

# Internet of Things and Frameworks

# IoT Definitions

## General observations:

“ Internet of things is a twenty-first century phenomenon in which physical consumer products connect to the web and start communicating with each other by means of sensors and actuators.”

## ITU-T Views:

**View A:** IoT is just a concept: the IoT does not refer to a network infrastructure; the IoT is not a technical term but a concept or a phenomenon.

**View B:** IoT is an infrastructure: The IoT refers to an infrastructure.

As shown in the below figure 2.1, if IoT is defined as an infrastructure, IoT should be identified for all aspects of infrastructure such as service and functional requirements, architectures, and so on.

We can see machine-to-machine (M2M) deployments into 4 domains:

- Sensors and controllers;
- “the edge,” where data from these devices are gathered;
- the cloud, where the data are stored and managed;
- and the client, where the data are ultimately evaluated.

# IoT Definitions

## ITU-T Views

- IoT should be identified for all aspects of infrastructure such as service and functional requirements, architectures.

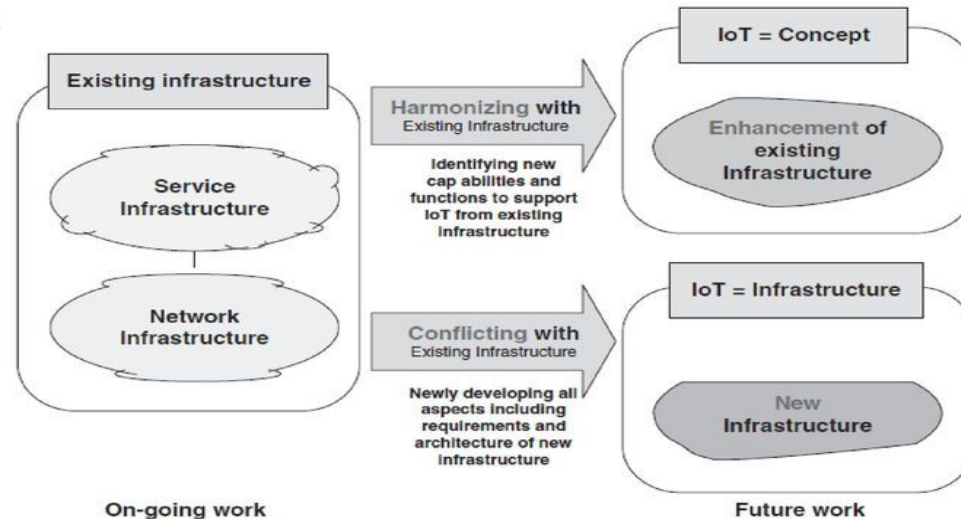


FIGURE 2.1 Direction for standardization according to IoT definition.

## 2.1.3 Working Definition

*A broadly-deployed aggregate computing/communication application and/or application-consumption system, that is deployed over a local (L-IoT), metropolitan (M-IoT), regional (R-IoT), national (N-IoT) or global (G-IoT) geography, consisting of*

- (i) Dispersed instrumented objects (“things”) with embedded one or two-way communications and some computing capabilities.
- (ii) where objects are reachable over a variety of wireless or wired local area and/or wide area networks, and

(iii) whose inbound data and/or outbound commands are pipelined to or issued by a system (an application) with a (high) degree of (human or computer-based intelligence).

Two other related definitions are as follows:

“Sensors are active devices that measure some variable of the natural or man-made environment.”

Eg., a building, assembly line

“An actuator is a mechanized device of various sizes (from ultra-small to very large) that accomplishes a specified physical action. An actuator is the mechanism by which an entity acts upon an environment.”

# Classifications of Things (objects) :

Things (objects) are classified as shown in the following figure.

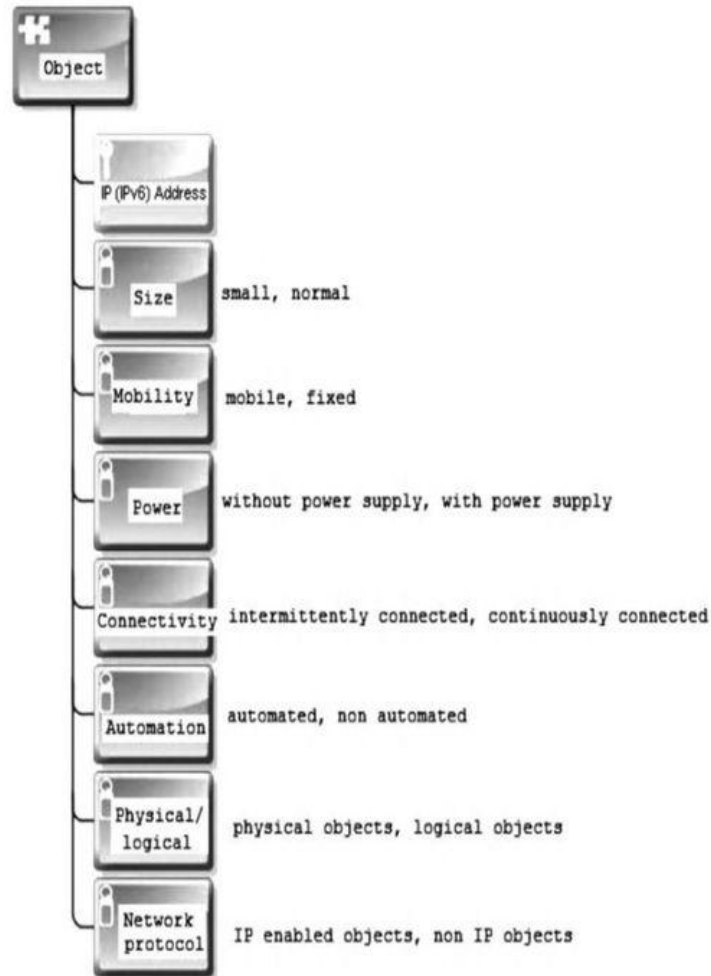
Objects have the following characters:

- have the ability to sense and/or actuate
- are generally small (but not always)
- are energy/power limited
- are connected to the physical world
- sometimes have intermittent connectivity
- are mobile (but not always)
- of interest people
- managed by devices, not people (but not always)

# IoT Definitions

## Working Definition

- Object classification





## 2.2 IoT Frameworks

A high level M2M system architecture (HLSA) comprises the device and gateway domain, the network domain, and the applications domain.

The **device and gateway domain** is composed of the following elements:

1. **M2M device:** A device that runs M2M applications using M2M service capabilities. M2M devices connect to network domain in the following manners:
  - a. **Case 1 “Direct Connectivity”** : M2M devices connect to the network domain via the access network. The M2M DEVICE performs the procedures such as
    - i. Registration
    - ii. authentication

iii. Authorization

iv. Management and

v. provisioning with the network domain.

The M2M device may provide service to other devices connected to it that are hidden from the network domain.

b. **Case 2 “Gateway as a Network Proxy”** : The M2M device connects to the network domain via an M2M gateway. M2M devices connect to the M2M gateway using the M2M area network. The M2M gateway acts as a proxy for the network domain toward the M2M devices that are connected to it.

Examples of procedures that are proxied include authentication, authorization, management and provisioning.

**2. M2M area network:** it provides connectivity between M2M devices and M2M gateways.

Examples of M2M area networks include personal area network technologies such as IEEE 802.15.1, Zigbee, Bluetooth, IETF ROLL, ISA 100.11a among others or local networks such as power line communication.

3. **M2M gateway:** a gateway that runs M2M applications using M2M service capabilities.

The gateway acts as a proxy between M2M devices and the network domain.

The M2M gateway may provide service to other devices connected to it that are hidden from the network domain.

# Network Domain

It is composed of the following elements

1. **Access Network:** a network that allows the M2M device and gateway domain to communicate with the core network.
2. **Core network:** a network that provides the following capabilities
  - a. IP connectivity at a minimum and possibly other connectivity means
  - b. Service and network control functions
  - c. Interconnection
  - d. Roaming
  - e. Core networks include 3GPP CoNs, ETSI TISPAN CoN and 3GPP2 CoN
3. **M2M service capabilities:**

### 3. **M2M service capabilities:**

- a. Provide M2M functions that are to be shared by different applications
- b. Expose functions through a set of open interfaces
- c. Use CoN functionalities
- d. Simplify and optimize application development and deployment through hiding of network specificities

The M2M service capabilities along with the core network is known collectively as the M2M core.

# Applications Domain

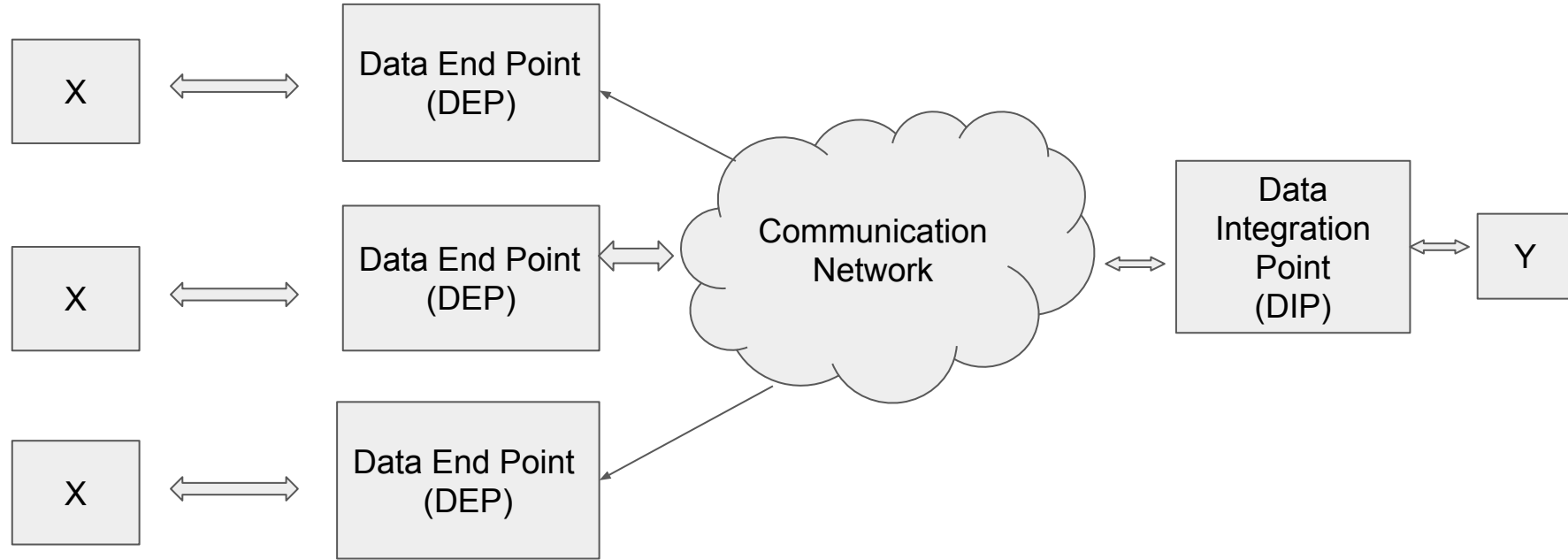
It is composed of the following elements:

1. **M2M applications:** applications that run the service logic and use M2M service capabilities accessible via an open interface.

There are also management functions within an overall M2M service provider domain. Which are as follows:

- A. **Network Management functions:**
- B. **M2M management functions:**

Figure 2.5: Basic elements of an M2M application.



**IoT Endpoints** are the devices that are monitoring a service, process, or machine, by collecting **data** and sending it back to be analyzed.



## **Network management functions :**

Consists of all the functions required to manage the access and core networks; these functions include provisioning, supervision, fault management.

## **M2M management functions:**

Consists of all the functions required to manage M2M service capabilities in the network domain.

# Basic Nodal Capabilities

Consistent with the HLSA, a remote device generally needs to have a basic protocol stack that supports as a minimum local connectivity.

Distributed M2M typically entails continuously changing variables to control the behaviour of an application.

Typical requirements include the following capabilities:

- Retransmission
  - Network recovers from packet loss or informs application
  - Recovery is immediate: on the order of RTT (round-trip time)s, not seconds.
- Network independent of MAC/PHY (medium access control /physical coding layer)

- Scale
  - Thousands of nodes
  - Multiple link speeds
- Multicast
  - Throughout network
  - Reliable
- Duplicate suppression (Caused by inconsistent or inaccurate business listings,)
- Emergency messages
  - Routed and/or queued around other traffic
  - Other traffic slushed as delivered
- Routine traffic delivered in sequence
- Separate timers by peer/message
- Polling of nodes
  - Sequential
  - Independent of responses

- Paradigm supports peer-to-peer
  - Not everything is client/server
- Capabilities
  - Discover nodes
  - Discover node capabilities
  - Deliver multi segment records
- Exchange of multisegment records
- Network and application versioning
- Security
  - Strong encryption
  - Mutual authentication
  - Protection against record/playback attacks