CHAPTER 1

WHAT IS THE INTERNET OF THINGS?

1.1 OVERVIEW AND MOTIVATIONS

The proliferation of an ever-growing set of devices able to be directly connected to the Internet is leading to a new ubiquitous-computing paradigm. Indeed, the Internet—its deployment and its use—has experienced significant growth in the past four decades, evolving from a network of a few hundred hosts (in its ARPAnet form) to a platform capable of linking billions of entities globally. Initially, the Internet connected institutional hosts and accredited terminals via specially developed gateways (routers). More recently, the Internet has connected servers of all kinds to users of all kinds seeking access to information and applications of all kinds. Now, with social media, it intuitively and effectively connects all sorts of people to people, and to virtual communities. The growth of the Internet shows no signs of slowing down, and it is steadily becoming the infrastructure fabric of choice for a new paradigm for all-inclusive pervasive computing and communications. The next evolution is to connect all "things" and objects that have (or will soon have) embedded wireless (or wireline) connectivity to control systems that support data collection, data analysis, decision-making, and (remote) actuation. "Things" include, but are not limited to, machinery, home appliances, vehicles, individual persons, pets, cattle, animals, habitats, habitat occupants, as well as enterprises. Interactions are achieved utilizing a plethora of possibly different networks; computerized devices of various functions, form factors,

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

sizes, and capabilities such as iPads, smartphones, monitoring nodes, sensors, and tags; and a gamut of host application servers.

This new paradigm seeks to enhance the traditional Internet into a smart *Internet of Things* (IoT) created around intelligent interconnections of diverse objects in the physical world. In the IoT, commonly deployed devices and objects contain an embedded device or microprocessor that can be accessed by some communication mechanism, typically utilizing wireless links. The IoT aims at closing the gap between objects in the material world, the "things," and their logical representation in information systems. It is perceived by proponents as the "next-generation network (NGN) of the Internet." Thus, the IoT is a new type of Internet *application* that endeavors to make the thing's information (whatever that may be) available on a global scale using the Internet as the underlying connecting fabric (although other interconnection data networks, besides the Internet, can also be used such as private local area networks and/or wide area networks). The IoT has two attributes: (i) being an Internet application and (ii) dealing with the thing's information. The term *Internet of Things* was coined and first used by Kevin Ashton over a decade ago[1] (1). The "things" are also variously known as "objects," "devices," "end nodes," "remotes," or "remote sensors," to list just a few commonly used terms.

The IoT generally utilizes low cost information gathering and dissemination devices—such as sensors and tags—that facilitate fast-paced interactions in any place and at any time, among the objects themselves, as well as among objects and people. Actuators are also part of the IoT. Hence, the IoT can be described as a new-generation information network that enables seamless and continuous machine-to-machine (M2M)[2] and/or human-to-machine (H2M) communication. One of the initial goals of the IoT is to enable connectivity for the various "things"; a next goal is to be able to have the "thing" provide back appropriate, application-specific telemetry; an intermediary next step is to provide a web-based interface to the "thing" (especially when human access is needed); the final step is to permit actuation by the "thing" (i.e., to cause a function or functions to take place). Certain "things" are stationary, such as an appliance in a home; other "things" may be in motion, such as a car or a carton (or even an item within the carton) in a supply chain environment (either end-to-end, or while in an intermediary warehouse).

At the "low end" of the spectrum, the thing's information is typically coded by the unique identification (UID) and/or electronic product code (EPC); the information is (typically) stored in a radio frequency identification (RFID) electronic tag; and, the information is uploaded by noncontact reading using an RFID reader. In fact, UID and RFID have been mandated by the Department of Defense (DoD) for all their suppliers to modernize their global supply chain; RFID and EPC were also mandated

[1] Synonym key words are: "Ubiquitous computing (Ubi-comp), pervasive computing, ambient intelligence, sentient computing, and internet of objects." Multiple terminology terms should not confuse the reader, because, as a side note, often industry players redefine terms just to give the concept some cachet. For example, what some in the late 1960s called "time-sharing," others in the 1980s called it "utility computing." Then in the 1990s, people called it "grid computing." And now in the 2000s–2010s all the rage is "cloud." Same concepts, just new names.

[2] Some (e.g., 3GPP) also use the term machine-type communications (MTC) to describe M2M systems.

by Wal-Mart to all their suppliers as of January 1, 2006, and many other commercial establishments have followed suit since then. More generally, smart cards (SCs) will also play an important role in IoT; SCs typically incorporate a microprocessor and storage.

At the "mid range" of the spectrum, one finds devices with embedded intelligence (microprocessors) and embedded active wireless capabilities to perform a variety of data gathering and possibly control functions. On-body biomedical sensors, home appliance and power management, and industrial control are some examples of these applications.

At the other end of the spectrum, more sophisticated sensors can also be employed in the IoT: some of these sensor approaches use distributed wireless sensor network (WSN) systems that (i) can collect a wide variety of environmental data such as temperature, atmospheric and environmental chemical content, or even low- or high resolution ambient video images from geographically dispersed locations; (ii) can optionally pre-process some or all of the data; and (iii) can forward all these information to a centralized (or distributed/virtualized) site for advanced processing. These objects may span a city, region, or large distribution grid.

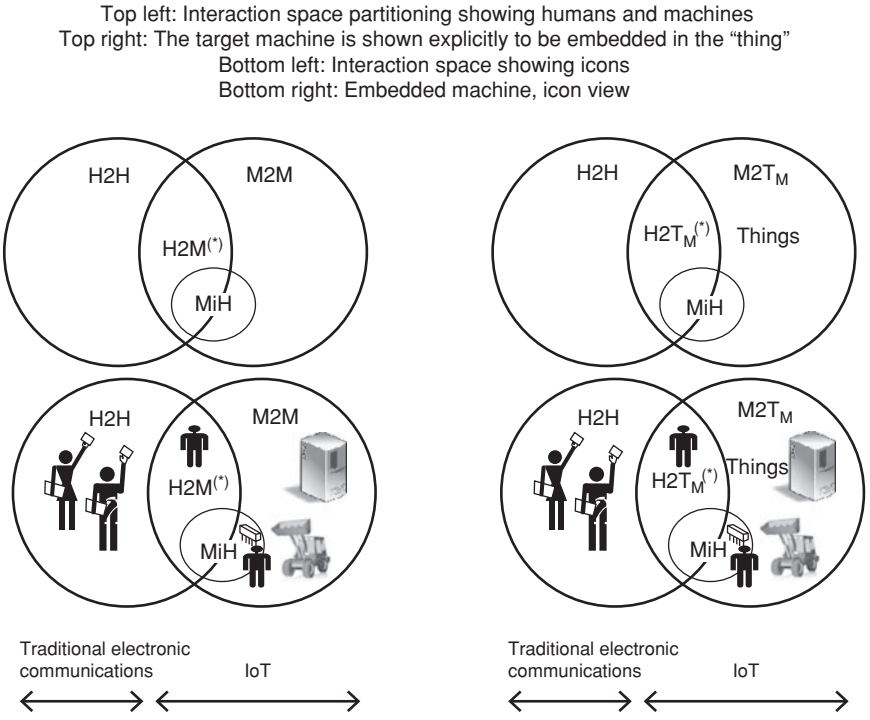
Other "things" may be associated with personal area networks (PANs), vehicular networks (VNs), or delay tolerant networks (DTNs).

The IoT is seen by many as a comprehensive extension of the Internet and/or Internet services that can establish and support pervasive connections between objects (things) (and their underlying intrinsic information) and data collection and management centers located in the network's "core" (possibly even in a distributed "cloud") (2,3). The IoT operates in conjunction with real-time processing and ubiquitous computing. The IoT is also perceived as a global network that connects physical objects with virtual objects through the combination of data capture techniques and communication networks. As such, the IoT is predicated on the expansion of the scope, network reach, and possibly even the architecture of the Internet through the inclusion of physical instrumented objects, such expansion fused with the ability to provide smarter services to the environment or to the end user, as more *in situ* transferable data become available. Some see the IoT in the context of ambient intelligence; namely, a vision where environment becomes smart, friendly, context aware, and responsive to many types of human needs. In such a world, computing and networking technology coexist with people in a ubiquitous, friendly, and pervasive way: numerous miniature and interconnected smart devices create a new intelligence and interact with each other seamlessly (4).

The IoT effectively eliminates time and space isolation between geographical space and virtual space, forming what proponents label as "smart geographical space" and creating new human-to-environment (and/or H2M) relationships. The latter implies that the IoT can advance the goal of integration of human beings with their surroundings. A smart environment can be defined as consisting of networks of federated sensors and actuators and can be designed to encompass homes, offices, buildings, and civil infrastructure; from this granular foundation, large-scale end-to-end services supporting smart cities, smart transportation, and smart grids (SGs), among others, can be contemplated. Recently, the IEEE Computer Society stated that

"... The Internet of Things (IoT) promises to be the most disruptive technology since the advent of the World Wide Web. Projections indicate that up to 100 billion uniquely identifiable objects will be connected to the Internet by 2020, but human understanding of the underlying technologies has not kept pace. This creates a fundamental challenge to researchers, with enormous technical, socioeconomic, political, and even spiritual, consequences. IoT is just one of the most significant emerging trends in technology ..." (5).

Figure 1.1 depicts the high level logical partitioning of the interaction space, showing where the IoT applies for the purpose of this text; the figure illustrates human-to-human (H2H) communication, M2M communication, H2M communications, and machine in (or on) humans (MiH) communications (MiH devices may include human embedded chips, medical monitoring probes, global positioning system (GPS) bracelets, and so on). The focus of the IoT is on M2M, H2M, and MiH applications; this range of applicability is the theme captured in this text.



H2H: Human to Human
H2M: Human to Machine = $H2T_M$: Human to Thing with Microprocessor/Machine
M2M: Machine to Machine = $M2T_M$: Machine to Thing with Microprocessor/Machine
MiH: Machine in Humans
(e.g., medical sensors)
(also includes chips in animals/pets)

(*) People have been communicating with computers for over half-a-century, but in this context "machine" means a microprocessor embedded in some objects (other than a traditional computer)

FIGURE 1.1 H2H, H2M, and M2M environment.

Recently, the IoT has been seen as an emerging "paradigm of building smart communities" through the networking of various devices enabled by M2M technologies (but not excluding H2M), for which standards are now emerging (e.g., from European Telecommunications Standards Institute [ETSI]). *M2M services* aim at automating decision and communication processes and support consistent, cost-effective interaction for ubiquitous applications (e.g., fleet management, smart metering, home automation, and e-health). *M2M communications* per se is the communication between two or more entities that do not necessarily need direct human intervention: it is the communication between remotely deployed devices with specific roles and requiring little or no human intervention. M2M communication modules are usually integrated directly into target devices, such as automated meter readers (AMRs), vending machines, alarm systems, surveillance cameras, and automotive equipment, to list a few. These devices span an array of domains including (among others) industrial, trucking/transportation, financial, retail point of sales (POS), energy/utilities, smart appliances, and healthcare. The emerging standards allow both wireless and wired systems to communicate with other devices of similar capabilities; M2M devices, however, are typically connected to an application server via a mobile data communication network.

IoT applications range widely from energy efficiency to logistics, from appliance control to "smart" electric grids. Indeed, there is increasing interest in connecting and controlling in real time all sorts of devices for personal healthcare (patient monitoring and fitness monitoring), building automation (also known as building automation and control (BA&C)—for example, security devices/cameras; heating, ventilation, and air-conditioning (HVAC); AMRs), residential/commercial control (e.g., security HVAC, lighting control, access control, lawn and garden irrigation), consumer electronics (e.g., TV, DVRs); PC and peripherals (e.g., mouse, keyboard, joystick, wearable computers), industrial control (e.g., asset management, process control, environmental, energy management), and supermarket/supply chain management (this being just a partial list). Figures 1.2–1.5 provide some pictorial views of actual IoT applications; these figures only depict illustrative cases and are not exhaustive or normative. As it can be inferred, however, in an IoT environment there are a multitude of applications and players that need to be managed across multiple platforms (6). Some see IoT in the context of the "Web 3.0" (a name/concept advanced by John Markoff of *The New York Times* in 2006), although this term has not yet gained industry-wide, consistent support (7). The proposed essence of the term implies "an intelligent Web," such as supporting natural language search, artificial intelligence/machine learning, and machine-facilitated understanding of information, with the goal of providing a more intuitive user experience. IoT might fit such paradigm, but does not depend on it.

The initial vision of the IoT in the mid-2000s was of a world where physical objects are tagged and uniquely identified by RFID transponders; however, the concept has recently grown in multiple dimensions, encompassing dispersed sensors that are able to provide real-world intelligence and goal-oriented collaboration of distributed smart objects via local interconnections (such as through wireless LANs, WSNs, and so on), or global interconnections (such as through the Internet). The

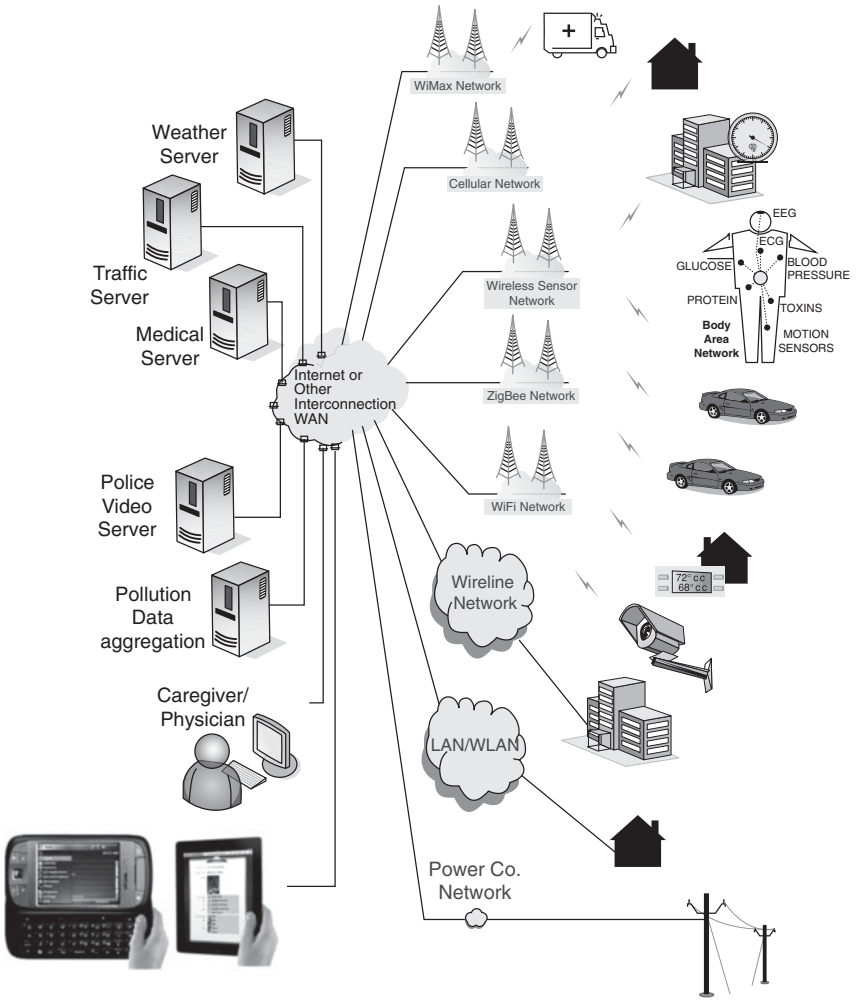


FIGURE 1.2 Illustrative example of the IoT.

seamless integration of communication capabilities between RFID tags, sensors, and actuators is seen as an important area of development. WSNs are likely the "outer tier" communication apparatus of the IoT. Thus, the IoT is not just an extension of today's Internet: it represents an aggregate of intelligent end-to-end systems that enable smart solutions, and, as such, it covers a diverse range of technologies, including sensing, communications, networking, computing, information processing, and intelligent control technologies, some of which are covered in this text.

As stated above, we take the IoT to encompass the M2M, H2M, and MiH space. It has been estimated that in 2011, there were 7 billion people on earth and 60 billion machines worldwide. Market research firm Frost & Sullivan recently forecasted that

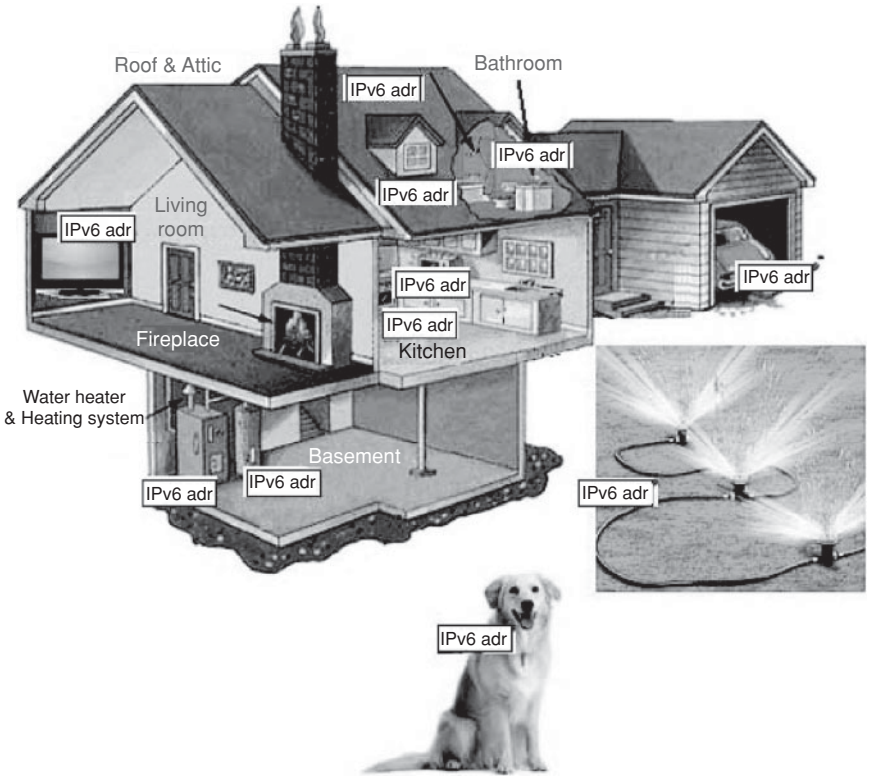


FIGURE 1.3 Another illustrative example of the IoT.

mobile computing devices, such as connected laptops, netbooks, tablets, and MiFi nodes, will increase to 50 million units by 2017 in the United States, while total cellular M2M connections are expected to increase from around 24 million in 2010 to more than 75 million over the same period; worldwide, the expectation is that the number of M2M device connections will grow from around 60 million in 2010 to over 2 billion in 2020 (8). Other market research puts the worldwide M2M revenues at over $38 billion in 2012 (9). Yet other market research companies project 15 billion connected devices moving 35 trillion gigabytes of data at a cost of $3 trillion annually by 2015 (10). These market data point to major development and deployment of the IoT technology in the next few years. Note that personal communication devices (smartphones, pads, and so on) can be viewed as machines or just simply as end nodes; when personal communication devices are used for H2M devices where the human employs the smartphone to communicate with a machine (such as a thermostat or a home appliance), then we consider the personal communication devices part of the IoT (otherwise we do not).

The definition of "IoT" has still some variability and can encompass different aspects depending on the researcher and/or the field in question. The European

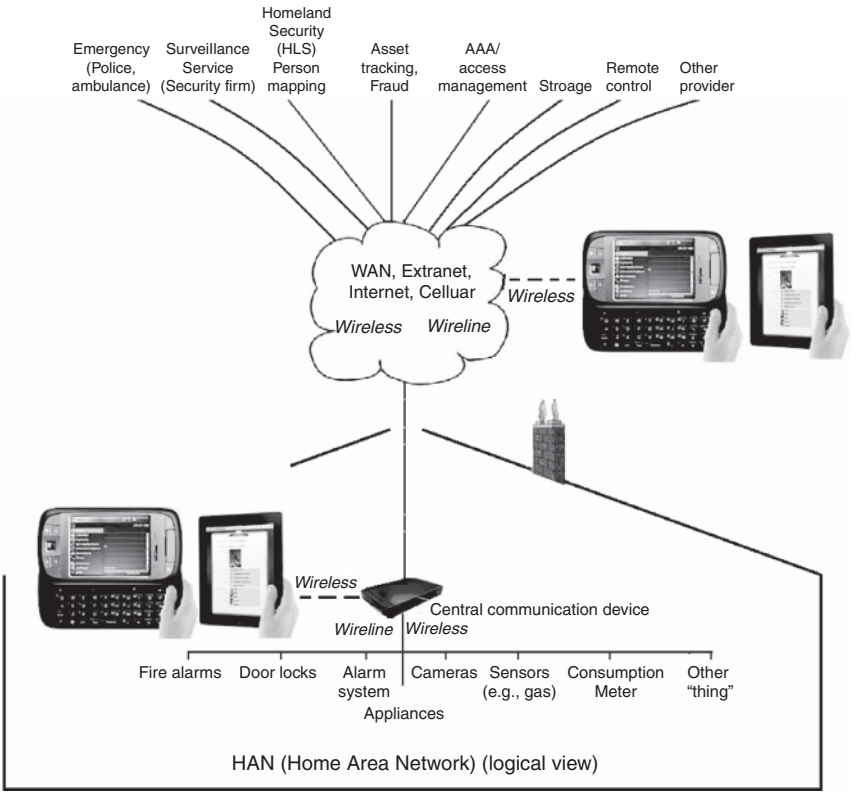


FIGURE 1.4 Yet another illustrative example of the IoT showing service providers.

Commission recently made these observations, which we can employ in our discussion of the IoT (11):

> "... Considering the functionality and identity as central it is reasonable to define the IoT as *"Things having identities and virtual personalities operating in smart spaces using intelligent interfaces to connect and communicate within social, environmental, and user contexts."* A different definition, that puts the focus on the seamless integration, could be formulated as "Interconnected objects having an active role in what might be called the Future Internet." The semantic origin of the expression is composed by two words and concepts: "Internet" and "Thing," where "Internet" can be defined as *"The world-wide network of interconnected computer networks, based on a standard communication protocol, the Internet suite (TCP/IP),"* while "Thing" is *"an object not precisely identifiable."* Therefore, semantically, "Internet of Things" means "a world-wide network of interconnected objects uniquely addressable, based on standard communication protocols ..."

Some see IoT as an environment where "things talk" and/or "things talk back" (7); effectively this simply means that devices have communication capabilities. The set of

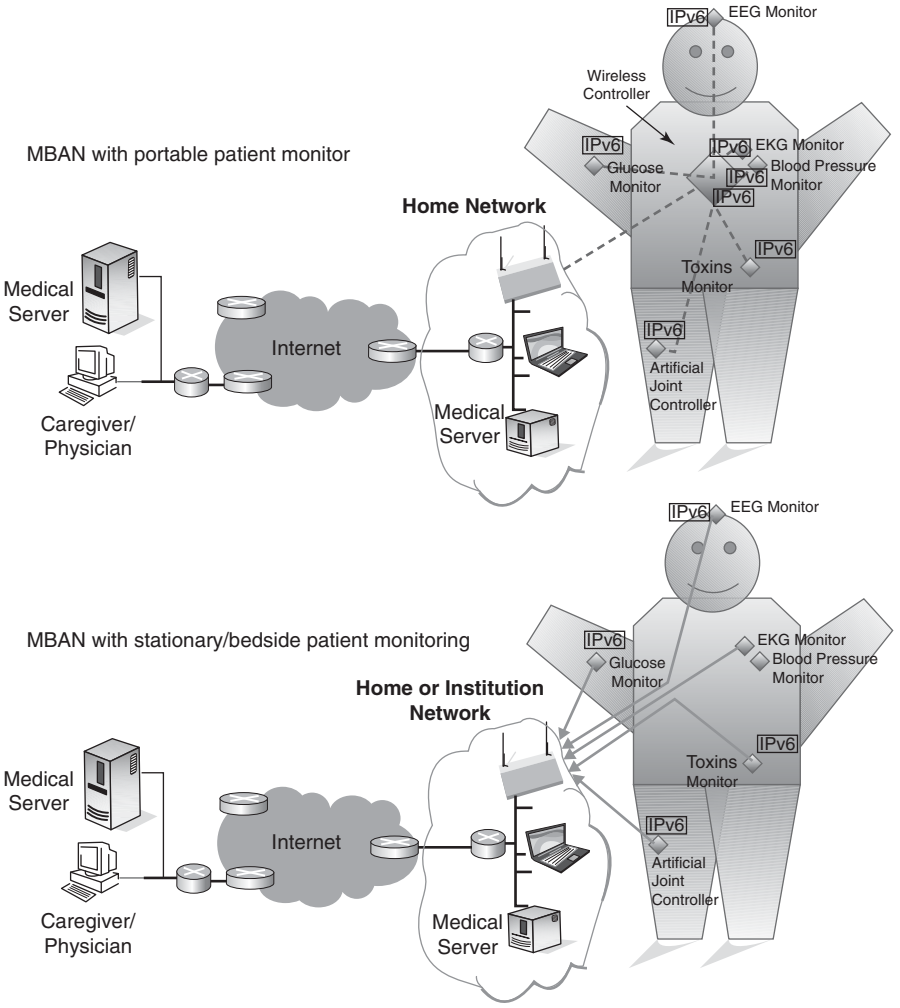


FIGURE 1.5 Yet another illustrative example of the IoT (body area network (BAN) application).

data and environmental awareness that objects should have depends on the application in question. Researchers are suggesting that objects should have the capability to be aware of such data as, but not limited to, its creation, transformation, ownership change, and physical-world parameters. Also, in some applications, objects should be able to interact actively with the environment, operating as actuators.

At a macro level, an IoT comprises a remote set of assets (a sensing domain), a network domain, and an applications domain. We define the data processing thing, also known as data integration point or person (DIPP), as the point (entity, person) where the administrative decisioning and/or the data accumulation takes place. We

define the "remote things," also known as data end points (DEPs), as the devices where events are sensed, data are collected, and/or an actuation takes place. Table 1.1 provides a working taxonomy of "things" in the IoT universe, as perceived in this text. There are interactions of interest between a DIPP being a human (H) and a "remote thing" being a machine/device (e.g., a thermostat) (such as a person changing the setting of the thermostat while away from home) or between two machines (M) (such as a server handling the usage reading from a residential electric meter). A person/human may use a PC or laptop, but increasingly a person may be using an iPad/tablet or a smartphone. The DIPP could be accessing the IoT system from a stationary location (e.g., a PC or server), from a wireless local environment (e.g., a fixed home hotspot), or from a completely mobile venue (e.g., using a smartphone). The "remote thing" could be stationary (e.g., a thermostat), on a wireless LAN or sensor network (but be relatively stationary), or be completely mobile (e.g., on a mobile ad hoc Network (MANET)—a self-configuring infrastructureless network of mobile devices connected by wireless links—or on a 3G/4G cellular network).

IoT is not seen by advocates as a future thing, but a set of capabilities that are already available at this time. Proponents and developers are endeavoring to reuse what is already available by way of the Internet suite of protocols, although there may be a need for some more research and/or standards, especially for large-scale, low power, broadly dispersed (where sensors are broadly dispersed in the environment) applications. An overriding goal is not to redesign the Internet (12); many researches position the IoT and work in support of the IoT simply as the (normal) "Evolution of the Internet" (what might be called by analogy with cellular networks, the long-term evolution of the Internet (LTEI)). A key observation is that if each of the large multitude of things in the IoT is to be addressed directly and individually, then a large address space is needed.

Cost as well as energy requirements of embedded devices require the use of efficient protocols and efficient communication architectures for the IoT. Standardization of IoT elements also becomes critical: the benefits of standardization include reduced complexity of IoT deployments, reduced deployment time for new services, lower capital requirements (CAPEX), and lower operating expense (OPEX). The IoT requires robust "last-yard," "last-mile," and "core" network technologies to make it a commercial reality.

Various technologies have indeed emerged in the past two decades that can be utilized for implementations, including PANs, such as IEEE 802.15.4; wireless local area networks (WLANs); WSNs; 3G/4G cellular networks; metro-Ethernet networks; multiprotocol label switching (MPLS); and virtual private network (VPN) systems. Wireless access and/or wireless ad hoc mesh systems reduce the "last-mile" cost of IoT applications, such as for distributed monitoring and control applications. However, we believe that the fundamental technical advancement that will foster the deployment of the IoT is IP Version 6 (IPv6). *In fact, IoT may well become the "killer-app" for IPv6.* IoT is deployable using IP Version 4 (IPv4) as has been the case in the recent past, but only IPv6 provides the proper scalability and functionality to make it economical, ubiquitous, and pervasive. There are many advantages in using IP for IoT, but we have to ascertain that the infrastructure and the supporting

TABLE 1.1 Taxonomy of "Things" in IoT

H2M										
DIPP "thing"	H	Stationary access/connectivity			Local mobility access/connectivity			Full mobility access/connectivity		
Remote "thing" (DEP)	M	Target device is stationary	Target device has local mobility	Target device has full mobility	Target device is stationary	Target device has local mobility	Target device has full mobility	Target device is stationary	Target device has local mobility	Target device has full mobility
Example		Access a home thermostat from an office PC	Access a monitor on a home-bound pet from an office PC	Access a GPS device on a teenager's car from an office PC	Access a home thermostat from a home, office, or hotspot wireless PC	Access a monitor on a home-bound pet from a home, office, or hotspot wireless PC	Access a GPS device on a teenager's car from a home, office, or hotspot wireless PC	Access a home thermostat from a smartphone	Access a monitor on a home-bound pet from a smartphone	Access a GPS device on a teenager's car from a smartphone
M2M										
DIPP "thing"	M1	Stationary access/connectivity			Local mobility access/connectivity			Full mobility access/connectivity		
Remote "thing" (DEP)	M2	Target device is stationary	Target device has local mobility	Target device has full mobility	Target device is stationary	Target device has local mobility	Target device has full mobility	Target device is stationary	Target device has local mobility	Target device has full mobility
Example		Access a home electrical meter from an office/ provider server	Access a monitor on a home-bound pet from an office/ provider server	Access a GPS device on a person's car from an office/ provider server	Access a home electrical meter from a WLAN-based office/ provider server	Access a monitor on a home-bound pet from a WLAN-based office/ provider server	Access a GPS device on a person's car from a WLAN-based office/ provider server	Access a home electrical meter from roaming-3G/ 4G based provider server	Access a monitor on a home-bound pet from a roaming-3G/ 4G-based provider server	Access a GPS device on a person's car from a roaming-3G/ 4G-based provider server

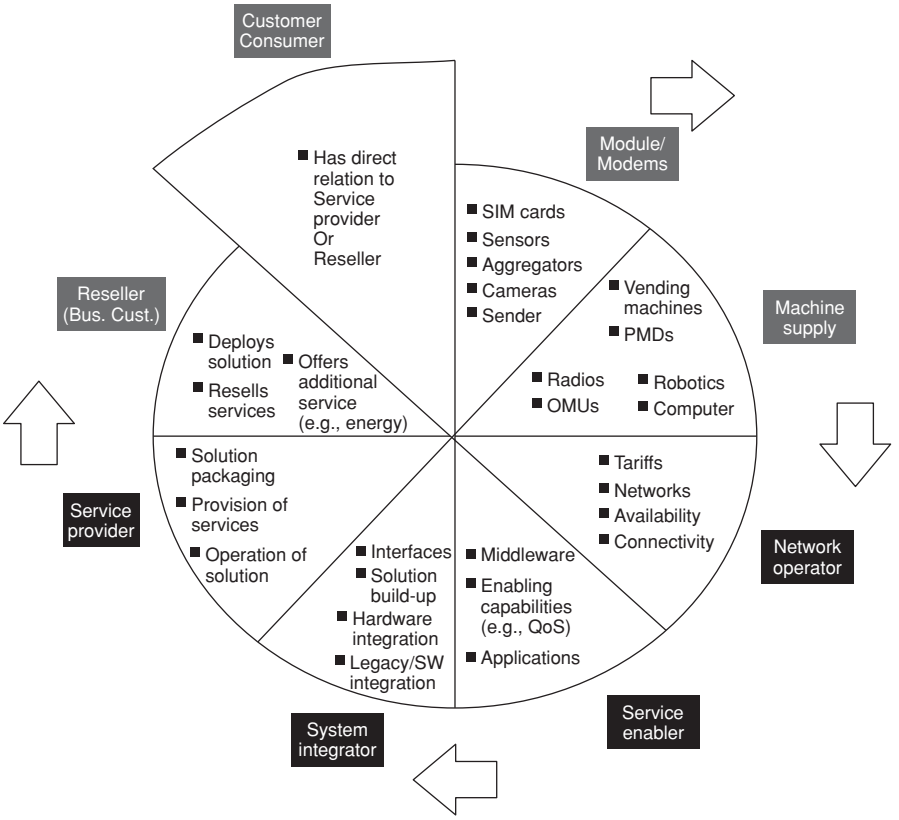


FIGURE 1.6 Stakeholder universe in the IoT/M2M world (representative, not complete view).

technology scale to meet the challenges. This is why there is a broad agreement that IPv6 is critical for the deployment of the IoT.

IoT stakeholders include technology investors, technology developers, planners with carriers and service providers, chief technical officers (CTOs), logistics professionals, engineers at equipment developers, technology integrators, Internet-backbone and ISP providers, cloud service providers, and telcos and wireless providers, both domestically and in the rest of the world. See Figure 1.6.

1.2 EXAMPLES OF APPLICATIONS

Vertical industries in arenas such as automotive and fleet management, telehealth (also called telecare by some) and Mobile Health (m-Health—when mobile communications are used), energy and utilities, public infrastructure, telecommunications, security and defense, consumer telematics, automated teller machines (ATMs)/kiosk/POS,

and digital signage are in the process of deploying IoT services and capabilities. Proponents make the claim that IoT will usher in a wide range of smart applications and services to cope with many of the challenges individuals and organizations face in their everyday lives. For example, remote healthcare monitoring systems could aid in managing costs and alleviating the shortage of healthcare personnel; intelligent transportation systems could aid in reducing traffic congestion and the issues caused by congestion such as air pollution; smart distribution systems from utility grids to supply chains could aid in improving the quality and reducing the cost of their respective goods and services; and, tagged objects could result in more systematic recycling and effective waste disposal (13). These applications may change the way societies function and, thus, have a major impact on many aspects of people's lives in the years to come. Many of today's home entertainment and monitoring systems often offer a web interface to the end user; the IoT aims at greatly extending those capabilities to many other devices and many other applications.

A short list of (early) applications includes the following (also see Table 1.2):

- Things on the move
  - Retail
  - Logistics
  - Pharmaceutical
  - Food
- Ubiquitous intelligent devices
- Ambient and assisted living
  - Health
  - Intelligent Home
  - Transportation
- Education and Information
- Environmental aspects/Resource Efficiency
  - Pollution and disaster avoidance

A longer, but far from complete, list of applications includes the following:

- Smart appliances
- Efficient appliances via the use of eco-aware/ambient-aware things
- Interaction of physical and virtual worlds; executable tags, intelligent tags, autonomous tags, collaborative tags
- Intelligent devices cooperation
- Ubiquitous readers
- Smart transportation
- Smart living
- *In vivo* health

TABLE 1.2 The Scope of IoT

Service Sector	Application Group	Location (Partial List)	Devices ("Things") of Interest (Partial List)
Real estate (industrial)	Commercial/ institutional	Office complex, school, retail space, hospitality space, hospital, medical site, airport, stadium	UPS, generator, HVAC, fire and safety (EHS), lighting, security monitoring, security control/access
	Industrial	Factory, processing site, inventory room, clean room, campus	
Energy	Supply providers/ consumers	Power generation, power transmission, power distribution, energy management, AMI	Turbine, windmills, UPS, batteries, generators, fuel cells
	Alternative energy systems	Solar systems, wind system, cogeneration systems	
	Oil/gas operations	Rigs, well heads, pumps, pipelines, refineries	
Consumer and home	Infrastructure	Home wiring/routers, home network access, home energy management	Power systems, HVAC/thermostats, sprinklers, MID, dishwashers, refrigerators, ovens, eReaders, washer/dryers, computers, digital videocameras, meters, lights, computers, game consoles, TVs, PDRs
	Safety	Home fire safety system, home environmental safety system (e.g., CO_2), home security/intrusion detection system, home power protection system, remote telemetry/video into home, oversight of home children, oversight of home based babysitters, oversight of home-bound elderly	
	Environmentals	Home HVAC, home lighting, home sprinklers, home appliance control, home pools and jacuzzis	
	Entertainment	TVs, PDRs	

TABLE 1.2 (*Continued*)

Service Sector	Application Group	Location (Partial List)	Devices ("Things") of Interest (Partial List)
Healthcare	Care	Hospitals, ERs, mobile POC, clinic, laboratories, doctor's office	MRIs, PDAs, implants, surgical equipment, BAN devices, power systems
	In vivo/home	Implants, home monitoring systems, body area networks (BANs)	
	Research	Diagnostic laboratory, pharmaceutical research site	
Industrial	Resource automation	Mining sites, irrigation sites, agricultural sites, monitored environments (wetlands, woodlands, etc.)	Pumps, valves, vets, conveyors, pipelines, tanks, motors, drives, converters, packaging systems, power systems
	Fluids management	Petrochemical sites, chemical sites, food preparation site, bottling sites, wineries, breweries	
	Converting operations	Metal processing sites, paper processing sites, rubber/plastic processing sites, metalworking site, electronics assembly site	
	Distribution	Pipelines, conveyor belts	
Transportation	Nonvehicular	Airplanes, trains, busses, ships/boats, ferries	Vehicles, ships, planes, traffic lights, dynamic signage, toll gates, tags
	Vehicles	Consumer and commercial vehicle (car, motorcycle, etc.), construction vehicle (e.g., crane)	
	Transportation subsystems	Toll booths, traffic lights and traffic management, navigation signs, bridge/tunnel status sensors	

(*continued*)

TABLE 1.2 (*Continued*)

Service Sector	Application Group	Location (Partial List)	Devices ("Things") of Interest (Partial List)
Retail	Stores	Supermarkets, shopping centers, small stores, distribution centers	POS terminals, cash registers, vending machines, ATMs, parking meters
	Hospitality	Hotel, restaurants, café', banquet halls, shopping malls	
	Specialty	Banks, gas stations, bowling, movie theaters	
Public safety and security	Surveillance	Radars, military security, speed monitoring systems, security monitoring systems	Vehicles, ferries, subway trains, helicopters, airplanes, video cameras, ambulances, police cars, fire trucks, chemical/radiological monitors, triangulation systems, UAVs
	Equipment	Vehicles, ferries, subway trains, helicopters, airplanes	
	Tracking	Commercial trucks, postal trucks, ambulances, police cars	
	Public infrastructure	Water treatment sites, sewer systems, bridges, tunnels	
	Emergency services	First responders	
IT systems and networks	Public networks	Network facilities, central offices, data centers, submarine cable, cable TV headends, telco hotels, cellular towers, poles, teleports, ISP centers, lights-off sites, NOCs	Network elements, switches, core routers, antenna towers, poles, servers, power systems, backup generators
	Enterprise networks	Data centers, network equipment (e.g., routers)	

- Security-based living
- Energy and resource conservation
- Advanced metering infrastructure (AMI)
- Energy harvesting (biology, chemistry, induction)
- Power generation in hash environments
- Energy recycling
- Ambient intelligence
- Authentication, trust, and verification

- Search the physical world ("Google of things")
- Virtual worlds
- Web of things (WoT) which aims for direct web connectivity by pushing its technology down to devices

Regarding **retail**, the first large-scale application of the IoT technologies will be to replace the bar code in retail environments. The challenge so far has been the (i) higher cost of the tag over the bar code, (ii) some needed technology improvement for transportation of metals and liquid items, and (iii) privacy concerns. Nonetheless, the replacement has already started in some pilot projects. Although one may expect to see the coexistence of the two identification mechanisms for many years into the future, advances in the electronics industry will make the RFID tag more affordable and, thus, more attractive and accessible to the retailers. **Logistics** aims at improving efficiency of processes or enables new value-added features. The warehouses of the future will likely become completely automated, with items being checked in and out and orders automatically passed to the suppliers. For example, with IoT techniques foods may be transported without human intervention from producer to consumer, and the manufacturers will have a direct feedback on the market's needs. **Health** logistics is one of the near-term applications of IoT, noting, for example, that reportedly more than 7000 people lose their lives in US hospitals every year because of the errors in medication delivery to the patient. *Health logistics, the flow of drugs and patients, requires one to design systems that can be supported by the healthcare workers and that can be integrated from the supply chain to the bedside, and even before the patient is admitted to a hospital (11).* The cost of healthcare is rising every year, having reached 16% to 17% of the US gross domestic product (GDP), with the trend to add at least 1% each year. Wide utilization of wireless communications in conjunction with mobile monitoring devices can reduce healthcare costs by billions of dollars on an annual basis, with much of that savings derived by reducing hospitalizations and extending independent living for seniors (14). These observations are but a small sample of the applications and scope of IoT. The evolution to a connected world spans the arena of measurement, data collection, state inference, and reaction. Some researchers also see a convergence of utility computing (cloud computing) with the IoT (15). These and other practical applications will be discussed in the chapters that follow, particularly in Chapter 3.

1.3 IPv6 ROLE

We retain the position that *IoT may well become the "killer-app" for IPv6.* Using IPv6 with its abundant address spaces, globally unique object (thing) identification and connectivity can be provided in a standardized manner without additional status or address (re)processing—hence, its intrinsic advantage over IPv4 or other schemes.

It is both desirable as well as feasible for all physical (and even virtual or logical) objects to have a permanent unique identifier, an object ID (OID). It is also desirable as well as feasible for all end-point network locations and/or intermediary-point

network locations to have a durable unique network address (NAdr); the IPv6 address space enables the concrete realization of these goals. When objects that have enough intelligence to (run a communication protocol stack so that they can) communicate are placed on a network, these objects can be tagged with an NAdr. Every object then has a tuple (OID, NAdr) that is always unique, although the second entry of the tuple may change with time, location, or situation. In a stationary, nonvariable, or mostly static environment, one could opt, if one so chose, to assign the OID to be identical to the NAdr where the object is expected to attach to the network; that is, the object inherits the tuple (NAdr, NAdr). In the rare case where the object moved, the OID could then be refreshed to the address of the new location; that is, the object then inherits the tuple (NAdr', NAdr'). However, there is a general trend toward object mobility, giving rise to a dynamic environment (e.g., for mobile or variable case); hence, to retain maximal flexibility it is best to separate, in principle, the OID from the NAdr and thus assign a general (OID, NAdr) tuple where the OID is completely invariant; however, the OID can still be drawn from the NAdr space, that is from the IPv6 address space.

What was described above is not feasible in an IPv4 world, because in the 32-bit address space, only $2^{32} \sim 10^{10}$ NAdr location can be identified uniquely. IPv6 offers a much larger 2^{128} space; hence, the number of available unique node addressees is $2^{128} \sim 10^{39}$. IPv6 has more than 340 undecillion (340,282,366,920,938,463,463,374, 607,431,768,211,456) addresses, grouped into blocks of 18 quintillion addresses. Already today many tags operate with a 128-bit OID field that allows $2^{128} \sim 10^{39}$ ($\approx 3.4 \times 10^{38}$) unique identifiers, but the tuple (OID, NAdr = OID) could not be defined uniquely in the IPv4 world.

IPv6 was originally defined in 1995 in request for comments (RFC) 1883 and then further refined by RFC 2460, "Internet Protocol, Version 6 (IPv6) Specification," authored by S. Deering and R. Hinden (December 1998). A large body of additional RFCs has emerged in recent years to add capabilities and refine the IPv6 concept. IPv6 embodies IPv4 best practices but removes unused or obsolete IPv4 characteristics; this results in a better-optimized Internet protocol. Some of the advantages of IPv6 include the following:

- Scalability and expanded addressing capabilities: as noted, IPv6 has 128-bit addresses versus 32-bit IPv4 addresses. With IPv4, the theoretical number of available IP addresses is $2^{32} \sim 10^{10}$. IPv6 offers a much larger 2^{128} space. Hence, the number of available unique node addressees is $2^{128} \sim 10^{39}$.
- "Plug-and-play": IPv6 includes a "plug-and-play" mechanism that facilitates the connection of equipment to the network. The requisite configuration is automatic; it is a serverless mechanism.
- Security: IPv6 includes and requires security in its specifications such as payload encryption and authentication of the source of the communication. End-to-end security, with built-in strong IP-layer encryption and authentication (embedded security support with mandatory IP security (IPsec) implementation), is supported.

- Mobility: IPv6 includes an efficient and robust mobility mechanism namely an enhanced support for mobile IP, specifically, the set of mobile IPv6 (MIPv6) protocols, including the base protocol defined in RFC 3775.

For the IoT as well as for other applications for smartphones and similar devices, there is a desire to support direct communication between mobile nodes (MNs) and far-end destinations, whether such far-ends are themselves a stationary node or another MN. Such far-end destination could be, for example, a roving sensor collecting environmental or other data. In order to efficiently maintain reacheability, thus supporting flexible mobility, the goal is to retain the same explicit IP address regardless of the real-time location or specific network elements and/or networks used to support connectivity. This is not easily achievable with IPv4 for a number of reasons; however, MIPv6 described in RFC 3775, "Mobility Support in IPv6" (June 2004), among others, facilitates this task. RFC 3775 is known as the "MIPv6 base specification." RFCs are specifications and related materials published by the Internet Engineering Task Force (IETF). IPv6 mobility, specifically MIPv6, relies on IPv6 capabilities.

RFC 3775 notes that without specific support for mobility in IPv6, packets destined to an MN would not be able to reach it while the MN is away from its home network. In order to continue communication in spite of its movement, an MN could change its IP address each time it moves to a new link, *but the MN would then not be able to maintain transport and higher-layer connections when it changes location*. Mobility support in IPv6 is particularly important, as mobile users are likely to account for a majority, or at least a substantial fraction, of the population of the Internet during the lifetime of IPv6, including instrumented objects, which is the topic of this text. MIPv6 allows nodes to remain reachable while moving around in the IPv6 Internet: it enables a device (an MN) to change its attachment point to the Internet without losing higher-layer functionality through the use of tunneling between it and a designated home agent (HA). Stated another way, MIPv6 enables an MN to maintain its connectivity to the Internet when moving from one AR to another, a process referred to as handover. See Figure 1.7.

Two fundamental questions are: (1) how to deliver and/or receive information from an instrumented object and (2) how to do so in the presence of mobility. It is to be understood that mobility management (items 1 and 2 just listed) can be handled, to some (considerable) degree, by acquiring new physical links at the physical layer, namely, via a new channel acquisition at the PHY layer as supported by a cellular-level cell handoff (or a WiFi, WiMAX, or ZigBee handoff), in a transparent manner to the upper layers (which include IP and higher layers supporting the video stream). However, there are situations where an IP-level handoff is desirable; MIPv6 addresses the latter case. Figure 1.8 depicts the protocol stacks at a generic level supporting these two modes.

These (IPv6) mechanisms, which give objects the ability of addressing each other and of verifying their respective identities, enable all the objects to exchange information, if they so choose and/or if it is necessary. This enables one to create a highly woven fabric of processing hosts, communication nodes and relays, sensors, and actuators.

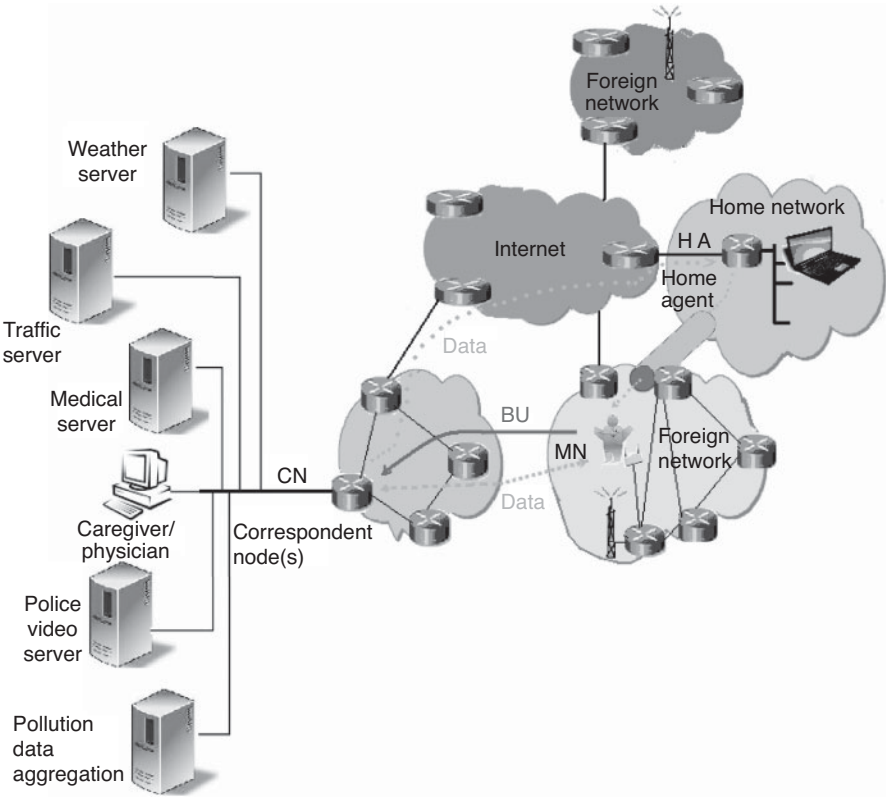


FIGURE 1.7 Communication supported in MIPv6 through the HA.

1.4 AREAS OF DEVELOPMENT AND STANDARDIZATION

Despite significant technological advances in many subtending disciplines, difficulties associated with the evaluation of IoT solutions under realistic conditions in real-world experimental deployments still hamper their maturation and significant rollout. Obviously, with limited standardization, there are capability mismatches between different devices; also, there are mismatches between communication and processing bandwidth. While IoT systems can utilize existing Internet protocols, as mentioned earlier, in a number of cases the power-, processing-, and capabilities-constrained IoT environments can benefit from additional protocols that help optimize the communications and lower the computational requirements. The M2M environment

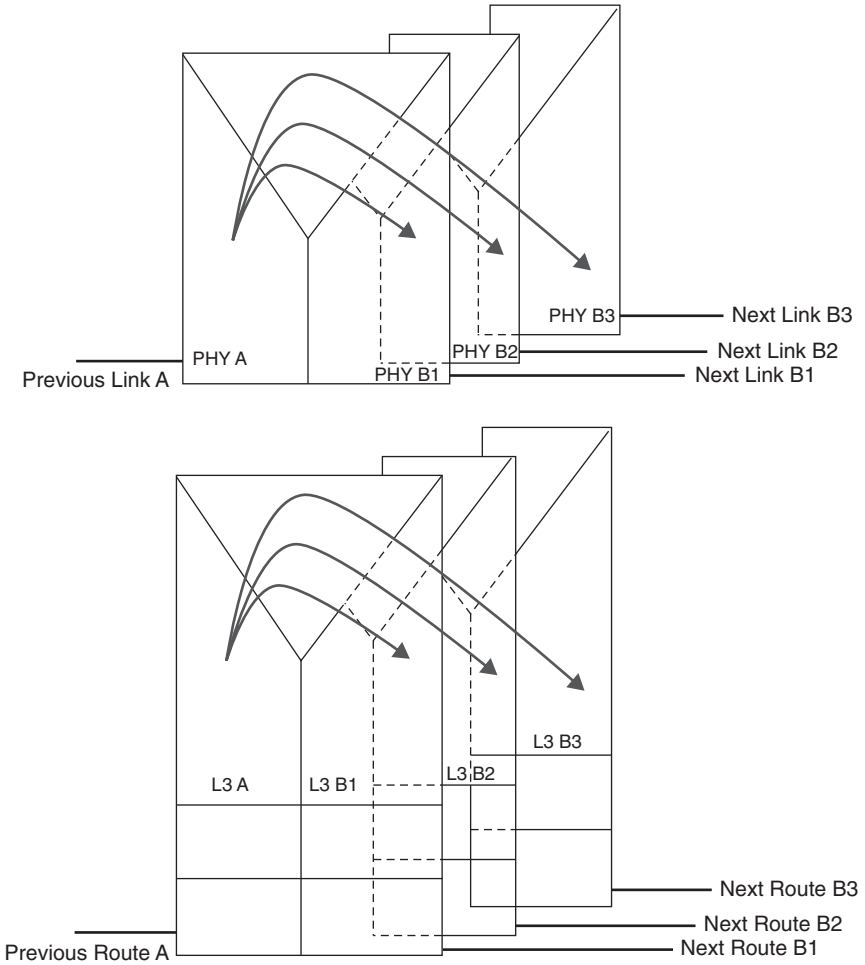


FIGURE 1.8 Handoff at the physical (e.g., cellular) or IP (e.g., routing) layer.

has been a fragmented space, but recent standardization efforts are beginning to show results.

Some see the four "pillars" supporting or defining the IoT: (i) M2M/MTC as the "Internet of devices"; (ii) RFID as the "Internet of objects"; (iii) WSN as the "Internet of transducers"; and (iv) supervisory control and data acquisition (SCADA) as the "Internet of controllers" (7). Certainly, these are the constituent elements of the IoT ecosystems, but they do not uniquely define the space, especially since WSNs are not uniquely well defined, and SCADA and RFIDs are legacy technologies. We see the IoT mostly, but not exclusively, as a new generation of collaborative, ubiquitous-computing entities that have significant embedded computing/communication capabilities, by and large using wireless links at the physical/media access layer and

migrating (or natively using) IPv6 at the networking layer; while not aiming at excluding any subsegment of the space, a forward-looking environment is assumed and predicated in our discussion.

Standards covering many of the underlying technologies are critical because proprietary solutions fragment the industry. Standards are particularly important when there is a requirement to physically or logically connect entities across an interface. Device-, network-, and application standards can enable global solutions for seamless operations at reduced costs. The focus of this text is to make the case that IPv6 is the fundamental optimal network communication technology to deploy IoT in a robust, commercial manner rather than just a preliminary desktop "science experiment" in some academic researcher's laboratory. (Layer 2 wireless technologies are also critical to IoT's end-to-end connectivity.)

IoT standardization spans several domains, including physical interfaces, access connectivity (e.g., low power IEEE802.15.4-based wireless standards such as IEC62591, 6LoWPAN, and ZigBee Smart Energy (SE) 2.0, DASH7, ETSI M2M), networking (such as IPv6), and applications. Some studies have shown that for the home two wireless physical layer communication technologies that best meet the overall performance and cost requirements are Wi-Fi (802.11/n) and ZigBee (802.15.4) (16). Examples of standardization efforts targeted for these environments include the initiatives known as "constrained RESTful environments (CoRE)," "IPv6 over low power WPAN (6LoWPAN)," and "routing over low power and lossy networks (ROLL)," which have been (and are being) studied by appropriate working groups of the IETF (12).

Some specific considerations need to be taken when designing protocols and architectures for interconnecting smart objects to the Internet, including scalability, power efficiency, interworking between different technologies and network domains, usability and manageability, and security and privacy (12). To make the IoT a practical pervasive reality, significant research needs to be conducted within and across these technological aspects of IoT. This has recently motivated a voluminous amount of research activities in the field. Some areas of active research include but are not limited to the following (13–15):

- Standardization at all layers/domains
- Architectures and middlewares for IoT integration
- Protocols for smart things: end-to-end/M2M protocols and standardization
- Mobility management
- Cloud computing and things internetworking
- Lightweight implementations of cryptographic stacks
- End-to-end security capabilities for the things
- Bootstrapping techniques
- Routing protocols for the IoT
- Global connectivity

1.5 SCOPE OF THE PRESENT INVESTIGATION

Given potential benefit of the technology, corporate and technical planners may be asking questions such as, but not limited to, "What is the IoT?", "How can it help my specific operation?", "What is the cost of deploying such a system?", and "What are the security implications?". This text addresses the following IoT aspects: IPv6 technologies, MIPv6 technologies, applications, key technologies for the IoT applications, implementation approaches, implementation challenges, and mid-range and long-range opportunities.

Observations such as these give impetus to the investigation in this text (11):

> "... RFID and related identification technologies will be the cornerstone of the upcoming Internet of Things ... While RFID was initially developed with retail and logistics applications in mind in order to replace the bar code, developments of active components will make this technology much more than a simple identification scheme. In the not too distant future, it can be expected that a single numbering scheme, such as IPv6, will make every single object identifiable and addressable. Smart components will be able to execute different set of actions, according to their surroundings and the tasks they are designed for. There will be no limit to the actions and operations these smart "things" will be able to perform: for instance, devices will be able to direct their transport, adapt to their respective environments, self-configure, self-maintain, self-repair, and eventually even play an active role in their own disposal. To reach such a level of ambient intelligence, however, major technological innovations and developments will need to take place. Governance, standardization and interoperability are absolute necessities on the path towards the vision of things able to communicate with each other..."

and (8):

> "The M2M Evolution: In a "Perfect Storm" of technology adoption, M2M is leveraging modern Internet technologies and infrastructures with mature IT middleware and solutions to address the Enterprise's desire for better utilizing operational assets and their associated information."

and (9):

> "M2M is poised to become an integral part of the telecoms landscape with a potentially transformative impact on a vast number of industries—with an equally vast number of services and applications to monetize. As operators struggle to gain market share in a time of subscriber saturation, M2M represents an opportunity to transform revenue streams, ARPU and churn rates... M2M is already being successfully utilized in several industries, with impressive results... With other industries as diverse as automotive and e-health... smart services, smart metering and the connected home promise a future of eco-friendly energy use, technologically advanced living spaces and machine to machine connectivity. M2M seeks to improve the lives of subscribers, the success of enterprises and the operations of service providers..."

and (17):

> "After years of anticipation, the M2M era has finally arrived. A new Yankee Group forecast predicts enterprise cellular M2M connections worldwide will surge from 81.8 million in 2011 to nearly 217.5 million in 2015. In the same time frame, connectivity revenue will more than double from U.S. $3.1 billion to U.S. $6.7 billion, making the M2M market one of the highest growth areas in the wireless arena during the next decade . . . Falling hardware prices and the increased availability of end-to-end solutions have established a more accessible M2M market for enterprises around the world."

and (18):

> "The IoT makes possible for virtually any object around us to exchange information and work in synergy to increase quality of our life. There are smart clothes which will interact intelligently with climate control of car and home to select the most suitable temperature and humidity for the person. Smart book interacts with entertainment devices such as TV in order to elaborate the topic we are reading . . . "

and (19):

> " . . . the possibilities and opportunities are endless . . . "

and (20):

> The IoT is a key enabler for the realization of M2M, as it allows for the pervasive interaction with/between smart things leading to a effective integration of information into the digital world. These smart (mobile) things – which are instrumented with sensing, actuation, and interaction capabilities – have the means to exchange information and influence the real world entities and other actors of a smart city eco-system in real time, forming a smart pervasive computing environment. The objective is to reach a global access to the services and information through the so-called Web of Things and efficient support for global communications, in order to embrance the M2M communications in the future IoT composed of IPv6 network and various smart things . . . issues such as the adaptation of legacy technologies and RFID to IPv6 and the Future IoT, security and privacy requirements in Smart Cities and the design of a secure and privacy-aware IoT, as well as the definition of new advanced architectures and models for the Internet and its application to smart livable Cities, [are important].

After the introductory chapter, Chapter 2 provides a formal framework for the IoT. Chapter 3 identifies a number of practical IoT applications, including BANs and over-the-air-passive surveillance (such as the Ring of Steel in London and now in many US cities). Chapter 4 looks at fundamental IoT mechanisms, for example, addressing, followed by a survey of key technologies to support the IoT applications. Emerging and applicable standards are discussed in Chapter 5. Chapter 6 discusses wireless connectivity at Layer 1 and Layer 2. Chapter 7 discusses connectivity at Layer 3, specifically IPv6 mechanisms, which are critical to the large-scale deployment of the IoT. Chapter 8 reviews MIPv6 technologies for possible mobile applications

while Chapter 9 provides an overview of 6LoWPAN which is ideally suited to IoT environments.

Interested readers include technology investors, researchers and academics, technology developers, planners with carriers and service providers, technology integrators, Internet-backbone and ISP providers, cloud service providers, and telcos and wireless providers.

This text is one in a series of texts by the author on the topic of IPv6. We are not implying in this text that IPv6 and/or MIPv6 is *strictly and uniquely required* to support IoT developments—early deployments are, in fact, using IPv4. We are advocating, however, that platforms based on these protocols provide an ideal, future-proof, scalable, and ubiquitous environment for such evolving services and capabilities. Appendix 1.A identifies some related books, a number of which are edited monographs; our treatise endeavors to put emphasis on the use of IPv6.

APPENDIX 1.A: SOME RELATED LITERATURE

This appendix contains some related literature. As it can be seen, most of this IoT literature is fairly recent and, therefore, does not uniquely cover the focus of this text, which is related to IPv6 being the fundamental optimal communication technology to deploy IoT in a robust commercial manner rather than just a desktop "science experiment" in some academic researcher's laboratory.

Here are some related books, a number of which are edited monographs:

- (Edited text) Giusto D, Iera A, Morabito G, Atzori L, editors, *The Internet of Things: 20th Tyrrhenian Workshop on Digital Communications*.1st ed. Springer; 2010.
- (Edited text) Uckelmann D, Harrison M, Michahelles F, editors, *Architecting the Internet of Things*, Springer; 2011.
- (Edited text) Chaouchi H, editor, *The Internet of Things: Connecting Objects*, Wiley; 2012.
- (Edited text) Chabanne H, Urien P, Susini J-F, editors, *RFID and the Internet of Things*, Wiley-ISTE; 2011.
- Lu Yan, Yan Zhang, Laurence T. Yang, *The Internet of Things: from RFID to the Next-generation Pervasive Networked Systems*, Wireless Networks and Mobile Communications Series, CRC Press, Taylor and Francis Group; 2008.
- Evdokimov S, Fabian B, Günther O, Ivantysynova L, Ziekow H, *RFID and the Internet of Things: Technology, Applications, and Security Challenges*, Hanover, Mass.: Now Publishers Inc.; 2011.
- Hazenberg W, Huisman M, *Meta Products: Building the Internet of Things*,Amsterdam, NL: BIS Publishers; 2011.

- Hersent O, Boswarthick D, Elloumi O, *The Internet of Things: Key Applications and Protocols.* New York: Wiley; 2012.
- Zhou H, *The Internet of Things in the Cloud: A Middleware Perspective*, New York, NY: CRC Press; 2013.

REFERENCES

1. Ashton K. That 'Internet of things' thing. RFID Journal, 2009.
2. Ping L, Quan L, Zude Z, Wang H. Agile supply chain management over the Internet of Things. 2011 International Conference on Management and Service Science (MASS), 2011 Aug, 1–4; Wuhan, China.
3. Zheng J, Simplot-Ryl D, et al. The Internet of Things. IEEE Communications Magazine, November 2011;49(11):30–31.
4. Practel, Inc., Role of Wireless ICT in Health Care and Wellness – Standards, Technologies and Markets, May, 2012. CT: Published by Global Information, Inc. (GII).
5. IEEE Computer. The Internet of Things: The Next Technological Revolution. Special Issue, February 2013.
6. Schlautmann A. Embedded Networking Systems in the Smart Home & Office. *M2M Zone Conference* at the International CTIA Wireless 2011; 2011 Mar 22–24;Orange County Convention Center, Orlando Florida.
7. Zhou H. *The Internet of Things in the Cloud: A Middleware Perspective*. New York: CRC Press; 2013.
8. Duke-Woolley R. Wireless Enterprise, Industry & Consumer Apps for the Automation Age. *M2M Zone Conference* at the International CTIA Wireless 2011; 2011 Mar 22–24; Orange County Convention Center, Orlando Florida.
9. Peerun S. Machine to Machine (M2M) Revenues Will Reach $38.1bn in 2012. Visiongain Report, United Kingdom; 2012.
10. Kreisher K. Intel: M2M data tsunami begs for analytics, security. Online Magazine, (Oct 8), 2012. Available at http://www.telecomengine.com.
11. *Internet of Things in 2020 – Roadmap For The Future,* INFSO D.4 Networked Enterprise & RFID, INFSO G.2 Micro & Nanosystems in co-operation with the Working Group RFID Of The ETP EPOSS. (European Commission – Information Society and Media.) Version 1.1–27, May, 2008.
12. Internet Architecture Board, Interconnecting Smart Objects with the Internet Workshop 2011, 25th March 2011, Prague.
13. Gluhak A, Krco S, et al. A Survey on Facilities for Experimental Internet of Things research. Communications Magazine, IEEE, 2011;49(11):58–67.
14. Staff. Smart networked objects and Internet of Things. White paper, January 2011, Association Instituts Carnot, 120 avenue du Général Leclerc, 75014 Paris, France.
15. Ladid L. Keynote Speech, International Workshop on Extending Seamlessly to the Internet of Things (esloT-2012), in conjunction with IMIS-2012 International Conference; 2012 July 4–6; Palermo, Italy.
16. 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.

17. Yankee Group. *Global Enterprise Cellular M2M Forecast*, April 2011, Boston, MA. Available at www.yankeegroup.com.
18. Lee GM, Park J, Kong N, Crespi N. The Internet of Things – Concept and Problem Statement. July 2011. Internet Research Task Force, July 11, 2011, draft-lee-iot-problem-statement-02.txt.
19. Principi B. CTIA: Global M2M deployments becoming a reality. Telecom Engine Online Magazine, (May 9) 2012. Available at www.telecomengine.com.
20. Ladid L, Skarmeta A, Ziegler S. Symposium On Selected Areas In Communications: Internet Of Things Track, IEEE 2013 Globecom, December 9–13, Atlanta, GA, U.S.A.