MODULE 1

Emergence of IoT

Learning Outcomes

After reading this chapter, the reader will be able to:

- Explain the chronology for the evolution of Internet of Things (IoT)
- Relate new concepts with concepts learned earlier to make a smooth transition to IoT
- List the reasons for a prevailing universal networked paradigm, which is IoT
- Compare and correlate IoT with its precursors such as WSN, M2M, and CPS
- List the various enablers of IoT
- Understand IoT networking components and various networking topologies
- Recognize the unique features of IoT which set it apart from other similar paradigms

4.1 Introduction

The modern-day advent of network-connected devices has given rise to the popular paradigm of the Internet of Things (IoT). Each second, the present-day Internet allows massively heterogeneous traffic through it. This network traffic consists of images, videos, music, speech, text, numbers, binary codes, machine status, banking messages, data from sensors and actuators, healthcare data, data from vehicles, home automation system status and control messages, military communications, and many more. This huge variety of data is generated from a massive number of connected devices, which may be directly connected to the Internet or connected through gateway devices. According to statistics from the Information Handling Services [7], the total number of connected devices globally is estimated to be around 25 billion. This figure is projected

to triple within a short span of 5 years by the year 2025. Figure 4.1 shows the global trend and projection for connected devices worldwide.

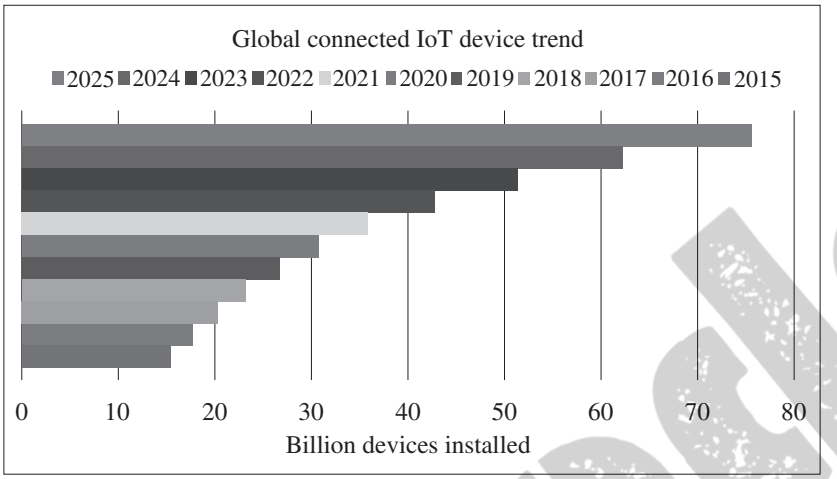


Figure 4.1 10-year global trend and projection of connected devices (statistics sourced from the Information Handling Services [7])

The traffic flowing through the Internet can be attributed to legacy systems as well as modern-day systems. The miniaturization of electronics and the cheap affordability of technology is resulting in a surge of connected devices, which in turn is leading to an explosion of traffic flowing through the Internet.

Points to ponder

"The Internet of Things (IoT) is the network of physical objects that contain embedded technology to communicate and sense or interact with their internal states or the external environment."

—Gartner Research [5]

One of the best examples of this explosion is the evolution of smartphones. In the late 1990's, cellular technology was still expensive and which could be afforded only by a select few. Moreover, these particular devices had only the basic features of voice calling, text messaging, and sharing of low-quality multimedia. Within the next 10 years, cellular technology had become common and easily affordable. With time, the features of these devices evolved, and the dependence of various applications and services on these gadgets on packet-based Internet accesses started rapidly increasing. The present-day mobile phones (commonly referred to as smartphones) are more or less Internet-based. The range of applications on these gadgets such as messaging, video calling, e-mails, games, music streaming, video streaming, and others are solely dependent on network provider allocated Internet access or WiFi. Most of

the present-day consumers of smartphone technology tend to carry more than one of these units. In line with this trend, other connected devices have rapidly increased in numbers resulting in the number of devices exceeding the number of humans on Earth by multiple times. Now imagine that as all technologies and domains are moving toward smart management of systems, the number of sensor/actuator-based systems is rapidly increasing. With time, the need for location-independent access to monitored and controlled systems keep on rising. This rise in number leads to a further rise in the number of Internet-connected devices.

The original Internet intended for sending simple messages is now connected with all sorts of "Things". These things can be legacy devices, modern-day computers, sensors, actuators, household appliances, toys, clothes, shoes, vehicles, cameras, and anything which may benefit a product by increasing its scientific value, accuracy, or even its cosmetic value.

Internet of Things

"In the 2000s, we are heading into a new era of ubiquity, where the 'users' of the Internet will be counted in billions and where humans may become the minority as generators and receivers of traffic. Instead, most of the traffic will flow between devices and all kinds of "Things", thereby creating a much wider and more complex Internet of Things."

—ITU Internet Report 2005 [6]

IoT is an anytime, anywhere, and anything (as shown in Figure 4.2) network of Internet-connected physical devices or systems capable of sensing an environment and affecting the sensed environment intelligently. This is generally achieved using low-power and low-form-factor embedded processors on-board the "things" connected to the Internet. In other words, IoT may be considered to be made up of connecting devices, machines, and tools; these things are made up of sensors/actuators and processors, which connect to the Internet through wireless technologies. Another school of thought also considers wired Internet access to be inherent to the IoT paradigm. For the sake of harmony, in this book, we will consider any technology enabling access to the Internet—be it wired or wireless—to be an IoT enabling technology. However, most of the focus on the discussion of various IoT enablers will be restricted to wireless IoT systems due to the much more severe operating constraints and challenges faced by wireless devices as compared to wired systems. Typically, IoT systems can be characterized by the following features [2]:

- Associated architectures, which are also efficient and scalable.
- No ambiguity in naming and addressing.
- Massive number of constrained devices, sleeping nodes, mobile devices, and non-IP devices.
- Intermittent and often unstable connectivity.

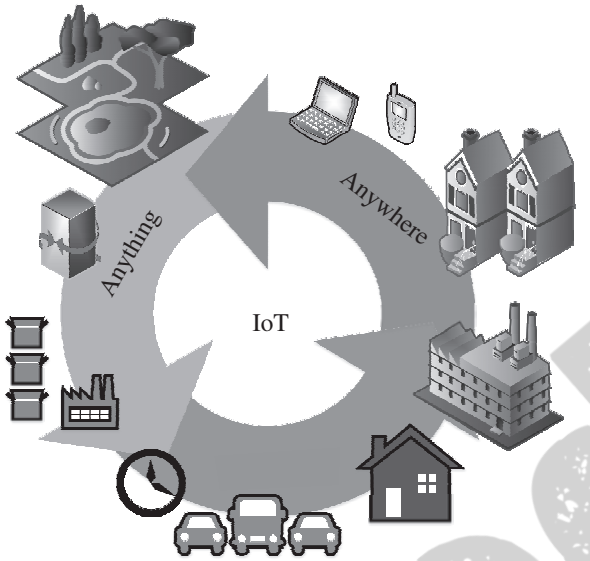


Figure 4.2 The three characteristic features—anytime, anywhere, and anything—highlight the robustness and dynamic nature of IoT

IoT is speculated to have achieved faster and higher technology acceptance as compared to electricity and telephony. These speculations are not ill placed as evident from the various statistics shown in Figures 4.3, 4.4, and 4.5.

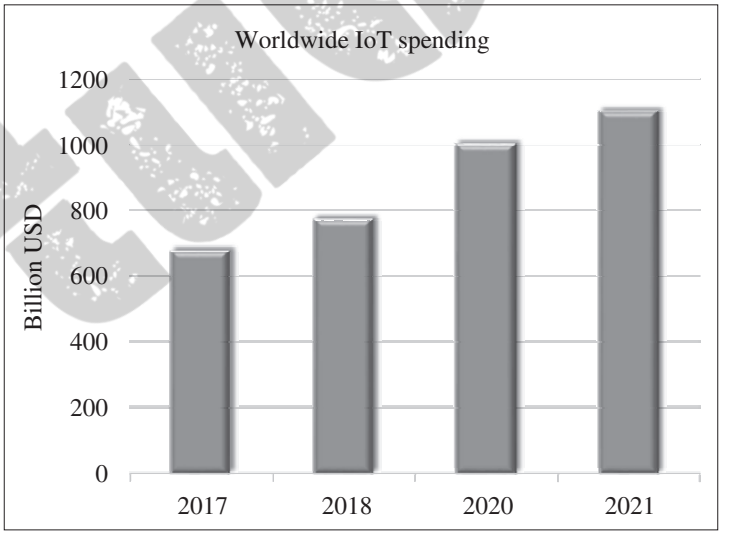


Figure 4.3 The global IoT spending across various organizations and industries and its subsequent projection until the year 2021 (sourced from International Data Corporation [1])

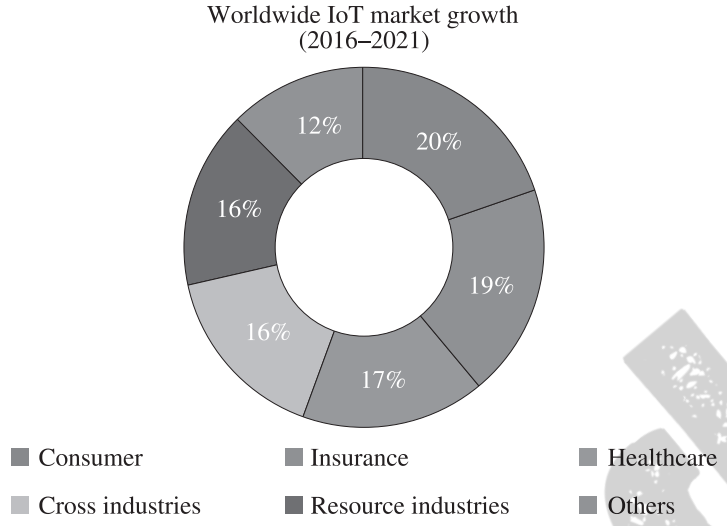


Figure 4.4 The compound annual growth rate (CAGR) of the IoT market (statistics sourced from [1])

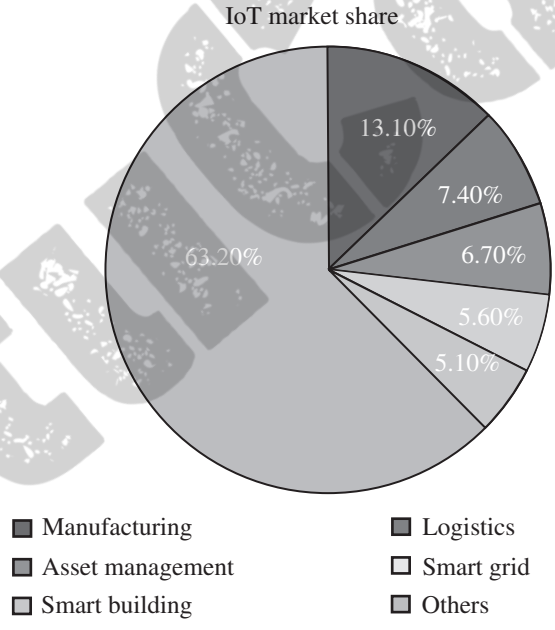


Figure 4.5 The IoT market share across various industries (statistics sourced from International Data Corporation [8])

According to an International Data Corporation (IDC) report, worldwide spending on IoT is reported to have crossed USD 700 billion. The projected spending on IoT-based technologies worldwide is estimated to be about USD 1.1 trillion [1]. Similarly,

the compounded annual growth rate of IoT between the years 2016 and 2021, as depicted in Figure 4.4, shows that the majority of the market share is captured by consumer goods, which is closely followed by insurance and healthcare industries. However, the combined industrial share of IoT growth (both cross and resource) is 32% of the collective market, which is again more than that of the consumer market. In continuation, Figure 4.5 shows the IoT market share of various sectors. The manufacturing, logistics, and asset management sectors were purported to be the largest receivers of IoT-linked investments in 2017 [8].

4.2 Evolution of IoT

The IoT, as we see it today, is a result of a series of technological paradigm shifts over a few decades. The technologies that laid the foundation of connected systems by achieving easy integration to daily lives, popular public acceptance, and massive benefits by using connected solutions can be considered as the founding solutions for the development of IoT. Figure 4.6 shows the sequence of technological advancements for shaping the IoT as it is today. These sequence of technical developments toward the emergence of IoT are described in brief:

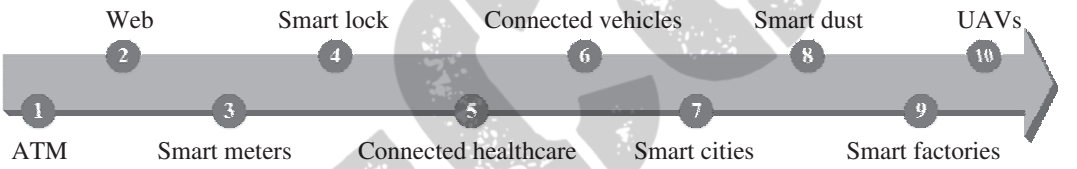


Figure 4.6 The sequence of technological developments leading to the shaping of the modern-day IoT

- ATM: ATMs or automated teller machines are cash distribution machines, which are linked to a user's bank account. ATMs dispense cash upon verification of the identity of a user and their account through a specially coded card. The central concept behind ATMs was the availability of financial transactions even when banks were closed beyond their regular work hours. These ATMs were ubiquitous money dispensers. The first ATM became operational and connected online for the first time in 1974.
- Web: World Wide Web is a global information sharing and communication platform. The Web became operational for the first time in 1991. Since then, it has been massively responsible for the many revolutions in the field of computing and communication.
- Smart Meters: The earliest smart meter was a power meter, which became operational in early 2000. These power meters were capable of communicating remotely with the power grid. They enabled remote monitoring of subscribers' power usage and eased the process of billing and power allocation from grids.

- Digital Locks: Digital locks can be considered as one of the earlier attempts at connected home-automation systems. Present-day digital locks are so robust that smartphones can be used to control them. Operations such as locking and unlocking doors, changing key codes, including new members in the access lists, can be easily performed, and that too remotely using smartphones.
- Connected Healthcare: Here, healthcare devices connect to hospitals, doctors, and relatives to alert them of medical emergencies and take preventive measures. The devices may be simple wearable appliances, monitoring just the heart rate and pulse of the wearer, as well as regular medical devices and monitors in hospitals. The connected nature of these systems makes the availability of medical records and test results much faster, cheaper, and convenient for both patients as well as hospital authorities.
- Connected Vehicles: Connected vehicles may communicate to the Internet or with other vehicles, or even with sensors and actuators contained within it. These vehicles self-diagnose themselves and alert owners about system failures.
- Smart Cities: This is a city-wide implementation of smart sensing, monitoring, and actuation systems. The city-wide infrastructure communicating amongst themselves enables unified and synchronized operations and information dissemination. Some of the facilities which may benefit are parking, transportation, and others.
- Smart Dust: These are microscopic computers. Smaller than a grain of sand each, they can be used in numerous beneficial ways, where regular computers cannot operate. For example, smart dust can be sprayed to measure chemicals in the soil or even to diagnose problems in the human body.
- Smart Factories: These factories can monitor plant processes, assembly lines, distribution lines, and manage factory floors all on their own. The reduction in mishaps due to human errors in judgment or unoptimized processes is drastically reduced.
- UAVs: UAVs or unmanned aerial vehicles have emerged as robust public-domain solutions tasked with applications ranging from agriculture, surveys, surveillance, deliveries, stock maintenance, asset management, and other tasks.

The present-day IoT spans across various domains and applications. The major highlight of this paradigm is its ability to function as a cross-domain technology enabler. Multiple domains can be supported and operated upon simultaneously over IoT-based platforms. Support for legacy technologies and standalone paradigms, along with modern developments, makes IoT quite robust and economical for commercial, industrial, as well as consumer applications. IoT is being used in vivid and diverse areas such as smart parking, smartphone detection, traffic congestion, smart lighting, waste management, smart roads, structural health, urban noise maps, river floods, water flow, silos stock calculation, water leakages, radiation levels, explosive and hazardous gases, perimeter access control, snow

level monitoring, liquid presence, forest fire detection, air pollution, smart grid, tank level, photovoltaic installations, NFC (near-field communications) payments, intelligent shopping applications, landslide and avalanche prevention, early detection of earthquakes, supply chain control, smart product management, and others.

Figure 4.7 shows the various technological interdependencies of IoT with other domains and networking paradigms such as M2M, CPS, the Internet of environment (IoE), the Internet of people (IoP), and Industry 4.0. Each of these networking paradigms is a massive domain on its own, but the omnipresent nature of IoT implies that these domains act as subsets of IoT. The paradigms are briefly discussed here:

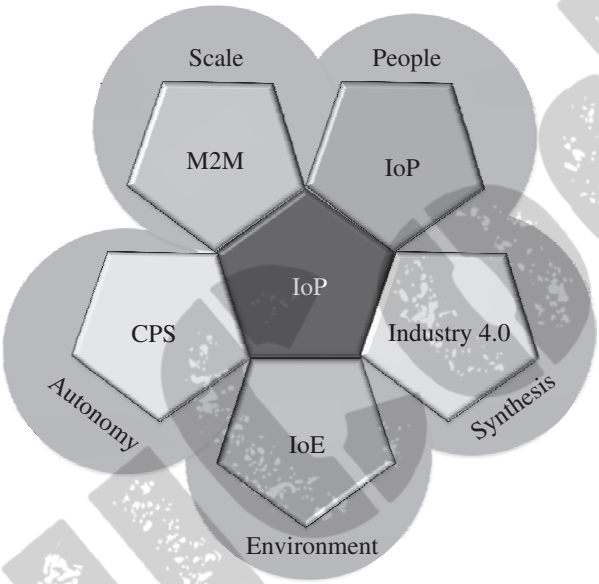


Figure 4.7 The interdependence and reach of IoT over various application domains and networking paradigms

(i) **M2M**: The M2M or the machine-to-machine paradigm signifies a system of connected machines and devices, which can talk amongst themselves without human intervention. The communication between the machines can be for updates on machine status (stocks, health, power status, and others), collaborative task completion, overall knowledge of the systems and the environment, and others.

(ii) **CPS**: The CPS or the cyber physical system paradigm insinuates a closed control loop—from sensing, processing, and finally to actuation—using a feedback mechanism. CPS helps in maintaining the state of an environment through the feedback control loop, which ensures that until the desired state is attained, the system keeps on actuating and sensing. Humans have a simple supervisory role in CPS-based systems; most of the ground-level operations are automated.

(iii) **IoE**: The IoE paradigm is mainly concerned with minimizing and even reversing the ill-effects of the permeation of Internet-based technologies on the environment [3]. The major focus areas of this paradigm include smart and sustainable farming, sustainable and energy-efficient habitats, enhancing the energy efficiency of systems and processes, and others. In brief, we can safely assume that any aspect of IoT that concerns and affects the environment, falls under the purview of IoE.

(iv) **Industry 4.0**: Industry 4.0 is commonly referred to as the fourth industrial revolution pertaining to digitization in the manufacturing industry. The previous revolutions chronologically dealt with mechanization, mass production, and the industrial revolution, respectively. This paradigm strongly puts forward the concept of smart factories, where machines talk to one another without much human involvement based on a framework of CPS and IoT. The digitization and connectedness in Industry 4.0 translate to better resource and workforce management, optimization of production time and resources, and better upkeep and lifetimes of industrial systems.

(v) **IoP**: IoP is a new technological movement on the Internet which aims to decentralize online social interactions, payments, transactions, and other tasks while maintaining confidentiality and privacy of its user's data. A famous site for IoP states that as the introduction of the Bitcoin has severely limited the power of banks and governments, the acceptance of IoP will limit the power of corporations, governments, and their spy agencies [4].

4.2.1 IoT versus M2M

M2M or the machine-to-machine paradigm refers to communications and interactions between various machines and devices. These interactions can be enabled through a cloud computing infrastructure, a server, or simply a local network hub. M2M collects data from machinery and sensors, while also enabling device management and device interaction. Telecommunication services providers introduced the term M2M, and technically emphasized on machine interactions via one or more communication networks (e.g., 3G, 4G, 5G, satellite, public networks). M2M is part of the IoT and is considered as one of its sub-domains, as shown in Figure 4.7. M2M standards occupy a core place in the IoT landscape. However, in terms of operational and functional scope, IoT is vaster than M2M and comprises a broader range of interactions such as the interactions between devices/things, things, and people, things and applications, and people with applications; M2M enables the amalgamation of workflows comprising such interactions within IoT. Internet connectivity is central to the IoT theme but is not necessarily focused on the use of telecom networks.

4.2.2 IoT versus CPS

Cyber physical systems (CPS) encompasses sensing, control, actuation, and feedback as a complete package. In other words, a digital twin is attached to a CPS-based system. As mentioned earlier, a digital twin is a virtual system–model relation, in which the system signifies a physical system or equipment or a piece of machinery, while the model represents the mathematical model or representation of the physical system's behavior or operation. Many a time, a digital twin is used parallel to a physical system, especially in CPS as it allows for the comparison of the physical system's output, performance, and health. Based on feedback from the digital twin, a physical system can be easily given corrective directions/commands to obtain desirable outputs. In contrast, the IoT paradigm does not compulsorily need feedback or a digital twin system. IoT is more focused on networking than controls. Some of the constituent sub-systems in an IoT environment (such as those formed by CPS-based instruments and networks) may include feedback and controls too. In this light, CPS may be considered as one of the sub-domains of IoT, as shown in Figure 4.7.

4.2.3 IoT versus WoT

From a developer's perspective, the Web of Things (WoT) paradigm enables access and control over IoT resources and applications. These resources and applications are generally built using technologies such as HTML 5.0, JavaScript, Ajax, PHP, and others. REST (representational state transfer) is one of the key enablers of WoT. The use of RESTful principles and RESTful APIs (application program interface) enables both developers and deployers to benefit from the recognition, acceptance, and maturity of existing web technologies without having to redesign and redeploy solutions from scratch. Still, designing and building the WoT paradigm has various adaptability and security challenges, especially when trying to build a globally uniform WoT. As IoT is focused on creating networks comprising objects, things, people, systems, and applications, which often do not consider the unification aspect and the limitations of the Internet, the need for WoT, which aims to integrate the various focus areas of IoT into the existing Web is really invaluable. Technically, WoT can be thought of as an application layer-based hat added over the network layer. However, the scope of IoT applications is much broader; IoT also which includes non-IP-based systems that are not accessible through the web.

4.3 Enabling IoT and the Complex Interdependence of Technologies

IoT is a paradigm built upon complex interdependencies of technologies (both legacy and modern), which occur at various planes of this paradigm. Regarding Figure 4.8, we can divide the IoT paradigm into four planes: services, local connectivity, global connectivity, and processing. If we consider a bottom-up view, the services offered fall

under the control and purview of service providers. The service plane is composed of two parts: 1) things or devices and 2) low-power connectivity.

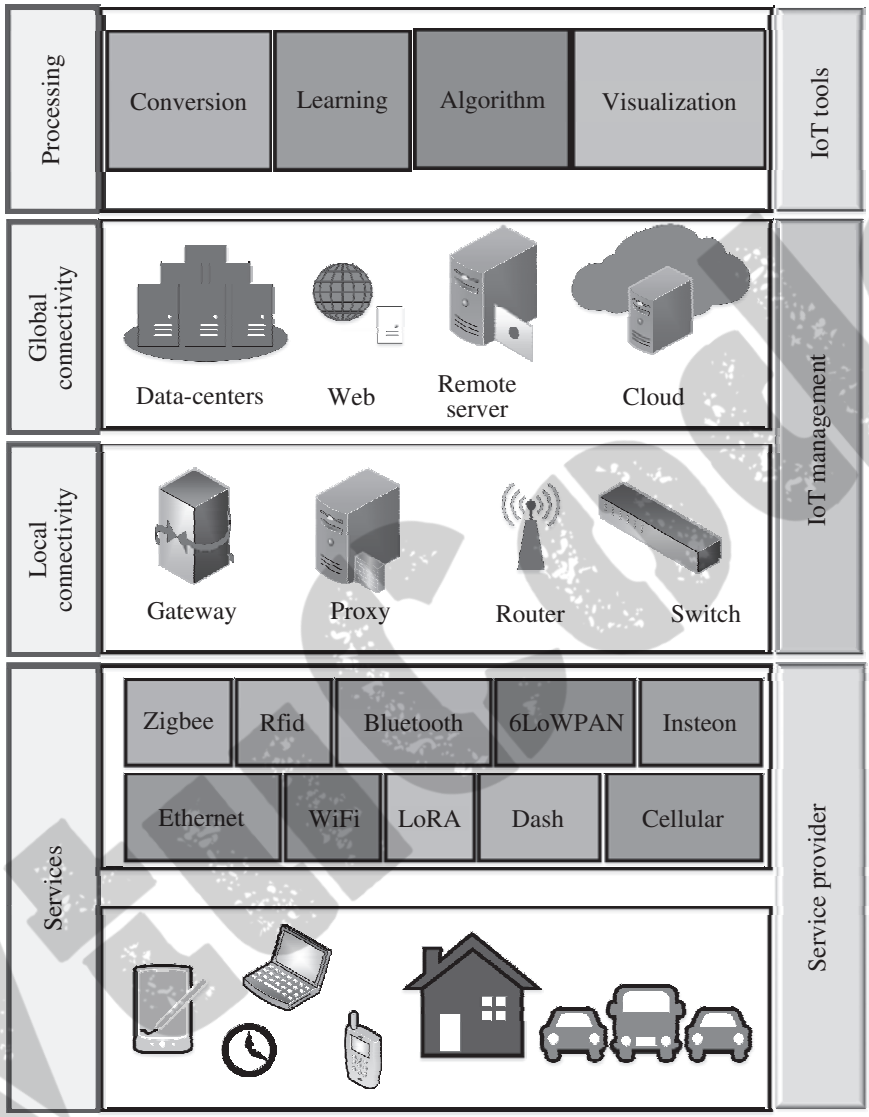


Figure 4.8 The IoT planes, various enablers of IoT, and the complex interdependencies among them

Typically, the services offered in this layer are a combination of things and low-power connectivity. For example, any IoT application requires the basic setup of sensing, followed by rudimentary processing (often), and a low-power, low-range network, which is mainly built upon the IEEE 802.15.4 protocol. The things may be wearables, computers, smartphones, household appliances, smart glasses, factory

machinery, vending machines, vehicles, UAVs, robots, and other such contraptions (which may even be just a sensor). The immediate low-power connectivity, which is responsible for connecting the things in local implementation, may be legacy protocols such as WiFi, Ethernet, or cellular. In contrast, modern-day technologies are mainly wireless and often programmable such as Zigbee, RFID, Bluetooth, 6LoWPAN, LoRA, DASH, Insteon, and others. The range of these connectivity technologies is severely restricted; they are responsible for the connectivity between the things of the IoT and the nearest hub or gateway to access the Internet.

The local connectivity is responsible for distributing Internet access to multiple local IoT deployments. This distribution may be on the basis of the physical placement of the things, on the basis of the application domains, or even on the basis of providers of services. Services such as address management, device management, security, sleep scheduling, and others fall within the scope of this plane. For example, in a smart home environment, the first floor and the ground floor may have local IoT implementations, which have various things connected to the network via low-power, low-range connectivity technologies. The traffic from these two floors merges into a single router or a gateway. The total traffic intended for the Internet from a smart home leaves through a single gateway or router, which may be assigned a single global IP address (for the whole house). This helps in the significant conservation of already limited global IP addresses. The local connectivity plane falls under the purview of IoT management as it directly deals with strategies to use/reuse addresses based on things and applications. The modern-day "edge computing" paradigm is deployed in conjunction with these first two planes: services and local connectivity.

In continuation, the penultimate plane of global connectivity plays a significant role in enabling IoT in the real sense by allowing for worldwide implementations and connectivity between things, users, controllers, and applications. This plane also falls under the purview of IoT management as it decides how and when to store data, when to process it, when to forward it, and in which form to forward it. The Web, data-centers, remote servers, Cloud, and others make up this plane. The paradigm of "fog computing" lies between the planes of local connectivity and global connectivity. It often serves to manage the load of global connectivity infrastructure by offloading the computation nearer to the source of the data itself, which reduces the traffic load on the global Internet.

The final plane of processing can be considered as a top-up of the basic IoT networking framework. The continuous rise in the usefulness and penetration of IoT in various application areas such as industries, transportation, healthcare, and others is the result of this plane. The members in this plane may be termed as IoT tools, simply because they wring-out useful and human-readable information from all the raw data that flows from various IoT devices and deployments. The various sub-domains of this plane include intelligence, conversion (data and format conversion, and data cleaning), learning (making sense of temporal and spatial data patterns), cognition (recognizing patterns and mapping it to already known patterns), algorithms (various control and monitoring algorithms), visualization (rendering

numbers and strings in the form of collective trends, graphs, charts, and projections), and analysis (estimating the usefulness of the generated information, making sense of the information with respect to the application and place of data generation, and estimating future trends based on past and present patterns of information obtained). Various computing paradigms such as "big data", "machine Learning", and others, fall within the scope of this domain.

4.4 IoT Networking Components

An IoT implementation is composed of several components, which may vary with their application domains. Various established works such as that by Savolainen et al. [2] generally outline five broad categories of IoT networking components. However, we outline the broad components that come into play during the establishment of any IoT network, into six types: 1) IoT node, 2) IoT router, 3) IoT LAN, 4) IoT WAN, 5) IoT gateway, and 6) IoT proxy. A typical IoT implementation from a networking perspective is shown in Figure 4.9. The individual components are briefly described here:

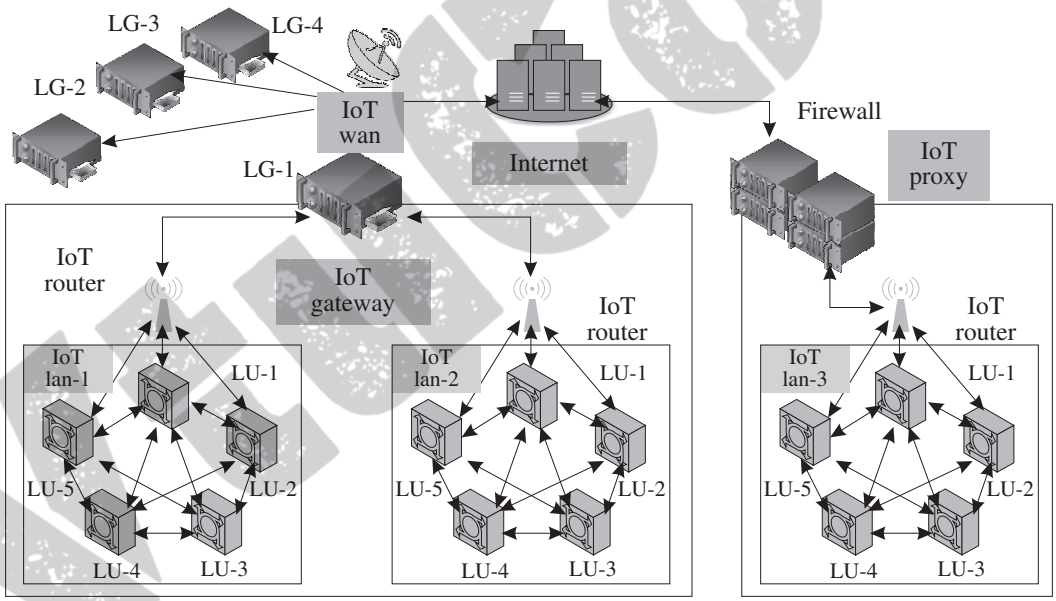


Figure 4.9 A typical IoT network ecosystem highlighting the various networking components—from IoT nodes to the Internet

(i) **IoT Node**: These are the networking devices within an IoT LAN. Each of these devices is typically made up of a sensor, a processor, and a radio, which communicates with the network infrastructure (either within the LAN or outside it). The nodes may be connected to other nodes inside a LAN directly or by

means of a common gateway for that LAN. Connections outside the LAN are through gateways and proxies.

(ii) **IoT Router**: An I oT router is a piece of networking equipment that is primarily tasked with the routing of packets between various entities in the IoT network; it keeps the traffic flowing correctly within the network. A router can be repurposed as a gateway by enhancing its functionalities.

(iii) **IoT LAN**: The local area network (LAN) enables local connectivity within the purview of a single gateway. Typically, they consist of short-range connectivity technologies. IoT LANs may or may not be connected to the Internet. Generally, they are localized within a building or an organization.

(iv) **IoT WAN**: The wide area network (WAN) connects various network segments such as LANs. They are typically organizationally and geographically wide, with their operational range lying between a few kilometers to hundreds of kilometers. IoT WANs connect to the Internet and enable Internet access to the segments they are connecting.

(v) **IoT Gateway**: An IoT gateway is simply a router connecting the IoT LAN to a WAN or the Internet. Gateways can implement several LANs and WANs. Their primary task is to forward packets between LANs and WANs, and the IP layer using only layer 3.

(vi) **IoT Proxy**: Proxies actively lie on the application layer and performs application layer functions between IoT nodes and other entities. Typically, application layer proxies are a means of providing security to the network entities under it ; it helps to extend the addressing range of its network.

In Figure 4.9, various IoT nodes within an IoT LAN are configured to to one another as well as talk to the IoT router whenever they are in the range of it. The devices have locally unique (LU-*x*) device identifiers. These identifiers are unique only within a LAN. There is a high chance that these identifiers may be repeated in a new LAN. Each IoT LAN has its own unique identifier, which is denoted by IoT LAN-*x* in Figure 4.9. A router acts as a connecting link between various LANs by forwarding messages from the LANs to the IoT gateway or the IoT proxy. As the proxy is an application layer device, it is additionally possible to include features such as firewalls, packet filters, and other security measures besides the regular routing operations. Various gateways connect to an IoT WAN, which links these devices to the Internet. There may be cases where the gateway or the proxy may directly connect to the Internet. This network may be wired or wireless; however, IoT deployments heavily rely on wireless solutions. This is mainly attributed to the large number of devices that are integrated into the network; wireless technology is the only feasible and neat-enough solution to avoid the hassles of laying wires and dealing with the restricted mobility rising out of wired connections.

4.5 Addressing Strategies in IoT

Table 4.1 lists the differences in features of IPv4 and IPv6. The most interesting point to note is that as compared to IPv4, which relies more on reliable delivery of packets between source and destination, an IPv6 packet is more address-oriented. Due to the increasing rate of devices being connected to the Internet, the early developers of IPv6 felt the need for accommodating addresses as more crucial than the need for reliable transmission of packets (which was the main feature of IPv4-based routing of packets).

Table 4.1 Feature-wise difference between IPv4 and IPv6 capabilities

Feature	IPv4	IPv6
Developed	IETF 1974	IETF 1998
Address length (bits)	32	128
No. of addresses	2^{32}	2^{128}
Notation	Dotted decimal	Hexadecimal
Dynamic allocation of addresses	DHCP	DHCPv6, SLAAC
IPSec	Optional	Compulsary
Header size	Variable	Fixed
Header checksum	Yes	No
Header options	Yes	No
Broadcast addresses	Yes	No
Multicast addresses	No	Yes
Feature	Focus on reliable transmission	Focus on addressing

In the context of IoT, we will consider and center our discussions on addressing schemes primarily focused on IPv6. The IPv4 and IPv6 header packet formats are shown in Chapter 1 of this book. In continuation, Figure 4.10 shows the address format of IPv6, which is 128 bits long.

The first three blocks are designated as the global prefix, which is globally unique. The next block is designated as the subnet prefix, which identifies the subnet of an interface/gateway through which LANs may be connected to the Internet. Finally, the last four blocks (64 bits) of hexadecimal addresses are collectively known as the interface identifier (IID). IIDs may be generated based on MAC (media access control) identifiers of devices/nodes or using pseudo-random number generator algorithms [2]. The IPv6 addresses can be divided into seven separate address types, which is generally based on how these addresses are used or where they are deployed.

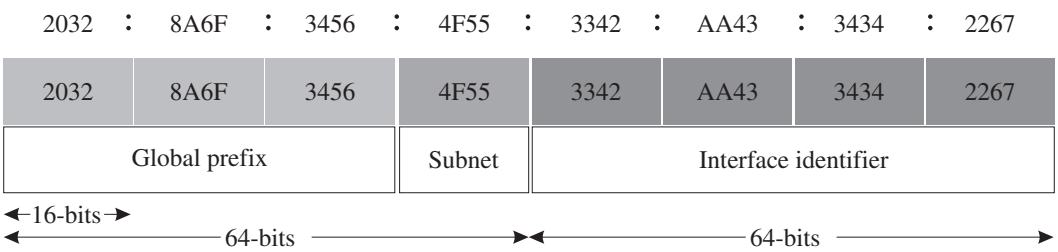


Figure 4.10 The IPv6 address format

(i) **Global Unicast (GUA)**: These addresses are assigned to single IoT entities/interfaces; they enable the entities to transmit traffic to and from the Internet. In regular IoT deployments, these addresses are assigned to gateways, proxies, or WANs.

(ii) **Multicast**: These addresses enable transmission of messages from a single networked entity to multiple destination entities simultaneously.

(iii) **Link Local (LL)**: The operational domain of these addresses are valid only within a network segment such as LAN. These addresses may be repeated in other network segments/LANs, but are unique within that single network segment.

(iv) **Unique Local (ULA)**: Similar to LL addresses, ULA cannot be routed over the Internet. These addresses may be repeated in other network segments/LANs, but are unique within that single network segment.

(v) **Loopback**: It is also known as the localhost address. Typically, these addresses are used by developers and network testers for diagnostics and system checks.

(vi) **Unspecified**: Here, all the bits in the IPv6 address are set to zero and the destination address is not specified.

(vii) **Solicited-node Multicast**: It is a multicast address based on the IPv6 address of an IoT node or entity.

Points to ponder

Multihoming in IoT networks: It is a network configuration in which a node/network connects to multiple networks simultaneously for improved reliability. Network proxies are used to manage multiple IP addresses and map them to LL addresses of IoT nodes in small deployments, where the allotment of address prefixes is not possible. Other approaches for multihoming include the use of gateways for assigning LL addresses to IoT nodes under the gateway's operational purview.

4.5.1 Address management classes

As discussed previously, the IoT deployment and network topology are largely dependent on where it is deployed. Unlike traditional IPv4 networked devices, the newer IoT devices largely depend on IPv6 for address allocation and management of addresses, which again is dictated by the application and the place of deployment of the IoT solution. Keeping these requirements in consideration, the addressing strategies in IoT may be broadly differentiated into seven classes, as shown in Figure 4.11. These classes are as follows:

(i) **Class 1**: The IoT nodes are not connected to any other interface or the Internet except with themselves. This class can be considered as an isolated class, where the communication between IoT nodes is restricted within a LAN only. The IoT nodes in this class are identified only by their link local (LL) addresses, as shown in Figure 4.11(a). These LL addresses may be repeated for other devices outside the purview of this network class. The communication among the nodes may be direct or through other nodes (as in a mesh configuration).

(ii) **Class 2**: The class 1 configuration is mainly utilized for enabling communication between two or more IoT LANs or WANs. The IoT nodes within the LANs cannot directly communicate to nodes in the other LANs using their LL addresses, but through their LAN gateways (which have a unique address assigned to them). Generally, ULA is used for addressing; however, in certain scenarios, GUA may also be used. Figure 4.11(b) shows a class 2 IoT network topology. L1–L5 are the LL addresses of the locally unique IoT nodes within the LAN; whereas U1 and U2 are the unique addresses of the two gateways extending communication to their LANs with the WAN. The WAN may or may not connect to the Internet.

(iii) **Class 3**: Figure 4.11(c) shows a class 3 IoT network configuration, where the IoT LAN is connected to an IoT proxy. The proxy performs a host of functions ranging from address allocation, address management to providing security to the network underneath it. In this class, the IoT proxy only uses ULA (denoted as L*x*-U*x* in the figure).

(iv) **Class 4**: In this class, the IoT proxy acts as a gateway between the LAN and the Internet, and provides GUA to the IoT nodes within the LAN. A globally unique prefix is allotted to this gateway, which it uses with the individual device identifiers to extend global Internet connectivity to the IoT nodes themselves. This configuration is shown in Figure 4.11(d). An important point to note in this class is that the gateway also enables local communication between the nodes without the need for the packets to be routed through the Internet. Additionally, the IoT nodes within the gateway can talk to one another directly without always involving the gateway. A proxy beyond the gateway enables global communication through the Internet.

(v) **Class 5**: This class is functionally similar to class 4. However, the main difference with class 4 is that this class follows a star topology with the gateway as the center of the star. All the communication from the IoT nodes under the gateway has to go through the gateway, as shown in Figure 4.11(e). A proxy beyond the gateway enables global communication through the Internet. The IoT nodes within a gateway's operational purview have the same GUA.

(vi) **Class 6**: The configuration of this class is again similar to class 5. However, the IoT nodes are all assigned unique global addresses (GUA), which enables a point-to-point communication network with an Internet gateway. A class 6 IoT network configuration is shown in Figure 4.11(f). Typically, this class is very selectively used for special purposes.

(vii) **Class 7**: The class 7 configuration is shown in Figure 4.11(g). Multiple gateways may be present; the configuration is such that the nodes should be reachable through any of the gateways. Typically, organizational IoT deployments follow this class of configuration. The concept of multihoming is important and inherent to this class.

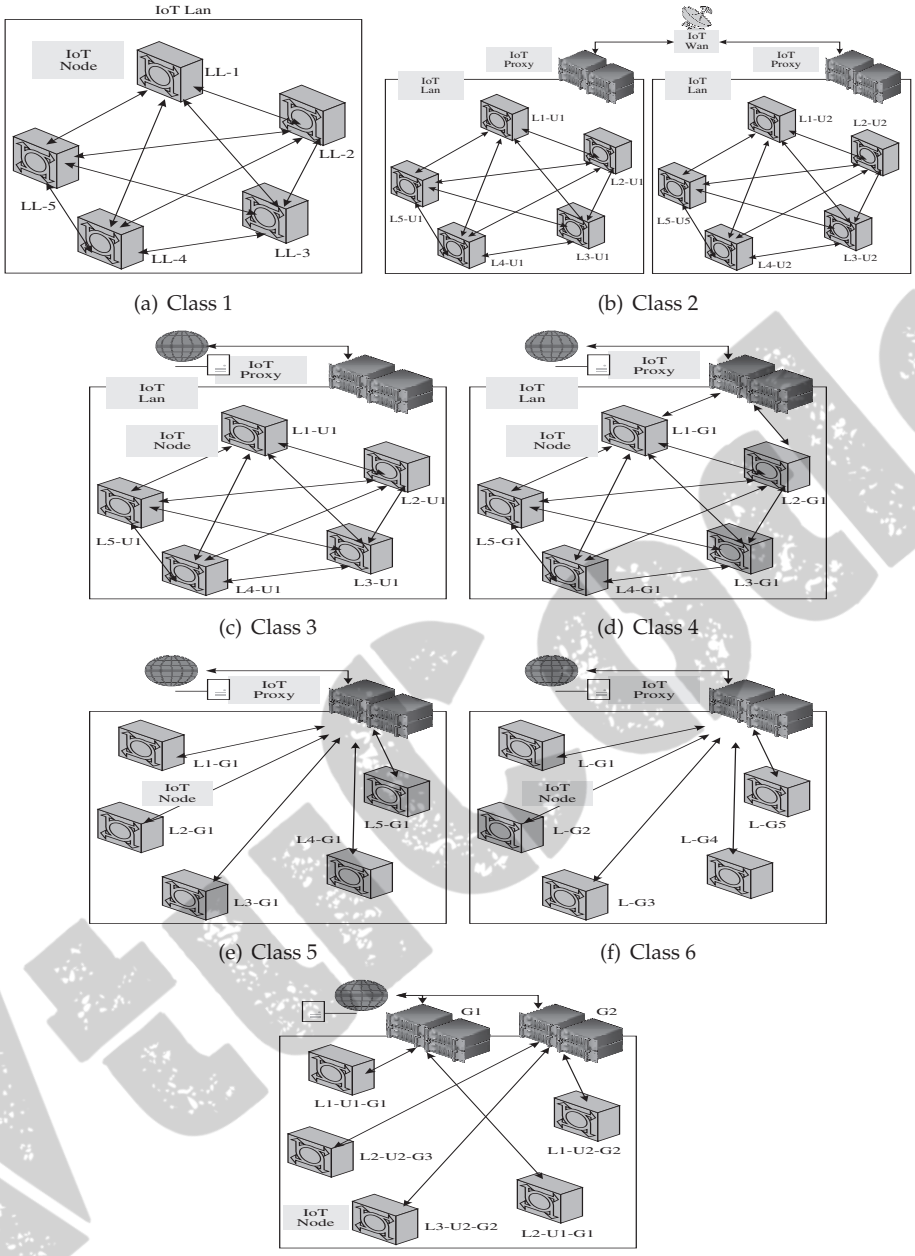
Points to ponder

Tunneling: It is a networking protocol in which data from private networks can be seamlessly streamed over a public network in the form of encapsulated packets. This is mainly used for ensuring connectivity and security of data generated from various technologies and protocols that may not be supported over the public communication channel. Some of the best examples of tunneling are virtual private networks (VPNs), secure shell (SSH), and others.

4.5.2 Addressing during node mobility

Traditional networks, mainly computer networks, and even paradigms such as M2M and CPS seldom take into account the need for addressing strategies when the IoT nodes are mobile. However, in a realistic scenario, especially in modern-day IoT systems (which are low-power and have low form-factor), the need for addressing of mobile nodes is extremely crucial to avoid address clashes of addresses accommodating a large number of IoT nodes. One of the following three strategies may be to for ensure portability of addresses in the event of node mobility in IoT deployments [2] as shown in Figure 4.12:

(i) **Global Prefix Changes**: Figure 4.12(a) abstracts the addressing strategy using global prefix changes. A node from the left LAN moves to the LAN on the right. The node undergoing movement is highlighted in the figure. The nodes in the first LAN have the prefix **A**, which changes to **B** under the domain of the new gateway overseeing the operation of nodes in the new LAN. However, it may



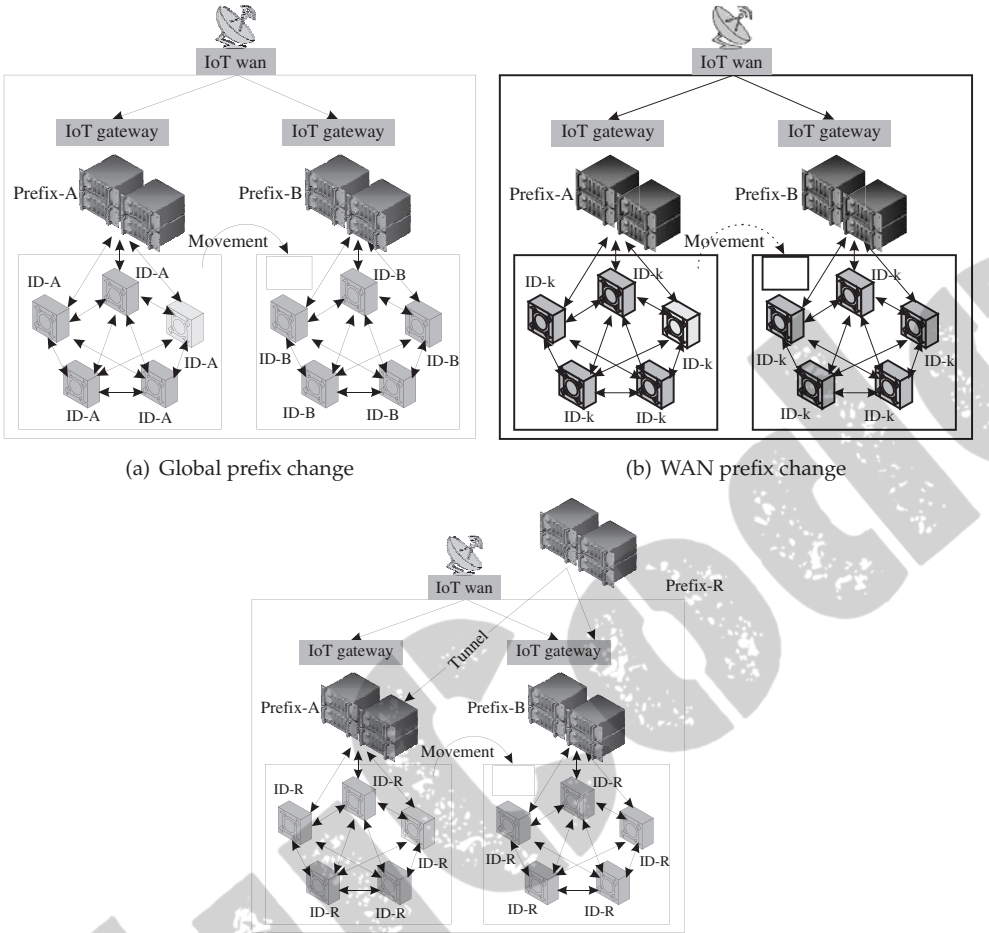
(a) Class 1 (b) Class 2

(c) Class 3 (d) Class 4

(e) Class 5 (f) Class 6

(g) Class 7

Figure 4.11 Various IoT topology configurations. LL/L denotes the link local addresses, LU denotes the locally unique link addresses (ULA), and LG denotes the globally unique link addresses (GUA)



(a) Global prefix change

(b) WAN prefix change

(c) Remote anchoring

Figure 4.12 Various scenarios during mobility of IoT nodes and their addressing strategies. ID-***prefix*** denotes the point to which the IoT node is attached to for address allocation

happen that due to movement, the device identifier may face clashes. Recall the structure of the IPv6 address (Figure 4.10). The device identifier, if allotted randomly, might face an address clash upon the node's arrival into the new LAN as there may already be a similar node identifier present in it. Typically, addresses are assigned using DHCPv6/ SLAAC; however, in this scenario, it is always prudent to have static node IP addresses to avoid a clash of addresses. This strategy is, in most cases, beneficial as the IoT nodes may be resource-constrained and have low-processing resources due to which it may not be able to handle protocols such as DHCPv6 or SLAAC.

(ii) **Prefix Changes within WANs**: Figure 4.12(b) abstracts the addressing strategy for prefix changes within WANs. In case the WAN changes its global prefix, the network entities underneath it must be resilient to change and function normally. The address allocation is hence delegated to entities such as gateways and proxies, which make use of ULAs to manage the network within the WAN.

(iii) **Remote Anchoring**: Figure 4.12(c) abstracts the addressing strategy using a remote anchoring point. This is applicable in certain cases which require that the IoT node's global addresses are maintained and not affected by its mobility or even the change in network prefixes. Although a bit expensive to implement, this strategy of having a remote anchoring point from which the IoT nodes obtain their global addresses through tunneling ensures that the nodes are resilient to changes and are quite stable. Even if the node's original network's (LAN) prefix changes from **A** to **B**, the node's global address remains immune to this change.