CHAPTER 19

# Wireless Personal Area Network—Bluetooth

## 19.1 Introduction

Several technical committees of IEEE are responsible for developing standards of the local area network (LAN), wireless local area network (WLAN), and wireless personal area network (WPAN). Table 19.1 summarizes them to familiarize the readers.

In a WPAN, the residence is connected to a public switched telephone network (PSTN) for telephone services, Internet for web access, and cable network for multichannel television services. In this chapter, we first introduce the concept of WPAN and discuss the roles of the IEEE 802.15[6] committee. We then provide details of Bluetooth wireless technology[1,3–5].

Bluetooth enables users to connect a wide range of computing and telecommunication devices without any additional or proprietary cables. Ultrawide band (UWB-IEEE 802.15.3a) is the IEEE standard for a high-data-rate WPAN designed to provide sufficient quality of service for real-time distribution of content such

**Table 19.1 IEEE 802 working groups.**

| | Working group |
|---|---|
| 802.1 | Higher Layer LAN Protocol |
| 802.2 | Logical Link Control (LLC) |
| 802.3 | Ethernet |
| 802.11 | WLAN |
| 802.15 | WPAN |
| 802.16 | Broadband Wireless Access (BWA) |
| 802.17 | Resilient Packet Ring |
| 802.18 | Radio Regulatory TAG |
| 802.20 | Mobile Broadband Wireless Access (MBWA) |
| Link Security | Executive Committee Study Group |
| 802 Handoff | Executive Committee Study Group |

as video and music. It is ideally suited for a home multimedia wireless network. We will discuss UWB in Chapter 22.

The Bluetooth wireless specification includes RF, link layer, and application layer definitions for product developers for data, voice, and content-centric applications. The specification contains the information necessary to ensure that diverse devices supporting Bluetooth wireless technology can communicate with each other worldwide.

## 19.2 The Wireless Personal Area Network

Within the home, computers and printers are connected to the Internet through voice band modems, XDSL services, or cable modems. The number of home networks in the United States is expected to almost double each year. The industry has two distinct segments—home access and home distribution. Home access technology uses different wireless and wired alternatives to secure a broadband Internet access to the home gateway to be distributed to the user's information appliances. The home distribution or WPAN interconnects all home appliances and connects them to the Internet through a home gateway. It is expected that more than 80% of U.S. households will have a broadband data access by the year 2008+.

The WPAN provides an infrastructure to interconnect a variety of home appliances and enables them to access the Internet through a central home gateway. Home computing equipment used for computing and Internet transaction interface access includes PCs, laptops, printers, scanners, and web cameras. A home computing network allows multiple computers as well as multiple devices to connect with a network protocol.

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, cell phones, 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. Many cell phones already have two radio interfaces—one for the cellular network and the other for PAN connections.

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. However, many control and command applications require much lower data rates and also the lowest possible cost, thus ZigBee. At this time most WPAN applications target cable replacements (e.g., Bluetooth headsets) but these technologies are capable of forming elegant peer-to-peer networks, offering more enhanced application capabilities such as sensor networks and so on (see Chapter 22).

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 such as PCs, PDAs, cell phones, printers, speakers, microphones, and other consumer electronics. IEEE 802.15.1 and 802.15.4 focus on the devices with the following characteristics:

- Power management: low current consumption
- Range: 0–10 m
- Rate: 19.2–100 kbps
- Size: 0.5 $in^3$ 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

The IEEE 802.15 committee consists of the following task groups (see Figure 19.1):

- **Task group I:** It is for Bluetooth and defines physical (PHY) and medium access control (MAC) specifications for wireless connectivity with fixed, portable, and moving devices within or entering a personal operating space (POS). A POS is the space around a person or object that typically extends up to 10 m in all directions and envelops the person whether stationary or in motion.
- **Task group II:** It focuses on the coexistence of WPAN and IEEE 802.11 WLANs. The goal of the WPAN group is to achieve a level of interoperability that allows the data transfer between a WPAN device and an IEEE 802.11 device.
- **Task group III:** It works on PHY and MAC layers for high-rate WPANs that operate at a data rate of more than 20 Mbps, and will provide for

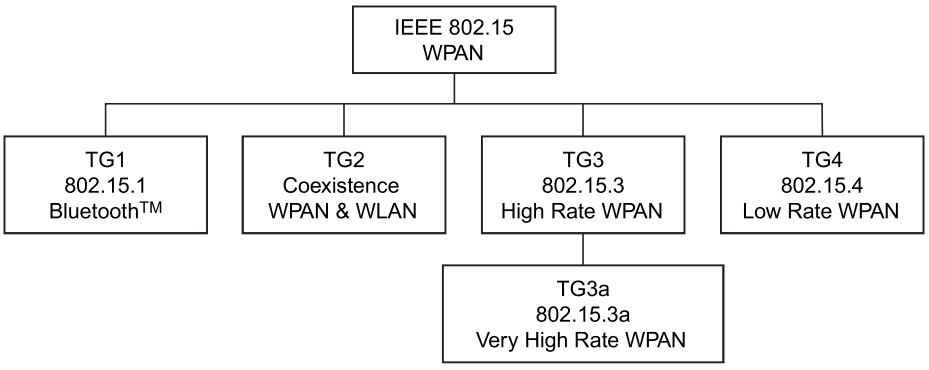



**Figure 19.1 IEEE 802.15 task groups.**

low-power, low-cost solutions to address the needs of portable consumer digital imaging and multimedia applications. The standards aim at providing compatibility with Bluetooth specifications.

- **Task group IV:** It investigates an ultra-low complexity, ultra-low power consuming, ultra-low-cost PHY and MAC layer for data rates of up to 200 kbps. Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation.

## 19.3 Bluetooth (IEEE 802.15.1)

In 1994, the Swedish telecommunication company Ericsson decided to honor old, weird Herald I. Bluetooth, king of Denmark between 940 and 985 AD, by naming its new wireless networking standard after him. Table 19.2 outlines the evolution of Bluetooth technology.

Bluetooth provides short-range, low-cost (<$10 per device) connectivity between portable devices. Bluetooth is limited in range (<10 meters) and bandwidth (780 kbps compared to Home RF that goes to 1–2 Mbps and IEEE 802.11b that goes to 11 Mbps with 150 m and greater distance).

Bluetooth radio characteristics [8–10] include low power, short range, and medium transmission speed. The low power consumption makes Bluetooth ideal for small, battery-powered devices like mobile phones and pocket PCs. Bluetooth is poised to capitalize on the emerging market of small mobile devices that is expected to grow. Bluetooth's short range (<10 m) is ideal for the concept of "personal operating space" and integrates the notion of using a device carried or worn on the body or otherwise located within immediate reach. Bluetooth's transmission speed of 780 kbps works well for transferring small to medium-sized files.

Bluetooth enables users to connect a wide range of computing and telecommunication devices easily and simply, without the need to buy additional or proprietary cables. The cable solution is complicated since it may require a cable specific to the device that is being connected. The infrared solution eliminates the cable, but requires line of sight. To solve all these problems the Bluetooth standard has been developed.

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

**Table 19.2 Evolution of Bluetooth technology.**

| | |
|---|---|
| 1998 | Special Interest Group (SIG)[2] was formed including 3Com, Ericsson, IBM, Intel, Lucent, Microsoft, Motorola, Nokia, and Toshiba. |
| 1999 | The first open Bluetooth specification 1.0 released. |
| 2000 | The first certified Bluetooth products on market. |
| 2001 | The latest protocol 1.1 released. |

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.

A WPAN can be formed with a Bluetooth-enabled pocket PC to dial into an ISP and access the Internet. After downloading a file, you could walk within 10 m of a Bluetooth-enabled printer and send the file from the pocket PC to the printer to have it printed. These examples show how Bluetooth can eliminate the need for a cable to the phone or printer.

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. Because it can be done spontaneously according to immediate need, it is known as *ad hoc networking*. Because a WPAN involves directly networking between different points, without the use of network infrastructure, it is also referred to as a "point-to-point network" [7,11,12].

The Bluetooth market focuses on four categories of users: professional and field workers who need to travel off-site but still require access to corporate communications and information; technology-savvy electronic consumers; industrial and retail workers involved in automated processes where cables can get in the way; and office workers whose worksites are outfitted with Bluetooth devices.

Bluetooth is an ideal solution for connecting the increasing number of devices designed to be held in the hand or worn on the body. These devices are being embraced by industries using mobile automation systems. For example, at a car rental facility, an employee could use a Bluetooth-enabled pocket PC equipped with a bar code scanner to scan a vehicle identification number, enter mileage and fuel data, then instantly transmit a receipt to a Bluetooth-enabled portable printer worn on the hip. Because of the GSM subscriber identity module (SIM), industry experts foresee Bluetooth-enabled GSM phones to be used like credit cards. For example, one could use the Bluetooth-enabled mobile phone at a Bluetooth-enabled vending machine to charge one's account and buy a drink.

One of Bluetooth's greatest advantages is that it can be used absolutely anywhere that at least two Bluetooth devices share a 10-m range. It is possible because Bluetooth is designed for direct point-to-point networking between devices and does not require proximity to infrastructure stations like signal towers or access points.

Bluetooth radio technology provides a universal bridge to existing data networks, a peripheral interface, and a mechanism to form small private ad hoc groupings of connected devices away from fixed network infrastructures. Bluetooth radio uses a fast acknowledgment and frequency hopping scheme to make the link robust. Bluetooth typically 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. Use of a forward error correction (FEC) scheme limits the

**Table 19.3 Bluetooth air interface details.**

| Feature | Values | Notes |
|---|---|---|
| Frequency range: | | |
| • USA, Europe, and most other countries | 2.4–2.4835 GHz | 79 RF channels |
| • Spain | 2.445–2.475 GHz | 23 RF channels |
| • France | 2.4465–2.4835 GHz | 23 RF channels |
| Bandwidth of each RF channel | 1 MHz | |
| Gross data rate | 1 Mbps (initial)<br>2 Mbps (latter) | |
| Time slot duration | 626 μs | Time division multiplexing (TDM) is used to divide the channel into time slots. Transmission occurs in packets that occupy an odd number of slots (up to 5). |
| One-to-one connection allowable maximum data rate | 721 kbps | 3 voice channels |
| Signal modulation | Gaussian frequency shift keying (GFSK) | |
| Piconet access | | FH-TDD-TDMA |
| Scatternet access | | FH-CDMA |
| Frequency hopping rate | 1600 hops/second | |
| Range | 10 meters | |

impact of random noise on long-distance links. Table 19.3 lists the parameters of Bluetooth air interface.

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 now has a formalized standards development in process for Bluetooth known as 802.15.1. The IEEE is also exploring the enhancement of 802.15.1 with a high data rate Bluetooth standard: 802.15.3.

Transmitter equipment is classified into three power classes (see Table 19.4). A power control is required for power class 1 equipment, whereas power controls for power class 2 and 3 equipment is optional. The power control is used for limiting the transmitted power over 0 dBm. Power control capability under 0 dBm is optional and could be used for optimizing the power consumption and overall interference level. The power steps form a monotonic sequence, with a maximum step size of 8 dB and a minimum step size of 2 dB. Class 1 equipment with a maximum transmit power of 20 dBm must be able to control its transmit power down to 4 dBm or less. Equipment with power control capability optimizes the output power in a link.

**Table 19.4 Bluetooth transmitter characteristics.**

| Power class | Maximum output power (Pmax) | Nominal output power | Minimum output power* | Power control |
|---|---|---|---|---|
| 1 | 100 mW (20 dBm) | N/A | 1 mW (0 dBm) | Pmin <4 dBm to Pmax<br>Optional: Pmin** to Pmax |
| 2 | 2.5 mW (4 dBm) | 1 mW (0 dBm) | 0.25 mW (−6 dBm) | Optional: Pmin** to Pmax |
| 3 | 1 mW (0 dBm) | N/A | N/A | Optional: Pmin** to Pmax |

* Minimum output power at maximum power setting.

** The lower power limit Pmin <−30 dBm is suggested but it is not mandatory, and may be chosen according to application needs.

The actual sensitivity level is defined as an input level for which a raw bit error rate (BER) of 0.1% is met. The requirement for a Bluetooth receiver is an actual sensitivity level of −70 dBm or better. The receiver must achieve a −70 dBm sensitivity level with any Bluetooth transmitter compliant to the transmitter specification given in Table 19.4.

## 19.4 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. All Bluetooth devices are peer units and have identical implementations. However, when establishing 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.
- **Scatternet.** Two or more independent and nonsynchronized 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).
- **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.

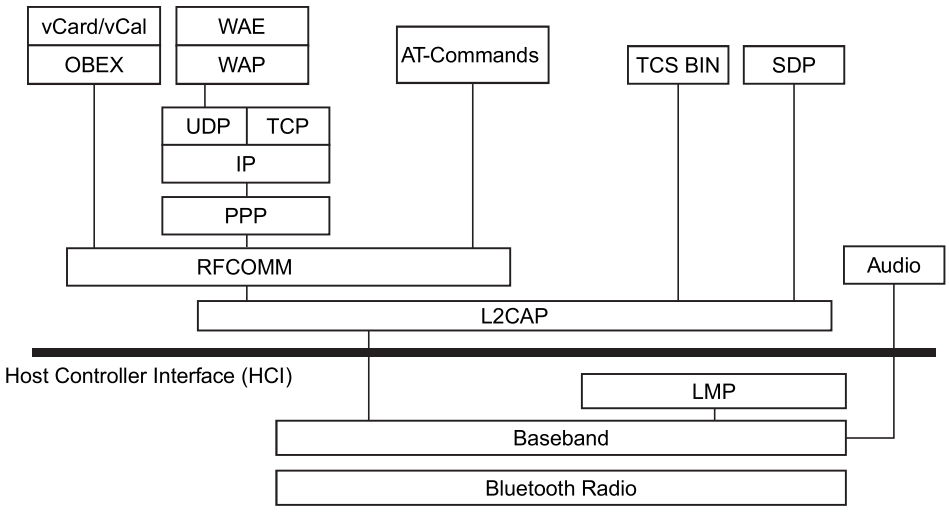



**Figure 19.2 Bluetooth protocol stack.**

## 19.5 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, and application group (see Figure 19.2).

### 19.5.1 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.

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, and host controller interface (HCI).

- **Logical link control and adaptation protocol (L2CAP) layer.** All data traffic is routed through the logical link control and adaptation protocol layer. This layer shields the higher layers from the details of the lower layers. The

higher layers need not be aware of the frequency hops occurring at the radio and baseband level. 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 in two peer devices facilitates the maintenance of the desired grade of service. 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.

- **Link manager layer (LML).** The link manager layers in communicating devices 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. This is an important step in establishing a communication between two devices. If this fails, the communication link may get severed. The link managers are also responsible for power control and may request adjustments in power levels.
- **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. This layer also manages the links between the devices and is responsible for determining the packet types supported for synchronous and asynchronous traffic.
- **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. Higher layers are informed of certain events through the HCI. The HCI is not a required part of the specification. It has been developed to serve the purpose of interoperability between host devices and Bluetooth modules. Bluetooth product implementation need not be HCI compliant to support a fully compliant Bluetooth air interface.

### 19.5.2 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)[2] for Bluetooth wireless communication. The protocols in this

group can include TCP, IP, PPP, etc. A serial port emulator protocol, RFCOMM, enables applications that normally would interface with a serial port to operate with Bluetooth links. A packet-based telephony control protocol for advanced telephony operations is also present. This group has a service discovery protocol (SDP), which lets devices discover each other's services.

- **RFCOMM layer.** Serial ports are the most common communication interface in use today. These serial ports invariably involve the use of cable. 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.
- **Infrared data association (IrDA) interoperability protocols.** The SIG has adopted some IrDA protocols to ensure interoperability between applications. IrDA and Bluetooth share some important attributes. The Infrared Object Exchange Protocol is designed to enable units supporting infrared communication to exchange a wide variety of data and comments.
- **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. In addition, the OBEX protocol defines a folder-listing object, which is used to browse the contents of folders on a remote device.
- **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. AT commands over RFCOMM are used for some applications. Audio traffic is treated separately in Bluetooth. Audio traffic is isochronous, 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 or continuous variable slope delta modulation.

### 19.5.3 Application Group

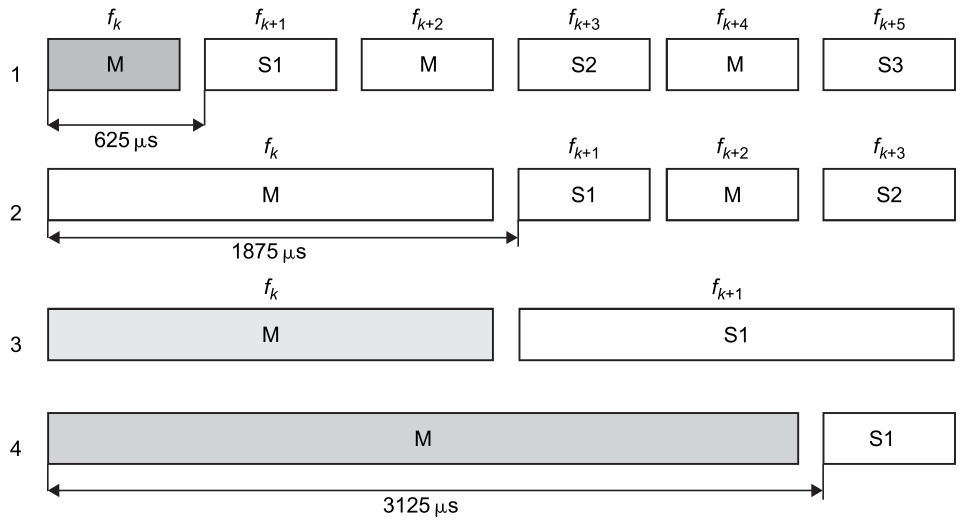
This group consists of actual applications that make use of Bluetooth links and refers to the software that exists above the protocol stack. The software uses the protocol stack to provide some function to the user of the Bluetooth devices. The most interesting applications are those that substantiate the Bluetooth profiles. 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.

## 19.6 Bluetooth Link Types

The Bluetooth baseband technology supports two link types: a synchronous connection oriented (SCO) type (used primarily for voice) and an 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. 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 circuit-switched, point-to-point connections and is used often for voice traffic. The data rate for SCO links is 64 kbps.




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

**Figure 19.3 Bluetooth packets.**

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. Figure 19.3 shows the Bluetooth packets and Table 19.5 provides the details.

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. 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.

**Table 19.5 Bluetooth packet types.**

| 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 64 kbps voice, no FEC encoding |
| 0110 | SCO | HV2 | 1 | Carries 160 bits for user voice samples and 80 bits of parity for $^1/_3$ FEC encoding |
| 0111 | SCO | HV3 | 1 | Carries 80 bits for user voice samples and 160 bits of parity for $^2/_3$ FEC encoding |
| 1000 | SCO | DV | 1 | Combined data (150 bits) and voice (50 bits) packet data field, $^2/_3$ 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, $^2/_3$ 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, $^2/_3$ FEC encoded |
| 1111 | ACL | DH5 | 5 | Carries 341 information bytes + 16-bit CRC, not FEC encoded |

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. Table 19.6 lists the ACL packet types and their data rates.

**Table 19.6 ACL packet types and data rates.**

| | | Asymmetric (kbps) | |
|---|---|---|---|
| **Link** | **Symmetric (kbps)** | **Master** | **Slave** |
| DM1 | 108.8 | 108.8 | 108.8 |
| DH1 | 172.8 | 172.8 | 172.8 |
| DM3 | 256 | 384 | 54.4 |
| DH3 | 384 | 576 | 86.4 |
| DM5 | 286.7 | 477.8 | 36.3 |
| DH5 | 432.6 | 723.2 | 57.6 |

### Example 19.1

What is the hopping rate of Bluetooth, and how many bits are transmitted in one slot? If each frame of the HV3 voice packet in Bluetooth carries 80 bits of sample speech, what is the efficiency of the packet transmission? How often do HV3 packets have to be sent to support 64 kbps voice in each direction?

#### Solution

- Hopping rate = 1600 hops per second, 240 bits in one slot packet
- $\eta = \frac{80}{240} = 0.3333$
- Let $x$ be the number of times a packet is sent

  $x \times 80 = 64{,}000$
  $\therefore x = 800$

### Example 19.2

A symmetric 1-slot DM1 link between a master and a slave carries 136 bits per slot at a rate of 800 slots per second (every other slot) in each direction. Find the associated data rate.

#### Solution

- Associated data rate $= \frac{136 \times 800}{1000} = 108.8\,\text{kbps}$

## 19.7 Bluetooth Security

**Bluetooth security supports authentication and encryption.** These features are based on a secret link key that is shared by pair of devices. A pairing procedure is

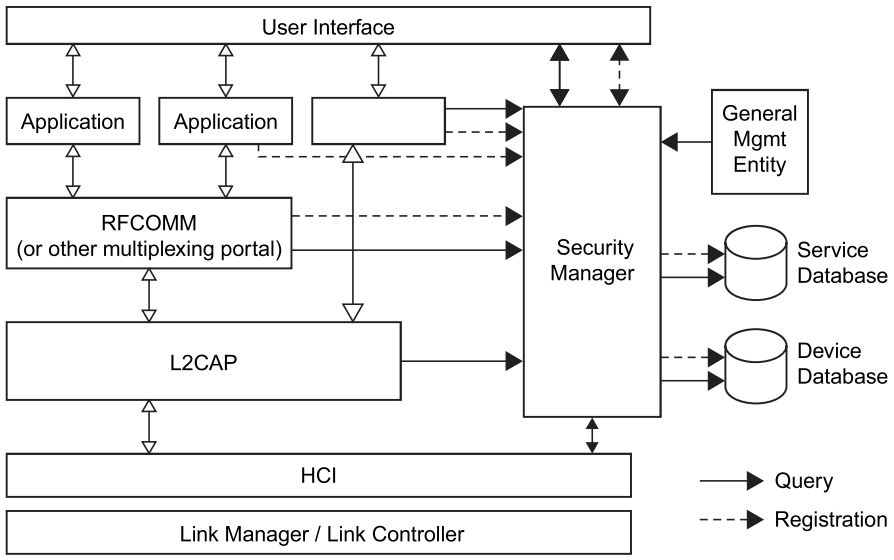



**Figure 19.4 Bluetooth security architecture.**

used when two devices communicate for the first time to generate this key. There are three security modes to a device:

- **Non-secure.** A device will not initiate any security procedure.
- **Service level enforced security.** A device does not initiate security procedures before channel establishment at the L2CAP level. This mode allows different and flexible access policies for applications, especially running applications with different security requirements in parallel.
- **Link level enforced security.** A device initiates security procedures before the link set-up at the LMP is completed.

Figure 19.4 shows Bluetooth security architecture.

### 19.7.1 Security Levels

There are two kinds of security levels: authentication and authorization.

- **Authentication** verifies who is at the other end of the link. In Bluetooth this is achieved by the authentication procedure based on the stored link key or by the pairing procedure. To meet different requirements on availability of services without user intervention, authentication is performed after determining what the security level of the requested service is. Thus, authentication cannot be performed when the ACL link is established.

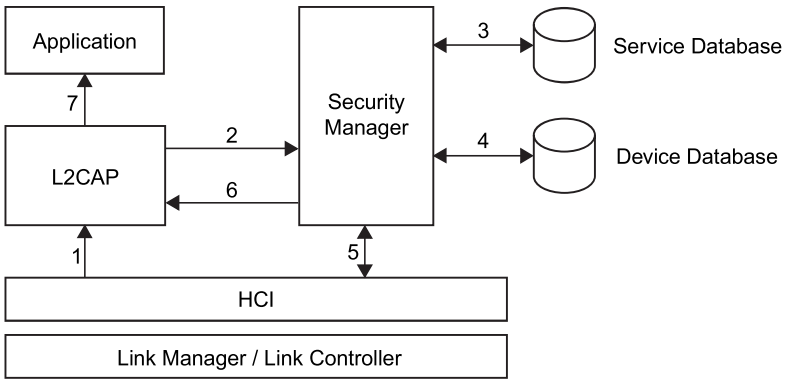



**Figure 19.5 Authentication procedures.**

The authentication is performed when a connection request to a service is submitted. The following procedure is used (see Figure 19.5):

1. The connect request to L2CAP is sent.
2. L2CAP requests access from the security manager.
3. The security manager enquires the service database.
4. The security manager enquires the device database.
5. If necessary, the security manager enforces the authentication and encryption procedure.
6. The security manager grants access, and L2CAP continues to set up the connection.

Authentication can be performed in both directions: client authenticates server and vice versa.

- **Authorization.** When one device is allowed to access the other, the concept of trust comes into existence. Trusted devices are allowed access to services. While, on the contrary, untrusted devices may require authorization based on user interaction before access to services is granted. There are two kinds of device trust levels:

  1. *Trusted device:* A device with a fixed relationship (paired) that has trusted and unrestricted access to all services.
  2. *Untrusted device:* This device has been previously authenticated, a link key is stored, but the device is not marked as trusted in the device database.
  3. *An unknown device* is also an untrusted device. No security information is available for this device.

For services, the requirement for authorization, authentication, and encryption are set independently (although some restrictions apply). The access requirements define three security levels:

- Services that require authorization and authentication—automatic access is only granted to trusted devices. Other devices need a manual authorization.
- Services that require authentication only—authorization is not necessary.
- Services open to all devices—authentication is not required, no access approval is required before service access is granted.

A default security level is defined to serve the needs of legacy applications. This default policy will be used unless other settings are found in a security database related to a service.

### 19.7.2 Limitations of Bluetooth Security

Only a device is authenticated, and not its user. There is no mechanism to preset authorization per service. However, a more flexible security policy can be implemented with the present architecture without a need to change the Bluetooth protocol stack. Also, it is not possible to enforce unidirectional traffic.

## 19.8 Network Connection Establishment in Bluetooth

Before any connection in a piconet is created, all devices are in *STANDBY* mode. In this mode, an unconnected unit periodically listens for messages every 1.28 seconds. Each time a device wakes up, it listens on a set of 32 hop frequencies defined for that unit. The number of hop frequencies varies in different geographic regions.

The connection procedure is initiated by any one of the devices, which then becomes master. A connection is made by a *PAGE* message if the address is already known, or by an *INQUIRY* message followed by a subsequent *PAGE* message if the address is unknown (see Figure 19.6).

In the initial *PAGE* state, the master unit sends a train of 16 identical page messages on 16 different hop frequencies defined for the device to be paged (slave unit). If no response is received, the master transmits a train on the remaining 16 hop frequencies in the wake-up sequence. The maximum delay before the master reaches the slave is twice the wake-up period (2.56 seconds) while the average delay is half the wake-up period (0.64 seconds).

The *INQUIRY* message is typically used for finding Bluetooth devices, including public printers, fax machines, and similar devices with an unknown address. The *INQUIRY* message is similar to the *PAGE* message, but may require one additional train period to collect all responses.

A power saving mode can be used for connected units in a piconet if no data needs to be transmitted. The master unit can put slave units into *HOLD* mode, where only the internal timer is running. Slave units can also demand to be put

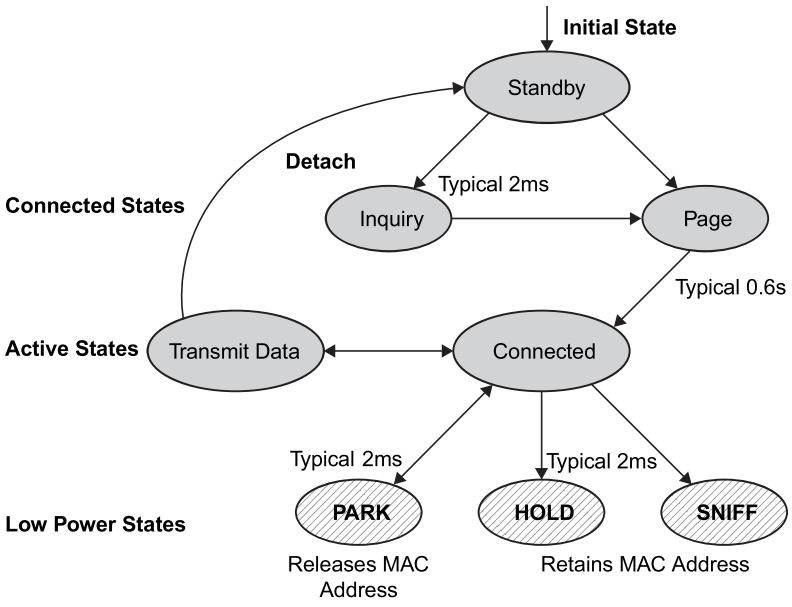



**Figure 19.6 Device states in Bluetooth.**

into *HOLD* mode. Data transfer restarts instantly when units transition out of *HOLD* mode. The *HOLD* is used when connecting several piconets or managing a low-power device such as a temperature sensor.

Two more low-power modes are also available: the *SNIFF* mode and *PARK* mode. In the *SNIFF* mode, a slave device listens to the piconet at a reduced rate, thus reducing its duty cycle. The *SNIFF* interval is programmable and depends on the application. In the *PARK* mode, a device is still synchronized to the piconet but does not participate in the traffic. Parked devices have given up their MAC address and occasionally listen to the traffic of the master to resynchronize and check on broadcast messages.

If we list the modes in increasing order of power efficiency, then the *SNIFF* mode has the higher duty cycle, followed by the *HOLD* mode with a lower duty cycle, and the *PARK* mode with the lowest duty cycle.

## 19.9 Error Correction in Bluetooth

Three error correction schemes are defined for the Bluetooth baseband controller:

- $^1/_3$ rate forward error correction (FEC) code
- $^2/_3$ rate forward error correction code
- Automatic repeat request (ARQ) scheme for data

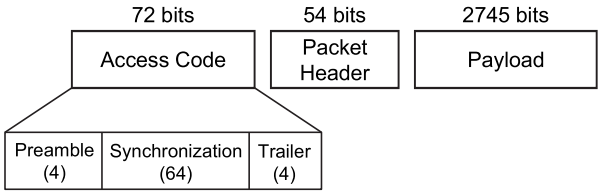



**Figure 19.7 Packet format in Bluetooth.**

The purpose of the FEC scheme on the data payload is to reduce the number of retransmissions. However, in a reasonably error-free environment, FEC creates unnecessary overhead that reduces the throughput. Therefore, the packet definitions have been kept flexible as to whether or not to use FEC in the payload. The packet header is always protected by a 1/3 rate FEC. It contains link information and should survive bit errors. An unnumbered ARQ scheme is applied in which data transmitted in one slot is directly acknowledged by the recipient in the next slot. For a data transmission to be acknowledged, both the header error check and the cyclic redundancy check must be satisfied, otherwise a negative acknowledgment is returned.

## 19.10 Network Topology in Bluetooth

Bluetooth devices can create both point-to-point and point-to-multipoint connections. A connection with two or several (maximum 8 devices) devices is a piconet where all devices follow the same frequency-hop scheme. To avoid interference between devices, one of the devices automatically becomes a master of the piconet. In each slot, a packet can be exchanged between the master (M) and one of the slaves (S). Packets have a fixed format (see Figure 19.7).

A Bluetooth packet format is based on one packet per hop and a basic 1-slot packet of 625 μs that can be extended to 3-slot (1875 μs) and 5-slot (3125 μs). A frame format allows the master to poll multiple slaves.

Each packet begins with a 72-bit access code that is derived from the master identity and is unique for the channel. Every packet exchanged on the channel is preceded by this access code. Recipients on the piconet compare incoming signals with the access code. If the two do not match, the received packet is not considered valid on the channel and the rest of its contents are ignored. Besides packet identification, the access code is also used for synchronization and compensating for offset. The access code is robust and resistant to interference.

Two or several piconets can communicate with each other and are then called a scatternet.

## 19.11 Bluetooth Usage Models

In this section we discuss some of the Bluetooth usage models. Each usage model has one or more profiles.

- **Three-in-one phone.** The three-in-one phone usage model describes how a telephone handset may connect to three different service providers. The telephone may act as a cordless telephone connecting to the PSTN at home, charged at a fixed line charge. The telephone can also connect directly to other telephones acting as a walkie-talkie or handset extension. Finally, the telephone may act as a cellular phone connecting to the cellular infrastructure.
- **File transfer.** The file transfer usage model offers the capability to transfer data objects from one Bluetooth device to another. Files, entire folders, directories, and streaming media formats are supported in this model. The model also offers the possibility of browsing the contents of the folders on a remote device.
- **Synchronization.** The synchronization usage model provides the means for automatic synchronization between, for instance, a desktop PC, a portable PC, a PDA, and a notebook. The synchronization requires business card, calendar, and task information to be transferred and processed by computers, cellular phones, and PDAs utilizing a common protocol and format.
- **Internet bridge.** The Internet bridge usage model describes how a mobile phone or cordless modem provides a PC with dial-up networking capabilities without the need for physical connection to the PC. This networking scenario requires a two-piece protocol stack, one for AT-commands to control the mobile phone and another stack to transfer payload data.
- **Ultimate handset.** The ultimate handset usage model defines how a Bluetooth-equipped wireless handset can be connected to act as a remote unit's audio input and output interface. This unit is probably a mobile phone or a PC for audio input and output.

## 19.12 Bluetooth Applications

The following are some of the areas where Bluetooth can be used:

- Replacing serial cables with radio links
- Wearable networks/WPANs
- Desktop/room wireless networking
- Hot-spot wireless networking
- Medical: Transfer of measured values from training units to analytical systems, patient monitoring
- Automotive: Remote control of audio/video equipment, hands-free telephony
- Point-of-sale payments: Payments by mobile phone

## 19.13 WAP and Bluetooth

Bluetooth can be used with WAP like any other wireless network. Bluetooth wireless networks can be used to transport data from a WAP client to a WAP server. The WAP client can make use of Bluetooth's SOP to find the WAP server/gateway. This is very useful when the WAP device is a mobile phone and when it comes into the range of a WAP server, it can use Bluetooth's SDP to discover the gateway. The Bluetooth SDP must be able to provide some details about the WAP server to the WAP client.

The other feature that can be supported is the reverse of the above. The WAP server can periodically check for the availability of WAP-enabled clients in its range. It can use Bluetooth's SDP to do this. If there are any clients, the server can push any data to the client. The client of course is not required to accept the data pushed to it.

## 19.14 Summary

In this chapter we discussed Bluetooth technology that allows for replacing many proprietary cables that connect one device to another with one universal short-range radio link. Bluetooth radio technology provides a universal bridge to existing data networks, a peripheral interface, and a mechanism to form small, private ad hoc groupings of connected devices away from fixed network infrastructures. The Bluetooth technology has a number of advantages including minimal hardware dimensions, low cost of components, and low power consumption. These advantages make it possible to introduce Bluetooth in many types of devices at a low cost. The 720 kbps data capability provided by Bluetooth can be used for cable replacement and several other applications, such as LAN.

## Problems

**19.1** What are piconet and scatternet in Bluetooth?

**19.2** Discuss transport protocol group in Bluetooth.

**19.3** Define link types in Bluetooth.

**19.4** How is security achieved in Bluetooth?

**19.5** The hopping rate of 1600 hops per second is used in Bluetooth that carries 240 bits in a 1-slot packet. If each frame of the HV2 voice packet carries 160 bits of sample speech, what is the efficiency of packet transmission? How often are HV2 packets sent to support 64 kbps voice in each direction?

**19.6** A symmetric 1-slot DH1 link of Bluetooth between a master and a slave carries 216 bits per slot. What is the associated rate?

**19.7** The asymmetric DM5 link of Bluetooth uses a 5-slot packet to carry 1792 bits per packet by the master terminal and a 1-slot packet to carry 136 bits per packet by the slave terminal. What are the data rates of the master and slave terminal?

## References


1. Bisdikian, C., and Miller, B. *Blue Tooth Revealed*. Upper Saddle River, NJ: Prentice Hall, 2000.
2. Bluetooth Special Interest Group (SIG). "Specifications of the Bluetooth System," vol. 1 v.1.1, "Core" and vol. 2 v. 1.0 B "Profiles," 2000.
3. Bluetooth Specification Release 1.0, section F:4, "Interoperability Requirements for Bluetooth as WAP Bearer."
4. Bray, J., and Sturman, C. F. *Bluetooth: Connect without Cables*. Upper Saddle River, NJ: Prentice Hall, 2001.
5. http://www.bluetooth.com/.
6. IEEE 802.15 Working Group. http://grouper.ieee.org/groups/802/15/.
7. Moran, P. Ed. "Bluetooth LAN Access Profile using PPP." *Bluetooth Special Interest Group*, version 1.0, 1999.
8. Muller, N. J. *Bluetooth Demystified*. New York: McGraw Hill, 2000.
9. Pahlavan, K., and Krishnamurthy, P. *Principle of Wireless Networks*. Upper Saddle River, NJ: Prentice Hall, 2002.
10. Sand Kjell, Tik-111.550 Seminar on Multimedia: "Bluetooth," March, 4, 1999.
11. Simpson, W. Ed. "The Point-to-Point Protocol (PPP)." *STD 50, RFC1661. Day-dreamer,* July 1994.
12. Simpson, W. Ed. "PPP in HDLC Framing." *STD51, RFC1662. Day-dreamer,* July 1994.