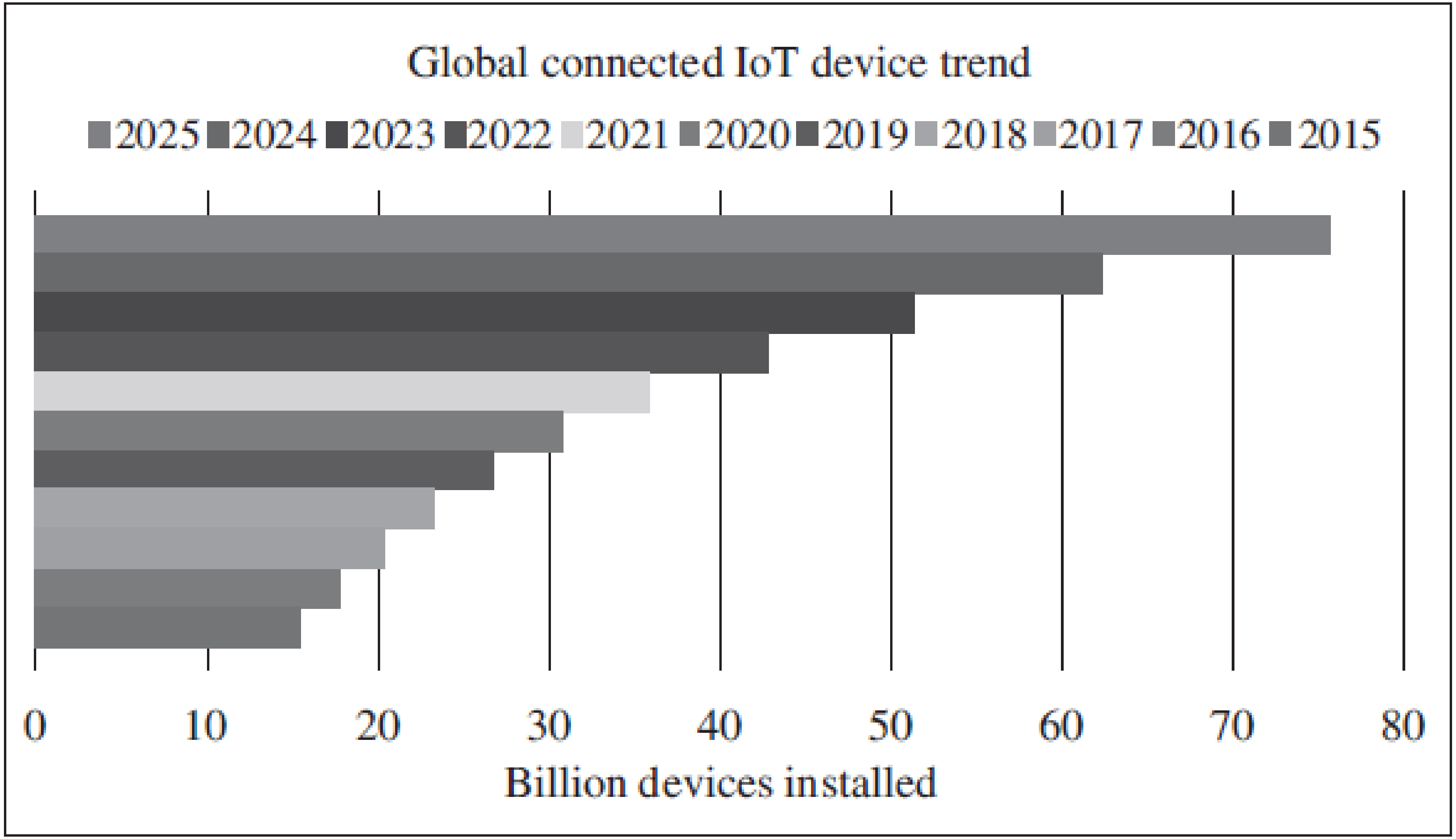
Module-1

Emergence of IoT

Introduction

- The modern-day advent of network-connected devices has given rise to the popular paradigm of the Internet of Things (IoT).
- Internet allows massively heterogeneous traffic
  - videos, images, 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
  - Massive data generated from numerous devices connected to internet via gateway devices
  - Estimated 25 billion devices connected world wide



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

- Traffic flow through legacy and new systems
- Explosion in traffic flow is also through miniaturization of electronics and the cheap affordability of technology is resulting in a surge of connected devices
- 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."

Internet traffic explosion - Smart phones

Things refers to

- 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.

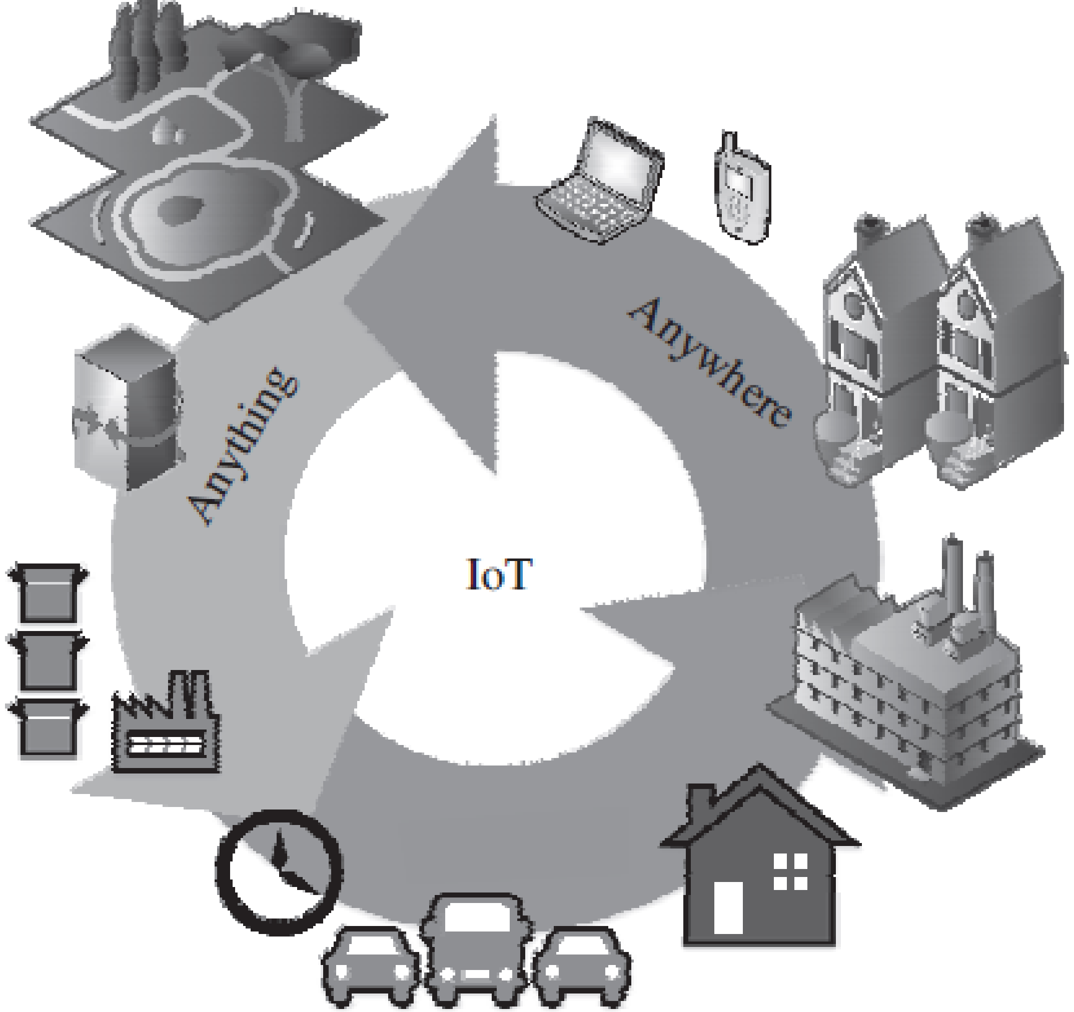
Internet of Things

"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]

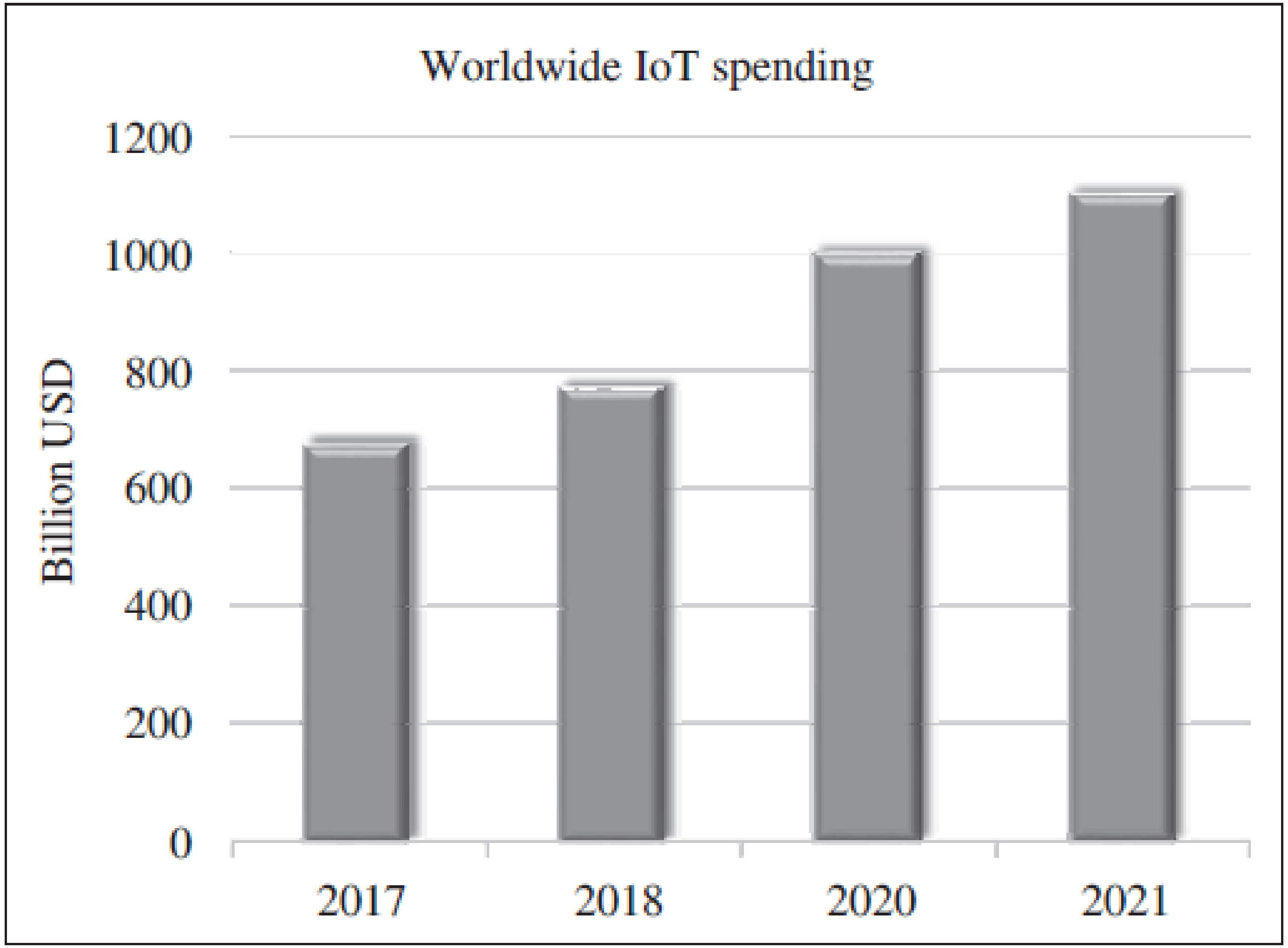
Internet of Things

- IoT is an anytime, anywhere, and anything network of Internet-connected physical devices or systems capable of sensing an environment and affecting the sensed environment intelligently

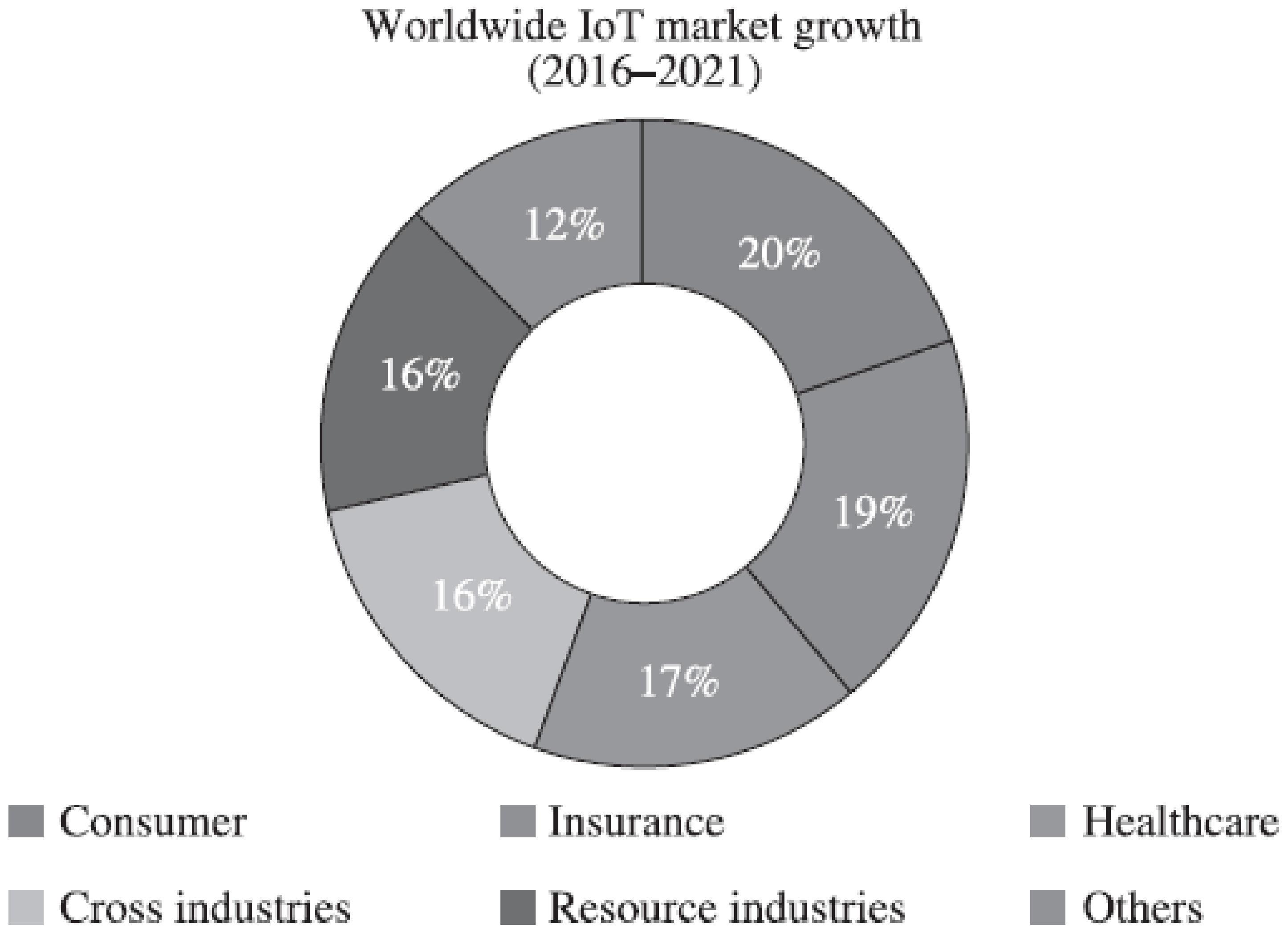


IoT systems can be characterized

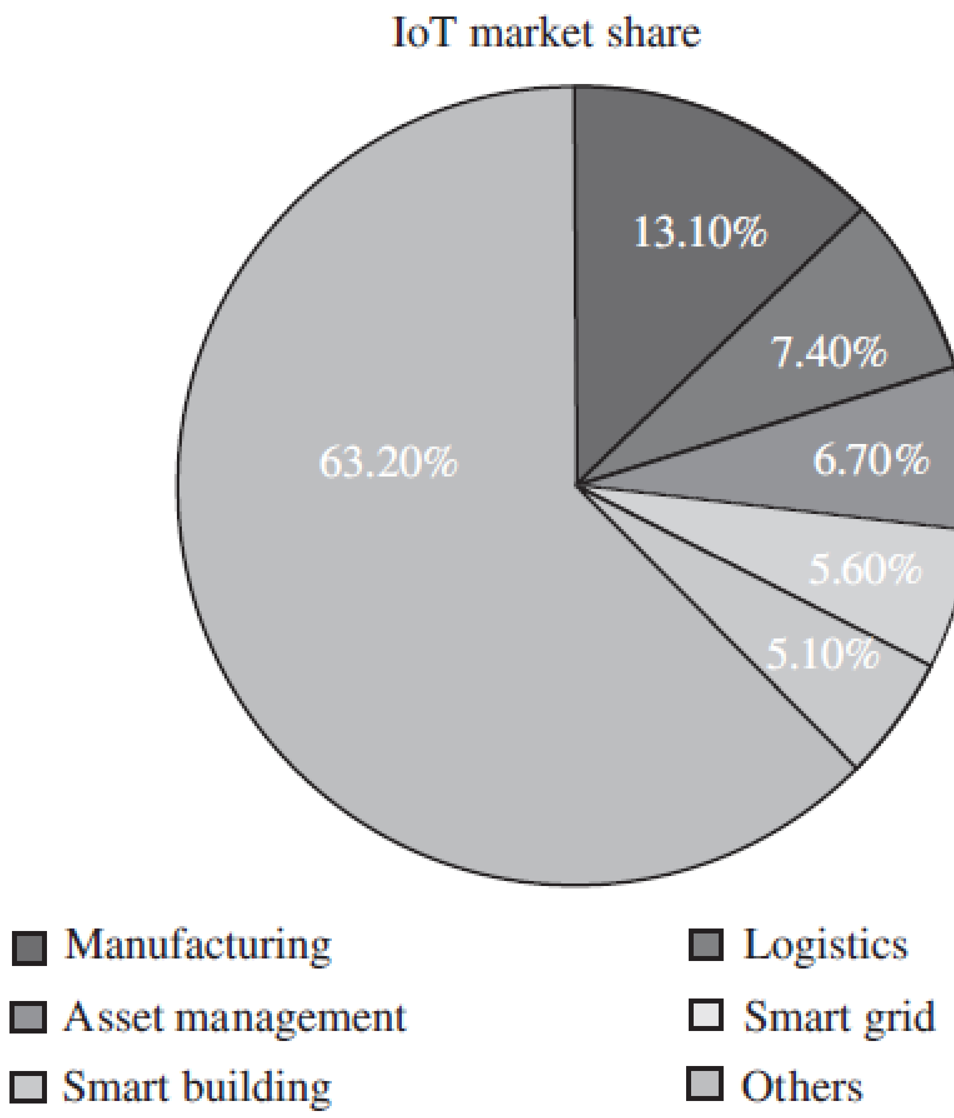
- Associated architectures, which are also efficient and scalable.
- No ambiguity in naming and addressing.
- Massive number of constrained devices, sleeping nodes, mobile devices, and non-IP devices.
- Intermittent and often unstable connectivity.



The global IoT spending across various organizations and industries and its subsequent projection until the year 2021



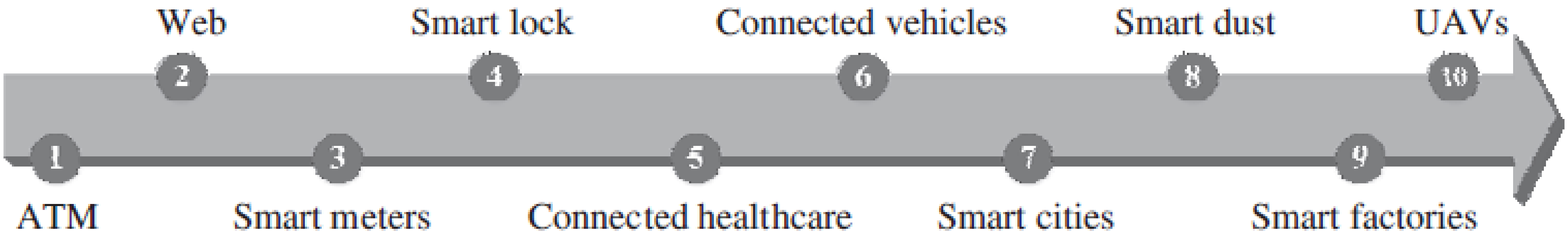
The compound annual growth rate (CAGR) of the IoT market



The IoT market share across various industries

Evolution of IoT

- 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,
  - Massive benefits by using connected solutions



Evolution of IoT

- ATM(1974): automated teller machines are cash distribution machines, availability of financial transactions even when banks were closed beyond their regular work hours, ubiquitous money dispensers
- Web (1991): World Wide Web is a global information sharing and communication platform, massively responsible for the many revolutions in the field of computing and communication
- Smart Meters (2000): earliest smart meter was a power meter, capable of communicating remotely with the power grid, remote monitoring of subscribers’ power usage and eased the billing and power allocation
- Digital Locks: used in home-automation, robust enough to be controlled by smart phones, locking, unlocking, changing codes, access list manipulation, remote access
- Connected Health Care: healthcare devices connect to hospitals, doctors, and relatives to alert them of medical emergencies and take preventive measures, simple wearable appliances, monitors vital health parameters, availability of medical records and test results much faster, cheaper, and convenient

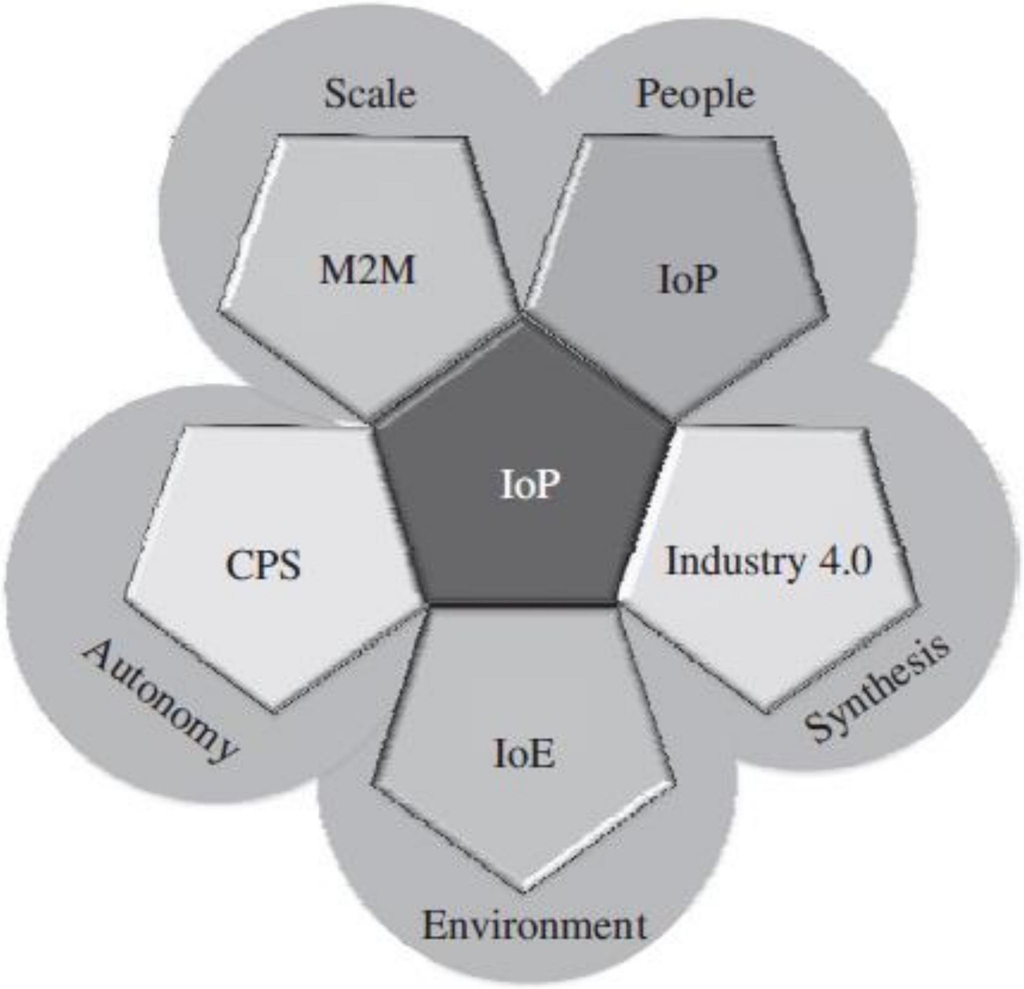
Evolution of IoT

- Connected Vehicles: communicate via Internet with other vehicles, or even with sensors and actuators contained within it, used for self-diagnosis and alert owners
- Smart Cities: city-wide implementation of smart sensing, monitoring, and actuation systems, communicating amongst themselves enables unified and synchronized operations and information dissemination. Ex: Parking, Transportation etc..
- Smart Dust: microscopic computers, Smaller than grain of sand, sprayed to measure chemicals in the soil, diagnose problems in the human body.
- Smart Factories: 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: unmanned aerial vehicles tasked with applications ranging from agriculture, surveys, surveillance, deliveries, stock maintenance, asset management, and other.

Evolution of IoT

- 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 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.

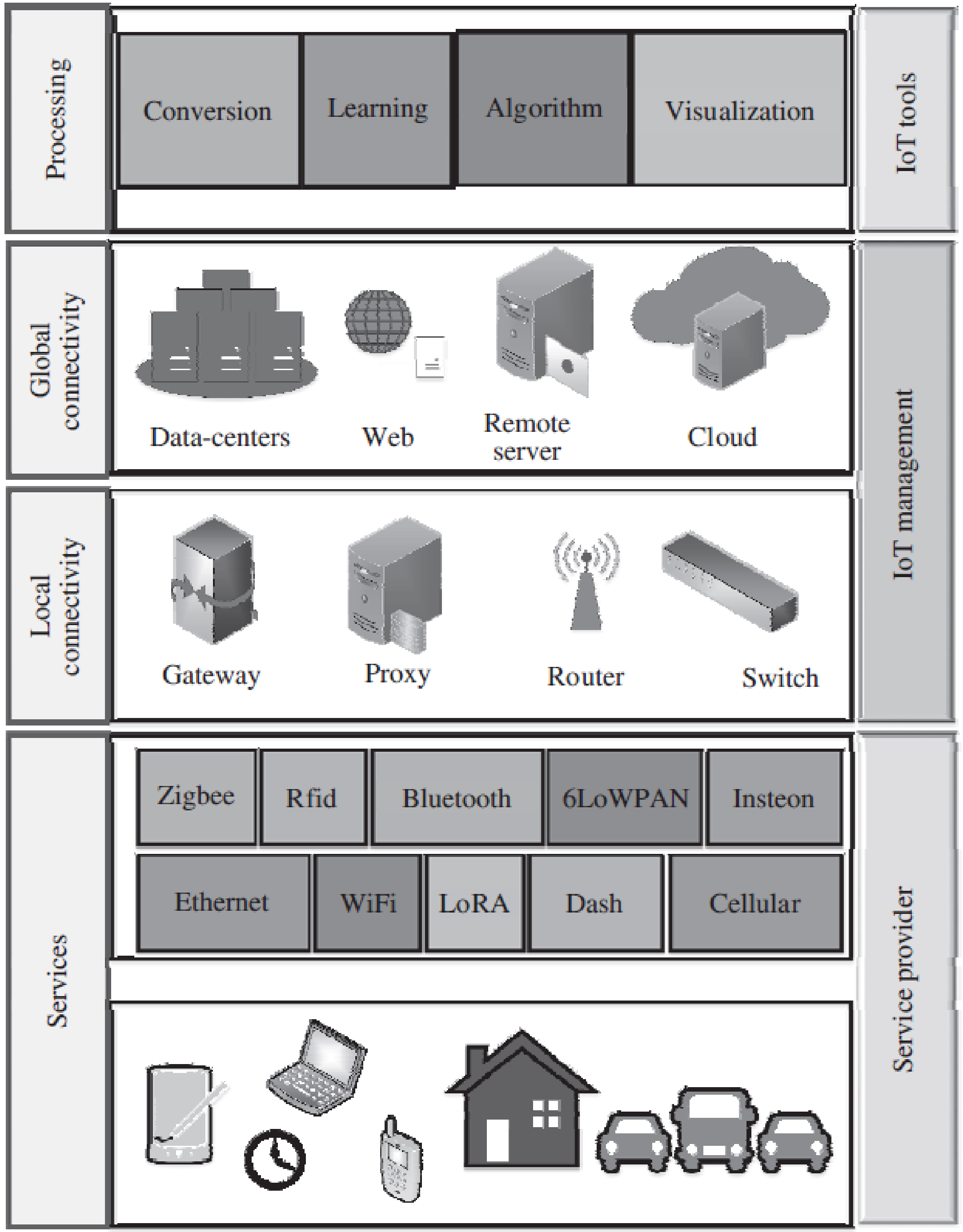
The interdependence and reach of IoT over various application domains and networking paradigms



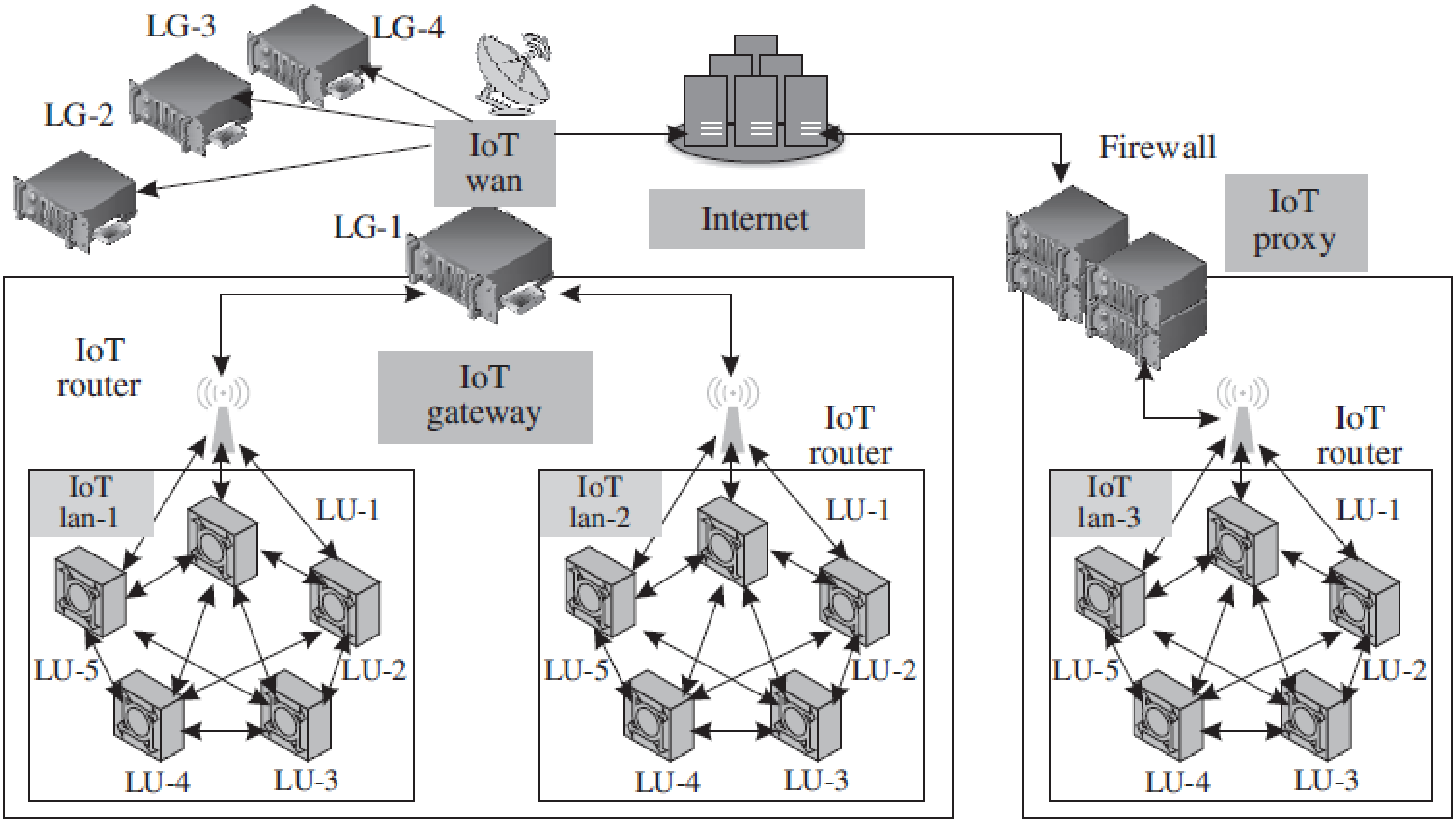
Interdependency

- **M2M** (machine-to-machine) - can talk amongst themselves without human intervention, communicates on on machine status, collaborative task completion, overall knowledge of the systems and the environment
- **CPS** (Cyber Physical Systems) - closed control loop—from sensing, processing, actuation—using a feedback mechanism, until the desired state is attained, automated, simple supervisory human role
- **IoE** (Internet of Everything) - mainly concerned with minimizing and even reversing the ill-effects of the permeation of Internet-based technologies on the environment. (any aspect of IoT that concerns and affects the environment) Ex: smart and sustainable farming, sustainable and energy-efficient habitats, enhancing the energy efficiency of systems and processes
- **Industry 4.0**: (fourth industrial revolution - digitization in the manufacturing industry) - smart factories, where machines talk to one another without much human involvement based on a framework of CPS and IoT. Enable better resource and workforce management, optimization of production time and resources, and better upkeep and lifetimes of industrial systems.
- **IoP**:(Internet of People) the connection and communication capabilities between people enabled by the internet and other aware technologies

Enabling IoT and the Complex Interdependence of Technologies



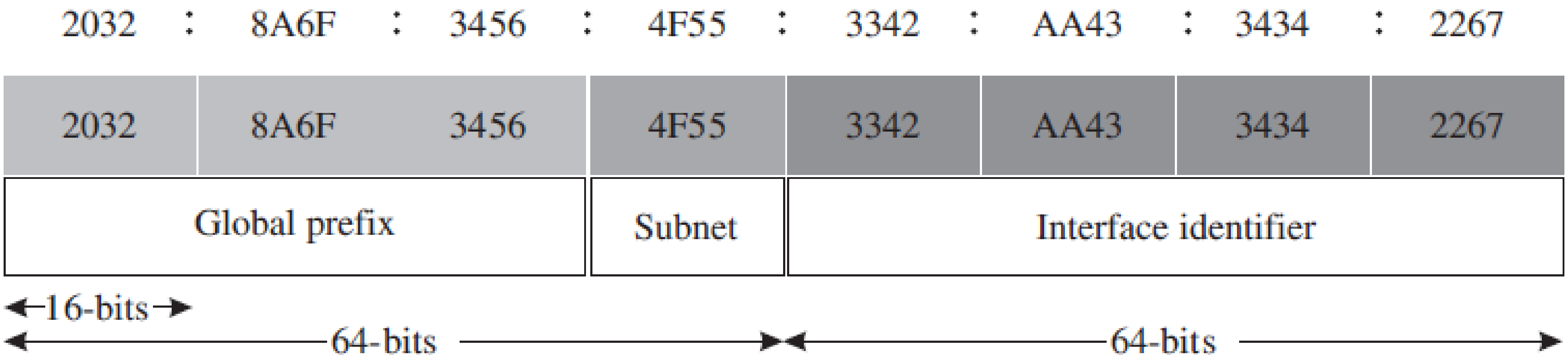
IoT Networking Components



Addressing Strategies in IoT

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

IPv6 address format



Global prefix - globally unique.
Subnet prefix - which identifies the subnet of an interface/gateway through which LANs may be connected to the Internet.
Interface identifier (IID) - generated based on MAC (media access control) or using pseudo-random number generator algorithms 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.

IPv6 addresses - seven types

- **(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)**: Operates only in LAN. These addresses are unique within that single network segment.
- (iv) **Unique Local (ULA)**: Similar to LL addresses, ULA cannot be routed over the Internet.
- (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.

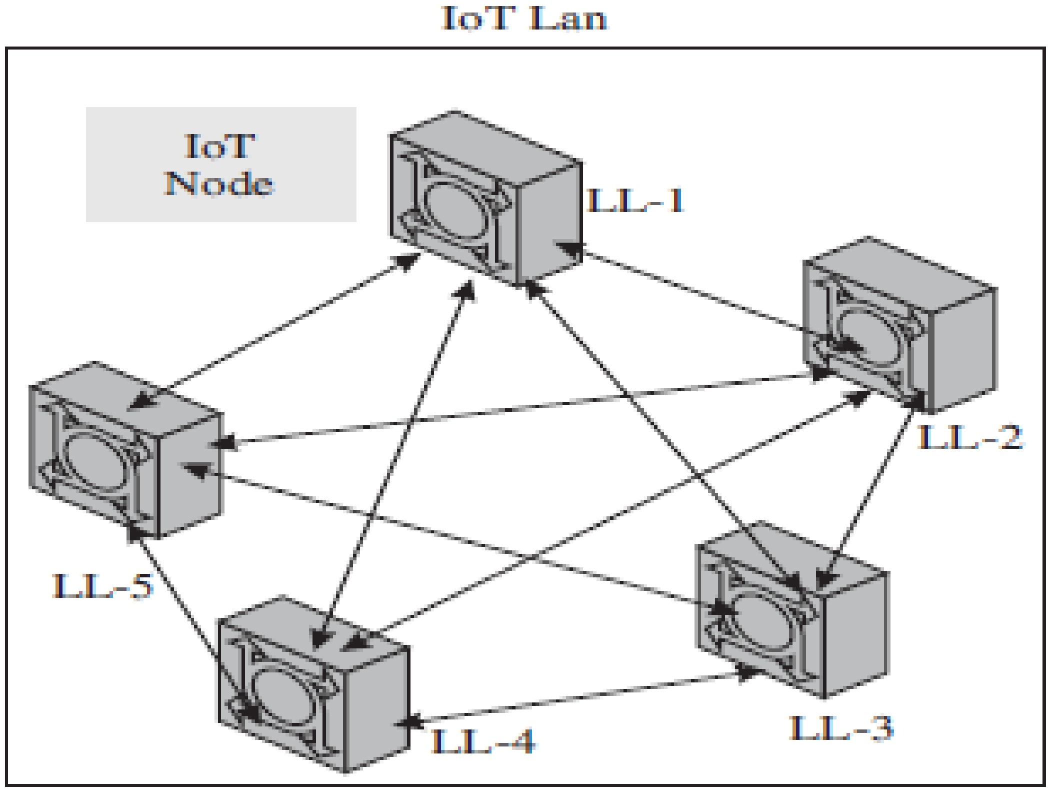
Points to ponder

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.

Address management classes

Class 1:

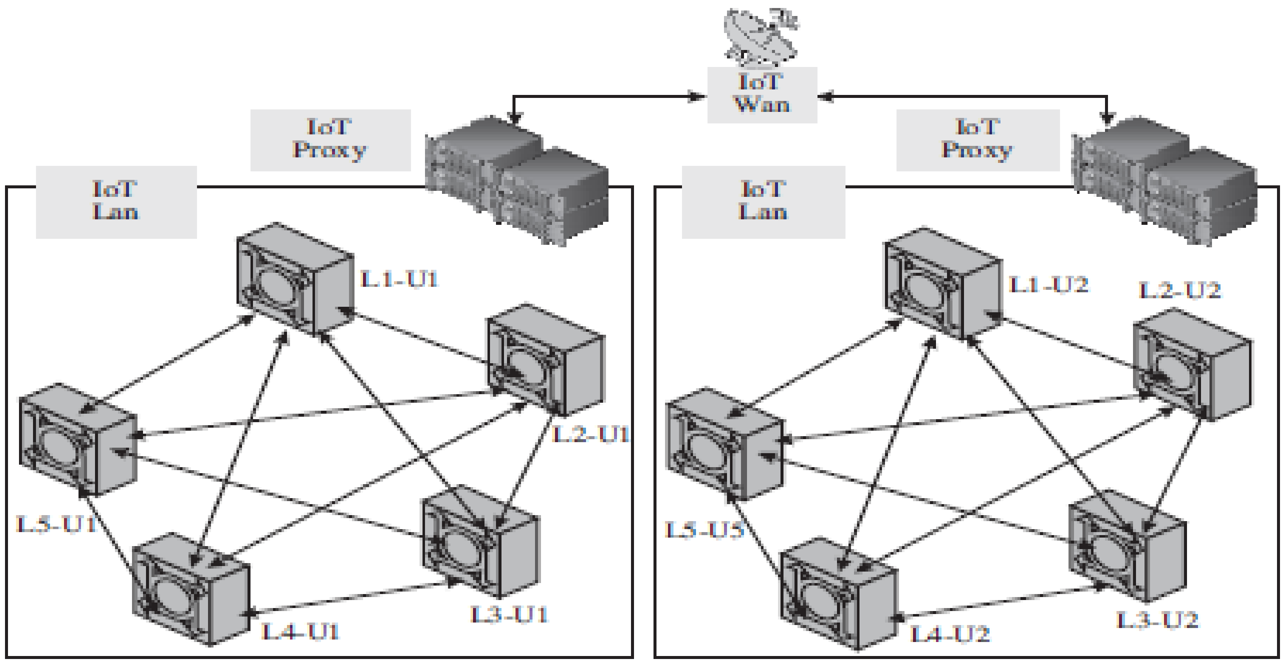
- This class can be considered as an isolated class, where the communication between IoT nodes is restricted within a LAN only
- Uses link local (LL) addresses
- The communication among the nodes may be direct or through other nodes (as in a mesh configuration)



Address management classes

Class 2:

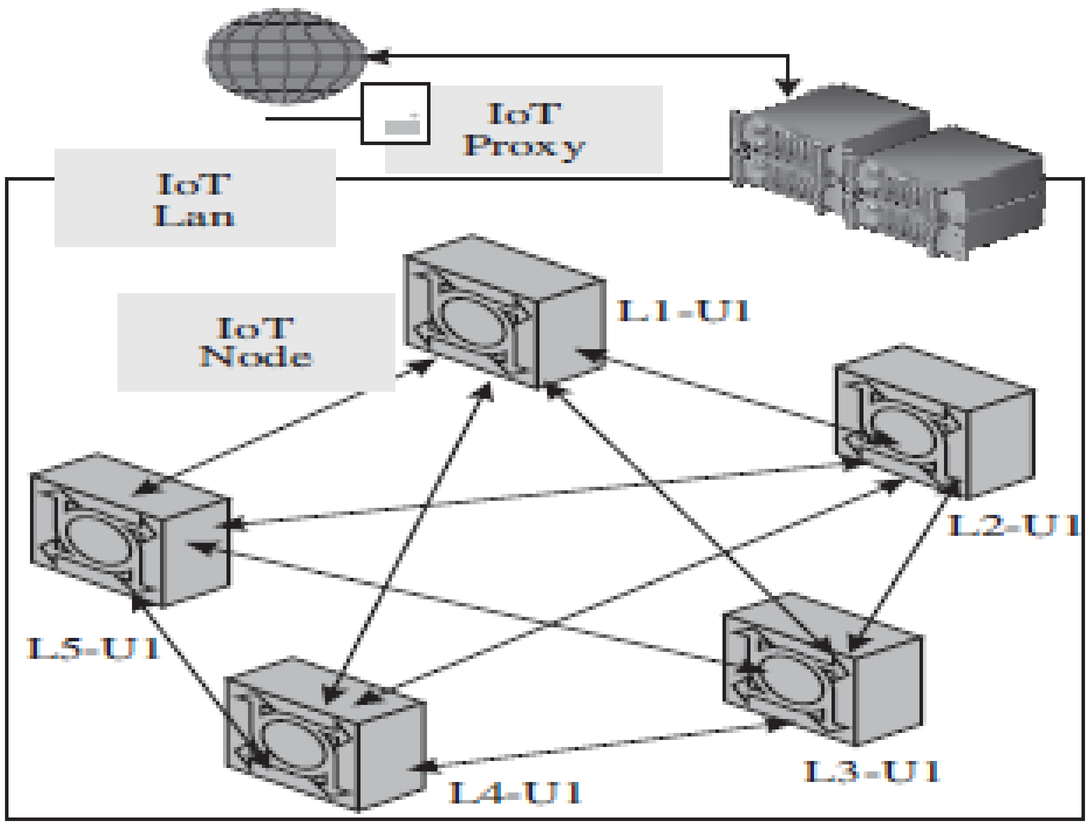
- Generally, ULA is used for addressing; however, in certain scenarios, GUA may also be used
- L1–L5 are the LL addresses of the locally unique IoT nodes within the LAN
- whereas U1 and U2 are the unique addresses of the two gateways extending communication to their LANs with the WAN



Address management classes

Class 3:

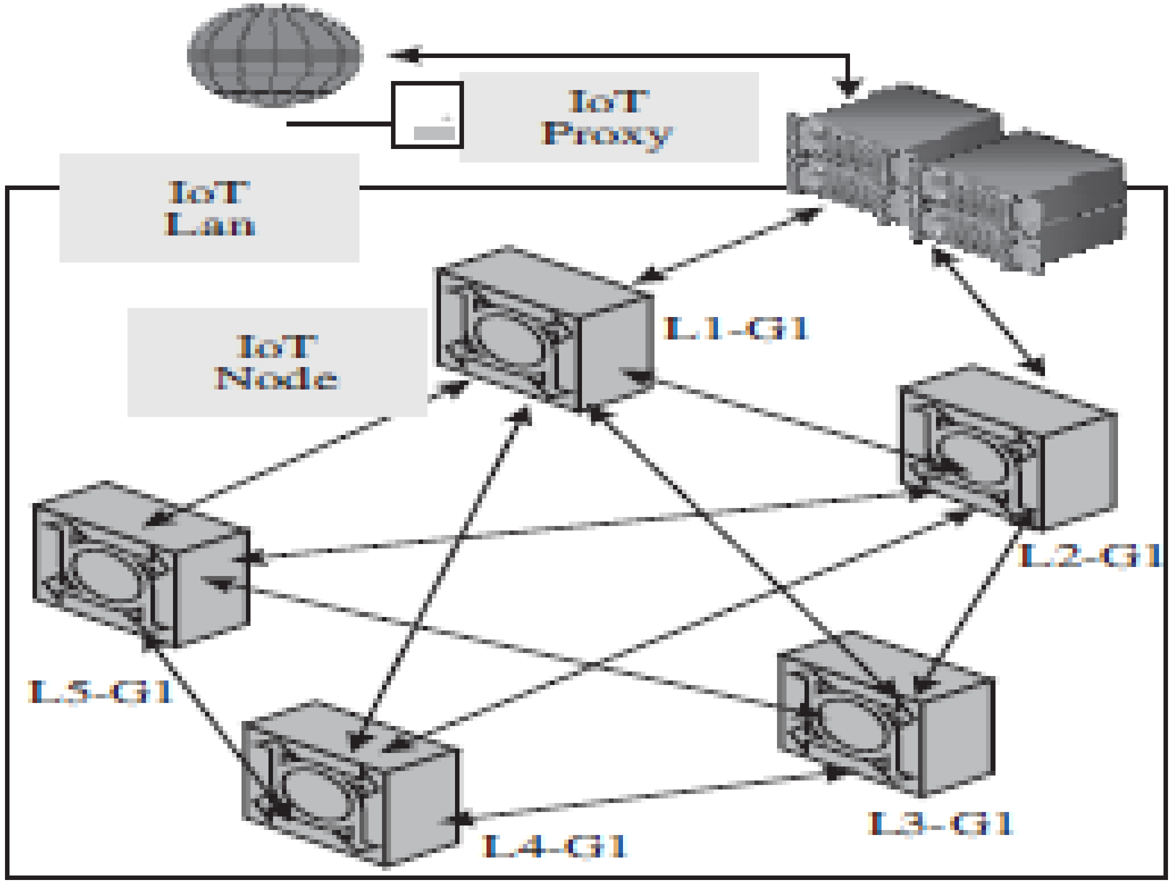
- IoT LAN is connected to an IoT proxy
- proxy functions: address allocation, address management to providing security to the network underneath it.
- IoT proxy only uses ULA



Address management classes

Class 4:

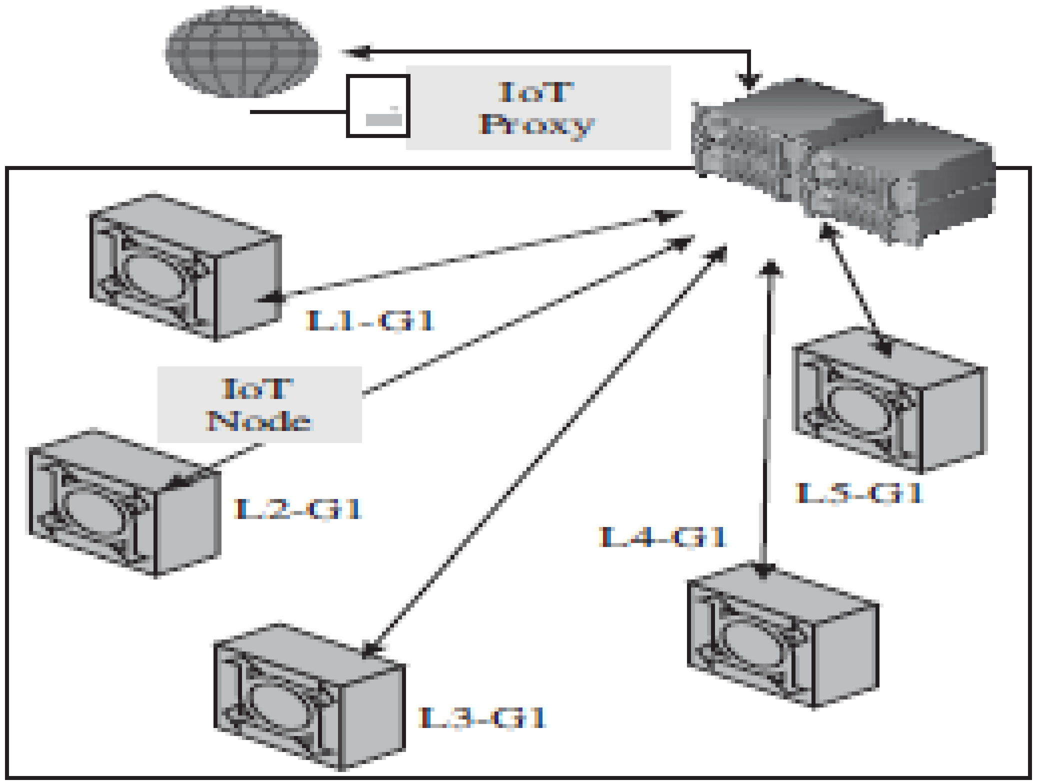
- IoT proxy acts as a gateway between the LAN and the Internet
- provides GUA to the IoT nodes within the LAN
- globally unique prefix is allotted to this gateway
- gateway also enables local communication between the nodes without the need for the packets to be routed through the Internet



Address management classes

Class 5:

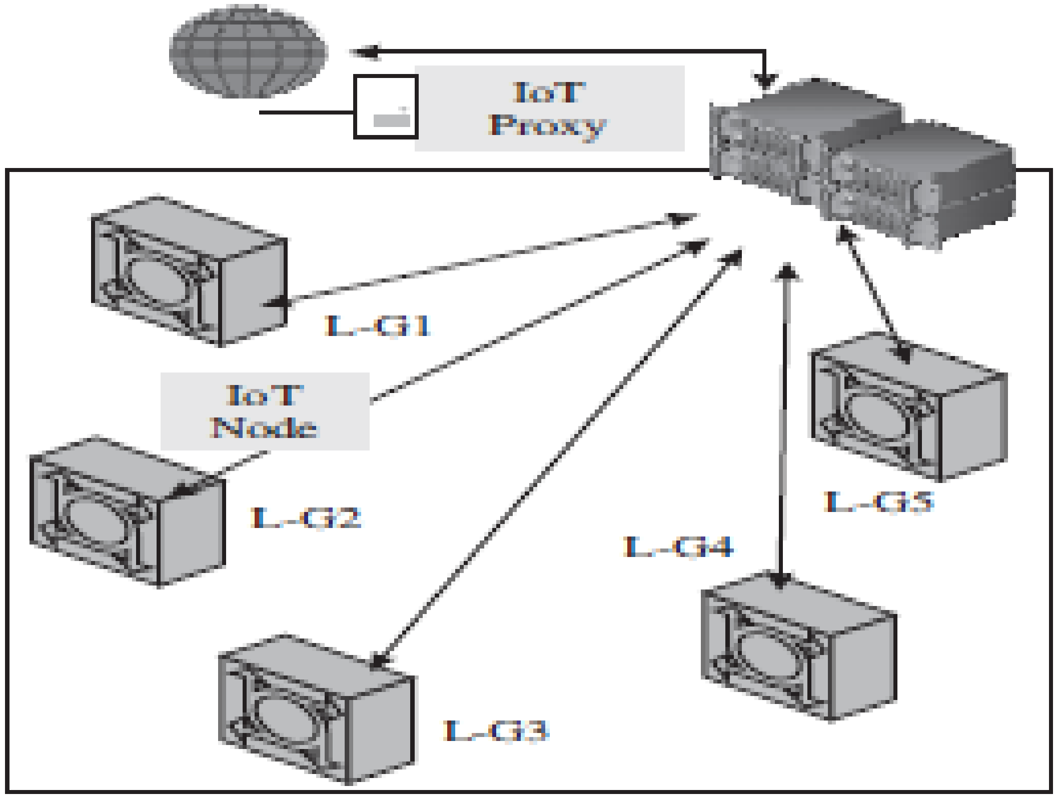
- star topology with the gateway as the center of the star
- proxy beyond the gateway enables global communication through the Internet
- The IoT nodes within a gateway's operational purview have the same GUA.



Address management classes

Class 6:

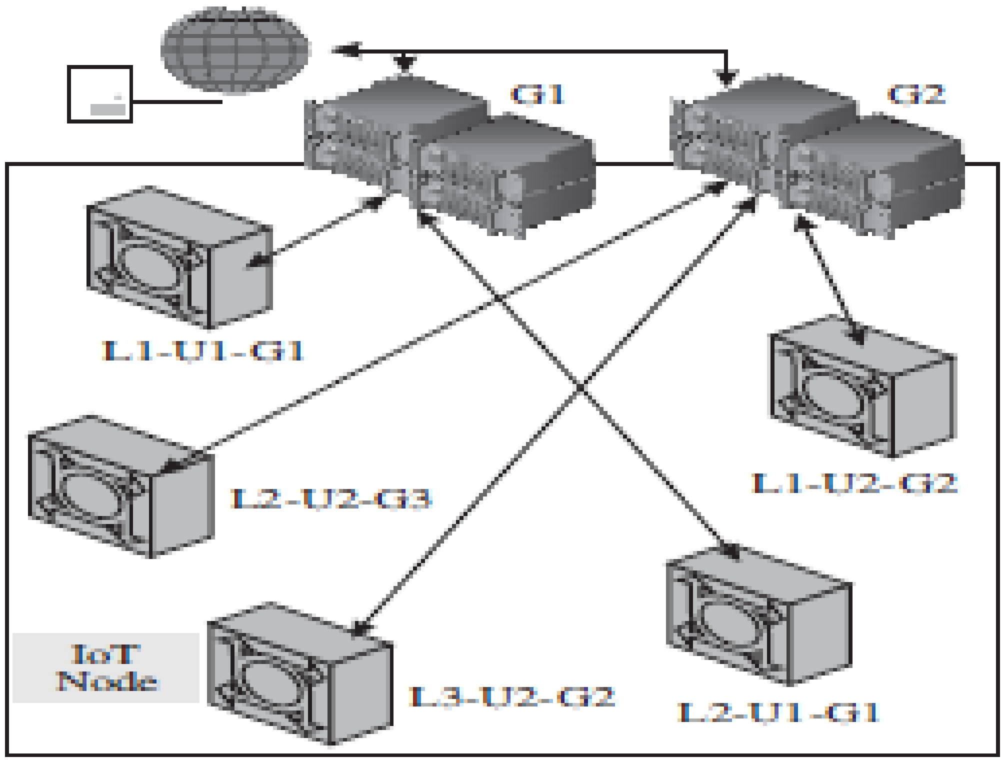
- IoT nodes are all assigned unique global addresses (GUA), which enables a point-to-point communication network with an Internet gateway
- Typically, this class is very selectively used for special purposes.



Address management classes

Class 7:

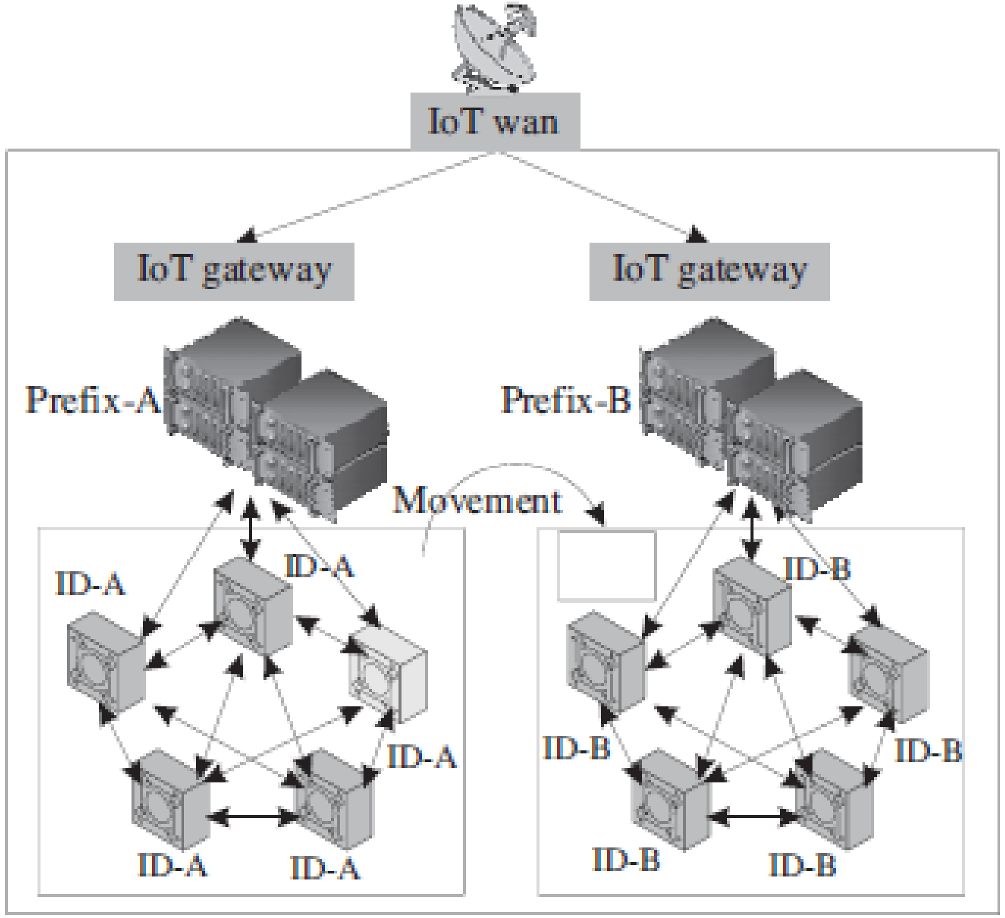
- Multiple gateways may be present;
- the configuration is such that the nodes should be reachable through any of the gateways.
- Typically, organizational IoT deployments follow this class of configuration.
- The concept of multihoming is important and inherent to this class.



Addressing during node mobility

Global Prefix Changes

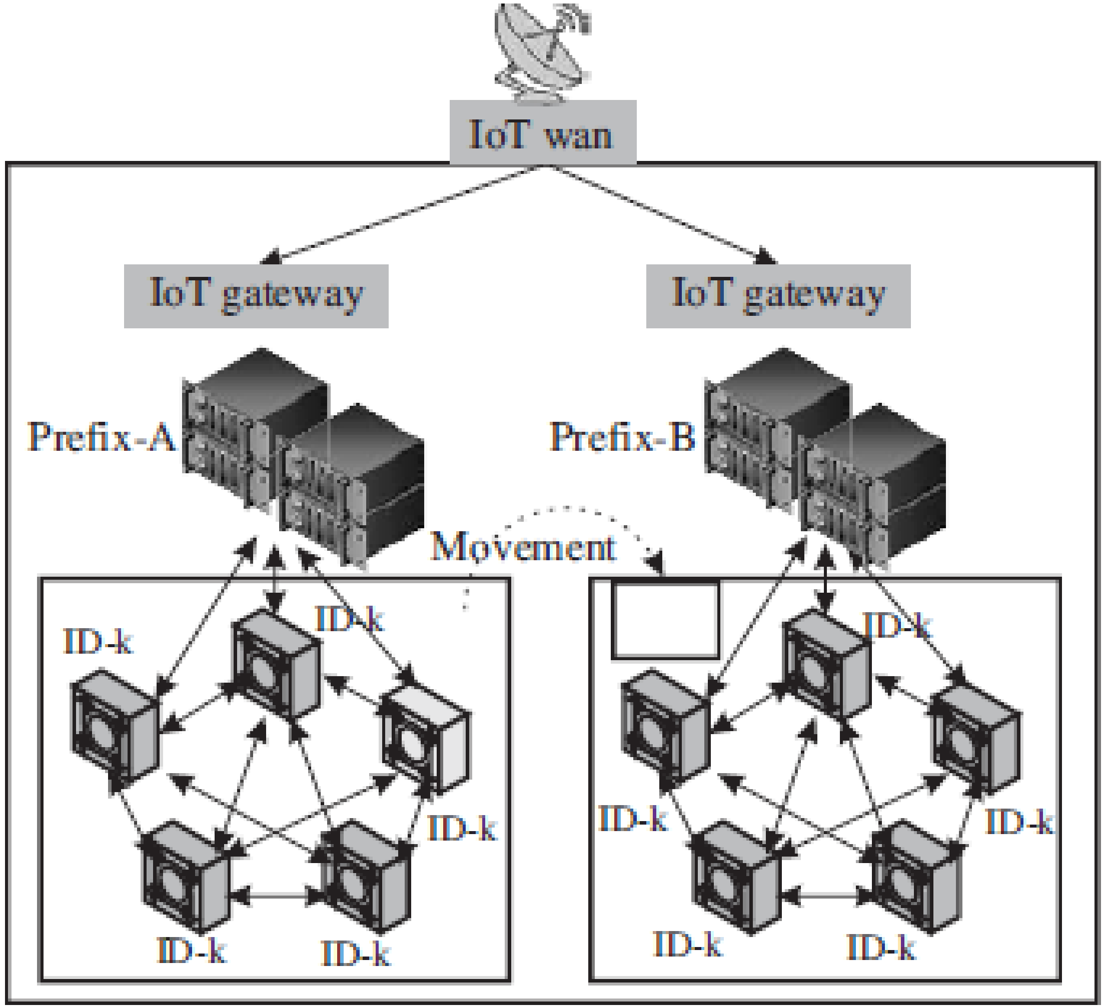
- abstracts the addressing strategy using global prefix changes
- Node moving from one LAN to another LAN, prefix changes, causes clash with native interface identifier
- Nodes constrained with low-power and low-processing cannot handle DHCPv6/SLAAC



Addressing during node mobility

Prefix Changes within WANs

- abstracts the addressing strategy for prefix changes within WANs
- The address allocation is hence delegated to entities such as gateways and proxies
- Uses ULA to manage network within WAN



Addressing during node mobility

Remote Anchoring

- abstracts the addressing strategy using a remote anchoring point
- applicable in 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.
- remote anchoring point from which the IoT nodes obtain their global addresses through tunneling (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