms which search for new access points, set up new connections between intermediate systems and signal the actual change of the access point.
- **QoS and traffic control:** In contrast to wireless networks offering only best effort traffic,and to cellular networks offering only a few different types of traffic, WATM should be able to offer many QoS parameters. To maintain these parameters, all actions such as rerouting, handover etc. have to be controlled. The network must pay attention to the incoming traffic (and check if it conforms to some traffic contract) in a similar way to today‘s ATM (policing).
- **Network management:** All extensions of protocols or other mechanisms also require an extension of the management functions to control the network.

1.7.4 Frame Format for WATM

Wireless header	ATM header (5 bytes)	ATM payload (48 bytes)	Wireless trailer

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The ATM cells were operating on reliable optical channels that do not need acknowledgement. When the same packet format is used in a wireless environment, another additional 16 bytes for the PLCP header is used and a few more for a wireless MAC layer that makes the overhead so large that a 48 – byte payload length makes the transmission inefficient.

1.7.6 WIRELESS ATM ARCHITECTURE

Wireless ATM architecture is obtained by incorporating new wireless protocols at the access level and extensions into the standard ATM protocol stack which is shown in Figure. At the access level, new protocols are needed for:

- Physical layer radio channels between the mobile terminals and base stations,
- Medium access control (MAC) to arbitrate the shared use of the radio channels by the mobile terminals,
- Data/logical link control (DLC/LLC) to detect and/or correct the radio channel errorsand maintain end-to-end QoS.
- Wireless control to support such functions as radio resource management at the physical, MAC and DLC layers, as well as mobility management.

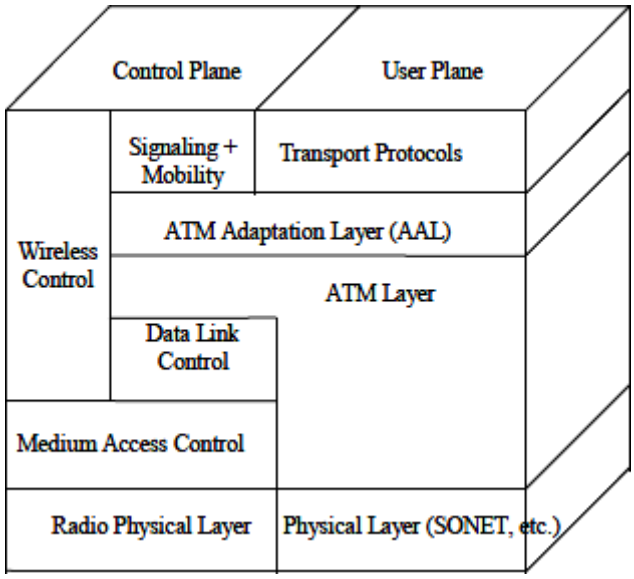


Fig. 1.18 Wireless ATM Architecture

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

WATM protocol architecture is based on integration of radio access and mobility features capabilities within the standard ATM protocol stack. A WATM system may be partitioned into two relatively independent parts: a mobile ATM infrastructure and a radio access segment, each of which can be designed and specified separately. This facilitates standardization by multiple organizations and allows for gradual evolution of radio access technologies without having to modify the core mobile ATM network specification.

The WATM radio access structure consists of Radio Physical Layer (PHY), Medium Access Control (MAC), Data Link Control (DLC) and wireless control. The WATM DLC layer interfaces each ATM virtual circuit (both service data and signaling) with the ATM network layer above. An additional wireless control interface is provided within the control plane to deal with radio link specific control functions such as initial registration, resource allocation, and power control.

1.7.7 Handover

As a mobile terminal moves from one place to another, it becomes necessary to hand overits ongoing connections from the old radio port to the new one. The decision to change the radio port is made either by the mobile terminal or the base station based on signal strength measurements.

There are three handover scenarios. In the first scenario, the old and new radio ports belong to the same base station. This case can be handled completely by the radio-level protocols. In the second scenario, the target radio port belongs to different base stations, with the old and new base stations connected to (and supported by) the same ATM switch.

This latter switch controls the rerouting of the connections from the old to the new base stations, and is called the crossover switch. In the third case, each of the two base stations is crossover switch for rerouting connections from the old to the new access switch.

The discovery and selection of the crossover switch is an important issue in handover. Unless handover occurs within the same base station, ATM-level protocols are said to be required for discovery of crossover switch, path rerouting, etc.

There are two types of handovers:

1. Soft hand over
2. Hard hand over

In soft handover, the mobile terminal connections are passed to the new base station without interrupting communication with the old base station.

In hard handover, the connections are interrupted at the old base station and reestablished at the new base station. Only hard handover is supported in the current WATM specification.

1.7.8 Location Management

Location management is required to maintain the association between the mobile‘s physical location at a foreign switch and its permanent address at the home switch. To achieve this, a mobile terminal must register with the base station of every new service area it may enter. The main purpose of location management in wireless ATM networks is to allow a mobile terminal to use its permanent address in connection set-up messages regardless of its attachment to the network. In addition, location management incorporates features for access control, privacy, accounting and inter-provider roaming.

The functions of location management are handled by mobility-enhanced switches, location servers, authentication servers, and mobile terminals. The location server is a database of associations between the permanent and temporary addresses of mobile terminals. The temporary address identifies the location of the mobile terminal away from its permanent home address (switch). This database is queried and updated according to specific protocols.

On the other hand, the authentication server is a database containing secure information relating to the privacy and identification of each mobile terminal.
Location management is required in local and wide area WATM networks. Local location management enables any host connected to a switch to establish a virtual circuit with any mobile terminal moving between the base stations within a local network. Wide area location management permits mobile terminals attached to one local network to establish connections with hosts (or other mobile terminals) attached to remote network groups.

1.7.9 Mobile quality of service

Quality of service (QoS) guarantees are one of the main advantages predicted for WATM networks compared to, e.g., mobile IP working over packet radio networks.
While the internet protocol IP does not guarantee QoS, ATM networks do (at the cost of higher complexity). WATM networks should provide mobile

QoS (M-QoS). M-QoS is composed of three different parts:

- Wired QoS: The infrastructure network needed for WATM has the same QoS properties as any wired ATM network. Typical traditional QoS parameters are link delay, cell delay variation, bandwidth, cell error rate etc.
- Wireless QoS: The QoS properties of the wireless part of a WATM network differ from those of the wired part. Again, link delay and error rate can be specified, but

Now error rate is typically some order of magnitude that is higher than, e.g., fiber optics. Channel reservation and multiplexing mechanisms at the air interface strongly influence cell delay variation.

- Handover QoS: A new set of QoS parameters are introduced by handover. For example, handover blocking due to limited resources at target access points, cell loss during handover, or the speed of the whole handover procedure

1.4 IEEE 802.11b

IEEE 802.11b was the first wireless LAN standard to be widely adopted and built in to many laptop computers and other forms of equipment. It was only after 802.11 was ratified and products became available that W-Fi took off in a large way. This standard describes a new PHY layer and is by far the most successful version of IEEE 802.11 available today. The standards are named according to the order in which the respective study groups have been established. Although the IEEE 802.11a standard was introduced atthe same time, it did not catch on in the same way even though it was capable of higher speeds.

1.4.1 802.11b specification

It is able to transfer data with raw data rates up to 11 Mbps, and has a good range, although not when operating at its full data rate.

Table 1.1 Wi-Fi Standard Specifications

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

PARAMETER	VALUE
Date of standard approval	July 1999
Maximum data rate (Mbps)	11
Typical data rate (Mbps)	5
Typical range indoors (Metres)	~30
Modulation	CCK (DSSS)
RF Band (GHz)	2.4
Channel width (MHz)	20

When transmitting data 802.11b uses the CSMA/CA technique that was defined in the original 802.11 base standard and retained for 802.11b. Using this technique, when a node wants to make a transmission it listens for a clear channel and then transmits. With 802.11b WLANs, mobile users can get Ethernet levels of performance, throughput, and availability. The standards-based technology allows administrators to build networks that seamlessly combine more than one LAN technology to best fit their business and user needs. The basic architecture features, and services of 802.11b are defined by the original
802.11 standard. The 802.11b specification affects only the physical layer, adding higher data rates and more robust connectivity.

1.4.2 802.11b Enhancements to the PHY Layer

The key contribution of the 802.11b addition to the wireless LAN standard was to standardize the physical layer support of two new speeds, 5.5 Mbps and 11 Mbps. To

accomplish this, DSSS had to be selected as the sole physical layer technique for the standard since, as noted above, frequency hopping cannot support the higher speeds without violating current FCC regulations. The implication is that 802.11b systems will interoperate with 1 Mbps and 2 Mbps 802.11 DSSS systems, but will not work with 1 Mbps and 2 Mbps 802.11 FHSS systems.

The original 802.11 DSSS standard specifies an 11-bit chipping—called a Barker sequence—to encode all data sent over the air. Each 11-chip sequence represents a single data bit (1 or 0), and is converted to a waveform, called a symbol, that can be sent over theair. These symbols are transmitted at a 1 MSps (1 million symbols per second) symbol rate using a technique called Binary Phase Shift Keying (BPSK).

In the case of 2 Mbps, a more sophisticated implementation called Quadrature Phase Shift Keying (QPSK) is used; it doubles the data rate available in BPSK, via improved efficiency in the use of the radio bandwidth. To increase the data rate in the 802.11b standard, advanced coding techniques are employed.

Rather than the two 11-bit Barker sequences, 802.11b specifies Complementary Code Keying (CCK), which consists of a set of 64 8-bit code words. As a set, these code words have unique mathematical properties that allow them to be correctly distinguished from one another by a receiver even in the presence of substantial noise and multipath interference (e.g., interference caused by receiving multiple radio reflections within a building).

To support very noisy environments as well as extended range, 802.11b WLANs use dynamic rate shifting, allowing data rates to be automatically adjusted to compensate for the changing nature of the radio channel. Ideally, users connect at the full 11 Mbps rate. However when devices move beyond the optimal range for 11 Mbps operation, or if substantial interference is present, 802.11b devices will transmit at lower speeds, falling back to 5.5, 2, and 1 Mbps. Likewise, if the device moves back within the range of a higher-speed transmission, the connection will automatically speed up again. Rate shiftingis a physicallayer mechanism transparent to the user and the upper layers of the protocol stack.

Table 1.2 802.11b data rate specifications

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Data Rate	Modulation	Modulation Rate	Chip Size	Symbol Rate	Bits/Symbol
1Mbps	BPSK	11.000.000	11	1.000.000	1
2Mbps	QPSK	11.000.000	11	1.000.000	2
5.5 Mbps	QPSK	11.000.000	8	1.375.000	4

11 Mbps	QPSK	11.000.000	8	1.375.000	8

The following figure shows two packet formats standardized for 802.11b. The mandatory format is called long PLCP PPDU and is similar to the format illustrated in figure. One difference is the rate encoded in the signal field this is encoded in multiples of 100 kbit/s. Thus, 0x0A represents 1 Mbit/s, 0x14 is used for2 Mbit/s, 0x37 for 5.5 Mbit/s and 0x6E for 11 Mbit/s. Note that the preamble and the header are transmitted at 1 Mbit/s using DBPSK. The optional short PLCP PPDU format differs in several ways.

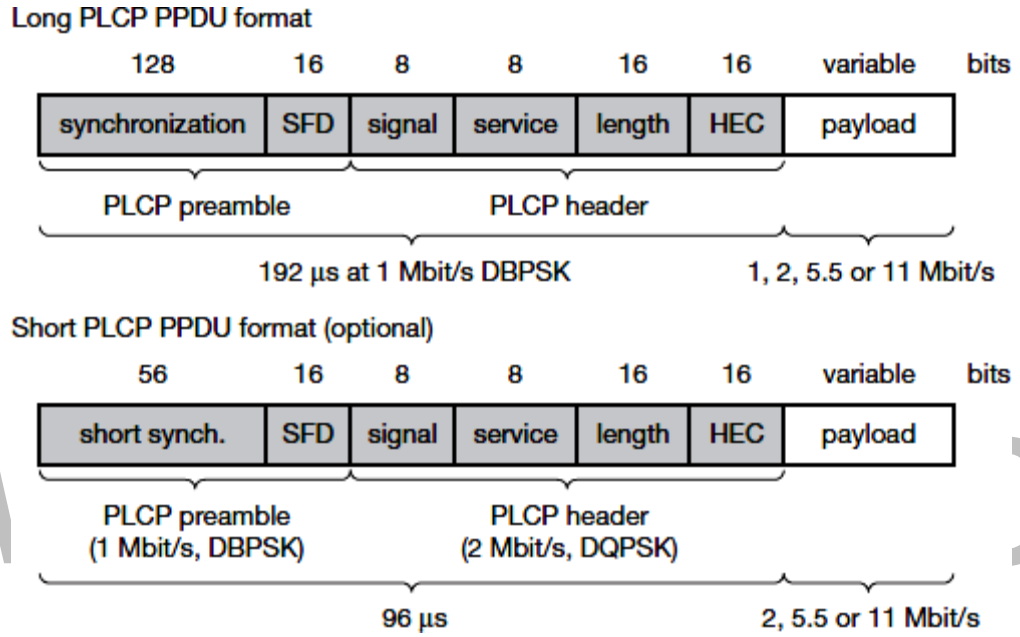


Fig. 1.14 IEEE 802.11b Phypacket formats

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The short synchronization field consists of 56 scrambled zeros instead of scrambled ones.The short start frame delimiter SFD consists of a mirrored bit pattern compared to the SFDof the long format: 0000 0101 1100 1111 is used for the short PLCP PDU instead of 1111 0011 1010 0000 for the long PLCP PPDU. Receivers that are unable to receive the shortformat will not detect the start of a frame (but will sense the medium is busy). Only the preamble is transmitted at 1 Mbit/s, DBPSK. The following header is already transmittedat 2 Mbit/s, DQPSK, which is also the lowest available data rate.

As IEEE 802.11b is the most widespread version, some more information is given for practical usage. The standards operates (like the DSSS version of802.11) on certain frequencies in the 2.4 GHz ISM band.

The following figure illustrates the non-overlapping usage of channels for an IEEE 802.11b installation with minimal interference in the US/Canada and Europe. The spacing between the center frequencies should be at least 25 MHz(the occupied bandwidth of the main lobe of the signal is 22 MHz). This results in the channels 1, 6, and 11 for the US/Canada or 1, 7, 13 for Europe, respectively. It may be the case that, e.g., travelers fromthe US cannot use the additional channels (12 and 13) in Europe as their hardware is limited to 11channels. Some European installations use channel 13 to minimize interference.

Users can install overlapping cells for WLANs using the three non-overlapping channels toprovide seamless coverage. This is similar to the cell planning for mobile phone systems.

Table 1.3 IEEE 802.11b channel plan

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Channel	Frequency [MHz]	US/Canada	Europe	Japan
1	2412	X	X	X
2	2417	X	X	X
3	2422	X	X	X
4	2427	X	X	X
5	2432	X	X	X
6	2437	X	X	X
7	2442	X	X	X
8	2447	X	X	X
9	2452	X	X	X
10	2457	X	X	X
11	2462	X	X	X
12	2467	–	X	X
13	2472	–	X	X
14	2484	–	–	X

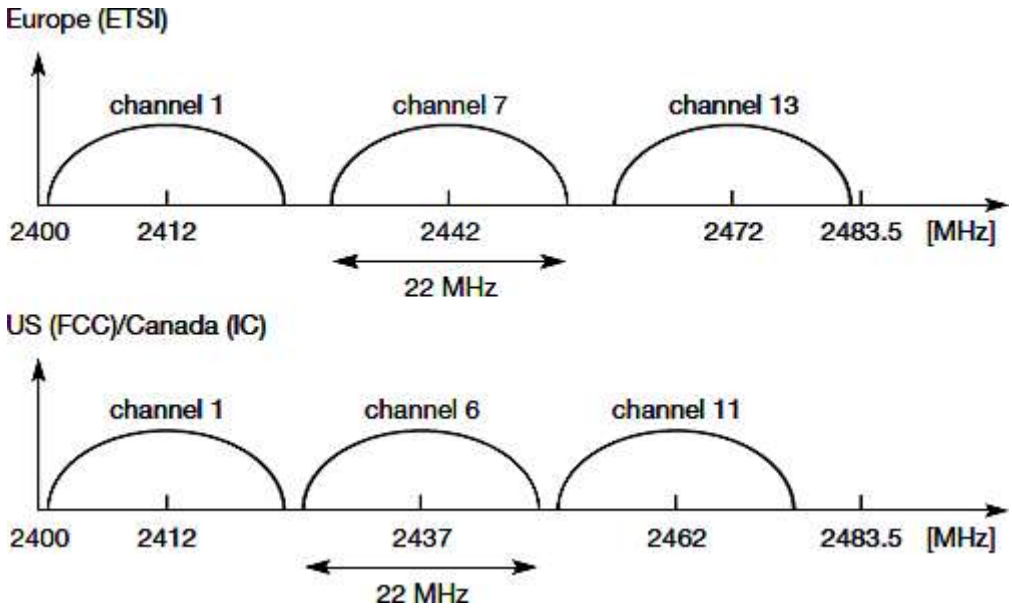


Fig. 1.15 IEEE 802.11b non overlapping channel selection

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.5 802.11a

An 802.11a wireless network supports a maximum theoretical bandwidth of 54Mbps, substantially better than the 11 Mbps of 802.11b and on par with what 802.11g would start to offer a few years later. The performance of 802.11a made it an attractive technology, but achieving that level of performance required using relatively higher cost hardware.

The IEEE 802.11a is an Orthogonal Frequency Division Multiplexing (OFDM) system very similar to Asymmetrical Digital Subscriber Loop (ADSL) Discrete Multi Tone (DMT) modems sending several sub-carriers in parallel using the Inverse Fast Fourier Transform (IFFT), and receiving those subcarriers using the Fast Fourier Transform (FFT).

In 802.11a the transmission medium is wireless and the operating frequency band is 5 GHz. The OFDM of the 802.11a system provides a Wireless LAN with data payload communication capabilities of 6, 9, 12, 18, 24, 36, 48 and 54 Mbps. The support of transmitting and receiving at data rates of 6, 12, and 24 Mbps is mandatory in the standard. The 802.11a system uses 52 subcarriers that are modulated using binary or quadrature phase shift keying (BPSK/QPSK), 16 Quadrature Amplitude Modulation

(QAM), or 64 QAM. Forward Error Correction (FEC) coding (convolutional coding) is used with a coding rate of 1/2, 2/3, or 3/4.

The OFDM PHY layer consists of two protocol functions: first a PHY convergence functions, which adapts the capabilities of the Physical Medium Dependent (PMD) system to the PHY service. This function is supported by the Physical Layer Convergence Procedure (PLCP), which defines a method of mapping the IEEE 802.11 PHY Sublayer Service Data Units (PSDU) into a framing format suitable for sending and receiving user data and management information between two or more stations using the associated PMD system.

Second a PMD system whose function defines the characteristics and method of transmitting and receiving data through a wireless medium between two or more stations, each using the OFDM system.
IEEE 802.11a uses the same MAC layer as all 802.11 physical layers. IEEE 802.11a uses many different technologies to offer data rates up to 54 Mbit/s. The system uses 52 subcarriers (48 data + 4 pilot) that are modulated using BPSK, QPSK, 16-QAM, or 64- QAM. To mitigate transmission errors, FEC is applied using coding rates of 1/2, 2/3, or 3/4.The following table gives an overview of the standardized combinations of modulation andcoding schemes together with the resulting data rates. To offer a data rate of 12 Mbit/s, 96 bits are coded into one OFDM symbol. These 96 bits are distributed over 48 subcarriers and2 bits are modulated per sub-carrier using QPSK (2 bits per point in the constellation diagram). Using a coding rate of 1/2 only 48 data bits can be transmitted.

Table 1.4 Rate dependent parameters for IEEE 802.11a

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Data rate [Mbit/s]	Modulation	Coding rate	Coded bits per subcarrier	Coded bits per OFDM symbol	Data bits per OFDM symbol
6	BPSK	1/2	1	48	24
9	BPSK	3/4	1	48	36
12	QPSK	1/2	2	96	48
18	QPSK	3/4	2	96	72
24	16-QAM	1/2	4	192	96
36	16-QAM	3/4	4	192	144
48	64-QAM	2/3	6	288	192
54	64-QAM	3/4	6	288	216

1.5.1 OFDM PLCP sublayer of the 802.11a

The PHY Sublayer Service Data Units (PSDU) of the 802.11a is converted to a PLCP Protocol Data Unit (PPDU). The PSDU of the 802.11a is provided with a PLCP preamble and header to create the PPDU. At the receiver of the 802.11a, the PLCP preamble and header are processed to aid in demodulation and delivery of the PSDU. The PPDU is unique to the OFDM PHY. The PPDU format of the standard 802.11a is shown in figure and it includes: "PLCP preamble. This field is used to acquire the incoming OFDM signal and train and synchronize the demodulator.

The PLCP preamble consists of 12 symbols, 10 of which are short symbols and 2 long symbols. The short symbols are used to train the receiver‘s AGC and to estimate a coarse estimate of the carrier frequency and the channel. The long symbols are used to fine-tune the frequency and the channel estimates. Twelve subcarriers are used for the sort symbols and 53 for the long.

The PLCP preamble is BPSK-OFDM modulated at 6 Mbps using convolutional encoding rate R=1/2. The first 4 bits (R1-R4) are used to encode the rate. The next bit is 1 reserved bit. A continuation they are 12 bits used for the length that indicated the number of octets in the PSDU. A continuation is a parity bit and 6 tail bits. This field contains 16 bits for theservice field, the PSDU, tails bits and pad bits. A total of 6

tail bits containing 0s are appended to the PPDU to ensure that the convolutional encoder is brought back to zero state. The data portion of the packet is transmitted at the data rate indicated in the signal field.

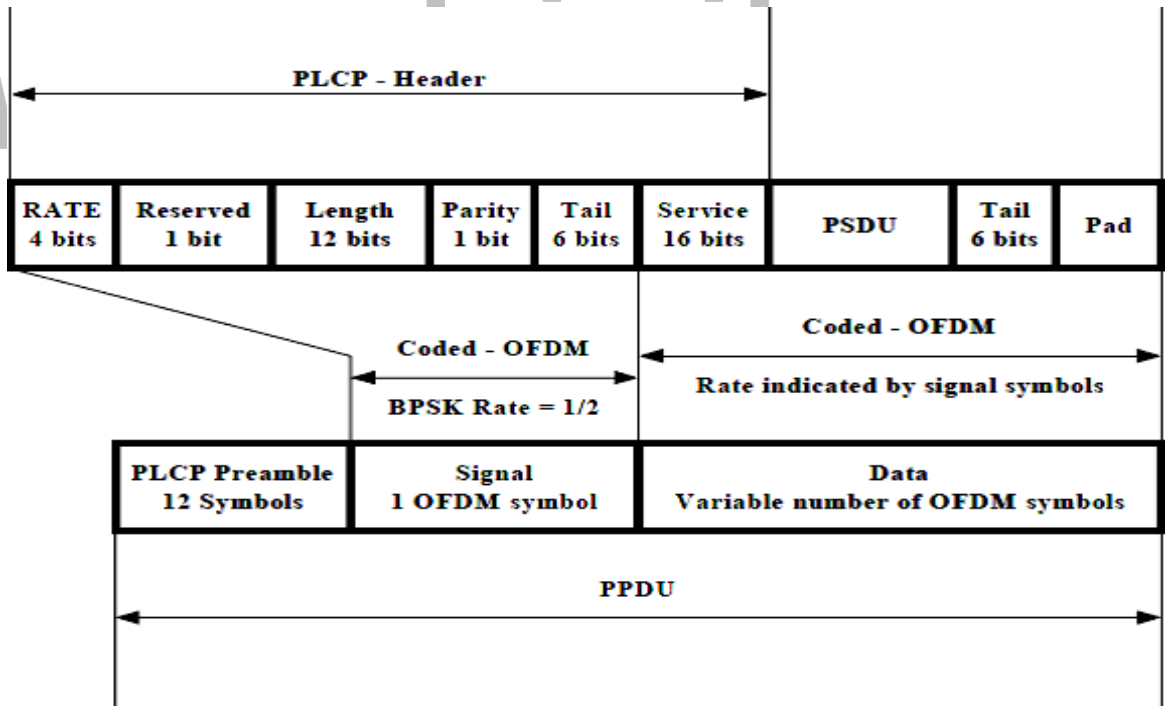


Fig. 1.16 OFDM PLCP Preamble, Header, PSDU of 802.11a
[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The PLCP header of 802.11a contains:

- 4 bits for the rate
- 1 reserved bit

- 12 bits for length
- 1 bit for parity
- 6 bits for tail
- 16 bits for service

Compared to IEEE 802.11b working at 2.4 GHz IEEE 802.11a at 5 GHz offers much higher data rates. However, shading at 5 GHz is much more severe compared to 2.4 GHz and depending on the SNR, propagation conditions and the distance between sender and receiver, data rates may drop fast (e.g., 54 Mbit/s may be available only in an LOS or near LOS condition). Additionally, the MAC layer of IEEE 802.11 adds overheads. User data rates are therefore much lower than the data rates listed above. Typical user rates in Mbit/s are (transmission rates in brackets) 5.3 (6), 18 (24), 24 (36), and 32 (54).

1.5.2 Data Scrambler

All the bits transmitted by the 802.11a OFDM PMD in the data portion are scrambled using a frame synchronous 127 bits sequence generator. Scrambling is used to randomize the service, PSDU, pad and data patterns, which may contain long strings of binary 1s or 0s. The tail bits are not scrambled. The octets of the PSDU are placed in the transmitted serial bit stream, bit 0 first and bit 7 last.

The frame synchronous scrambler uses the generator polynomial S(x) as follows:

$$\mathbf{S(x) = x^7 + x^4 + 1}$$

The 127bit sequence generated repeatedly by the scrambler is (leftmost used first),
00001110 11110010 11001001 00000010 00100110 00101110 10110110 00001100
11010100 11100111 10110100 00101010 11111010 01010001 10111000 1111111, when
the "all ones" initial state is used. The same scrambler is used to scramble transmit dataand to de-scramble receive data.

When transmitting, the initial state of the 802.11a scrambler will be set to a pseudo random non-zero state. The seven LSBs of the SERVICE field will be set to all zeros priorto scrambling to enable estimation of the initial state of the scrambler in the receiver. The contents of the SIGNAL field of the 802.11a are not scrambled. The PLCP length field of the 802.11a is an unsigned 12 bits integer that indicates the number of octets in the PSDU that the MAC is currently requesting the PHY to transmit. This value is used by the PHY to determine the number of octet transfers that will occur between the MAC and the PHY after receiving a request to start transmission.

The bits from 0-6 of the SERVICE field, which are transmitted first, are set to zeros and are used to synchronize the descrambler in the receiver. The remaining 9 bits (7-15) of the SERVICE field is reserved for future use. All reserved bits are set to zero.

1.5.3 Data Interleaving

In the 802.11a standard blocks inter - leaver interleaves all encoded data bits. The block size corresponds to the number of bits in a single OFDM symbol, NCBPS. The inter - leaver is defined by a two steps permutation. The first permutation ensures that adjacent coded bits are mapped onto nonadjacent subcarriers. The second ensures that adjacent coded bits are mapped alternately onto less and more significant bits of the constellation and, thereby, long runs of low reliability (LSB) bits are avoided.

1.5.4 Operating frequency and maximum power of the 802.11a

For the 802.11a standard the 5 GHz U-NII frequency bans is segmented into three 100 MHz bands for operation in the US. The lower band ranges from 5.15 –5.25 GHz, the middle band ranges from 5.25-5.35 GHz and the upper band ranges from 5.725-5.825 GHz. The lower and middle band, accommodate 8 channels in a total bandwidth of 200 MHz and the upper band accommodates 4 channels in a 100 MHz bandwidth.

The frequency channel center frequencies are spaced 20 MHz apart. The outermost channels of the lower and middle bands are centered 30 MHz from the outer edges. In the upper band the outermost channel centers are 20 MHz from the outer edges. In addition to the frequency and channel allocations, transmit power is a key parameter regulated in the5 GHz U-NII band. Three transmit power levels are specified: 40 mW, 200 mW and 800 mW. The upper band defines RF transmit power levels suitable for bridging applications while the lower band specifies a transmit power level suitable for short-range indoor homeand small office environments.

The following table shows the operating frequency and maximum power of the 802.11a standard.

Table 1.5Operating frequency and maximum power of the 802.11a standard.

Band	Channel numbers	Frequency (MHz)	Maximum output power
U-NII lower band 95.15 to 5.25 MHz	36	5180	40mW (2.5mW/MHz)
	40	5200	
	44	5220	
	48	5240	
U-NII lower band 95.15 to 5.25 MHz	52	5260	200mW (12.5mW/MHz)
	56	5280	
	60	5300	
	64	5320	
U-NII lower band 95.15 to 5.25 MHz	149	5745	800mW (50mW/MHz)
	153	5765	
	157	5785	
	161	5805	

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen S

1.3 IEEE 802.11

The IEEE standard 802.11 (IEEE, 1999) is the most famous family of WLANs in which many products are available. As the standard‘s number indicates, this standard belongs to the group of 802.x LAN standards, e.g., 802.3 Ethernet or 802.5 Token Ring. The standard specifies the physical and medium access layer adapted to the special requirements of wirelessLANs.

The primary goal of the standard was the specification of a simple and robust WLAN which offers time-bounded and asynchronous services. Additional features of the WLAN should include the support of power management to save battery power, the handling of hidden nodes, and the ability to operate worldwide. The 2.4 GHz ISM band, which is available in most countries around the world, was chosen for the original standard. Data rates envisaged for the standard were 1 Mbit/s mandatory and 2 Mbit/s optional.

1.3.1 System architecture

Wireless networks can exhibit two different basic system architectures as: infrastructure- based or ad-hoc. Several nodes, called stations (Stain), are connected to access points (AP). Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP. The stations and the AP which are within the same radio coverage form a basic service set (Byssi).

The example shows two BSSs – BSS1 and BSS2 – which are connected via a distribution system. A distribution system connects several BSSs via the AP to form a single network and thereby extends the wireless coverage area. This network is now called an extended service set (ESS) and has its own identifier, the ESSID. The ESSID is the _name ‘of a network and is used to separate different networks.

Without knowing the ESSID (and assuming no hacking) it should not be possible to participate in the WLAN. The distribution system connects the wireless networks via

The APs with a portal, which forms the interworking unit to other LANs.

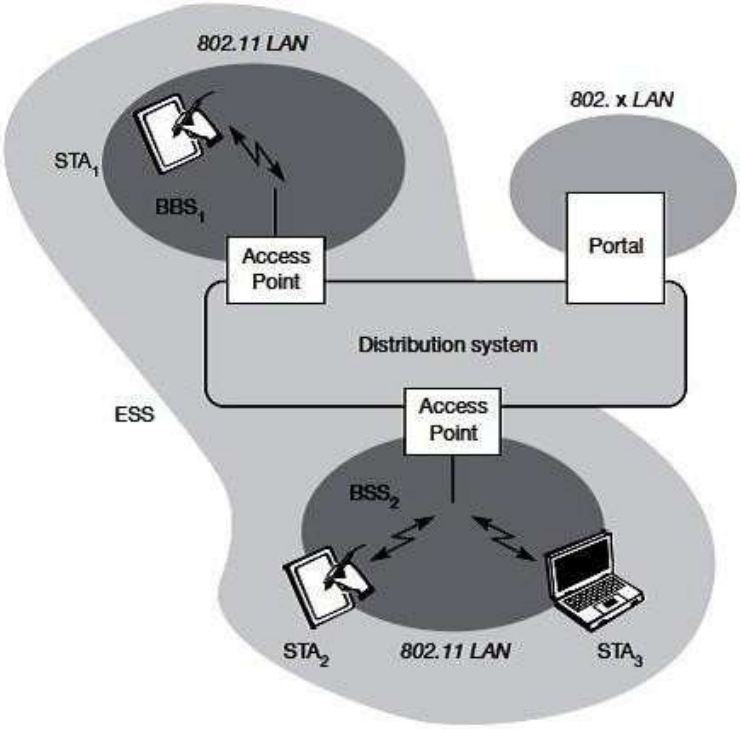


Fig. 1.3 Architecture of Infrastructure IEEE 802.11

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

The architecture of the distribution system consists of bridged IEEE LANs, wireless links, or any other networks. The APs support roaming (i.e., changing access points), the distribution system handles data transfer between the different APs. APs provide synchronization within a BSS, support power management, and can control medium access to support time-bounded service. In addition IEEE 802.11 allows the building of ad-hoc networks between stations, thus forming one or more independent BSSs (IBSS). In this case, an IBSS comprises a group of stations using the same radio frequency. Stations STA1, STA2, and STA3 are in IBSS1, STA4 and STA5 in IBSS2. This means for example that STA3 can communicate directly with STA2 but not with STA5. Several IBSSs can either be formed via the distance between the IBSSs or by using different carrier frequencies (then the IBSSs could overlap physically). IEEE 802.11 does not specify any special nodes 1 or

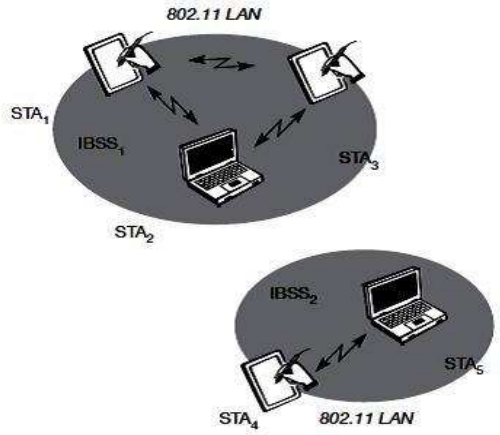


Fig. 1.4 Architecture of Adhoc IEEE 802.11

[Source: Text book - Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.2 Protocol architecture

IEEE 802.11 fits into the other 802.x standards for wired LANs. In the most common scenario: an IEEE 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via layers (application, TCP, IP) look the same for wireless nodes as for wired nodes. The upper part of the data link control layer, the logical link control (LLC), covers the differences of the medium access control layers needed for the different media.

The IEEE 802.11 standard only covers the physical layer PHY and medium access layer MAC like the other 802.x LANs do. The physical layer is subdivided into the physical layer convergence protocol (PLCP) and the physical medium dependent sub layer PMD. The basic tasks of the MacKaye comprise medium access, fragmentation of user data, and encryption. The PLCP sub layer provides a carrier sense signal, called clear channel assessment (CCA), and provides a common PHY service access point (SAP) independent of the transmission technology. Finally, the PMD sub layer handles modulation and encoding/decoding of signals.

Apart from the protocol sub layers, the standard specifies management layers and the station management. The MAC management supports the association and re-association of a station to an access point and roaming between different access points. It also controls authentication mechanisms, encryption, synchronization of a station with regard to an access point, and power management to save battery power. MAC management also maintains the MAC management information base (MIB).

The main tasks of the PHY management include channel tuning and PHYMIB maintenance. Finally, station management interacts with both management layers and is responsible for additional higher layer functions (e.g., control of bridging and interaction with the distribution system in the case of an access point).

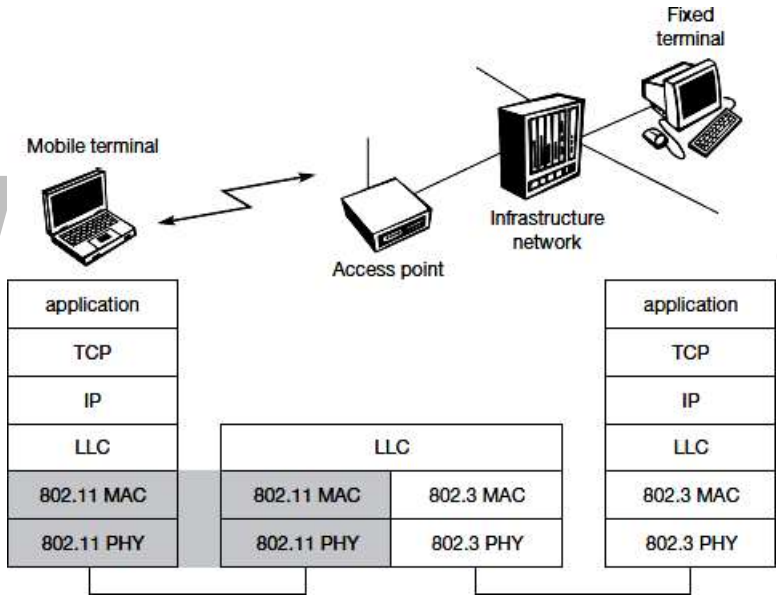
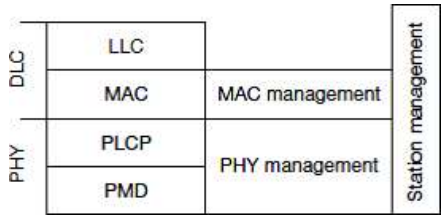


Fig. 1.5 IEEE 802.11 Protocol architecture and bridging

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]



[Source: Text book - Mobile Communications, Second Edition, Pearson Education bySchiller]

1.3.3 Physical layer

IEEE 802.11 supports three different physical layers: one layer based on infrared and two layers based on radio transmission (primarily in the ISM band at 2.4GHz, which is available worldwide). All PHY variants include the provision of the clear channel assessment signal (CCA). This is needed for the MAC mechanisms controlling medium access and indicates if the medium is currently idle.

The transmission technology determines exactly how this signal is obtained.

The PHY layer offers a service access point (SAP) with 1 or 2 Mbit/s transfer rate to the MAC layer (basic version of the standard).

1.3.4 Frequency hopping spread spectrum

Frequency hopping spread spectrum (FHSS) is a spread spectrum technique which allows for the coexistence of multiple networks in the same area by separating different networks using different hopping sequences. The original standard defines 79 hopping channels for North America and Europe, and 23 hopping channels for Japan (each with a bandwidth of1 MHz in the 2.4 GHz ISM band). The selection of a particular channel is achieved by using a pseudo-random hopping pattern.

The standard specifies Gaussian shaped FSK (frequency shift keying), GFSK, as modulation for the FHSS PHY. For 1 Mbit/s a 2 level GFSK is used (i.e., 1 bit is mappedto one frequency), a 4 level GFSK for 2 Mbit/s (i.e., 2 bits are mapped to one frequency). While sending and receiving at 1 Mbit/s is mandatory for all devices, operation at 2 Mbit/s is optional. This facilitated the production of low-cost devices for the lower rate only and more powerful devices for both transmission rates in the early days of 802.11.

The physical layer used with FHSS has the frame that consists of two basic parts, the PLCP part (preamble and header) and the payload part. While the PLCP part is always transmitted at 1 Mbit/s, payload, i.e.MAC data, can use 1 or 2 Mbit/s.

The fields of the frame fulfill the following functions:

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.

Start frame delimiter (SFD): The following 16 bits indicate the start of the frame and provide frame synchronization. The SFD pattern is0000110010111101.

PLCP_PDU length word (PLW): 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.

PLCP signaling field (PSF): This 4 bit field indicates the data rate of the payload following. All bits set to zero (0000) indicate the lowest data rate of 1 Mbit/s. The granularity is 500 kbit/s, thus 2 Mbit/s is indicated by 0010and the maximum is 8.5 Mbit/s(1111). This system obviously does not accommodate today‘s higher data rates.

Header error check (HEC): Finally, the PLCP header is protected by a16 bit checksum with the standard ITU-T generator polynomial
G(x) = x16 + x12 + x5 + 1.

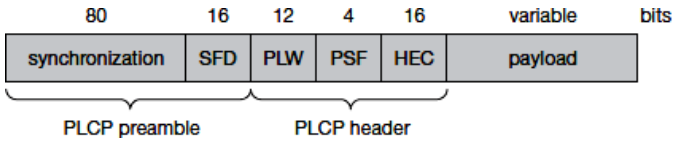


Fig. 1.6 Frame Format of IEEE 802.11 using FHSS

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.5 Direct sequence spread spectrum

Direct sequence spread spectrum (DSSS) is the alternative spread spectrum method separating by code and not by frequency. In the case of IEEE 802.11DSSS, spreading is achieved using the 11-chip Barker sequence (+1, –1, +1, +1, –1,+1, +1, +1, –1, –1,–1). The key characteristics of this method are its robustness against interference and its insensitivity to multipath propagation (time delay spread). However, the implementation is more complex compaIEEE114andoffersboth1and2bit/ binary

Phase shift keying (DBPSK) for 1 Mbit/s transmission and differential quadrature phase shift keying (DQPSK) for 2 Mbit/s as modulation schemes. The symbol rate is1 MHz, resulting in a chipping rate of 11 MHz All bits transmitted by the DSSSPHY are scrambled with the polynomial s(z) = z7 + z4 + 1 for DC blocking and whitening of the spectrum. Many of today's products offering 11 Mbit/s according to 802.11b are still backward compatible to these lower data rates.

The fields of the frame have the following functions:

Synchronization: The first 128 bits are not only used for synchronization, but also gain setting, energy detection (for the CCA), and frequency offset compensation. The synchronization field only consists of scrambled 1 bits.

Start frame delimiter (SFD): This 16 bit field is used for synchronization at the beginning of a frame and consists of the pattern 1111001110100000.

Signal: Originally, only two values have been defined for this field to indicate the data rate often 2 Mbit/s (and thus DQPSK). Other values have been reserved for future use, i.e., higher bit rates.

Service: This field is reserved for future use; however, 0x00 indicates an IEEE 802.11 compliant frame.

Length: 16 bits are used in this case for length indication of the payload in microseconds.

Header error check (HEC): Signal, service, and length fields are protected by this checksum using the ITU-T CRC-16 standard polynomial.

Fig. 1.7 Frame Format of IEEE 802.11 using DSSS

[Source: Text book - Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.6 Medium access control layer (MAC LAYER)

\The MAC layer has to control medium access, but it can also offer support for roaming, authentication, and power conservation. The basic services provided by the MAC layer are the mandatory asynchronous data service and an optional time-bounded service. While802.11 only offer the asynchronous service in ad-hoc network mode, both service types can be offered using an infrastructure-based network together with the access point coordinating medium access. The asynchronous service supports broadcast and multi- cast packets, and packet exchange is based on a _best effort 'model, i.e., no delay bounds can be given for transmission.

The following three basic access mechanisms have been defined for IEEE802.11:

- The mandatory basic method based on a version of CSMA/CA,
- An optional method avoiding the hidden terminal problem, and
- Finally a contention-free polling method for time-bounded service.

The first two methods are also summarized as distributed coordination function (DCF), The third method is called point coordination function (PCF). DCF only offers asynchronous service, while PCF offers both asynchronous and time-bounded service but needs an access point to control medium access and to avoid contention. The MAC mechanisms are also called distributed foundation wireless medium access control (DFWMAC).

For all access methods, several parameters for controlling the waiting time before medium access are important. The three different parameters that define the priorities of medium access. The values of the parameters depend on the PHY and are defined in relation to a slot time. Slot time is derived from the medium propagation delay, transmitter delay, and other PHY dependent parameters. Slot time is 50 μs for FHSS and 20 μs for DSSS. The medium, as shown, can be busy or idle (which is detected by the CCA).If the medium is busy this can be due to data frames or other control frames.

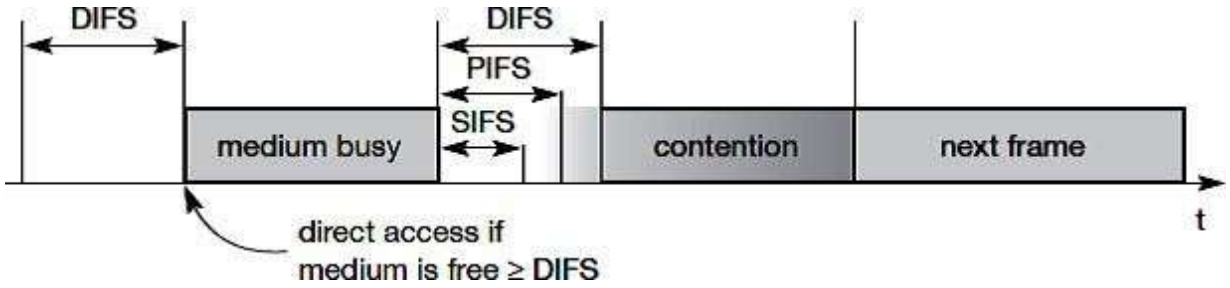


Fig. 1.8 Medium access and inter frame spacing

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

During a contention phase several nodes tryto access the medium.

Short inter-frame spacing (SIFS): The shortest waiting time for medium access (so the highest priority) is defined for short control messages, such as acknowledgements of data packets or polling responses. For DSSS SIFS is10 µs and for FHSS it is 28 µs.

PCF inter-frame spacing (PIFS): A waiting time between DIFS and SIFS (and tHus a medium priority) is used for a time-bounded service. An access point polling other nodes only has to wait PIFS for medium. PIFS is defined as SIFS plus one slot time.

DCF inter-frame spacing (DIFS): This parameter denotes the longest waiting Time and has the lowest priority for medium access. This waiting time is used for asynchronous data service within a contention period. DIFS is defined as SIFS plus two slottimes.

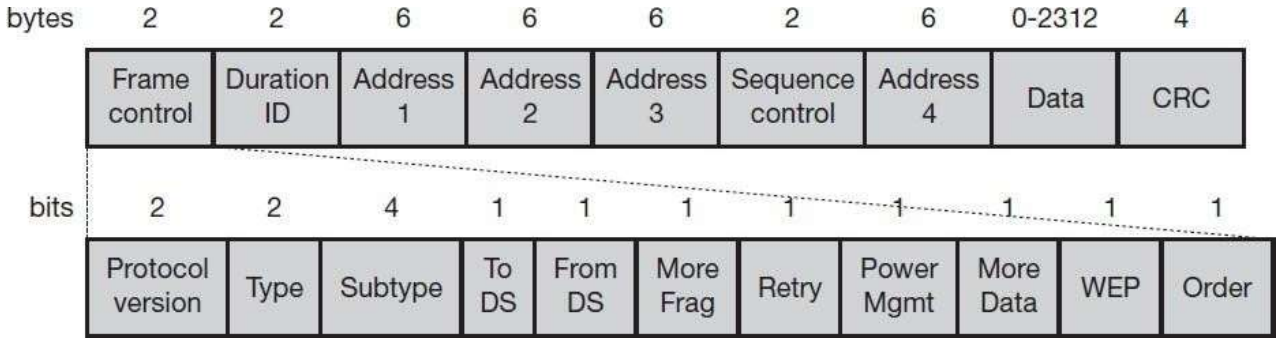


Fig. 1.9 Frame Control

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.7 MAC frames

The following figure shows the basic structure of an IEEE 802.11 MAC data ram together with the content of the frame control field.

● Frame control: The first 2 bytes serve several purposes. They contain several sub-fields.

● Duration/ID: If the field value is less than 32,768, the duration field contains the value indicating the period of time in which the medium is occupied (in μs). This field is used forsetting the NAV for the virtual reservation mechanism using RTS/CTS and during fragmentation. Certain values above 32,768 are reserved for identifiers.

● Address 1 to 4: The four address fields contain standard IEEE 802 MAC addresses (48 address depends on

● 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.

MAC frames can be transmitted

- Between mobile stations;
- Between mobile stations and
- An access point and between accesses points over a DS.

Two bits within the Frame Control field, _to DS 'and _from DS', differentiate these cases and control the meaning of the four addresses used. The following Table will gives an overview of the four possible bit values of the DS bits and the associated inter predation of the four address fields.

to DS	from DS	Address 1	Address 2	Address 3	Address 4
0	0	DA	SA	BSSID	–
0	1	DA	BSSID	SA	–
1	0	BSSID	SA	DA	–
1	1	RA	TA	DA	SA

Fig. 1.10 Interpretation of the MAC addresses in an 802.11 MAC frame

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

Every station, access point filters on address 1. This address identifies the physical receiver(s) of the frame. Based on this address, a station can decide whether the frame is relevant or not. The second address, address 2, represents the physical transmitter of a frame. This information is important because this particular sender is also the recipient of the MAC layer acknowledgement. If a packet from a transmitter (address 2) is received by the receiver with address 1, this receiver in turn acknowledges the data packet using address 2 as receiver address as shown in the Figure. The remaining two addresses address 3and address 4, are mainly necessary for the logical assignment of frames (logical sender, BSS identifier, logical receiver). If address 4 is not needed the field is omitted.

For addressing, the following four scenarios are possible:

- **Ad-hoc network:** If both DS bits are zero, the MAC frame organizes a packet which is exchanged between two wireless nodes without a distribution system. DA indicates the destination address, SA is the source address of the frame, which is identical to the physical receiver and sender addresses respectively. The third address identifies the basic service set (BSSID, the fourth address is unused.
- **Infrastructure network, from AP:** If the bit only from DS is set, the frame physically originates from an access point. DA is the logical and physical receiver, the second

Address identifies the BSS, and the third address specifies the logical sender, the source address of the MAC frame.

- **Infrastructure network, to AP:** If a station sends a packet to another station through the access point, only the _to DS 'bit is set. Now the first address represents the physical receiver of the frame, the access point, via the BSS identifier. The second address is the logical and physical sender of the frame, while the third address indicates the logical receiver.
- **Infrastructure network, within DS:** For packets transmitted between two access points over the distribution system, both bits are set. The first receiver address (RA), represents the MAC address of the receiving access point. Similarly, the second address transmitter address (TA), identifies the sending access point within the distribution system. Now two more addresses are needed to identify the original destination DA of the frame and the original source of the frame SA.

1.3.8 MAC management

MAC management plays a vital role in an IEEE 802.11 station as it controls all the functions related to integration of a wireless station into a BSS, formation of an ESS, synchronization of stations etc.

- Synchronization: It is used to support finding a wireless LAN, synchronization of internal clocks, and generation of beacon signals.
- Power management: It is used to control transmitter activity for power conservation,e.g., periodic sleep, buffering, without missing a frame.
- Roaming: Functions for joining a network (association), changing access points, scanning for access points.
- Management information base (MIB): All parameters representing the current state of a wireless station and an access point are stored within a MIB for internal and external access. A MIB can be accessed via standardized protocols such as the simple network management protocol (SNMP).

1.3.9 Synchronization

An internal clock is maintained by each node of an 802.11 network. Timing synchronization function is specified by the IEEE 802.11 to synchronize the clocks of all nodes.

In power management synchronized clocks are needed, but also for coordination of the PCF and for synchronization of the hopping sequence in an FHSS system. The start of a super frame can be predicted by the local timer of the node. FHSS physical layers need the same hopping sequences so that all nodes can communicate within a BSS.

A beacon contains a timestamp and other management information used for power management and roaming (e.g., identification of the BSS).The timestamp is used by a node to adjust its local clock. The node is not required to hear every beacon to stay synchronized; however, from time to time internal clocks should be adjusted. The transmission of a beacon frame is not always periodic because the beacon frame is also delayed if the medium is busy.

Within infrastructure-based networks, the access point performs synchronization by transmitting the (quasi)periodic beacon signal. However, the access point always tries to schedule transmissions according to the target beacon interval, i.e., beacon intervals are not shifted if one beacon is delayed. The timestamp of a beacon always reflects the real transmit time, not the scheduled time.

Ad-hoc networks, does not have an access point for beacon transmission. In this case, each beacon frame after the beacon interval. All other stations now adjust their internal clocks according to the received collision occurs, the beacon is lost.

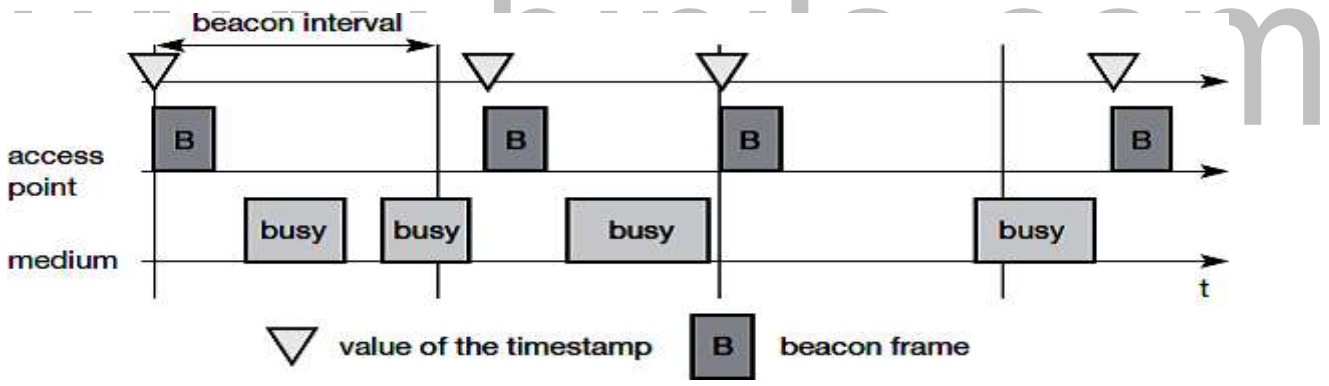


Fig. 1.11 Beacon transmission in a 802.11 network

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

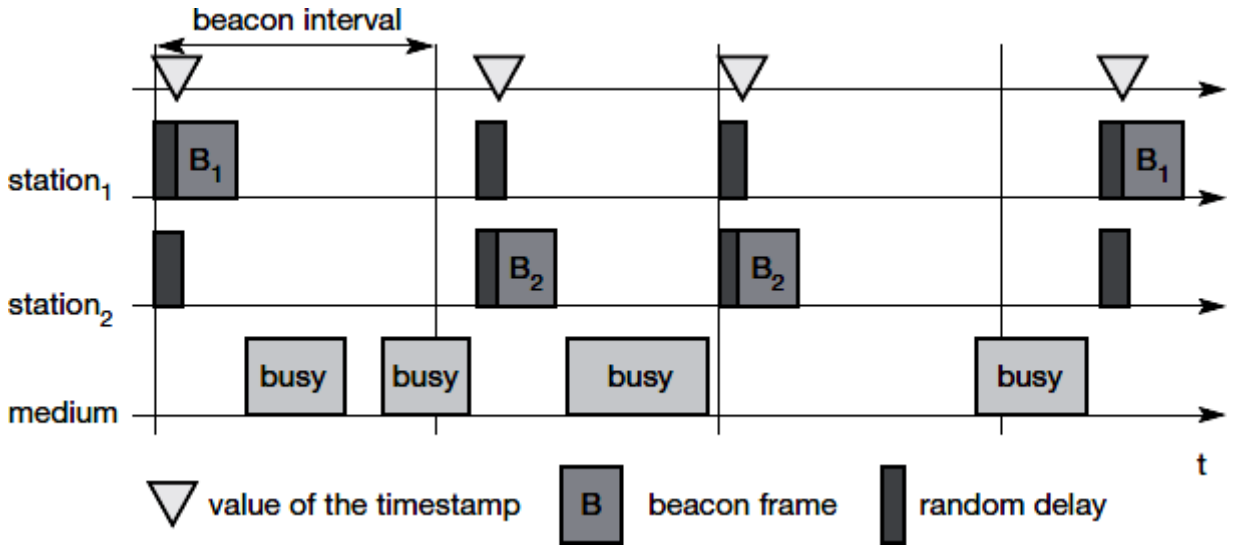


Fig. 1.11 Beacon transmission in a adhoc network

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.10 Power management

Wireless devices are battery powered. Hence power-saving mechanisms are critical for such devices. Standard LAN protocols are always ready to receive data, although receivers are idle most of the time in lightly loaded networks.

In IEEE 802.11 power management is to switch off the transceiver whenever it is not needed. This is simple for the sending device to achieve as the transfer is generated by the device itself. However, since the power management of a receiver cannot know in advance when the transceiver has to be active for a specific packet, it has to _wake up' the transceiver periodically.

Switching off the transceiver should be transparent to present protocols and able to support different applications. However, through put can be traded-off for battery life. Longer off-periods save battery life but average throughput will be reduce and vice versa.

The basic idea of power saving includes two states for a station: sleep and awake, and buffering of data in senders. If a sender aims to communicate with a power-saving station, if the station is a sleep it needs to buffer data. On the other hand the sleeping station has to wake up periodically and stay awake for a certain time. During this time, all senders can reveal the destinations of their buffered data frames. If a station detects that it is a destination of a buffered packet it has to stay awake until the transmission takes place. All stations have to wake up or be awake at the same time.

Compared to ad-hoc networks infrastructure-based networks has a simpler power

Management. The access point buffers all frames of stations operating in power-save mode. With every beacon sent by the access point, a traffic indication map (TIM) is Transmitted. The TIM contains a list of stations for which unicast data frames are buffered in the access point.
If the TIM indicates a unicast frame for the station, the station stays awake for transmission. Stations will always stay awake for multi-cast/broadcast transmission.
A sleeping station still has the TSF timer running.

The following figure shows an example with an access point and one station.

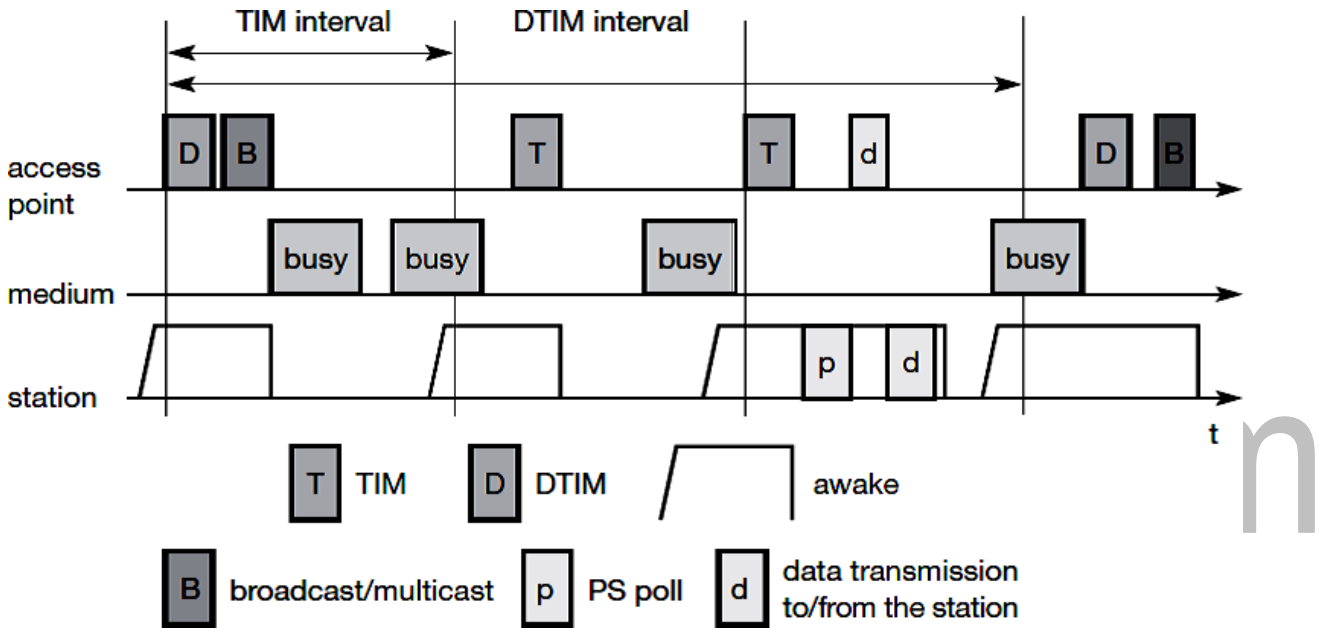


Fig. 1.12 Access Point with one station

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.11 Power management in IEEE 802.11 Network

The state of the medium is indicated. The access point transmits a beacon frame each beacon interval. This interval is now the same as the TIM interval. For sending broadcast/multicast frames, the access point maintains a delivery traffic indication map(DTIM) interval. The DTIM interval is always a multiple of the TIM interval.
In the first case, the access point has to transmit abroad cast frame and the station stays awake to receive it. After receiving the broadcast frame, the station returns to sleeping mode. Before the next TIM transmission starts, the station wakes up. This time the TIM is delayed due to a busy medium so, the station stays awake. The access point has nothing to send and the station goes back to sleep.

At the next TIM interval, the station is the destination for a buffered frame indicated by the access point. The access point then transmits the data for the station; the station acknowledges the receipt and may also send some data and it is acknowledged by the access point, afterwards, the station switches to sleep mode again. Finally, the access point has more broadcast data to send during the next DTIM interval, which is again delayed bay busy medium. A station may stay awake if the sleeping period would be too short.

This mechanism clearly shows the trade-off between short delays in station access and saving battery power. The shorter the TIM interval, the shorter the delay, but the lower the power-saving effect.

The power management for ad-hoc networks is much more complicated than in infrastructure networks. In this case, there is no access point to buffer data in one location but each station wants to buffer data if it wants to communicate with a power-saving station. Buffered frames list are announced by the stations during a period when they are all awake. Destinations are announced using ad-hoc traffic indication map (ATIMs) – the announcement period is called the ATIM window.

All stations stay awake for the ATIM interval as shown in the first two steps and go to sleep again if no frame is buffered for them. In the third step, station1 has data buffered forstation2. This is indicated in an ATIM transmitted by station1.

Station2 acknowledges this ATIM and stays awake for the transmission. After the ATIM window, station1can transmit the data frame, and station2 acknowledges its receipt. In this case place, more collisions happen and more stations are delayed. The access delay of large nitwits difficult

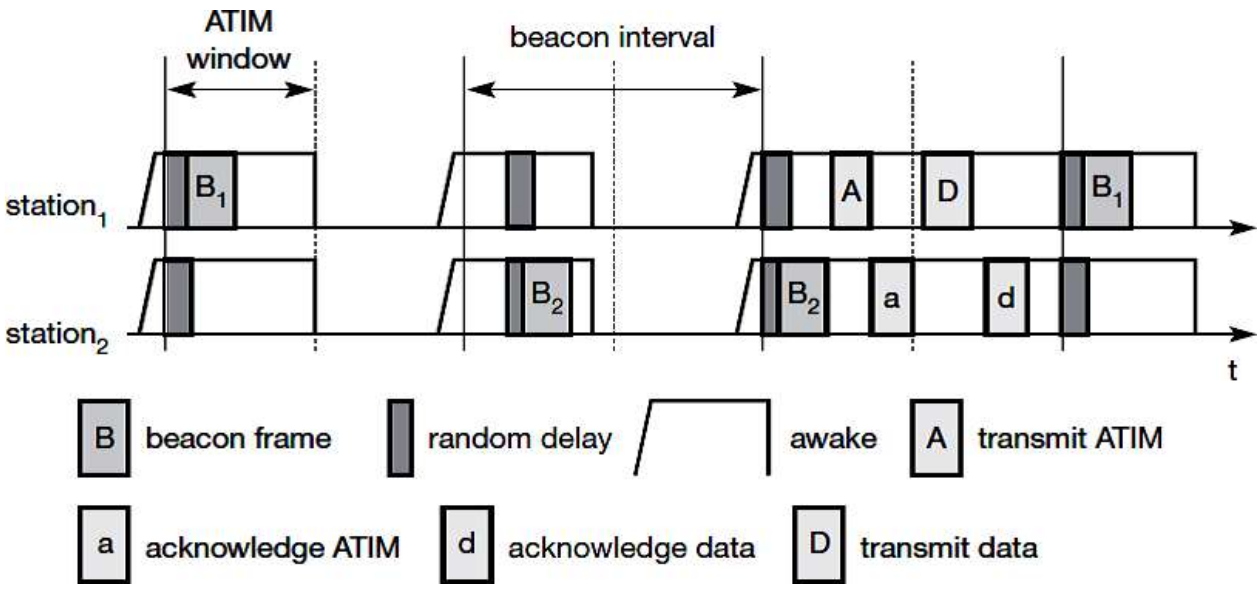


Fig. 1.13 Power management in IEEE 802.11 ad-hoc network

[Source: Text book -Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.3.12 Roaming

Access point more than one is required to cover all rooms when the wireless networks are within the buildings. Depending on the structure of the walls, one access point has a transmission range of 10–20 m. Each story of a building needs its own access point(s) as quite often walls are thinner than floors. If a user walks around within a wireless station, the station has to change from one access point to another to provide uninterrupted service. Moving between accesses points is refers to roaming.

The steps for roaming between access points are:

- When the current link quality to its access point AP1 is too poor. The station then starts scanning for another access point.

- Scanning will search for another BSS and can also be used for setting up a new BSS in case of ad-hoc networks. IEEE 802.11 specifies scanning on single or multiple channels and differentiates between passive scanning and active scanning. Passive scanning means listening into the medium to find other i.e., receiving the beacon of another network issued by the synchronization function within access point. Active scanning comprises sending a probe on each channel and waiting for a response. Beacon and probe responses contain the information necessary to join the new BSS.
- strength, and sends
- The new access point AP2 answers with an association response. If the response is successful, the station has roamed to the new access point AP2.

The access point accepting an association request indicates the new station in its BSS to the distribution system (DS). The DS then updates its database, which contains the current location of the wireless stations. This database is needed for forwarding frames between different BSSs, i.e. between the different access points controlling the BSSs, which combine to form an ESS.

The standard IEEE 802.11f should provide a compatible solution for all vendors. This also includes load-balancing between access points and key generation for security algorithms based on IEEE 802.1x (IEEE, 2001).

INTRODUCTION

1.1 WIRELESS LAN

A wireless LAN (or WLAN, for wireless local area network, sometimes referred to as LAWN, for local area wireless network) is one in which a mobile user can connect to a local area network (LAN) through a wireless (radio) connection. The IEEE802.11 group of standards specify the technologies for wireless LANs. 802.11 standards use the Ethernet protocol and CSMA/CA protocol.

There are three main ways by which WLANs transmit information: microwave, spread spectrum and infrared. WLANs have data transfer speeds ranging from 1 to 54Mbps, with some manufacturers offering proprietary 108Mbps solutions. The 802.11n standard can reach 300 to 600Mbps.

1.1.1 Types of Wireless LAN

There are two types of wireless LAN: "ad-hoc" and "infrastructure" networks.

1.1.1. Ad-hoc Networks

This network can be set up by a number of mobile users meeting in a small room. It does not implement this

- **Broadcasting/Flooding**
  Suppose that a mobile user A wants to send data to another user B in the same area. When the packets containing the data are ready, user A broadcasts the packets. On receiving the packets, the receiver checks the identification on the packet. If that receiver was not the correct destination, then it rebroadcasts the packets. This process is repeated until user B gets the data.
- **Temporary Infrastructure**
  In this method, the mobile users set up a temporary infrastructure. But this methods complicated and it introduces overheads. It is useful only when there is a small number of mobile users.

  Ad-hoc wireless networks, however, do not need any infrastructure to work. Each node can communicate directly with other nodes, so no access point controlling medium access is necessary. Nodes within an ad-hoc network can only

if they can reach each other physically, i.e., if they are within each other‘s radio range

or if other nodes can forward the message.

In ad-hoc networks, the complexity of each node is higher because every node has to implement medium access mechanisms, mechanisms to handle hidden or exposed terminal problems, and perhaps priority mechanisms, to provide a certain quality of service. This type of wireless network exhibits the greatest possible flexibility as it's, for example, needed for unexpected meetings, quick replacements of infrastructure or communication scenarios far away from any infrastructure.

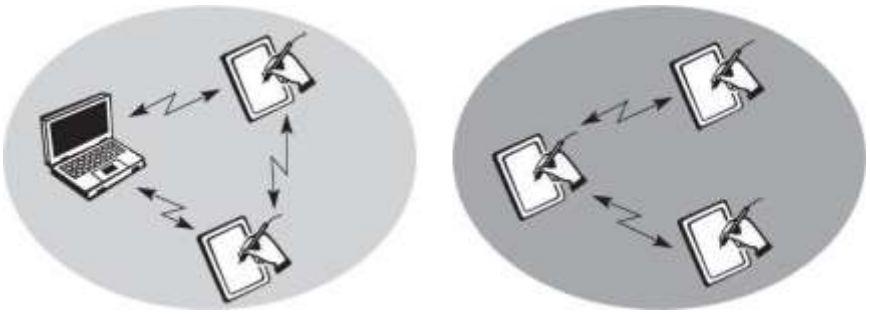


Fig. 1.1 Two adhoc wireless networks

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.1.1. Infrastructure Networks

The design of infrastructure-based wireless networks is simpler because most of The network functionality lies within the access point, whereas the wireless client's can remain quite simple. This structure is reminiscent of switched Ethernet or other star- based networks, where a central element (e.g., as witch) controls network flow. This type of network can use different access schemes with or without collision.

This type of network allows users to move in a building while they are connected to computer resources. The IEEE Project 802.11 specified the components in a wirelessLAN architecture. In an infrastructure network, a cell is also known as a Basic Service Area (BSA). It contains a number of wireless stations. The size of a BSA depends on the power of the transmitter and receiver units; it also depends on the environment. A number of BSAs are connected to each other and to a distribution system by Access Points (APs). A group of stations belonging to an AP is called a Basic Service Set (BSS).

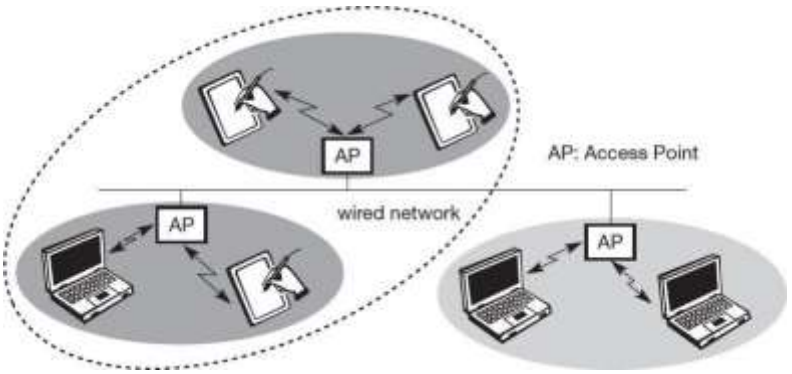


Fig. 1.2 Three infrastructure based wireless networks

[Source: Text book- Mobile Communications, Second Edition, Pearson Education by Jochen Schiller]

1.2 WLAN TECHNOLOGIES

1.2.1 INFRARED (IR)

Infrared is an invisible band of radiation that exists at the lower end of the visible electromagnetic spectrum. This type of transmission is most effective when a clear Line-of- sight exists between the transmitter and the receiver.

Two types of infrared WLAN solutions are available: diffused-beam and direct-beam (or line-of-sight). Currently, direct-beam WLANs offer a faster data rate than diffused-beam networks, but is more directional since diffused-beam technology uses reflected rays to transmit/receive a data signal, it achieves lower data rates in the 1-2 Mbps range.

Infrared optical signals are often used in remote control device applications. The users connect to the local wired network via an infrared device for retrieving information or using fax and print functions on a server. A group of users may also set up a peer-to peer infrared network while on location to share printer, fax, or other server facilities within their own LAN environment. When used indoors, it can be limited by solid objects such as doors, walls, merchandise, or racking. In addition, the lighting environment can affect signal quality.

For example, loss of communications may occur because of the large amount of sunlight or background light in an environment. Fluorescent lights also may contain large amounts of infrared. This problem may be solved by using high signal power and an optical bandwidth filter, which reduces the infrared signals coming from outside sources

Advantages

- No government regulations controlling use
- Immunity to electromagnetic and RF interference

Dis – Advantages

- A short range technology (30 to 50 ft. radius)
- Signals cannot penetrate solid objects
- Signal affected by light, fog, snow, etc.
- Dirt can interfere with infrared

1.2.2 UHF (Narrowband)

UHF wireless data communication systems normally transmit in the 430 to 470 MHz frequency range, with rare systems using segments of the 800 MHz range. The lower portion of this band 430-450 MHz is often referenced as unprotected (unlicensed) and 450-470 MHz is referred to as the protected (licensed) band.

In the unprotected band, RF licenses are not granted for specific frequencies and anyone is allowed are granted for specific frequencies, giving customers some assurance that they will have complete use of that frequency.

Other terms for UHF include narrowband and 400 MHz RF. Because independent narrowband RF systems cannot coexist on the same frequency, government agencies allocate specific radio frequencies to users through RF site licenses. A limited amount of unlicensed spectrum is also available in some countries. In order to have many frequencies that very small.

The term –narrowband is used to describe this technology because the RF signal is sENT in a very narrow bandwidth, typically 12.5 kHz or 25 kHz. Power levels range from 1 to 2 watts for narrowband RF data systems. This narrow bandwidth combined with high power results in large transmission distances than are available from 900 MHz or 2.4 GHz spread spectrum systems, which have lower power levels and wider bandwidths.

Wireless Universal Serial Bus (Wireless USB)

A Wireless USB (WUSB) is a Universal Serial Bus (USB) built on ultra-wideband (UWB) technology, which uses a radio frequency (RF) link, rather than cables, to transfer information between compatible USB devices.

The USB Implementers Forum, Inc. (USB-IF) discourages the WUSB abbreviation and prefers to reference the term as Certified Wireless USB.

WUSB enables 127-point connections with compatible devices and has a signal radius of three to 10 meters, with signal strength ranging from 480 to 110 Mbps. Security is ensured via transmission encryption.
Key WUSB features include:

- Plug and Play (PnP) compatibility and hot swapping with other devices
- Compatibility with earlier USB versions. However, a Device Wire Adapter (DWA) or WUSB hub is used to to facilitate the wired to wireless transition, enabling the wireless use of USB 2.0 devices and WUSB host connectivity.
- Host capability, which may be used with a PC through a Host Wire Adapter (HWA) that connects to a USB port or the Minibar Interface
- Support of a dual-role device (DRD), which works as a WUSB device, as well as a host with several features
- Like any successful standard, USB, Universal Serial Bus has kept pace with technology and the standard has been updated seeing USB 1, USB 1.1, USB2, USB3 and then USB 3.1, USB 3.2 and then USB 4.
- Each successive USB standard has added more to the technology, improving and refining the performance.
- With the use of USB being so widespread, backwards compatibility as far as is possible is very important, along with a future upgrade path.

- It is sometimes useful to compare USB1, vs USB 2, or USB2 vs USB3 etc looking at the different capabilities and specifications of each USB version.

USB Implementers Forum

- In order to ensure that USB is an industry standard and not one that is a standard for a particular manufacturer, the USB standard is developed and maintained by the USB Implementers Forum, USB-IF.
- This is a non-profit corporation that has been founded by the companies that developed the USB standard and now want to use and develop it.
- Some of the member companies for the USB-IF include companies such as Hewlett Packard, Intel, LSI Corporation, Rennes's, Microsoft, etc...
- The USB Implementers Forum develops and maintains the USB standards, including Wireless USB and runs a compliance programmer to maintain the quality of USB products and ensure compatibility between devices.

ZIGBEE

ZIGBEE is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless it networks. The Zigbee standard operates on the IEEE 802.15.4 physical radio specification and operates in unlicensed bands including 2.4 GHz, 900 MHz and 868 MHz.

The 802.15.4 specification upon which the Zigbee stack operates gained ratification by the Institute of Electrical and Electronics Engineers (IEEE) in 2003. The specification is a packet-based radio protocol intended for low-cost, battery-operated devices. The protocol

Allows devices to communicate in a variety of network topologies and can have battery life lasting several years.

The Zigbee 3.0 Protocol

The Zigbee protocol has been created and ratified by member companies of the Zigbee Alliance. Over 300 leading semiconductor manufacturers, technology firms, OEMs and service companies comprise the Zigbee Alliance membership. The Zigbee protocol was designed to provide an easy-to-use wireless data solution characterized by secure, reliable wireless network architectures.

ZIGBEE ADVANTAGE

The Zigbee 3.0 protocol is designed to communicate data through noisy RF environments that are common in commercial and industrial applications. Version 3.0 builds on the existing Zigbee standard but unifies the market-specific application profiles to allow all devices to be wirelessly connected in the same network, irrespective of their market designation and function. Furthermore, a Zigbee 3.0 certification scheme ensures the interoperability of products from different manufacturers. Connecting Zigbee 3.0 networks to the IP domain opens up monitoring and control from devices such as smartphones and tablets on a LAN or WAN, including the Internet, and brings the true Internet of Things to fruition.

Zigbee protocol features include:

- Support for multiple network topologies such as point-to-point, point-to-multipoint and mesh networks
- Low duty cycle – provides long battery life
- Low latency
- Direct Sequence Spread Spectrum (DSSS)
- Up to 65,000 nodes per network

- 128-bit AES encryption for secure data connections
- Collision avoidance, retries and acknowledgements

The Zigbee 3.0 software stack incorporates a ‘base device’ that provides consistent behavior for commissioning nodes into a network. A common set of commissioning methods is provided, including Touchline, a method of proximity commissioning.

Zigbee 3.0 provides enhanced network security. There are two methods of security that give rise to two types of network:

- Centralized security: This method employs a coordinator/trust center that forms the network and manages the allocation of network and link security keys to joining nodes.
- Distributed security: This method has no coordinator/trust center and is formed by a router. Any Zigbee router node can subsequently provide the network key to joining nodes.

Nodes adopt whichever security method is used by the network they join. Zigbee 3.0 supports the increasing scale and complexity of wireless networks, and copes with large local networks of greater than 250 nodes. Zigbee also handles the dynamic behavior of these networks (with nodes appearing, disappearing and re-appearing in the network) and allows orphaned nodes, which result from the loss of a parent, to re-join the network via a different parent. The self-healing nature of Zigbee Mesh networks also allows nodes to drop out of the network without any disruption to internal routing.

The backward compatibility of Zigbee 3.0 means that applications already developed under the Zigbee Light Link 1.0 or Home Automation 1.2 profile are ready for Zigbee 3.0. The Smart Energy profile is also compatible with Zigbee 3.0 at the functional level, but Smart Energy has additional security requirements that are only addressed within the profile.

Zigbee's Over-The-Air (OTA) upgrade feature for software updates during device operation ensures that applications on devices already deployed in the field can be seamlessly migrated to Zigbee 3.0. OTA upgrade is an optional functionality that manufacturers are encouraged to support in their Zigbee products.

Mesh Networks

A key component of the Zigbee protocol is the ability to support mesh networking. In a mesh network, nodes are interconnected with other nodes so that multiple pathways connect each node. Connections between nodes are dynamically updated and optimized through sophisticated, built-in mesh routing table.

Mesh networks are decentralized in nature; each node is capable of self-discovery on the network. Also, as nodes leave the network, the mesh topology allows the nodes to reconfigure routing paths based on the new network structure. The characteristics of mesh topology and ad-hoc routing provide greater stability in changing conditions or failure at single nodes.

Zigbee Applications

Zigbee enables broad-based deployment of wireless networks with low-cost, low-power solutions. It provides the ability to run for years on inexpensive batteries for a host of monitoring and control applications. Smart energy/smart grid, AMR (Automatic Meter Reading), lighting controls, building automation systems, tank monitoring, HVAC control, medical devices and fleet applications are just some of the many spaces where Zigbee technology is making significant advancements.

6LoWPAN

The 6LoWPAN system is used for a variety of applications including wireless sensor networks. This form of wireless sensor network sends data as packets and using IPv6 - providing the basis for the name - IPv6 over Low power Wireless Personal Area Networks.

6LoWPAN provides a means of carrying packet data in the form of IPv6 over IEEE 802.15.4 and other networks. It provides end-to-end IPv6 and as such it is able to provide direct connectivity to a huge variety of networks including direct connectivity to the Internet.

In this way, 6LoWPAN adopts a different approach to the other low power wireless sensor network solutions.

6LoWPAN and IETF

6LoWPAN is an open standard defined by the Internet Engineering Task Force, IETF in their document RFC 6282. The IETF is the standards body that defines many of the open standards used in the Internet including HTTP, TCP, UDP and many others.

Whilst 6LoWPAN was originally conceived to build on top of IEEE 802.15.4, a standard that set out the lower layers for a 2.4 GHz low power wireless system, it is now being developed and adapted to work with many other wireless bearers including Bluetooth Smart; power line control, PLC, and low power Wi-Fi.

The 6LoWPAN group have then defined the encapsulation and compression mechanisms that enable the IPv6 data to be carried of the wireless network.

The development of the 6LoWPAN system was not as easy as might be thought as the basic natures of the two systems are very different. However it was believed that using packet data over a low power wireless sensor network would offer significant advantages in terms of data handling and management.

6LoWPAN application areas

With many low power wireless sensor networks and other forms of ad hoc wireless networks, it is necessary that any new wireless system or technology has a defined area which it addresses. While there are many forms of wireless networks including wireless sensor networks, 6LoWPAN addresses an area that is currently not addressed by any other system, i.e. that of using IP, and in particular IPv6 to carry the data.

The overall system is aimed at providing wireless internet connectivity at low data rates and with a low duty cycle. However there are many applications where 6LoWPAN is being used:

- ***General Automation:*** There are enormous opportunities for 6LoWPAN to be used in many different areas of automation.
- ***Home automation:*** There is a large market for home automation. By connecting using IPv6, it is possible to gain distinct advantages over other IoT systems. The Thread initiative has been set up to standardize on a protocol running over 6LoWPAN to enable home automation.
- ***Smart Grid:*** Smart grids enable smart meters and other devices to build a micro mesh network and they are able to send the data back to the grid operator's monitoring and billing system using the IPv6 backbone.
- ***Industrial monitoring:*** Automated factories and industrial plants provide a great opportunity for 6LoWPAN and using automation, can enable major savings to be made. The ability of 6LoWPAN to connect to the cloud opens up many different areas for data monitoring and analysis.

6LoWPAN basics

The 6LoWPAN technology utilizes IEEE 802.15.4 to provide the lower layers for this low power wireless network system. While this seems a straightforward approach to the development of an packet data wireless network or wireless sensor network, there are incompatibilities between IPv6 format and the formats allowed by IEEE 802.15.4. This differences are overcome within 6LoWPAN and this allows the system to be used as a layer

Over the basic 802.15.4.

In order to send packet data, IPv6 over 6LowPAN, it is necessary to have a method of converting the packet data into a format that can be handled by the IEEE 802.15.4 lower layer system.

IPv6 requires the maximum transmission unit (MTU) to be at least 1280 bytes in length. This is considerably longer than the IEEE802.15.4's standard packet size of 127 octets which was set to keep transmissions short and thereby reduce power consumption.

To overcome the address resolution issue, IPv6 nodes are given 128 bit addresses in a hierarchical manner. The IEEE 802.15.4 devices may use either of IEEE 64 bit extended addresses or 16 bit addresses that are unique within a PAN after devices have associated. There is also a PAN-ID for a group of physically co-located IEEE802.15.4 devices.

6LoWPAN security

It is anticipated that the Internet of Things, IoT will offer hackers a huge opportunity to take control of poorly secured devices and also use them to help attack other networks and devices.

Accordingly security is a major issue for any standard like 6LoWPAN, and it uses AES-128 link layer security which is defined in IEEE 802.15.4. This provides link authentication and encryption.

Further security is provided by the transport layer security mechanisms that are also included. This is defined in RFC 5246 and runs over TCP.

For systems where UDP is used the transport layer protocol defined under RFC 6347 can be used, although this may require some specific hardware requirements.

6LoWPAN interoperability

One key issue of any standard is that of interoperability. It is vital that equipment from

Different manufacturers operates together.

When testing for interoperability, it is necessary to ensure that all layers of the OSI stack are compatible. To ensure that this can be achieved there several different specifications that are applicable.

Any item can be checked to conform it meets the standard, and also directly tested for interoperability.

6LoWPAN is a wireless / IoT style standard that has quietly gained significant ground. Although initially aimed at usage with IEEE 802.15.4, it is equally able to operate with other wireless standards making it an ideal choice for many applications.

6LoWPAN uses IPv6 and this alone has to set it aside from the others with a distinct advantage. With the world migrating towards IPv6 packet data, a system such 6LoWPAN offers many advantages for low power wireless sensor networks and other forms of low power wireless networks.

Wireless HART

Wireless HART uses a **2.4 GHz band**—license-free and used worldwide—as a transfer medium for several radio technologies, including WLAN, Bluetooth, and ZigBee. But, **Wireless HART** is much more than a WLAN variant.

Wireless HART uses a **flat mesh network** where all radio stations (field devices) form a network. Every participating station serves simultaneously as a **signal source** and a **repeater**. The original transmitter sends a message to its nearest neighbor, which passes the message on until the message reaches the base station and the actual receiver. In addition, **alternative routes** are set up in the initialization phase. If the message cannot be transmitted on a particular path, due to an obstacle or a defective receiver, the message is automatically passed to an alternative route. So, in addition to extending the range of the

Network, the **flat mesh network** provides redundant communication routes to increase reliability.

The communication in the **Wireless Network** is coordinated with TDMA (Time Division Multiple Access), which synchronizes the network participants in 10 ms timeframes. This enables a very reliable (collision-free) network, and reduces the lead and lag times during which a station must be active.

To avoid jamming, **Wireless HART** uses also FHSS (Frequency Hopping Spread Spectrum). All 15 channels as defined in IEEE802.15.4 are used in parallel; **Wireless HART** uses FHSS to "hop" across these channels. Channels that are already in use are blacked out to avoid collisions with other wireless communication systems.

The combination of 10s synchronization and 15 channels allows 1500 communications per second.

Wireless HART is a wireless communications protocol for process automation applications. It adds wireless capabilities to HART technology while maintaining compatibility with existing HART devices, commands, and tools. Wireless HART uses mesh networking technology. Each device in a mesh network can serve as a router for messages from other devices. In other words, a device doesn't have to communicate directly to a gateway, but just forward its message to the next closest device. This extends the range of the network and provides redundant communication routes to increase reliability, particularly in the difficult radio environment found in process facilities.

Each Wireless HART network includes three main elements:

- Wireless field devices connected to process or plant equipment. This device could be a device with Wireless HART built in or an existing installed HART-enabled device with a Wireless HART adapter attached to it.

- Gateways enable communication between these devices and host applications connected to a high-speed backbone or other existing plant communications network.
- A Network Manager is responsible for configuring the network, scheduling communications between devices, managing message routes, and monitoring network health. The Network Manager can be integrated into the gateway, host application, or process automation controller.

WPAN – IEEE 802.15.4

IEEE 802.15.4 is a standard that was developed to provide a framework and the lower layers in the OSI model for low cost, low power wireless connectivity networks.

IEEE 802.15.4 provides the MAC and PHY layers, leaving the upper layers to be developed for specific higher later standards like Thread, Zigbee, 6LoWPAN and many others.

As a result, IEEE 802.15.4 does not take the limelight in the way that other standards might, but nevertheless it forms the basis for a large number of standards and accordingly it is far more widely deployed than may be apparent at first sight.

Low power is one of the key elements of 802.15.4 as it is used in many areas where remote sensors need to operate on battery power, possibly for years without attention.

IEEE 802.15.4 basics

The IEEE 802.15.4 standard is aimed at providing the essential lower network layers for a wireless personal area network, WPAN. The chief requirements are low-cost, low-speed ubiquitous communication between devices.

IEEE 802.15.4 does not aim to compete with the more commonly used end user-oriented systems such as IEEE 802.11 where costs are not as critical and higher speeds are demanded and power may not be quite as critical. Instead, IEEE 802.15.4 provides for very low cost communication of nearby devices with little to no underlying infrastructure.

The concept of IEEE 802.15.4 is to provide communications over distances up to about 10 meters and with maximum transfer data rates of 250 kbps. Anticipating that cost reduction will require highly embedded device solutions, the overall concept of IEEE 802.15.4 has been devised to accommodate this.

IEEE 802.15.4 standard

The IEEE 802.15.4 standard has undergone a number of releases. In addition to this there are a number of variants of the IEEE 802.15.4 standard to cater for different forms of physical layer, etc. These are summarized below in the table.

IEEE 802.15.4 STANDARD SUMMARY

IEEE 802.15.4 VERSION	DETAILS AND COMMENTS
IEEE 802.15.4 - 2003	This was the initial release of the IEEE 802.15.4 standard. It provided for two different PHYs - one for the lower frequency bands of 868 and 915 MHz, and the other for 2.4 GHz.
IEEE 802.15.4 - 2006	This 2006 release of the IEEE 802.15.4 standard provided for an increase in the data rate achievable on the lower frequency bands. This release of the standard updated the PHY for 868 and 915 MHz It also defined four new modulation schemes that could be used - three for the lower frequency bands, and one for 2.4 GHz.
IEEE 802.15.4a	This version of the IEEE 802.15.4 standard defined two new PhysX

IEEE 802.15.4 STANDARD SUMMARY

IEEE 802.15.4 VERSION	DETAILS AND COMMENTS
	One used UWB technology and the other provided for using chirp spread spectrum at 2.4 GHz.
IEEE 802.15.4c	Updates for 2.4 GHz, 868 MHz and 915 MHz, UWB and the China 779-787 MHz band.
IEEE 802.15.4d	2.4 GHz, 868 MHz, 915 MHz and Japanese 950 - 956 MHz band.
IEEE 802.15.4e	This release defines MAC enhancements to IEEE 802.15.4 in support of the ISA SP100.11a application.
IEEE 802.15.4f	This will define new PHYs for UWB, 2.4 GHz band and also 433 MHz
IEEE 802.15.4g	This will define new PHYs for smart neighborhood networks. These may include applications such as smart grid applications for the energy industry. It may include the 902 - 928 MHz band.

Although new versions of the standard are available for use by any of the higher layer standards, Zigbee still uses the initial 2003 release of the IEEE 802.15.4 standard.

IEEE 802.15.4 applications

The IEEE 802.15.4 technology is used for a variety of different higher layer standards. In this way the basic physical and MAC layers are already defined, allowing the higher layers to be provided by individual system in use.

IEEE 802.15.4 DERIVED STANDARDS

APPLICATION OR SYSTEM	DESCRIPTION OF THE IEEE 802.15.4 APPLICATION OR SYSTEM
Zigbee	Zigbee is supported by the Zigbee Alliance and provides the higher levels required for low powered radio system for control applications including lighting, heating and many other applications.
Wireless HART	Wireless HART is an open-standard wireless networking technology that has been developed by HART Communication Foundation for use in the 2.4 GHz ISM band. The system uses IEEE802.15.4 for the lower layers and provides a time synchronized, self-organizing, and self-healing mesh architecture.
RF4CE	RF4CE, Radio Frequency for Consumer Electronics has amalgamated with the Zigbee alliance and aims to provide low power radio controls for audio visual applications, mainly for domestic applications such as set to boxes, televisions and the like. It promises enhanced communication and facilities when compared to existing controls.
MiWi	MiWi and the accompanying MI WI P2P systems are designed by

IEEE 802.15.4 DERIVED STANDARDS

APPLICATION SYSTEM	OR DESCRIPTION OF THE IEEE 802.15.4 APPLICATION OR SYSTEM
	Microchip Technology. They are designed for low data transmission rates and short distance, low cost networks and they are aimed at applications including industrial monitoring and control, home and building automation, remote control and automated meter reading.
ISA100.11a	This standard has been developed by ISA as an open-standard Wireless networking technology and is it described as a wireless system for industrial automation including process control and other related applications.
6LoWPAN	This rather unusual name is an acronym for "IPv6 over Low power Wireless Personal Area Networks" It is a system that uses the basic IEEE 802.15.4, but using packet data in the form of Ipv6.

While the IEEE 802.15.4 standard may not be as well-known as some of the higher level standards and systems such as Zigbee that use IEEE 802.15.4 technology as the underpinning lower levels system, it is nevertheless very important. It spans a variety of different systems, and as such provides a new approach - providing only the lower layers, and allowing other systems to provide the higher layers which are tailored for the relevant application.

IEEE 802.15.4 frequencies and frequency bands

The IEEE 802.15.4 frequency bands align with the licence free radio bands that are available around the globe. Of the bands available, the 2.4 GHz (2 400 MHz) band is the most widely used in view of the fact that it is available globally and this brings many economies of scale.

IEEE 802.15.4 RF CHANNEL DETAILS

FREQUENCY BAND (MHZ)	CHANNELS AVAILABLE	THROUGHPUT AVAILABLE (KBPS)	REGION USE ALLOWABLE
868 - 868.6	1	20	Europe
902 - 928	10 (2003 rel) 30 (2006 rel)	30	USA
2 400	16	250	Global

With new allocations arising as a result of issues such as the digital dividend and other countries adopting and using IEEE 802.15.4, other frequencies and bands are being considered. These include: 314-316 MHz, 430-434 MHz, and 779-787 MHz frequency bands in China and the 950 MHz-956 MHz band in Japan. Other frequencies are also being considered for UWB variants of IEEE 802.15.4.

IEEE 802.15.4 modulation formats

There were two different modulation schemes defined for IEEE 802.15.4 in the original standard released in 2003. Both these air interface or radio interface configurations are based on direct sequence spread spectrum, DSSS techniques. The one for the lower frequency bands provides a lower data rate in view if

the smaller channel width, whereas the format used at 2.4 GHz enables data to be transferred at rates up to 250 kbps.

The 2006 release of the 802.15.4 standard upgraded an number of areas of the air interface and the modulation schemes. There were four different physical layers that were defined. Three used the DSS approach using either binary or offset quadrature phase shift keying, BPSK and OQPSK. An optional physical layer approach was defined using amplitude sift keying, ASK.

IEEE 802.15.4 MAC overview

The purpose of the IEEE 802.15.4 MAC layer is to provide an interface between the PHY or physical layer and the application layer. The as IEEE 802.15.4 does not specify an application layer, this is generally an application system such as Zigbee, RF4CE, MiWi, etc.

The IEEE 802.15.4 MAC provides the interface to the application layer using two elements:

- ***FFD:*** Full Function Device - a node that has full levels of functionality. It can be used for sending and receiving data, but it can also route data from other nodes.
- ***RFD:*** Reduced Function Device - a device that has a reduced level of functionality. Typically it is an end node which may be typically a sensor or switch. RFDs can only talk to FFDs as they contain no routing functionality. These devices can be very low power devices because they do not need to route other traffic and they can be put into a sleep mode when they are not in use.

  These RFDs are often known as child devices as they need other parent devices with which to communicate.
- ***Coordinator:*** This is the node that controls the IEEE 802.15.4 network. This is a special form of FFD. In addition to the normal FFD functions it also sets the IEEE 802.15.4 network up and acts as the coordinator or manager of the network. ***MAC Management Service:*** This is called the MAC Layer

- ***Star topology:*** As the name implies the start format for an IEEE 802.15.4 network topology has one central node called the PAN coordinator with which all other nodes communicate.
- ***Peer to Peer network topology:*** In this form of network topology, there is still what is termed a PAN coordinator, but communications may also take place between different nodes and not necessarily via the coordinator.

It is worth defining the different types of devices that can exist in a network. There are three types:
Management Entity, MLME. It provides the service interfaces through which layer management functions may be called or accessed. The IEEE
802.15.4 MAC MLME is also responsible for controlling a database of objects for the MAC layer. This database is referred to as the MAC layer PAN information base or PIB. The MLME also has access to MCPS services for data transport activities.

- ***MAC Data Service:*** This si called the MAC Common Port Layer, MCPS. This entity within the IEEE 802.15.4 MAC provides data transport services between the peer MACs.

IEEE 802.15.4 network topologies

There are two main forms of network topology that can be used within IEEE 802.15.4. These network topologies may be used for different applications and offer different advantages.

The two IEEE 802.15.4 network topologies are:

These definitions were originally generated for use in Zigbee, but their use has now been introduced with IEEE 802.15.4 network terminology.

IEEE 802.15.4 star topology

In the star topology, all the different nodes are required to talk only to the central PAN coordinator. Even if the nodes are FFDs and are within range of each other, in a star network topology, they are only allowed to communicate with the coordinator node.

Having a star network topology does limit the overall distances that can be covered. It is limited to one hop.

IEEE 802.15.4 peer to peer topology

A peer to peer, or p2p network topology provides a number of advantages over a star network topology. In addition to communication with the network coordinator, devices are also able to communicate with each other. FFDs are able to route data, while the RFDs are only able to provide simple communication.

The fact that data can be routed via FFD nodes means that the network coverage can be increased. Not only can overall distances be increased, but nodes masked from the main network coordinator can route their data via another FFD node that it may be able to communicate with.