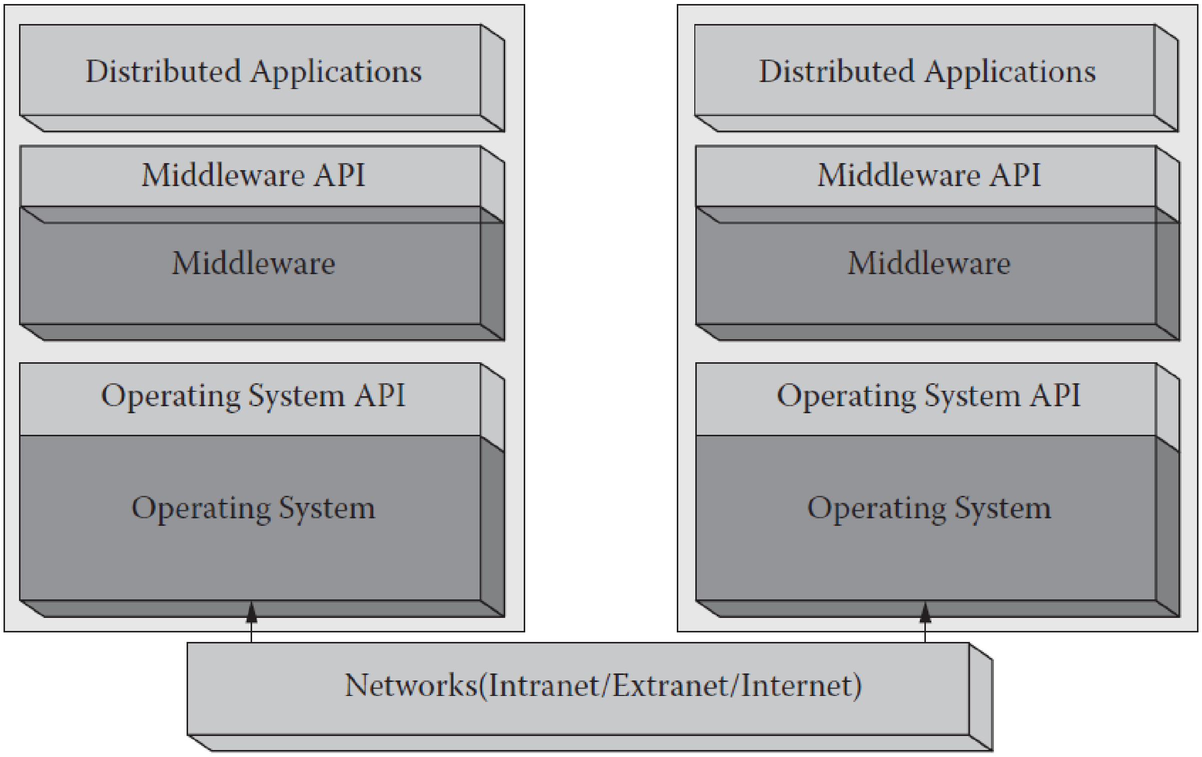
Unit– II
IoT Middleware & Internet Principles

2.1 Middleware: Definition & Its types.
2.2 M2M Communication: Journey from M2M to IoT, M2M system Architecture.
2.3 RFID: Middleware Architecture, Frequency ranges Bar code format & Application.
WSN: Middleware Architecture, the Internet of Transducers & its Application.
SCADA: Middleware Architecture, the Internet of Controllers & its Application.
2.4 IP Addresses & its types: static and dynamic, TCP/IP layers: TCP and UDP.
2.5 MAC addresses Application layer protocols.

<u>Middleware:</u>



<u>Definition:</u>

“Runtime system software that directly enables application-level interactions among programs in a distributed computing environment”

The term *middleware* refers to a layer that is arranged on top of operating systems and communications stacks and thus hides heterogeneity from the applications through a set of common, well-defined interfaces. Middleware is a piece of reusable software that communicates to other processes, most of the time over a network connection.

Middleware is software that serves as an interface between components of the IoT, making communication possible among elements that would not otherwise be capable, often described as "software glue," middleware makes it easier for software developers to implement communication and input/output so that they can shift their focus to the specific purpose of their application.
In this way, the distributed client and server components of which an application is made up can be programmed in the same manner as if they were executed on the same host.

Middleware brings the following values

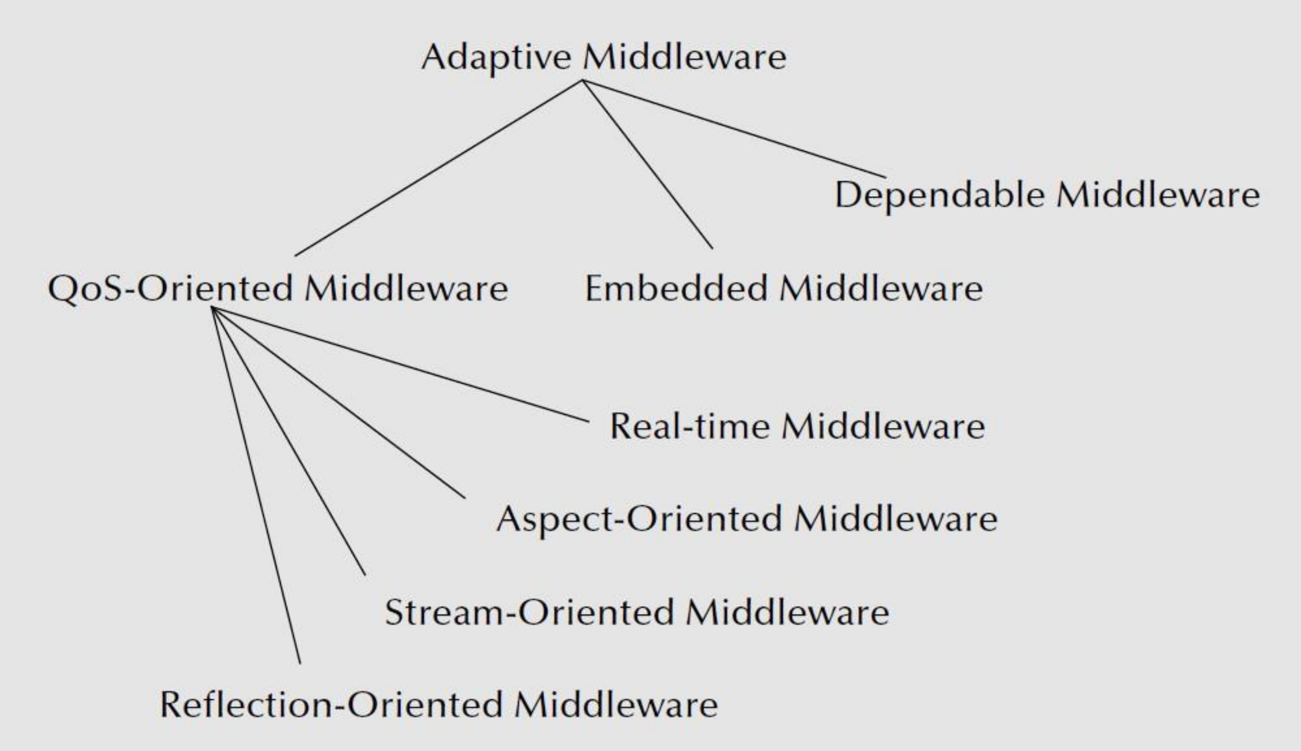
Enables applications running across multiple platforms to

- communicate with each other
- Shields the developer from dependencies on network protocols,
- operating systems, and hardware platforms
- Is a software layer that lies between the operating system
- and the applications on each site of the system
- Hides heterogeneity and location independence
- Increases software portability
- Provides common functionality needed by many applications
- Aids application interoperability
- Aids scalability
- Helps integrate legacy facilities

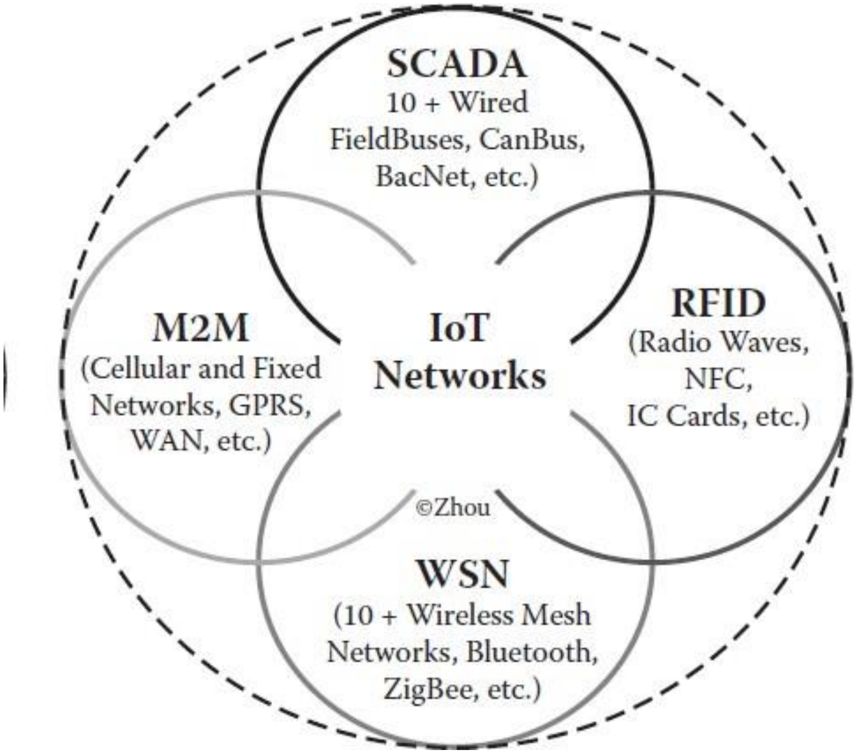
Types of Middleware:

- Message-Oriented Middleware
- CEP (complex event processing) Middleware
- Adaptive and Reflective Middleware
- Transaction Middleware
- Peer-to-Peer Middleware
- Grid Middleware
- Model-Driven Middleware
- Games Middleware
- Mobile Computing Middleware
- Radio-frequency Identification (RFID) (Smart Cards)Middleware)
- Three-tiered Application Server Middleware
- Real-time CORBA Middleware
- High-Availability Middleware
- Security Middleware
- RFID Edge Middleware
- Process-Oriented Middleware
- Business-to-Business (B2B)-Oriented Middleware
- Middleware for Location-Based Services

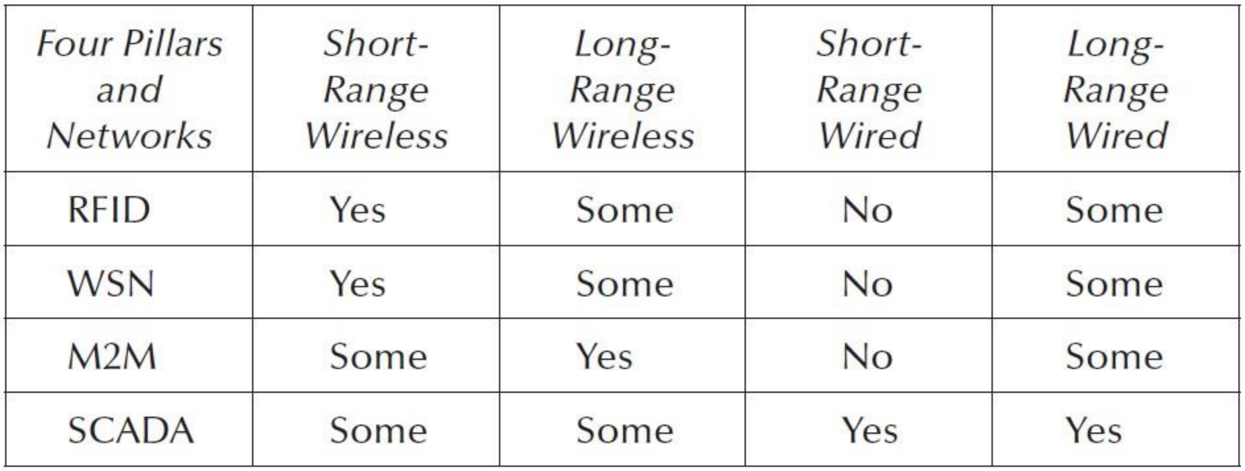
- Surveillance Middleware



The four pillars of IoT paradigms and related networks.



IoT is the glue that fastens the four pillars through a common set of best practices, networking methodology, and middleware platform. This enables the user to connect all of their physical assets with a common infrastructure and a consistent methodology for gathering machine data and figuring out what it means.



Four Pillars and Networks	Short-Range Wireless	Long-Range Wireless	Short-Range Wired	Long-Range Wired
RFID	Yes	Some	No	Some
WSN	Yes	Some	No	Some
M2M	Some	Yes	No	Some
SCADA	Some	Some	Yes	Yes

- **M2M (Internet of Devices)**uses devices (such as an in-vehicle gadget) to capture events (such as an engine disorder), via a network (mostly cellular wireless networks, sometimes wired or hybrid) connection to a central server (software program), that translates the captured events into meaningful information (alert failure to be fixed).
- **RFID (Internet of Objects)**uses radio waves to transfer data from an electronic tag attached to an object to a central system through a reader for the purpose of identifying and tracking the object.
- A **WSN(Internet of Transducers)** consists of spatially distributed autonomous sensors to monitor physical or environmental conditions, such as temperature, pressure, motion, or pollutants, and to cooperatively pass their data through the network, mostly short-range wireless mesh networks, sometimes wired or hybrid, to a main location reports on the overlaps or coverage differences when WSN was compared with M2M and RFID; SCADA or smart system was not mentioned in the report.)
- **SCADA(Internet of controllers)** is an autonomous system based on closed-loop control theory or a smart system or a CPS that connects, monitors, and controls equipment via the network (mostly wired short-range networks, also known as., field buses, sometimes wireless or hybrid) in a facility such as a plant or a building.

Journey from M2M to IoT

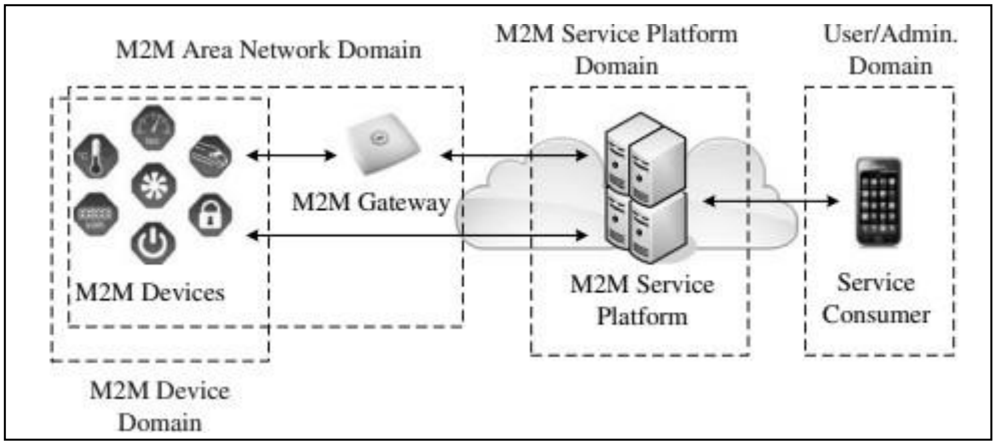
Machine-to-machine communication, or M2M, is exactly as it sounds: two machines "communicating," or exchanging data, without human interfacing or interaction. uptake of both M2M and IoT solutions will increase dramatically.

Reasons for using M2M and IoT

1. An increased need for understanding the physical environment in its various forms, from industrial installations through to public spaces and consumer demands.
2. The improvement of technology

3. Improved networking capabilities.
4. Reduced costs of components and the ability to more cheaply collect and analyse the data they produce.

M2M system Archtecture:



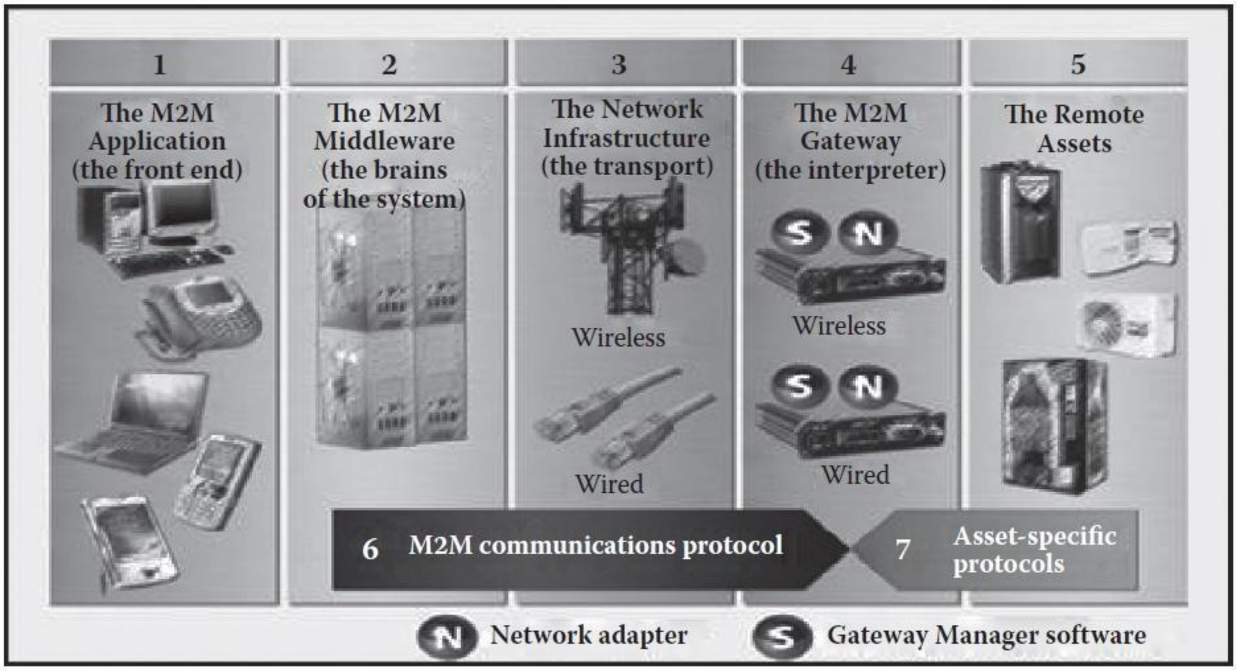
- M2M system is divided into three main domains:
  - ➢ M2M area network domain (or M2M device domain)
  - ➢ M2M service platform domain,
  - ➢ user/administrator domain.

M2M area network domain

- The M2M devices can connect to the M2M service platform directly through a wide area network (WAN) connection (e.g., cellular 3G/4G) or an M2M gateway (aggregation point).
  - ➢ The M2M gateway collects and processes data from simpler M2M devices and manages their configuration/operation. Also, it ensures that the M2M devices interoperate with and are interconnected with the communication network.
  - ➢ The M2M devices and M2M gateway are comprised of an M2M area network, which provides connectivity among them.
  - ➢ Typically, the use of an M2M area network is preferred when the cost, power, or location of the M2M devices is a deciding factor. In this case, several wireless personal area network (WPAN) technologies, such as Wi-Fi, ZigBee/IEEE 802.15.4, and Bluetooth, can be adopted, through which these devices can communicate.
- **M2M network domain**
  - ➢ M2M network domain acts as a bridge between the M2M application domain and the M2M device domain. It is made of two parts called the M2M core and M2M service capabilities.
  - ➢ The network domain includes the core and access networks.
- **M2M application domain**
  - ➢ As the name suggests, the M2M application domain offers applications to use M2M technology conveniently. Examples include server and end-user applications.

M2M architecture based on middleware.

Figure shows the typical architecture of an M2M system. The integration middleware at the server side is the brain of the entire system.


1
The M2M Application (the front end)
2
The M2M Middleware (the brains of the system)
3
The Network Infrastructure (the transport)
Wireless
Wired
4
The M2M Gateway (the interpreter)
S N
Wireless
S N
Wired
5
The Remote Assets
6 M2M communications protocol
7 Asset-specific protocols
N Network adapter
S Gateway Manager software

M2M Service Enablement Middleware

Vertical Applications
Applications to connect to and communicate with objects tailored for specific verticals. Must be done in partnership with industry.

Service Enablement Middleware (APIs over Internet)
Reduce complexities with regard to fragmented connectivity, device standards, application information protocols, etc., and device Management. Build on and extend connectivity.

Connectivity (ADSL, SMS, USSD, GSM, GPRS, UMTS, HSPA, WiFi, Satellite, Zigbee, RFID, Bluetooth, etc.)

Connectivity tailored for object communication
with regards to business model, service level, SIM provisioning, billing, etc.

Comparison between M2M and IoT

Sr.NO	**Basis of**	**IoT(**Internet of Things)	**M2M(**Machine to Machine)
1	Intelligence	Devices have objects that are responsible for decision making	Some degree of intelligence is observed in this.

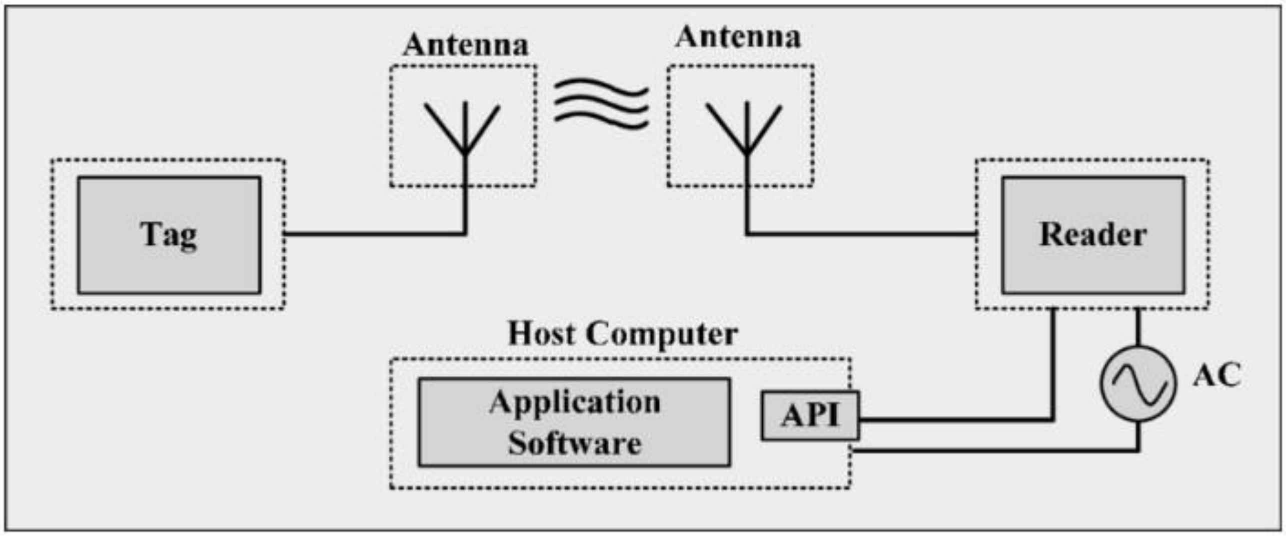
2	Connection type used	The connection is via Network and using various communication types.	The connection is a point to point
3	Communication protocol used	Internet protocols are used such as HTTP, FTP, and Telnet.	Traditional protocols and communication technology techniques are used
4	Data Sharing	Data is shared between other applications that are used to improve the end-user experience.	Data is shared with only the communicating parties.
5	Internet	Internet connection is required for communication	Devices are not dependent on the Internet.
6	Type of Communication	It supports cloud communication	It supports point-to-point communication.
7	Computer System	Involves the usage of both Hardware and Software.	Mostly hardware-based technology
8	Scope	A large number of devices yet scope is large.	Limited Scope for devices.

RFID: The Internet of Objects

RFID = Radio Frequency IDentification.
An ADC (Automated Data Collection) technology that uses radiofrequency waves to transfer data between a reader and a movable item to identify, categorize, track

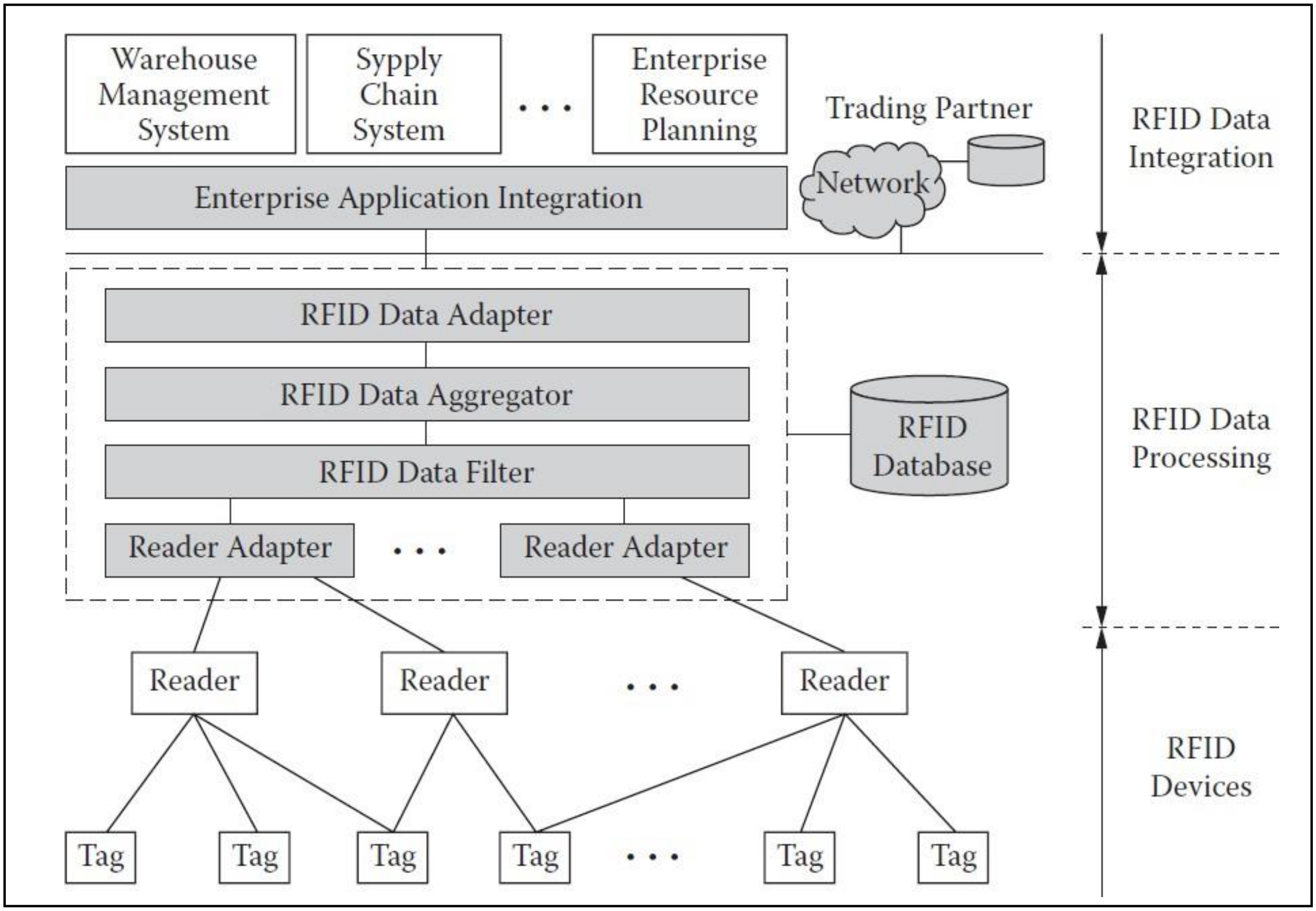
- Is fast and does not require physical sight or contact between reader/scanner and the tagged item. – Performs the operation using low cost components.
- Attempts to provide unique identification and backend integration that allows for wide range of applicationOther ADC technologies: Bar codes, OCR

RFID System components:



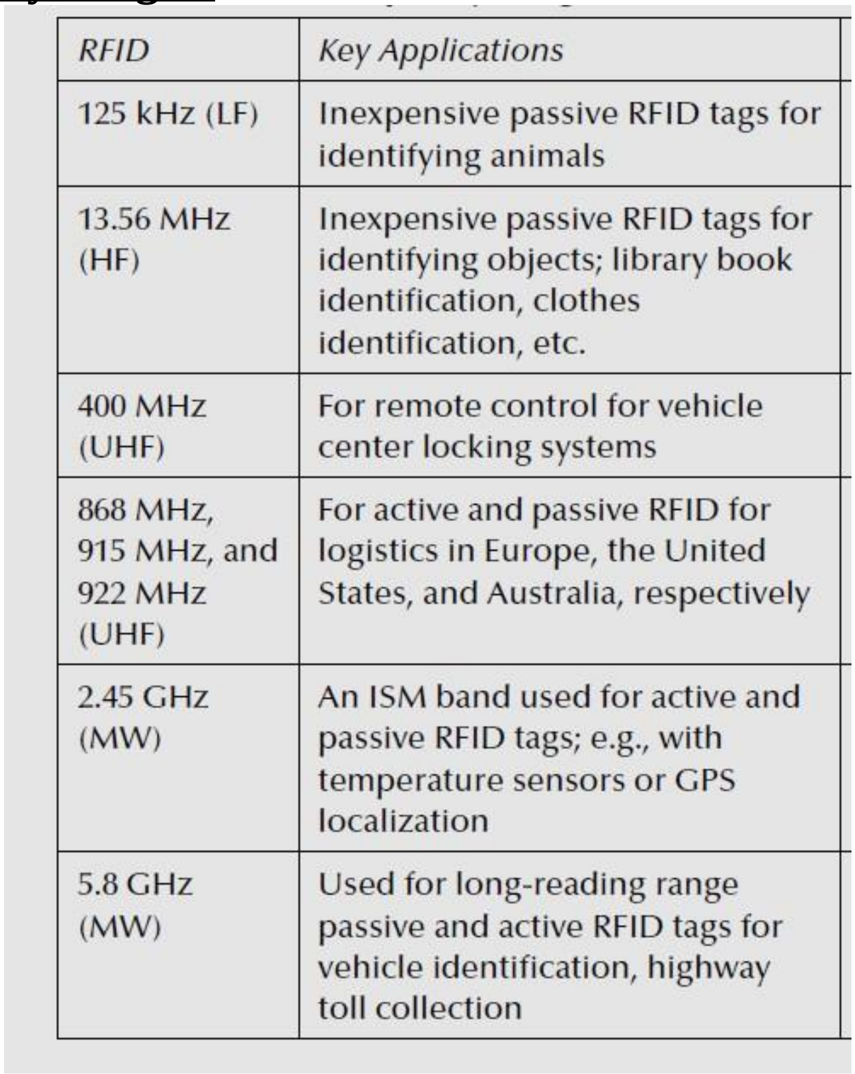
- An RFID system involves hardware known as
  - readers
  - Tags
  - RFID software or RFID middleware
- RFID tags can be active, passive, or semipassive. Passive RFID does not use a battery, while an active has an on-board battery that always broadcasts its signal. A semipassive RFID has a small battery on board that is activated when in the presence of a RFID reader.

RFID MIDDLEWARE ARCHITECTURE:



- RFID networking shares similar three-tiered communication architecture. RFID readers are the gateways similar to MAN. Data from the readers go to the corporate LAN and then are transmitted to the Internet as needed.
- In a general, the RFID middleware manages the readers and extracts Electronic Product Code (EPC) data from the readers; performs tag data filtering, aggregating, and counting; and sends the data to the enterprise WMSs (warehouse management systems), backend database, and information exchange broker.
- An RFID middleware works within the organization, moving information (i.e., EPC data) from the RFID tag to the integration point of high-level supply-chain management systems through a series of data-related services.
- From the architectural perspective, RFID middleware has four layers of functionality:
  - Reader adapter
  - RFID Data Filter
  - Data Aggregator
  - RFID Data Adapter
- The application integration provides varieties of reliable connection mechanisms (e.g., messaging, adaptor, or the driver) that connect the RFID data with existing enterprise systems such as ERP or WMS.

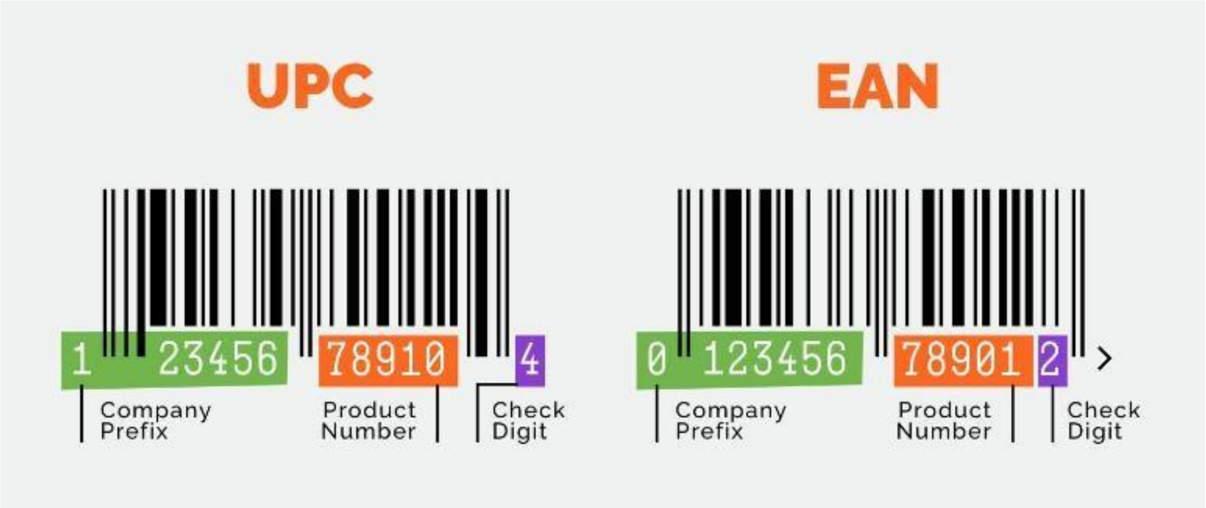
RFID Frequency ranges:



RFID	Key Applications
125 kHz (LF)	Inexpensive passive RFID tags for identifying animals
13.56 MHz (HF)	Inexpensive passive RFID tags for identifying objects; library book identification, clothes identification, etc.
400 MHz (UHF)	For remote control for vehicle center locking systems
868 MHz, 915 MHz, and 922 MHz (UHF)	For active and passive RFID for logistics in Europe, the United States, and Australia, respectively
2.45 GHz (MW)	An ISM band used for active and passive RFID tags; e.g., with temperature sensors or GPS localization
5.8 GHz (MW)	Used for long-reading range passive and active RFID tags for vehicle identification, highway toll collection

Bar code format

The U.P.C. stands for Universal Product Code (UPC-A) and E.A.N. stands for European Article Number (EAN-13 or International Article Number).. The UPC was the original format for product barcodes in the 1970s. Later on, as demand in Europe, Asia and Australia grew country codes were added to the front of the barcode number increasing it to 13 digits. USA and Canada have a country code of zero which is not printed under the barcode nor is it entered in US and Canadian Inventory Point of Sale systems.



RFID Applications:

- Product Tracking
- Toll Road Payments
- Passports
- Logistics and inventories in the retail industry.
- Shipping
- Security control and jewelry.
- Cosmetics and medicines.
- Control of disposals and tools in hospitals.
- Libraries.
- Files and archives.
- Aviation baggage control

WSN-Internet of Transducers:

WSN- wireless sensor network

Middleware Architecture

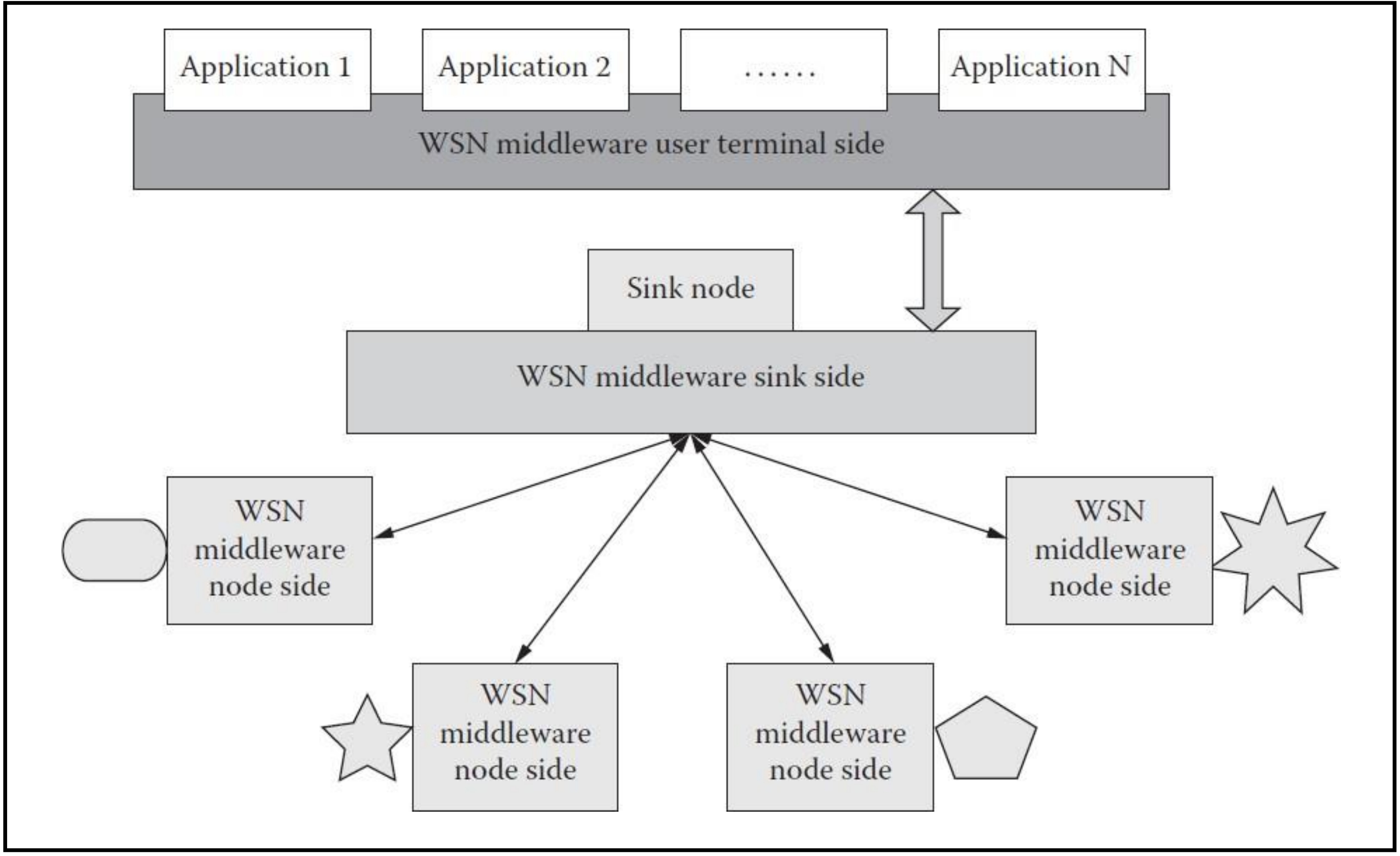
WSN middleware is a kind of middleware providing the desired services for sensor-based pervasive computing applications that make use of a WSN and the related embedded operating system or firmware of the sensor nodes. In most cases, WSN middleware is implemented as embedded middleware on the node

A complete WSN middleware solution should include four major components

- Programming abstractions- Programming abstractions define the interface of the middleware to the application programmer.
- System services- System services provide implementations to achieve the abstractions.

- runtime support- Runtime support serves as an extension of the embedded operating system to support the middleware services
- Quality of service (QoS) mechanisms- QoS mechanisms define the QoS constraints of the system.

Middleware for WSN should also facilitate development, maintenance, deployment, and execution of sensing-based applications.



Challenges of WSN middleware:

- Limited power and resources, e.g., battery issues
- Mobile and dynamic network topology
- Heterogeneity, various kinds of hardware and network protocols
- Dynamic network organization, ad-hoc capability

Applications:

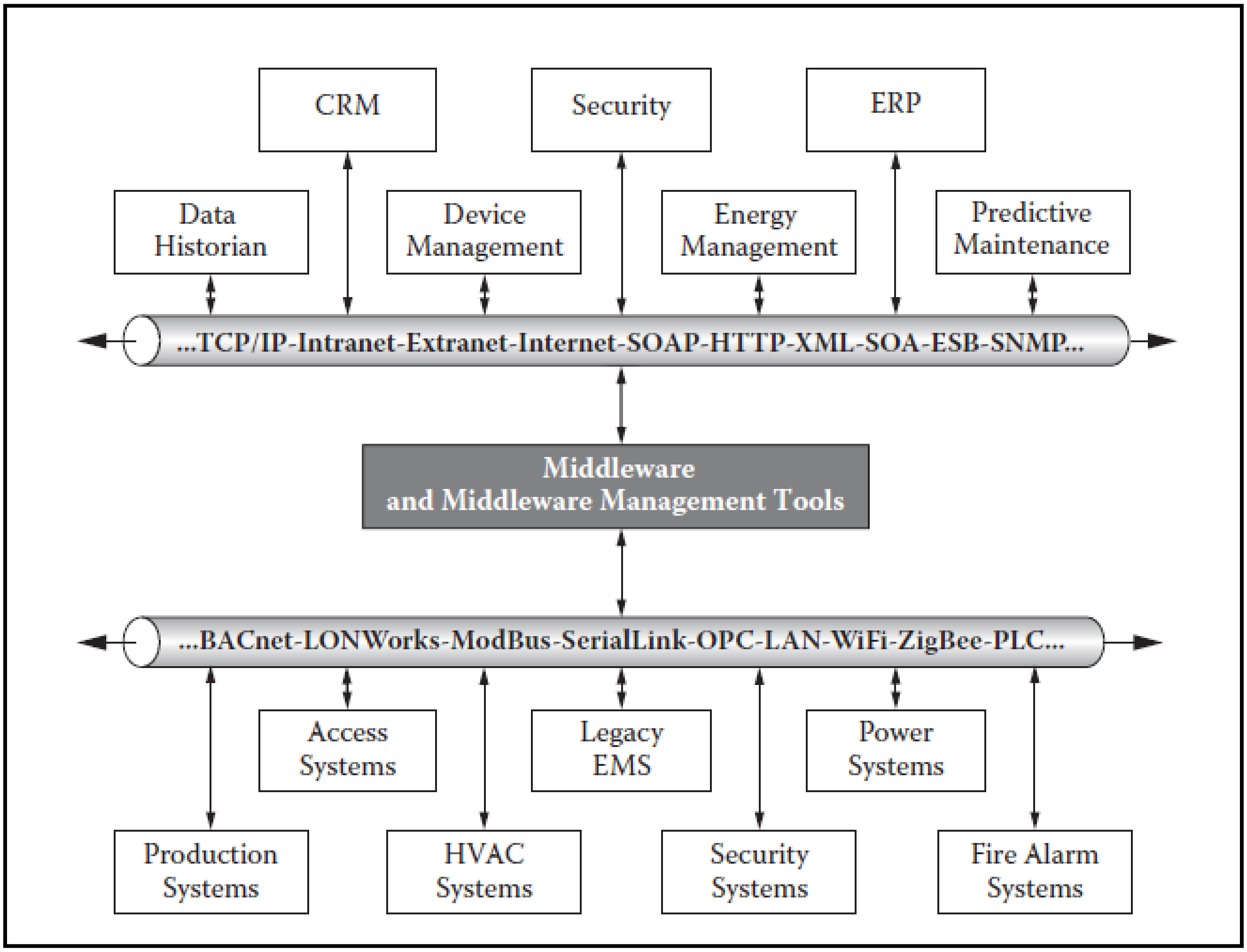
- healthcare domain,
- image/vision processing
- communication and networking
- distributed and embedded processing
- surveillance
- Environmental monitoring
- smart homes
- virtual reality

SCADA: The Internet of Controllers

SCADA (supervisory, control and data acquisition) systems, as the core technology of the controls–IT convergence, will evolve and take the center stage. By their very nature, SCADA, low-data- rate (LDR), and M2M/IoT services are closely related and largely overlapped in technologies and deployment approaches,
An existing SCADA system usually consists of the following
subsystems

- A human–machine interface (HMI), which is the apparatus that presents process data to a human operator, and through this, the human operator monitors and controls the process.
- Remote terminal units (RTUs) connect to sensors in the process, convert sensor signals to digital data, and send digital data to the supervisory system.
- PLCs are used as field devices because they are more economical, versatile, flexible, and configurable than special-purpose RTUs.
- DCSs; as communication infrastructures with higher capacity become available, the difference between SCADA and DCS will fade. SCADA is combining the traditional DCS and SCADA.

SCADA Middleware Architecture:



Applications:

- Water management and water treatment systems
- Oil and gas facilities
- Manufacturing sites

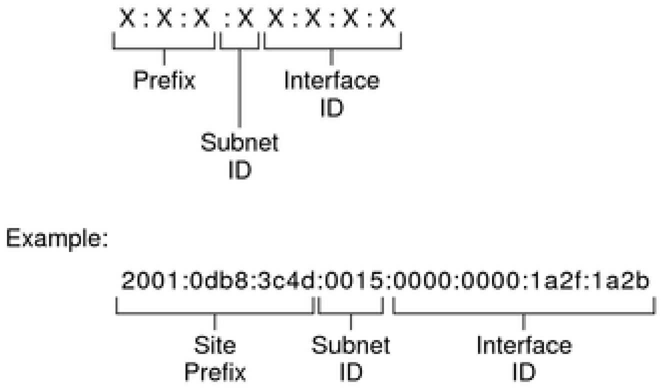
IP ADDRESSING IN THE IoT

An IP header consists of source and destination addresses, called IP addresses. The Internet generally uses IPv4 addresses. IoT/M2M use IPv6 addresses.

IPv6 addresses for IoT/M2M

An IPv6 address is 128 bits in length and consists of eight, 16-bit fields, with each field bounded by a colon. Each field must contain a hexadecimal number, in contrast to the dotted-decimal notation of IPv4 addresses. In the figure, the x's represent hexadecimal numbers.

Basic IPv6 Address Format



- The leftmost three fields (48 bits) contain the **site prefix**. The prefix describes the **public topology**

- The next field is the 16-bit subnet ID. The subnet ID describes the **private topology**,

- The rightmost four fields (64 bits) contain the interface ID, also referred to as a **token**. The interface ID is either automatically configured from the interface's MAC address or manually configured in EUI-64 format.

IP V4 address for Internet

IPv4 address consists of 32 bits. However, it can be considered as four decimal numbers separated by dots.
For example, 198.136.56.2 for 32 bit
11000110 10001000 00111000 00000010.
Each decimal number is decimal value of an Octet (= 8 bits). IP addresses can be between 0.0.0.0 to 255.255.255.255; total 232 addresses due to 32-bit address. Three separate fields with a decimal number each for each set of 8 bits are easier to use. Let’s see an analogy with postal network addressing method.

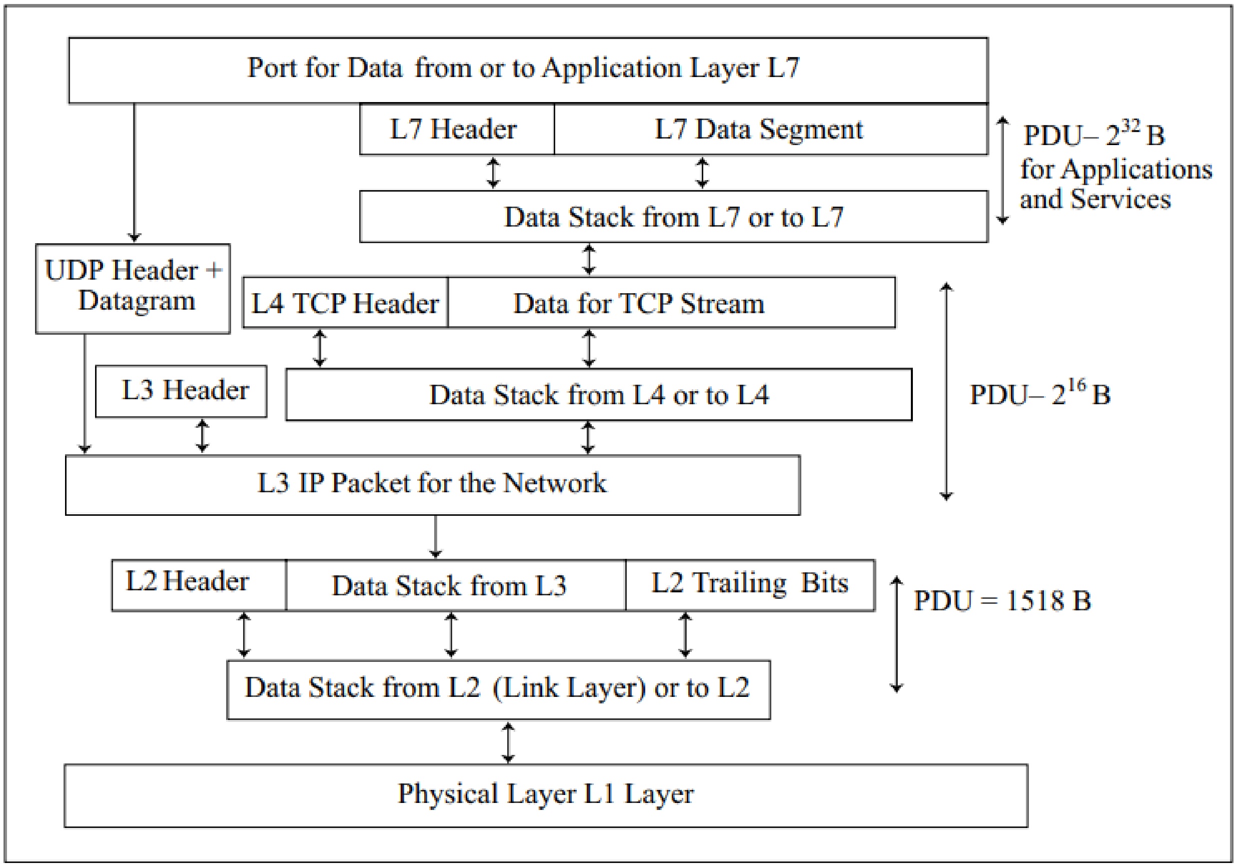
Types of IP addresses

- **Static IP address**
  A static IP address is the one assigned by the Internet service provider. The service provider may provide an individual just one address. When a company has a number of hosts, a service provider may provide a class C network address consisting of a group of254 (= 2^8 -2) IP addesses.
- **Dynamic IP address**
  Once a device connects to the Internet, it needs to be allotted an individual IP address. When the device connects to a router, the router and device use the DHCP (Dynamic Host Control Protocol) which assigns an IP address at an instance to the device. This address is called dynamic IP address. When a device disconnects or switches off or the router boots again, then the dynamic IP address is lost and a new allocation takes place when the device reconnects.

TCP/IP layers:

Fig:TCI/IP suite four layers generating data stack for the network and for physical layer during Internet communication

- Layer 1 is per communication protocol for physical link to routers. Figure shows the communication between the source and destination. Internet-based TCP/IP communication uses application layer L7, transport L4, Internet L3 and link L2 layers.
- A data segment (maximum 2^{32} B per segment) is accepted from L7 layer for transport layer TCP. L4 then generates a TCP stream. The stream packetizes at the Internet layer L3.
- Alternatively, a datagram (maximum 2^{14} B) is accepted from L7 layer for transport layer UDP usage. L4 then generates a UDP datagram (maximum 2^{16}B). The stream packetises at the Internet layer L3 into packets.
- Packet sent from L3 has maximum size 216B including L3 header. The datagram sent from L3 also has maximum size 216B.


Port for Data from or to Application Layer L7
L7 Header
L7 Data Segment
PDU– 2^32 B for Applications and Services
Data Stack from L7 or to L7
UDP Header + Datagram
L4 TCP Header
Data for TCP Stream
L3 Header
Data Stack from L4 or to L4
PDU– 2^16 B
L3 IP Packet for the Network
L2 Header
Data Stack from L3
L2 Trailing Bits
PDU = 1518 B
Data Stack from L2 (Link Layer) or to L2
Physical Layer L1 Layer

MEDIA ACCESS CONTROL (MAC Address)

- Each network connected node has an MAC address. A device node receives data stacks using its MAC address.
- Media means physical media, fibre or wire using which a device or node accesses the Internet. The nodes can use the same physical network and IP address.
- Node means an IoT device or sensor or actuator or controller or computer, the data-link layer of which communicates to the Internet.
- MAC address is 48 bit. Each network card or Ethernet protocol using a communicating node has a unique MAC address for the source and destination node addresses. Ethernet frame communicates before the data stack source-node MAC address and destination-node MAC address.

Application layer protocols: HTTP, HTTPS, FTP, TELNET

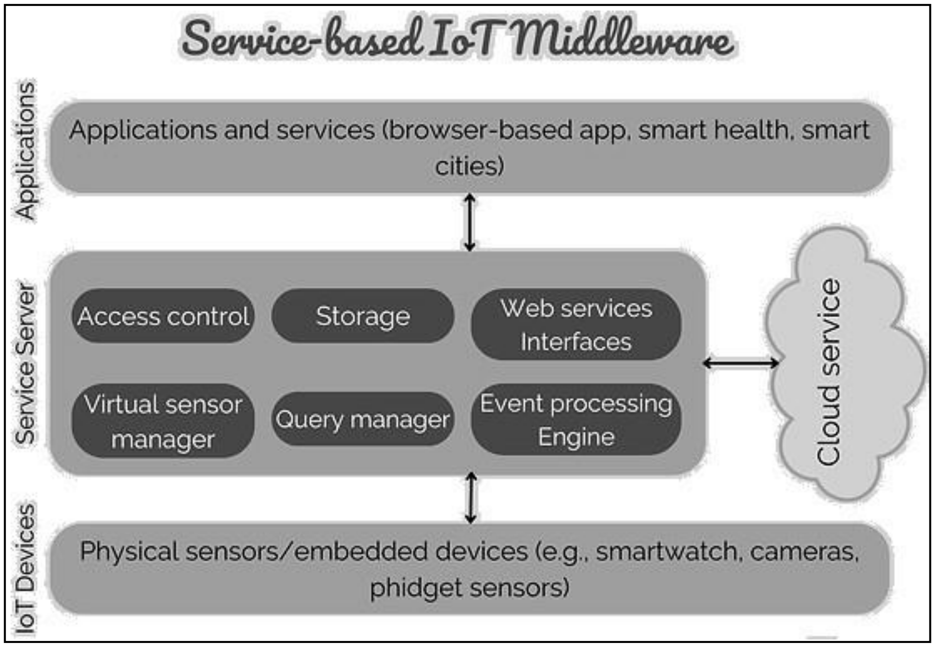
- TCP/IP suite consists of a number application layer protocols. For example, HTTP, HTTPS, FTP, Telnet and others
- Hyper Text Transfer Protocol (HTTP) port number is 80. A web HTTP server listens to port 80 only and responds to port 80 only. An HTTP port sends application data stack at the output to the lower layer using the HTTP protocol.

- An HTTP port uses a URL like http://www. mheducation.com/. The default port is taken as 80. The port number can be specified after the TLD. For example, after '.com' in URL http://www. mheducation.com:80/.
- HTTP is the standard protocol for· requesting a URL defined web-page resource, and for sending a response to the web server. An HTTP client requests an HTTP server on the Internet and the server responds by sending a response. The response may be with or without applying a process.
- HTTP is a stateless protocol. This is because for an HTTP request, the protocol assumes a fresh request. It means there is no session or sequence number field or no field that is retained in the next exchange.
- FTP-File Transfer Protocol
  FTP is a file transfer protocol. It is a stateful protocol.
- Telnet is for remote connection to a computer. SMTP is for mail transfer and PoP3 for mail retrieval from a mail server.

- **Service-based IoT Middleware**
- **Cloud-based IoT Middleware**
- **Actor-based IoT Middleware:**

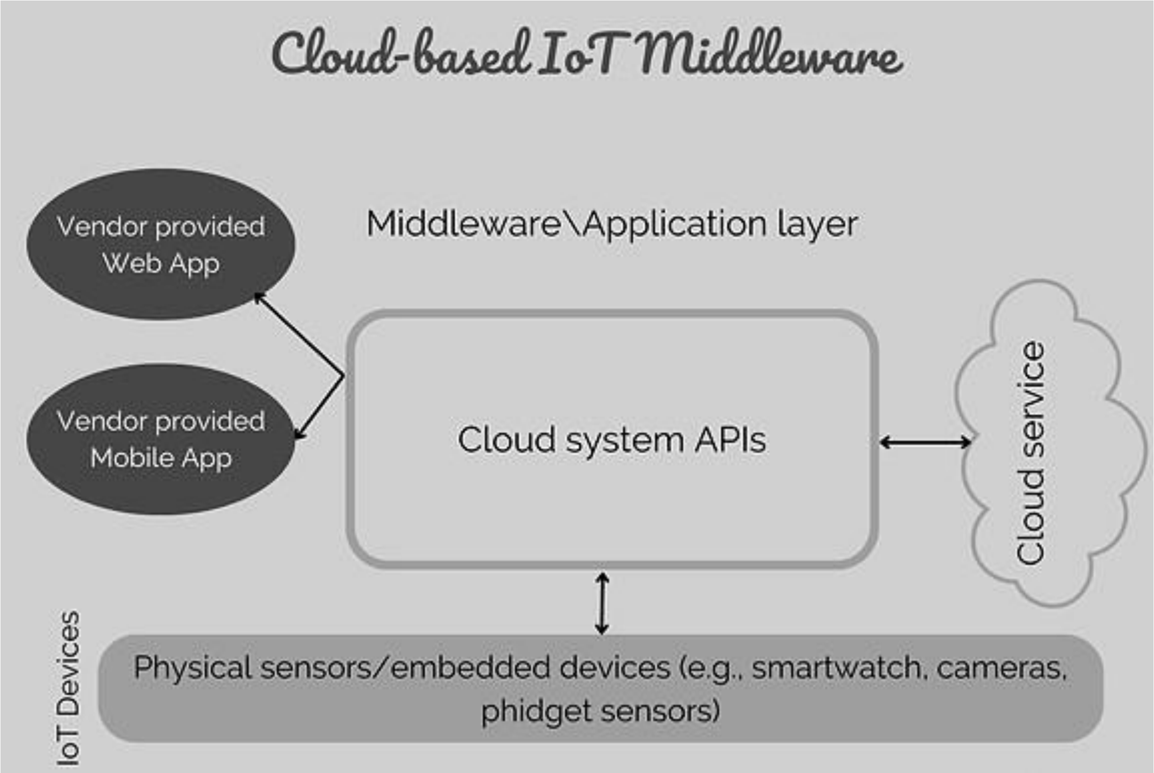
Service-based IoT Middleware :

- The first type, which we refer to it as a service-based solution, generally adopts the Service Oriented Architecture (SOA) and allows developers or users to add or deploy a diverse range of IoT devices as services.
- Service-based middleware can be deployed on premise or in the cloud. It provides users with a simple toolkit to view the raw collected IoT data.


Service-based IoT Middleware
Applications
Applications and services (browser-based app, smart health, smart cities)
Service Server
Access control
Storage
Web services Interfaces
Virtual sensor manager
Query manager
Event processing Engine
Cloud service
IoT Devices
Physical sensors/embedded devices (e.g., smartwatch, cameras, phidget sensors)

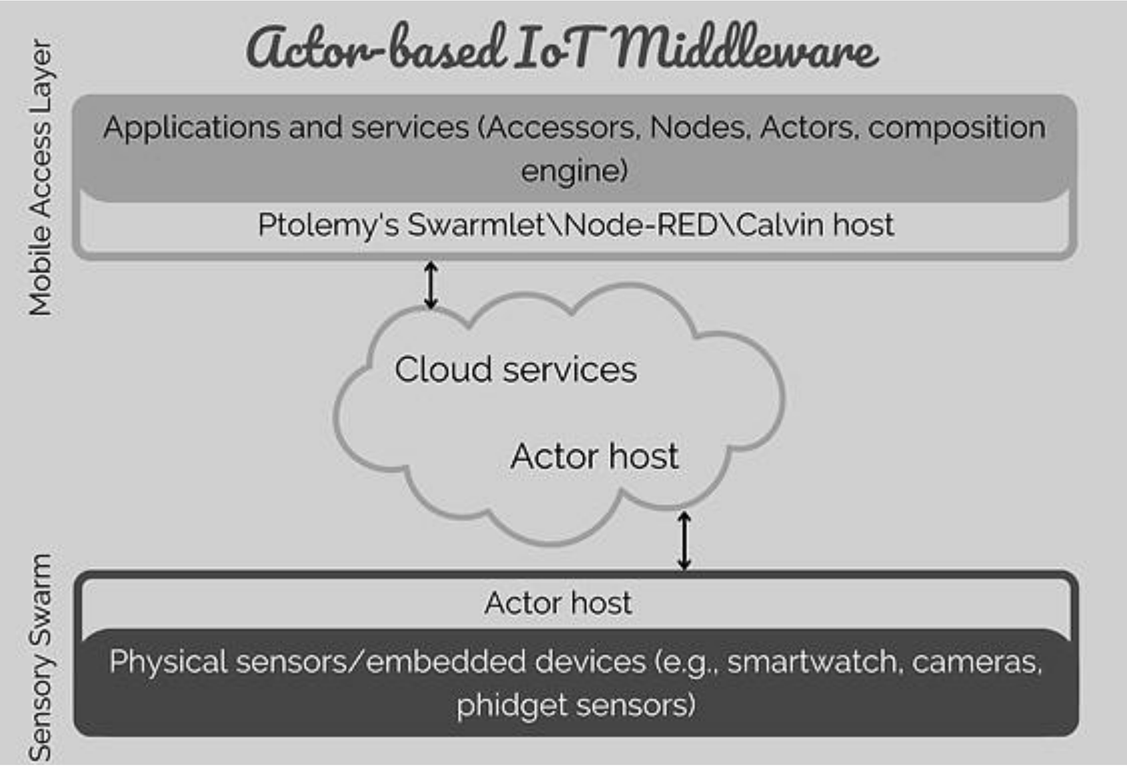
Cloud-based IoT Middleware

- The second type, which is known as cloud-based solution, limits the users on the type and the number of IoT devices that they can deploy, but enables users to connect, collect and interpret the collected data with ease since possible use cases can be determined and programmed a-priori.
- Meanwhile, it allows users to collect data easily due to pre-set scenarios. Cloud-based architecture helps achieve interoperability by applying specific standards.
- The core con is the high dependence on the vendor - the middleware stops working when the provider ends the service.


Cloud-based IoT Middleware
Vendor provided Web App
Middleware\Application layer
Vendor provided Mobile App
Cloud system APIs
Cloud service
IoT Devices
Physical sensors/embedded devices (e.g., smartwatch, cameras, phidget sensors)

Actor-based IoT Middleware:

- The third type is the actor-based framework that emphasizes on the open, plug and play IoT architecture. A variety of IoT devices can be exposed as reusable actors and distributed in the network.
- Each smart device can work as a reusable actor distributed in the network. Actor-based middleware ensures better latency and scalability for large-scale connected IoT devices because of its ability to be deployed in all layers.


Actor-based IoT Middleware
Mobile Access Layer
Applications and services (Accessors, Nodes, Actors, composition engine)
Ptolemy's Swarmlet\Node-RED\Calvin host
Cloud services
Actor host
Sensory Swarm
Actor host
Physical sensors/embedded devices (e.g., smartwatch, cameras, phidget sensors)