CHAPTER 6

LAYER 1/2 CONNECTIVITY: WIRELESS TECHNOLOGIES FOR THE IoT

This chapter surveys basic lower-layer wireless technologies to support IoT/machine-to-machine (M2M) applications, as it appears that many such implementations will entail wireless connectivity at the PHY/MAC layer. Available wireless networks[1] that can be utilized for IoT/M2M applications include the following:

- Personal area networks (PANs): Zigbee®, Bluetooth®, especially Bluetooth low energy (BLE), near field communications (NFC), and proprietary systems (e.g., ANT+,[2] NIKE+[3]); specifically, there is interest in low-power wireless personal area networks (LoWPANs); some of these PANs are also classified as low-rate wireless personal area networks (LR-WPANs);

[1] Some refer to the entire "wireless networks" field as wireless information and communication technology (WICT).

[2] ANT/ANT+ is a proprietary wireless sensor network technology targeted at manufacturers of bike computers, speed/cadence sensors, foot pods, power meters, heart rate monitors, calorimeters, body mass index-measuring devices, blood pressure monitors, blood glucose meters, and so on, promoted by the ANT+ Alliance. It is principally used for compatible Garmin device. For example, an ANT+ heart rate strap will send heart rate data to a watch, phone, bike computer, tablet, and/or any other device that reads ANT+ heart rate.

[3] Nike+® is a proprietary wireless technology developed by Nike and Apple to allow users to monitor their activity levels while exercising.

Building the Internet of Things with IPv6 and MIPv6: The Evolving World of M2M Communications,
First Edition. Daniel Minoli.

- Wireless local area networks (WLANs): Wi-Fi® IEEE Standard 802.11 (including vendor-specific implementations for low power[4]);
- Metropolitan area networks (MANs): WiMAX;
- Wireless sensor networks (WSN): application-specific technology, in general;
- Third generation (3G)/4G cellular: Universal mobile telecommunications system (UMTS), general packet radio service (GPRS), enhanced data rates (EDRs) for GSM evolution (EDGE), and long-term evolution (LTE); and,
- Global: Satellite networks.

While IoT/M2M connectivity might be achieved by wired means, for example power line communication (PLC)-based grid management, some operators have used wireless technology for meter reading. Furthermore, although energy suppliers routinely utilize supervisory control and data acquisition (SCADA)-based systems to enable remote telemetry functions in the power grid and, and although, traditionally, SCADA systems have used wireline networks to link remote power grid elements with a central operations center, at this time an increasing number of utilities are turning to public cellular networks to support these functions. Some of the wireline technologies, including PLC, are briefly discussed in the appendix to this chapter.

6.1 WPAN TECHNOLOGIES FOR IoT/M2M

A PAN (also called WPAN) is a network used for communication among intelligent devices physically close to a person (including smartphones, tablets, body monitors, and so on). PANs can be used to support wireless body area networks (WBANs) (also known as wireless medical body area networks [WMBANs] and/or medical body area network systems [MBANSs]), but they can also be used to support other applications. As discussed in Chapter 3, Medical applications include, among others, vital sign monitoring, respiration monitoring, electrocardiography (ECG), pH monitoring, glucose monitoring, disability assistance, muscle tension monitoring, and artificial limb support. Nonmedical applications of WBANs include, among others, video streaming, data transfer, and entertainment and gaming. The reach of a PAN is typically a few meters. The devices in question are sometimes known as short-range devices (SRDs) (1). PANs can be used for communication among the personal devices themselves (intrapersonal communication), or for connecting to a higher level network such as the Internet. Table 6.1 (partially based on Reference 2) summarizes a coarse comparison between three wireless technologies, highlighting the features of BANs/WBANs. The WBAN technologies can satisfy, in various degrees, major requirements that the healthcare industry considers important: (i) very low-power

[4] In recent years, several improvements have been made to the Wi-Fi LAN standard; some of these improvements (including IEEE Standard 802.11v) are aimed at reducing its power consumption. Wi-Fi is optimized for traditional office automation (OA) large data transfer, where high throughput is needed; it is not generally intended for coin cell operation.

TABLE 6.1 Comparison of Technologies

	WBAN	WSN	Cellular Wireless Networks
Traffic	Application specific, sporadic/cyclic, modest data rate		Multimedia, high data rate
Topology	Dynamic	Random, dynamic	Few infrastructure changes
Configuration/ maintenance	Some flexibility Specialists are needed	Self-configurable, unattended operation	Managed by large organizations/ carriers
Battery	Multimonth to multiyear battery life		Replaced as needed
Network size	Dense distribution limited by body size	Unlimited number (typically 10^2–10^6)	Tens of nodes
Node	Low/modest complexity		High complexity
Overall design goals	Limited electromagnetic exposure, energy efficiency	Energy efficiency, self-operability cost optimization	Bandwidth efficiency. QoS (throughput/ delay)
Standardization	Multiple (IEEE) standards especially at lower layers	Relatively little standardization	Multiple international standards, ITU-T, ETSI, etc.

sensor consumption, (ii) very low transmitted power, and (iii) high reliability and quality of service (QoS).

Focusing specifically on WBANs, the key wireless standards include ZigBee/IEEE 802.15.4 along with the Personal, Home and Hospital Care (PHHC) Profile—ZigBee Health Care, IEEE 802.15.1 (Bluetooth), and the newer IEEE 802.15.6 and IEEE 802.15.4j; other standards include ISO/IEEE 11073 and ETSI TR 101 557 V1.1.1 (2012–02). Note that both ZigBee and Bluetooth have been extended and modified in recent years to satisfy particular requirements of medical/fitness industries (3). Low-power consumption IEEE 802.11 Wi-Fi is considered generally less attractive at this time, although some proponents argue in favor.[5]

In this chapter, we focus predominantly on PANs and 3G/4G technologies. See Table 6.2 for a tabulation of some important technologies. It is not the goal of this

[5] Proponents make the case that no other wireless technology is as IP friendly as Wi-Fi. For example, ZigBee IP that requires the use of a bridge. ZigBee may have lower node costs, but it requires new infrastructure. Wi-Fi also provides the highest bandwidth of any wireless technologies—some low-power implementations provide up to 11 Mbps, with a fallback to 1 Mbps. ZigBee offers less than 250 Kbps, with no fallback. Wi-Fi also provides well-proven encryption, authentication, and end-to-end network security (WPA2, EAP, TLS/SSL); ZigBee still requires testing, since some security holes have been identified (4). On the other hand, Wi-Fi's power requirements are high. Work is being conducted in Wi-Fi groups to lower power consumption. Currently, however, proprietary drivers are needed, with the technology only applicable to the personal computer market where receiver power budgets are higher (5).

TABLE 6.2 Key Wireless Technology and Concepts Supporting IoT/M2M Applications

Technology/Concept	Description
3GPP	3GPP unites six telecommunications standard bodies, known as "organizational partners" and provides their members with a stable environment to produce the reports and specifications that define 3GPP technologies. These technologies are constantly evolving through—what have become known as—generations of commercial cellular/mobile systems. 3GPP was originally the standards partnership evolving Global System for Mobile communication (GSM) systems toward the 3G. However, since the completion of the first LTE and the Evolve Packet Core (EPC) specifications, 3GPP has become the focal point for mobile systems beyond 3G. From 3GPP Release 10 onward, 3GPP is compliant with the latest ITU-R requirements for IMT-Advanced "Systems beyond 3G." The standard now allows for operation at speeds up to100 Mbps for high-mobility and 1 Gbps for low-mobility communication. The original scope of 3GPP was to produce Technical Specifications and Technical Reports for a 3G Mobile System based on evolved GSM CNs and the radio access technologies that they support (i.e., Universal Terrestrial Radio Access (UTRA) both frequency division duplex [FDD] and time division duplex [TDD] modes). The scope was subsequently amended to include the maintenance and development of the GSM Technical Specifications and Technical Reports including evolved radio access technologies (e.g. GPRS and EDGE) (6). The term "3GPP specification" covers all GSM (including GPRS and EDGE), W-CDMA, and LTE (including LTE-Advanced) specifications. The following terms are also used to describe networks using the 3G specifications: UTRAN, UMTS (in Europe), and FOMA (in Japan)
3GPP2 (Third-Generation Partnership Project 2)	3GPP2 is a collaborative 3G telecommunications specification-setting project comprising North American and Asian interests developing global specifications for ANSI/TIA/EIA-41 Cellular Radiotelecommunication Intersystem Operations network evolution to 3G and global specifications for the radio transmission technologies (RTTs) supported by ANSI/TIA/EIA-41. 3GPP2 was born out of the International Telecommunication Union's (ITU) International Mobile Telecommunications "IMT-2000" initiative, covering HS, broadband, and Internet protocol (IP)-based mobile systems featuring network-to-network interconnection, feature/service transparency, global roaming, and seamless services independent of location (7)

(*continued*)

TABLE 6.2 (*Continued*)

Technology/Concept	Description
6LoWPAN: IPv6 over low-power area networks (IEEE 802.15.4)	6LoWPAN is now a widely accepted approach to run IP on 802.15.4 based on RFC 4944 (September 2007). It is supported in TinyOS, Contiki, and in standards such as ISA100, ZigBee SE 2.0. RFC 4944 makes 802.15.4 look like an IPv6 link. It provides basic encapsulation, efficient representation of packets $< \sim 100$ bytes. It addresses topics such as (8): • Fragmentation (how to map 1280-byte MTU to packets 128 bytes or less); • First approach to stateless header compression; • Datagram tag/datagram offset; • Mesh forwarding; • Identify originator/final destination; • Minimal use of complex MAC layer concepts
ANT/ANT+	ANT$^{\text{TM}}$ is a low-power proprietary wireless technology introduced in 2004 by the sensor company Dynastream. The system operates in the 2.4 GHz band. ANT devices can operate for years on a coin cell. ANT's goal is to allow sports and fitness sensors to communicate with a display unit. ANT+$^{\text{TM}}$ extends the ANT protocol and makes the devices interoperable in a managed network. ANT+ recently introduced a new certification process as a prerequisite for using ANT+ branding (5)
Bluetooth	Bluetooth is a PAN technology based on IEEE 802.15.1. It is a specification for short-range wireless connectivity for portable personal devices initially developed by Ericsson. The Bluetooth SIG made their specifications publicly available in the late 1990s, at which time the IEEE 802.15 Group has took the Bluetooth work and developed a vendor-independent standard. The sublayers of IEEE 802.15:include: (i) RF layer; (ii) baseband layer; (iii) the link manager; and (iv) the L2CAP. Bluetooth has evolved through four versions; all versions of the Bluetooth standards maintain downward compatibility. BLE is a subset to Bluetooth v4.0 with an entirely new protocol stack for rapid build-up of simple links. BLE is an alternative to the "power management" features that were introduced in Bluetooth v1.0 to v3.0 as part of the standard Bluetooth protocols (Bluetooth is a trademark of the Bluetooth Alliance, a commercial organization that certifies the interoperability of specific devices designed to the respective IEEE standard.)

TABLE 6.2 (*Continued*)

Technology/Concept	Description
EDGE (Enhanced Data Rates for Global Evolution)	An enhancement of the GSM^{TM} radio access technology to provide faster bit rates for data applications, both circuit and packet switched. As an enhancement of the existing GSM PHY layer, EDGE is realized via modifications of the existing layer 1 specifications rather than by separate, standalone specifications. Other than providing improved data rates, EDGE is transparent to the service offering at the upper layers, but is an enabler for HS circuit switched data (HSCSD) and enhanced GPRS (EGPRS). By way of illustration, the GPRS can offer a data rate of 115 Kbps, whereas EDGE can increase this to 384 Kbps. This is comparable with the rate for early implementations of Wideband Code Division Multiple Access (W-CDMA), leading some parties to consider EDGE as a 3G technology rather than 2G (a capability of 384 Kbps allows EDGE systems to meet the ITU's IMT-2000 requirements). EDGE is generally viewed as a bridge between the two generations: a sort of 2.5G (9)
DASH7	A long range low-power wireless networking technology, with the following features: • Range: dynamically adjustable from 10 m to 10 km • Power: <1 milliwatt power draw • Data rate: dynamically adjustable from 28 Kbps to 200 Kbps • Frequency: 433.92 MHz (available worldwide) • Signal propagation: penetrates walls, concrete, water • Real-time locating precision: within 4 m • Latency: configurable, but worst case is less than 2 s • P2P cessaging • IPv6 support • Security: 128-bit AES, public key • Standard: ISO/IEC 18000-7; advanced by the DASH7 Alliance
GPRS (General Packet Radio Service)	Packet-switched functionality for GSM, which is essentially circuit switched. GPRS is the essential enabler for always-on data connection for applications such as web browsing and push-to-talk over cellular. GPRS was introduced into the GSM specifications in Release 97 and usability was further approved in Releases 98 and 99. It offers faster data rates than plain GSM by aggregating several GSM time slots into a single bearer, potentially up to eight, giving a theoretical data rate of 171 Kbps. Most operators do not offer such high rates, because obviously if a slot is being used for a GPRS bearer, it is not available for other traffic. Also, not all mobiles are able to aggregate all combinations of slots.

(*continued*)

TABLE 6.2 (***Continued***)

Technology/Concept	Description
	The “GPRS class number” indicates the maximum speed capability of a terminal, which might be typically 14 Kbps in the uplink direction and 40 Kbps in the downlink, comparable with the rates offered by current wireline dial-up modems. Mobile terminals are further classified according to whether or not they can handle simultaneous GSM and GPRS connections: class A = both simultaneously, class B = GPRS connection interrupted during a GSM call, automatically resumed at end of call, class C = manual GSM/GPRS mode switching. Further data rate increases have been achieved with the introduction of EDGE (9)
GSM EDGE Radio Access Network (GERAN)	GERAN is an Radio Access Network (RAN) architecture, based on GSM/EDGE radio access technologies. GERAN is the term given to the second-generation digital cellular GSM radio access technology, including its evolutions in the form of EDGE and, for most purposes, the GPRS. The GERAN is harmonized with the UTRAN through a common connectivity to the UMTS CN, making it possible to build a combined network for GSM/GPRS and UMTS. GERAN is also the name of the 3GPP^{TM} Technical Specification Group responsible for its development. The technical specifications which together comprise a 3GPP system with a GERAN are listed in 3GPP TS 41.101
IEEE 802.15.4	IEEE Standard for Local and MANs. Part 15.4: *Low-Rate Wireless Personal Area Networks (LR-WPANs)*. IEEE 802.15.4-conformant devices support a wide range of industrial and commercial applications. The amended MAC sublayer facilitates industrial applications such as process control and factory automation in addition to the MAC behaviors that support the Chinese wireless personal area network (CWPAN) standard
IEEE 802.15.4j (TG4j) MBANs	The purpose of Task Group 4j (TG4j) is to create an amendment to 802.15.4, which defines a PHY layer for IEEE 802.15.4 in the 2360 to 2400 MHz band and complies with FCC MBAN rules. The amendment may also define modifications to the MAC needed to support this new PHY layer. This amendment allows 802.15.4- and MAC-defined changes to be used in the MBAN band (10)
Infrared Data Association (IrDA®)	IrDA is an SIG consisting of about 40 members at press time. The SIG is pursuing a 1 Gbps connectivity link; however, this link only operates over a distance of less than 10 cm. One of the challenges with IR signaling is its requirement for LOS requirement. Additionally, IrDA is also not very power efficient (power per bit) when compared with radio technologies

TABLE 6.2 (*Continued*)

Technology/Concept	Description
ISA100.11a	ISA SP100 standard for wireless industrial networks developed by the International Society of Automation (ISA) to address all aspects of wireless technologies in a plant. The ISA100 Committee addresses wireless manufacturing and control systems in the areas of the: (i) environment in which the wireless technology is deployed; (ii) technology and life cycle for wireless equipment and systems; and (iii) application of wireless technology. The wireless environment includes the definition of wireless, radio frequencies (starting point), vibration, temperature, humidity, electromagnetic compatibility (EMC), interoperability, coexistence with existing systems, and physical equipment location. ISA100.11a Working Group Charter addresses (11): • Low-energy consumption devices, with the ability to scale to address large installations • Wireless infrastructure, interfaces to legacy infrastructure and applications, security, and network management requirements in a functionally scalable manner • Robustness in the presence of interference found in harsh industrial environments and with legacy systems • Coexistence with other wireless devices anticipated in the industrial work space • Interoperability of ISA100 devices
LTE (Long Term Evolution)	LTE is the 3GPP initiative to evolve the UMTS technology toward a 4G. LTE can be viewed as an architecture framework and a set of ancillary mechanisms that aim at providing seamless IP connectivity between UE and the packet (IPv4, IPv6) data network without any disruption to the end-users' applications during mobility. In contrast to the circuit-switched model of previous-generation cellular systems, LTE has been designed to support *only* packet-switched services
NFC (Near Field Communication)	A group of standards for devices such as PDAs, smartphones, and tablets that support the establishment of wireless communication when such devices are in immediate proximity of a few inches. These standards encompass communications protocols and data exchange formats; they are based on existing RFID standards including ISO/IEC 14443 and FeliCa (a contactless RFID smart card system developed by Sony, e.g., utilized in electronic money cards in use in Japan). NFC standards include ISO/IEC 18092, as well as other standards defined by the NFC Forum. NFC standards allow two-way communication between endpoints (earlier generation systems were one-way systems only). Unpowered NFC-based tags can also be read by NFC devices; therefore, this technology can substitute for earlier one-way systems. Applications of NFC include contactless transactions

(*continued*)

TABLE 6.2 (*Continued*)

Technology/Concept	Description
NIKE+	Nike+® is a proprietary wireless technology developed by Nike and Apple to allow users to monitor their activity levels while exercising. Its power consumption is relatively high, returning only 40 days of battery life from a coin cell. It is a proprietary radio that only works between Nike and Apple devices. Nike+ devices are shipped as a single unit: processor, radio, and sensor (5)
RF4CE (Radio Frequency for Consumer Electronics)	RF4CE is based on ZigBee and was standardized in 2009 by four CE companies: Sony, Philips, Panasonic, and Samsung. Two silicon vendors support RF4CE: Texas Instruments and Freescale Semiconductor, Inc. RF4CE's intended use is as a device RC system, for example for television set-top boxes. The intention is that it overcomes the common problems associated with IR: interoperability, line of sight, and limited enhanced features (5)
Satellite systems	Satellite communication plays a key role in commercial, TV/media, government, and military communications because of its intrinsic multicast/broadcast capabilities, mobility aspects, global reach, reliability, and ability to quickly support connectivity in open-space and/or hostile environments. Satellite communications is a LOS one-way or two-way RF transmission system that is comprised of a transmitting station (uplink), a satellite system that acts as a signal regeneration node, and one or more receiving stations (downlink). Satellites can reside in a number of orbits. A geosynchronous (GEO) satellite circles the earth at the earth's rotational speed and with the same direction of rotation, therefore appearing at the same position in the sky at a particular time each day. When the satellite is in the equatorial plane, it appears to be permanently stationary when observed at the earth's surface, so that an antenna pointed to it will not require tracking or (major) positional adjustments at periodic intervals of time (this satellite arrangement is also known as "geostationary"). The geostationary orbit is at 35,786 km (22,236 mi) of altitude from the earth's surface. Other orbits include the following: low earth orbits (LEOs), medium earth orbits (MEOs) (aka intermediate circular orbits [ICOs]), polar orbits, and highly elliptical orbits (HEOs). LEOs are either elliptical or (more commonly) circular orbits that are at a height of 2000 km or less above the surface of the earth. The advantage of LEOs is that they significantly reduce the propagation delay of the signal. The orbit period at these altitudes varies between 90 min and 2 h and the maximum time during which a satellite in LEO orbit is above the local horizon for an observer on the earth is up to 20 min.

TABLE 6.2 (*Continued*)

Technology/Concept	Description
	With LEOs, there are long periods during which a given satellite is out of view of a particular ground station; this may be acceptable for some applications, for example, for earth monitoring. Coverage can be extended by deploying more than one satellite and using multiple orbital planes. A complete global coverage system using LEO orbits requires a large number of satellites (>12+), in multiple orbital planes, and in various orbits. See Reference 12 for extensive treatment of this topic
UTRAN (UMTS Terrestrial Access Network)	A collective term for the NodeBs (base stations) and radio network controllers (RNCs) that comprise the UMTS RAN. NodeB is the equivalent to the BTS concept used in GSM. The UTRAN allows connectivity between the UE and the CN
UMTS (Universal Mobile Telecommunications System)	UMTS is a 3G mobile cellular technology for networks supporting voice and data (IP) based on the GSM standard developed by the 3GPP
Very small aperture terminal (VSAT)	A complete end-user terminal (typically with a small 4–5 ft antenna) that is designed to interact with other terminals in a satellite delivered data IP-based network, commonly in a "star" configuration through a hub. Contention and/or traffic engineering are typical of these services. Hub or network operator to control the system and present billing based on a data throughput, or other form of usage basis. VSATs are utilized in a variety of remote applications and are designed as low-cost units (say $1500–$3000 depending on application and data rate)
Wi-Fi	WLANs based on the IEEE 802.11 family of standards, including 802.11a, 802.11b, 802.11g, and 802.11n (13). (Wi-Fi is a trademark of the Wi-Fi Alliance, a commercial organization that certifies the interoperability of specific devices designed to the respective IEEE standard.)
WiMAX	WiMAX is defined as Worldwide Interoperability for Microwave Access by the WiMAX Forum, formed in June 2001 to promote conformance and interoperability of the IEEE 802.16 standard. The WiMAX Forum describes WiMAX as "a standards-based technology enabling the delivery of last mile wireless broadband access as an alternative to cable and DSL." (53)
Wireless Meter-Bus (M-Bus)	The Wireless M-Bus standard (EN 13757–4:2005) specifies communications between water, gas, heat, and electric meters and is becoming widely accepted in Europe for smart metering or AMI applications. Wireless M-Bus is targeted to operate in the 868 MHz band (from 868 MHz to 870 MHz); this band enjoys good trade-offs between RF range and antenna size. Typically chip manufacturers, for example Texas Instruments, have both single-chip (SoC) and two-chip solutions for Wireless M-Bus

(*continued*)

TABLE 6.2 (*Continued*)

Technology/Concept	Description
WSN (Wireless Sensor Network)	A sensor network is an infrastructure comprised of sensing (measuring), computing, and communication elements that gives the administrator the ability to instrument, observe, and react to events and phenomena in a specified environment. Typically, the connectivity is by wireless means, hence the term WSN. See reference (14) for an extensive treatment of this topic
WirelessHART (aka IEC 62591)	WirelessHART is a wireless sensor networking technology based on the highway addressable remote transducer protocol (HART). In 2010, WirelessHart was approved by the International Electrotechnical Commission (IEC) as IEC 62591 as a wireless international standard. IEC 62591 entails operation in the 2.4 GHz ISM band using IEEE 802.15.4 standard radios and makes use of a time-synchronized, self-organizing, and self-healing mesh architecture. WirelessHART/IEC 62591 was defined for the requirements of process field device networks. It is a global IEC-approved standard that specifies an interoperable self-organizing mesh technology in which field devices form wireless networks that dynamically mitigate obstacles in the process environment. This architecture creates a cost-effective automation alternative that does not require wiring and other supporting infrastructure (15)
ZigBee RF4CE specification	The specialty-use driven specification was designed for simple, two-way device-to-device control applications that do not require the full-featured mesh networking capabilities offered by ZigBee 2007. ZigBee RF4CE offers lower memory size requirements, thereby enabling lower cost implementations. The simple device-to-device topology provides easy development and testing, resulting in faster time to market. ZigBee RF4CE provides a multivendor interoperable solution for consumer electronics featuring a simple, robust, and low-cost communication network for two-way wireless connectivity. Through the ZigBee Certified program, the Alliance independently tests platforms implementing this specification and has a list of ZigBee Compliant Platforms offering support for ZigBee RF4CE (16)
ZigBee specification	The core ZigBee specification defines ZigBee's smart, cost-effective, and energy-efficient mesh network based on IEEE 802.15.4. It is a self-configuring, self-healing system of redundant, low-cost, very low-power nodes that enable ZigBee's unique flexibility, mobility, and ease of use. ZigBee is available as two feature sets, ZigBee PRO and ZigBee. Both feature sets define how the ZigBee mesh networks operate. ZigBee PRO, the most widely used specification, is optimized for low-power consumption and to support large networks with thousands of devices (16). (ZigBee is a trademark of the ZigBee Alliance, a commercial organization that certifies the interoperability of specific devices designed to the respective IEEE standard.)

(*continued*)

TABLE 6.2 (*Continued*)

Technology/Concept	Description
Z-wave	Z-wave is a wireless ecosystem that aims at supporting connectivity of home electronics, and the user, via Remote Control (RC). It uses low-power radio waves that easily travel through walls, floors, and cabinets. Z-wave control can be added to almost any electronic device in the home, even devices that one would not ordinarily think of as "intelligent," such as appliances, window shades, thermostats, smoke alarms, security sensors, and home lighting. Z-wave operates around 900 MHz (the band used by some cordless telephones but avoids interference with Wi-Fi devices). Z-wave was developed by Zen-Sys, a Danish startup around 2005; the company was later acquired by Sigma Designs. The Z-wave Alliance was established in 2005; it is comprised of about 200 industry leaders dedicated to the development and extension of Z-wave as the key enabling technology for "smart" home and business applications

chapter to provide an in-depth technical review of all these technologies, since each would require a text of its own, but the goal is to expose the reader to a plethora of available choices (furthermore, we are not attempting to exhaustively list all possibly applicable wireless or wireline standards, but to focus on a handful of key ones).

The following network topologies are applicable to personal low-power radio networks (5) (also see Table 6.3):

- **Broadcast:** environment where a message is sent from a device in the hope that it is received by a receiver within range. The broadcaster does not receive signals;
- **Mesh:** environment where a message can be relayed from one point in a network to any other by hopping through multiple nodes;
- **Star:** environment where a central device can communicate with a number of connected devices;
- **Scanning:** environment where a scanning device is constantly in receive mode, waiting to pick up a signal from anything transmitting within range;
- **Point-to-point:** in this mode, a one-to-one connection exists, where only two devices are connected over the communication path.

6.1.1 Zigbee/IEEE 802.15.4

As we have seen, the commercialization of consumer-based IoT services requires the introduction of wireless, low-power, battery-powered sensors and actuators in people's premises. Until recently, this space has been comprised of several PHY/MAC-specific nonstandardized protocol stacks that do not interoperate. ZigBee's focus has been aimed at the "little devices" (things, objects) often overlooked in an IT-centric

TABLE 6.3 Topologies Supported by PAN Wireless Technologies

		ZigBee	RF4CE	BLE	Wi-Fi	NFC	ANT/ANT+	NIKE+	IrDA
Topology	Broadcast	No	No	Yes	No	No	Yes	No	No
	Mesh	Yes	Yes	Yes	No	No	Yes	No	No
	Point-to-point	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
	Scanning	Yes	Yes	Yes	No	No	Yes	Yes	No
	Star	Yes	Yes	Yes	Yes	No	Yes	No	No
Technology aspects	Range	100 m	100 m	280 m	150 m	5 cm	30 m	10 m	10 cm
	Processor costs	N/A	N/A	N/A	High cost	High cost	Low cost	Low cost	N/A
	Radio cost	Low cost	Low cost	Low cost	High cost (~$3)	High cost (~$1)	Very low cost	Very low cost	Very low cost
	Throughput	~100 Kbps	(same as ZigBee)	~305 Kbps	~6 Mbps (lowest power 802.11b mode)	~424 Kbps	~20 Kbps	~272 bps	~1 Gbps
	Latency	~20 ms	(same as ZigBee)	~2.5 ms	~1.5 ms	Manufacturer specific (typically polled every second)	~Zero	~1 s	~25 ms
	Peak current draw (manganese dioxide lithium coin batteries such as the CR2032)	~40 mA	(same as ZigBee)	~12.5 mA	>100 mA	~50 mA	~17 mA	~12.3 mA	~10.2 mA
	Power per bit	~185.9 μW/bit	(same as ZigBee)	0.153 μW/bit	0.00525 μW/bit for high throughput	NA	0.71 μW/bit	2.48 μW/bit	11.7 μW/bit

Note 1: ANT/ANT+, NIKE+, and IrDA systems are only cited in passing in this chapter.
Note 2: Some parameters included here are based on data derived in Reference 5.

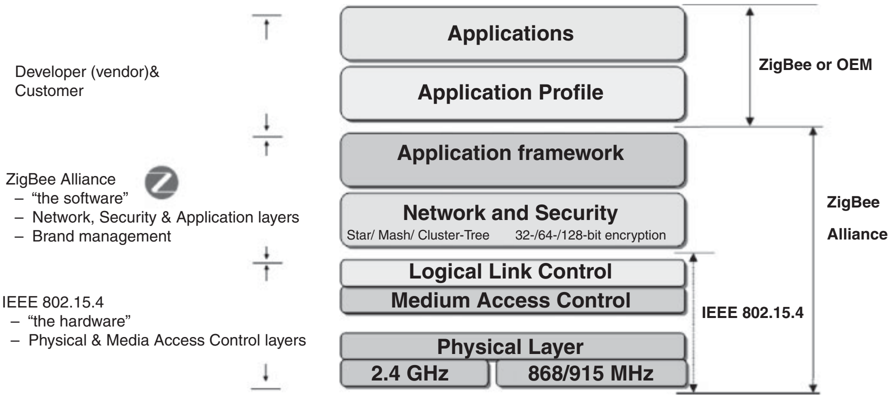


FIGURE 6.1 ZigBee protocol stack (overview).

world, such as light switches, thermostats, electricity meters, remote controls (RCs), as well as more complex sensor devices found in the healthcare, commercial building, and industrial automation sectors (17). To avoid multiple separate consumer networks, a PHY/MAC-agnostic solution is needed upon which IP standards and other well-known higher-layer protocols can run with little changes (18). ZigBee is one such open standard, as discussed below. ZigBee IP (ZIP) discussed in Chapter 5 is an example where Zigbee systems operate in an IP context. Here we focus more on the wireless lower-layer aspects of Zigbee and not the IP part *per se*.

ZigBee makes use of the physical radio specified by IEEE 802.15.4; it adds logical network capabilities, and security and application software. Figure 6.1 depicts the ZigBee protocol stack at a general level and Figure 6.2 depicts the stack at a more specific level. ZigBee utilizes the globally available, license-free 2.4 GHz industrial, scientific, and medical (ISM) frequency band to provide low data rate wireless applications (more generally, under IEEE 802.15.4, wireless links can operate in three unlicensed frequency bands, namely the 858 MHz band, the 902-to-928 MHz band, and the 2.4 GHz band[6]).

IEEE 802.15.4 defines a robust radio PHY (physical) layer and MAC (medium access control) layer, while ZigBee defines the network, security, and application framework for an IEEE 802.15.4-based system. (Table 6.4 provides an overview of the IEEE 802.15 family of PAN standards.) ZigBee networks support star, mesh, and cluster-tree topologies. These capabilities enable a network to have over 65,000 devices on a single wireless network. ZigBee offers low-latency communication between devices without the need for the initial network synchronization delays as required by Bluetooth. ZigBee can create robust self-forming, self-healing wireless mesh networks. The ZigBee mesh network connects sensors and controllers without being restricted by distance or range limitations; ZigBee mesh networks allow all

[6] 858 MHz in Europe; 902-to-928 MHz in the United States and Australia; 2.5 GHz in India; and 2.4 GHz in most countries worldwide

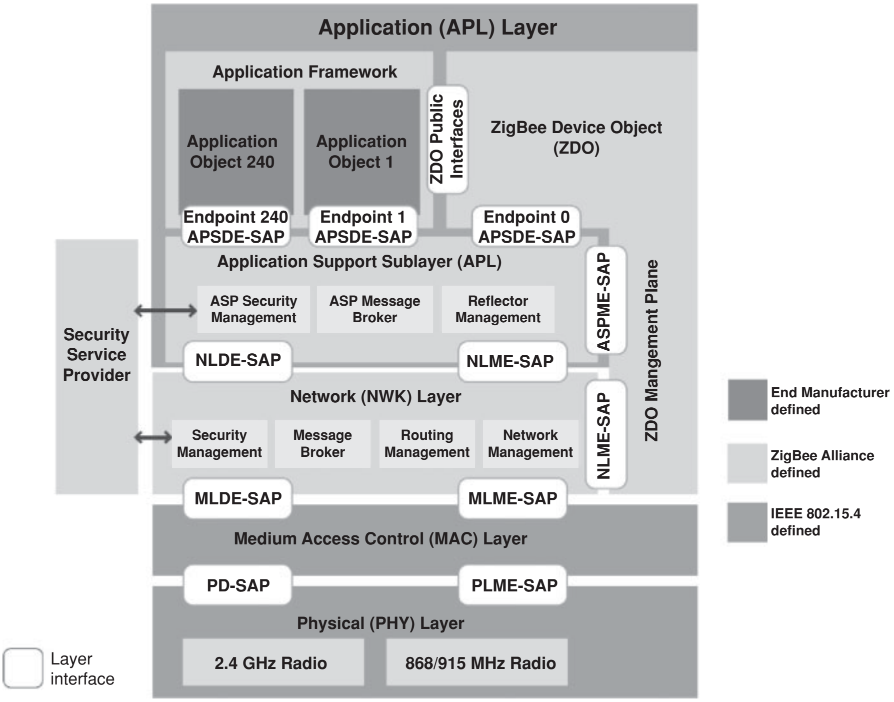


FIGURE 6.2 ZigBee protocol stack (details).

participating devices to communicate with one another and act as repeaters transferring data between devices.

ZigBee is available as two feature sets, ZigBee PRO^{TM} and ZigBee. Both feature sets define how the ZigBee mesh networks operate. ZigBee PRO, the most widely used specification, is optimized for low-power consumption and to support large networks with thousands of devices (16). In October 2007, the ZigBee Alliance announced an expanded set of features for the ZigBee protocol. This new stack profile is universally referred to as ZigBee PRO and for the most part defines specific stack settings and makes mandatory many of the features that are optional in the ZigBee stack that was ratified in 2006. ZigBee PRO also adds some new application profiles such as automatic meter reading, commercial building automation, and home automation. In general, ZigBee PRO features implement support for larger networks, for example stochastic addressing to assign addresses using probability analysis to simplify network formation. The Alliance likes to position ZigBee PRO as a seamless extension of 2006 ZigBee (a ZigBee 2006 node can join a 2007 network, and vice-versa, but designers cannot mix 2006 routers with 2007 routers) (19). ZigBee PRO implements a technique known as frequency agility (not hopping): a network node is able to scan for clear spectrum (with a choice of 16 available channels) and communicate its findings back to the ZigBee coordinator so that a new channel can

TABLE 6.4 The IEEE 802.15$^{\text{TM}}$ Family of Wireless PANs

Standard and Date	Description
IEEE 802.15.1$^{\text{TM}}$-2005	IEEE Standard for Information technology—Telecommunications and Information Exchange between systems: Local and MAN-specific requirements. Part 15.1: *Wireless Medium Access Control (MAC) and Physical layer (PHY) specifications for Wireless Personal Area Networks (WPANs)*
IEEE 802.15.2$^{\text{TM}}$-2003	IEEE Recommended Practice for Telecommunications and Information Exchange between systems: Local and MAN-specific requirements. Part 15.2: *Coexistence of Wireless Personal Area Networks with Other Wireless Devices Operating in Unlicensed Frequency Band*
IEEE 802.15.3$^{\text{TM}}$-2003	IEEE Standard for Information Technology—Telecommunications and Information Exchange between systems: Local and MAN-specific requirements. Part 15.3: *Wireless Medium Access Control (MAC) and Physical layer (PHY) specifications for High Rate Wireless Personal Area Networks (WPAN)*
IEEE 802.15.3b$^{\text{TM}}$-2005	IEEE Standard for Information Technology—Telecommunications and Information Exchange between systems: Local and MAN-specific requirements. Part 15.3b: *Wireless Medium Access Control (MAC) and Physical layer (PHY) specifications for High Rate Wireless Personal Area Networks (WPANs) Amendment 1: MAC Sublayer*
IEEE 802.15.3c$^{\text{TM}}$-2009	IEEE Standard for Information Technology—Telecommunications and Information Exchange between systems: Local and MAN-specific requirements. Part 15.3: *Wireless Medium Access Control (MAC) and Physical layer (PHY) specifications for High Rate Wireless Personal Area Networks (WPANs) Amendment 2: Millimeter-wave-based Alternative PHY layer extension*
IEEE 802.15.4$^{\text{TM}}$-2011	IEEE Standard for Local and MANs. Part 15.4: *Low-Rate Wireless Personal Area Networks (LR-WPANs)*
IEEE 802.15.4e$^{\text{TM}}$-2011	IEEE Standard for Local and MANs. Part 15.4: *Low-Rate Wireless Personal Area Networks (LR-WPANs) Amendment 1: MAC sublayer*
IEEE 802.15.5$^{\text{TM}}$-2009	IEEE Standard for Recommended Practice for Information technology - Telecommunications and information exchange between systems: Local and MANs - Specific requirements Part 15.5: Mesh Topology Capability in WPANs.
IEEE 802.15.6$^{\text{TM}}$-2012	IEEE Standard for Local and MANs. Part 15.6: *Wireless Body Area Networks*
IEEE 802.15.7$^{\text{TM}}$-2011	IEEE Standard for Local and MANs. Part 15.7: *Short-Range Wireless Optical Communication Using Visible Light*

be used across the network (5). ZigBee PRO networks have the ability to aggregate routes through the use of “many-to-one” routing; this allows each device to share the same routing path reducing broadcast and network traffic and greatly improves the efficiency and stability of the network routing table. The ZigBee 802.15.4 spec defines a maximum packet size of 128 octets; this packet size is optimal for short control messages, but there may be instances where the network needs to send larger messages; therefore, ZigBee PRO now has the means to automatically fragment and reassemble a message at a receiving node relieving the host application of this overhead.

At press time, there were over 600 certified products from 400 companies. The interoperability process has been fostered by the ZigBee Alliance. The ZigBee Alliance is a global ecosystem of 400+ companies in the M2M/IoT space developing standards and producing products for use in commercial building automation, consumer electronics, health care and fitness, home automation, energy management, retail management, and wireless telecommunications. The Alliance was established in October 2002 to create global standards to connect a wide range of devices into secure, low-cost, low-power, and easy-to-use wireless sensor and control networks. Nine interoperable standards published by the Alliance enable manufacturers to bring to market a variety of energy management, commercial, and consumer application products.

LR-WPANs applications require a low-cost, small-size, highly reliable technology which offers long battery life, measured in months or even years, and automatic or semiautomatic installation. The IEEE 802.15.4 standard supports these requirements by trading off higher speed and performance for architectures that benefit from low-power consumption and low cost. ZigBee is a low-power wireless specification that introduces mesh networking to the low-power wireless space and is targeted toward applications such as smart meters, home automation, and RC units. ZigBee technology provides reasonably efficient low-power connectivity and ability to connect a large number of devices into a single network. Some studies have shown that for the home, two wireless PHY layer communications technologies that best meet the overall performance and cost requirements are Wi-Fi (802.11/n) and ZigBee (802.15.4) (20). 6LoWPAN, discussed in Chapter 9, makes use of the IEEE 802.15.4 PAN structure. Other researchers, however, argue that ZigBee’s relative complexity (as seen in the protocol stack of Fig. 6.2) and the apparent fact that the power consumption of ZigBee devices is higher than the consumption of some alternatives (e.g., BLE) tend to make ZigBee not always the most ideal solution *for unmaintained devices that need to operate for extensive periods of time from a limited power source*; hence, while many home applications make ideal use of ZigBee, other IoT/M2M applications can also be supported by other approaches.

The PHY layer of the reference model specifies the network interface components, their parameters, and their operation. To support the operation of the MAC layer, the PHY layer includes a variety of features, such as receiver energy detection (RED), link quality indicator (LQI), and clear channel assessment (CCA). The PHY layer is also specified with a number of operational low-power features, including low-duty cycle operations, strict power management, and low transmission overhead. IEEE 802.15.4 defines several addressing modes: it allows the use of either IEEE 64-bit extended addresses or (after an association event) 16-bit addresses unique within the PAN. The MAC layer handles network association and disassociation. It also regulates access to the medium; this is achieved through two modes of operation, namely beaconing and nonbeaconing. The beaconing mode is specified for environments where control and data forwarding is achieved by an always active device. The nonbeaconing mode specifies the use of unslotted, nonpersistent CSMA-based MAC protocol. The network layer provides the functionality required to support network routing capabilities, configuration and device discovery, association and disassociation, topology management, MAC layer management, and routing and security management. Three network topologies, namely star, mesh, and cluster tree, are supported. The security layer leverages the basic security services specified by the IEEE 802.15.4 security model to provide support for infrastructure security and application data security. The application layer consists of the application support sublayer (APS), the ZigBee device object (ZDO), and the manufacturer-defined application objects. The responsibilities of the APS sublayer include maintaining tables for binding devices together, based on their services and their needs, and forwarding messages between bound devices. Refer to Table 6.3 for some technical parameters of this technology.

ZigBee channels are similar to those for BLE in that they are 2 MHz wide; however, they are separated by 5 MHz, thus wasting spectrum, to some degree. ZigBee is not a frequency-hopping technology; therefore, it requires careful planning during deployment in order to ensure that there are no interfering signals in the vicinity (5). The design of the PHY layer is driven by the need for low-cost, power-effective PHY layer for cost-sensitive, low data rate monitoring and control applications. Under IEEE 802.15.4, wireless links can operate in three unlicensed frequency bands, already identified above, namely in the 858 MHz band, in the 902-to-928 MHz band, and in the 2.4 GHz band. Based on these frequency bands, the IEEE 802.15.4 standard defines three physical media (14):

- Direct sequence spread spectrum (DSSS) using binary phase shift keying (BPSK), operating in the 868 MHz at a data rate of 20 Kbps;
- DSSS using BPSK, operating in the 915 MHz at a data rate of 40 Kbps; and
- DSSS using offset quadrature phase shift keying (O-QPSK), operating in the 2.4 GHz at a data rate of 140 Kbps.

These operating frequency bands are depicted in Figure 6.3. The spreading code of the 868 MHz and the 915 MHz PHY layers is a 15-chip m-sequence. Both specifications use BPSK with differential encoding data modulation scheme. The data rate of 868 MHz layer is 20 Kbps, while the data rat of the 915 MHz specification is 40 Kbps. The resulting chip rate is 300 Kchips/s for the 868 MHz PHY layer and 600 Kchips/s for the 915 MHz PHY layer. The data modulation of the 2.4 GHz PHY layer is a 16-ary orthogonal modulation. Consequently, 16 symbols are orthogonal set of 32-chip Pseudorandom Noise (PN) codes. The resulting data rate is 250 Kbps (4 bits/symbol, 62.5 Ksymbols/s). The specification uses O-QPSK with half-sine pulse shaping, which is equivalent to minimum shift keying; the resulting chip rate is 2.0 Mchips/s.

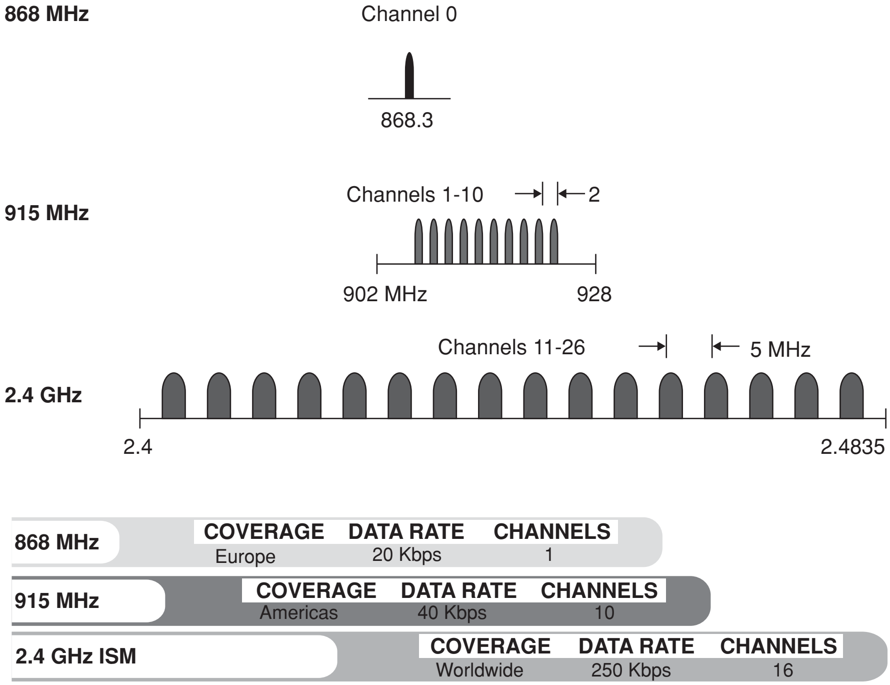


FIGURE 6.3 IEEE 802.15.4 PHY layer operating frequency bands.

IEEE 802.15.4 defines four types of frames: beacon frames, MAC command frames, acknowledgement frames, and data frames (see Fig. 6.4). As noted earlier, IEEE 802.15.4 networks can either be nonbeacon enabled or beacon enabled. The latter is an optional mode in which devices are synchronized by a so-called coordinator's beacons. This allows the use of superframes within which a contention-free guaranteed time service (GTS) is possible. In nonbeacon-enabled networks, data frames are sent via the contention-based channel access method of unslotted carrier sense multiple access/collision detect (CSMA/CD). In nonbeacon-enabled networks, beacons are not used for synchronization; however, they are still useful for link-layer device discovery to aid in association and disassociation events (21).

The packet structure of the IEEE 802.15.4 PHY layer is depicted in Figure 6.5. The first field of this structure contains a 32-bit preamble; this field is used for symbol synchronization. The next field represents the start of packet delimiter; this field of 8 bits is used for frame synchronization. The 8-bit PHY header field specifies the length of the PHY service data unit (PSDU). The PSDU field can carry up to 127 bytes of data.

In order to accommodate the MAC protocol, the IEEE 802.15.4 standard distinguishes devices based on their hardware complexity and capability. Accordingly, the standard defines two classes of physical devices, namely a full function device (FFD) and a reduced function device (RFD). These device types differ in their use and

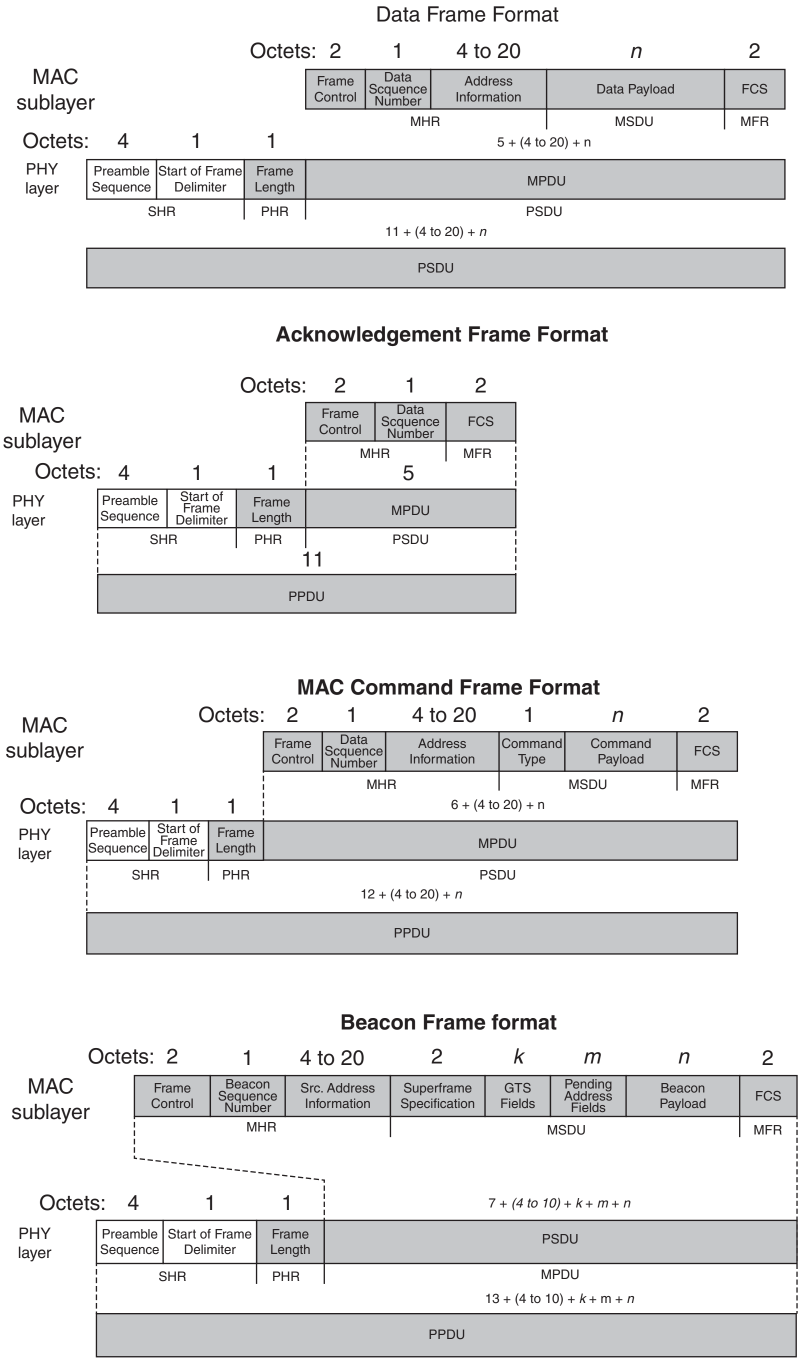


FIGURE 6.4 IEEE 802.15.4 frames.

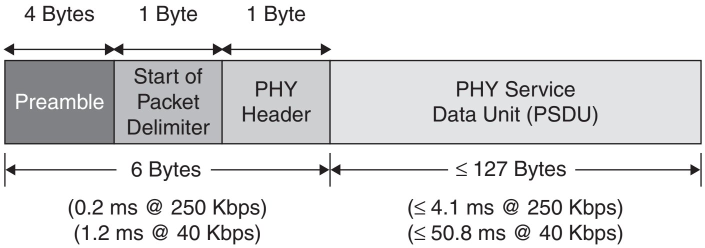


FIGURE 6.5 IEEE 802.15.4 PHY layer packet structure.

how much of the standard they implement. An FFD is equipped with the adequate resources and memory capacity to handle all the functionalities and features specified by the standard. It can, therefore, assume multiple network responsibilities; it can also communicate with any other network device. An RFD is a simple device that carries a reduced set of functionalities, for lower cost and complexity. It typically contains a physical interface to the wireless modem and executes the specified IEEE 802.15.4 MAC layer protocol. Furthermore, it can only associate and communicate with an FFD. Based on these physical device types, ZigBee defines a variety of logical device types. These logical devices are distinguished based on their physical capabilities and the role they play in the deployed network (14). There are three categories of logical devices:

- ***Network coordinator***: An FFD device responsible for network establishment and control. The coordinator is responsible for choosing key parameters of the network configuration and for starting the network. It also stores information about the network and acts as the repository for security keys.
- ***Router***: An FFD device that supports the data routing functionality, including acting as an intermediate device to link different components of the network and forwarding message between remote devices across multihop paths. A router can communicate with other routers and end devices.
- ***End Devices***: An RFD device that contains (just) enough functionality to communicate with its parent node, namely the network coordinator or a router. An end device does not have the capability to relay data messages to other end devices.

A PAN coordinator is the designated principal controller of the WPAN. Every network has exactly one PAN coordinator, selected from within all the coordinators of the network. A coordinator is a network device configured to support network functionalities and additional responsibilities, including:

- Managing a list of all associated network devices;
- Exchanging data frames with network devices and peer coordinator;

- Allocating 16-bit short addresses to network devices. The short addresses, assigned on-demand, are used by the associated devices in lieu of the 64-bit addresses for subsequent communications with the coordinator;
- Generating, on a periodic basis, beacon frames. These frames are used to announce the PAN identifier, the list of outstanding frames, and other network and device parameters.

Based on these logical device types, a ZigBee WPAN can be organized into one of three possible topologies, namely a star, a mesh (peer-to-peer), or a cluster tree. (See Fig. 6.6.) The *star* network topology supports a single coordinator, with up to 65,536 devices. In this topology configuration, one of the FFD-type devices assumes the role of network coordinator. All other devices act as end devices. The selected coordinator is responsible for initiating and maintaining the end devices on the network. Upon initiation, the end devices can only communicate with the coordinator. The *mesh* configuration allows path formation from any source device to any destination device, using tree- and table-driven routing algorithms. *Cluster-tree* networks enable a peer–peer network to be formed with a minimum of routing overhead, using multihop routing. The topology is suitable for latency-tolerant applications. A cluster-tree network is self-organized and supports network redundancy to achieve a high degree of fault resistance and self-repair. The cluster can be rather large, comprising up to 255 clusters of up to 254 nodes each, for a total of 64,770 nodes. It may also span large physical areas. Any FFD can be a coordinator. Only one coordinator is selected for the PAN. The PAN coordinator forms the first cluster and assigns to it a cluster identity (CID) of value 0. Subsequent clusters are then formed with a designated cluster head for each cluster.

Public application profiles are agreements for messages, message formats, and processing actions. Profiles enable developers to create interoperable, distributed application entities residing on separate devices. These applications (written by the device manufacturer) send commands, request data, and process commands and

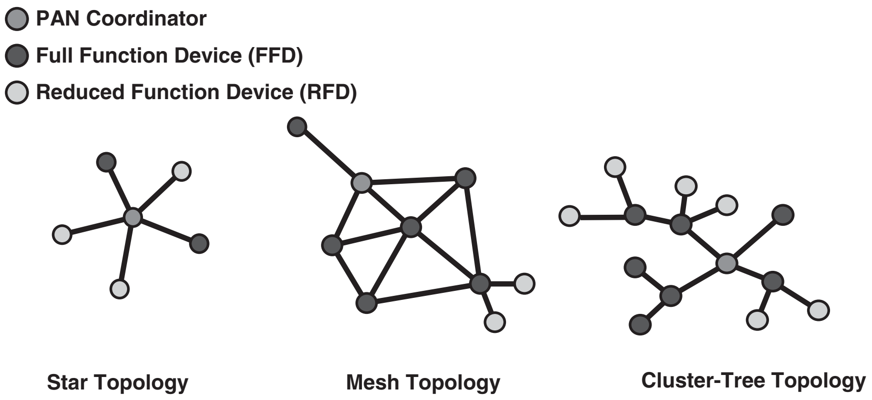


FIGURE 6.6 Network topologies.

requests over the ZigBee network. The ZDO represents a predefined base class of functionality upon which all applications are written. The ZDO creates an abstraction so that the developer can focus on writing application-specific code rather than dealing with the low-level details. The ZDO provides an interface between the application objects, the profile (e.g., the ZigBee Health Care), and the APS. The ZDO satisfies the common requirements of all applications operating in a ZigBee protocol stack. The ZDO is responsible for initializing the APS, the network layer, and the security service provider. Table 6.5 lists specific application standards defined and supported by ZigBee and the ZigBee Alliance.

Note: IEEE 802.15.4 mandates link-layer security based on Advanced Encryption Standard (AES), but it does not specify capabilities for bootstrapping, key management, and security at higher layers.

The ZigBee Alliance's focus on health care has resulted in the development of the ZigBee Health Care public application profile, also known as the PHHC Profile or simply the Medical Profile. ZigBee Health Care was designed for use by assistive devices operating in noninvasive health care. ZigBee Health Care provides an industry-wide standard for exchanging data between a variety of medical and nonmedical devices. The PHHC Profile supports secure monitoring and management of noncritical, low-acuity healthcare services in support of chronic disease management. This profile also provides support for IEEE 11073-conformant devices (e.g., glucometers, pulse oximeters, ECGs, blood pressure monitors, respirometers, weight scales, and thermometers). The ZigBee Health Care definitions are comprised of device specializations defined by IEEE, including IEEE 11073 device specializations of standards point-of-care medical device communication. One of the standards that are part of this family, the 11073–20601 standard, is a transport-independent, optimized exchange protocol. This standard forms the basis of the data exchanges between the devices that will support the PHHC Profile. This protocol provides methods for (i) establishing logical connections between devices, (ii) presenting the capabilities of devices, and (iii) servicing communication needs. In summary, the ZigBee Health Care public application profile fully supports ISO/IEEE 11073 for point-of-care medical device communication and provides support for additional devices. The ZigBee Health Care also supports all device specializations; device specializations for a number of medical devices already exist including the pulse oximeter, blood pressure monitor, pulse monitor, weight scale, and glucose meter (16, 17).

Earlier, we mentioned ZIP as an example of an IP-based stack (IPv6 in particular) that supports Zigbee. A typical ZIP product implementation would have parameters similar to these:

- ZigBee: ZigBee Pro compliant and Full ZigBee Smart Energy (SE) Profile support
- Radio: IEEE 802.15.4 compliant ZigBee radio
- Operating frequency: 2405–2483.5 MHz, supports ZigBee channels 11 to 26, 5 MHz spacing
- Receiver sensitivity: −95 dBm

TABLE 6.5 Application Standards Defined and Supported by ZigBee and the ZigBee Alliance

Standard	Application Description
ZigBee Building Automation (used for efficient commercial spaces)	ZigBee Building Automation offers a global standard for interoperable products enabling the secure and reliable monitoring and control of commercial building systems. It is the only BACnet®-approved wireless mesh network standard for commercial buildings
ZigBee Health Care (used for health and fitness monitoring)	ZigBee Health Care offers a global standard for interoperable products enabling secure and reliable monitoring and management of noncritical, low-acuity healthcare services targeted at chronic disease, aging independence and general health, and wellness and fitness. ZigBee Alliance has joined forces with the Continua Health Alliance, a nonprofit, open industry coalition of the finest healthcare and technology companies collaborating to improve the quality of personal health care. Continua has endorsed ZigBee Health Care as its low-power LAN standard in the Continua 2010 Design Guidelines
ZigBee Home Automation (used for smart homes)	ZigBee Home Automation offers a global standard for interoperable products enabling smart homes that can control appliances, lighting, environment, energy management and security, as well as the expandability to connect with other ZigBee networks
ZigBee Input Device (easy-to-use touchpads, mice, keyboards, wands)	ZigBee Input Device is a global standard for greener, innovative, and easy-to-use mice, keyboards, touchpads, wands, and other input devices used with computers and CE devices. This standard allows consumers to use their devices from greater distances or even from another room because operation is not limited to LOS. The standard operates with existing ZigBee Remote Control-equipped HDTVs, set-top boxes, and other devices and existing computers. ZigBee Input Device is a standard designed specifically for the ZigBee RF4CE specification
ZigBee Light Link (LED lighting control)	ZigBee Light Link gives the lighting industry a global standard for interoperable and very easy-to-use consumer lighting and control products. It allows consumers to gain wireless control over all their LED fixtures, light bulbs, timers, remotes, and switches. Products using this standard will let consumers change lighting remotely to reflect ambiance, task, or season, all while managing energy use and making their homes greener. Since ZigBee Light Link is a ZigBee standard, lighting products will interoperate effortlessly with products using other ZigBee standards already in consumers' homes, including ZigBee Home Automation, ZigBee Input Device, ZigBee Remote Control, and ZigBee Health Care

(*continued*)

TABLE 6.5 (*Continued*)

Standard	Application Description
ZigBee network devices (assist and expand ZigBee networks)	ZigBee network device is the category for device specific standards designed to assist and expand ZigBee PRO-based networks. These universal devices can work on just about any ZigBee PRO network; they also work with most ZigBee standards. ZigBee Gateway is the first standard to join this category, and work is underway to develop standards for bridge and range extender devices. ZigBee Gateway makes it easy to connect Internet-based service provider systems with ZigBee users everywhere, allowing them both to take advantage of cost and energy efficiencies. This standard complements a number of ZigBee standards using the ZigBee PRO specification: (i) ZigBee Building Automation; (ii) ZigBee Health Care; (iii) ZigBee Home Automation; (iv) ZigBee Retail Services; (v) ZigBee SE; and (vi) ZigBee Telecom Services
ZigBee Remote Control (used for advanced RCs)	ZigBee Remote Control provides a global standard for advanced, greener, and easy-to-use RF remotes that remove LOS restrictions while also delivering two-way communication, longer range of use, and extended battery life. It was designed for a variety of CE devices including HDTV, home theater equipment, set-top boxes, and other audio equipment
ZigBee Retail Services (used for smarter shopping)	ZigBee Retail Services is a global standard of interoperable products to monitor, control, and automate the purchase and delivery of goods. It will also help retailers' manage their supply chain. ZigBee Retail Services will support a fully integrated ecosystem of technology suppliers, merchants, distribution centers, and both residential and commercial consumers in providing a standard way to purchase, fulfill, automate, and monitor the purchase and delivery of goods
ZigBee Smart Energy (SE) (used for home energy savings)	ZigBee SE is a leading standard for interoperable products that monitor, control, inform, and automate the delivery and use of energy and water. It helps create greener homes by giving consumers the information and automation needed to easily reduce their consumption and save money, too. ZigBee SE version 1.1, the newest version for product development, adds several important features including dynamic pricing enhancements, tunneling of other protocols, prepayment features, over-the-air updates, and guaranteed backward compatibility with certified ZigBee SE products version 1.0. All ZigBee SE products are ZigBee certified to perform regardless of manufacturer, allowing utilities and consumers to purchase with confidence. Every product needed to implement a robust ZigBee SE HAN is available. These products make it easy for utilities and governments to deploy smart grid solutions that are secure, easy to install, and consumer friendly

(*continued*)

TABLE 6.5 (*Continued*)

Standard	Application Description
	SE Profile version 2.0 was under development at press time, in cooperation with a number of other standard development groups. SE 2.0 offers IP-based control for AMI and HANs; the IP-based protocol is used to monitor, control, and automate the delivery and use of energy and water. This version will not replace ZigBee SE version 1, rather it will offer utilities and energy service providers another choice when creating their AMI and HANs. In addition to all the services and devices found in ZigBee SE version 1, version 2.0 will feature control of PEV charging, installation, configuration and firmware download for HAN devices, prepay services, user information and messaging, load control, demand response and common information, and application profile interfaces for wired and wireless HANs. Development partners include HomeGrid, HomePlug Powerline Alliance, International Society of Automative Engineers SAE International, IPSO Alliance, SunSpec Alliance, and the Wi-Fi Alliance On August 25, 2012, the Alliance closed the final public comment period on the latest draft 0.9 version of the Draft Standard (public application profile) and supporting documents. This was the final comment period because SE Profile 2 development is nearly complete. Public and member comments will be integrated to produce a final version 1 of the standard
ZigBee Telecom Services (used for value-added services)	ZigBee Telecom Services offers a global standard for interoperable products enabling a wide variety of value-added services, including information delivery, mobile gaming, location-based services, secure mobile payments, mobile advertising, zone billing, mobile office access control, payments, and peer-to-peer data-sharing services. This single standard offers an affordable and easy way to introduce innovative new services that touch almost everyone using mobile phones and other portable electronic devices. It offers a variety of value-added services for mobile phone network operators, retailers, businesses, and governments

Source: ZigBee Alliance.

- Transmitter power: +18 dBm output power (<100 mW)
- Ethernet and TCP/IP specifications:
  - Ethernet 10/100 base TX with auto negotiation
  - Supports standard socket-based communications
  - Protocols supported: IPv6, UDP, TCP, Telnet, ICMP, ARP, DHCP, BOOTP, Auto IP, HTTP, SMTP, TFTP, HTTPS, SSH, SSL, FTP, PPP, SNMP
  - Encryption: end-to-end AES 128-bit encryption, 3DES and RC4 encryption for SSH and SSL
  - Authentication: SHA-1, MD5

It should be noted that ZigBee and Bluetooth protocols are substantially different and are designed for different purposes: ZigBee is designed for low-to-very-low-duty cycle static and dynamic environments with many active nodes; Bluetooth, on the other hand, is designed for high QoS, variety of duty cycles, and moderate data rates in networks with limited active nodes.

6.1.2 Radio Frequency for Consumer Electronics (RF4CE)

The specialty-use-driven ZigBee RF4CE protocol has been designed for simple, two-way device-to-device control applications that do not require the full-featured mesh networking capabilities offered by ZigBee 2007. ZigBee RF4CE offers lower memory size requirements, thereby enabling lower cost implementations.

RF4CE is based on ZigBee and was standardized in 2009 by four consumer electronics (CE) companies: Sony, Philips, Panasonic, and Samsung.

The ZigBee RF4CE specification defines an RC network that defines a simple, robust, and low-cost communication network allowing wireless connectivity in applications for CE devices. The ZigBee RF4CE specification enhances the IEEE 802.15.4 standard by providing a simple networking layer and standard application layer that can be used to create a multivendor interoperable solution for use within the home. Some of the characteristics of ZigBee RF4CE include the following (16):

- Operation in the 2.4 GHz frequency band according to IEEE 802.15.4;
- Frequency agile solution operating over three channels;
- Incorporates power-saving mechanisms for all device classes;
- Discovery mechanism with full application confirmation;
- Pairing mechanism with full application confirmation;
- Multiple star topology with inter-PAN communication;
- Various transmission options including broadcast;
- Security key generation mechanism;
- Utilizes the industry standard AES-128 security scheme;
- Specifies a simple RC control profile for CE products;
- Support alliance-developed standards or manufacturer-specific profiles.

RF4CE's intended use is as a device RC system, for example for television set-top boxes. The intention is that it overcomes the common problems associated with infrared (IR): interoperability, line-of-sight (LOS), and limited enhanced features (5). At least wo-chip vendors supported RF4CE as of press time: Texas Instruments and Freescale Semiconductor, Inc.

6.1.3 Bluetooth and its Low-Energy Profile

6.1.3.1 Overview Bluetooth is a WPAN technology based on IEEE 802.15.1. It is a specification for short-range wireless connectivity for portable personal devices, including computer peripherals. It is now one of the most popular technologies in consumer electronics. Bluetooth was initially developed by Ericsson; in the late 1990s, the Bluetooth Special Interest Group (SIG) made their specifications publicly available. Soon thereafter, the IEEE 802.15 Group took the Bluetooth work and developed a vendor-independent standard. The Bluetooth SIG, in conjunction with the IEEE, has managed enhancements of the basic standard over the years. Bluetooth has evolved through four versions (see Table 6.6); all versions of the Bluetooth standards maintain downward compatibility. The Bluetooth SIG has approximately 17,000 member companies in telecommunication, computing, and CE.

TABLE 6.6 Versions of Bluetooth

Version	Description
Bluetooth v1.0 and v1.0B	Original versions; had limited interoperability
Bluetooth v1.1	This is original IEEE Standard 802.15.1–2002
Bluetooth v1.2	Ratified as IEEE Standard 802.15.1–2005. Incorporates a number of enhancements compared with v1.1 including (i) faster connection and discovery; (ii) use of AFH spread spectrum; (iii) supports higher transmission speeds up to 721 Kbps; and (iv) adds flow control mechanisms
Bluetooth v2.0 + EDR	Published in 2004. Incorporates a number of enhancements compared with v1.1 including faster data transfer of about 3 Mbps and lower power consumption through a reduced duty cycle. Note: To be exact, Version 2.0 devices have a higher power consumption; however, the fact that the transmission rate is three times faster (thereby reducing the transmission burst times), effectively reduces consumption to half that of 1.x devices
Bluetooth v2.1 + EDR	Published in July 2007. This release adds secure simple pairing (SSP), which improves the pairing process for Bluetooth devices while improving security; it also incorporates a subrating mechanism that reduces the power consumption in low-power mode
Bluetooth v3.0 + HS	Published in April 2009. This release supports a theoretical data transfer speeds of up to 24 Mbps by using the Bluetooth link for negotiation and establishment of a session for high data rate traffic carried over a collocated 802.11 link. It adds alternate MAC/PHY (AMP) for the use of 802.11 as a HS transport. Note: The HS portion of the specification is not mandatory, and only devices with the "+HS" label actually support the Bluetooth over 802.11 HS data transfer. The enhanced power control feature updates the power control feature to remove the open loop power control and also to clarify ambiguities in power control as related to EDR
Bluetooth v4.0	Published in June 2010. This version includes *Classic Bluetooth*, *Bluetooth high speed*, and BLE protocols. Bluetooth high speed is based on Wi-Fi and Classic Bluetooth consists of legacy Bluetooth protocols

Bluetooth is a short-range data exchange communication protocol widely used in cellular phones, smartphones, tablets, and PDAs (has a range of about 10 m, or a maximum of 100 m with power boost). Bluetooth is designed for a small variety of tasks, such as synchronization, voice headsets, cell-modem calls, and mouse and keyboard input. The Bluetooth specification defines a low-power, low-cost technology that provides a standardized platform for eliminating cables between mobile devices and facilitating connections between products.

Bluetooth operates in the 2.4-GHz ISM band and has a bandwidth of approximately 1–3 Mbps (newer version support higher speeds). Bluetooth uses frequency-hopping spread spectrum. While the cost of Bluetooth equipment is significantly lower than the cost of WLAN, the transmission range of 10 m or less and the data transfer rate 12 Mbps or less (in Version 2.0 of the standard) are often considered a drawback. By comparison, EEE 802.11a/b/g/n is a collection of related technologies that operate in the 2.4-GHz ISM band, the 5-GHz ISM band, and the 5-GHz U-NII bands; it provides the highest power and longest range of the common unlicensed wireless technologies. Transmission data rates can reach 54 Mbps (twice as much with the latest 802.11n protocol). Typically, hardware implementation of some or all of 802.11 protocols comes preinstalled on most new laptop computers; the technology is often also available for PDAs and cellular phones. Also by comparison, the IEEE 802.15.4 (ZigBee) standard supports a maximum data rate of 250 Kbps, with rates as low as 20 Kbps; however, it has the lowest power requirement of the group: ZigBee devices are designed to run several years on a single set of batteries, making them ideal candidates for unattended or difficult-to-reach locations. See Table 6.7.

The sublayers of IEEE 802.15 are as follows: (i) RF layer; (ii) baseband layer; (iii) the link manager (an MAC-level protocol); and (iv) the logical link control and adaptation protocol (L2CAP) (also an MAC-level protocol). Bluetooth is designed for high QoS applications, a variety of duty cycles, and moderate data rates in networks with limited active nodes. Compared with WLANs, Bluetooth is limited as a transmission technology in terms of both bandwidth and distance. The functionality of the layers is as follows:

- **RF layer**: The air interface is based on antenna power range starting from 0 dBm up to 20 dBm, 2.4 GHz band, and the link range from 0.1 to 10 m.
- **Baseband layer**: The baseband layer establishes the Bluetooth *piconet*. The piconet is formed when two Bluetooth devices connect. In a piconet, one device acts as the master and the other devices act as slaves.
- **Link manager**: The link manager establishes the link between Bluetooth devices. Additional functions include security, negotiation of Baseband packet sizes, power mode and duty cycle control of the Bluetooth device, and the connection states of a Bluetooth device in a piconet.
- **L2CAP**: This sublayer provides the upper-layer protocols with connectionless and connection-oriented services. The services provided by this layer include protocol multiplexing capability, segmentation and reassembly of packets, and group abstractions.

TABLE 6.7 Wireless Protocol Comparison

IEEE Standard Property	802.11 WLANs	802.15.1/ Bluetooth	802.15.4/ ZigBee
Battery life measured in:	Minutes to hours	Hours to days	Days to years
Data throughput	• 802.11a: up to 54 Mbps • 802.11b: up to 11 Mbps • 802.11g: up to 54 Mbps • 802.11n: up to 150 Mbps (at 40 MHz operation at 5 GHz) • 802.11ac: up to 867 Mbps (160 MHz operation at 5 GHz)	~1 Mbps (Version 1) to 3 Mbps (Version 2)	~0.25 Mbps
Power consumption	Medium	Low	Very low
Range	~250 m (this figure is for 802.11n, otherwise ~100 m) Note: IEEE 802.11y-2008 extended operation of 802.11a to the licensed 3.7 GHz band (co-primary basis in the 3650 to 3700 MHz band in the U.S. band); this increased power limits allow a range up to 5000 m. This band has traditionally been used for satellite communications and is known as the C-band	~10 to 100 m	~10 m

BLE (originally known as WiBree and/or Bluetooth ultra low power [ULP][7]) is a low-power subset to Bluetooth v4.0, with an entirely new protocol stack for rapid build-up of simple links. BLE is an alternative to the "power management" features that were introduced in Bluetooth v1.0 to v3.0 as part of the standard Bluetooth protocols. BLE is aimed at very low-power applications running off a coin cell: it is capable of reporting data from a sensor for up to a year from a small button battery without recharging. Although the BLE data rate and radio range are lower than the same metrics in classic Bluetooth, the low-power and long battery life make it suitable for short-range monitoring applications in medicine. BLE sensor devices are typically required to operate for many years without needing a new battery; they commonly use a coin cell, for example, the popular CR2032 (22). The aim of the BLE technology is to enable power-sensitive devices to be permanently connected to the Internet. BLE per se is primarily aimed at mobile telephones, where it is envisaged

[7] BLE started as a project in the Nokia Research Centre with the name Wibree. In 2007, the technology was adopted by the Bluetooth SIG and renamed Bluetooth ultra low power; later, it was renamed Bluetooth low energy.

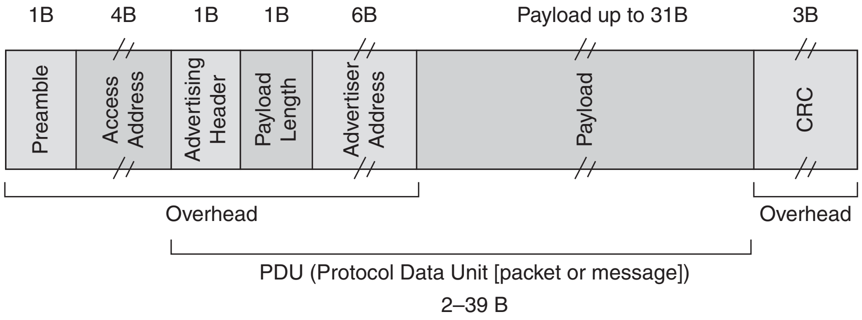


FIGURE 6.7 BLE packet.

that a star network topology, similar to Bluetooth, will often be created between the phone and an ecosystem of other devices.

Figure 6.7 depicts the BLE packet, while Figure 6.8 shows the frequency plan. Current chip designs allow for two types of implementation—dual mode and single mode. In a single-mode implementation, the BLE protocol stack is implemented solely. In a dual-mode implementation, BLE functionality is integrated into an existing Classic Bluetooth controller. Most new Bluetooth chipsets from leading Bluetooth silicon manufacturers are expected to support Bluetooth and the new BLE functionality; a number of companies had announced support of BLE by press time, including Broadcom and Texas Instruments.

As implied in Figure 6.8, there are some coexistence scenarios in a corporate setting, in a home, or in a small office home office (SOHO) where Wi-Fi is used. The IEEE 802.11b and 802.11g specifications postulate a partitioning of the spectrum into 14 overlapping, staggered channels whose center frequencies are 5 MHz apart; within this partitioning of the ISM spectrum, channels 1, 6, and 11 (and, if available in the regulatory domain, channel 14) do not overlap. These channels (or other sets with similar gaps) can be used so that multiple networks can operate in close proximity without interfering with each other. See Figure 6.9. The spectral mask for 802.11b requires that the signal be at least 30 dB down from its peak energy at ±11 MHz from the center frequency and at least 50 dB down from its peak energy at ±22 MHz from the center frequency. Note that if the transmitter is sufficiently powerful, the signal can be quite strong even beyond the ±22 MHz point (e.g., a powerful transmitter on channel 6 can easily overwhelm a weaker transmitter on channel 11); in most situations, however, the signal in a given channel is sufficiently attenuated to minimally interfere with a transmitter on any other channel. Each BLE channel is 2 MHz wide, but the spacing and placement of ZigBee channels implies that only four channels are likely to be free in the presence of average Wi-Fi network settings (typically, channels 1, 6, and 11 are defaults). With an on-air signaling data rate of only 250 Kbps and the inability to implement hopping, ZigBee is at risk of nondelivery of its packets; BLE, on the other hand, makes much more efficient use of the spectrum and employs adaptive frequency hopping (AFH) as proven by

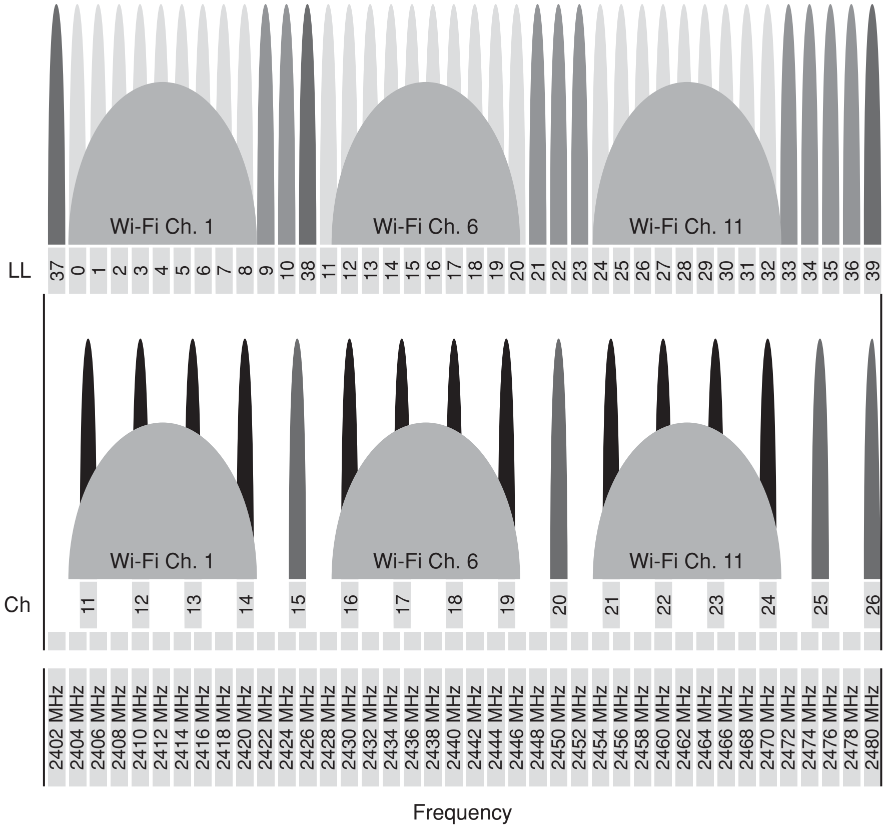
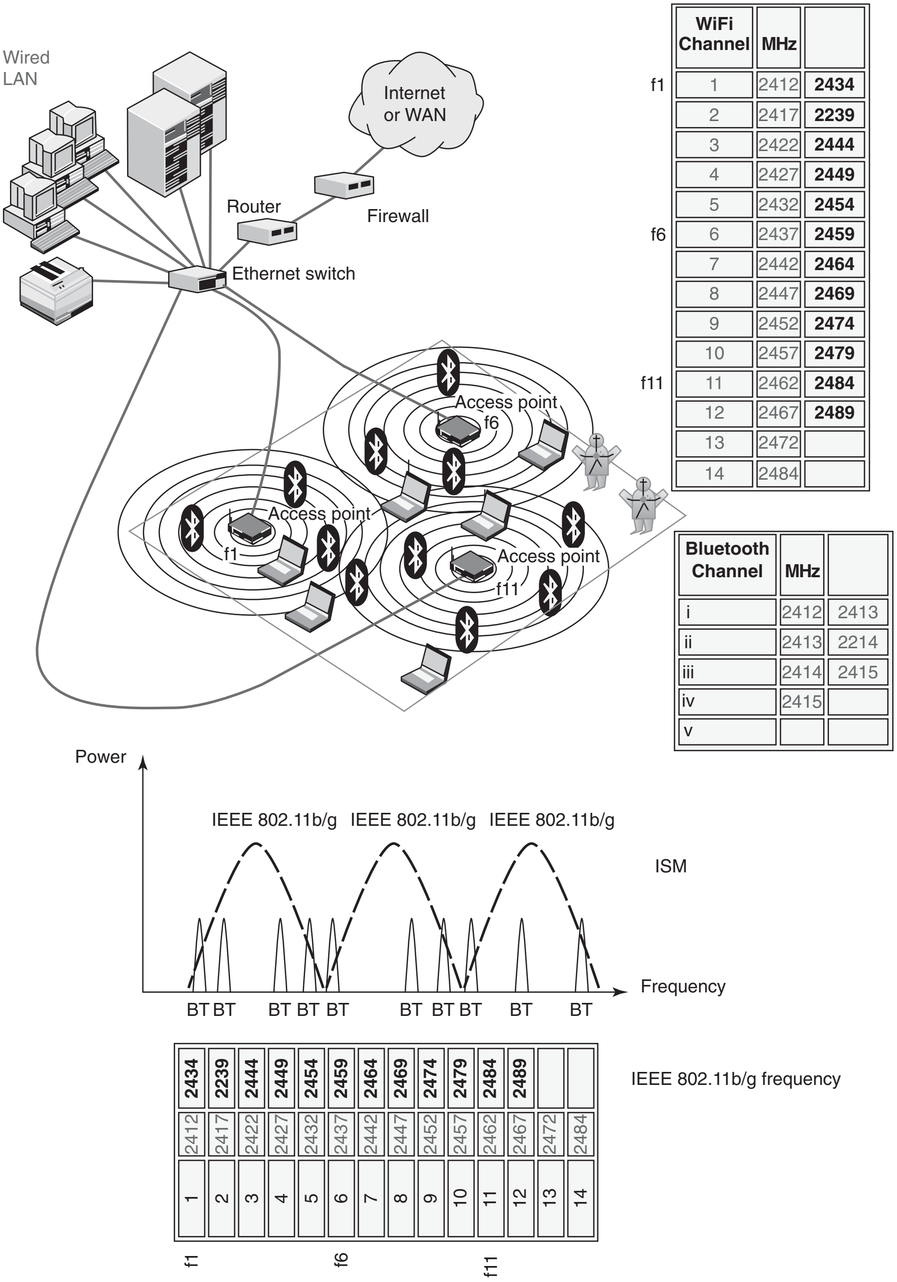


FIGURE 6.8 Frequency spectrum. Top: BLE channel allocations (each channel is 2 MHz wide). Bottom: ZigBee channel allocations (each channel is 2 MHz wide but there is a 5 MHz spacing; in the presence of a multichannel Wi-Fi, only four channels may actually to be available).

Bluetooth. As noted earlier, a device that operates Bluetooth v4.0 may not necessarily implement other versions of Bluetooth; in such cases, it is known as a single-mode device (5).

In the recent past, Bluetooth was used in health care mostly just for interconnection of various medical apparatus. The situation is changing with the development of the Bluetooth Health Device Profile (HDP). Under Bluetooth, a profile defines the characteristics and features including function of a Bluetooth system. The HDP is used for connecting application data source devices such as blood pressure monitors, weight scales, glucose meters, thermometers, and pulse oximeters to application data sink devices such as mobile phones, laptops, desktop computers, and health appliances without the need for cables. This profile can be combined with BLE to make sure that medical devices can be in the operational conditions for many months and even years (3). The topic is revisited below.



	WiFi Channel	MHz	
f1	1	2412	**2434**
	2	2417	**2239**
	3	2422	**2444**
	4	2427	**2449**
	5	2432	**2454**
f6	6	2437	**2459**
	7	2442	**2464**
	8	2447	**2469**
	9	2452	**2474**
	10	2457	**2479**
f11	11	2462	**2484**
	12	2467	**2489**
	13	2472	
	14	2484	

Bluetooth Channel	MHz	
i	2412	2413
ii	2413	2214
iii	2414	2415
iv	2415	
v		

2434	**2239**	**2444**	**2449**	**2454**	**2459**	**2464**	**2469**	**2474**	**2479**	**2484**	**2489**		
2412	2417	2422	2427	2432	2437	2442	2447	2452	2457	2462	2467	2472	2484
1	2	3	4	5	6	7	8	9	10	11	12	13	14
f1					f6					f11			

FIGURE 6.9 IEEE 802.11b/g frequency bands, typical topology, and Bluetooth interaction.

6.1.3.2 Details As noted, Bluetooth is a specification for short-range RF-based connectivity for portable personal devices. The specification originally started out as a de facto industry standard; more recently, the IEEE Project 802.15.1 developed a wireless PAN standard based on the Bluetooth v1.1 Foundation Specifications. The IEEE 802.15.1 standard was published in 2002. Bluetooth is principally directed to the support of personal communication devices such as telephones, printers, headsets, PC keyboards/mice, etc. The technology has restricted performance characteristics by design; hence, its applicability to WSN is rather limited in most cases.

As part of its effort, the IEEE has reviewed and provided a standard adaptation of the Bluetooth Specification v1.1 Foundation MAC (L2CAP, LMP, and baseband) and PHY (radio). Also specified is a clause on service access points (SAPs) that includes an LLC/MAC interface for the ISO/IEC 8802-2 LLC. A Protocol Implementation Conformance Statement (PICS) proforma has been developed. Also specified is an informative high-level behavioral ITU-T Z.100 specification and description language (SDL) model for an integrated Bluetooth MAC sublayer (23).

The system uses omnidirectional radio waves that can transmit through walls and other nonmetal barriers. Unlike other wireless standards, the Bluetooth wireless specification includes both link-layer and application layer definitions for product developers. Radios that comply with the Bluetooth wireless specification operate in the unlicensed, 2.4-GHz ISM radio spectrum ensuring communication compatibility worldwide.

Bluetooth radios use a spread spectrum, frequency-hopping, full-duplex signal. While point-to-point connections are supported, the specification allows up to seven simultaneous connections to be established and maintained by a single radio (24). AFH available with newer versions allows for better graceful coexistence with IEEE 802.11 WLAN systems. The signal hops among 79 frequencies at 1 MHz intervals to give an acceptable degree of interference immunity between multiple Bluetooth devices and between a Bluetooth device and a WLAN device (at least in the case where not all the available frequencies are used by the WLAN—this is likely the case in a SOHO environment where only one or two access points are used at a location). Refer again to Figure 6.9. In order to minimize interference with other protocols that use the same band, the protocol can change channels up to 1600 times per second. If there is interference from other devices, the transmission does not stop, but its speed is downgraded.

Bluetooth version 1.2 allowed a maximum data rate of 1 Mbps; this results in an effective throughput of about 723 Kbps. In late 2004, a new version of Bluetooth, known as Bluetooth Version 2, was ratified; among other features, it included EDR. With EDR, the maximum data rate is able to reach 3 Mbps (throughput of 2.1 Mbps) within a range of 10 m (up to 100 m with a power boost). Older and newer Bluetooth devices can work together with no special effort (25). Because a device such as a telephone headset can transmit the same information faster with Bluetooth 2.0+EDR, it will use less energy since the radio is on for shorter periods of time. The data rate is improved by more efficient coding of the data sent across the air; this also means that for the same amount of data, the radio will be active less of the time, thus reducing the power consumption (24). Newer Bluetooth devices are efficient at using small amounts of power when not actively transmitting: for example, the headset is able to burst two to three times more data in a transmission; it is able to sleep longer between transmissions. Noteworthy features of Bluetooth Core Specification Version 2.0 + EDR include:

- Three times faster transmission speed compared with pre-existing technology
- Lower power consumption through reduced duty cycle
- Simplification of multilink applications due to increased available bandwidth
- Backward compatibility to earlier versions
- Improved BER (bit error rate) performance

In the recent past, hardware developers were shifting from Bluetooth 1.1 to Bluetooth 1.2 and then Bluetooth 2.0. To be exact, Version 2.0 devices have a higher power consumption; however, the fact that the transmission rate is three times faster (thereby reducing the transmission burst times) effectively reduces consumption to half that of 1.x devices.

Devices are able to establish a trusted relationship; a device that wants to communicate only with a trusted device can cryptographically authenticate the identity of the other device. Trusted devices may also encrypt the data that they exchange over the air.

A Bluetooth device playing the role of “master” can communicate with up to seven devices playing the role of “slave” (these groups of up to eight devices are called piconets). At any given instant in time, data can be transferred between the master and one slave; but the master switches rapidly from slave to slave in a round-robin fashion. (Simultaneous transmission from the master to multiple slaves is possible, but not used much in practice.) The Bluetooth specification also allows connecting two or more piconets together to form a scatternet, with some devices acting as a bridge by simultaneously playing the master role in one piconet and the slave role in another piconet.

6.1.3.3 Bluetooth HDP Until recently, Bluetooth systems for medical application made use of proprietary implementations and data format; typically applications are placed on top of the serial port profile (SPP); however, they were not interoperable across vendors. To address the interoperability issue, the Bluetooth SIG started a program several years ago to define a new medical application, and in 2008 it released the HDP elluded to earlier.

The end result of this work was the HDP specification that included the multichannel adaptation protocol (MCAP) and that made use of the device ID (DI) profile. Figure 6.10 describes the architecture of a Bluetooth system with the HDP and applications. Table 6.8 describes the key components (26). HDP provides several critical features; these include control channel connection/disconnection, data link creation (reliable or streaming), data link deletion, data link abort, data link reconnection, data transmission (over one or more data links), and clock synchronization.

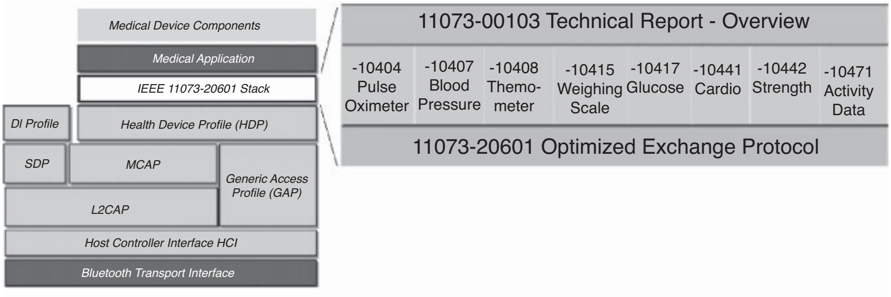

Medical Device Components
Medical Application
IEEE 11073-20601 Stack
DI Profile
Health Device Profile (HDP)
SDP
MCAP
Generic Access Profile (GAP)
L2CAP
Host Controller Interface HCI
Bluetooth Transport Interface
11073-00103 Technical Report - Overview
-10404 Pulse Oximeter
-10407 Blood Pressure
-10408 Themo-meter
-10415 Weighing Scale
-10417 Glucose
-10441 Cardio
-10442 Strength
-10471 Activity Data
11073-20601 Optimized Exchange Protocol

FIGURE 6.10 Bluetooth protocol and a HDP in a medical device application.

TABLE 6.8 Description of the HDP Functional Blocks

Functional Block	Description
Medical application	Describes the actual device application, including its user interface, application behavior, and integration layer to the IEEE 11073-20601 stack implementation
IEEE 11073-20601	Stack performs building, transmission, reception, and parsing of IEEE PDU packets for the associated agent/manager being developed. This component will directly link to the HDP
DI profile	Bluetooth profile designed to provide device-specific information through the use of the service discovery protocol (SDP). If vendor-specific information is required as part of a particular medical device, this profile provides specific behavior to acquire this information. A good HDP implementation offers APIs to register and query for such vendor-specific information. These APIs can then be integrated directly into the medical application
HDP	The core Bluetooth profile designed to facilitate transmission and reception of medical device data. The APIs of this layer interact with the lower-level MCAP layer, but also perform SDP behavior to connect to remote HDP devices
SDP	The discovery protocol used by all Bluetooth profiles to register and/or discover available services on remote devices so that connections over L2CAP can be established
MCAP	Used by HDP and facilitates the creation of a communications link (MCL) for exchanging generic commands, and also one or more data links (MDL) to transfer actual medical device data. MCAP is specific for the HDP and guarantees reliable transmission of data
Generic access profile (GAP)	Describes the required features of all core Bluetooth profiles including inquiry, connection, and authentication procedures
L2CAP	Supports protocol multiplexing, packet segmentation and reassembly, QoS, retransmission, and flow control for the Bluetooth packets transmitted through MCAP
Host controller interface (HCI)	Describes the commands and events that all Bluetooth hardware implementations (controllers) can understand
Bluetooth transport interface	Describes the UART, USB, SDIO, three-wire, ABCSP, etc. transport interface to the actual Bluetooth hardware components being used. Typically, UART and USB are the most widely used transports

HDP devices act as sinks and/or sources. A source is the small device that will act as the transmitter of the medical data (weight scale, glucose meter, thermometer, etc.). The sink is the feature-rich device that will act as the receiver of the medical data (mobile phone, desktop computer, health appliances, etc.). HDP devices acting as a source device are weight scales, blood pressure meters, thermometers, or glucose meters which transmit application data over a reliable data channel to a sink (PC, mobile phone, or PDA). Other source devices such as pulse oximeter, EEG, or ECG transmit application data over a streaming data channel to a sink (PC, mobile phone, or PDA). Multiple source devices transmit application data over reliable and streaming data channels to a sink. This data can then be routed on to a physician through an alternate transport (e.g., the Internet or a mobile phone network) to a medical server application at a hospital. A source device may be a combination device (pulse oximeter with thermometer capability) utilizing multiple data channels (26).

HDP does not define the data format and data content. The Bluetooth SIG requires for HDP the usage of the IEEE 11073-20601 Personal Health Device Communication Application Profile as the only allowed protocol for data exchange between HDP devices and the IEEE 11073-104xx Device Specification. IEEE 11073-20601 defines the data exchange protocol and IEEE 11073-104xx defines the data format including size and coding of all data exchanged between HDP devices. The data exchange protocol includes services for a reliable communication, mechanism for event reporting, object access via GET/SET, and the domain information (object-oriented description with attributes for the device configuration). Device description and attribute definitions are using ASN.1. Refer again to Figure 6.10 for the architecture of a Bluetooth device with IEEE 11073-20601 and device specifications with IEEE 11073 (-104xx). The length of transmitted data is in most cases 896 bytes for transmit and 224 bytes for receive. The exception is the oximeter (transmit: 9216 bytes; receive: 256 bytes).

6.1.4 IEEE 802.15.6 WBANs

At press time, the IEEE 802.15 Task Group (TG) 6 was in the process of developing a communication standard optimized for low-power devices and operation on, in, or around the human body (but nonetheless not limited to humans) to serve a variety of applications including medical, CE/personal entertainment, and others. The technology is intended to support low-power in-body/on-body nodes to serve a variety of medical and nonmedical applications. The IEEE TG postulated that for a successful implementation of WBAN, a standard model was required, which would be able to address both medical and CE applications.

The IEEE 802.15 TG6 was formed in November 2007 and begun operations as TG6 in January 2008. It had received 34 proposals, which were merged into a single candidate proposal. A draft of the standard was developed in March 2009. The draft has undergone significant editing and underwent five Letter Ballots; the last was Letter Ballot 79. On July 22, 2011, the draft was approved to start Sponsor Ballot. The standard defines an MAC layer supporting several PHY layers.

The selection of the PHYs (frequency bands) was an important issue.[8] Generally, the available frequencies for WBANs are regulated by communication authorities in different countries. Medical Implant Communication Service (MICS) band is a licensed band used for implant communication and has the same frequency range (402–405 MHz) in most of the countries. Wireless Medical Telemetry Services (WMTS) is a licensed band used for medical telemetry system. Both MICS and WMTS bandwidths do not support high data rate applications. The ISM band supports high data rate applications and is available worldwide. However, there are high chances of interference as many wireless devices including IEEE 802.1 and IEEE 802.15.4 operate at ISM band. The current IEEE 802.15.6 standard defines three PHY layers as follows: the narrowband (NB) layer, the ultra wideband (UWB) layer, and the human body communications (HBC) layer. The selection of each PHY depends on the application requirements. On the top of the PHY layer, the standard defines a sophisticated MAC protocol that controls access to the channel. For time-referenced resource allocations, the hub (or the coordinator) divides the time axis (or the channel) into a series of superframes. The superframes are bounded by beacon periods of equal length. To ensure high-level security, the standard defines three levels: (a) level 0—unsecured communication, (b) level 1—authentication only, (c) level 2—both authentication and encryption (27). Table 6.9, also from Reference 27, describes the PHY layers.

Regarding the MAC layer in IEEE 802.15.6, the entire channel is divided into superframe structures. Each superframe is bounded by a beacon period of equal length. The hub selects the boundaries of the beacon period and thereby selects the allocation slots. The hub may also shift the offsets of the beacon period. Generally, the beacons are transmitted in each beacon period except in inactive superframes or unless prohibited by regulations such as in MICS band. The IEEE 802.15.6 network operates in one of three modes listed in Table 6.10 and also from Reference 27. The access mechanisms used in each period of the superframe are divided into three categories: (1) random access mechanism, which uses either CSMA/CA or a slotted Aloha procedure for resource allocation, (2) improvized and unscheduled access (connectionless contention-free access), which uses unscheduled polling/posting for resource allocation, and (3) scheduled access and variants (connection-oriented contention-free access), which schedules the allocation of slots in one or multiple upcoming superframes. These mechanisms are described in detail in the standard.

6.1.5 IEEE 802.15 WPAN TG4j MBANs

The purpose of TG4j is to create an amendment to 802.15.4, which defines a PHY layer for IEEE 802.15.4 in the 2360 to 2400 MHz band and complies with Federal Communications Commission (FCC) MBAN rules. The amendment may also define modifications to the MAC needed to support this new PHY layer. This amendment allows 802.15.4- and MAC-defined changes to be used in the MBAN band. TG4j work

[8] This discussion is based on and summarized from reference (7) which the reader should consult for additional details.

TABLE 6.9 PHY Layer Specification for the IEEE 802.15.6 Standard

PHY	Description
NB PHY	The NB PHY is responsible for activation/deactivation of the radio transceiver, CCA within the current channel, and data transmission/reception. The Physical Protocol Data Unit (PPDU) frame of NB PHY contains a Physical Layer Convergence Procedure (PLCP) preamble, a PLCP header, and a PSDU. The PLCP preamble helps the receiver in the timing synchronization and carrier-offset recovery; it is the first component transmitted. The PLCP header conveys information necessary for a successful decoding of a packet to the receiver. The PLCP header is transmitted after PLCP preamble using the given header data rate in the operating frequency band. The last component of PPDU is PSDU which consists of an MAC header, MAC frame body, and frame check sequence (FCS) and is transmitted after PLCP header using any of the available data rates in the operating frequency band. A WBAN device should be able to support transmission and reception in one of the frequency bands available, including the following: 402–405 MHz; 420–450 MHz; 863–870 MHz; 902–928 MHz; 950–956 MHz; 2360–2400 MHz; and 2400–2483.5 MHz. The table further shows the data rate-dependent modulation parameters for PLCP header and PSDU. In NB PHY, the standard uses differential binary phase-shift keying (DBPSK), differential quadrature phase-shift keying (DQPSK), and differential 8-phase-shift keying (D8PSK) modulation techniques except 420–450 MHz which uses a Gaussian minimum shift keying (GMSK) technique
UWB PHY	UWB PHY operates in two frequency bands: low band and high band. Each band is divided into channels, all of them characterized by a bandwidth of 499.2 MHz. The low band consists of three channels (1–3) only. The channel 2 has a central frequency of 3993.6 MHz and is considered a mandatory channel. The high band consists of eight channels (4–11) where channel 7 with a central frequency 7987.2 MHz is considered a mandatory channel, while all other channels are optional. A typical UWB device should support at least one of the mandatory channels. The UWB PHY transceivers allow low implementation complexity and generate signal power levels in the order of those used in the MICS band. The UWB PPDU that contains a synchronization header (SHR), a PHY header (PHR), and PSDU. The SHR is composed of a preamble and a start frame delimiter (SFD). The PHR conveys information about the data rate of the PSDU, length of the payload, and scrambler seed. The information in the PHR is used by the receiver in order to decode the PSDU. The SHR is formed of repetitions of Kasami sequences of length 63. Typical data rates range from 0.5 Mbps up to 10 Mbps, with 0.4882 Mbps as the mandatory one

TABLE 6.9 (*Continued*)

PHY	Description
HBC PHY	HBC PHY operates in two frequency bands centered at 16 MHz and 27 MHz with the bandwidth of 4 MHz. Both operating bands are valid for the United States, Japan, and Korea, and the operating band at 27MHz is valid for Europe. HBC is the electrostatic field communication (EFC) specification of PHY, which covers the entire protocol for WBAN such as packet structure, modulation, preamble/SFD, etc. The PPDU structure of EFC that is composed of a preamble, SFD, PHY header, and PSDU. The preamble and SFD are fixed data patterns. They are pre-generated and sent ahead of the packet header and payload. The preamble sequence is transmitted four times in order to ensure packet synchronization while the SFD is transmitted only once. When the packet is received by the receiver, it finds the start of the packet by detecting the preamble sequence, and then it finds the start of the frame by detecting the SFD

TABLE 6.10 MAC Layer Modes for the IEEE 802.15.6 Standard

Beacon Mode	Description
Beacon mode with beacon period superframe boundaries	In this mode, the beacons are transmitted by the hub in each beacon period except in inactive superframes or unless prohibited by regulations. The superframe structure of IEEE 802.15.6 is divided into exclusive access phase 1 (EAP1), random access phase 1 (RAP1), type I/II phase, EAP2, random access phase 2 (RAP2), type I/II phase, and a contention access phase (CAP). In EAP, RAP, and CAP periods, nodes contend for the resource allocation using either CSMA/CA or a slotted Aloha access procedure. The EAP1 and EAP2 are used for highest priority traffic such as reporting emergency events. The RAP1, RAP2, and CAP are used for regular traffic only. The type I/II phases are used for uplink allocation intervals, downlink allocation intervals, bilink allocation intervals, and delay bilink allocation intervals. In type I/II phases, polling is used for resource allocation. Depending on the application requirements, the coordinator can disable any of these periods by setting the duration length to zero
Nonbeacon mode with superframe boundaries	In this mode, the entire superframe duration is covered by either a type I or a type II access phase but not by both phases
Nonbeacon mode without superframe boundaries	In this mode, the coordinator provides unscheduled type II polled allocation only

started in 2010 and a standard could emerge in 2013.[9] The title of the standard under development is: *IEEE Standard for Information Technology—Telecommunications and Information Exchange Between Systems: Local and Metropolitan Area Network-Specific Requirements. Part 15.4: Wireless Medium Access Control (MAC) and Physical Layer (PHY) Specifications for Low-Rate Wireless Personal Area Networks (WPANs) Amendment: Alternative Physical Layer Extension to support Medical Body Area Network (MBAN) services operating in the 2360–2400 MHz band.*

IEEE 802.15.4 has always supported operation in appropriate frequency bands, and an opportunity is now available to extend the operation of 15.4 into a band that is reserved for MBAN use by the FCC. As noted elsewhere in this text, the FCC has issued a Notice of Proposed Rule Making (NPRM) (FCC NPRM 09-57) to allocate the band 2360 to 2400 MHz for MBANSs using body sensor devices. Service and technical rules allow such devices to operate in this band either on a licensed-by-rule basis under the Medical Device Radiocommunication Service (MedRadio Service) in Part 95 or on a licensed and nonexclusive basis under Part 90 along with a frequency coordination model to minimize interference to incumbent users in the band. This project defines an alternate PHY and the necessary modifications to the MAC that are needed to support the PHY operation according to the FCC rules in the MBAN band (10). The proposed amendment to IEEE 802.15.4 provides a solution for the use of the MBAN spectrum that makes use of existing silicon solutions. The proposed amendment to IEEE 802.15.4 targets both on and off body applications.

By way of comparison, and as noted above, the IEEE P802.15.6 group is also working on BANs with potential medical applications. The two projects address a common application but provide a different set of capabilities. IEEE 802.15.6 is addressing communication in the vicinity of, or inside, a human body. The proposed amendment to IEEE 802.15.4 will address low data rate applications. IEEE P802.15.6 is targeting significant high data rates and lower power consumption applications.

6.1.6 ETSI TR 101 557

The 2012 ETSI TR 101 557 Technical Report (TR) has been produced by the ETSI Technical Committee, Electromagnetic Compatibility and Radiospectrum Matters (ERM) to address bandwidth allocations for WBANs/MBANSs. Previously (in 2011) ERM developed a system reference document (SRdoc) (TR 102 889-2) for technical characteristics for SRD equipment for *wireless industrial applications* using technologies different from UWB. ETSI has also identified two of the candidate frequency bands proposed for MBANSs (2360–2400 MHz and 2483.5–2500 MHz) as candidate bands for these wireless industrial applications. Both applications are

[9] Final agreement on the features of the amendment were agreed to during the March, 2012 meeting in Waikoloa, Letter Ballot #81 was approved by the Work Group, opened on March 28, 2012 and closed on April 27, 2012. The Letter Ballot passed with 90.83% Yes votes and generated 575 comments. There were 2 recirculations of the letter ballot, Letter Ballot #82 and Letter Ballot #84, both of which also passed. There were no new comments on the final recirculation ballot and no remaining NO votes. The Work Group has asked the Executive Committee to approve the amendment for Sponsor Ballot at the September 2012 meeting in Palm Springs, USA.

license-exempt SRD applications but can be both considered as critical within their environment and hence why the usual SRD bands are not intended to be used by these systems. MBANSs are used to provide wireless networking of multiple body sensors and actuators used for monitoring patient physiological parameters, patient diagnosis, and patient treatment, primarily in healthcare facilities as well as in other healthcare monitoring situations such as ambulances and the patient's home; the use of MBANSs holds the promise of improved quality and efficiency of patient care by reducing or eliminating a wide array of hardwired, patient-attached cables used by present monitoring technologies. MBANSs are intended to be used mainly in hospitals or, at a later stage of the treatment, at the patient's home. In any case, the environment for the application is far away from the application of wireless sensors used for machine automation in a factory environment. This is *why these two applications in such clearly defined but totally different environments will not harmfully interfere with each other* (1).

The ISM radio bands are radio bands allocated internationally for the said purpose. The ISM bands are defined by the ITU-R in 5.138, 5.150, and 5.280 of the radio regulations. Unfortunately, individual countries' use of the bands designated in these sections may differ due to variations in national radio regulations. In the United States, uses of the ISM bands are governed by Part 15 and Part 18 of the FCC rules. There are a number of ISM bands, but the most well known is the one covering the 2400–2500 MHz region (some other bands include allocations of 6.7 MHz, 13.5 MHz, 26.9 MHz, 40.6 MHz, 433 MHz, 902 MHz, and 5725 MHz).

In Europe, MBANS proponents (e.g., Philips, Zarlink, Texas Instruments, and Dutch Ministry of Economic Affairs Agriculture and Innovation) have an interest in addressing a growing market for MBANS services in the frequency range 1785–2500 MHz, but are concerned that no specific regulatory guidance from CEPT/ECC exists for administrations wishing to implement the MBANSs. A spectrum of 40 MHz between 1785 MHz and 2500 MHz is required for MBANS operation. A 40 MHz spectrum designation plays a key role in enabling MBANS devices achieve harmonized coexistence with other services. It enables MBANS equipment to use low-power and limited duty cycle while providing sufficient space for MBANSs to avoid interference to/from other services. It is also needed to support MBANS coexistence in high-density deployment scenarios. The proposed 40 MHz designation affords meaningful frequency diversity that would allow MBANS devices to use lower transmission power and therefore mitigate potential interference to other services. Initially, only the band 2360–2400 MHz has been proposed by the SRdoc to be considered for use by MBANS. However, during the SRdoc development process, the 1785–1805 MHz, 2400–2483.5 MHz, and 2483.5–2500 MHz bands were suggested as other candidate bands to be considered for designation for MBANS use. See Figure 6.11 for a view to the ITU-R radio regulations current allocation of the candidate bands (1710–2500 MHz). Also see Reference 1 for an extensive discussion of band availability and options, particularly for Europe.

In ETSI TR 101 557, it is proposed that the bigger portion (75%) of the required operational band should be used only inside the healthcare facilities such as hospitals, clinics, emergency rooms, etc. (indoor use), and the smaller portion (25%) should

<table>
<tr><th colspan="3">Allocation to services</th></tr>
<tr><th>Region 1</th><th>Region 2</th><th>Region 3</th></tr>
<tr><td>Europe, Africa,
Middle East west
of the Persian Gulf,
former Soviet Union,
and Mongolia.</td><td>Americas,
Greenland,
and some of
the eastern
Pacific Islands</td><td>Asia,
and most of
Oceania</td></tr>
<tr><td colspan="3"><b>1710 MHz to 1930 MHz</b> <b>FIXED</b>
<b>MOBILE</b></td></tr>
<tr><td><b>2300 MHz to 2450 MHz</b>
FIXED
MOBILE
Amateur
Radiolocation</td><td colspan="2"><b>2300 MHz to 2450 MHz</b>
FIXED
MOBILE
RADIOLOCATION
Amateur</td></tr>
<tr><td><b>2450 MHz to 2483.5 MHz</b>
FIXED
MOBILE
Radiolocation</td><td colspan="2"><b>2450 MHz to 2483.5 MHz</b>
FIXED
MOBILE
RADIOLOCATION</td></tr>
<tr><td><b>2483.5 MHz to 2500 MHz</b>
FIXED
MOBILE
MOBILE-SATELLITE
(space-to-Earth)
Radiolocation</td><td><b>2483.5 MHz to 2500 MHz</b>
FIXED
MOBILE
MOBILE-SATELLITE
(space-to-Earth)
RADIOLOCATION
RADIODETERMINATION-
SATELLITE (space-to-Earth)</td><td><b>2483.5 MHz to 2500 MHz</b>
FIXED
MOBILE
MOBILE-SATELLITE
(space-to-Earth)
RADIOLOCATION
Radiodetermination-
satellite (space-to-Earth)</td></tr>
</table>

FIGURE 6.11 Current allocation of the candidate bands (1710–2500 MHz) in the ITU-R radio regulations. *Note:* the ISM (industrial, scientific and medical) radio band in the 2.5 GHz region covers the region 2400–2500 MHz. Bluetooth, 802.11/Wi-Fi, IEEE 802.15.4, and ZigBee may use this band, possibly among other bands.

be used both inside and outside the boundaries of healthcare facilities (indoor and outdoor). The required emission bandwidth is up to 5 MHz for proper operation of the MBANS. The emission bandwidth used would depend on the data-rate requirement of the particular MBANS application. For high data-rate applications (e.g., 250 Kbps and beyond), the bandwidth would be 3–5 MHz. For low data-rate applications, the bandwidth would be 1–3 MHz. For MBANS transmitters operating within the healthcare facility sub-band (indoor), the maximum transmitted power over the emission bandwidth is 1 mW EIRP (effective isotropic radiated power). For MBANS transmitters operating within the location-independent sub-band, the maximum transmitted power over the emission bandwidth is 20 mW EIRP. The proposed MBANSs will operate at limited duty cycle to reduce power consumption and avoid interference to other services. It is expected that the duty cycle of a MBANS for in-hospital use will not be more than 25%. For location-independent MBANS applications, such as in patient homes, a much lower duty cycle of usually less than 2% is expected (1).

6.1.7 NFC

NFC can be used for IoT/M2M applications; it provides wireless connectivity, but it is not a WBAN technology. NFC[10] is a form of contactless communication between devices such as smartphones, tablets, and other devices. Contactless communication allows a user to wave the smartphone over an NFC-compatible device to send information without needing to touch the devices together or go through multiple steps setting up a connection. NFC is an offshoot of radio frequency identification (RFID), with the exception that NFC is designed for use by devices within close proximity to each other. NFC utilizes electromagnetic radio fields while technologies such as Bluetooth and Wi-Fi rely on radio transmissions. NFC technology is popular in parts of Europe and Asia and is spreading throughout the United States. As noted elsewhere in this text, Google has launched Google Wallet that supports MasterCard PayPass; PayPal offers money transfers between smartphones; and other companies are expected to offer comparable services. As the technology grows, more NFC-compatible smartphones will be available and more stores will offer NFC card readers for customer use.

The technology behind NFC allows a device, known as a reader, interrogator, or active device, to create an electromagnetic field that interacts with another NFC-compatible device or a small NFC tag holding the information the reader requires. Passive devices, such as the NFC tag in smart posters, store information, and communicate with the reader, but these devices do not actively read other devices. Peer-to-peer communication through two active devices is also possible with NFC, allowing both devices to send and receive information. Three forms of NFC technology exist—Type A, Type B, and FeliCa; all three types are similar, but communicate in slightly different ways.

Compatibility is the key to the growth of NFC as a popular payment and data communication method; hence, NFC-based device must be able to communicate with other wireless technologies and be able to interact with different types of NFC transmissions. NFC maintains interoperability between different wireless communication methods such as Bluetooth and other NFC standards (e.g., FeliCa, popular in Japan) through the NFC Forum. Founded in 2004 by Sony, Nokia, and Philips, the forum enforces standards that manufacturers must meet when designing NFC-compatible devices; this ensures that NFC is secure and remains easy to use with different versions of the technology.

Standards exist to ensure all forms of NFC technology can interact with other NFC-compatible devices and will work with newer devices in the future. Two major

[10] This discussion is based on materials from the NearFieldCommunication.org, an advocacy group for NFC applications. The organization aims at offering insightful information that keeps stakeholders informed on both the benefits and possible drawbacks of this evolving technology.

specifications exist for NFC technology: ISO/IEC 14443 and ISO/IEC 18000-3. The first defines the ID cards used to store information, such as that found in NFC tags. The latter specifies the RFID communication used by NFC devices. ISO/IEC 18000-3 is an international standard for all devices communicating wirelessly at the 13.56 MHz frequency using Type A or Type B cards, as is the case for NFC. The devices must be within 4 cm of each other before they can transfer information. The standards define how a device and the NFC tag it is reading should communicate with one another. The device is known as the interrogating device while the NFC tag is simply referred to as the tag.

To operate, the interrogator sends out a signal to the tag. If the devices are close enough to each other, the tag becomes powered by the interrogator's signal. Since the interrogator's signal powers the tag, the tag can be small in size and can function without any battery or power source of its own. The two devices create a high-frequency magnetic field between the loosely coupled coils in both the interrogating device and the NFC tag. Once this field is established, a connection is formed and the information can be passed between the interrogator and the tag. The interrogator sends the first message to the tag to find out what type of communication the tag uses, such as Type A or Type B. When the tag responds, the interrogator sends its first commands in the appropriate specification. The tag receives the instruction and checks if it is valid. If not, nothing occurs. If it is a valid request, the tag then responds with the requested information. For sensitive transactions such as credit card payments, a secure communication channel is first established, and all information sent is encrypted.

NFC tags function at half duplex; the interrogator functions at full duplex. Half duplex refers to a device that can only send or receive, but not both at once; full duplex can do both simultaneously. An NFC tag can only receive or send a signal, while the interrogating device can receive a signal at the same time it sends a command. Commands are transmitted from the interrogator using phase jitter modulation (PJM) to modify the surrounding field and send out a signal. The tag answers using inductive coupling by sending a charge through the coils in it.

Devices using NFC may be active or passive. A passive device, such as an NFC tag, contains information that other devices can read but does not read any information itself; an example could be a poster or a commercial sign on a wall where other devices can read the information, but the sign itself only transmits the stored information to authorized devices. Active devices can read information and send it. An active NFC device, such as a smartphone, is not only able to collect information from NFC tags, but it is also able to exchange information with other compatible phones or devices and could even alter the information on the NFC tag if authorized to make such changes.

To ensure security, NFC often establishes a secure channel and uses encryption when sending sensitive information such as credit card numbers. Users can further protect their private data by keeping antivirus software on their smartphones and adding a password to the phone.

As noted, NFC is limited to a distance of approximately 4 cm; Bluetooth does offer a longer signal range for connecting during data communication and transfers. NFC technology consumes little power when compared to standard Bluetooth technology (but not when compared with BLE which uses less power than NFC). Only when NFC has to power a passive, unpowered source such as an NFC tag does it require more power than a traditional Bluetooth transmission. Another benefit of NFC technology comes in its ease of use. Bluetooth requires users to manually set up connections between smartphones and takes several seconds. NFC connects automatically in a fraction of a second. Although the users must be close to one another to use NFC technology, it is faster and easier to set up than a Bluetooth connection. Also see the technical parameters depicted in Table 6.3 for this technology.

6.1.8 Dedicated Short-Range Communications (DSRC) and Related Protocols

DSRC is a two-way short-to-medium-range wireless communications capability that permits very high data transmission critical in communications-based active safety applications. DSRC-based communications is a major research priority of the Joint Program Office (ITS JPO) at the U.S. Department of Transportation (U.S. DOT) Research and Innovative Technology Administration (RITA). The cross-modal program is conducting research using DSRC and other wireless communications technologies to ensure safe, interoperable connectivity to help prevent vehicular crashes of all types and to enhance mobility and environmental benefits across all transportation system modes. In Report and Order FCC-03-324, the FCC allocated 75 MHz of spectrum in the 5.9 GHz band for use by Intelligent Transportation Systems (ITS) vehicle safety and mobility applications. Vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) applications utilizing DSRC may have the potential to significantly reduce many of the most deadly types of crashes through real-time advisories alerting drivers to imminent hazards—such as veering close to the edge of the road; vehicles suddenly stopped ahead; collision paths during merging; the presence of nearby communications devices and vehicles; and sharp curves or slippery patches of roadway ahead. Convenience V2I services such as e-parking and toll payment are also able to communicate using DSRC. Anonymous information from electronic sensors in vehicles and devices can also be transmitted over DSRC to provide better traffic and travel condition information to travelers and transportation managers. DSRC was developed with a primary goal of enabling technologies that support safety applications and communication between vehicle-based devices and infrastructure to reduce collisions. DSRC is the only short-range wireless alternative today that provides (28):

- Designated licensed bandwidth: For secure, reliable communications to take place. It is primarily allocated for vehicle safety applications by FCC Report and Order FCC 03-324.
- Fast network acquisition: Active safety applications require the immediate establishment of communication and frequent updates.
- Low latency: Active safety applications must recognize each other and transmit messages to each other in milliseconds without delay.

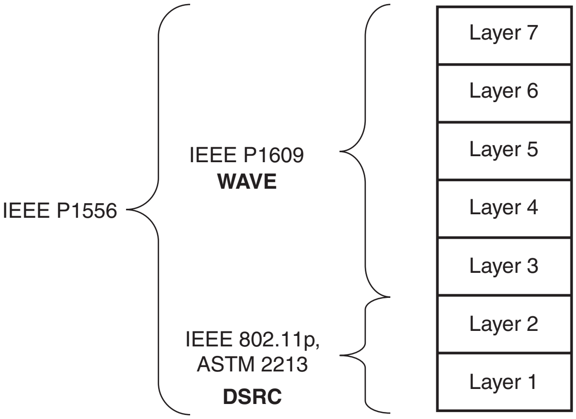


FIGURE 6.12 Relationship of WAVE, DSRC, and other protocols.

- High reliability when required: Active safety applications require a high level of link reliability. DSRC works in high vehicle speed mobility conditions and delivers performance immune to extreme weather conditions (e.g., rain, fog, snow, etc.).
- Priority for safety applications: Safety applications on DSRC are given priority over nonsafety applications.
- Interoperability: DSRC ensures interoperability, which is the key to successful deployment of active safety applications, using widely accepted standards. It supports both V2V and V2I communications.
- Security and privacy: DSRC provides safety message authentication and privacy.

The ASTM (American Society for Testing and Materials) Standard E2213-03,[11] based on IEEE 802.11a, is planned to be used for IoT applications in ITS environments. It uses a band around 5.9 GHz allocated to DSRC applications in the ITS environment—to be exact, the applicable band is now[12] 5.850–5.925 GHz range, which is divided into seven channels (each 10 MHz—these are licensed channels). Transmission has a range of 300–1000 m and a data rate of 6–27 Mbps. Half-duplex operation is used: a station can only send or transmit, but not both at the same time. DSRC devices are IEEE 802.11 systems using the WAVE (wireless access in vehicular environments) mode of operation in the DSRC band. The 5.9 GHz DSRC was originally developed for the U.S. market, and currently it is at the beginning of commercialization. Figure 6.12 depicts the relationship of WAVE, DSRC, and other support protocols.

[11] ASTM E2213-03 Standard Specification for Telecommunications and Information Exchange Between Roadside and Vehicle Systems—5 GHz Band Dedicated Short-Range Communications (DSRC) Medium Access Control (MAC) and Physical Layer (PHY) Specifications.

[12] Originally, the band was in the 915 MHz region, with a single unlicensed channel.

IEEE 802.11p (*802.11p-2010—IEEE Standard for Information technology: Local and Metropolitan Area Network-Specific Requirements. Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*) is an amendment that specifies the extensions to IEEE Standard 802.11 for WLANs providing reliable wireless communications while in a vehicular environment. IEEE 802.11p is based on ASTM Standard E2213-03 and defines the MAC layer for wireless communication in vehicular environments. It supports two different stacks:

- IPv6, but only on service channels (not control channel)
- WAVE short message protocol (WSMP): can be sent on any channel and allows applications to directly control physical characteristics (channel number and transmitter power)

The IEEE 802.11p standard is positioned as an underlying protocol for car-to-car and car-to-infrastructure applications worldwide. At the PHY layer, it has essentially the same structure as 802.11a and 802.11g: the modulation format, based on orthogonal frequency-division multiplexing (OFDM), the forward-error-correction (FEC), the structure of the preamble sequences, and the pilot-symbol schemes are identical. Furthermore, 802.11p uses the same medium access scheme common to all IEEE 802.11 standards, namely CSMA/CA (29).

WAVE is a mode of operation used by IEEE 802.11 devices to operate in the DSRC band. WAVE is part of the IEEE 1609 specification, which defines the architecture, the communications model, the management structure, the security, and physical access. The key architecture components are: (i) the on-board unit (OBU), (ii) the road side unit (RSU), and (iii) the WAVE interface. Figure 6.13, loosely based on Reference 30, depicts the WAVE protocol stack. Supportive standards are as follows (31):

- P1609.1 *Resource Manager* describes key components of WAVE system architecture and defines data flows and resources; it also defines command message formats and data storage formats. Finally it also specifies the types of devices that may by supported by OBU;
- P1609.2 *Security Services for Applications and Management Messages* defines secure message formats and processing and describes circumstances for using secure message exchanges;
- P1609.3 *Networking Services* defines network and transport layer services, including addressing and routing, in support of secure WAVE data exchange; it defines WAVE short messages (WSMs), providing an efficient WAVE-specific alternative to IP that can be directly supported by applications. Also it defines the MIB for WAVE protocol stack;
- P1609.4 *Multichannel Operations* defines enhancements to 802.11 MAC to support WAVE.

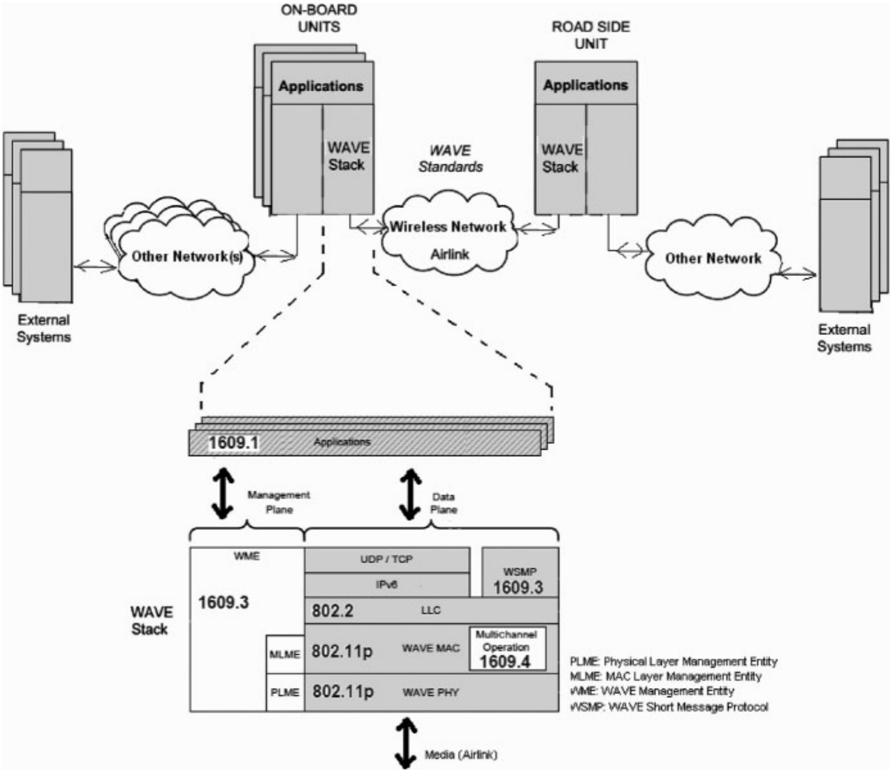


FIGURE 6.13 WAVE elements and protocol stack.

6.1.9 Comparison of WPAN Technologies

This section makes some general comparisons between some of the key PAN technologies discussed in this chapter, following observations and conclusion made in Reference 5. A basic comparison was already provided in Table 6.3, while Table 6.11 (also synthesized from Reference 5) describes some additional factors to take into account when comparing PAN technologies.

ANT/ANT+ is a mass production technology, establishing itself as the “sports and fitness” space. It is a proprietary technology, and it is unlikely that it will become pervasive. It had only been integrated into three mobile handsets at press time. ANT endeavors at operating from limited power sources and has built a niche ecosystem. ANT/ANT+ is not perceived to be a major IoT/M2M technology, but it is part of the ecosystem. The same can be said about NIKE+.

BLE is the closest competitor to ANT/ANT+ from an overall raw performance perspective. BLE is targeting the same markets as the competitive alternatives, but it offers the mobile handset manufacturers access to a larger product opportunity environment. BLE provides the best power per bit requirements of the PAN

TABLE 6.11 Some Additional Factors to Take into Account when Comparing PAN Technologies

Issue	Description
Implementation complexity	Implementation complexity is established by assessing the amount of software that would be required to implement a simple program along with hardware requirements It was noted in the text that BLE chipsets come in two categories: single mode and Bluetooth + BLE. Single-mode configurations are shipped as an SoC that contains the host processor and radio. The protocol stack is integrated in the silicon and exposes some simple application programming interfaces (API) for a developer to use. As a result, there is little effort required by the developer when creating a new product. Single-mode BLE devices are often shipped from silicon vendors as precertified units. This means that original end manufacturers (OEMs) do not need to spend resources qualifying their new products. If the developer decides to deviate significantly from a given reference design, then it is possible that some features may need retesting. The hardware for a single-mode LE device is simple. The main costs associated with a low-power sensor are the processor, radio, antenna, battery, battery connector, sensor, regulator, and the printed circuit board (PCB). A BLE device is expected to cost about $3 in components (about $2 for the Bluetooth IC and the EEPROM) and $1 for the rest (particularly the battery and the RF crystal); these component costs will be lower when mass production is activated. Dual-mode Bluetooth chipsets, as used in a mobile handset, have a host processor present. Silicon vendors normally ship a protocol stack that executes on the host processor and provides a simple API to access Bluetooth and LE. Dual-mode Bluetooth chips may also contain their own application processor. Such devices have the sensitive protocol stack burnt into read-only memory (ROM) and expose an API as a virtual machine. These types of chips are often found in consumer electronics, like headsets, where more than just sensing applications are necessary
Protocol efficiency	A wireless transmission protocol consists of the payload and overhead. The efficiency of the protocol can be defined as the ratio of payload to total packet length. If a protocol is inefficient, it will effectively imply that the transmission channel and the radio emanations are used to transferring nonpayload information; this will rapidly discharge the battery while transferring a limited amount of useful data. Alternatively, a protocol that is very efficient will transfer a larger amount of useful data on a single charge. There is a trade-off between reliability and efficiency; for example an ultra-efficient protocol that does not incorporate a checksum or error corrections; given the intrinsic possibility of interference in the 2.4 GHz band, this may require retransmissions (assuming that there are upper-layer protocols to address this predicament). For example, BLE protocol efficiency is around 66%

(*continued*)

TABLE 6.11 (***Continued***)

Issue	Description
Power efficiency	Power efficiency is one of the most critical factors in selecting the PAN technology for a given application. This efficiency is typically measured as the power per bit An ANT device is configured to transmit 32 bytes/s and consumes 61 μA. The power per bit = 0.183 mW/256 bits = 0.71 μW/bit In BLE, connectable advertising packets (adverts) are broadcast every 500 ms. Each packet has 20 bytes of useful payload and consumes 49 μA at 3 V. For this particular setup, the power per bit is 0.153 μW/bit For IrDA, the power per bit is 11.7 μW/bit A NIKE+ foot pod lasts 1000 h and transmits its payload every second. The power per bit is 2.48 μW/bit Wi-Fi consumes approximately 116 mA at 1.8 V when transmitting a 40 Mbps user datagram protocol (UDP) payload. Power per bit is 0.00525 μW/bit. Unfortunately, current consumption does not reduce when throughput is reduced in a Wi-Fi chipset. Hence, this measure is not completely comparable to the other data cited here. Also Wi-FI's peak current consumption exceeds the capabilities of a coin battery A Zigbee device consumes 0.035706 W when transferring 24 bytes of data. Hence, the power per bit is 0.035706/192 = 185.9 μW/bit
Peak power consumption	Peak power consumption is an important parameter when designing long-life devices. The common CR2032 coin cell can only provide about 15 mA peaks without damage (drawing 30 mA at peaks will reduce realized capacity by about 10% of manufacturers' stated figures). Acceptable continuous standard loads are typically 2 mA or less, in order to achieve published capacity figures. The PAN technologies discussed in this chapter have peak current requirements in the 10–50 mA, with the exception of Wi-Fi, which has a higher requirement
Robustness and coexistence	Packet transfer reliability impacts on battery life and the user experience: if a data packet is undeliverable due to suboptimal transmission environments, or interference from nearby radios, a transmitter may keep retransmitting until the packet is successfully delivered, expanding battery energy. A method to address these issues is to use channel hopping (which also helps with interference). If a wireless system is restricted to a single channel, its reliability may deteriorate in congested environments. Bluetooth and BLE use channel hopping: Bluetooth devices use AFH, which allows each node to map out frequently congested areas of the spectrum to be avoided in future transactions Coexistence is typically thought of as the ability of technologies to operate in the presence of other radios in the same room or building. ZigBee can interplay with a Wi-Fi access point; as can BLEs (refer to earlier figures on this issue). Colocation of PAN technologies with WLANs must be carefully designed, especially as Wi-Fi output power increases with advances in technology

(*continued*)

TABLE 6.11 (*Continued*)

Issue	Description
	BLE implements passive interference avoidance schemes. For example, AFH can be used to keep clear of channels where interference is detected. BLE advertising channels are also specifically chosen to be in the least congested regions of the 2.4 GHz ISM band. Wi-Fi has active coexistence technology implemented, when integrated with a device containing Bluetooth, and a mechanism to reduce its data rates, when interferers are detected from neighboring wireless technology. ZigBee does not implement a coexistence scheme, but it does have the ability to continuously listen for clear time on its channel. If the channel is heavily used, ZigBee throughput and latency are adversely affected, eventually halting. ZigBee PRO has a feature known as frequency agility (not the same as hopping) where it may be possible to search for a clear channel (of the 16 channels defined) and then re-establish the network

Note: Synthesized from Reference 5; consult reference for additional details.

technologies, exceeded only by Wi-Fi. BLE is likely to turn out to be an important IoT/M2M technology in the healthcare and/or home environment, for example for peripheral and/or smartphone connectivity.

Wi-Fi is normally intended for bulk traffic transfer at high speed (HS). It should come as no surprise that Wi-Fi is the most complicated technology to integrate into a system. Wi-Fi requires various drivers and a full protocol stack. In addition, such systems typically consume significant power at the PC end of the link to minimize latency.

ZigBee and RF4CE are practically the same technology and appear prima facia to require more power compared with the other PAN radio technologies. These systems are likely to turn out to be important IoT/M2M technologies in the healthcare and/or home environment.

NFC is not seen as a competitor to most low-power wireless technologies; the interest in this technology is that it brings new use cases to the mobile space. IR transmit-only devices are inexpensive and may still remain a viable option in low-end televisions for the near future, but the technology is also relatively power hungry. IR is being replaced in many areas by non-LOS radio technology.

6.2 CELLULAR AND MOBILE NETWORK TECHNOLOGIES FOR IoT/M2M

6.2.1 Overview and Motivations

Developers of IoT/M2M applications that are geographically dispersed over a city, region, or nation may find cellular networks to be the practical connectivity technology of choice. This section looks at some key capabilities of these networks. In the near future, M2M applications are expected to become important sources of traffic (and revenues) for cellular data networks. For example, energy suppliers routinely utilize SCADA-based systems to enable remote telemetry functions in the power grid. Traditionally, SCADA systems have used wireline networks to link remote power grid elements with a central operations center; however, at this time an increasing number of utilities are turning to public cellular networks to support these functions. Naturally, reliability and security are key considerations; endpoints typically will support virtual private network (VPN) built on IPsec mechanisms in addition to other embedded firewall capabilities.

In starting the discussion about mobile networks, one should keep in mind that IoT/M2M traffic has specific characteristics, discussed briefly in Chapter 4, which relate to the priority of the data being communicated, the size of the data, the real-time streaming needs on one end of the requirements spectrum to the extremely high delay tolerance of the data on the other end of the requirements spectrum, and varying degrees of mobility; cellular/mobile networks are characterized by varying capacity, bandwidth, link conditions, link utilization, and overall network load, which affect their ability to reliably transfer such M2M data (32). These details have to be reconciled in order to be able to cost-effectively utilize cellular technologies for a broad set of applications (while some applications may be less sensitive to cost consideration, many more applications will indeed require optimized connectivity cost metrics). Initial 3GPP efforts have focused on the ability to differentiate MTC-type devices, allowing operators to selectively handle such devices in congestion/overload situations. Specifically, low priority indicator has been added to the relevant UE (user equipment)-to-network procedures; with this, overload and congestion control is done on both core network (CN) and radio access network (RAN) based on this indicator (33).

There are different opinions as to which cellular technologies are practical and/or ideal for M2M. Some proponents claim that many developers are concentrating on 4G products. However, the cost of 4G modules is two times more expensive than 3G modules and three times more expensive than 2G modules; hence some proponents only recommend a 4G device if it is going to be deployed in an urban setting and the cost of connectivity was unimportant. Others argue that if a service provider or organization wanted to deploy an inexpensive system with a short lifespan of 1 or 2 years, they could go with 2G; but if a service provider or organization wanted to build a device to have longevity of around 10 years, then they should consider using 3G (34).

6.2.2 Universal Mobile Telecommunications System

UMTS is a 3G mobile cellular technology for networks supporting voice and data (IP) based on the GSM standard developed by the 3GPP (Third-Generation Partnership Project). UMTS is a component of the ITU IMT-2000 standard set and is functionally comparable with the CDMA2000 standard set for networks based on the competing cdmaOne technology. UMTS can carry many traffic types from real-time circuit switched to IP-based packet switched.

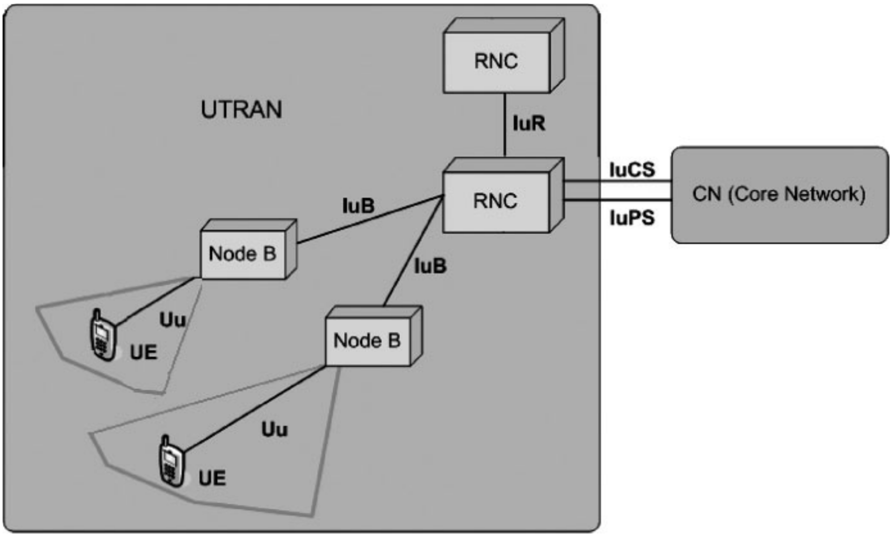


FIGURE 6.14 UTRAN.

Universal terrestrial radio access network (UTRAN) is a collective term for the NodeBs (base stations) and radio network controllers (RNC) that comprise the UMTS RAN. NodeB is the equivalent to the base transceiver station (BTS) concept used in GSM. The UTRAN allows connectivity between the UE and the CN. As seen in Figure 6.14, UTRAN contains the base stations, which are called NodeBs, and the RNC; the RNC provides control functionalities for one or more NodeBs.

As noted earlier, video can be supported over the data (IP) capability of a 3G system; mobility is generally supported at the PHY level, but could also be supported with the MIPv6 mechanisms. The challenge of 3G system is related to bandwidth availability.

6.2.3 LTE

6.2.3.1 Overview LTE is the 3GPP initiative to evolve the UMTS technology toward a 4G. LTE can be viewed as an architecture framework and a set of ancillary mechanisms that aims at providing seamless IP connectivity between UE and the packet (IPv4, IPv6) data network without any disruption to the end-users' applications during mobility. In contrast to the circuit-switched model of previous-generation cellular systems, LTE has been designed to support *only* packet-switched services.

System architecture evolution (SAE) is the corresponding evolution of the GPRS/3G packet CN evolution. LTE/SAE standards are defined in 3GPP Rel.8 specifications. Colloquially, the term LTE is typically used to represent both LTE and SAE.

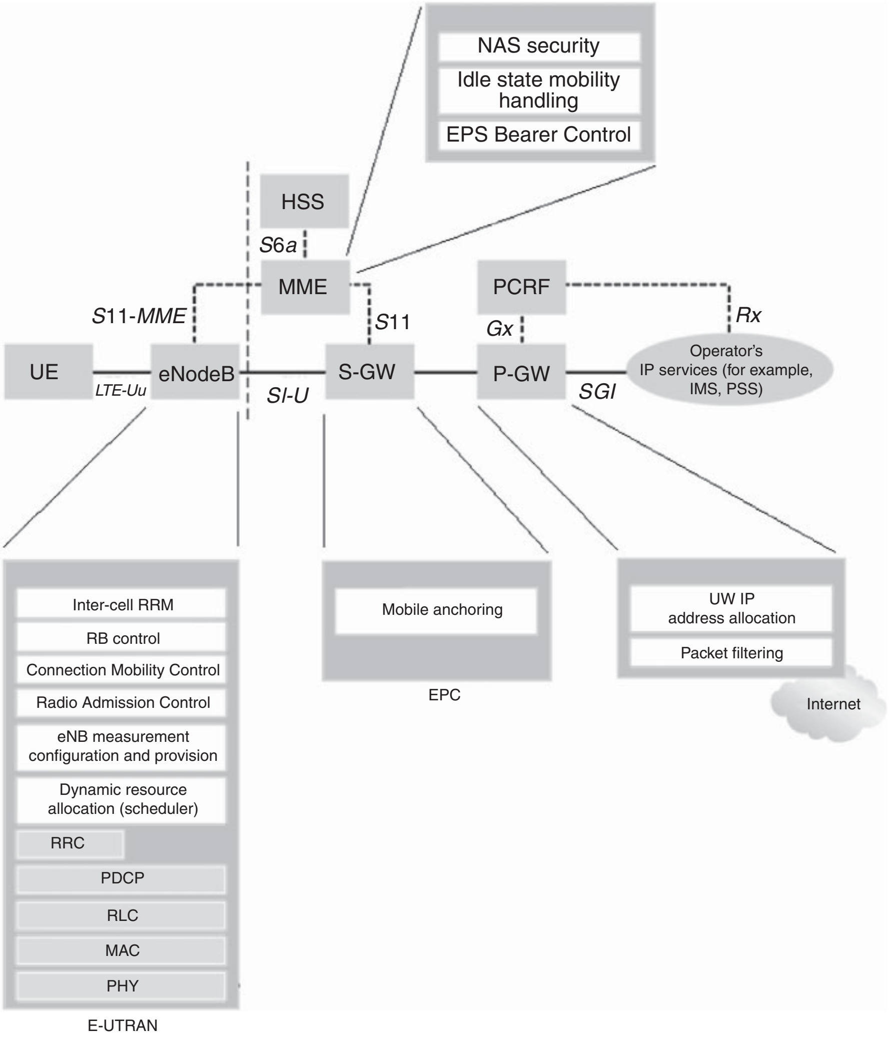


FIGURE 6.15 The EPS network elements.

The key element provided by LTE/SAE is the EPS (evolved packet system), that is, together LTE and SAE comprise the EPS. EPS provides the user with IP connectivity to a packet data network for accessing the Internet, as well as for supporting services such as streaming video. Figure 6.15 shows the overall network architecture, including the network elements and the standardized interfaces. The EPS consists of the:

- New air interface E-UTRAN (evolved UTRAN) and
- The evolved packet core (EPC) network

TABLE 6.12 Basic Comparison Between Two Generations of Cellular Technologies

3G Systems	4G/LTE/SAE Systems
Competing standards Limited set of devices Lack of applications Multiple bands and frequency Slow rollout Interoperability and interworking	– Complex technology • 130+ 3GPP specifications • 35 specs for devices, 56 specs for eNodeB, 41 specs for EPC • New network and functional elements (e.g., MME, SGW, PGW, PCRF, . . .) • New interfaces (**S6a**, **S8**, S9, S13, S13’, . . .) • **S6a**/S6d in LTE is the equivalent of MAP-based Gr and D in Pre-Rel.8 • S13/S13’ in LTE is the equivalent of MAP-based Gf in Pre-Rel.8 • New protocols (PMIP, GTPv2, diameter, SIP, . . .) – Limited availability of network/user devices – Voice, video, data, and messaging • Lack of voice support in early LTE networks – Multiple frequency/spectrum fragmentation – Expanded ecosystem – Interoperability and interworking • 15 network types with which to interoperate • Access networks • Converged core • CS core and PS core – Billing and settlement capabilities

Hence, while the term “LTE” encompasses the evolution of the UMTS *radio access* through the E-UTRAN, it is accompanied by an evolution of the *nonradio aspects* under the term SAE, which includes, as just noted, the EPC network.

Table 6.12 (based on observations made in Reference 35) provides a short comparison between two generations of cellular technologies.

In principle, LTE promises the following benefits:

- Simplified network architecture (Flat IP based);
- Efficient interworking;
- Robust QoS framework;
- Common evolution for multiple technologies;
- Real-time, interactive, low-latency true broadband;
- Multisession data;
- End-to-end enhanced QoS management (see below);
- Policy control and management;
- High level of security.

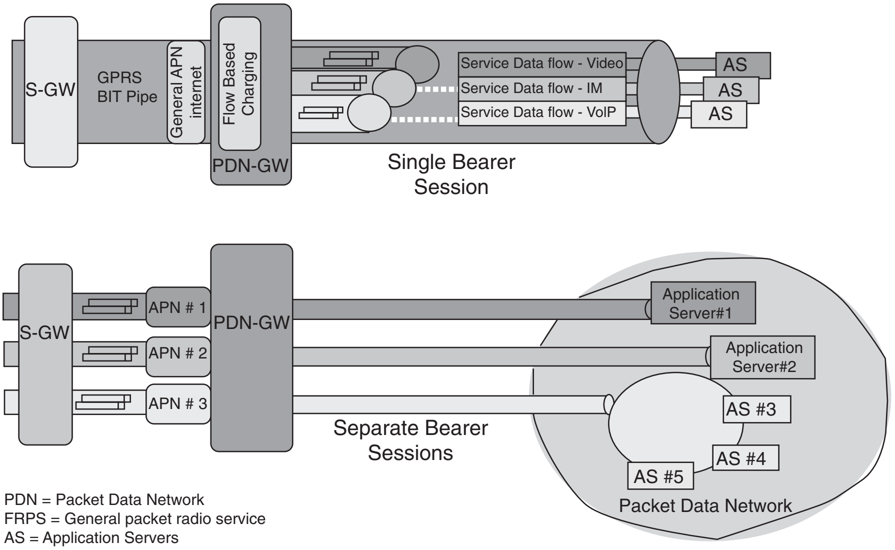


FIGURE 6.16 Bearers in EPS.

The EPS uses the concept of *bearers* to route IP traffic from a gateway in the packet data network to the UE. A bearer is an IP packet flow with a defined QoS between the gateway and the UE. The E-UTRAN and EPC together set up and release bearers as required by applications. An EPS bearer is often associated with a QoS. Multiple bearers can be established for an end-user in order to provide different QoS streams or connectivity to different packet data networks or applications reachable via that network. For example, a user might be engaged in watching a video clip while at the same time performing web browsing or FTP download; a video bearer would provide the necessary QoS for the video stream, while a best-effort bearer would be suitable for the web browsing or file transfer session (see Fig. 6.16). This is achieved by means of several EPS network elements that have different roles.

6.2.3.2 Core Network At a high level, the network is comprised of the CN (i.e., the EPC) and the access network E-UTRAN. While the CN consists of many logical nodes, the access network is comprised of essentially just one node, the evolved NodeB (eNodeB), which connects to the UEs. Each of these network elements is interconnected over interfaces that are standardized in order to allow multivendor interoperability.

The logical CN nodes are shown in Figure 6.15 and briefly discussed in Table 6.13 (36, 37). The CN is responsible for the overall control of the UE and establishment of the bearers. The main logical nodes of the CN are: (i) PDN gateway (P-GW); (ii) serving gateway (S-GW); and (iii) mobility management entity (MME). In addition to these nodes, the CN also includes other logical nodes and functions such as the Home Subscriber Server (HSS) and the Policy Control and Charging Rules Function

TABLE 6.13 CN Nodes

Function	Description
Policy Control and Charging Rules Function (PCRF)	The PCRF is responsible for policy control decision-making, as well as for controlling the flow-based charging functionalities in the Policy Control Enforcement Function (PCEF), which resides in the P-GW. The PCRF provides the QoS authorization (QCI and bit rates) that decides how a certain data flow will be treated in the PCEF and ensures that this is in accordance with the user's subscription profile
Home Subscriber Server (HSS)	The HSS contains users' Systems Architecture Evolution (SAE) subscription data such as the EPS-subscribed QoS profile and any access restrictions for roaming. It also holds information about the packet data networks to which the user can connect. This could be in the form of an access point name (APN) (which is a label according to DNS naming conventions describing the access point to the PDN) or a PDN address (indicating subscribed IP address(es)). In addition, the HSS holds dynamic information such as the identity of the MME to which the user is currently attached or registered. The HSS may also integrate the authentication center (AUC), which generates the vectors for authentication and security keys
Packet data network Gateway (P-GW)	The P-GW is responsible for IP address allocation for the UE, as well as QoS enforcement and flow-based charging according to rules from the PCRF. It is responsible for the filtering of downlink user IP packets into the different QoS-based bearers. This is performed based on traffic flow templates (TFTs). The P-GW performs QoS enforcement for GBR bearers. It also serves as the mobility anchor for interworking with non-3GPP technologies such as CDMA2000 and WiMAX® networks
Serving Gateway (S-GW)	All user IP packets are transferred through the S-GW, which serves as the local mobility anchor for the data bearers when the UE moves between eNodeBs. It also retains the information about the bearers when the UE is in the idle state (known as "EPS Connection Management — IDLE" [ECM-IDLE]) and temporarily buffers downlink data while the MME initiates paging of the UE to re-establish the bearers. In addition, the S-GW performs some administrative functions in the visited network such as collecting information for charging (e.g., the volume of data sent to or received from the user) and lawful interception. It also serves as the mobility anchor for interworking with other 3GPP technologies such as GPRS and UMTS
Mobility Management Entity (MME)	The MME is the control node that processes the signaling between the UE and the CN. The protocols running between the UE and the CN are known as the nonaccess stratum (NAS) protocols. The main functions supported by the MME can be classified as: (i) *Functions related to bearer management*—This includes the establishment, maintenance, and release of the bearers and is handled by the session management layer in the NAS protocol and (ii) *Functions related to connection management*—This includes the establishment of the connection and security between the network and UE and is handled by the connection or mobility management layer in the NAS protocol layer

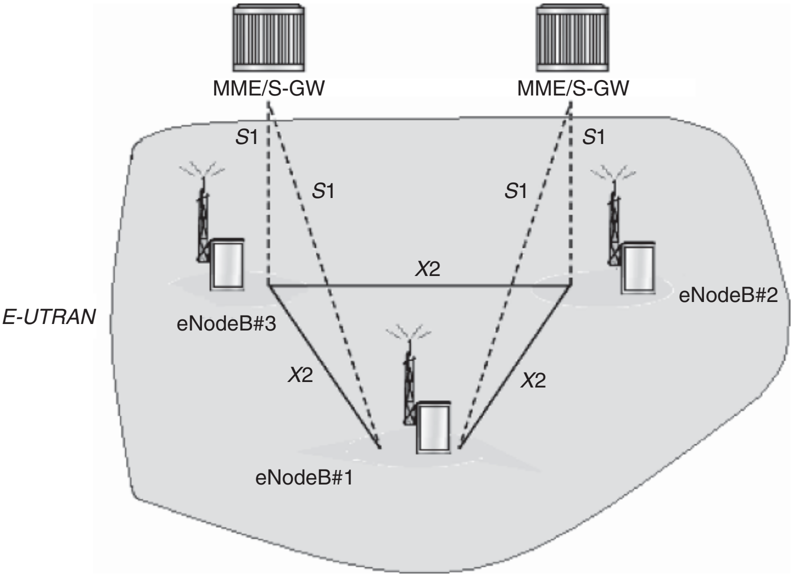


FIGURE 6.17 E-UTRAN.

(PCRF). Since the EPS only provides a bearer path of a certain QoS, control of multimedia applications such as packet video is provided by the IP multimedia subsystem (IMS), which is considered to be outside the EPS itself.

6.2.3.3 Access Network The access network of LTE, E-UTRAN, consists of a network of eNodeBs, as illustrated in Figure 6.17. For normal user traffic (as opposed to broadcast), there is no centralized controller in E-UTRAN; hence the E-UTRAN architecture is said to be flat. The eNodeBs are normally interconnected with each other by means of an interface known as "X2" and to the EPC by means of the S1 interface—more specifically, to the MME by means of the S1–MME interface and to the S-GW by means of the S1–U interface. The protocols that run between the eNodeBs and the UE are known as the "AS protocols." The E-UTRAN is responsible for all radio-related functions, as depicted in Table 6.14 (36, 37). On the network side, all of these functions reside in the eNodeBs, each of which can be responsible for managing multiple cells. Unlike some of the previous second-generation and 3G technologies, LTE integrates the radio controller function into the eNodeB; this allows tight interaction between the different protocol layers of the RAN, thus reducing latency and improving efficiency. Such distributed control eliminates the need for a high-availability, processing-intensive controller, which in turn has the potential to reduce costs and avoid "single points of failure." Furthermore, as LTE does not support soft handover, there is no need for a centralized data-combining function in the network. One consequence of the lack of a centralized controller node is that, as the UE moves, the network must transfer all information related to a UE, that

TABLE 6.14 E-UTRAN Functions

Function	Description
Radio resource management (RRM)	This function covers all activities related to the radio bearers, such as radio bearer control, radio admission control, radio mobility control, scheduling, and dynamic allocation of resources to UEs in both uplink and downlink
Header compression	This function is used to ensure efficient use of the radio interface by compressing the IP packet headers that could otherwise represent a significant overhead, especially for small packets such as Voice Over IP (VoIP) or video
Security	All data sent over the radio interface is encrypted
Connectivity to the EPC	This function consists of the signaling toward MME and the bearer path toward the S-GW

is, the UE context, together with any buffered data, from one eNodeB to another; mechanisms are, therefore, needed to avoid data loss during handover.

6.2.3.4 Roaming A network run by one operator in a jurisdiction (or service area) is known as a "public land mobile network (PLMN)." Roaming is the capability where users are allowed to connect to PLMNs other than those to which they are directly subscribed, as shown in Figure 6.18. A roaming user is connected to the E-UTRAN, MME, and S-GW of the visited LTE network; however, LTE/SAE allows the P-GW of either the visited or the home network to be used (36, 37). Using the home network's P-GW allows the user to access the home operator's services even while in a visited network.

6.2.3.5 Interworking Interworking with other networks is also critically important. The EPS also supports interworking and mobility (handover) with networks such as GSM, UMTS, CDMA2000, and WiMAX (worldwide interoperability for microwave access). The architecture for interworking with 2G and 3G GPRS/UMTS networks is depicted in Figure 6.19; in Figure 6.19 the S-GW acts as the mobility anchor for interworking with other 3GPP technologies such as GSM and UMTS, while the P-GW serves as an anchor allowing seamless mobility to non-3GPP networks such as CDMA2000 or WiMAX. The P-GW may also support a Proxy Mobile Internet Protocol (PMIPv6)-based interface.

6.2.3.6 Protocol Architecture The protocol architecture spans the user plane and the control plane. The user plane protocols operate as follows: an IP packet for a UE is encapsulated in an EPC-specific protocol and tunneled between the P-GW and the eNodeB for transmission to the UE. Different tunneling protocols are used across different interfaces; A 3GPP-specific tunneling protocol called the GPRS tunneling protocol (GTP) is used over the CN interfaces, S1, and S5/S8. The E-UTRAN user plane protocol stack is shown in Figure 6.20 top, consisting of the packet data

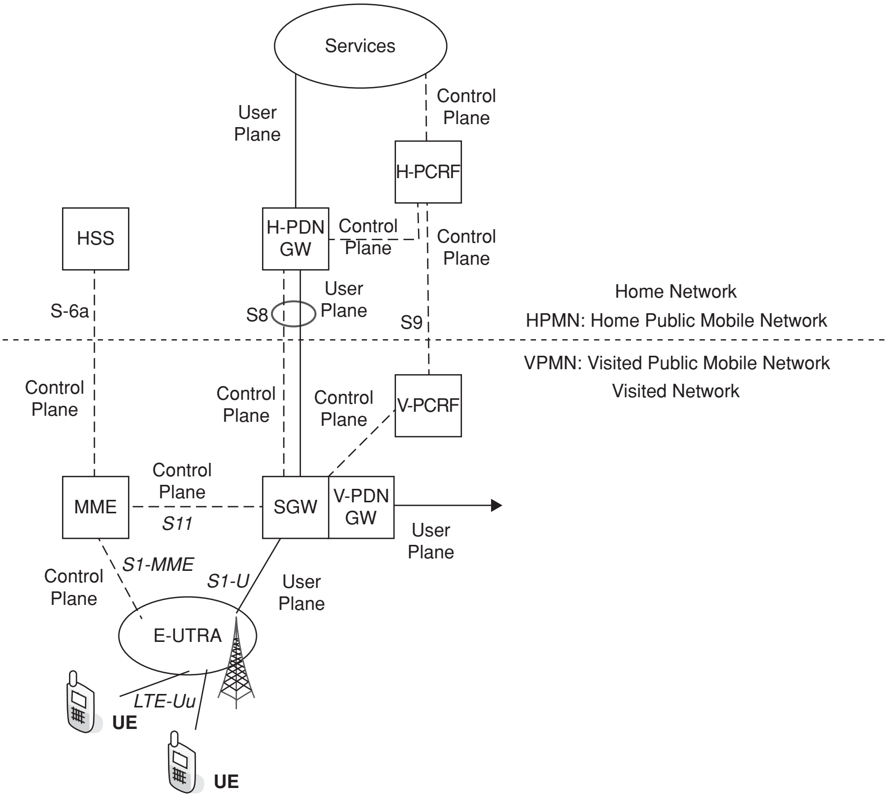


FIGURE 6.18 Roaming architecture for 3GPP accesses with P-GW in home network.

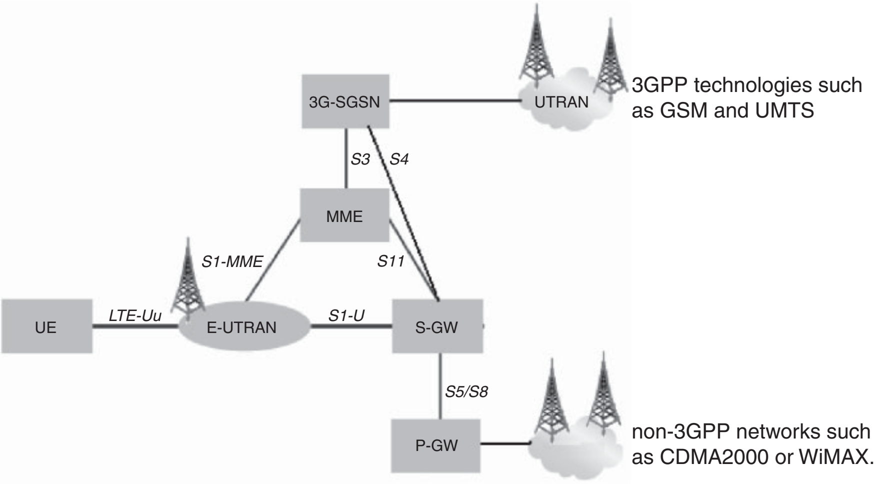

3G-SGSN
UTRAN
3GPP technologies such as GSM and UMTS
S3
S4
MME
S1-MME
S11
UE
LTE-Uu
E-UTRAN
S1-U
S-GW
S5/S8
P-GW
non-3GPP networks such as CDMA2000 or WiMAX.

FIGURE 6.19 LTE and pre-LTE interworking mechanisms.

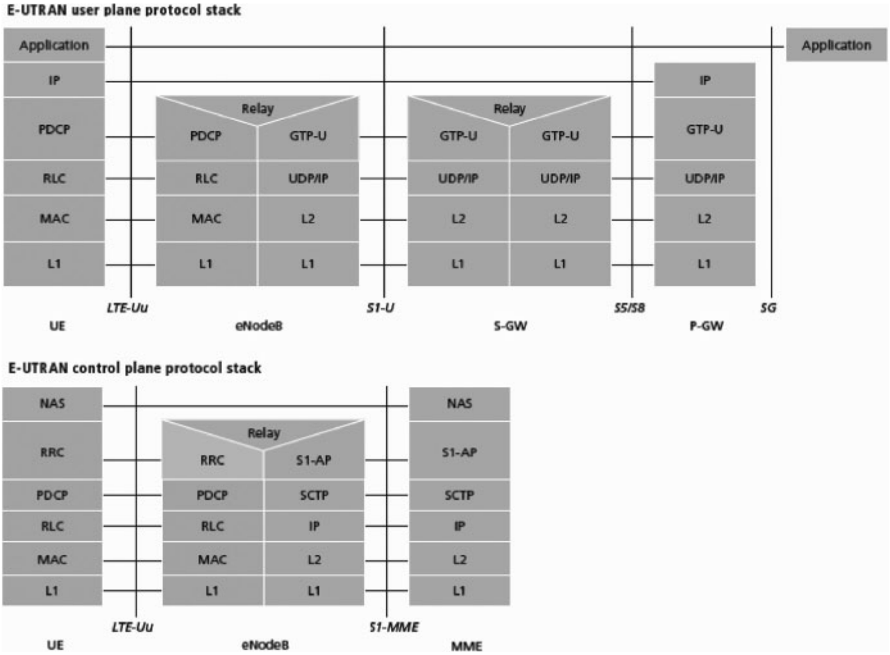


FIGURE 6.20 LTE protocol stack at the E-UTRAN.

convergence protocol (PDCP), radio link control (RLC) and MAC sublayers that are terminated in the eNodeB on the network side. The protocol stack for the control plane between the UE and MME is shown in Figure 6.12 bottom. The lower layers perform the same functions as for the user plane; the radio resource control (RRC) protocol is known as “layer 3” in the AS protocol stack and it is the key controlling function in the AS, being responsible for establishing the radio bearers and configuring all the lower layers using RRC signaling between the eNodeB and the UE (36, 37).

6.2.3.7 Multiple QoS Management In order to support multiple QoS requirements, different bearers are set up within the EPS, each being associated with a QoS, being that in a typical environment, multiple applications may be running in a UE at any time, each one having different QoS requirements. In the access network, it is the responsibility of the eNodeB to ensure the necessary QoS for a bearer over the radio interface. Bearers can be classified into two categories:

- Minimum guaranteed bit rate (GBR) bearers that can be used for applications such as mobile video. These bearers have an associated GBR value for which dedicated transmission resources are permanently allocated at bearer establishment or modification (bit rates higher than the GBR may be allowed for a GBR bearer if resources are available).

- Non-GBR bearers that do not guarantee any particular bit rate. These bearers can be used for applications such as, but not limited to, web browsing or FTP transfer. For these bearers, no bandwidth resources are allocated permanently to the bearer.

Each bearer has an associated QoS class identifier (QCI), and an allocation and retention priority (ARP). The QCI is a scalar identifying a set of transport characteristics and used to infer node-specific parameters that control packet-forwarding treatment. Each packet flow is mapped to a QCI value based on the level of service required by the application. Transport characteristics include bearer with/without GBR, priority, packet loss rate, packet latency budget, and so on. Packet-forwarding treatment includes scheduling weights, admission thresholds, queue management thresholds, and link-layer protocol configuration. Nine QCI values were defined and standardized in the Release 8 version of the specifications, as depicted in Table 6.15; standardization ensures that an LTE operator can expect uniform traffic-handling behavior throughout the network regardless of the manufacturers of the eNodeB equipment. The usage of the QCI avoids the transmission of a full set of QoS-related parameters over the network interfaces and reduces the complexity of QoS negotiation. The QCI, along with ARP and, if where needed, GBR and maximum bit rate (MBR), determines the QoS associated to an EPS bearer. Hence, each QCI is characterized by priority, packet delay budget, and acceptable packet loss rate; the QCI label for a bearer determines how it is handled in the eNodeB. A mapping between EPS and pre-Release 8 QoS parameters has been defined to allow proper interworking with legacy networks.

TABLE 6.15 Standardized QCIs in LTE (Current List)

Resource Type	QCI	APP	Packet Delay Budget (ms)	Packet Loss Rate	Examples
GBR	1	2	100	10^{-2}	Voice
GBR	2	4	150	10^{-3}	Video streaming (live)
GBR	3	5	300	10^{-6}	Video streaming (buffered)
GBR	4	3	50	10^{-3}	Interactive gaming
Non-GBR	5	1	100	10^{-6}	IMS signaling
Non-GBR	6	7	100	10^{-3}	Voice, video (live streaming), interactive gaming
Non-GBR	7	6	300	10^{-6}	Video streaming (buffered)
Non-GBR	8	8	300	10^{-6}	WWW, e-mail, FTP, progressive video, p2p file sharing, TCP-based apps
Non-GBR	9	9	300	10^{-6}	

The priority and packet delay budget (and to some extent the acceptable packet loss rate) from the QCI label determine the RLC mode configuration and how the scheduler in the MAC handles packets sent over the bearer (e.g., in terms of scheduling policy, queue management policy, and rate-shaping policy). For example, a packet with higher priority can be expected to be scheduled before a packet with lower priority. For bearers with a low acceptable loss rate, an acknowledged mode can be used within the RLC protocol layer to ensure that packets are delivered successfully across the radio interface. The ARP of a bearer is used for call admission control—that is, to decide whether or not the requested bearer should be established in case of radio congestion. It also governs the prioritization of the bearer for pre-emption with respect to a new bearer establishment request. Once successfully established, a bearer's ARP does not have any impact on the bearer-level packet-forwarding treatment (e.g., for scheduling and rate control). Such packet-forwarding treatment should be solely determined by the other bearer-level QoS parameters such as QCI, GBR, and MBR (36, 37).

6.2.3.8 Signaling 2G/3G networks use SS7-MAP protocol for the following functions:

- location
- subscriber access
- handover
- authentication
- security/identity management
- handover services

In LTE/SAE (3GPP Rel.8), Diameter Base Protocol (RFC 3588) has been chosen by 3GPP for many of these procedures and is increasingly used for interoperator signaling network and roaming infrastructure. For example, registration messages received will be based on diameter (rather than SS7-MAP). The LTE interfaces based on diameter include the following (35):

- Packet core-related interfaces toward HSS and EIR
  - S6a (MME to HSS) and S6d (SGSN to HSS)
  - S6b, S6c (external AAA functions for non-3GPP accesses)
  - S13 (MME to EIR) and S13' (SGSN to EIR)
- Network signaling for policy control and charging
  1. S9 (H-PCRF to V-PCRF)
  2. S7 (PCRF to P-GW)
  3. Gx (PCRF to PCEF)
  4. Gxc (PCRF to S-GW)
  5. Rx (AF to PCRF)
  6. Gy (PCEF to OCS)

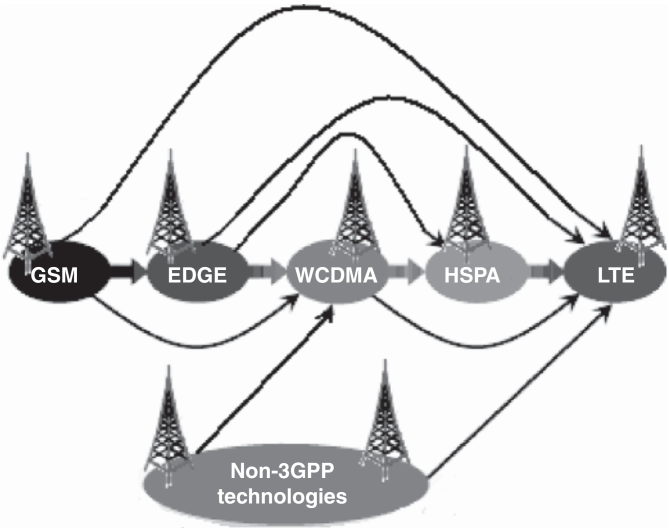


FIGURE 6.21 Evolution to LTE.

6.2.3.9 Evolution Paths to 4G/LTE Mobile operators are evolving toward LTE/SAE using different evolution paths, as follows (see Fig. 6.21):

- 3GPP environments: GSM, GPRS, EDGE, WCDMA, HSPA
- Non-3GPP environments: 1xRTT, EV-DO, 3xRTT, WLAN, WiMAX

Some of the challenges in LTE deployment were hinted in Table 6.12, the key factors being the complexity of the technology and the plethora of interfaces that have to be supported. The evolution from a 2G/3G baseline will also be nontrivial. Network element evolution from 2G/3G to LTE includes the following upgrades in the provider network:

- GERAN and UTRAN -> **E-UTRAN**
- SGSN/PDSN-FA ->**S-GW**
- GGSN/PDSN-HA ->**PDN-GW**
- HLR/AAA ->**HSS**
- VLR ->**MME**

In addition, the following signaling evolution from 2G/3G to LTE is needed:

- SS7-MAP/ANSI-41/RADIUS ->**Diameter**
- GTPc-v0 and v1 ->**GTPc-v2**
- MIP ->**PMIP**

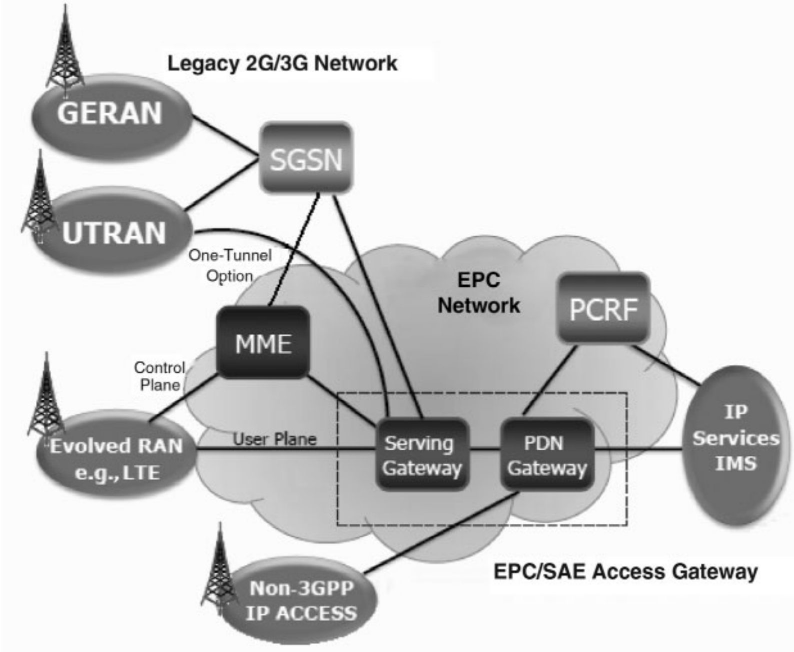


FIGURE 6.22 EPS and support of legacy environments.

After the LTE environment is established in a portion of the provider's environment, legacy components of the provider's network can be supported by the LTE infrastructure as depicted pictorially in Figure 6.22 (35).

APPENDIX 6.A: NON-WIRELESS TECHNOLOGIES FOR IoT: POWERLINE COMMUNICATIONS

This appendix provides a brief description of some non-wireless networking technologies that have been considered for IoT/M2M. See Table 6A.1 for a listing of some of the key technologies. SCADA was discussed in the context of standards in the Appendix to Chapter 5. Here we focus on PLC.

PLC refers to any technology that enables data transfer through powerlines by using advanced modulation technology. Data communication can take place at NB or broadband speeds. The technology has been around since the 1950s, but initially only supported NB applications for relay management, for example for public lighting. Broadband over PLC only began at the end of the 1990s. PLC is thus a term used to identify technologies, equipments, applications and services aiming at providing users with communication means over existing "powerlines" (cables transmitting electricity). The term broadband over powerline (BPL) is used to underline the technology capability to address broadband services. As for the term access PLC, it

TABLE 6A.1 Listing of Some of the Key Non-Wireless Technologies used for IoT-Like Services Over the Years

Technology/Concept	Description
KNX and KNX-RF	KNX (administered by the KNX Association) is an OSI-based network communications protocol for intelligent buildings defined in standards CEN EN 50090 and ISO/IEC 14543. KNX is the follow-on standard built on the European Home Systems Protocol (EHS), BatiBUS, and the European Installation Bus (EIB or Instabus). Effectively, KNX uses the communication stack of EIB but augmented with the PHY layers and configuration modes BatiBUS and EHS; thus, KNX includes the following PHYs: • Twisted pair wiring (inherited from the BatiBUS and EIB Instabus standards). This approach uses differential signaling with a signaling speed of 9.6 Kbps. MAC is controlled with the CSMA/CA method; • Powerline networking (inherited from EIB and EHS); • Radio (KNX-RF); • IR; and, • Ethernet (also known as EIBnet/IP or KNXnet/IP).
M-Bus	The M-Bus is a European standard for remote reading of gas and electric meters; it is also usable for all other types of consumption meters. It is specified as follows: • EN 13757-2 (PHY and link layer) • EN 13757-3 (application layer) • Note: the frame layer uses IEC 870 and the network (packet layer) is optional A radio variant of M-Bus (wireless M-Bus) is also specified in EN 13757-4
PLC	PLC (also called powerline communication as a singular term; also called powerline telecommunications [or PLT]) refers to any technology that enables data transfer through powerlines. Data communication can take place at NB or broadband speeds. The technology has been around since the 1950s, but initially only supported NB applications for relay management, for example for public lighting. Broadband over PLC only began at the end of the 1990s. PLC is thus a term used to identify technologies, equipments, applications, and services aiming at providing users with communication means over existing "powerlines" (cables transmitting electricity). The term BPL is used to underline the technology capability to address broadband services. As for the term access PLC, it is used to identify those PLC solutions aiming at providing consumers with broadband services through the external electricity grid, while in-home PLC is used to identify PLC solutions aiming at applications within the home (38)

TABLE 6A.1 (*Continued*)

Technology/Concept	Description
SCADA	A long-existing industrial control system (ICS). It is a centralized system used to monitor and control systems deployed over large geographic areas, such as a power grid. There are three main elements in a SCADA system, multiple RTUs (remote telemetry units), a communications apparatus, and a HMI (human machine interface) mechanism
xDSL	A 1990s technology that exploits unused frequencies on copper telephone lines to transmit traffic typically at multimegabit speeds. DSL can allow voice and HS data to be sent simultaneously over the same line. Because the service is “always available,” end-users do not need to dial in or wait for call set-up. Asymmetrical variations include ADSL, G.lite ADSL (or simply G.lite), VDSL (ITU-T G.993.1), and VDSL2 (ITU-T G.993.2). The standard forms of ADSL (ITU G.992.3, G.992.5, and ANSI T1.413—Issue 2) are all built upon the same technical foundation, discrete multitone (DMT). The suite of ADSL standards facilitates interoperability between all standard forms of ADSL (39)

is used to identify those PLC solutions aiming at providing consumers with broadband services through the external electricity grid, while in-home PLC is used to identify PLC solutions aiming at applications within the home (38). A brief history is as follows (40):

- **1950**: at a frequency of 10 Hz, 10 kW of power, one-way: town lighting, relay RC;
- **Mid-1980s**: beginning of research into the use of the electrical grid to support data transmission; on bands between 5 and 500 KHz, always in a one-way direction;
- **1997**: first tests for bidirectional data signal transmission over the electrical supply network and the beginning of research by Ascom (Switzerland) and Norweb (United Kingdom);
- **2000**: first tests carried out in France by EDF R&D and Ascom;
- **2011-12**: Publication of IEEE 1901 standards.

PLC transmission works by superimposing a high-frequency signal at low-energy levels over the 50 Hz electrical signal. The powerline is transformed into a communication network through the superposition of a low-energy information signal to the power wave. In order to ensure a suited coexistence and separation between the two systems, the frequency range used for communication is very far from the one used for the power wave (50 Hz in Europe): 3–148.5 kHz for PLC NB applications and from 1–30 MHz for PLC broadband applications. The modulated signal is transmitted via the power infrastructure and can be received and decoded remotely. Thus, the PLC signal is received by any PLC receiver located on the same electrical network. An integrated coupler at the PLC receiver entry points eliminates low frequency components before the signal is treated.

There now is standardization work underway in the PLC Forum and in ETSI. CENELEC has issued regulations for transmission in defined bands. The CENELEC A-band is reserved by law in CENELEC regulated countries for the exclusive use of utilities and their licensees. The CENELEC C-band is available for consumer and commercial use without restriction, but a common access protocol and coexistence protocol is mandated (41).

A plethora of NB (some Kbps) and broadband (tens or even hundreds of Mbps) applications can be provided through access and in-home PLC solutions, for the benefit of end consumers and of utilities (to increase their performances and improve their service quality). NB applications include home control, home automation, automatic meter reading, remote surveillance, and control of home appliances. Broadband applications include (for access PLC) Internet access, telephony, TV and (for in-home PLC) Internet access sharing, computer resource sharing, and AV whole-house distribution. PLC can be used in places where radio frequency (RF) cannot be used or is unreliable; for example, smart meters in the basement of a building are unlikely to be able to use RF to communicate with the neighborhood data concentrator—PLC communication can utilize the power wires to reach the data concentrator. It is estimated today that more than 80 PLC initiatives in more than 40 countries have been launched, worldwide, by electric utilities. Pilot sites, technological or commercial trials, and deployments are numerous in Europe. Among the most important initiatives are the ones developed by EDF (France), EDP (Portugal), EEF (Switzerland), ENDESA and IBERDROLA (Spain), PPC (Germany), and SSE (Scotland) (38).

IEEE 1901 is a group of PLC standards that enables transmission of data over AC electrical powerlines. Its goal was to replace a set of different powerline specs now in existence but maintaining a mandatory coexistence with legacy PLC approaches. There are two basic standards: (i) a BPL standard and (ii) a low-frequency narrowband (LF NB) standard.

- The IEEE 1901$^{\text{TM}}$ BPL standard was finalized and published in December 2010. The standard was sponsored by the IEEE Communications Society. The BPL standard is designed for use in a wide range of applications including SE, transportation, and LANs in both the home and the enterprise. Networking products that fully comply with IEEE 1901 will deliver data rates in excess of 500 Mbps in LAN applications. In first-mile/last-mile applications, IEEE 1901-compliant devices will achieve ranges of up to 1500 m. The technology specified by IEEE 1901 uses sophisticated modulation techniques to transmit data over standard AC powerlines of any voltage at transmission frequencies of less than 100 MHz. In the transportation sector, for example, the standard's data rates and range make it possible to deliver A/V entertainment to the seats of airplanes, trains, and other mass transit vehicles. Electric vehicles (EVs) can download a new entertainment playlist to the A/V system while the car is charging overnight. In the home, PLC will complement wireless LANs by providing a link through walls and other RF impediments as well as over distances beyond the normal range of wireless networks. It will complement wireless networks in hotels and other multistory buildings by carrying multimedia data over the longer distances and allowing wireless to complete the communication link over the last few meters. IEEE 1901 may also benefit utilities, service providers, and consumer electronics companies—anyone with a stake in smart grid technologies—as well as smart-meter providers and home appliance manufacturers (42).

- The IEEE has been working on IEEE P1901.2^{TM}, a standard for LF NB (less than 500 kHz) PLC for smart grid applications. The specification entered its final approval process in early 2012 and was expected to be ratified soon thereafter. LF NB PLC is needed, according to proponents, to accelerate wider-scale rollout of smart grids. IEEE P1901.2 is designed to support smart grid applications such as grid to utility meter, EV to charging station, home area networking, and solar-panel communications. More than 30 semiconductor manufacturers, meter and systems manufacturers, software developers, service providers, and utilities have contributed to the work of the IEEE P1901.2 Working Group since its inception in fall 2009. The work was sponsored by the Powerline Communications Standards Committee of the IEEE Communications Society (ComSoc). IEEE P1901.2 is designed to specify secure PLC at data rates up to 500 Kbps and at transmission frequencies of less than 500 kHz for applications such as grid to utility meter, EV to charging station, home area networking and lighting, and solar-panel communications. The standard addresses LF NB PLC over low-voltage lines of less than 1000 V between transformer and meter, through transformer low-voltage to medium-voltage (1000 V up to 72 kV) and through transformer medium-voltage to low-voltage powerlines in both urban and long-distance (multikilometer) rural communications. IEEE P1901.2 supports the balanced and efficient use of the PLC channel by all classes of LF NB devices by defining detailed mechanisms for coexistence among standard technologies operating in the same field, data rate, and frequency band. This standard assures coexistence with broadband powerline (BPL) devices by minimizing out-of-band emissions in frequencies greater than 500 kHz. The standard addresses the necessary security requirements that assure communication privacy and allow use for security sensitive services. This standard defines the PHY layer and the medium access sublayer of the data link layer, as defined by the International Organization for Standardization (ISO) Open Systems Interconnection (OSI) Basic Reference Model (43).

The PLCforum is a leading international association that represents the interests of manufacturers, energy utilities, and other organizations (universities, other PLC associations, consultants, etc.) active in the field of access and in-home PLC technologies.

Beyond the PLCforum, a number of industry groups and electric utilities, all around the world, are supporting the development of the PLC technology. Among industry groups are UPLC and PLCA (in the United States), PLC-J (in Japan), APTEL (in South America), PUA (PLC Utilities Alliance) in Europe, Utilitel in Australia, the Universal Powerline Alliance, and the HomePlug® Powerline Alliance, among others.

The HomePlug Alliance's mission[13] is to enable and promote rapid availability, adoption, and implementation of cost-effective, interoperable, and standards-based home powerline networks and products. By working with utility companies and the Wi-Fi Alliance and ZigBee Alliance, the HomePlug Alliance aims at helping to build the home area network (HAN) ecosystem that enables intelligent energy management and efficiency in the home and small businesses. With the goal of providing a complimentary wireless (ZigBee) and wired (HomePlug) infrastructure, the coverage for large homes and multidwelling units can be assured.

Basic applications include the use of in-home wires to distribute signals to support Smart Grid & Smart Energy, HDTV Networking, Whole Home Audio, and Gaming. Technology standards defined by the Alliance include the following:

- HomePlug Green PHY™ ("GP")
- IEEE 1901 Powerline Networking Standard
- HomePlug Broadband-Speed Technologies
- SE Profile 2

HomePlug Green PHY Specification. This is a new powerline networking specification that targets smart grid/SE applications. HomePlug GP is based on customer requirements for cost, coverage, and performance and driven by input from utility companies, as well as from companies that manufacture meters, automobiles, and appliances. In addition to low cost and power consumption, IPv6 networking and interoperability with the installed base of powerline products are critical to the success of products. As such, HomePlug GP will be interoperable with both HomePlug AV and IEEE 1901, just cited; this means that HomePlug Green PHY is a certification profile of IEEE 1901. HomePlug Green PHY has ample bandwidth to support critical functionality such as IP networking, but with power consumption estimated to be 75% lower than HomePlug AV, with similar cost savings projected. The specification is designed to the specific requirements of Smart Grid applications while interoperating with HomePlug AV and AV2 products and the IEEE 1901 standard. GP chips are already available; certified products are expected to ship in early 2013.

- Principal applications: Monitor and control devices via low speed, low-cost PLC, including smart energy applications such as demand response, load control, energy efficiency Home/Building Automation. It targets smart grid

[13] This section is based on material from The HomePlug® Powerline Alliance (44).

applications such as HVAC/thermostats, smart meters, home appliances, and plug-in electric vehicles (PEVs).

- Features: (i) interoperable with HomePlug AV; (ii) HomePlug GP is a profile of IEEE P1901; and (iii) low-power consumption, low cost
  - Estimated, up to 75% lower cost, 75% less power consumption than HomePlug AV
  - Internet (IP) networking: 802.2, IPv6 support
  - Minimum 1 Mbps effective data rate (3.8 Mbps peak PHY rate)
  - Support for firmware updates

IEEE 1901 Powerline Networking Standard. Regarding IEEE 1901.2010—For HS communication devices (HomePlug AV), the HomePlug Alliance and its members first collaborated with IEEE in 2005 with the inception of the P1901 workgroup, tasked to develop a standard for HS communication devices. In December 2008, the IEEE P1901 working group voted to include HomePlug technology in the baseline standard for PLC. The IEEE 1901.2010 standard was ratified in September 2010, and multiple semiconductor vendors are now shipping integrated circuits (ICs) based on the standard. In addition, the installed base of tens of millions of HomePlug AV products are fully interoperable with the 1901 standard, ensuring a seamless roadmap for existing users of HomePlug technology. The HomePlug Alliance conducts a comprehensive compliance and interoperabilty (C&I) program for products based on the HomePlug AV IEEE P1901 standard, ensuring that reliable, interoperable products are available from multiple suppliers. Additionally, the HomePlug Alliance plans to launch a new certification program—Netricity PLC—to provide C&I testing of products built on the IEEE P1901.2 LF NB PLC standard.

HomePlug Broadband-Speed Technologies. In June 2011, the HomePlug Alliance put its support behind the IEEE P1905 working group's efforts to define the first standard for hybrid home networks. A P1905 network would include combinations of stationary home networking devices such as set-top boxes, home gateways, Blu-Ray players and televisions, and mobile devices such as laptops, tablets, and smartphones. The IEEE P1905 standard provides an abstraction layer to established powerline, wireless, coaxial cable, and Ethernet home networking technologies. The standard enables consumers and service providers to combine the capabilities of otherwise disparate networks to maximize a home network's overall performance and reliability. IEEE P1905's abstraction layer common interface allows applications and upper-layer protocols to be agnostic to the underlying home networking technologies. Packets can arrive and be transmitted over any technology according to QoS priorities. IEEE P1905 also simplified the network set-up by providing common set-up procedures for adding devices, establishing secure links, implementing QoS, and managing the network.

SE Initiative. In 2008, a number of utility companies (American Electric Power, Consumers Energy, Pacific Gas and Electric Company, Reliant Energy, Sempra, and Southern California Edison) announced that they are working with the ZigBee and

HomePlug alliances to develop a common application layer integrated solution for advanced metering infrastructure (AMI) and HANs. The three groups are expanding the application layer, enabling it to run on HomePlug technology, and providing utilities with industry standards for both wireless and wired HAN options when implementing new AMI programs. Shortly after the formation of the group, the Electric Power Research Institute (EPRI) began to collaborate to develop a common language for HAN devices to utilize the AMI. This arrangement further expands the Smart Grid by creating a standard communication approach between AMI systems and HANs, as well as a common set of certification procedures. As noted elsewhere, the term “smart energy” refers generally to actions and technologies that are used to improve the efficiency of energy consumption. Energy demand and costs are increasing rapidly, so utility companies are focusing on adopting communications and networking technologies to help consumers monitor and reduce their energy consumption.

REFERENCES

1. ETSI TR 101 557 V1.1.1 (2012-02), Electromagnetic Compatibility and Radio spectrum Matters (ERM); System Reference document (SRdoc); Medical Body Area Network Systems (MBANSs) in the 1785 MHz to 2500 MHz range.
2. Coronel P, Schott W, Schwieger K, Zimmermann E, Zasowski T, Chevillat P, editors. Briefing on Wireless Body Area and Sensor Networks, 8th Wireless World Research Forum (WWRF8bis) Meeting, Beijing, China, February 2004; (ii) 11th Wireless World Research Forum Meeting, Oslo, Norway, June 2004.
3. Practel, Inc., Role of Wireless ICT in Health Care and Wellness—Standards, Technologies and Markets, May 2012, Published by Global Information, Inc. (GII), 195 Farmington Avenue, Suite 208 Farmington, CT 06032 USA.
4. Gainspan, Gainspan Low-Power Embedded WI-FI VS ZigBee. GainSpan Corporation, 3590 N. First Street, Suite 300, San Jose, CA 95134, Available at http://www.gainspan.com.
5. Smith P. Comparing Low-Power Wireless Technologies. Tech Zone, Digikey Online Magazine, Digi-Key Corporation, 701 Brooks Avenue, South Thief River Falls, MN 56701 USA.
6. 3rd Generation Partnership Project (3GPP) Organization, Available at www.3gpp.org.
7. Third Generation Partnership Project 2 Organization, Available at http://www.3gpp2.org.
8. Bormann C. Getting Started with IPv6 in Low-Power Wireless. “Personal Area” Networks (6LoWPAN), Universität Bremen TZI, IETF 6lowpan WG and CoRE WG Co-Chair, IAB Tutorial on Interconnecting Smart Objects with the Internet, Prague, Saturday, 2011-03-26, Available at http://www.iab.org/about/workshops/smartobjects/tutorial.html.
9. ETSI Documentation, ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex—FRANCE.
10. Krasinski R, Nikolich P, Heile RF. IEEE 802.15.4j Medical Body Area Networks Task Group PAR, IEEE P802.15 Working Group for Wireless Personal Area Networks (WPANs), January18, 2011.

11. ISA, 67 Alexander Drive, P.O. Box 12277, Research Triangle Park, NC 27709, info@isa.org.
12. Minoli D. Satellite Systems Engineering in an IPv6 Environment. Boca Raton, FL: Francis and Taylor; 2009.
13. Minoli D. Hotspot Networks: Wi-Fi for Public Access Locations. New York, NY: McGraw-Hill; 2002.
14. Minoli D, *Wireless Sensor Networks* (co-authored with K. Sohraby and T. Znati). Hoboken, NJ: Wiley; 2007.
15. Emerson Process Management, IEC 62591 WirelessHART, System Engineering Guide, Revision 2.3, Emerson Process Management, 2011.
16. ZigBee Alliance, Available at http://www.zigbee.org/.
17. ZigBee Wireless Sensor Applications for Health, Wellness and Fitness, March 2009, ZigBee Alliance, Available at www.zigbee.org.
18. Duffy P. Zigbee IP: Extending the Smart Grid to Consumers. Cisco Blog – The Platform, June 4, 2012, Cisco Systems, Inc., 170 West Tasman Dr., San Jose, CA 95134 USA.
19. Shandle J. What does ZigBee Pro mean for your application?. EETimes Online Magazine, 11/27/2007, Available at http://www.eetimes.com.
20. Drake J, Najewicz D, Watts W. Energy efficiency comparisons of wireless communication technology options for smart grid enabled devices. White Paper, General Electric Company, GE Appliances & Lighting, December 9, 2010.
21. Montenegro G, Kushalnagar N, Hui J, Culler D. Transmission of IPv6 Packets over IEEE 802.15.4 Networks, RFC 4944, Updated by RFC 6282, RFC 6775 (was draft-ietf-6lowpan-format), September 2007.
22. Kingsley S. Personal Body Networks go Wireless at 2.4GHz. ElectronicsWeekly Online Magazine, 16 May 2012, Available at http://www.electronicsweekly.com.
23. IEEE 802.15 WPAN Task Group 1 (TG1), WPAN Home Page, Monday, June 20, 2005.
24. Bluetooth SIG Home page, Available at www.bluetooth.com (more info at www.bluetooth .org).
25. Fleishman G. Inside Bluetooth 2.0., Macworld, February 9, 2005.
26. Latuske R. Bluetooth Health Device Profile (HDP). White Paper, September 2009, ARS Software GmbH, Stanberger Strasse 22, D-82131, Gauting/Munchen, Germany, Available at http://www.ars2000.com/.
27. Kwak KS, Ullah S, Ullah N An Overview of IEEE 802.15.6 Standard (Invited Paper), ISABEL 2010 in Rome, Italy. UWB-ITRC Center, Inha University, 253 Yonghyun-dong, Nam-gu, Incheon (402–751), South Korea.
28. U.S. Department of Transportation, Research and Innovative Technology Administration. Intelligent Transportation Systems. December 2012, Available at http://www.its.dot.gov.
29. Fuxjäger P, Costantini A, et al. IEEE 802.11p Transmission Using GNURadio. Forschungszentrum Telekommunikation Wien, Donau-City-Strasse 1, A-1220 Vienna, Austria. And, University of Salento, 73100 Lecce, Italy. 2007.
30. TechnoCom. The WAVE Communications Stack: IEEE 802.11p, 1609.4 and, 1609.3. Presentation, September, 2007, TechnoCom, 2030 Corte del Nogal, Suite 200, Carlsbad, CA 92011 Available at http://www.ieeevtc.org/plenaries/vtc2007fall/34.pdf.

31. Weigle M. Standards: WAVE / DSRC /802.11p in Vehicular Networks, CS 795/895, Spring 2008, Old Dominion University.
32. IEEE WoWMoM 2012 Panel, San Francisco, California, USA June 25–28, 2012.
33. Rao YS, Pica F, Krishnaswamy D. 3GPP Enhancements for Machine Type Communications Overview. IEEE WoWMoM 2012 Panel, San Francisco, California, USA June 25–28, 2012.
34. Principi B. CTIA: Should M2M skip 3G and go right to 4G?. May 9, 2012, Online Article, Available at http://www.telecomengine.com.
35. Clark M, Neal BJ, Gullstrand C. Preparing for LTE Roaming. Syniverse Technologies, 120 Moorgate London, EC2M 6UR United Kingdom, March 2011, Available at www.syniverse.com.
36. Alcatel-Lucent. LTE—The UMTS Long Term Evolution: From Theory to Practice. Strategic Whitepaper, Available at www.alcatel-lucent.com, Wiley; 2009.
37. Sesia S, Toufik I, Baker M, editors, *LTE – The UMTS Long Term Evolution: From Theory to Practice*. Wiley; 2009.
38. PLCforum. Available at http://www.plcforum.org/frame_plc.html.
39. DSL Forum, DSL Forum, 48377 Fremont Blvd, Suite 117, Fremont, CA 94538, Available at http://www.dslforum.org.
40. Cacciaguerra F. Introduction to Power Line Communications (PLC). November 2003, Kioskea.net Online Magazine, Available at http://en.kioskea.net/contents/cpl/cpl-intro.php3.
41. Power Line Communications (PLC), Echelon Corporation, 550 Meridian Ave., San Jose, CA 95126 USA. Available at http://www.echelon.com.
42. Yu S. Final IEEE 1901 Broadband Over Power Line Standard Now Published. IEEE Press Release, February 1, 2011.
43. Yu S. IEEE P1901.2™ Standard FOR Low-Frequency, Narrowband Power Line Communications Enters Letter Balloting, IEEE Press Release, January 2012.
44. The HomePlug® Powerline Alliance, Available at http://www.homeplug.org.
45. 3GPP2 X.S0011-002-D. cdma2000 Wireless IP Network Standard: Simple IP and Mobile IP Access Services. Available at http://www.3gpp2.org/Public_html/specs/X.S0011-002-D_v1.0_060301.pdf, February 2006.
46. Alcatel-Lucent. Alcatel-Lucent Researches Opportunities for Delivering Enhanced Video Sharing Services with DOCOMO Euro-Labs. Press Release, Paris and Barcelona, February 15, 2011. Available at www.alcatel-lucent.com.
47. California Software Labs. Basic Streaming Technology and RTSP Protocol—A Technical Report, 2002. California Software Labs, 6800 Koll Center Parkway, Suite 100 Pleasanton CA 94566, USA.
48. Machine-to-Machine Communications (M2M); M2M Service Requirements. ETSI TS 102 689 V1.1.1 (2010-08). ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex—FRANCE.
49. Machine-to-Machine Communications (M2M); Functional Architecture Technical Specification, ETSI TS 102 690 V1.1.1 (2011-10), ETSI, 650 Route des Lucioles F-06921 Sophia Antipolis Cedex—FRANCE.
50. H.720. Overview of IPTV Terminal Devices and End-Systems. (also known as ex H.IPTV-TDES.0), October 2008. ITU-T Study Group 16. International Telecommunication Union, Telecommunication Standardization Bureau, Place des Nations, CH-1211 Geneva 20.

51. Near Field Communication.org, Advocacy Group, Available at http://www.nearfieldcommunication.or.
52. Patil B, Dommety G. Why the Authentication Data Suboption is Needed for Mobile IPv6 (MIPv6). RFC 5419, January 2009.
53. WiMAX Network Architecture—WiMAX End-to-End Network Systems Architecture. May 2008, Available at http://www.wimaxforum.org/documents/documents/WiMAX_Forum_Network_Architecture_Stage_23_Rel_1v1.2.zip.