

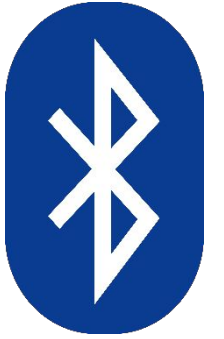
Module 4

Wireless Personal Area Networks and Ad hoc Networks

IEEE 802.15.1 (Bluetooth) – Piconet, Scatter net, Protocol Stack; IEEE 802.15.4 (ZigBee) – LRWPAN Device Architecture, Protocol Stack;

Wireless Sensor Network – Design Considerations, Issues and Challenges, WSN Architecture, Applications; Introduction of Ad hoc Networks – MANET and VANET – Characteristics, Applications, Advantages and Limitations; Overview of E-VANET(Electrical Vehicular AdHoc Networks).

Self-learning Topics:- HR-WPAN (UWB)



WIRELESS PERSONAL AREA NETWORK

BLUETOOTH

The Wireless Personal Area Network

- A wireless personal area network (WPAN) is a short-distance (typically 10 m but as far as 20 m) wireless network specially designed to support portable and mobile computing devices such as PCs, PDAs, printers, storage devices, cellphones, pagers, set-up boxes, and a variety of consumer electronic equipment.
- Bluetooth (IEEE 802.15.1), UWB (IEEE 802.15.3a), and ZigBee (IEEE 802.15.4) are examples of WPANs that allow devices within close proximity to join together in wireless networks in order to exchange information.

The Wireless Personal Area Network

- WPANs such as **Bluetooth** provide enough bandwidth and convenience to make data exchange practical for certain mobile devices requiring data exchanges at **rates up to 1 Mbps**.
- At the other end of the scale, **UWB** will provide the capability of streaming video signals at **data rates up to 1 Gbps**.
- Many control and command applications require much **lower data rates** and also the **lowest possible cost**, thus **ZigBee (250kbps)**.

The Wireless Personal Area Network

- The IEEE 802.15 committee has the responsibility for developing standards for short distance wireless networks used in the networking of portable and mobile computing devices.
- IEEE 802.15.1 and 802.15.4 focus on the following characteristics:**
 - Power management: Low current consumption
 - Range: 0–10 m
 - Rate: 19.2–1000 kbps
 - Size: 0.5 in³ without antenna
- Low cost relative to target device
- Should allow overlap of multiple networks in the same area
- Network supports a minimum of 16 devices

Bluetooth (IEEE 802.15.1)

- Bluetooth provides short-range, low-cost connectivity between portable devices.
- **The low power consumption makes Bluetooth ideal** for small, battery-powered devices like mobile phones and pocket PCs.
- Bluetooth is limited in range (**10 meters**) and bandwidth **780 kbps**
- The Bluetooth system operates in the **2.4 GHz Industrial Scientific Medicine (ISM) band**.
 - In a vast majority of countries around the world the range of this frequency band is **2.4–2.4835 GHz**.
 - The ISM band is open to any radio system such as cordless phones, garage door openers, and microwaves, and therefore is susceptible to strong interferences

Bluetooth (IEEE 802.15.1)

Some other features

- A Bluetooth WPAN involves up to **eight devices**, located within a 10-m radius personal operating space, that unite to exchange information or share services.
- *"ad hoc networking"*- Because it can be done spontaneously according to immediate need.
- *"point-to-point network"* -Because a WPAN involves directly networking between different points, without the use of network infrastructure.
- *absolutely anywhere*- at least two Bluetooth devices share a 10-m range.

Bluetooth (IEEE 802.15.1)

- fast acknowledgment and frequency hopping scheme - make the link robust.
- hops faster and uses shorter packets- Short packets and fast hopping limit the impact of interference from other radio systems that use the same frequency band.
- forward error correction (FEC) scheme- limits the impact of random noise on long-distance links.

Bluetooth (IEEE 802.15.1)

Uses of Bluetooth

- Bluetooth is being used in mobile computers, bar code laser scanners, cash registers, vending machines, GPS receivers, slide projectors, printers, digital cameras, digital camcorders, test and measurement equipment, and LAN access points.
- IEEE 802.15.1. standards development for Bluetooth
- The IEEE is also exploring the enhancement of 802.15.1 with a high data rate Bluetooth standard: 802.15.3

Definitions of the Terms Used in Bluetooth

Piconet: A collection of devices connected via Bluetooth technology in an ad hoc fashion

- A piconet starts with two connected devices, such as a PC and cellular phone, and may grow to eight connected devices.(Why piconet is having maximum 8 devices? Hint- Mac address **A 3-bit**)
- All Bluetooth devices are peer units and have identical implementations.
- In a piconet, one unit will act as a master for synchronization purposes, and the other(s) as slave(s) for the duration of the piconet connection.

Definitions of the Terms Used in Bluetooth

Scatternet: Two or more independent and non-synchronized piconets that communicate with each other.

- A slave as well as a master unit in one piconet can establish this connection by becoming a slave in the other piconet.

Master unit. The device in the piconet whose clock and hopping sequence are used to synchronize all other devices in the piconet.

Slave units. All devices in a piconet that are not the master (up to seven active units for each master).

Definitions of the Terms Used in Bluetooth

MAC address: A 3-bit medium access control address used to distinguish between units participating in the piconet

Parked units: Devices in a piconet which are time-synchronized but do not have MAC addresses.

Sniff and hold mode: Devices that are synchronized to a piconet, and which have temporarily entered power-saving mode in which device activity is reduced.

Bluetooth Protocol Stack

- The Bluetooth protocol stack allows devices to locate, connect, and exchange data with each other and to execute interoperable, interactive applications against each other.
- The Bluetooth protocol stack can be placed into three groups:
 - ✓ Transport protocol group,
 - ✓ Middleware protocol group,
 - ✓ Application group

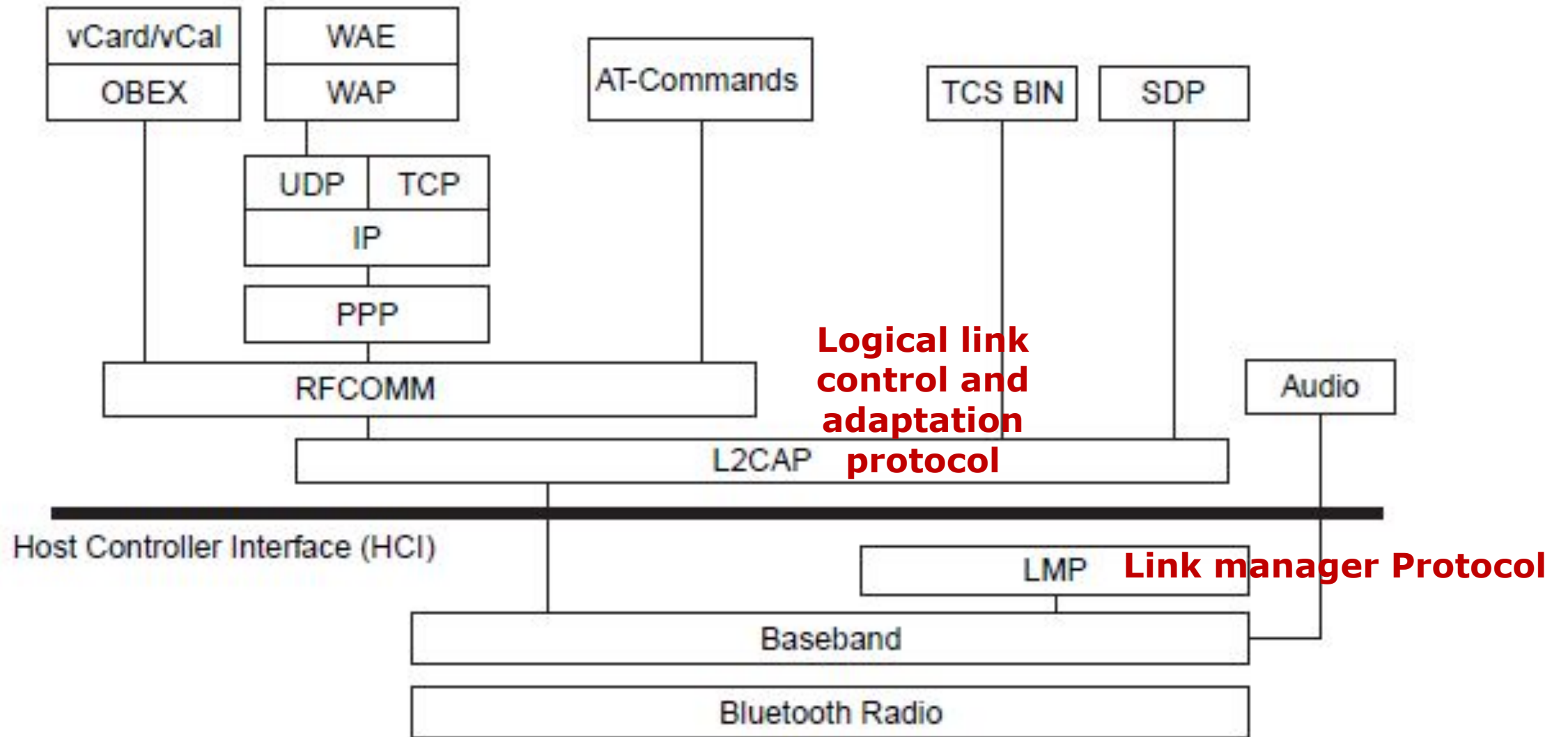
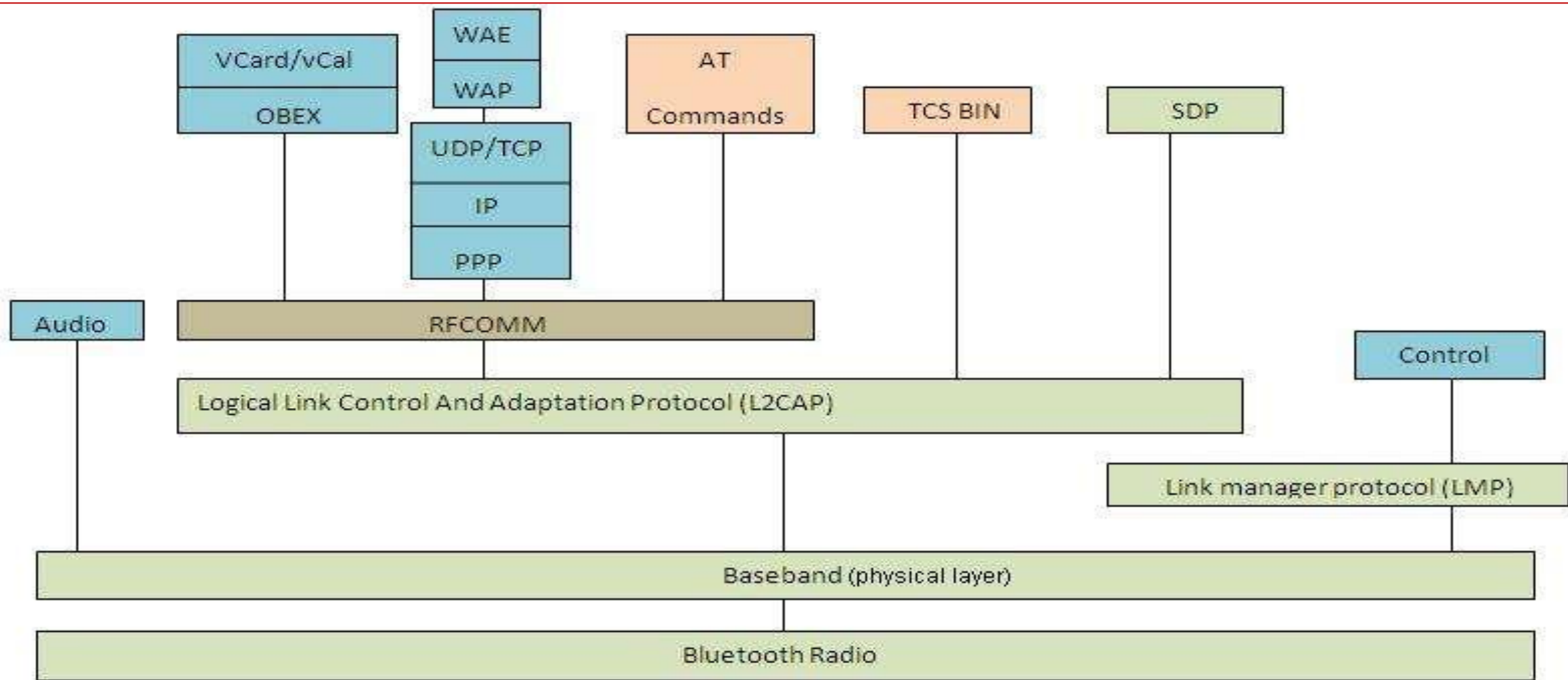






Figure 19.2 Bluetooth protocol stack.



Bluetooth Protocol Stack

-  Core protocols
-  Cable replacement protocol
-  Telephony Control protocols
-  Adopted protocols

Transport Protocol Group

- The protocols in this group are designed to allow Bluetooth devices to locate and connect to each other.
- These protocols carry audio and data traffic between devices and support both synchronous and asynchronous transmission for telephony-grade voice communication.
- Audio traffic is treated with high priority in Bluetooth.
- Audio traffic bypasses all protocol layers and goes directly to the baseband layer which then transmits it in small packets directly over Bluetooth's air interface.

Transport Protocol Group

- The protocols in this group are also responsible for managing the physical and logical links between the devices so that the layers above and applications can pass data through the connections.
- The protocols in this group are radio, baseband, link manager, logical link control and adaptation, and host controller interface (HCI).

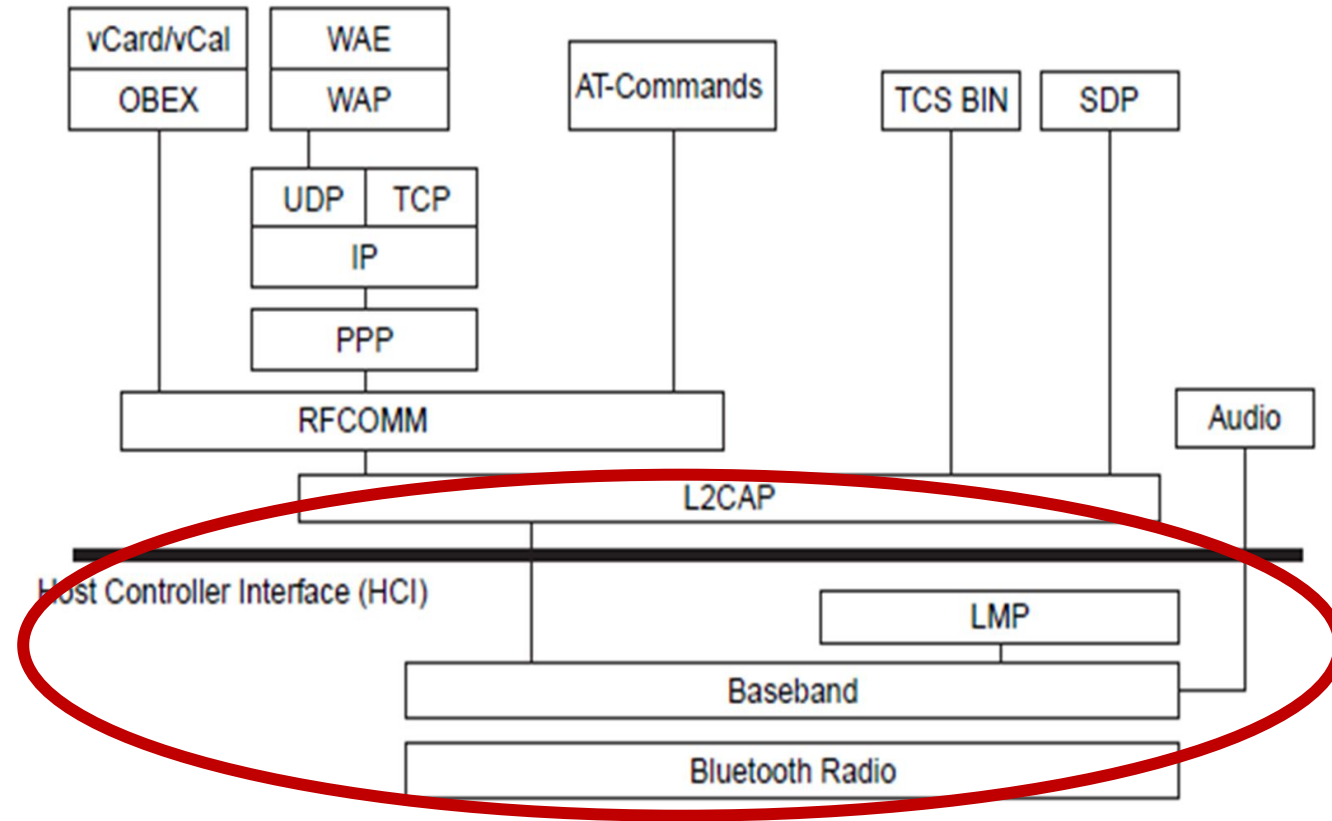


Figure 19.2 Bluetooth protocol stack.

Transport Protocol Group

Logical link control and adaptation protocol (L2CAP) layer:

- ✓ **All data traffic** is routed through L2CAP layer
- ✓ This layer shields the higher layers from the details of the lower layers.
- ✓ It is also responsible for segmenting larger packets from higher layers into smaller packets, which are easier to handle by the lower layer.
- ✓ The L2CAP layer is responsible for admission control based on the requested level of service and for coordinating with the lower layers to maintain this level of service.

Transport Protocol Group

Link manager Protocol(LMP):

- ✓ **The link manager** layers are responsible for negotiating the properties of the Bluetooth air interface between them.
- ✓ These properties may be anything from bandwidth allocation to support services of a particular type to periodic bandwidth reservation for audio traffic.
- ✓ This layer is responsible for supervising device pairing.
- ✓ Device pairing is the creation of a trust relationship between the devices by generating and storing an authentication key for future device authentication.
- ✓ The link managers are also responsible for power control and may request adjustments in power levels.

Transport Protocol Group

Baseband and radio layers:

- ✓ The baseband layer is responsible for the process of searching for other devices and establishing a connection with them.
- ✓ It is also responsible for assigning the master and slave roles.
- ✓ This layer also controls the Bluetooth unit's synchronization and transmission frequency hopping sequence.

Transport Protocol Group

Host controller interface (HCI) layer:

- The HCI allows higher layers of the stack, including applications, to access the baseband, link manager, etc., through a single standard interface.
- Through HCI commands, the module may enter certain modes of operation

Middleware Protocol Group

- ✓ This group comprises the protocols needed for existing applications to operate over Bluetooth links.
- ✓ The protocols in this group can be **third party and industry standard protocols and protocols developed specifically by the Special Interest Group (SIG) for Bluetooth wireless communication.**
- ✓ The protocols in this group can include **TCP, IP, PPP, A serial port emulator protocol RFCOMM, service discovery protocol (SDP), etc.,**

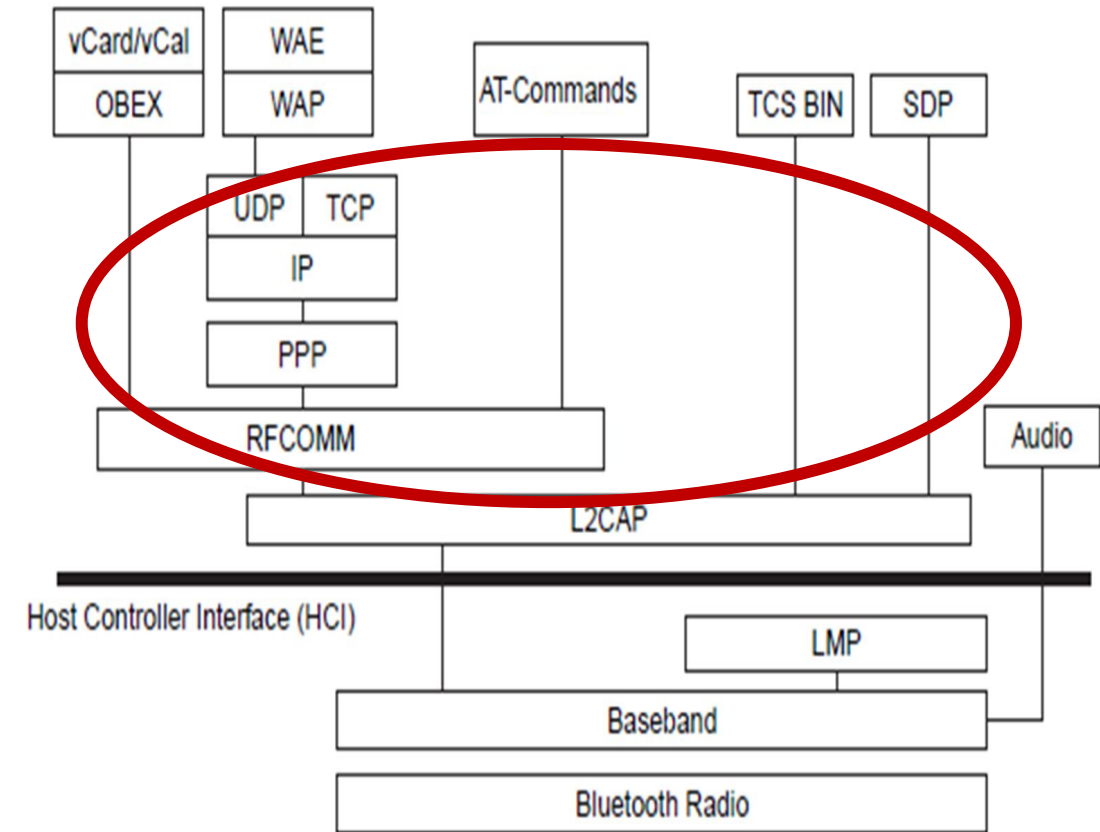


Figure 19.2 Bluetooth protocol stack.

RFCOMM layer:

- ✓ Bluetooth's prime aim is to eliminate cables and provide support for serial communication without cables.
- ✓ RFCOMM provides a virtual serial port to applications.
- ✓ The advantage provided by this layer is that it is easy for applications designed for cabled serial ports to migrate to Bluetooth.
- ✓ The applications can use RFCOMM much like a serial port to accomplish scenarios like dial-up networking, etc.
- ✓ RFCOMM is an important part of the protocol stack because of the function it performs.

Service discovery protocol (SDP) layer:

- ✓ In Bluetooth wireless communications any two devices can start communicating on the spur of the moment. Once a connection is established there is a need for the devices to find and understand the services the other devices have to offer. This is taken care of in this layer.
- ✓ The SDP is a standard method for Bluetooth devices to discover and learn about the services offered by the other device.
- ✓ Service discovery is important in providing value to the end-user.

Object exchange (OBEX) protocol.

- ✓ IrOBEX (in short, OBEX) is a session protocol developed by the Infrared Data Association to exchange objects in a simple and spontaneous manner.
- ✓ OBEX provides the same basic functionality as HTTP but in a much lighter fashion.
- ✓ It uses a client-server model and is independent of the transport mechanism and transport application programming interface (API), provided it realizes a reliable transport base.

Networking layers:

- ✓ Bluetooth wireless communication uses a **peer-to-peer network topology** rather than an LAN type topology.
- ✓ Dial-up networking uses the **attention (AT) command layer**.
- ✓ In most cases the network that is being **accessed is an IP network**.
Once a dial-up connection is established to an IP network, then **standard protocols like TCP, UDP, and HTTP can be used**.
- ✓ A device can also connect to an IP network using a network access point. **The Internet PPP is used to connect to the access point**.
- ✓ The specification does not define a profile that uses the TCP/IP directly over Bluetooth links.

Telephone control specification (TCS) layer and audio:

- ✓ This layer is designed to support telephony functions, which include call control and group management. These are associated with setting up voice calls.
- ✓ Once a call is established a Bluetooth audio channel can carry the call's voice content. TCS can also be used to set up data calls.
- ✓ The TCS protocols are compatible with ITU specifications.
- ✓ The SIG is also considered a second protocol called TCS-AT, which is a modem control protocol.

Audio and Data transmission in Bluetooth

- ✓ Audio traffic is treated separately in Bluetooth.
- ✓ Audio traffic is isochronous (occupying equal time), meaning that it has a time element associated with it.
- ✓ Audio traffic is routed directly to the baseband.
- ✓ Special packets called synchronous connection-oriented are used for audio traffic.
- ✓ Bluetooth audio communication takes place at a rate of 64 kbps using one of the two data encoding schemes —
 - 8-bit logarithmic pulse code modulation
 - continuous variable slope delta modulation.

Application Group

- ✓ This group consists of actual applications that make use of Bluetooth links and refers to the software that exists above the protocol stack.
- ✓ The software uses the protocol stack to provide some function to the user of the Bluetooth devices.
- ✓ The Bluetooth-SIG does not define any application protocols nor does it specify any API.
- ✓ Bluetooth profiles are developed to establish a base point for use of a protocol stack to accomplish a given usage case.

Bluetooth Link Types

The Bluetooth baseband technology supports two link types:

- ✓ Synchronous connection oriented (SCO) type
 - used primarily for voice
- ✓ Asynchronous connectionless (ACL) type
 - used primarily for packet data

Different master-slave pairs of the same piconet can use different link types and the link type may change arbitrarily during a session.

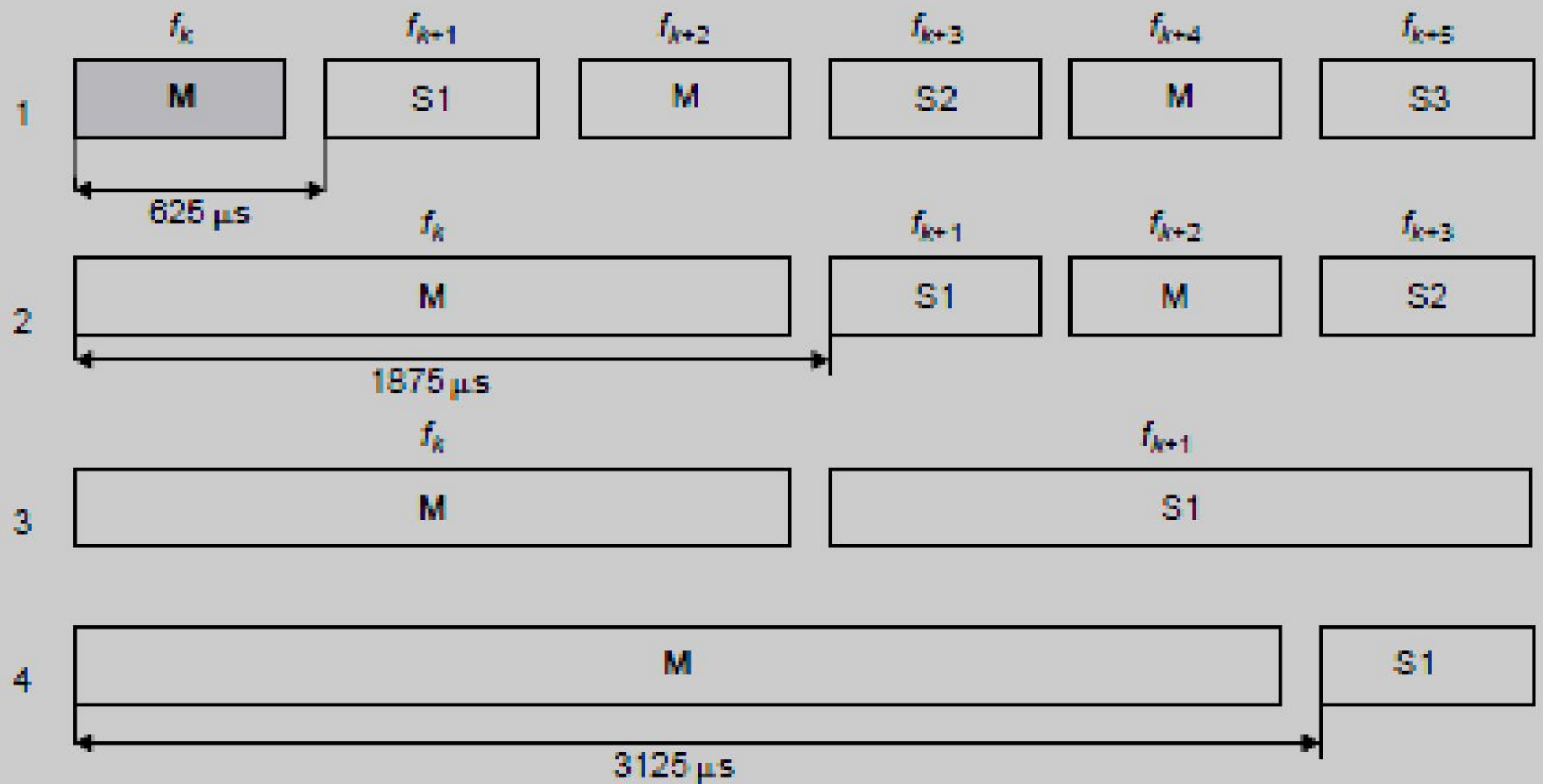
Features

- ✓ Each link type supports up to **sixteen different packet types**.
- ✓ **Four of these are control packets** and are common for both SCO and ACL links.
- ✓ Both link types use a **time division duplex (TDD)** scheme for full-duplex transmission.
- ✓ The SCO link is symmetric and typically **supports time-bounded voice traffic**.
- ✓ **SCO packets are transmitted over reserved intervals**.
- ✓ Once the connection is established, both master and slave units may send SCO packets without being polled.
- ✓ The SCO link type supports and is used often for voice traffic.
- ✓ **The data circuit-switched, point-to-point connections for SCO links is 64 kbps.**

Features

- ✓ The ACL link is **packet oriented** and supports both symmetric and asymmetric traffic.
- ✓ The **master unit controls the link bandwidth and decides how much piconet bandwidth is given to each slave**, and the symmetry of the traffic.
- ✓ **Slaves must be polled before they can transmit data.**
- ✓ The ACL link also **supports broadcast messages** from the master to all slaves in the piconet.
- ✓ Multislot packets can be used in ACL and they can reach maximum **data rates of 721 kbps in one direction and 57.6 kbps in the other direction if no error correction is used**

- ✓ Data packets are protected by an automatic retransmission query (ARQ) scheme.
- ✓ Thus, when a packet arrives, a check is performed on it.
- ✓ If there is an error detected, the receiving unit indicates this in the return packet.
- ✓ In this way, retransmission is done only for the faulty packets. Retransmission is not feasible for voice so better error protection is used.



1. One-slot symmetrical; 2. Three-slot asymmetrical; 3. Three-slot symmetrical;
4. Five-slot asymmetrical

Type	Link	Name	No. of slots	Description
0000	Common	Null	1	No payload; used to return link information to source about the success of previous transmission, or status of Rx buffer (flow); no ACK
0001	Common	Poll	1	No payload, used by master to poll slave; ACK
0010	Common	FHS	1	Special control packet for revealing device address and the clock of sender; used in page master response, inquiry response, and frequency hop synchronization; $2/3$ FEC encoded
0011	Common	DM1	1	Support control messages and can also carry user data, 16-bit CRC, $2/3$ FEC encoded
0100	ACL	DH1	1	Carries 28 information bytes (header + payload) + 16 bit-CRC; not FEC encoded; used for high-speed data services
0101	SCO	HV1	1	Carries 240 bits for user voice samples, used for 64kbps voice, no FEC encoding

Type	Link	Name	No. of slots	Description
0110	SCO	HV2	1	Carries 160 bits for user voice samples and 80 bits of parity for $\frac{1}{3}$ FEC encoding
0111	SCO	HV3	1	Carries 80 bits for user voice samples and 160 bits of parity for $\frac{2}{3}$ FEC encoding
1000	SCO	DV	1	Combined data (150 bits) and voice (50 bits) packet data field, $\frac{2}{3}$ FEC encoded
1001	ACL	AUX1	1	Carries 30 information bytes, no CRC or FEC, used for high-speed data services
1010	ACL	DM3	3	Carries 123 information bytes + 16-bit CRC, $\frac{2}{3}$ FEC encoded
1110	ACL	DH3	3	Carries 185 information bytes + 16-bit CRC, not FEC encoded
1110	ACL	DM5	5	Carries 226 information bytes + 16-bit CRC, $\frac{2}{3}$ FEC encoded
1111	ACL	DH5	5	Carries 341 information bytes + 16-bit CRC, not FEC encoded

- ✓ A symmetric 1-slot DH1 link between the master and slave carries **216 bits per slot at a rate of 800 slots per second** in each direction. The associated rate is $216 \times 800 = 172.8$ kbps.
- ✓ The asymmetric DM5 link uses a 5-slot packet carrying **1792 bits** per packet by the master and a 1-slot packet carrying **136 bits** per packet by the slave terminal.
- ✓ The number of packets per second in each direction is $1600/6$. (1600 hopping rate per second).
- ✓ The data rate of the master is **$1792 \times 1600/6 = 477.8$ kbps** and the data rate of the slave terminal is **$136 \times 1600/6 = 36.3$ kbps.**

Example 13.6: Data Rate of High Quality Voice Packets

The HV1 packets are 240 bits long, and so they are sent every six slots. The packets are 1-slot packets sent at the rate of 1,600 slots/sec. Therefore, we have

$$\frac{1,600 \text{ (slots/sec)}}{6 \text{ (slots)}} \times 240 \text{ (bits)} = 64 \text{ kbps}$$

- ✓ The asymmetric DH5 link uses a 5-slot packet carrying 2712 bits per packet by the master and a 1-slot packet carrying 216 bits per packet by the slave terminal.
- ✓ The number of packets in each direction is $1600/6$ packets per second.
- ✓ The data rate of the master is $2712 \times 1600/6 = 723.2$ kbps and the data rate of the slave terminal is $216 \times 1600/6 = 57.6$ kbps.

ZIGBEE TECHNOLOGY

Introduction

Low rate (LR) wireless personal access network (WPAN) (IEEE 802.15.4/LRWPAN)

is intended to serve a set of industrial, residential, and medical applications.

- very low power consumption, low cost requirement, and relaxed needs for data rate and QoS.
- The low data rate enables the LR-WPAN to consume little power.
- ZigBee technology is a low data rate, low power consumption, low cost, wireless networking protocol targeted toward automation and remote control applications.

□ The **IEEE 802.15.4** committee and **ZigBee Alliance** worked together and developed the technology commercially known as **ZigBee**.

Features/ characteristics:

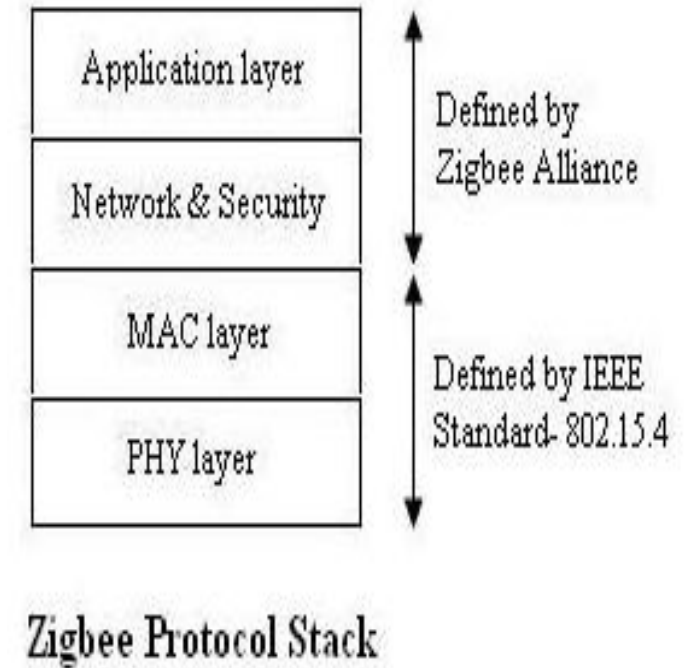
- 1) ZigBee-compliant wireless devices are expected to transmit **10–75 minutes**, depending on the RF environment and power output consumption required for a given application.
- 2) Operate in the unlicensed RF worldwide (**2.4 GHz global, 915 MHz America, or 868 MHz Europe**) bands.
- 3) The data rate is
250 kbps at 2.4 GHz,
40 kbps at 915 MHz, and
20 kbps at 868 MHz.

□ The IEEE 802.15.4 committee is focusing on the specifications of the lower two layers of the protocol (the physical and data link layers).

□ On the other hand, ZigBee Alliance aims to provide the upper layers of the protocol stack (from the network to the application layer) for interoperable data interworking, security services, and a range of wireless home and building control solutions.

□ ZigBee often uses a basic master-slave configuration suited to static star networks of many infrequently used devices that talk via small data packets. It allows up to 254 nodes.

□ Other network topologies such as peer-to-peer and cluster tree are also used.



ZigBee Components and Network Topologies

Device- A device can be a full-function device (FFD) or reduced-function device (RFD).

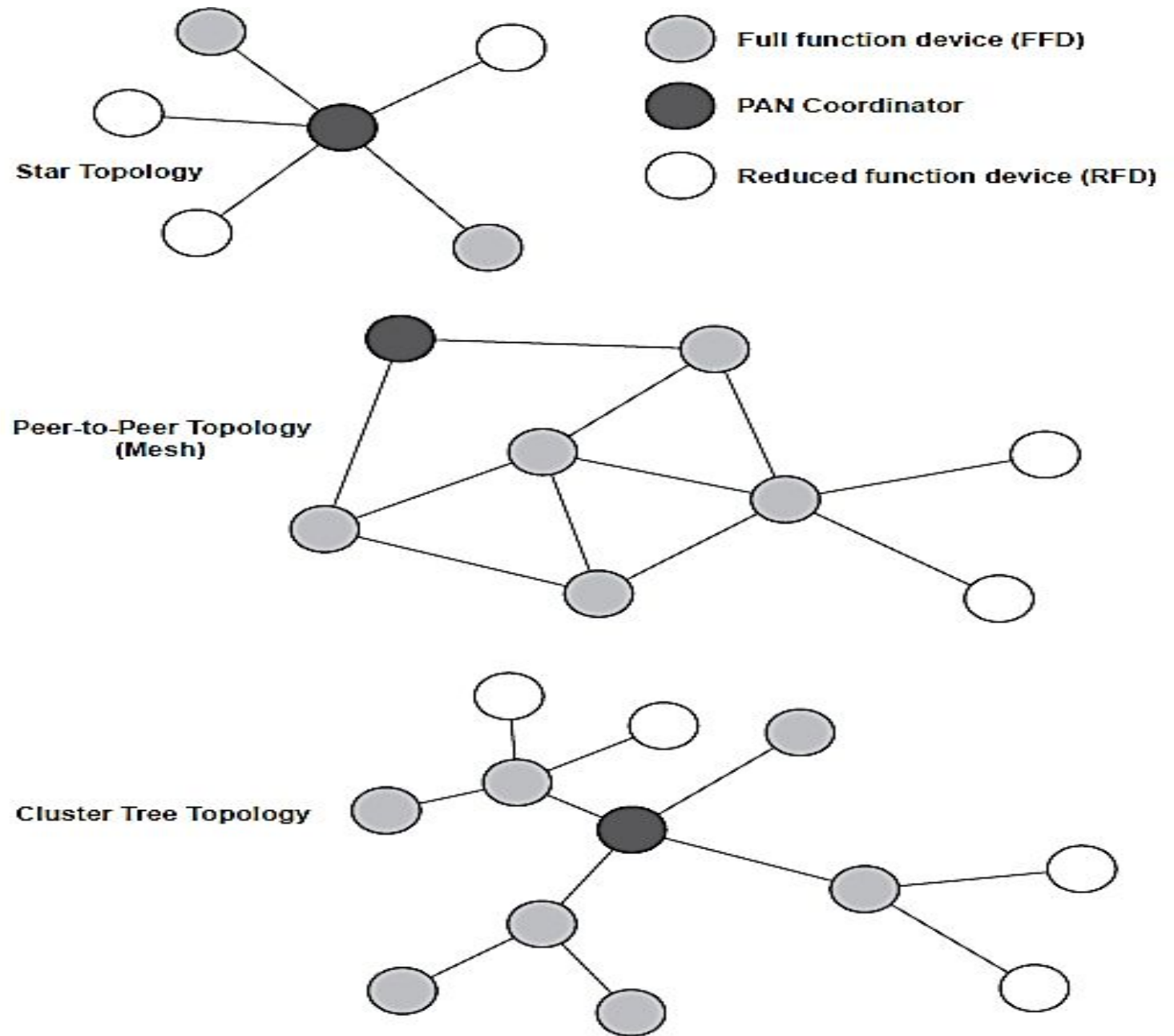
- A network includes **at least one FFD**, operating as the personal area network (PAN) coordinator.
- The FFD can operate in three modes:
 - a PAN coordinator,**
 - a coordinator,**
 - or a device.**
- An **RFD** is intended for applications that are extremely simple and do not need to send large amounts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

ZigBee supports three types of topologies:

- ✓ star topology,
- ✓ peer-to-peer topology
- ✓ cluster tree

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

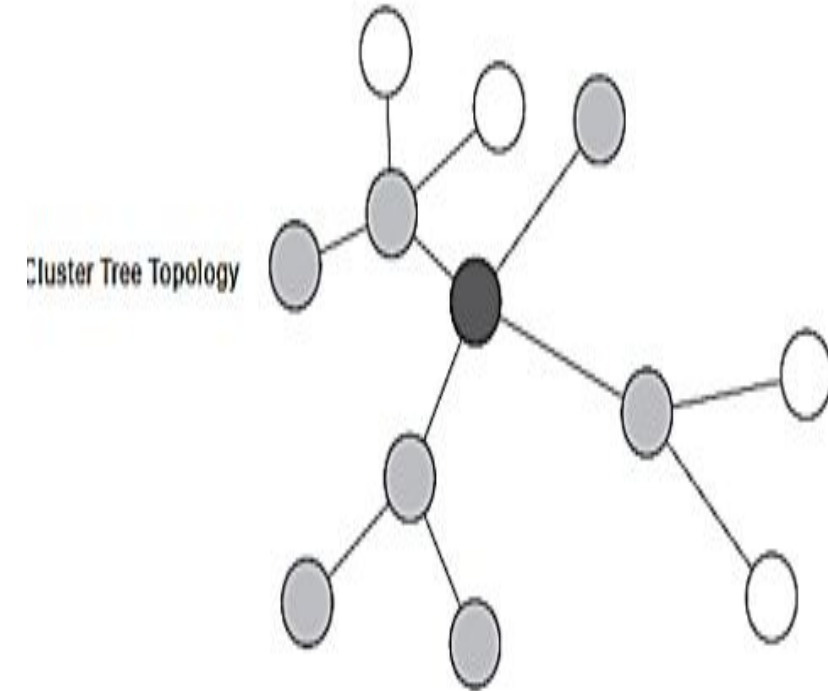
□ The PAN coordinator may be powered by mains while the devices will most likely be battery powered.



- Applications that benefit from this topology are home automation, personal computer (PC) peripherals, toys, and games.
- After an FFD is activated for the first time, it may establish its own network and become the PAN coordinator.
- Each star network chooses a PAN identifier, which is not currently used by any other network within the radio sphere of influence.
- This allows each star network to operate independently.

- In the **peer-to-peer topology**, there is also **one PAN coordinator**.
- In contrast to star topology, **any device can communicate with any other device** as long as they are in range of one another.
- 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.
- It also allows multiple hops to route messages from any device to any other device in the network.
- It can provide reliability by multipath routing.

- 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.**
- Any of the full-function devices can act as a coordinator and provide synchronization services to other devices and coordinators.
- However, only one of these coordinators is the PAN coordinator.
- The **PAN coordinator forms the first cluster by establishing itself as the cluster head (CLH)** with a **cluster identifier (CID) of zero**, choosing an unused PAN identifier, and broadcasting beacon frames to neighboring devices.

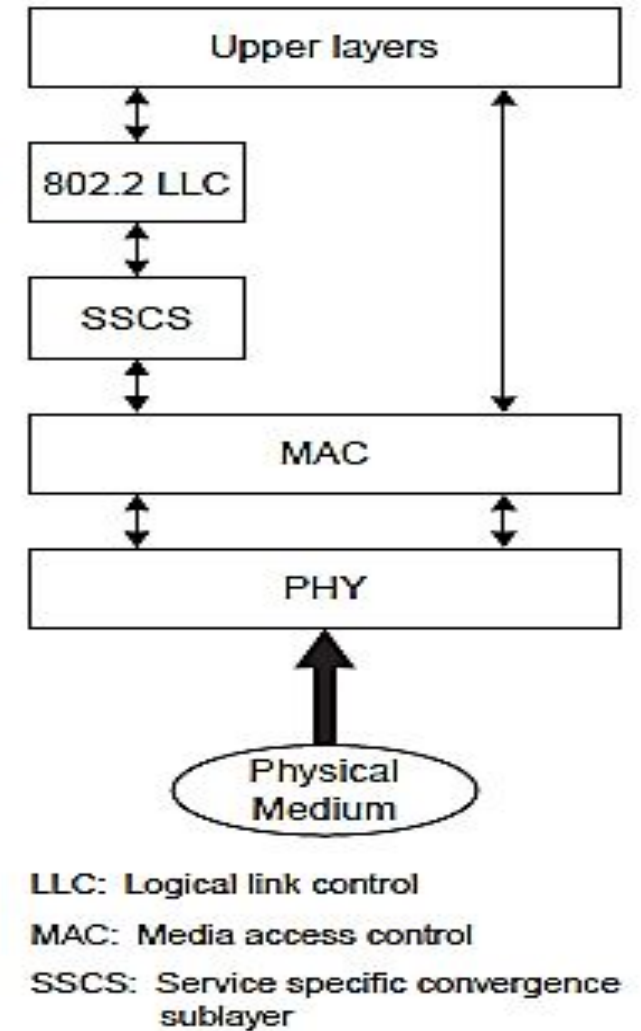


- A candidate device receiving a beacon frame may request to join the network at the cluster head. If the PAN coordinator permits the device to join, it will add this new device to its neighbor list.
- The newly joined device will add the cluster head as its parent in its neighbor list and begin transmitting periodic beacons such that other candidate devices may then join the network at that device.
- Once application or network requirements are met, the PAN coordinator may instruct a device to become the cluster head of a new cluster adjacent to the first one.
- The advantage of the clustered structure is the increased coverage at the cost of increased message latency.

IEEE 802.15.4 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).



WPAN device architecture.

Physical Layer

□ The PHY (IEEE 802.15.4) provides two services:

The PHY data service and

The PHY management service interfacing to the physical layer management entity (PLME).

□ The PHY data service enables the transmission and reception of PHY protocol data units (PPDUs) across the physical radio channel.

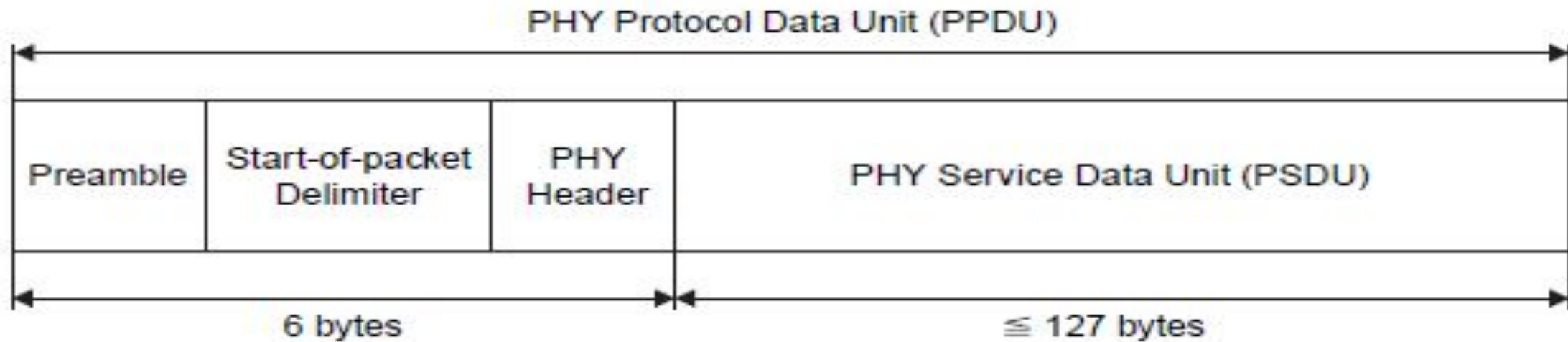
□ The features of the PHY are activation and deactivation of the radio transceiver, energy detection (ED), link quality indication (LQI), channel selection, clear channel assessment (CCA) and transmitting as well as receiving packets across the physical medium.

- The standard provides two options based on the frequency band. Both are based on **direct sequence spread spectrum (DSSS)**.
- The data rate is **250 kbps at 2.4 GHz, 40 kbps at 915 MHz, and 20 kbps at 868 MHz**.
- The higher rate at 2.4 GHz is attributed to a higher-order modulation scheme.
- Lower frequency provides **longer range due to lower propagation losses**. **Low rate can be translated into better sensitivity and larger coverage area**.
- **Higher rate means higher throughput, lower latency, or lower duty cycle**.

Table 20.3 Frequency bands and data rates.

PHY (MHz)	Freq. band (MHz) and number of channels	Spreading parameters		Data parameters		
		Chip rate (kcps)	Modulation	Bit rate (kbps)	Symbol rate (ksps)	Symbol
868/915	868–868.6 (1 channel)	300	BPSK	20	20	Binary
	902–928 (10 channels)	600	BPSK	40	40	Binary
2450	2400–2483.5 (16 channels)	2000	OQPSK	250	62.5	16-ary orthogonal

- To maintain a common simple interface with MAC, both PHY share a single packet structure (see Figure 20.7).
- Each PHY protocol data units PPDU contains a synchronization header (preamble plus start of packet delimiter), a PHY header to indicate the packet length, and the payload, or PHY service data unit (PSDU).
- The 32-bit preamble is designed for the acquisition of symbol and chip timing, and in some cases may be used for coarse frequency adjustment.
- Channel equalization is not required for either PHY due to the combination of small coverage area and relatively low chip rates.



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

Figure 20.7 IEEE 802.15.4 PHY packet structure.

- Within the PHY header, 8 bits are used to specify the length of the payload (in bytes). This supports packets of length 0–127 bytes, although, due to MAC layer overhead, zero-length packets will not occur in practice.

- Typical packet sizes for **home applications** such as monitoring and control security, lighting, air conditioning, and other appliances are expected to be **of the order of 30–60 bytes**,
- while more demanding applications such as interactive games and computer peripherals, or multihop applications with more address overhead, may require larger packet sizes.
- **Adjusting transmission rates in each frequency band, the maximum packet durations are**
 - 4.25 ms for the 2.4 GHz band,**
 - 26.6 ms for the 915 MHz band, and**
 - 53.2 ms for the 868 MHz band.**

868/915 MHz PHY features

- The 868/915 MHz PHY uses a **simple DSSS approach** in which each transmitted bit is represented by a **15-chip maximum length sequence**.
- **Binary data is encoded** by multiplying each m-sequence by 1 or -1, and the resulting chip sequence is **modulated onto the carrier using binary phase shift keying (BPSK)**.
- **Differential data encoding is used prior to modulation** to allow low-complexity differential coherent reception.

2.4 GHz PHY features

- The 2.4 GHz PHY uses a 16-ary quasi-orthogonal modulation technique based on DSSS methods.
- Binary data is grouped into 4-bit symbols, and each symbol specifies one of sixteen nearly orthogonal 32-chip, pseudo-random noise (PN) sequences for transmission.
- PN sequences for successive data symbols are concatenated, and the aggregate chip sequence is modulated onto the carrier using, offset-quadrature phase shift keying (OQPSK).

Data Link Layer

The data link layer (IEEE 802.15.4) is divided into two sublayers, the MAC and LLC sublayers.

The logical link control is standardized in IEEE 802.2 and is common among all IEEE 802 standards.

The IEEE 802.15.4 MAC provides services to an IEEE 802.2 type logical link control through the service-specific convergence sublayer (SCCS), or a proprietary LLC can access the MAC services directly without going through the SCCS.

The SCCS ensures compatibility between different LLC sublayers and allows the MAC to be accessed through a single set of access points.

The features of the IEEE 802.15.4 MAC are

- association and disassociation,
- acknowledged frame delivery,
- channel access mechanism,
- frame validation,
- guaranteed time slot management,
- beacon management.

- The MAC provides **two services** to higher layers that can be accessed through **two service access points (SAPs)**.
 - 1) The **MAC data service** is accessed through the **MAC common part sublayer (MCPS-SAP)**,
 - 2) The **MAC management services** are accessed through the **MAC layer management entity (MLME-SAP)**.
- These two services provide an interface between the **SCCS** or another **LLC** and the physical layer accommodate the needs of different applications and network topologies while maintaining a simple protocol.

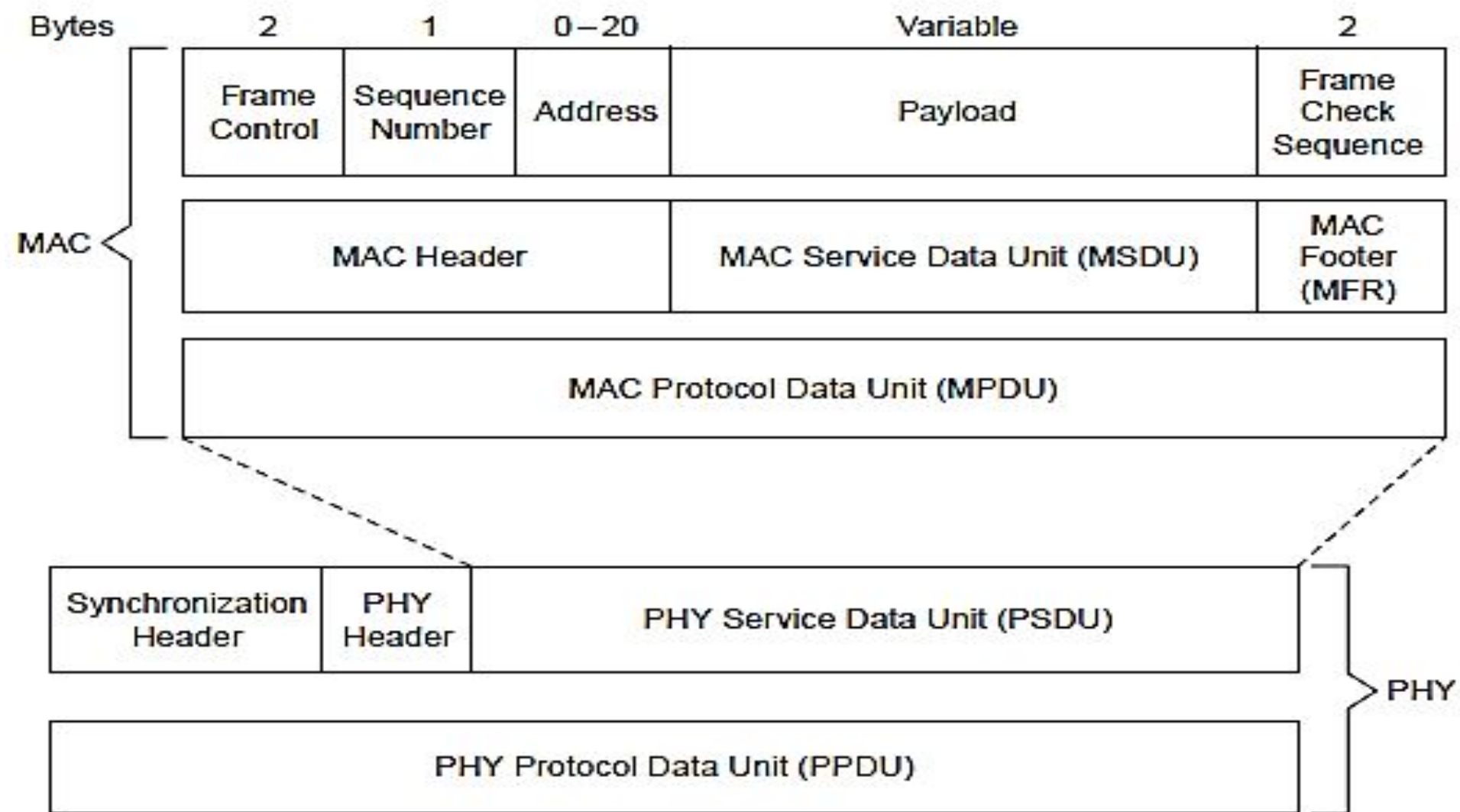


Figure 20.8 General MAC frame format.

□ The MAC protocol data unit (MPDU) consists of the
MAC header (MHR),
MAC service data unit (MSDU), and
MAC footer (MFR).

MAC header

Frame control field-indicates the type of MAC frame being transmitted,
specifies the format of the address field, and
controls the acknowledgment.

□ The frame control field specifies how the rest of the frame looks and what it contains.

Address field: The size of the address field may vary between 0 and 20 bytes.

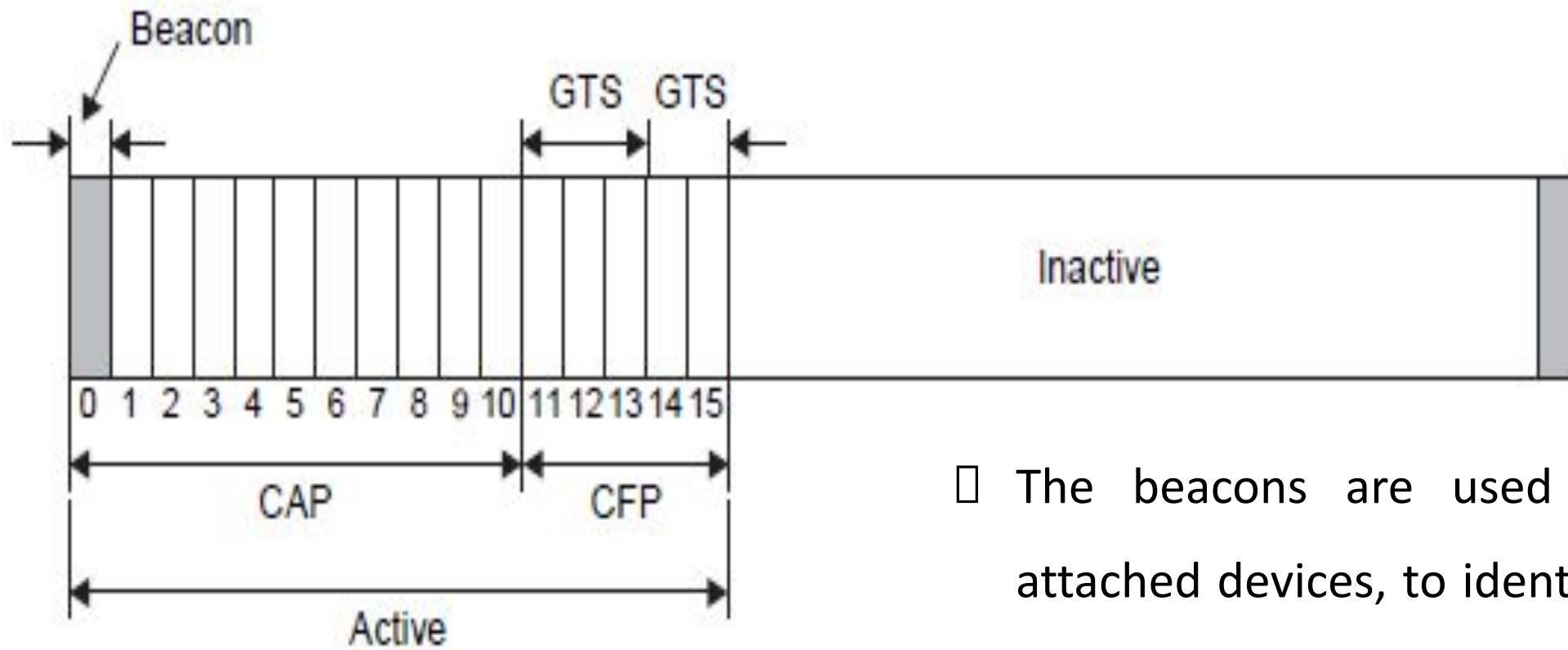
The flexible structure of the address field helps to increase the efficiency of the protocol by keeping the packet shorts.

Payload field

- The payload field is variable in length; however, the **complete MAC frame may not exceed 127 bytes in length**. The data contained in the payload is dependent on the frame type.
- The IEEE 802.15.4 MAC has four different frame types.
 - ✓ Beacon frame,
 - ✓ Data frame,
 - ✓ Acknowledgment frame
 - ✓ MAC command frame
- Only the data and beacon frames actually contain information sent by higher layers; the acknowledgment and MAC command frames originate in the MAC and are used for MAC peer-to-peer communication.

Superframe Structure

- Some applications may require a **dedicated bandwidth to achieve low latencies**.
To accomplish these low latencies, the IEEE 802.15.4 LR-WPAN can operate in an **optional superframe mode**.
- In a superframe (see Figure 20.9), a **dedicated PAN coordinator transmits superframe beacons in predetermined intervals**.
- These intervals can be **as short as 15 ms or as long as 245 seconds**.
- The time between two beacons is divided into 16 equal time slots independent of the duration of the superframe.
- The beacon frame is sent in the first slot of each superframe.



CAP: Contention-access period

CFP: Contention-free period

GTS: Guaranteed time slot

- The beacons are used to synchronize the attached devices, to identify PAN, and describe the structure of superframes.
- A device can transmit at any time during the slot, but must complete its transaction before the next superframe beacon.

Figure 20.9 IEEE 802.15.4 superframe structure.

- The channel access in time slots is contention based;
- however, the PAN coordinator may assign time slots to a single device that requires a dedicated bandwidth or low latency transmissions.
- These assigned time slots are called **guaranteed time slots (GTSs)**
- It form a **contention-free period (CFP)** located immediately before the next beacon.

- The size of the CFP may vary depending on the demand by the associated network devices;
- when guaranteed time slots are used, all devices must complete their contention-based transactions before the CFP begins.
- The beginning of the CFP and duration of the superframe are communicated to the attached network devices by the PAN coordinator.
- The PAN coordinator may allocate up to 7 of the GTSs and a GTS can occupy more than one slot period.

The Network Layer

- The network layer of Zigbee (IEEE 802.15.4) is responsible for topology construction and maintenance as well as naming and binding services, which include the tasks of addressing, routing, and security.
- The network layer should **be self organizing and self-maintaining to minimize energy consumption** and total cost.
- IEEE 802.15.4 supports multiple network topologies, including star, peer-to-peer, and cluster tree .The topology is an application design choice

Routing Protocol

- Routing protocols for ad hoc networks can be divided into two groups: ***table-driven (proactive) and source-initiated on-demand-driven (reactive)***
- The table-driven approach **has low latency and high overhead**, and is more suitable when time constraints are significant.
- The source-initiated on-demand-driven approach has **high latency and low overhead**.

Table-driven (proactive)

- It is more suitable for a mobile environment with a **limited bandwidth capacity**.
- The **table-driven routing protocols attempt to maintain consistent, up-to-date routing information from each node to every node in the network.**
- These protocols require each node to maintain one or more tables to store routing information,
- **The Destination Sequenced Distance Vector (DSDV), Wireless Routing Protocol (WRP), and Cluster Switch Gateway Routing (CSGR) protocol belong to this category**

source-initiated on-demand-driven (reactive)

- The source-initiated on-demand-driven routing protocols create routes **only when desired by a source node**.
- When a node requires a route to a destination, it initiates a **route discovery process** within the network.
- This process is completed once a route is found or all possible route permutations have been examined.

- The Ad hoc On-demand Distance Vector (AODV), Dynamic Source Routing (DSR), Temporally Ordered routing algorithm (TORA), and Cluster Based Routing Protocol (CBRP) belong to this category
- The **AODV** is a **pure on-demand route acquisition algorithm** in which nodes that do not lie on active paths neither maintain nor participate in any periodic routing table exchanges
- The **primary objectives of the algorithm are to broadcast discovery packets only when necessary**

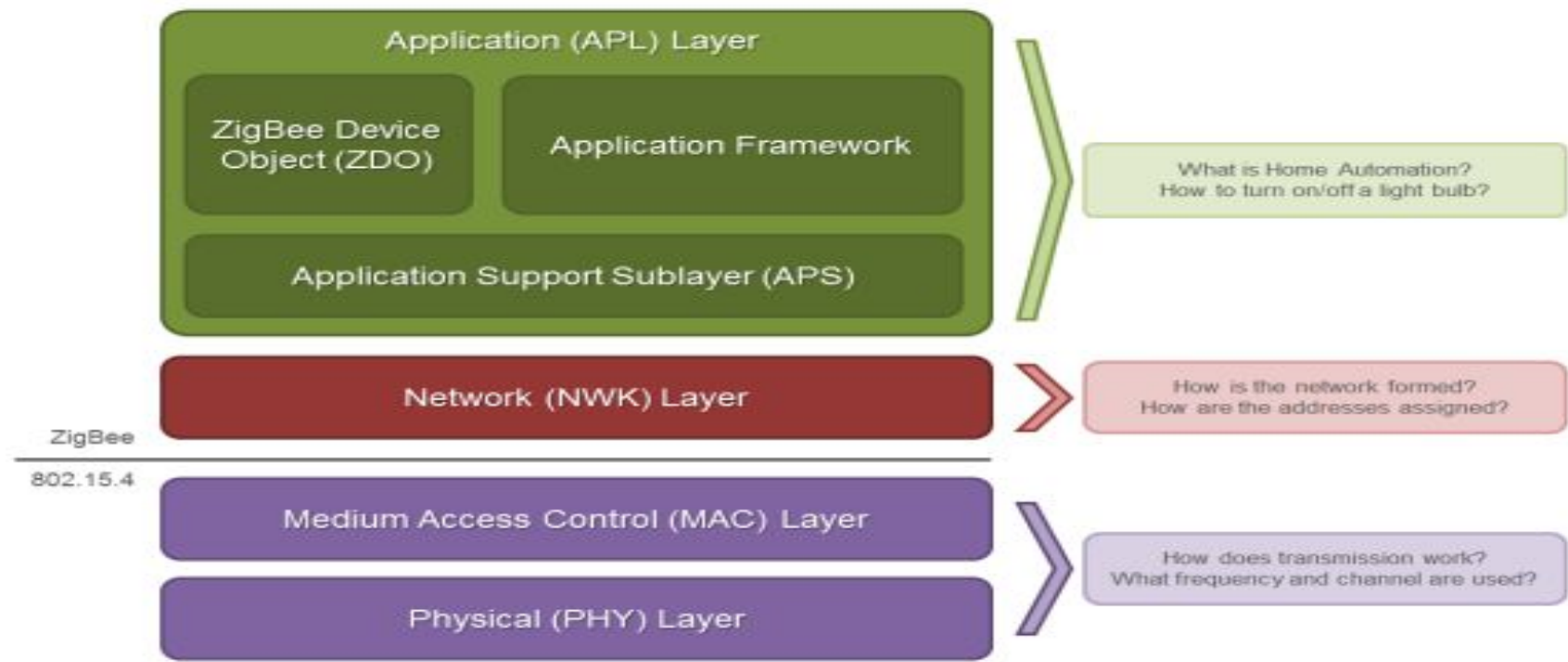
Application Layer:

There are two profiles at this layer.

1. **Manufacturer specific application profile-** Operate as closed systems and also ensure that they can coexist with other zigbee systems.
2. **Public application profile-** for this to work interoperability between various zigbee devices is a must.
 - A single zigbee node supports up to 240 application objects called end points.
 - An end point specifies specific application, for example, 0 dedicated to ZDO (Zigbee device object), provides control and management commands.
 - 6 used for control of light. 8 used for managing heating and air conditioning.

The ZigBee APL layer consists of three sections, shown in below Figure.

the application support (APS) sublayer, ZigBee Device Objects (ZDO), and the application framework. The application support sublayer (APS) provides an interface between the network layer (NWK) and the application layer (APL).

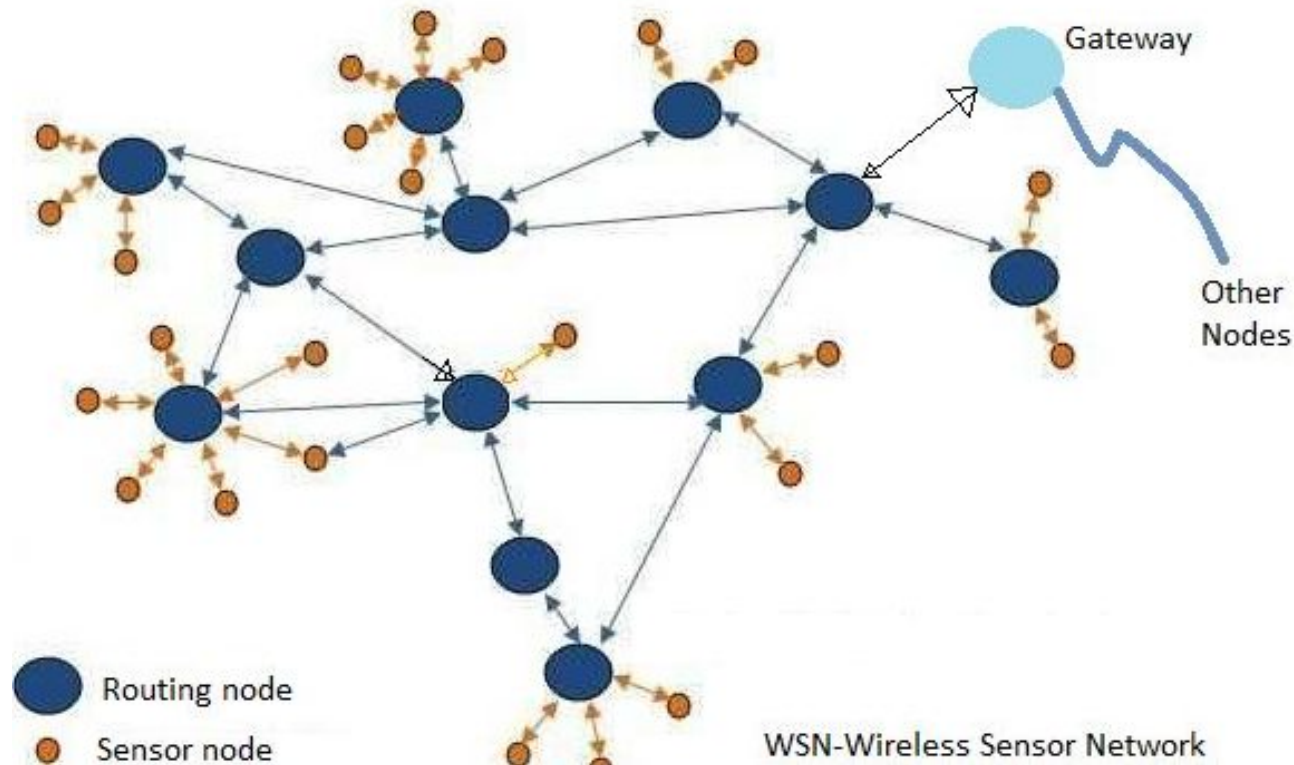


APS (AF)	Application layer that defines various addressing objects including profiles, clusters, and endpoints.
ZDO	Application layer that provides device and service discovery features and advanced network management capabilities.

WSN Wireless sensor Network)

What is WSN?

The WSN (Wireless Sensor Network) consists of end sensor nodes, routing nodes and base station or data collector sink node (or base station or gateway). The WSN should be scalable and secure to deliver efficient and reliable network.



The WSN can be classified based on network type, clustering, communication method, protocol, application usage and coverage.

WSN consists of spatially distributed autonomous sensing devices used to monitor physical or environmental conditions such as temperature, pressure, sound, vibration, motion or pollutants at different locations.

All the nodes communicate wirelessly in WSN and follows various routing protocols.

WSN operates in bandwidth and performance constrained environment. WSNs are self organizing multi-hop ad hoc networks.

Characteristics of Wireless Sensor Networks

- Wireless Sensor Networks mainly consists of **sensors**. **Sensors** are -
 - low power
 - limited memory
 - energy constrained due to their small size.
- Wireless networks can also be deployed in **extreme environmental** conditions and may be prone to enemy attacks.
- Although deployed in an ad hoc manner they need to be **self organized** and **self healing** and can face constant reconfiguration.

- Some of the characteristic features of sensor networks include the following
 - Sensor nodes are densely deployed.
 - Sensor nodes are prone to failures.
 - The topology of a sensor network changes very frequently.
 - Sensor nodes are limited in power, computational capacities, and memory.
 - Sensor nodes may not have global identification because of the large amount of overhead and the large number of sensors.

Benefits or advantages of WSN

Following are the benefits or **advantages of WSN**:

- ➡ It is scalable and hence can accommodate any new nodes or devices at any time.
- ➡ It is flexible and hence open to physical partitions.
- ➡ All the WSN nodes can be accessed through centralized monitoring system.
- ➡ As it is wireless in nature, it does not require wires or cables. Refer difference between [wired network vs wireless network](#)
- ➡ WSNs can be applied on large scale and in various domains such as mines, healthcare, surveillance, agriculture etc.
- ➡ It uses different security algorithms as per underlying wireless technologies and hence provide reliable network for consumers or users.

Drawbacks or disadvantages of WSN

Following are the drawbacks or **disadvantages of WSN**:

- ➡ As it is wireless in nature, it is prone to hacking by hackers.
- ➡ It can not be used for high speed communication as it is designed for low speed applications.
- ➡ It is expensive to build such network and hence can not be affordable by all.
- ➡ There are various challenges to be considered in WSN such as energy efficiency, limited bandwidth, node costs, deployment model, Software/hardware design constraints and so on.
- ➡ In star topology based WSN, failure of central node leads to whole network shutdown.

Challenges in WSN

A modern Wireless Sensor Network (WSN) faces several challenges, including:

- **Limited power and energy:** WSNs are typically composed of battery-powered sensors that have limited energy resources. This makes it challenging to ensure that the network can function for long periods of time without the need for frequent battery replacements.
- **Limited processing and storage capabilities:** Sensor nodes in a WSN are typically small and have limited processing and storage capabilities. This makes it difficult to perform complex tasks or store large amounts of data.
- **Heterogeneity:** WSNs often consist of a variety of different sensor types and nodes with different capabilities. This makes it challenging to ensure that the network can function effectively and efficiently.
- **Security:** WSNs are vulnerable to various types of attacks, such as eavesdropping, jamming, and spoofing. Ensuring the security of the network and the data it collects is a major challenge.

- **Scalability**: WSNs often need to be able to support a large number of sensor nodes and handle large amounts of data. Ensuring that the network can scale to meet these demands is a significant challenge.
- **Interference**: WSNs are often deployed in environments where there is a lot of interference from other wireless devices. This can make it difficult to ensure reliable communication between sensor nodes.
- **Reliability**: WSNs are often used in critical applications, such as monitoring the environment or controlling industrial processes. Ensuring that the network is reliable and able to function correctly in all conditions is a major challenge.

Challenges in sensor networks

- Energy constraint : Nodes are battery powered
- Unreliable communication : Radio broadcast, limited bandwidth, bursty traffic
- Unreliable sensors : False positives
- Ad hoc deployment : Pre-configuration inapplicable
- Large scale networks : Algorithms should scale well
- Limited computation power : Centralized algorithms inapplicable
: Difficult to debug & get it right
- Distributed execution

Operational Challenges of Wireless Sensor Networks

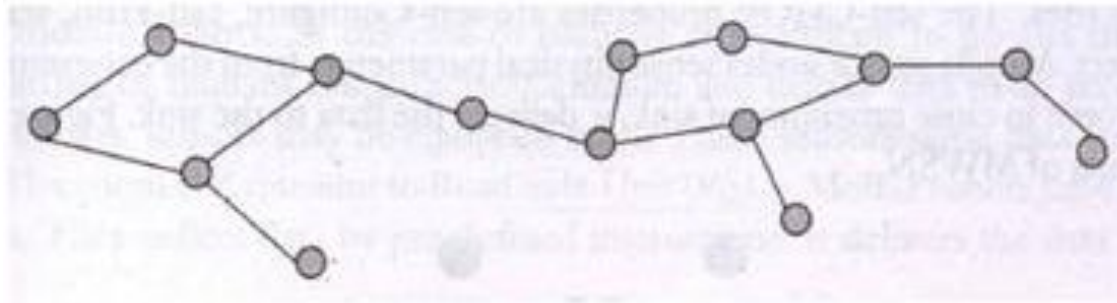
- Energy Efficiency
- Limited storage and computation
- Low bandwidth and high error rates
- Errors are common
 - Wireless communication
 - Noisy measurements
 - Node failure are expected
- Scalability to a large number of sensor nodes
- Survivability in harsh environments
- Experiments are time- and space-intensive

Factors Influencing WSN Design

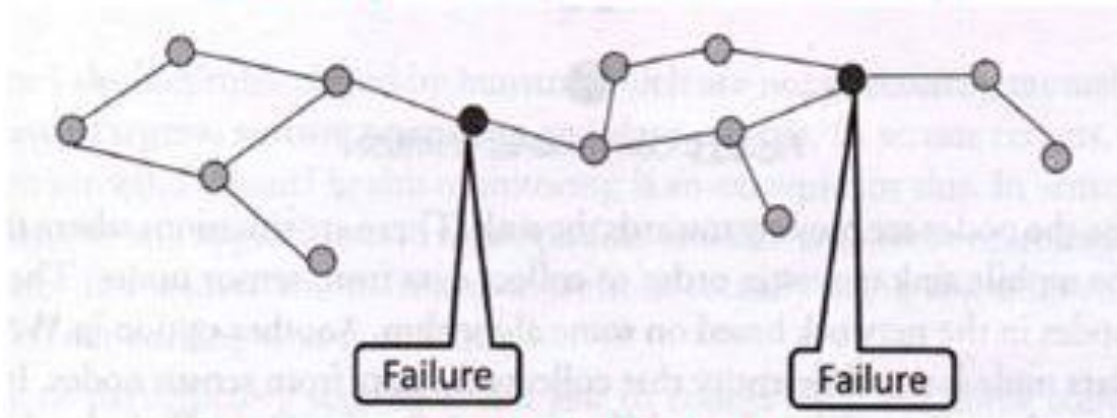
- Fault tolerance
- Scalability
- Production costs
- Hardware constraints
- Sensor network topology
- Environment
- Transmission media
- Power Consumption
 - Sensing
 - Communication
 - Data processing

- The following are important issues pertaining to WSNs:
 - ✓ sensor **t**ype;
 - ✓ sensor **p**lacement;
 - ✓ sensor **p**ower consumption,
 - ✓ **o**perating **e**nvironment,
 - ✓ **c**apabilities and signal **p**rocessing,
 - ✓ **c**onnectivity, and telemetry or **c**ontrol of remote devices.
- It is critical to note that node location and **fine-grained time (stamping)** are essential for proper operation of a sensor network.

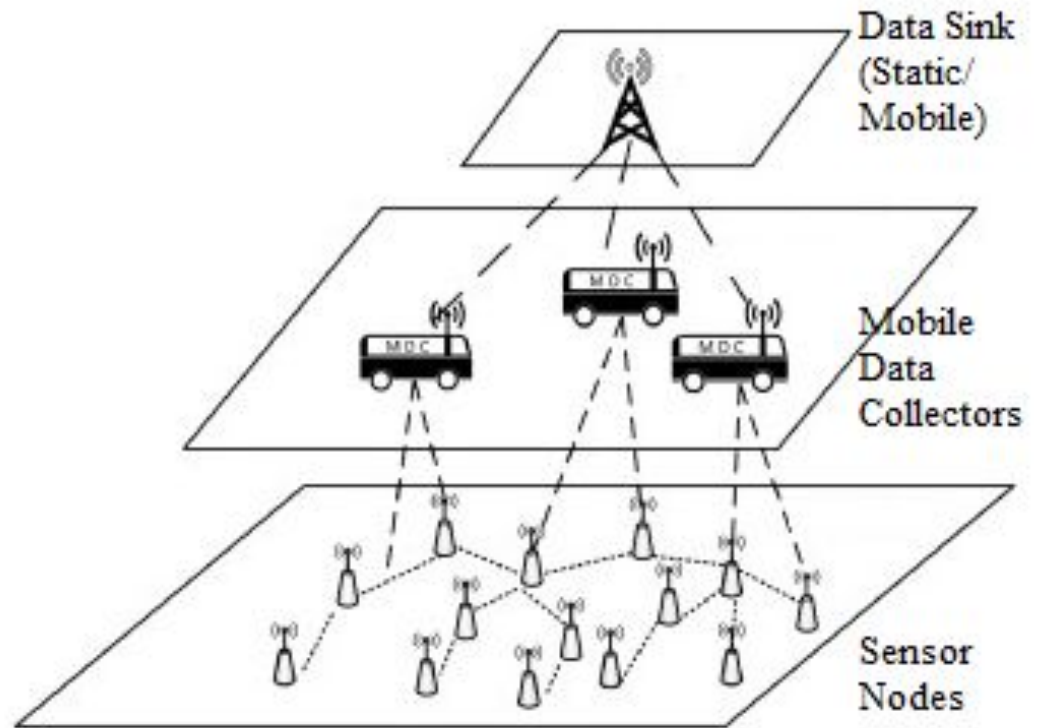
Types of Wireless Sensor Networks



Stationary WSN (Without Node failure)

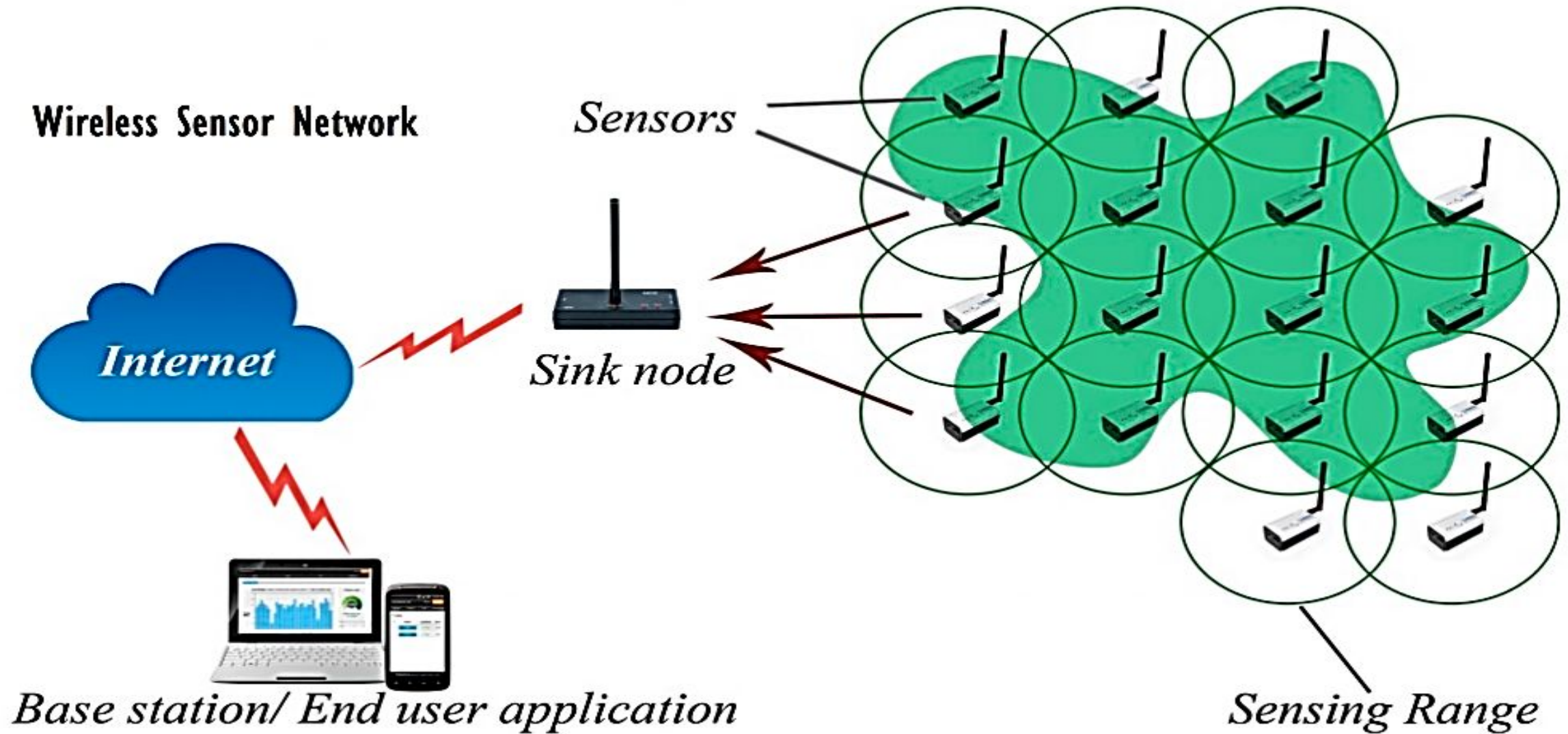


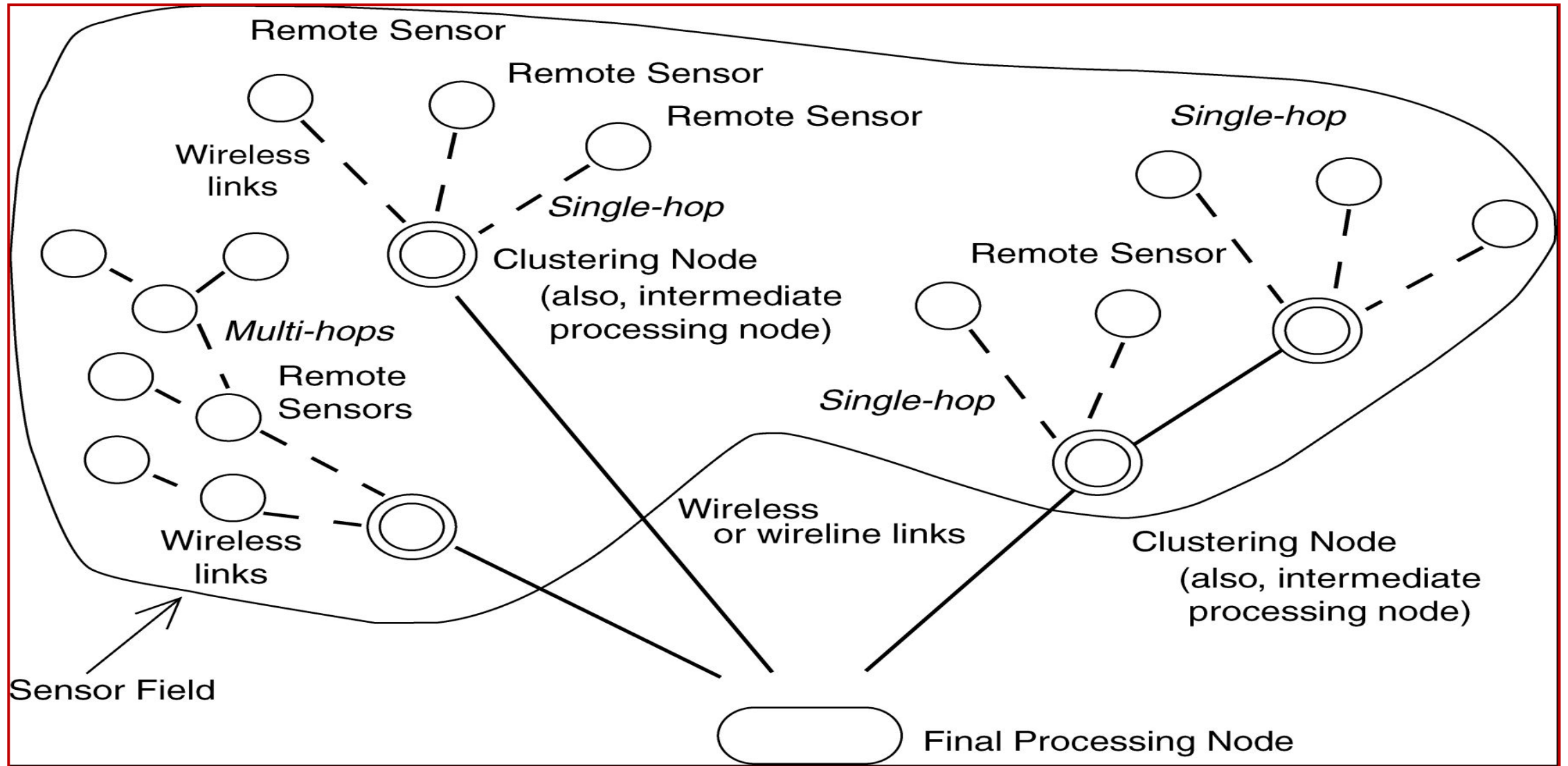
Stationary WSN (Node failure)



Mobile WSN Architecture

Wireless Sensor Network Architecture





Typical sensor network arrangement

- Sensor networks require sensing systems that are long-lived and environmentally resilient.
- Unattended, untethered, self-powered low-duty-cycle systems are typical.
- In most instances, communication circuitry and antennas are the primary elements that draw most of the energy.
- Sensors are either passive or active devices. Passive sensors in element form include seismic-, acoustic-, strain-, humidity-, and temperature-measuring devices.
- Passive sensors tend to be low-energy devices.
- Active sensors include radar and sonar; these tend to be high-energy systems

Architecture for a WSN

Special addressing requirement

- Local unique addresses
- Data-centric
- *Example: Each node has an unique number.*

Attribute-based naming architecture

- Data is named by one or more attributes.
- *Example: Each node is distinguished by an attribute – GPS sensors are practical for this.*

Components of WSN:

1.Sensor node:

Sensors in WSN are used to capture the environmental variables and which is used for data acquisition. Sensor signals are converted into electrical signals.

2.Radio Nodes:

It is used to receive the data produced by the Sensors and sends it to the WLAN access point. It consists of a microcontroller, transceiver, external memory, and power source.

3.WLAN Access Point:

It receives the data which is sent by the Radio nodes wirelessly, generally through the internet.

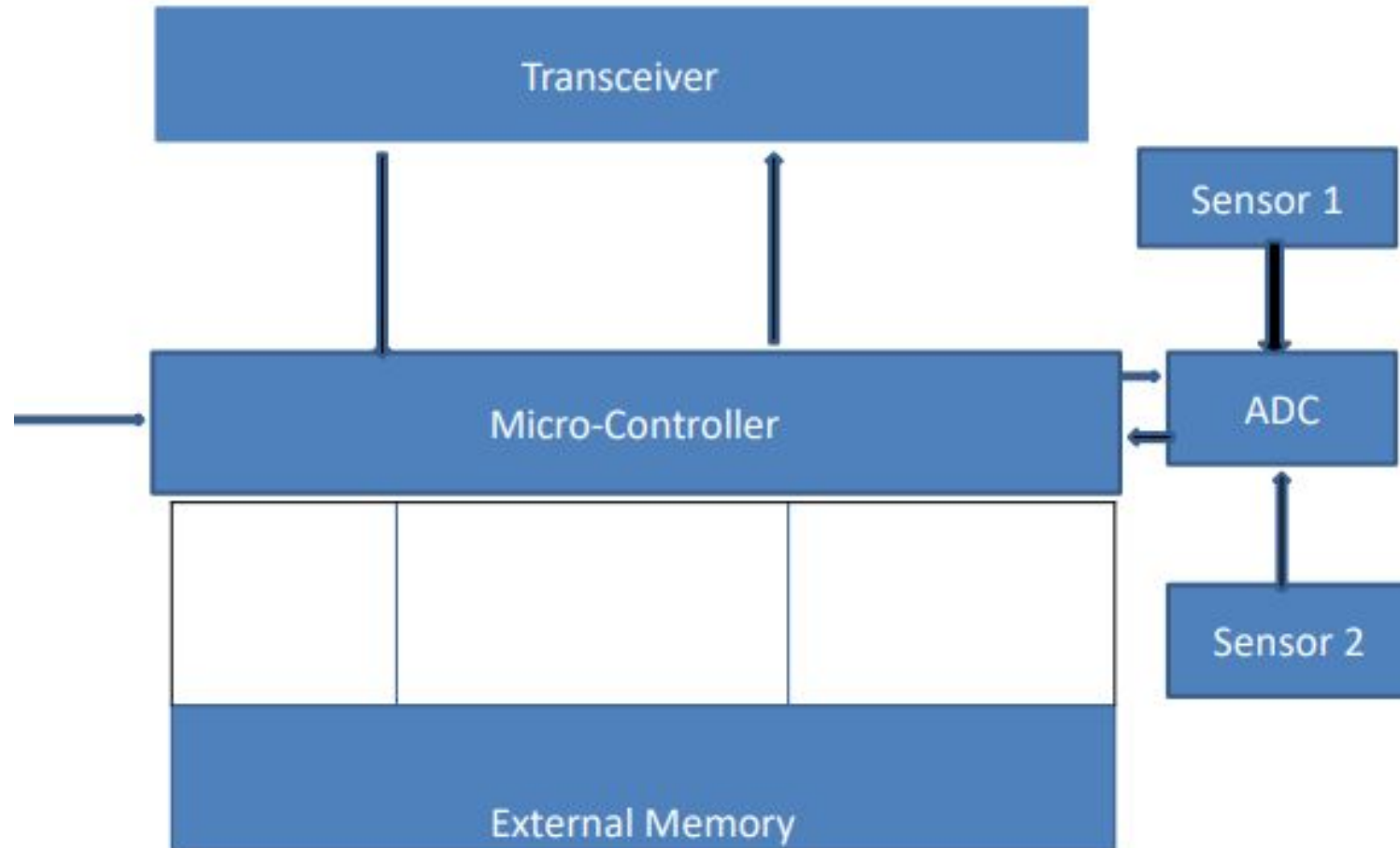
4.Evaluation Software:

The data received by the WLAN Access Point is processed by a software called as Evaluation Software for presenting the report to the users for further processing of the data which can be used for processing, analysis, storage, and mining of the data.

Wireless Sensor Node

- **sensor**
 - A transducer
 - converts physical phenomenon e.g. heat, light, motion, vibration, and sound into electrical signals
- **sensor node**
 - basic unit in sensor network
 - contains on-board sensors, processor, memory, transceiver, and power supply
- **sensor network**
 - consists of a large number of sensor nodes
 - nodes deployed either inside or very close to the sensed phenomenon

Architecture of Sensor Node



Applications of Wireless Sensor networks

The applications can be divided in three categories:

1. Monitoring of objects.
2. Monitoring of an area.
3. Monitoring of both area and objects.

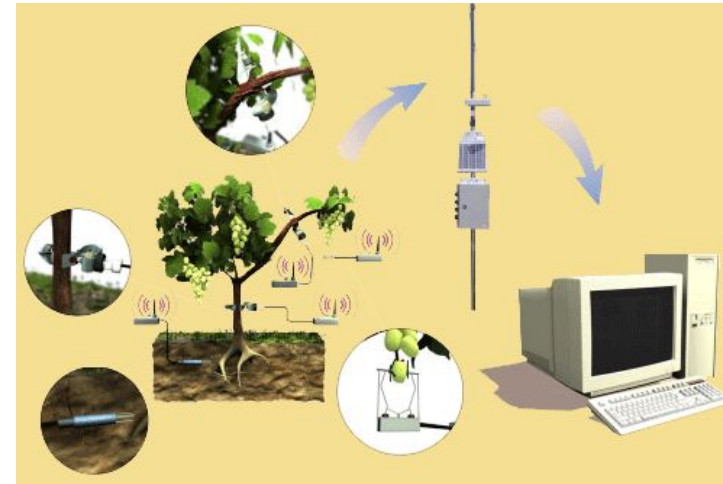
** Classification due to Culler, Estrin, Srivastava*

Monitoring Area

- Environmental and Habitat Monitoring
- Precision Agriculture
- Indoor Climate Control
- Military Surveillance
- Treaty Verification
- Intelligent Alarms

Example: Precision Agriculture

- Precision agriculture aims at making cultural operations more efficient, while reducing environmental impact.
- The information collected from sensors is used to evaluate optimum sowing density, estimate fertilizers and other inputs needs, and to more accurately predict crop yields.



Monitoring Objects

- Structural Monitoring
- Eco-physiology
- Condition-based Maintenance
- Medical Diagnostics
- Urban terrain mapping

Example: Condition-based Maintenance

- Intel fabrication plants
 - Sensors collect vibration data, monitor wear and tear; report data in real-time
 - Reduces need for a team of engineers; cutting costs by several orders of magnitude

Monitoring Interactions between Objects and Space

- Wildlife Habitats
- Disaster Management
- Emergency Response
- Ubiquitous Computing
- Asset Tracking
- Health Care
- Manufacturing Process Flows

Example: Habitat Monitoring

- The ZebraNet Project

Collar-mounted sensors monitor zebra movement in Kenya



Source: Margaret Martonosi, Princeton University

Future of WSN

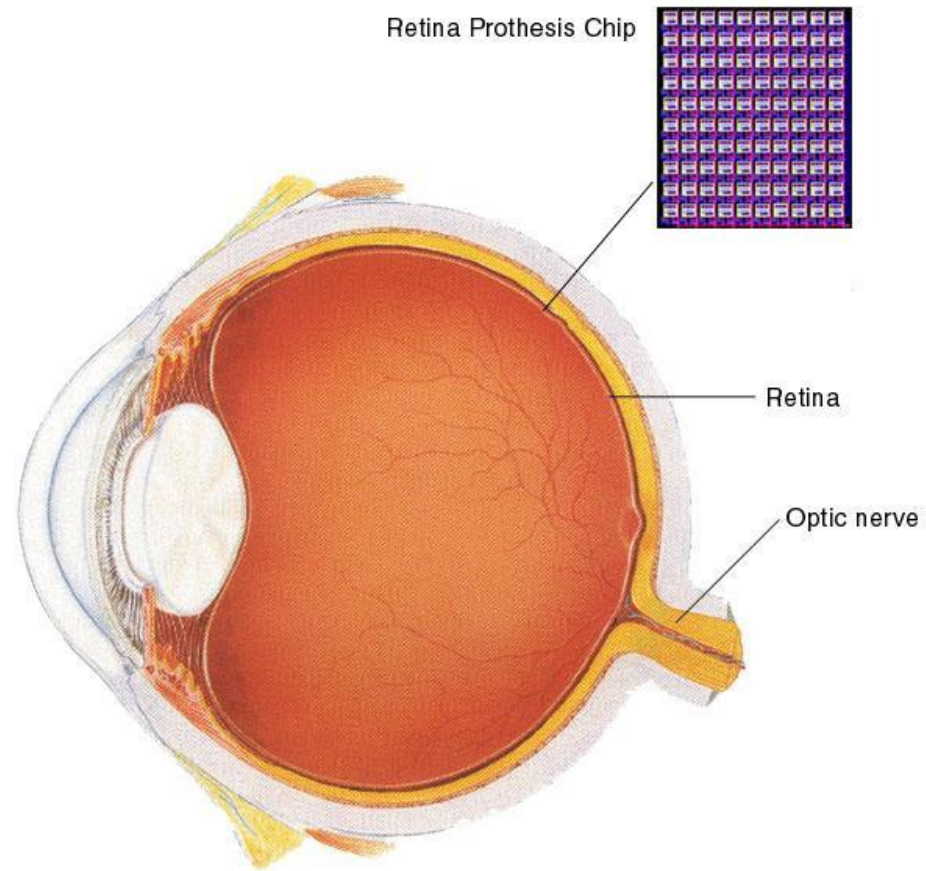
Smart Home / Smart Office



- Sensors controlling appliances and electrical devices in the house.
- Better lighting and heating in office buildings.
- The Pentagon building has used sensors extensively.

Biomedical / Medical

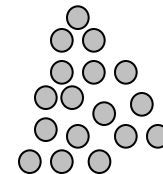
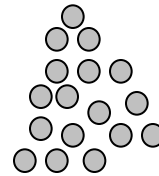
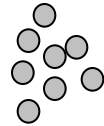
- Health Monitors
 - Glucose
 - Heart rate
 - Cancer detection
- Chronic Diseases
 - Artificial retina
 - Cochlear implants
- Hospital Sensors
 - Monitor vital signs
 - Record anomalies



Military

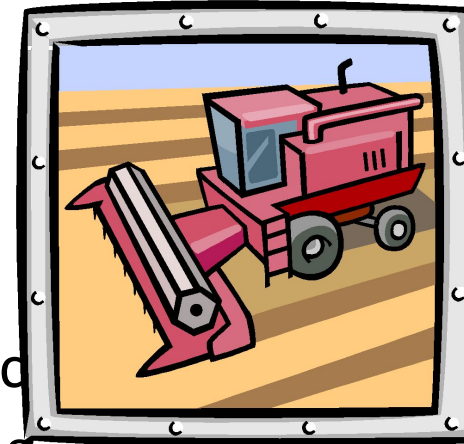


Remote deployment of
sensors for **tactical monitoring**
of enemy troop movements.



Industrial & Commercial

- Numerous industrial and commercial applications:
 - Agricultural Crop Conditions
 - Inventory Tracking
 - In-Process Parts Tracking
 - Automated Problem Reporting
 - RFID – Theft Deterrent and Customer Tracking
 - Plant Equipment Maintenance Monitoring



Traffic Management & Monitoring

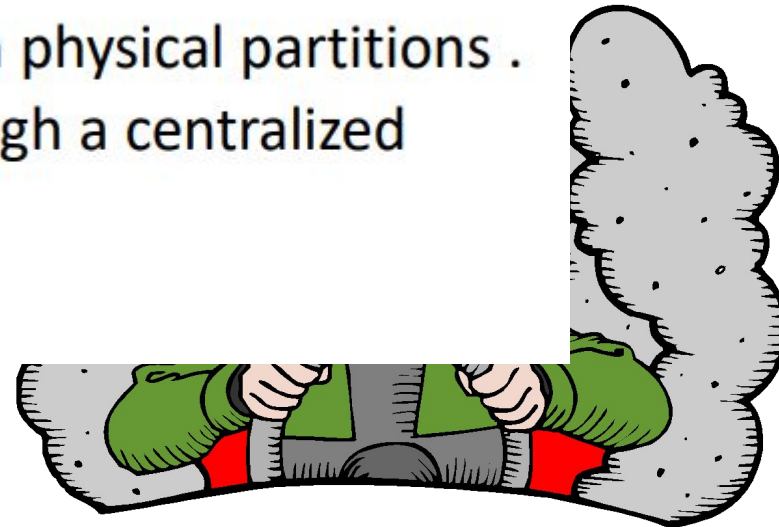
Advantages

- It avoids a lot of wiring .
- It can accommodate new devices at any time .
- It's flexible to go through physical partitions .
- It can be accessed through a centralized monitor

✓ See the

- Monitor traffic flows
- Provide real-time route updates

use
to:
ts



Disadvantages

- Lower speed compared to wired network.
- Less secure because hacker's laptop can act as Access Point. If you connected to their laptop, they'll read all your information (username, password.. etc).
- More complex to configure than wired network. ➤
Gets distracted by various elements like Blue-tooth . ➤
Still Costly at large.
- It does not make sensing quantities in buildings easier.
- It does not reduce costs for installation of sensors. ➤
It does not allow us to do more than can be done with a wired system

Wireless Sensor Network(WSN) vs. Mobile Ad Hoc Network (MANET)

	WSN	MANET
Similarity	Wireless	Multi-hop networking
Security	Symmetric Key Cryptography	Public Key Cryptography
Routing	Support specialized traffic pattern. Cannot afford to have too many node states and packet overhead	Support any node pairs Some source routing and distance vector protocol incur heavy control traffic
Resource	Tighter resources (power, processor speed, bandwidth)	Not as tight.