UNIT I **WIRELESS LAN** **9 HOURS**

Introduction- WLAN technologies: - IEEE802.11: System architecture, protocol architecture, 802.11b, 802.11a – Hiper LAN: WATM, BRAN, HiperLAN2 – Bluetooth: Architecture, WPAN – IEEE 802.15.4, Wireless USB, Zigbee, 6LoWPAN, WirelessHART

INTRODUCTION

A wireless LAN is a LAN that utilizes radio-frequency communication to permit data transmission among fixed, nomadic, or moving computers.

WLANs are designed to operate in industrial, scientific, and medical (ISM) radio bands. WLANs combine data connectivity with user mobility

Infrastructure mode: *Several computers are connected over the air to a central AP that in turn links to the wired network.*

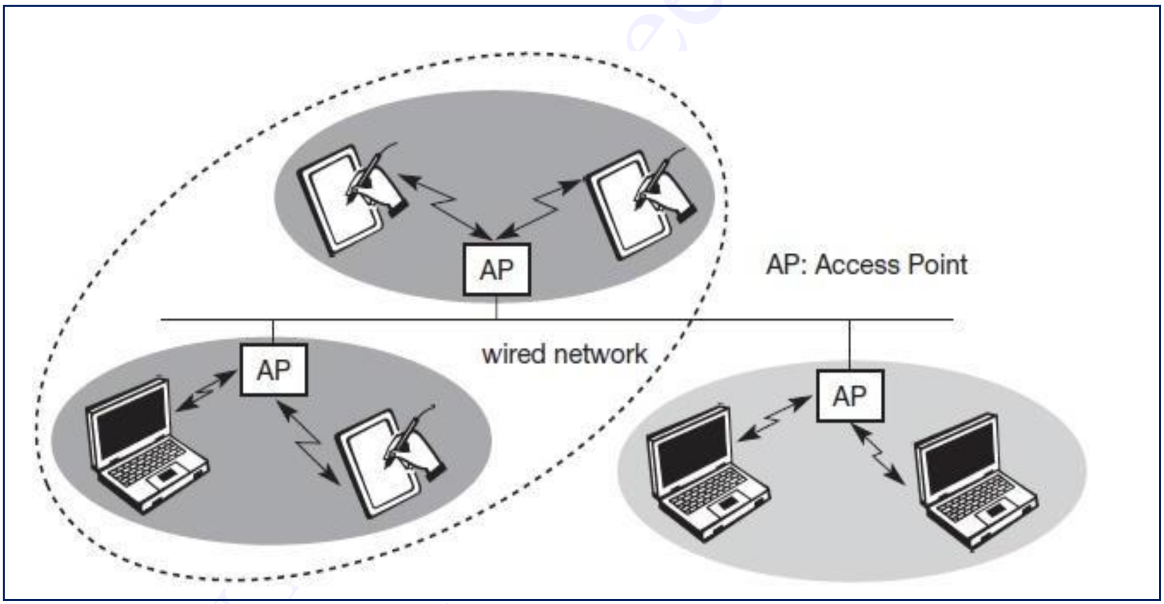


Fig 1: Three infrastructures based wireless networks

Ad hoc mode*: is more flexible than infrastructure mode in that it does not require any central or distributed infrastructure devices or computers to operate.*

Computers in an ad hoc wireless LAN temporarily self-organize into a group to serve each other in a peer-to-peer manner.

In some cases when it is not feasible to build a network infrastructure for technical or other reasons (e.g., troops on the battlefield or sports spectators in a huge stadium), an ad hoc wireless LAN seems a good solution.

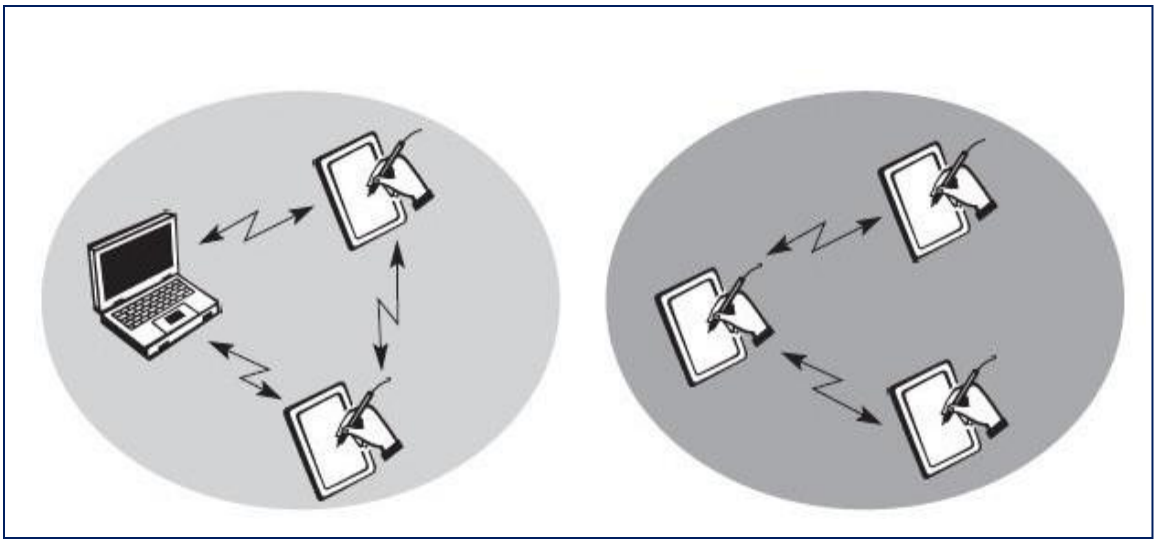


Fig 2: example of two ad-hoc wireless networks

- ***Wireless LAN (WLAN)s*** are typically restricted in their diameter to buildings, a campus, single rooms etc. and are operated by individuals, not by large-scale network providers.

- The global goal of WLANs is to replace office cabling, to enable tetherless access to the internet and, to introduce a higher flexibility for ad-hoc communication in, e.g., group meetings.

Advantages of WLANs :

1. **Flexibility:** Within radio coverage, nodes can communicate without further restriction. Radio waves can penetrate walls, senders and receivers can be placed anywhere (also non-visible, e.g., within devices, in walls etc.).

2. **Planning:** Only wireless ad-hoc networks allow for communication without previous planning, any wired network needs wiring plans.

3. **Design:** Wireless networks allow for the design of small, independent devices which can for example be put into a pocket. Cables not only restrict users but also designers of small PDAs, notepads etc.

4. **Robustness:** Wireless networks can survive disasters, e.g., earthquakes or users pulling a plug. If the wireless devices survive, people can still communicate.

5. **Cost:** After providing wireless access to the infrastructure via an access point for the first user, adding additional users to a wireless network will not increase the cost.

Disadvantages of WLANs :

1. **Quality of service:** WLANs typically offer lower quality than their wired counterparts. The main reasons for this are the lower bandwidth due to limitations in radio transmission (e.g., only 1–10 Mbit/s user data rate instead of 100–1,000 Mbit/s), higher error rates due to interference (e.g., 10–4 instead of 10–12 for fiber optics), and higher delay/delay variation due to extensive error correction and detection mechanisms.

2. **Proprietary solutions:** Due to slow standardization procedures, many companies have come up with proprietary solutions offering standardized functionality plus many enhanced features (typically a higher bit rate using a patented coding technology or special inter-access point protocols).

3. **Restrictions:** All wireless products have to comply with national regulations. Several government and non-government institutions worldwide regulate the operation and restrict frequencies to minimize interference.

Safety and security: Using radio waves for data transmission might interfere with other high-tech equipment in, e.g., hospitals. Special precautions have to be taken to prevent safety hazards.

WLAN TECHNOLOGIES

The technologies available for use in a WLAN include

infrared,

UHF (narrowband) and

spread spectrum implementation

Infrared Technology

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 the diffused-beam networks.

- Direct-beam 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 is a short-range technology. 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 communication may occur because of the large amount of sunlight or background light in an environment.

Considerations for choosing infrared technology

Advantages:	No government regulations controlling use Immunity to electro-magnetic (EM) and RF interference
Disadvantages:	Generally a short-range technology (30–50 ft radius under ideal conditions) Signals cannot penetrate solid objects Signal affected by light, snow, ice, fog Dirt can interfere with infrared

UHF Narrowband Technology

- UHF wireless data communication systems have been available since the early 1980s.
- These 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 referred to as the unprotected (unlicensed), and 450–470 MHz is referred to as the protected (licensed) band.
- 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.

Considerations for choosing UHF technology.

Advantages:	Longest range Low cost solution for large sites with low to medium data throughput Requirements
Disadvantages:	Large radio and antennas increase wireless client size RF site license required for protected bands No multivendor interoperability Low throughput and interference potential

Spread Spectrum Technology

- A wideband radio frequency technique that uses the entire allotted spectrum in a shared fashion as opposed to dividing it into discrete private pieces (as with narrowband).
- The spread spectrum system spreads the transmission power over the entire usable spectrum.
- This is obviously a less efficient use of the bandwidth than the narrowband approach. However, spread spectrum is designed to trade off bandwidth efficiency for reliability, integrity, and security.
- In commercial applications, spread spectrum techniques currently offer data rates up to 2 Mbps.

Two modulation schemes are commonly used to encode spread spectrum signals:
direct sequence spread spectrum (DSSS) and
frequency hopping spread spectrum (FHSS).

FHSS uses a narrowband carrier that changes frequency in a pattern known to both transmitter and receiver.

- Properly synchronized, the net effect is to maintain a single logical channel.
- To an unintended receiver, FHSS appears to be a short-duration impulse noise.

The transmitter device "listens" to a channel, if it detects an idle time (i.e. no signal is transmitted), it transmits the data using the full channel bandwidth.

If the channel is full, it "hops" to another channel and repeats the process. The transmitter and the receiver "jump" in the same manner.

DSSS generates a redundant bit pattern for each bit to be transmitted. This bit pattern is called a *spreading code*.

- The longer the code, the greater the probability that the original data can be recovered (and, of course the more bandwidth will be required).
- To an unintended receiver DSSS appears as low-power, wide band noise and is rejected by most narrowband receivers.

A code is transmitted with each signal so that the receiver can identify the appropriate signal transmitted by the sender unit.
The frequency at which such signals are transmitted is called the ISM (industrial, scientific and medical) band.
This frequency band is reserved for ISM devices.

The ISM band has three frequency ranges : 902-928, 2400-2483.5 and 5725-5850 MHz.

IEEE 802.11

Introduction:
A simple and robust WLAN offers time-bounded and asynchronous services.

The MAC layer of IEEE 802.11 should be able to operate with multiple physical layers (infra red and spread spectrum radio transmission techniques), each of which exhibits a different medium sense and transmission characteristic.

System Architecture

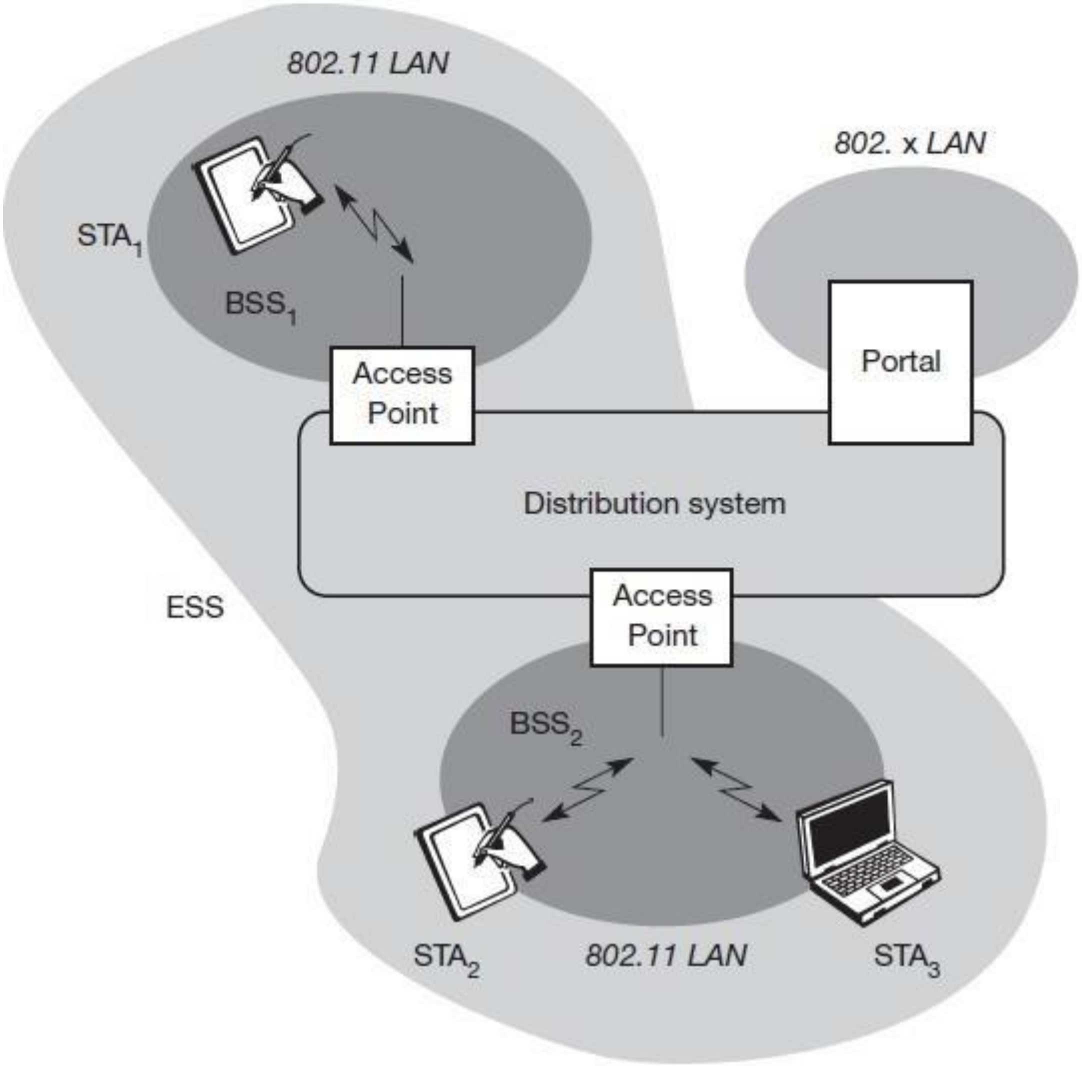


Fig 3: Architecture of infrastructure based IEEE 802.11

The above fig shows the components of an infrastructure and a wireless part as specified for IEEE 802.11.

1. Several nodes, called **stations (STAi)**, are connected to **access points (AP)**.

2. Stations are terminals with access mechanisms to the wireless medium and radio contact to the AP.

3. The stations and the AP which are within the same radio coverage form a **basic service set (BSSi)**.

4. 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.

5. 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.

6. The distribution system connects the wireless networks via the APs with a **portal**, which forms the interworking unit to other LANs.

7. Stations can select an AP and associate with it. The APs support roaming (i.e., changing access points), the distribution system handles data transfer between the different APs.

8. APs provide synchronization within a BSS, support power management, and can control medium access to support time-bounded service.

9. In addition to infrastructure-based networks, IEEE 802.11 allows the building of ad-hoc networks between stations, thus forming one or more independent BSSs (IBSS) as shown in figure below

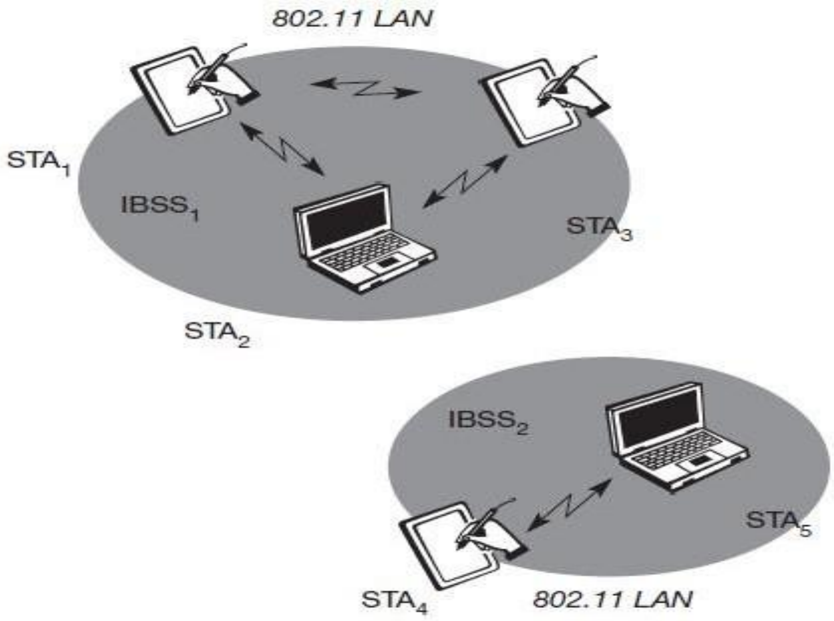


Fig 4: Architecture of IEEE 802.11 ad-hoc wireless LAN

10. 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.

11. 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).

Protocol Architecture

The WLAN behaves like a slow wired LAN. Consequently, the higher 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.

Figure below shows the most common scenario: an IEEE 802.11 wireless LAN connected to a switched IEEE 802.3 Ethernet via a bridge

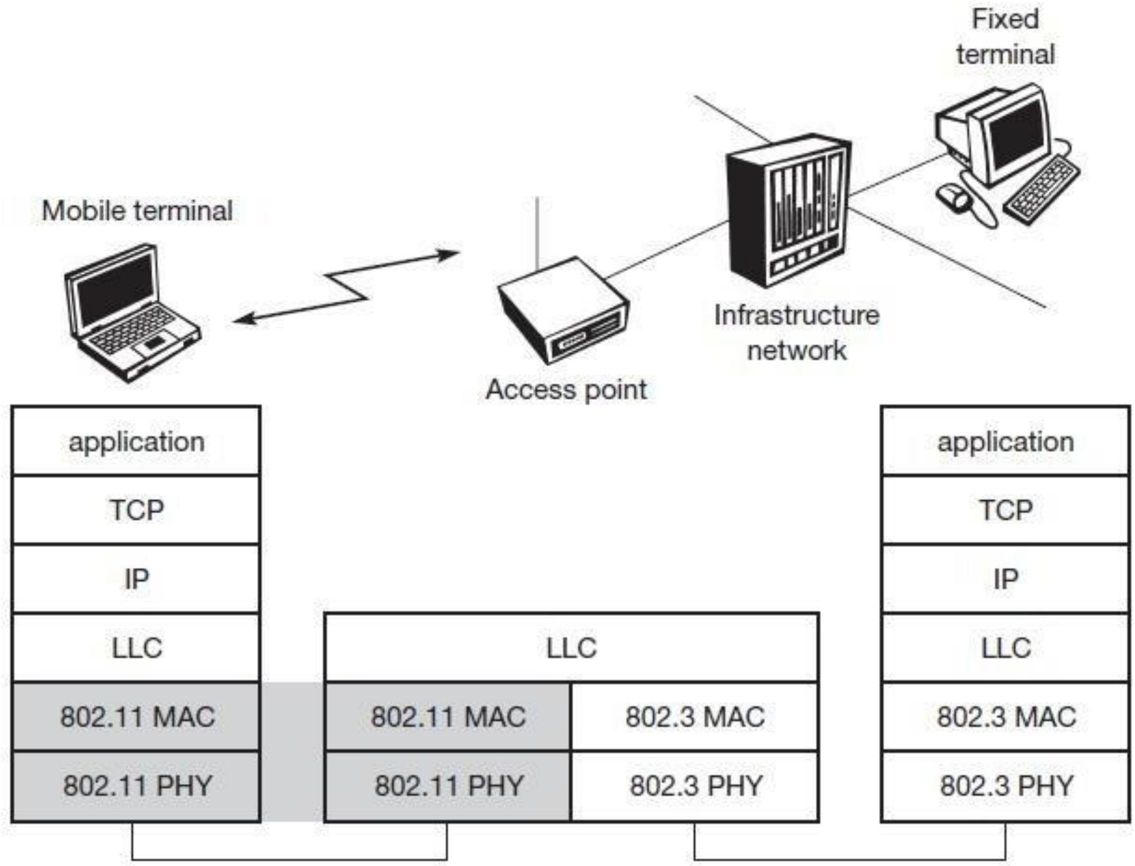


Fig 5: IEEE 802.11 Protocol Architecture and Bridging

1. The IEEE 802.11 standard only covers the physical layer **PHY** and medium access layer **MAC** like the other 802.x LANs do.

2. The physical layer is subdivided into the **physical layer convergence protocol (PLCP)** and the **physical medium dependent** sublayer **PMD**

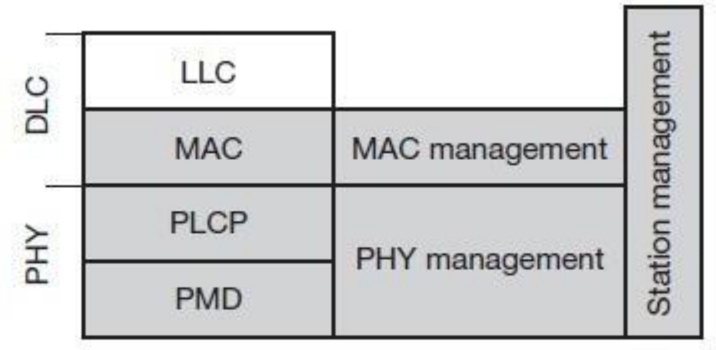


Fig 6: Detailed IEEE 802.11 protocol architecture and management

3. The basic tasks of the **MAC layer** comprise medium access, fragmentation of user data, and encryption.

4. The **PLCP sublayer** provides a carrier sense signal, called clear channel assessment (CCA), and provides a common PHY service access point (SAP) independent of the transmission technology.

5. Finally, the **PMD sublayer** handles modulation and encoding/decoding of signals.

6. Apart from the protocol sublayers, the standard specifies management layers and the station management.

7. The **MAC management** supports the association and re-association of a station to an access point and roaming between different access points.

8. 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).

9. The main tasks of the **PHY management** include channel tuning and PHY MIB maintenance.

10. 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).

IEEE 802.11b

IEEE 802.11 b standard only defines a new PHY layer. All the MAC schemes, management procedures etc., explained above are still used.

Depending on the current interference and the distance between sender and receiver 802.11b systems offer 11, 5.5, 2, or 1 Mbit/s.

Maximum user data rate is approx 6 Mbit/s.

The lower data rates 1 and 2 Mbit/s use the 11-chip Barker sequence and DBPSK or DQPSK, respectively.

The new data rates, 5.5 and 11 Mbit/s, use 8-chip complementary code keying (CCK)

The IEEE 802.11 b standard defines several packet formats for the physical layer.

- The below figure shows two packet formats standardized for 802.11b.
  - ■ The mandatory format is called long PLCP PPDU and
  - ■ The optional short PLCP PPDU format

Long PLCP PPDU

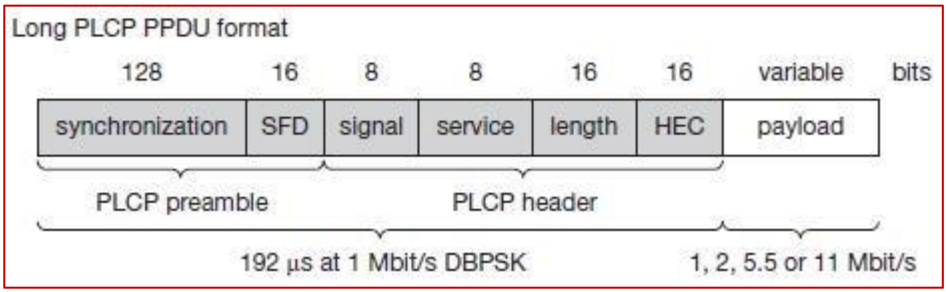


Fig 7: IEEE 802.11b PHY packet format

- In long PLCP PPDU the rate encoded in the signal field, is encoded in multiples of 100 kbit/s.
- Thus, 0x0A represents 1 Mbit/s, 0x14 is used for 2 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.

Short PLCP PPDU format (Optional)

- The optional short PLCP PPDU format differs in several ways.

- 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 SFD of 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 short format 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 transmitted at 2 Mbit/s, DQPSK, which is also the lowest available data rate.

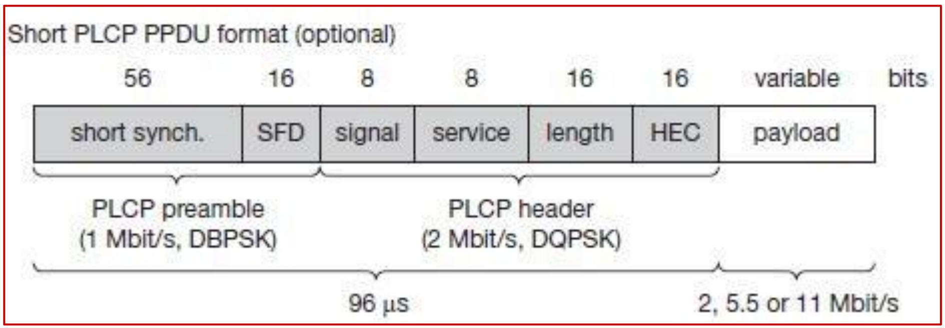


Fig 8: IEEE 802.11b PHY packet format

- The length of the overhead is only half for the short frames (96 μs instead of 192 μs). This is useful for, e.g., short, but time critical, data transmissions.

- ✓ The IEEE 802.11b standards operates (like the DSSS version of 802.11) on certain frequencies in the 2.4 GHz ISM band.

- ✓ These depend on national regulations. Altogether 14 channels have been defined as Table below shows.

- ✓ For each channel the center frequency is given.

- ✓ Depending on national restrictions 11 (US/Canada), 13 (Europe with some exceptions) or 14 channels (Japan) can be used.

Figure below illustrates the non-overlapping usage of channels for an IEEE 802.11b installation with minimal interference in the US/Canada and Europe.

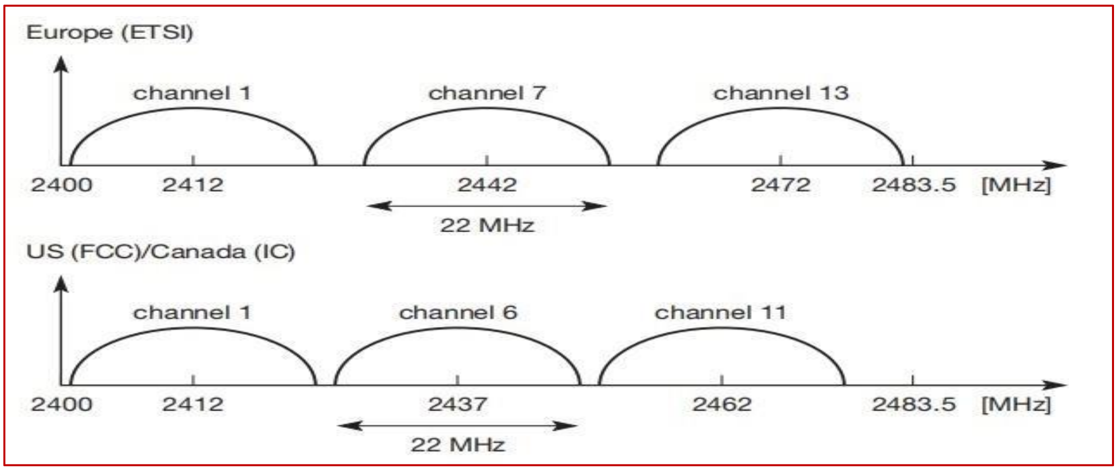
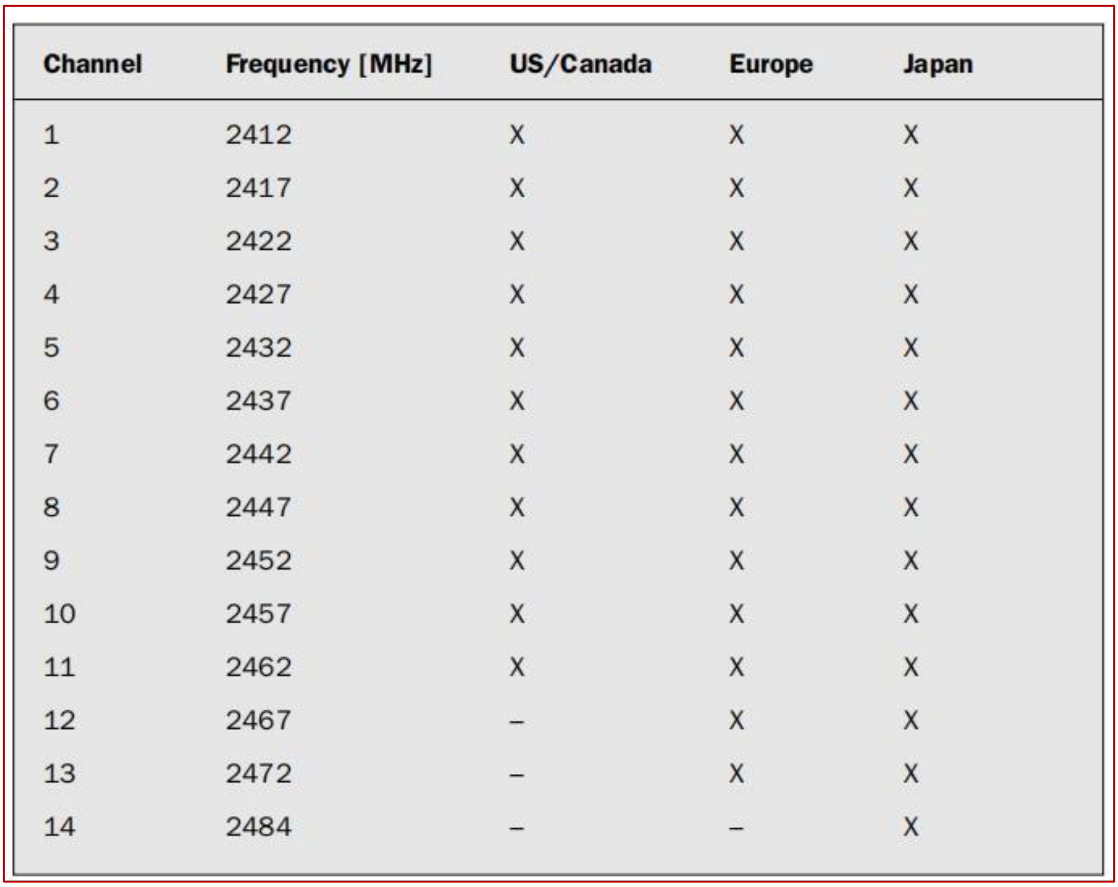


Fig 9: IEEE 802.11b non-overlapping channel selection

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.



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

Table 1: Channel Plan for IEEE 802.11b

IEEE 802.11a

IEEE 802.11a offers up to 54 Mbit/s using OFDM

The FCC (US) regulations offer three different 100 MHz domains for the use of 802.11a, each with a different legal maximum power output:

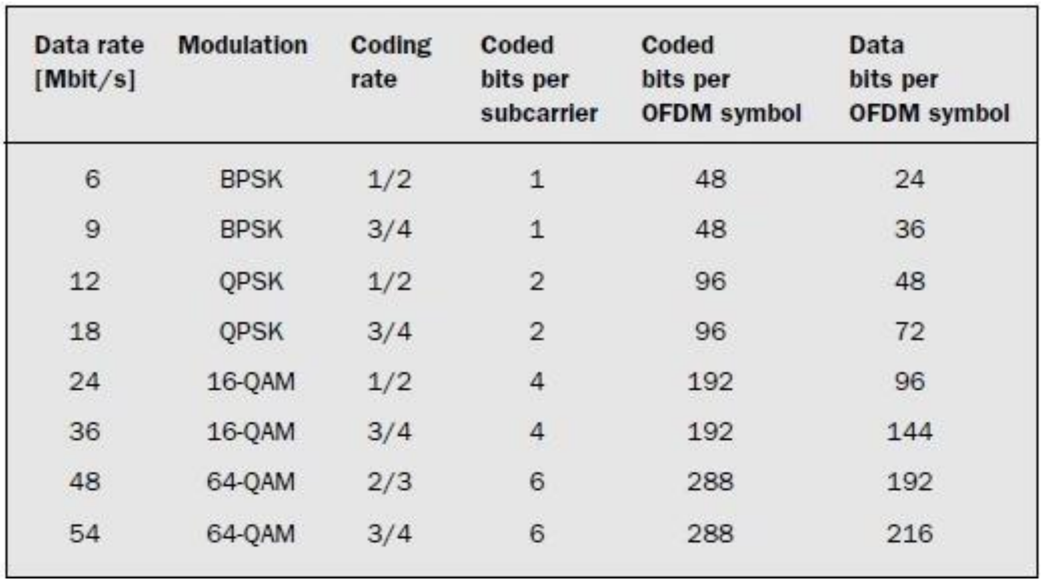
5.15–5.25 GHz/50 mW,
5.25–5.35 GHz/250 mW, and
5.725–5.825 GHz/1 W.

ETSI (Europe) defines different frequency bands for Europe:

5.15–5.35 GHz and
5.47–5.725 GHz

- To be able to offer data rates up to 54 Mbit/s IEEE 802.11a uses many different technologies.
- 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.

Table below gives an overview of the standardized combinations of modulation and coding schemes together with the resulting data rates.



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

Table 2:Rate dependent parameters for IEEE 802.11a

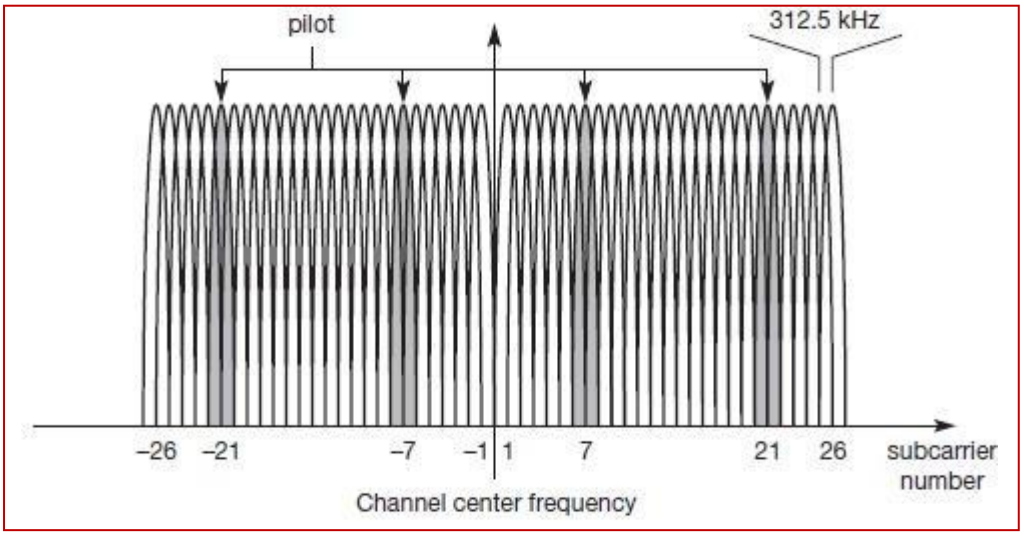


Fig 10: Usage of OFDM in IEEE 802.11a

- IEEE 802.11a uses a fixed symbol rate of 250,000 symbols per second independent of the data rate (0.8 μs guard interval for ISI mitigation plus 3.2 μs used for data results in a symbol duration of 4 μs).

- As Figure above shows, 52 subcarriers are equally spaced around a center frequency.

- The spacing between the subcarriers is 312.5 kHz. 26 subcarriers are to the left of the center frequency and 26 are to the right. The center frequency itself is not used as subcarrier.

- Subcarriers with the numbers –21, –7, 7, and 21 are used for pilot signals to make the signal detection robust against frequency offsets.

Due to the nature of OFDM, the PDU on the physical layer of IEEE 802.11a looks quite different from 802.11b or the original 802.11 physical layers.

Figure below shows the basic structure of an **IEEE 802.11a PPDU**

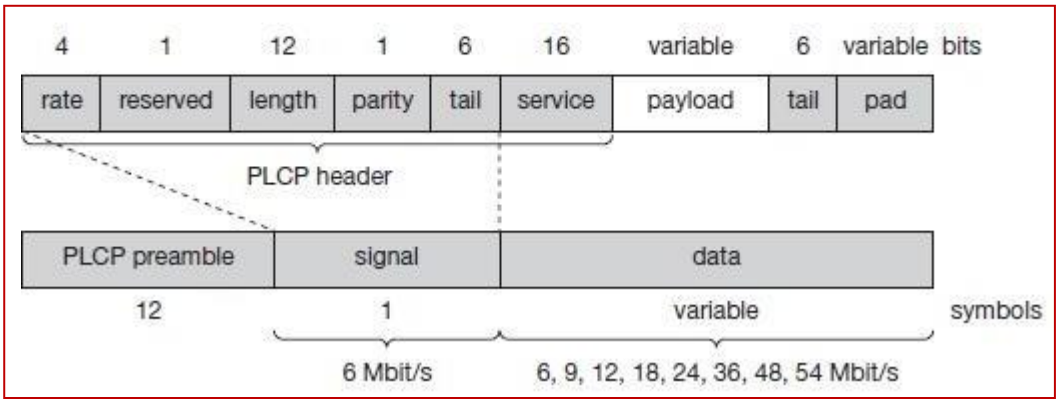


Fig 11: IEEE 802.11a physical layer PDU

1. The **PLCP preamble** consists of 12 symbols and is used for frequency acquisition, channel estimation, and synchronization. The duration of the preamble is 16 μs.

2. The following OFDM symbol, called **signal**, contains the following fields and is BPSK-modulated. The 4 bit **rate** field determines the data rate and the modulation of the rest of the packet (examples are 0x3 for 54 Mbit/s, 0x9 for 24 Mbit/s, or 0xF for 9 Mbit/s).

3. The **length** field indicates the number of bytes in the payload field.

4. The **parity** bit shall be an even parity for the first 16 bits of the signal field (rate, length and the reserved bit). Finally, the six **tail** bits are set to zero.

5. The **data** field is sent with the rate determined in the rate field and contains a **service** field which is used to synchronize the descrambler of the receiver (the data stream is scrambled using the polynomial x7 + x4 + 1) and which contains bits for future use.

6. The **payload** contains the MAC PDU (1-4095 byte). The **tail** bits are used to reset the encoder.

7. Finally, the **pad** field ensures that the number of bits in the PDU maps to an integer number of OFDM symbols.

Compared to IEEE 802.11b working at 2.4 GHz IEEE 802.11a at 5 GHz offers much higher data rates.

HIPERLAN

HIPERLAN stands for high performance local area network

In 1996, the ETSI standardized HIPERLAN 1 as a WLAN allowing for node mobility and supporting ad-hoc and infrastructure-based topologies

Introduction

- HIPERLAN Type 1 (HIPERLAN/1) is a wireless local area network that is ISO/IEC 8802-1 [5] compatible.
- It is intended to allow high performance wireless networks to be created, without existing wired infrastructure.
- HIPERLAN 1 offers functions to forward traffic via several other wireless nodes – a feature which is especially important in wireless ad-hoc networks without an infrastructure. This forwarding mechanism can also be used if a node can only reach an access point via other HIPERLAN 1 nodes.
- HIPERLAN 1 was 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 **1W** transmit power.
- The service offered by a HIPERLAN 1 is compatible with the standard MAC services known from IEEE 802.x LANs. Addressing is based on standard 48 bit MAC addresses.
- 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.

The following describes only the medium access scheme of HIPERLAN 1, a scheme that provides QoS and a powerful prioritization scheme.

Medium Access Scheme of HIPERLAN 1

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:

1. **Prioritization:** Determine the highest priority of a data packet ready to be sent by competing nodes.

2. **Contention:** Eliminate all but one of the contenders, if more than one sender has the highest current priority.

3. **Transmission:** Finally, transmit the packet of the remaining node. In a case where several nodes compete for the medium, all three phases are necessary (called 'channel access in **synchronized channel condition**').

   If the channel is free for at least 2,000 so-called high rate bit-periods plus a dynamic extension, only the third phase, i.e. transmission, is needed (called 'channel access in **channel-free condition**').

HIPERLAN 1 also supports 'channel access in the **hidden elimination condition**'.

The contention phase is further subdivided into an **elimination phase** and a **yield phase**. The purpose of the elimination phase is to eliminate as many contending nodes as possible (but surely not all).

Finally, the yield phase completes the work of the elimination phase with the goal of only one remaining node.

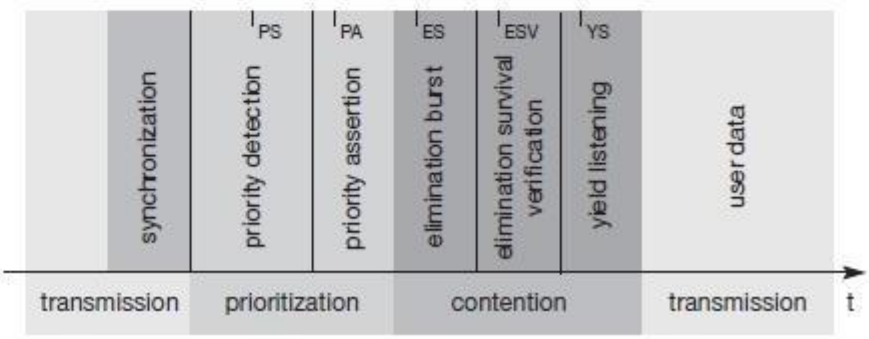


Fig 12: Phases of the HIPERLAN 1 EY-NPMA access scheme

Prioritization phase

1. HIPERLAN 1 offers five different priorities for data packets ready to be sent.

2. After one node has finished sending, many other nodes can compete for the right to send.

3. 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.

4. This mechanism always grants nodes with higher priority access to the medium, no matter how high the load on lower priorities.

Elimination phase

1. The elimination phase now resolves contention by means of elimination bursting and elimination survival verification.

2. 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.

3. The burst sent is the same as for the priority assertion.

4. 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

Yield phase

1. During the yield phase, the remaining nodes only listen into the medium without sending any additional bursts.

2. 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. Otherwise, it withdraws for the rest of the current transmission cycle.

3. 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 can sense.

4. It is important to note that at this point there can still be more than one surviving node so a collision is still possible.

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.

Quality of service support and other specialties.

1. The speciality of HIPERLAN 1 is its QoS support. The quality of service offered by the MAC layer is based on three parameters (HMQoS-parameters). The user can set a priority for data, priority = 0 denotes a high priority, priority = 1, a low priority.

2. The user can determine the lifetime of an MSDU to specify time bounded delivery.

3. Besides data transfer, the MAC layer offers functions for looking up other HIPERLANs within radio range as well as special power conserving functions.

4. Power conservation is achieved by setting up certain recurring patterns when a node can receive data instead of constantly being ready to receive.

HIPERLAN 1 MAC also offers user data **encryption** and **decryption** using a simple XOR-scheme together with random numbers

WATM - Wireless Asynchronous Transfer Mode

ATM (Asynchronous Transfer Mode) combines both the data and multimedia information into the wired networks while scales well from backbones to the customer premises networks.

Due to the success of ATM on wired networks,
Wireless ATM (WATM) is a direct result of the ATM "everywhere" movement.

Motivation for WATM

Several reasons led to the development of WATM:

1. The need for seamless integration of wireless terminals into an ATM network.
2. ATM networks scale well from LANs to WANs – and mobility is needed in local and wide area applications.
3. For ATM to be successful, it must offer a wireless extension.
4. WATM could offer QoS for adequate support of multi-media data streams.
5. For telecommunication service providers, it appears natural that merging of mobile wireless communication and ATM technology leads to wireless ATM.

Wireless ATM working group

- The main goal of this working group involved ensuring the compatibility of all new proposals with existing ATM Forum standards.
- It should be possible to upgrade existing ATM networks, i.e., ATM switches and ATM end-systems, with certain functions to support mobility and radio access if required.

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

1. **Location management:** 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.
2. **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 a new access point, the system must reroute traffic.
3. **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.

4. **QoS and traffic control:** WATM should be able to offer many QoS parameters. To maintain these parameters, all actions such as rerouting, handover etc. have to be controlled.

5. **Network management:** All extensions of protocols or other mechanisms also require an extension of the management functions to control the network

To ensure wireless access, the working group discussed the following topics belonging to a radio access layer (RAL):

- ✓ **Radio resource control:** As for any wireless network, radio frequencies, modulation schemes, antennas, channel coding etc. have to be determined.

- ✓ **Wireless media access:** Different media access schemes are possible, each with specific strengths and weaknesses for, e.g., multi-media or voice applications.

- ✓ **Wireless data link control:** The data link control layer might offer header compression for an ATM cell that carries almost 10 per cent overhead using a 5 byte header in a 53 byte cell. This layer can apply ARQ or FEC schemes to improve reliability.

- ✓ **Handover issues:** During handover, cells cannot only be lost but can also be out of sequence (depending on the handover mechanisms). Cells must be re-sequenced and lost cells must be re transmitted if required.

WATM services

WATM systems had to be designed for transferring voice, classical data, video (from low quality to professional quality), multimedia data, short messages etc.

1. **Office environments:** This includes all kinds of extensions for existing fixed networks offering a broad range of Internet/Intranet access, multi-media conferencing, online multi-media database access, and telecommuting.

2. **Universities, schools, training centres:** The main focus in this scenario are distance learning, wireless and mobile access to databases, internet access, or teaching in the area of mobile multi-media computing.

3. **Industry:** WATM may offer an extension of the Intranet supporting database connection, information retrieval, surveillance, but also real-time data transmission and factory management.

4. **Hospitals:** Applications could include the transfer of medical images, remote access to patient records, remote monitoring of patients, remote diagnosis of patients at home or in an ambulance, as well as tele-medicine. The latter needs highly reliable networks with guaranteed quality of service to enable, e.g., remote surgery.

5. **Home:** Many electronic devices at home (e.g., TV, radio equipment, CD-player, PC with internet access) could be connected using WATM technology.

6. **Networked vehicles:** All vehicles used for the transportation of people or goods will have a local network and network access in the future.

WATM system

The figure below shows a generic reference model for wireless mobile access to an ATM network.

1. A mobile ATM (MATM) terminal uses a WATM terminal adapter to gain wireless access to a WATM RAS (Radio Access System).

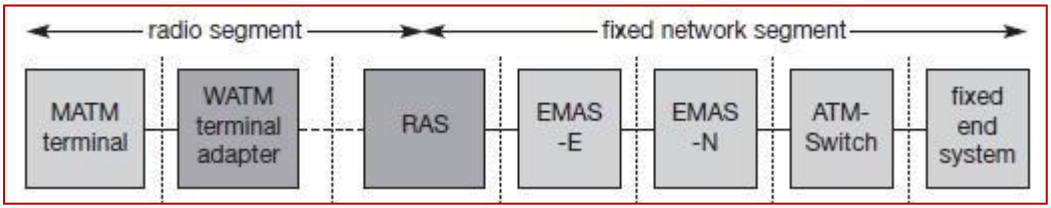


Fig 13: WATM system model

2. MATM terminals could be represented by, e.g., laptops using an ATM adapter for wired access plus software for mobility.

3. The WATM terminal adapter enables wireless access, i.e., it includes the transceiver etc., but it does not support mobility.

4. The RAS with the radio transceivers is connected to a mobility enhanced ATM switch (EMAS-E), which in turn connects to the ATM network with mobility aware switches (EMAS-N) and other standard ATM switches.

5. Finally, a wired, non-mobility aware ATM end system may be the communication partner in this example

Handover in WATM

One of the most important topics in a WATM environment is handover.

- The main problem for WATM during the handover is rerouting all connections and maintaining connection quality.

- While in connectionless, best-effort environments, handover mainly involves rerouting of a packet stream without reliable transport, an end-system in WATM networks could maintain many connections, each with a different quality of service requirements (e.g., limited delay, bounded jitter, minimum bandwidth etc.).

- Handover not only involves rerouting of connections, it also involves reserving resources in switches, testing of availability of radio bandwidth, tracking of terminals to perform look-ahead reservations etc

Many different requirements have been set up for handover such as

1. Handover of multiple connections
2. Handover of point-to-multi-point connections
3. QoS support
4. Data integrity and security
5. Signaling and routing support
6. Performance and complexity

Location management in WATM

As for all networks supporting mobility, special functions are required for looking up the current position of a mobile terminal, for providing the moving terminal with a permanent address, and for ensuring security features such as privacy, authentication, or authorization.

These and more functions are grouped under the term **location management**.

Several requirements for location management such as

1. **Transparency of mobility** - A user should not notice the location management function under normal operation. Any change of location should be performed without user activity.

2. **Security -** All location and user information collected for location management and accounting should be protected against unauthorized disclosure. Encryption is also necessary, at least between terminal and access point, but preferably end-to-end.

3. **Efficiency and scalability** - Every function and system involved in location management must be scalable and effificient. This includes distributed servers for location storage, accounting and authentication.

4. **Identification -** Location management must provide the means to identify all entities of the network. Radio cells, WATM networks, terminals, and switches need unique identifiers and mechanisms to exchange identity information.

5. **Inter-working and standards -** All location management functions must cooperate with existing ATM functions from the fixed network, especially routing.

Mobile quality of service

Qualities of service (QoS) guarantees are one of the main advantages described for WATM networks

WATM networks should provide mobile QoS (M-QoS). M-QoS is composed of three different parts:

1. **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.

2. **Wireless QoS:** 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.

3. **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 represent critical factors for QoS.

Two different types of QoS during handover:

Hard handover QoS: While the QoS with the current RAS may be guaranteed due to the current availability of resources, no QoS guarantees are given after the handover.

Soft handover QoS: Even for the current wireless segment, only statistical QoS guarantees can be given, and the applications also have to adapt after the handover.

Access scenarios

- **T (terminal):** A standard ATM terminal offering ATM services defined for fixed ATM networks.

- **MT (mobile terminal):** A standard ATM terminal with the additional capability of reconnecting after access point change. The terminal can be moved between different access points within a certain domain.

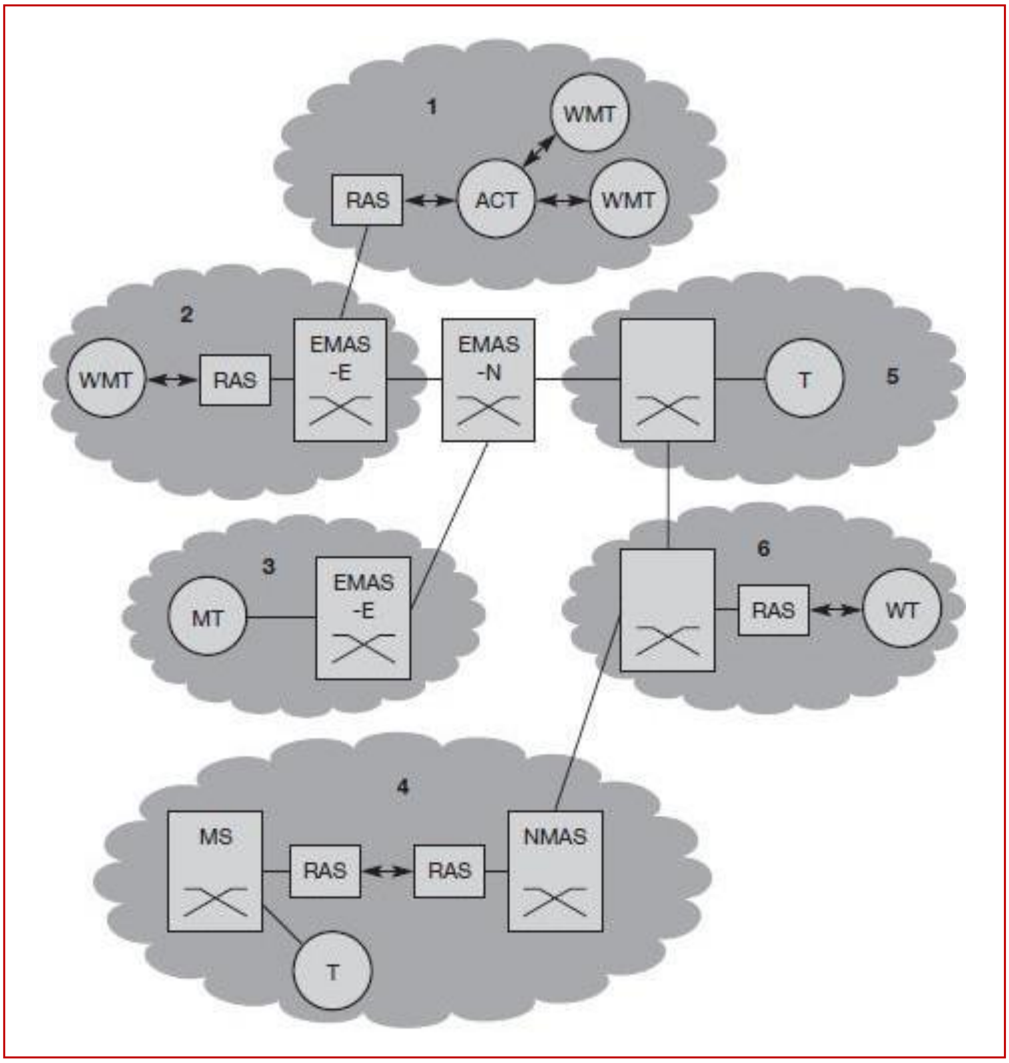


Fig 14: WATM reference model with several access scenarios

- **WT (wireless terminal):** This terminal is accessed via a wireless link, but the terminal itself is fixed, i.e., the terminal keeps its access point to the network.

- **WMT (wireless mobile terminal):** The combination of a wireless and a mobile terminal results in the WMT. This is exactly the type of terminal presented throughout this WATM section, as it has the ability to change its access point and uses radio access.

- **RAS (radio access system):** Point of access to a network via a radio link as explained in this chapter.

- **EMAS (end-user mobility supporting ATM switch, -E: edge, -N: network):** Switches with the support of end-user mobility.

- **NMAS (network mobility-supporting ATM switch):** A whole network can be mobile not just terminals. Certain additional functions are needed to support this mobility from the fixed network.

- **MS (mobile ATM switch):** ATM switches can also be mobile and can use wireless access to another part of the ATM network.

- **ACT (ad-hoc controller terminal):** For the configuration of ad-hoc networks, special terminal types might be required within the wireless network.

WATM specifies radio access, mobility management, handover schemes, mobile QoS, security etc.

BRAN – Broadband Radio Access Networks

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

□ The main motivation behind BRAN is the deregulation and privatization of the telecommunication sector in Europe.

□ Many new providers experience problems getting access to customers 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 traffific are supported, one can multiplex traffic for higher effificiency, and the connection can be asymmetrical

□ Radio access allows for economical 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.

BRAN standardization has a rather large scope including indoor and campus mobility, transfer rates of **25–155 Mbit/**s, and a transmission range of **50 m–5 km**.

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 fifixed 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 HIPERACCESS 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. Currently, there are no plans regarding this standard.

- As an access network, BRAN technology is independent from the protocols of the fixed network. BRAN can be used for ATM and TCP/IP networks.

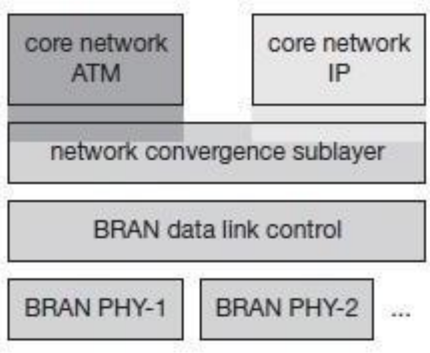


Fig 15: Layered model of BRAN wireless access networks

- 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 can be used by a wireless ATM network, Ethernet, Firewire, or an IP network.

HiperLAN2

HIPERLAN2 (High Performance Local Area Network Type 2) Standardized by ETSI (2000a), this wireless network works at **5 GHz** and offers data rates of up to **54 Mbit/s** including QoS support and enhanced security features.

HiperLAN2 reference model:

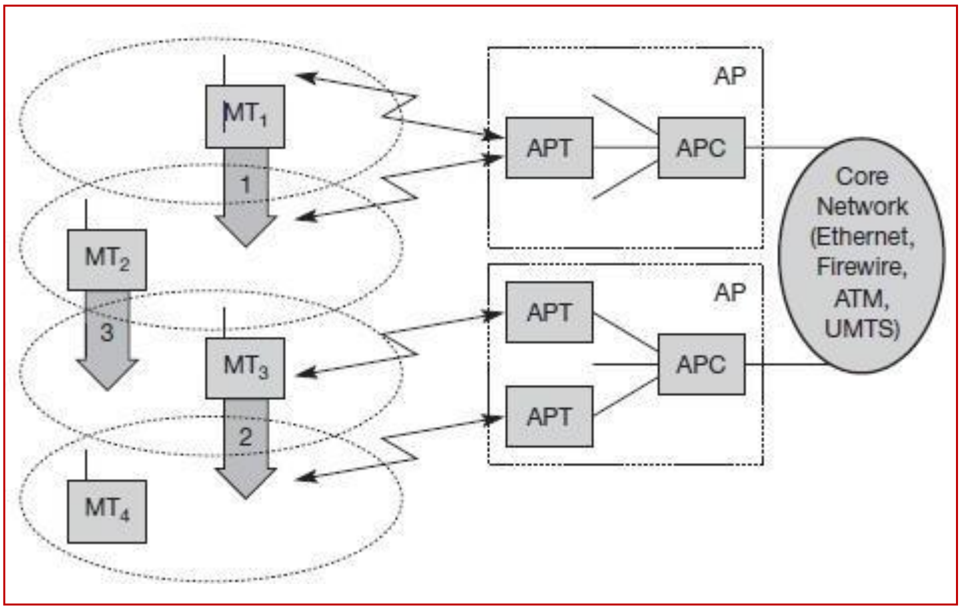


Fig 16: HiperLAN2 basic structure and handover scenarios

1. In the example, two **access points** (AP) are attached to a core network.

2. Each AP consists of an **access point controller** (APC) and one or more **access point transceivers** (APT).

3. An APT can comprise one or more sectors (shown as cell here).

4. Finally, four **mobile terminals** (MT) are also shown. MTs can move around in the cell area as shown. The system automatically assigns the APT/AP with the best transmission quality.

5. No frequency planning is necessary as the APs automatically select the appropriate frequency via **dynamic frequency selection**

HiperLAN2 networks can operate in two different modes

Centralized mode (CM):
This infrastructure-based mode is shown again in a more abstract way in Figure below (left side).

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 mandatory mode the AP takes complete control of everything.

Direct mode (DM):

The optional ad-hoc mode of HiperLAN2 is illustrated on the right side of Figure below. 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.

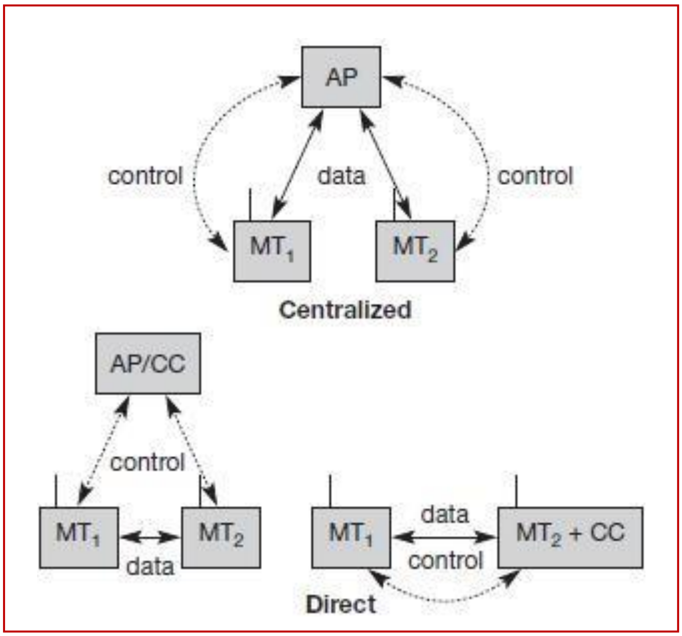
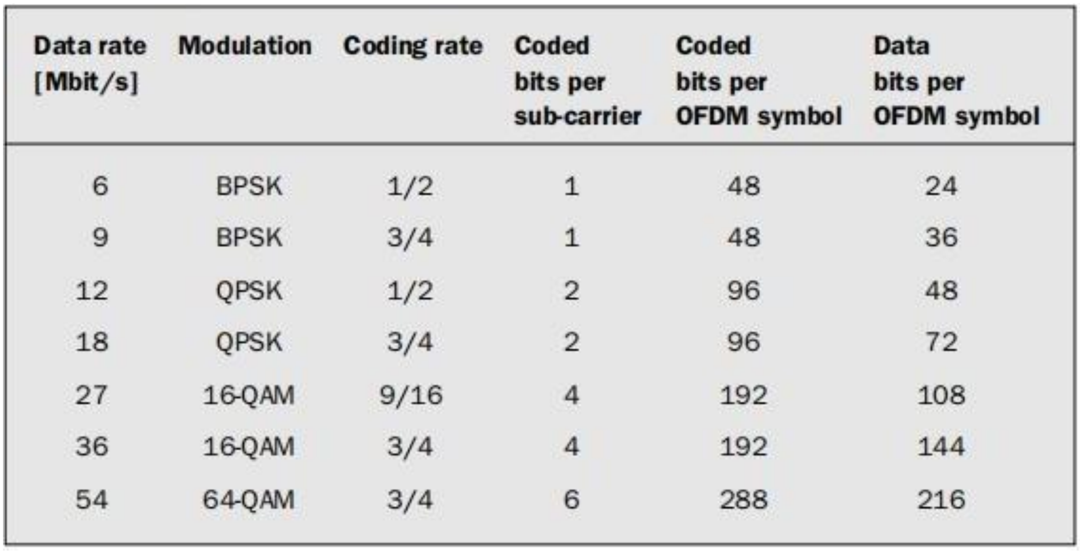


Fig 17: HiperLAN2 centralized vs direct mode

Physical layer

Table below gives an overview of the data rates offered by HiperLAN2 together with other parameters such as coding,



Data rate [Mbit/s]	Modulation	Coding rate	Coded bits per sub-carrier	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
27	16-QAM	9/16	4	192	108
36	16-QAM	3/4	4	192	144
54	64-QAM	3/4	6	288	216

Table 3: Rate dependent parameters for HiperLan2

Figure below illustrates the reference configuration of the transmission chain of a HiperLAN2 device.

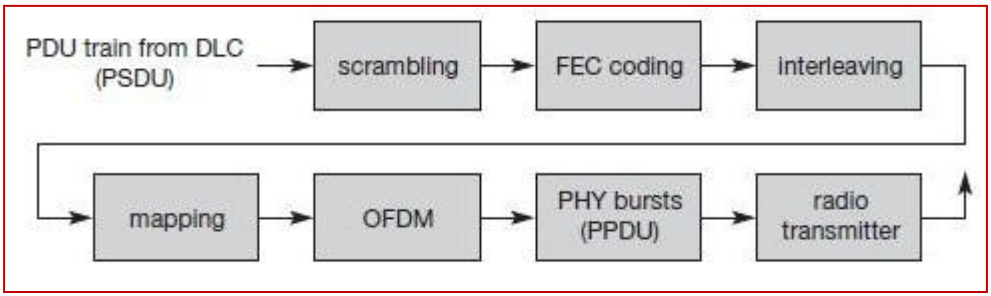


Fig 18: HiperLAN2 physical layer reference configuration

1. After selecting one of the above transmission modes, the DLC layer passes a PSDU to the physical layer (PSDUs are called DLC PDU trains in the HiperLAN2 context).

2. The first step is **scrambling** of all data bits with the generator polynomial x7 + x4 + 1 for DC blocking and whitening of the spectrum. The results of this first step are **scrambled bits**.

3. The next step applies **FEC coding** for error protection. Coding depends on the type of data (broadcast, uplink, downlink etc.) and the usage of sector or omni-directional antennas.

4. The result of this step is an **encoded bit**.

5. For mitigation of frequency selective fading **interleaving** is applied in the third step.

6. Interleaving ensures that adjacent encoded bits are mapped onto non-adjacent subcarriers (48 subcarriers are used for data transmission). Adjacent bits are mapped alternately onto less and more significant bits of the constellation. The result is an **interleaved bit**.

7. The following **mapping** process first divides the bit sequence in groups of 1, 2, 4, or 6 bits depending on the modulation scheme (BPSK, QPSK, 16-QAM, or 64-QAM).

8. The results of this mapping are **subcarrier modulation symbols**. The **OFDM** modulation step converts these symbols into a baseband signal with the help of the inverse FFT.

9. The symbol interval is 4 μs with 3.2 μs useful part and 0.8 μs guard time. Pilot sub-carriers (sub-carriers –21, –7, 7, 21) are added. The last step before radio transmission is the creation of **PHY bursts** (PPDUs in ISO/OSI terminology).

10. Each burst consists of a preamble and a payload. Five different PHY bursts have been defined: broadcast, downlink, uplink with short preamble, uplink with long preamble, and direct link (optional). The bursts differ in their preambles.

11. The final **radio transmission** shifts the baseband signal to a carrier frequency depending on the channel number and the formula already used for 802.11a: carrier_number = (carrier_frequency – 5000 MHz)/5 MHz.

Data link control layer in HiperLAN2

The DLC layer is divided into MAC, control and data part.

The medium access control creates frames of 2 ms duration as shown in Figure below. With a constant symbol length of four μs this results in 500 OFDM symbols. 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).

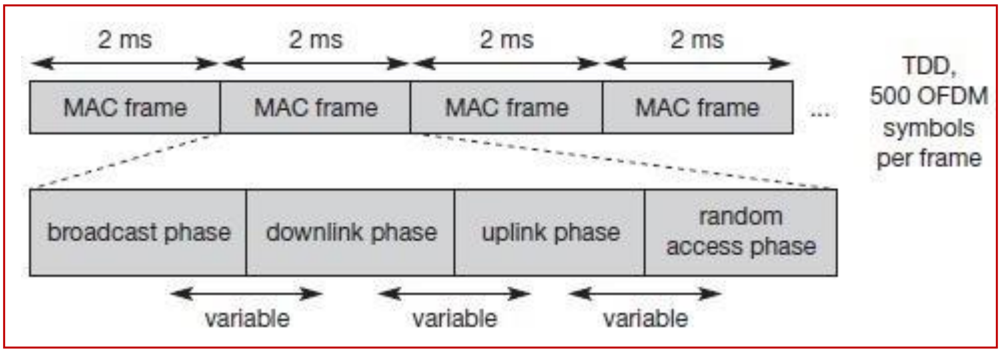


Fig 19 : Basic structure of HiperLAN2 MAC frames

HiperLAN2 defines six different so-called transport channels for data transfer in the above listed phases. These transport channels describe the basic message format within a MAC frame.

1. **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. The length is 15 bytes.

2. **Frame channel (FCH):** This channel contains a directory of the downlink and uplink phases (LCHs, SCHs, and empty parts). This also comprises the PHY mode used. The length is a multiple of 27 bytes.

3. **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.

4. **Long transport channel (LCH):** This channel transports user and control data for downlinks and uplinks. The length is 54 bytes.

5. **Short transport channel (SCH):** This channel transports control data for downlinks and uplinks. The length is 9 bytes.

6. **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. Access is via slotted Aloha so, collisions may occur. Collision resolution is performed with the help of an exponential back-off scheme. The length is 9 bytes.

Convergence layer

As the physical layer and the data link layer are independent of specific core network protocols, a special **convergence layer (CL)** is needed to adapt to the specific features of these network protocols.

HiperLAN2 supports two different types of CLs:

cell-based and
packet-based.

The **cell-based** CL expects data packets of fixed size (cells, e.g., ATM cells), while the **packet-based** CL handles packets that are variable in size.

Three examples of convergence layers follow:

- Ethernet
- IEEE 1394 (Firewire)
- ATM

Features of HiperLAN2:

□ High-throughput transmission
□ Connection-oriented
□ Quality of service support
□ Dynamic frequency selection
□ Security support
□ Mobility support
□ Application and network independence
□ Low power consumption

Bluetooth (IEEE 802.15.1)

The Bluetooth transceivers operate in the globally available unlicensed ISM (Industrial, Scientific and Medical) radio frequency band of 2.4GHz.

Bluetooth is a specification of Wireless Personal Area Networks (WPANs).

The Bluetooth technology uses a short-range radio link that has been optimized for small-size personal devices.

Bluetooth connections are created in ad-hoc manner to exchange information between devices such as mobile phones, laptops, printers, digital cameras etc.

Architecture

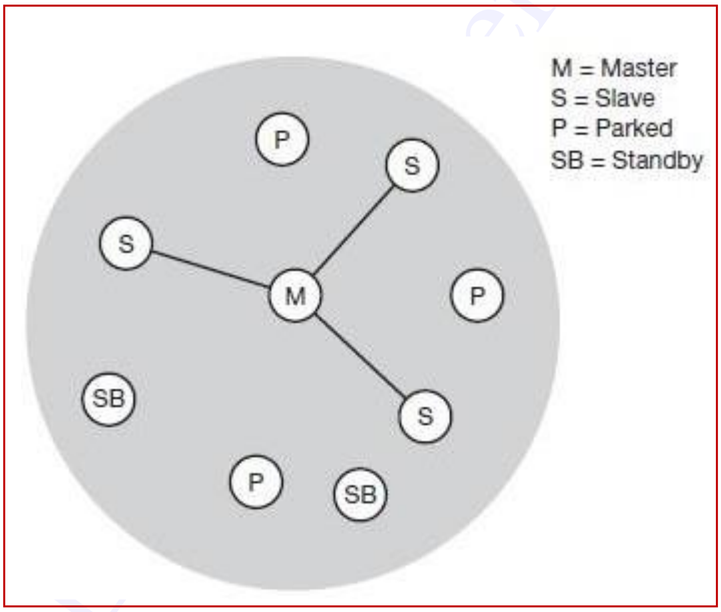


Fig 20: Simple Bluetooth Piconet

- Bluetooth is a **piconet**.

- A piconet is a collection of Bluetooth devices which are synchronized to the same hopping sequence.

- 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 to participate 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-bit address 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.

Protocol stack

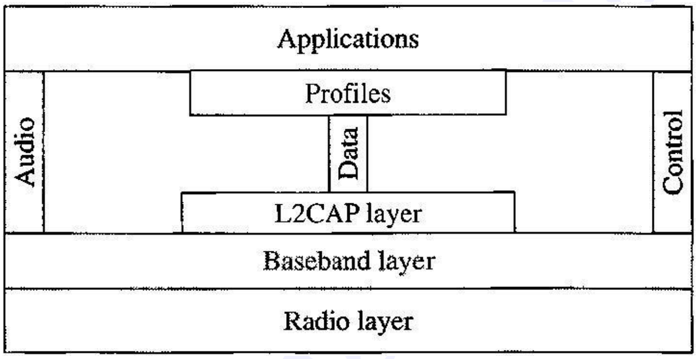


Fig 21: Bluetooth Protocol Stack

1. **Radio:** Specification of the air interface, i.e., frequencies, modulation, and transmit.

2. **Baseband:** Description of basic connection establishment, packet formats, timing, and basic QoS parameters.

3. **Link manager protocol:** Link set-up and management between devices including security functions and parameter negotiation.

4. **Logical link control and adaptation protocol (L2CAP):** Adaptation of higher layers to the baseband (connectionless and connection-oriented services).

5. **Service discovery protocol:** Device discovery in close proximity plus querying of service characteristics.

Radio layer

1. 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.

2. The combined use for data and voice transmission has to be reflected in the design, i.e., Bluetooth has to support multi-media data.

3. 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.

4. Bluetooth uses 79 hop carriers equally spaced with 1 MHz.

5. Bluetooth transceivers use Gaussian FSK for modulation.

Baseband layer

The functions of the baseband layer are quite complex as it not only performs frequency hopping for interference mitigation and medium access, but also defines physical links and many packet formats.

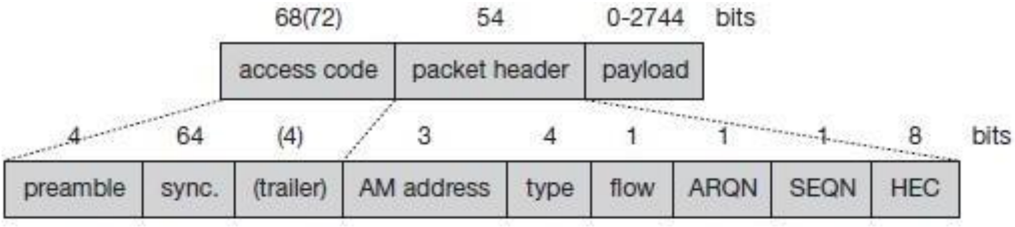


Fig 22: Baseband Packet Format

The packet typically consists of the following three fields:

Access code:

1. This first field of a packet is needed for timing synchronization and piconet identification.

2. It may represent special codes during paging and inquiry.

3. The access code consists of a 4 bit **preamble**, a **synchronization** field, and a **trailer** (if a packet header follows).

4. The 64-bit synchronization field is derived from the lower 24 bit of an address.

Packet header:

1. This field contains typical layer 2 features: address, packet type, flow and error control, and checksum.

2. The 3-bit **active member address** represents the active address of a slave. Active addresses are temporarily assigned to a slave in a piconet.

3. If a master sends data to a slave the address is interpreted as receiver address. If a slave sends data to the master the address represents the sender address. As only a master may communicate with a slave this scheme works well.

4. Seven addresses may be used this way. The zero value is reserved for a broadcast from the master to all slaves.

5. The 4-bit **type** field determines the type of the packet. Packets may carry control, synchronous, or asynchronous data.

6. A simple flow control mechanism for asynchronous traffic uses the 1-bit **flow** field.

7. If a packet is received with flow=0 asynchronous data, transmission must stop.

8. As soon as a packet with flow=1 is received, transmission may resume.

9. An 8-bit **header error check** (HEC) is used to protect the packet header.

10. The packet header is also protected by a one-third rate forward error correction (FEC) code because it contains valuable link information and should survive bit errors. Therefore, the 18-bit header requires 54 bits in the packet.

Payload: Up to 343 bytes payload can be transferred. The structure of the payload field depends on the type of link and is explained in the following sections.

Link manager protocol

The link manager protocol (LMP) manages various aspects of the radio link between a master and a slave.

LMP enhances baseband functionality, but higher layers can still directly access the baseband. The following groups of functions are covered by the LMP:

1. **Authentication, pairing, and encryption:** Although basic authentication is handled in the baseband, LMP has to control the exchange of random numbers and signed responses.

2. **Synchronization:** Precise synchronization is of major importance within a Bluetooth network.

3. **Capability negotiation:** Not only the version of the LMP can be exchanged but also information about the supported features.

4. **Quality of service negotiation:** Different parameters control the QoS of a Bluetooth device at these lower layers.

5. **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 transmit power.

6. **Link supervision:** LMP has to control the activity of a link, it may set up new SCO links, or it may declare the failure of a link.

7. **State and transmission mode change:** Devices might switch the master/slave role, detach themselves from a connection, or change the operating mode.

To save battery power, a Bluetooth device can go into one of three low power states:

Sniff state: The sniff state has the highest power consumption of the low power states. Here, the device listens to the piconet at a reduced rate

Hold state: The device does not release its AMA but stops ACL (Asynchronous connection less Link) transmission. A slave may still exchange SCO (Synchronous Connection Oriented Link) packets. If there is no activity in the piconet, the slave may either reduce power consumption or participate in another piconet.

Park state: In this state the device has the lowest duty cycle and the lowest power consumption. The device is still a member of the piconet, but gives room for another device to become active.

L2CAP

The **logical link control and adaptation protocol (L2CAP)** is a data link control protocol on top of the baseband layer offering logical channels between Bluetooth devices with QoS properties.

L2CAP provides three different types of logical channels that are transported via the ACL between master and slave:

- **Connectionless:** These unidirectional channels are typically used for broadcasts from a master to its slave(s).

- **Connection-oriented:** Each channel of this type is bi-directional and supports QoS flow specifications for each direction. These flow specs follow RFC 1363 (Partridge, 1992) and define average/peak data rate, maximum burst size, latency, and jitter.

- **Signaling:** This third type of logical channel is used to exchanging signaling messages between L2CAP entities.

Security

1. Bluetooth devices can transmit private data, e.g., schedules between a PDA and a mobile phone.

2. Bluetooth offers mechanisms for authentication and encryption on the MAC layer, which must be implemented in the same way within each device.

3. For each transaction, a new random number is generated on the Bluetooth chip. Key management is left to higher layer software.

Figure below shows several steps in the security architecture of Bluetooth.

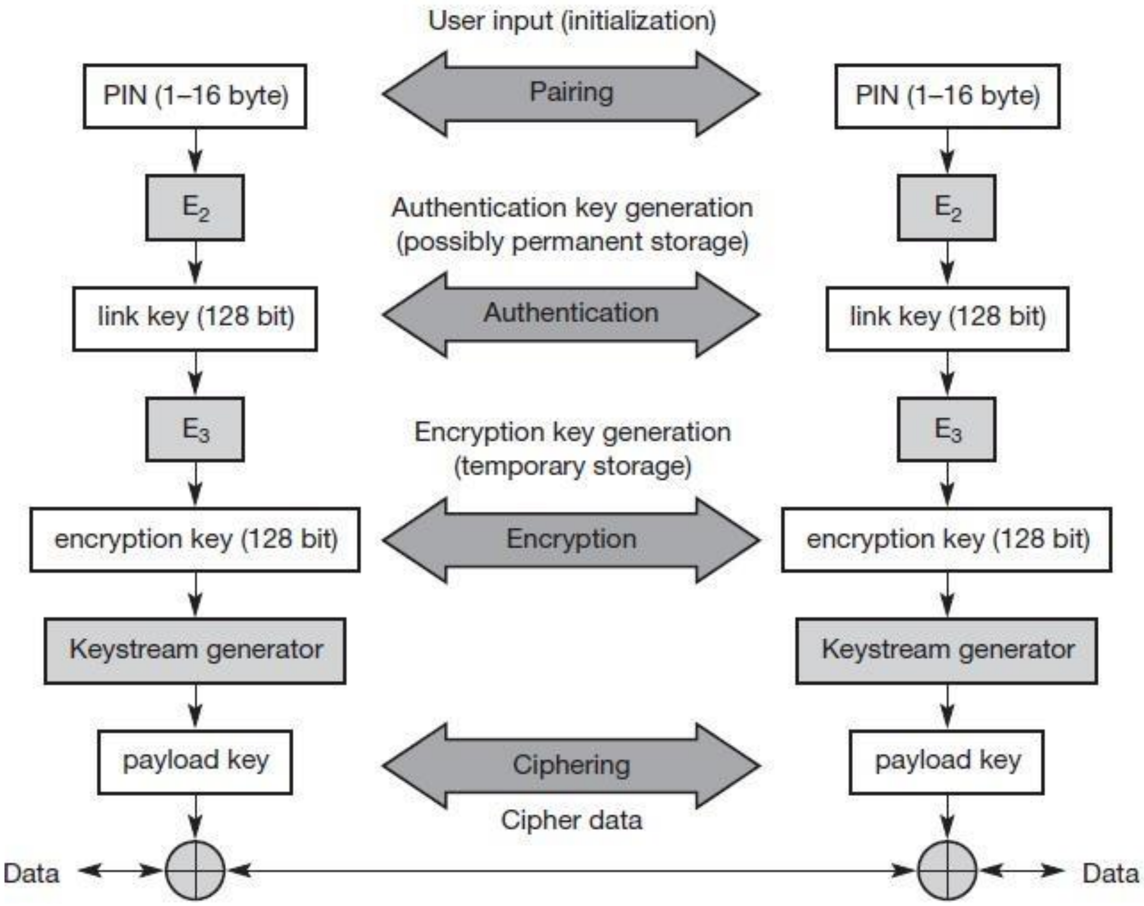


Fig 23: Bluetooth security components and protocols

4. The first step, called **pairing**, is necessary if two Bluetooth devices have never met before. To set up trust between the two devices a user can enter a secret PIN into both devices. This PIN can have a length of up to 16 byte.

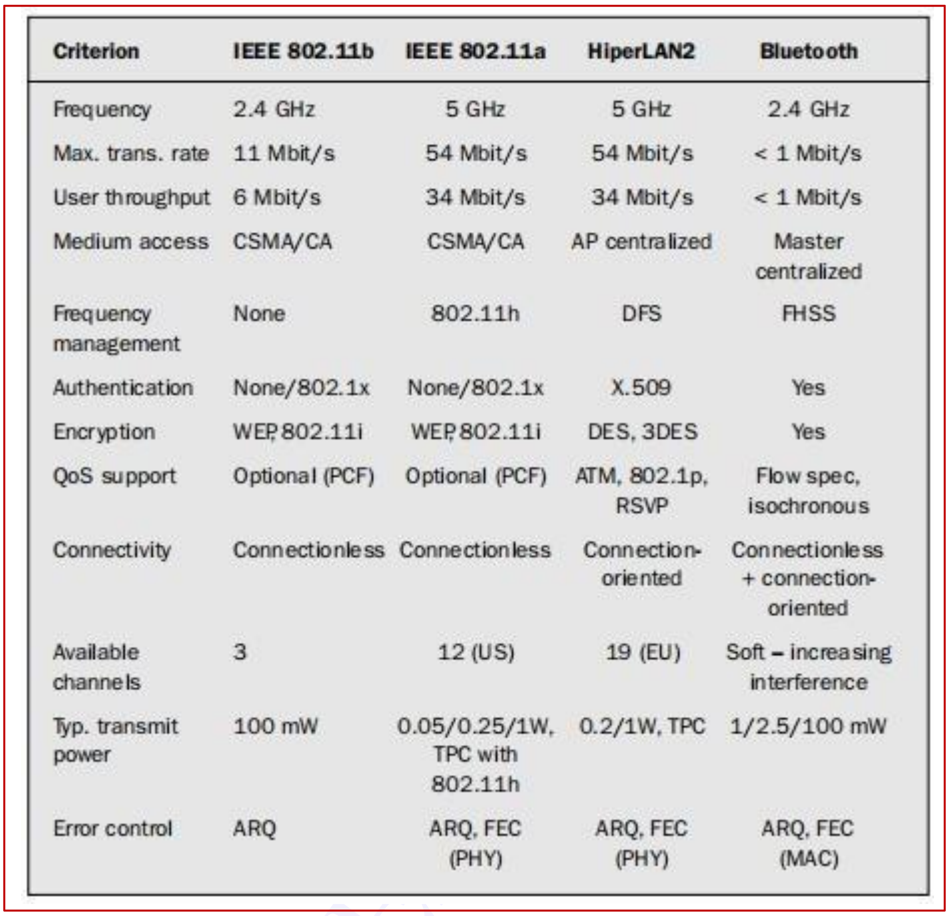
5. Based on the PIN, the device address, and random numbers, several keys can be computed which can be used as link key for **authentication**.

6.

APPLICATIONS OF BLUETOOTH

1. ReplAcing seriAl cAbles with rAdio links
2. WeArAble networks/WPANs
3. Desktop/room wireless networking
4. tfot-spot wireless networking
5. MedicAl: TrAnsfer of meAsured vAlues from trAining units to AnAlyticAl
6. systems, pAtient monitoring
7. Automotive: Remote control of Audio/video equipment, hAnds-free telephony

Comparison of wireless networks



Criterion	IEEE 802.11b	IEEE 802.11a	HiperLAN2	Bluetooth
Frequency	2.4 GHz	5 GHz	5 GHz	2.4 GHz
Max. trans. rate	11 Mbit/s	54 Mbit/s	54 Mbit/s	< 1 Mbit/s
User throughput	6 Mbit/s	34 Mbit/s	34 Mbit/s	< 1 Mbit/s
Medium access	CSMA/CA	CSMA/CA	AP centralized	Master centralized
Frequency management	None	802.11h	DFS	FHSS
Authentication	None/802.1x	None/802.1x	X.509	Yes
Encryption	WEP, 802.11i	WEP, 802.11i	DES, 3DES	Yes
QoS support	Optional (PCF)	Optional (PCF)	ATM, 802.1p, RSVP	Flow spec, isochronous
Connectivity	Connectionless	Connectionless	Connection-oriented	Connectionless + connection-oriented
Available channels	3	12 (US)	19 (EU)	Soft – increasing interference
Typ. transmit power	100 mW	0.05/0.25/1W, TPC with 802.11h	0.2/1W, TPC	1/2.5/100 mW
Error control	ARQ	ARQ, FEC (PHY)	ARQ, FEC (PHY)	ARQ, FEC (MAC)

WPAN – IEEE 802.15.4

The fourth working group goes in the opposite direction for data rates. This group standardizes low–rate wireless personal area networks (LR–WPAN)

IEEE 802.15.4 – Low-rate WPANs

- The reason for having low data rates is the focus of the working group on extremely low power consumption enabling multi-year battery life.
- Example, applications include industrial control and monitoring, smart badges, interconnection of environmental sensors, interconnection of peripherals (also an envisaged application area for Bluetooth!), remote controls etc.
- The new standard should offer data rates between **20 and 250 Kbit/s** as maximum and latencies down to **15 ms.**
- This is enough for many home automation and consumer electronics applications.

IEEE 802.15.4 LR-WPAN Device Architecture

Figure below shows an LR-WPAN device.

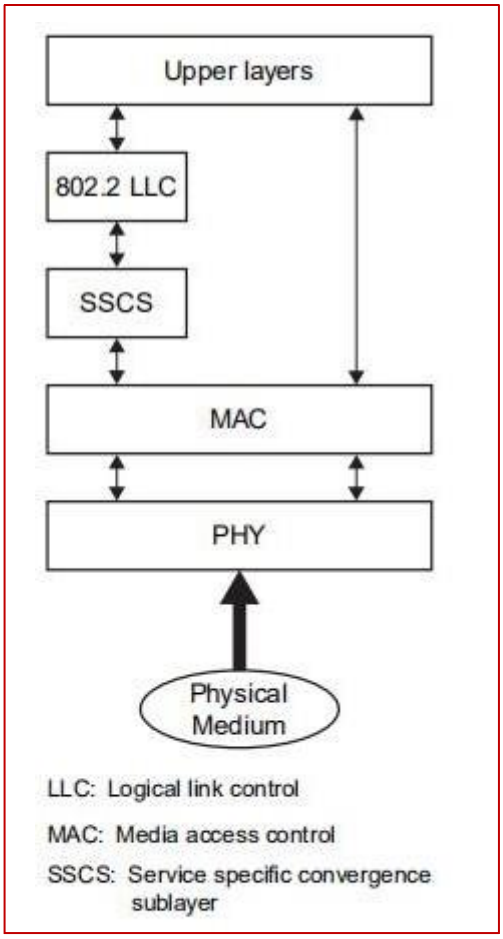

Upper layers
802.2 LLC
SSCS
MAC
PHY
Physical Medium
LLC: Logical link control
MAC: Media access control
SSCS: Service specific convergence sublayer

Fig 24:LR-WPAN device architecture.

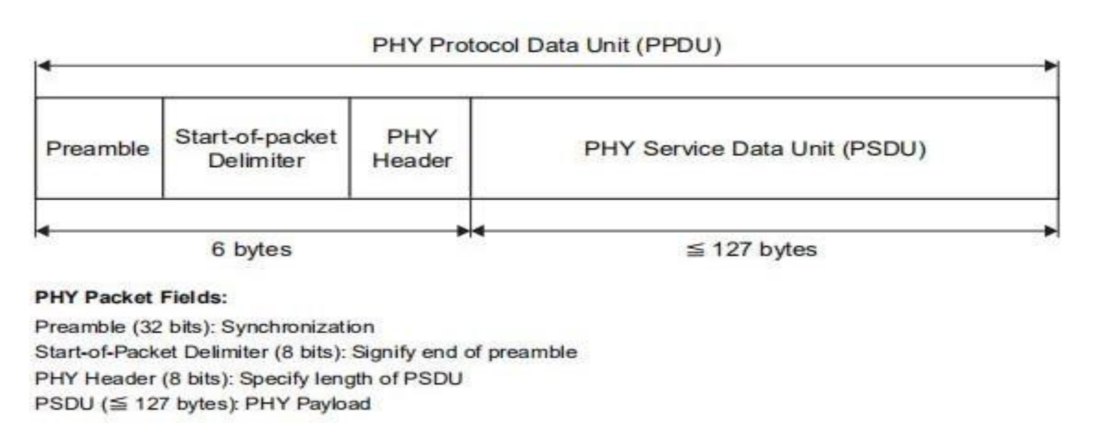
- The device comprises a physical layer (PHY), which contains the RF transceiver along with its low-level control mechanism.
- A MAC sublayer provides access to the physical channel for all types of transfer.
- The upper layers consist of a network layer, which provides network configuration, manipulation, and message routing, and an application layer, which provides the intended function of a device.
- An IEEE 802.2 logical link control (LLC) can access the MAC through the service specific convergence sublayer (SSCS).

Technical Specifications

1. IEEE 802.15.4 offers two different PHY options using DSSS.
2. The 868/915MHz PHY operates in Europe at 868.0–868.6 MHz and in the US at 902–928 MHz.
3. At 868 MHz one channel is available offering a data rate of 20 kbit/s.
4. At 915 MHz 10 channels with 40 kbit/s per channel are available (in Europe GSM uses these frequencies).
5. The advantages of the lower frequencies are better propagation conditions.
6. The 2.4 GHz PHY operates at 2.4–2.4835 GHz and offers 16 channels with 250 kbit/s per channel.
7. This PHY offers worldwide operation but suffers from interference in the 2.4 GHz ISM band and higher propagation loss.
8. Typical devices with 1 mW output power are expected to cover a 10–20 m range.
9. All PHY PDUs start with a 32 bit preamble for synchronization.
10. After a start-of-packet delimiter, the PHY header indicates the length of the payload (maximum 127 bytes).

The **MAC layer** of 802.15.4 is much simpler.

1. MAC frames start with a 2-byte frame control field, which specifies how the rest of the frame looks and what it contains.
2. The following 1-byte sequence number is needed to match acknowledgements with a previous data transmission.
3. The variable address field (0–20 bytes) may contain source and/or destination addresses in various formats.


PHY Protocol Data Unit (PPDU)
Preamble
Start-of-packet Delimiter
PHY Header
PHY Service Data Unit (PSDU)
6 bytes
≦ 127 bytes

PHY Packet Fields:

Preamble (32 bits): Synchronization
Start-of-Packet Delimiter (8 bits): Signify end of preamble
PHY Header (8 bits): Specify length of PSDU
PSDU (≦ 127 bytes): PHY Payload

Fig 25: IEEE 802.15.4 PHY packet structure.

4. The payload is variable in length; however, the whole MAC frame may not exceed 127 bytes in length.

5. A 16-bit FCS protects the frame.

Four different MAC frames have been defined:

1. beacon,
2. data,
3. acknowledgement, and
4. MAC command.

- Optionally, this LR-WPAN offers a superframe mode.

- In this mode, a PAN coordinator transmits beacons in predetermined intervals (15 ms–245 s).

- With the help of beacons, the medium access scheme can have a period when contention is possible and a period which is contention free.

- Furthermore, with beacons a slotted CSMA/CA is available.

Security

IEEE 802.15.4 specifies three levels of security: no security, access control lists, and symmetric encryption using AES-128. Key distribution is not specified further. Security is a must for home automation or industry control applications.

Wireless USB

USB requires connections via cables, which can become a jumble when many devices are involved.

And the cables limit the distance over which users can connect devices.

*To address this issue, a number of companies—including Alereon, Belkin International, D-Link, Fujitsu, Gemtek Technology, Hewlett Packard, Icron Technologies, Intel, Lenovo, LSI Corp., Realtek Semiconductor, Samsung, Staccato Communications, Synopsys, and Wisair—are beginning to release products based on **wireless USB (WUSB)**.*

WUSB uses much of wired USB's approach, including a host controller that does the work necessary to transfer data to and from peripherals and connected devices.

- CWUSB allows up to 127 devices to connect directly to a host and has a theoretical maximum speed and range of from 480 Mbps at 3 meters to 110 Mbps at 10 meters.
- The relatively short range lets multiple high-speed CWUSB clusters coexist within a small area without interference

UWB.

1. The WUSB standard is built on the WiMedia Alliance's Multiband Orthogonal Frequency Division Multiplexing (MB-OFDM) version of UWB.
2. UWB works via chip-based radios that modulate signals—in the form of high volumes of low-power electromagnetic pulses—across the entire available ultra wide band spectrum, which differs depending on the country involved.
3. For example, UWB is permitted in the 3.1 to 10.6 GHz spectrum range in the US, in the 3.4 to 4.8 GHz and 7.25 to 10.25 GHz ranges in Japan, and from a proposed 3.1 to 4.8 GHz in much of Europe.
4. By working with the entire spectrum, UWB can produce high performance with less energy use.
5. UWB's low power consumption makes WUSB suitable for battery powered devices.

Wi-Fi.

- While CWUSB works only with UWB, Icron has developed a WUSB version that also runs on Wi-Fi, which represents a set of Ethernet-based, wireless LAN technologies formalized as an evolving series of IEEE 802.11 standards.
- Wi-Fi moves data via radio waves in the 2.4 GHz or 5 GHz spectrum ranges. The technology commonly provides Internet availability, frequently via publicly accessible hotspots, and network connectivity for consumer electronics.

Security

- To protect sensitive transmissions from interception, CWUSB provides 128-bit Advanced Encryption Standard cryptography, WUSB provides an extra layer of security by enabling the host to randomly generate a one-time secret AES encryption key and transmit it to a device via either a USB cable used only for first-time setup or public-key encryption, in both cases to protect against interception

ZigBee Technology

ZigBee technology is a low data rate, low power consumption, low cost, wireless networking protocol targeted toward automation and remote control applications.

Introduction:

- The IEEE 802.15.4 committee and ZigBee Alliance worked together and developed the technology commercially known as ZigBee.
- It is expected to provide low-cost and low-power connectivity for devices that need battery life as long as several months to several years but does not require data transfer rates as high as those enabled by Bluetooth.
- ZigBee can be implemented in **mesh (peer- to-peer) networks larger** than is possible with Bluetooth.
- ZigBee-compliant wireless devices are expected to transmit 10–75 minutes, depending on the RF environment and power output consumption required for a given application, and operate in the unlicensed RF worldwide (2.4 GHz global, 915 MHz America, or 868 MHz Europe) bands.
- The data rate is 250 kbps at 2.4 GHz, 40 kbps at 915 MHz, and 20 kbps at 868 MHz.
- It allows up to 254 nodes. When ZigBee node is powered down, it can wake up and get a packet in around 15 msec.

Components of Zigbee:

A ZigBee system consists of several components.

- The most basic is the device.
- A device can be a
  full-function device (FFD) or
  reduced-function device (RFD).
- A network includes at least one FFD, operating as the personal area network (PAN) coordinator.
- The FFD can operate in three modes: a PAN coordinator, a coordinator, or a device.
- An RFD is intended for applications that are extremely simple and do not need to send large amounts of data.
- An FFD can talk to reduced-function or full-function devices, while an RFD can only talk to an FFD.

Topologies of Zigbee

ZigBee supports three types of topologies:

star topology,
peer-to-peer topology, and
cluster tree.

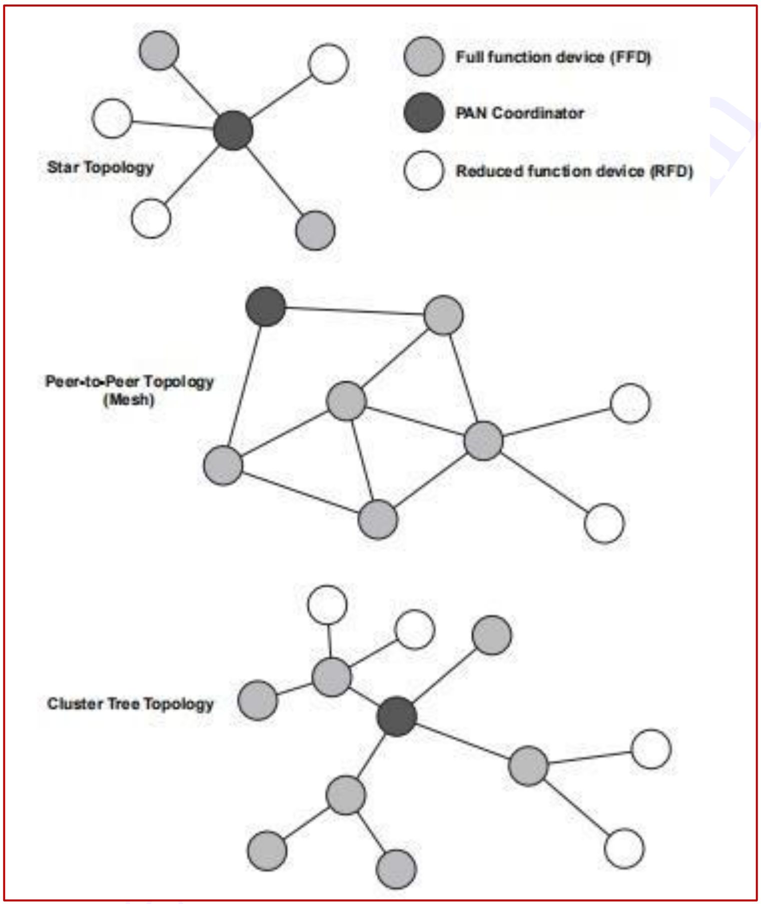

Full function device (FFD)
PAN Coordinator
Reduced function device (RFD)
Star Topology
Peer-to-Peer Topology (Mesh)
Cluster Tree Topology

Fig 26: ZigBee Topologies

1. In the ***star topology***, communication is established between devices and a single central controller, called the PAN coordinator.

2. In the ***peer-to-peer topology***, there is also one PAN coordinator. A peer-to-peer network can be ad hoc, self-organizing,and self-healing. Applications such as industrial control and monitoring, wireless sensor networks and asset and inventory tracking would benefit from such a topology.

3. The ***cluster-tree topology*** is a special case of a peer-to-peer network in which most devices are full-function devices and an RFD may connect to a cluster-tree network as a leaf node at the end of a branch.

6LoWPAN

IPV6 over Low Power Wireless Personal Area Network

6LoWPAN is an open standard defined in RFC 6282 by the Internet Engineering Task Force (IETF), the standards body that defines many of the open standards used on the Internet such as UDP, TCP and HTTP to name a few.

A powerful feature of 6LoWPAN is that while originally conceived to support IEEE 802.15.4 low-power wireless networks in the 2.4-GHz band, it is now being adapted and used over a variety of other networking media including Sub-1 GHz low-power RF, Bluetooth® Smart, power line control (PLC) and low-power Wi-Fi®.

- 6LoWPAN is a simple low cost communication network that allows wireless connectivity in applications with limited power and relaxed throughput requirements as it provides IPv6 networking over IEEE 802.15.4 networks

- It is formed by devices that are compatible with the IEEE 802.15.4 standard and characterized by short range, low bit rate, low power, low memory usage and low cost, where its architecture is shown in Figure below

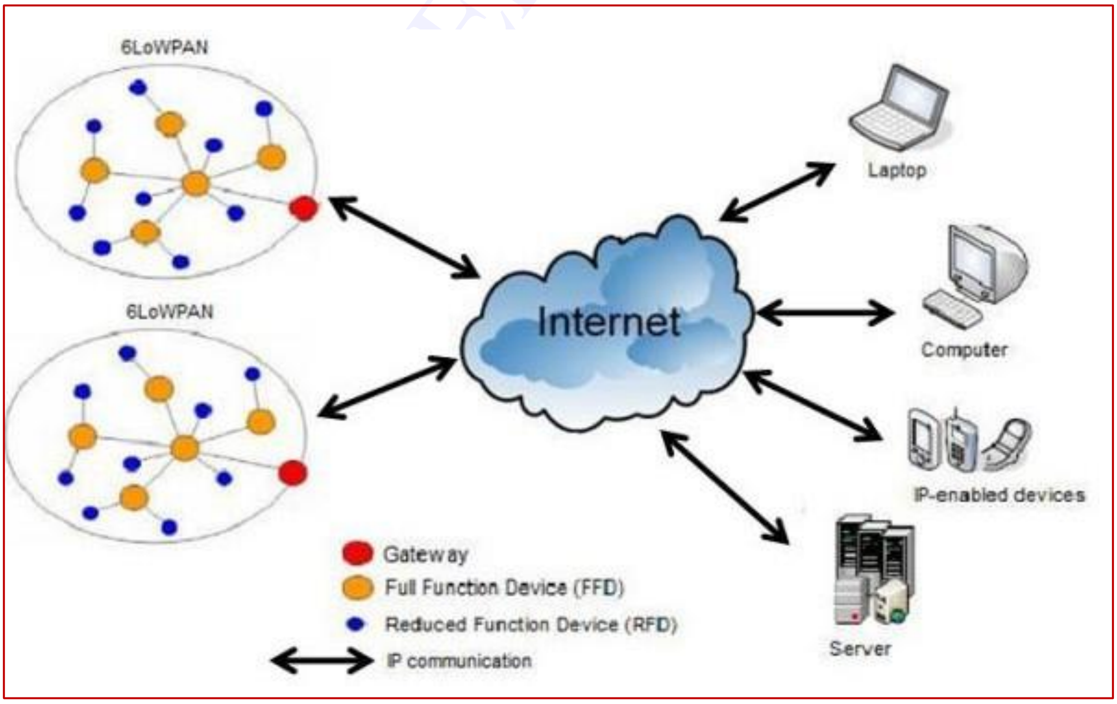


Fig 27: 6LoWPAN architecture

- When a lower processing capability sensor node in a 6LoWPAN or so-called reduced function device (RFD) wants to send its data packet to an IP-enabled device outside the 6LoWPAN, it first sends the packet to the higher processing capability sensor node or so-called full function device (FFD) in the same PAN.

- The FFDs which react as a router in 6LoWPAN will forward the data packet hop by hop to the 6LoWPAN gateway.

- The 6LoWPAN gateway that connect to the 6LoWPAN with the IPv6 domain will then forward the packet to the destination IP-enabled device by using the IP address.

Figure below describes the reference model of 6LoWPAN protocol stack.

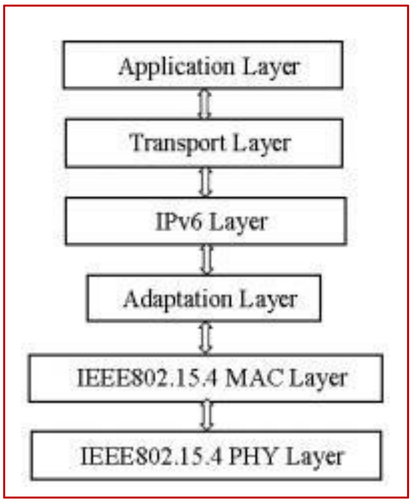


Fig 28: The reference model of 6LoWPAN protocol stack.

- It adopts IEEE 802.15.4 standard PHY and MAC layers as its bottom layers while chooses IPv6 in its network layer.

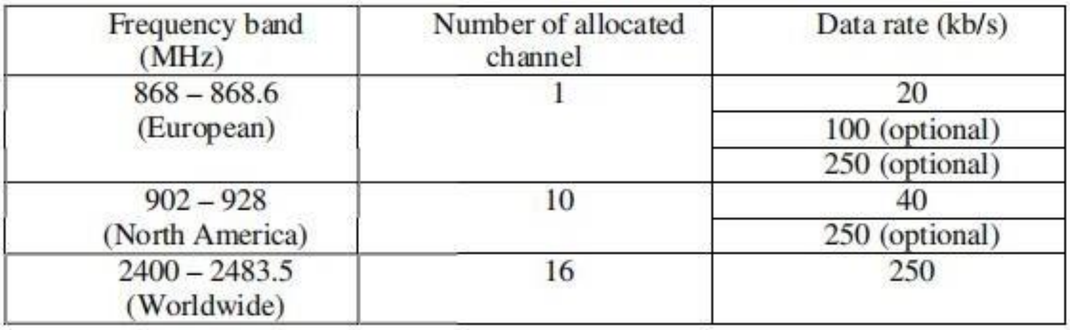
- Basically, IEEE 802.15.4 standard specifies PHY and MAC layers for low-rate wireless personal area network (LR-WPAN).

- The PHY layer specification dictates how the IEEE 802.15.4 devices may communicate with each other over a wireless channel.

- There are total of 27 channels defined in the PHY layer. These channels are allocated into different frequency bands with varying data rates as showed in Table below.

- 6LoWPAN working group suggested that adding an adaptation layer between MAC layer and the network layer to achieve the header compression, fragmentation and layer-two forwarding.

- LOAD protocol is a simplified on-demand routing protocol based on AODV. It is defined to be operating on top of the adaptation layer instead of the transport layer. It creates a mesh network topology underneath and unbeknownst to IPv6.



Frequency band (MHz)	Number of allocated channel	Data rate (kb/s)
868 – 868.6 (European)	1	20
		100 (optional)
		250 (optional)
902 – 928 (North America)	10	40
		250 (optional)
2400 – 2483.5 (Worldwide)	16	250

Table 4: Channel allocation in given frequency bands.

- At MAC layer, it specifies when the devices may access the channel for communication.

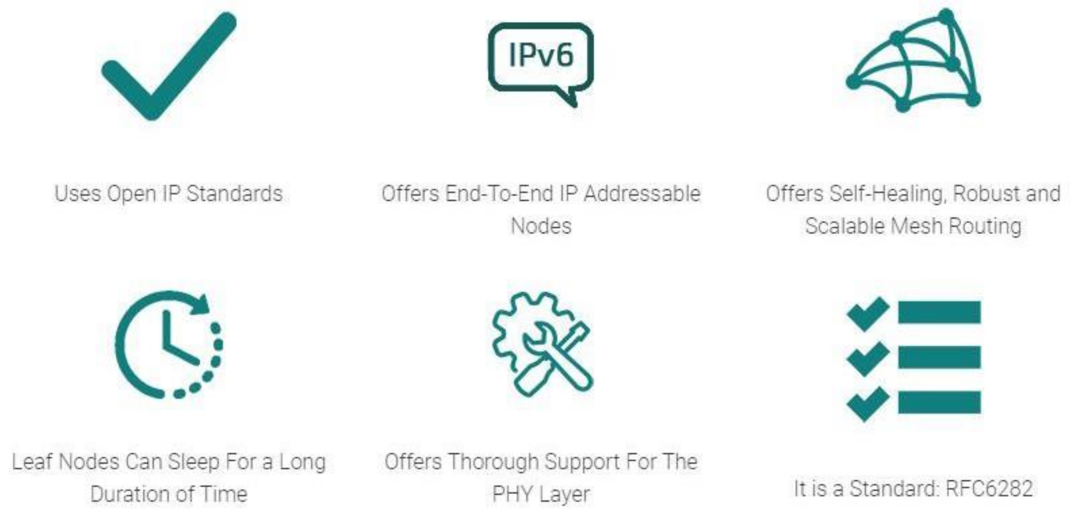
- The basic tasks provided by the MAC layer are beacon generation and synchronization, supporting PAN association and disassociation, managing channel access via Carriers Sense Multiple Access with Collision Avoidance (CSMA/CA) mechanism, and etc.

- IEEE 802.15.4 standard defined 4 frame structures for MAC layer: beacon frame, data frame, acknowledgement frame and MAC command frame.

- A beacon frame is used by a PAN coordinator to transmit beacons while a data frame is used for data transfers.

- For the acknowledgement frame and the MAC command frame, they are used for confirming successful frame reception and handling all MAC peer entity control transfers respectively.

Advantages of 6LoWPAN


IPv6
Uses Open IP Standards
Offers End-To-End IP Addressable Nodes
Offers Self-Healing, Robust and Scalable Mesh Routing
Leaf Nodes Can Sleep For a Long Duration of Time
Offers Thorough Support For The PHY Layer
It is a Standard: RFC6282

Applications where 6LoWPAN is being used:

1. **Automation:** There are enormous opportunities for 6LoWPAN to be used in many different areas of automation.

2. **Industrial monitoring:** Industrial plants and automated factories provide a great opportunity for 6LoWPAN.

3. **Smart Grid:** Smart grids enable smart meters and other devices to build a micro mesh network. They are able to send data back to the grid operator's monitoring and billing system using the IPv6.

4. **Smart Home:**By connecting your home IoT devices using IPv6, it is possible to gain distinct advantages over other IoT systems.

6LoWPAN Security

6LoWPAN can use AES-128 link layer security which is defined in IEEE 802.15.4. This provides link authentication and encryption.

WIRELESS HART

***WirelessHART** is a **wireless** sensor networking technology based on the Highway Addressable Remote Transducer Protocol (**HART**).*

- WirelessHART was defined for the requirements of process field device networks.

- The protocol utilizes a time synchronized, self-organizing, and self-healing mesh architecture.

- The protocol supports operation in the 2.4 GHz ISM band using IEEE 802.15.4 standard radios.

- HART is the global standard for sending and receiving digital information across the 4-20mA analog current loops that connect the vast majority of field instruments with distributed control systems.

- HART technology offers a reliable, long-term solution for plant operators who seek the benefits of intelligent devices with digital communication, while preserving existing investments in analog instrumentation and plant wiring.

- Much more than a communication protocol, with HART technology process plants have access to a wealth of digital process, maintenance, and diagnostic information.

- Information that is valuable throughout the plant lifecycle from design, to installation and configuration, through operation, and finally maintenance.

- HART is simple, reliable, and easy to use.

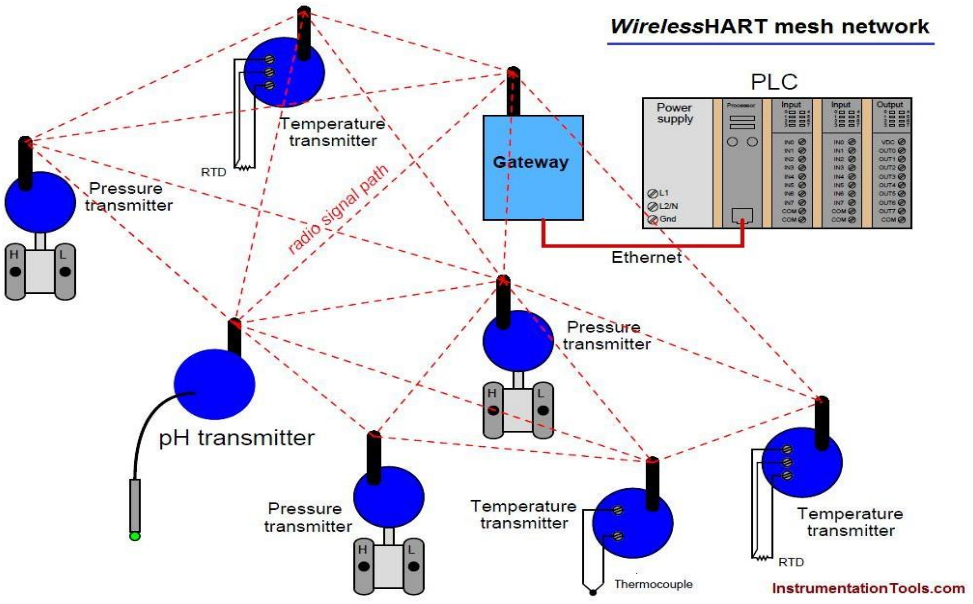


Fig 29: Wireless HART Mesh Network

ASSIGNMENT

1. **How is mobility restricted using WLANs? What additional elements are needed for roaming between networks, how and where can WLANs support roaming?**
   In your answer, think of the capabilities of layer 2 where WLANs reside.

Refer: "Mobile Communications" Second Edition - Jochen H. Schiller