UNIT 9 IoT NETWORKING AND CONNECTIVITY TECHNOLOGIES

9.1 INTRODUCTION

Machine-to-Machine or M2M is a technology that allows connectivity between network devices. It allows tapping of sensor data and transmitting it over a public network. IoT technology, on the other hand, expands the concept of M2M by creating large networks of devices in which devices communicate with one another through cloud networking platforms. It allows users to create high performance, fast and flexible networks that can connect a variety of devices.

9.2 OBJECTIVES

After going through this unit, you should be able to:

- Know about the M2M and IoT technology
- Know about the components required for IoT implementation
- Know about gateway prefix allotment & impact of mobility
- Know about various identification and data protocols
- Know about various connectivity technologies

9.3 M2M AND IoT TECHNOLOGY

Machine-to-Machine or M2M is a technology that allows connectivity between network devices. This point to point connectivity is established to transfer information over public networks like ethernet or cellular networks without human intervention. Its main purpose is to tap sensor data and transmit it over a public network. The use of public networks makes it cost efficient. It has many applications in the sectors like health care, insurance, business etc.

Various components that make up an M2M system are - sensors, RFID (Radio Frequency Identification) , Wi-Fi or cellular network, and a computing software which helps networking devices to interpret data and decision making. These M2M applications can translate data which in turn can trigger automated actions.Various benefits offered by M2M are -

1. It reduces cost by making use of public network and minimizing downtime
2. Increase revenue by identifying new business opportunities
3. Increase customer satisfaction by timely servicing equipment and regularly monitoring.

M2M Applications

Sensor telemetry is one of the first application of M2M communication. It has been used since the last century for transmitting operational data. Earlier people used telephone lines, then radio waves, to transmit measurements factors like- temperature, pressure etc for remote monitoring. Another example of M2M communication is ATM. ATM machine routes information regarding request for transaction to appropriate bank. The bank in turn through its system approves it and allows transactions to complete. It also has applications in supply chain management (SCM), warehouse management systems (WMS), Utility companies, etc. Fig 1 shows various applications of M2M.

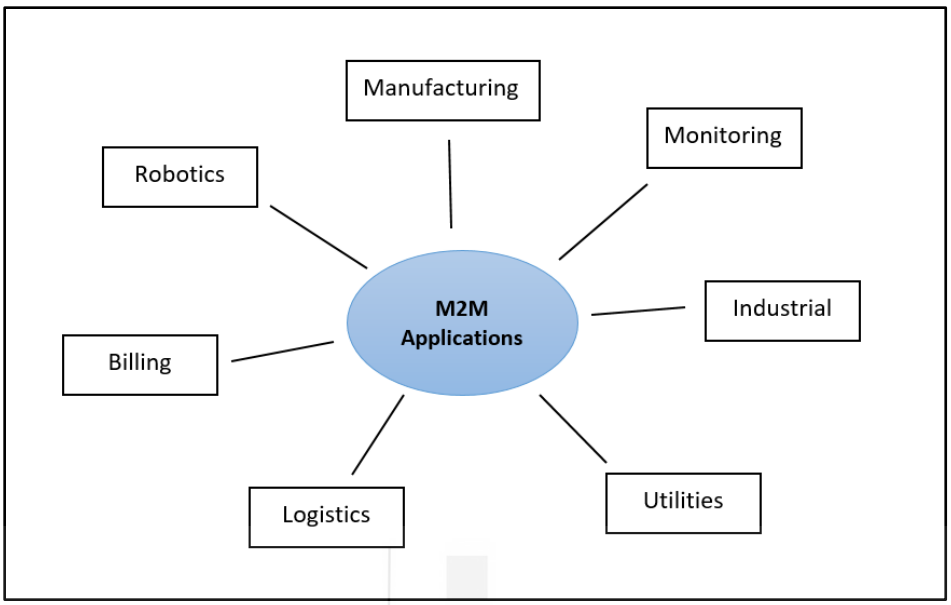

Fig 1. Applications of M2M

Internet of Things (IoT)

Internet of Things or IoT, is a technology that has evolved from M2M by increasing the capabilities at both consumers and enterprise level. It expands the concept of M2M by creating large networks of devices in which devices communicate with one another through cloud networking platforms. It allows users to create high performance, fast and flexible networks that can connect a variety of devices. Table 1 summarizes the differences between M2M and IoT devices.

IoT is a network of physical objects , called “Things” , embedded with hardware like - sensors or actuators or software, for exchanging data with other devices over the internet. With the help of this technology, it is possible to connect any kind of device like simple household objects example- kitchen appliances, baby monitors, ACs, TVs, etc to other objects like- cars, traffic lights, web camera, etc. Connecting these objects to the internet through embedded devices, allows seamless communication between things, processes or people. Some of the applications of IoT devices are – smart home voice assistant Alexa, smart traffic light system.

IoT devices when connected to cloud platforms, can provide a huge and wide variety of industrial or business applications. As the number of IoT devices are increasing, the problem of storing, accessing and processing is also emerging. IoT when used with Cloud technology provides solutions to these problems due to huge infrastructure provided by cloud providers.

Table 1. Difference between M2M and IoT devices

M2M – Machine 2 Machine	IoT – Internet of Things
Point to point connection establishment	Devices are connected through the network and also supports connecting to global cloud networks.
Limited amount of intelligence	Decision making is enabled
Makes use of internet protocols like- HTTP, FTP, etc.	Makes use of traditional communication protocols
Generally may not rely on internet connection	Generally Rely on internet connection
Less scalable	Highly scalable

9.4COMPONENTS OF IoT IMPLEMENTATION

IoT systems can be implemented by four components.

1. Sensors
   Sensors are devices that are capable of collecting data from the environment. There are various types of sensors available –temperature sensors, pressure sensors, RFID tags, light intensity detectors, electromagnetic sensors, etc.

2. Network
   Data collected from sensors are passed over the network for computations to the cloud or processing nodes. Depending upon the scale, they may be connected over LAN, MAN or WAN. They can also be connected through wireless networks like- Bluetooth, ZigBee, Wi-Fi, etc.

3. Analytics
   The process of generating useful insights from the data collected by sensors is called analytics. Analytics when performed in real time, can have numerous applications and can make the IoT system efficient.

4. Action

Information obtained after analytics must be either passed to the user using some user interface, messages, alerts, etc; or may also trigger some actions with the help of actuators. Actuators are the devices that perform some action depending on the command given to them over the network.

Fig 2 shows implementation of IoT. Data captured by sensors are passed on to the cloud servers over the internet via gateways. Cloud servers in turn perform analytics and pass on the decisions or commands to actuators.

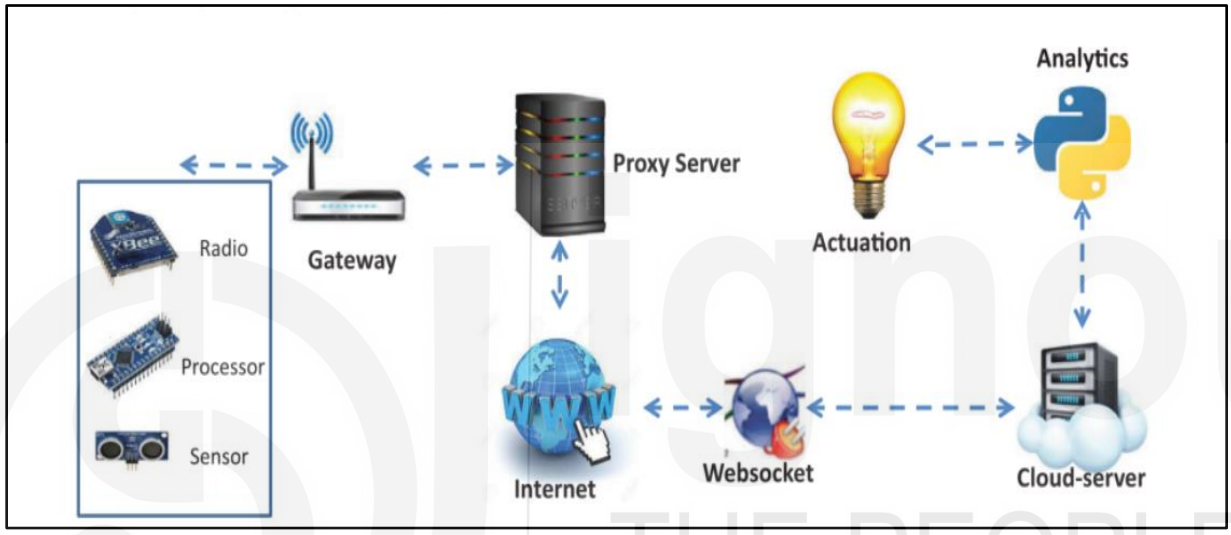

Fig 2:IoT implementation
(Source: Reference 1)

Check your Progress 1

1. What is IoT technology?
2. State differences between M2M and IoT technology.
3. What are the various components involved in implementation of IoT?

9.5 GATEWAY PREFIX ALLOTMENT

Gateways are networking devices that connect IoT devices like sensors or controllers to Cloud. In other ways we can say that data generated by IoT devices are transferred to Cloud servers through IoT gateways.

The number of IoT devices is increasing at an exponential rate. These IoT devices are connected in a LAN or a WAN. A number of IoT devices within a building, communicating to a gateway installed in the same building over a wi-fi connection can be called an IoT LAN. Geographically distributed LAN segments are interconnected and connected to the internet via gateways to form IoT WAN. Devices connected within LAN have unique IP addresses but may have addresses the same as devices of another LAN .

Gateways connect IoT LANs and WANs together. It is responsible for forwarding packets between them on the IP layer. Since a large number of devices are connected, address space needs to be conserved. Each connected device needs a unique address. IP addresses allocated to devices within a gateway's jurisdiction are valid only in its domain. Same addresses may be allocated in another gateway's domain. Hence to maintain uniqueness, each gateway is assigned a unique network prefix. It is used for global identification of gateways. This unique identifier removes the need of allocating a unique IP address to each and every device connected to the network, hence saves a lot of address space.

Gateway prefix allotment is shown in fig 3. Here two gateway domains are shown. Both of them are connected to the internet via router. This router has its own address space and allows connectivity to the internet. This router assigns a unique gateway prefix to both the gateways. Hence packets are forwarded from gateways to the internet via routers.

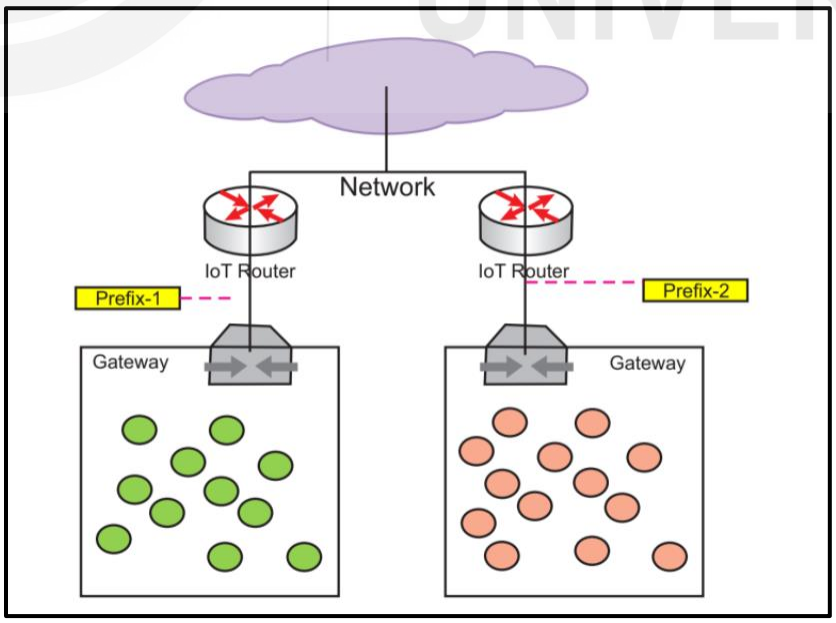

Fig 3: Gateway prefix allotment
(Source: Reference 1)

9.6 IMPACT OF MOBILITY ON ADDRESSING

When an IoT device moves from one location to another in a network, its address is affected. Network prefix allocated to gateways change due to mobility. WAN addresses allocated to devices through gateways changes without affecting IoT LAN addresses. This is possible because addresses allocated within a domain of gateway are unique. It is not affected by mobility of devices. These unique local addresses (ULA) are maintained independent of global addresses. For giving internet access to these ULAs, they are connected to application layer proxy which routes them globally.

Gateways are attached to a remote anchor point by using protocols like IPv6. These remote anchor points are immune to changes of network prefix. It is also possible for the nodes in a network to establish direct connection with remote anchor points to access the internet directly using tunneling. Fig 4 shows remote anchor points having access to gateways.

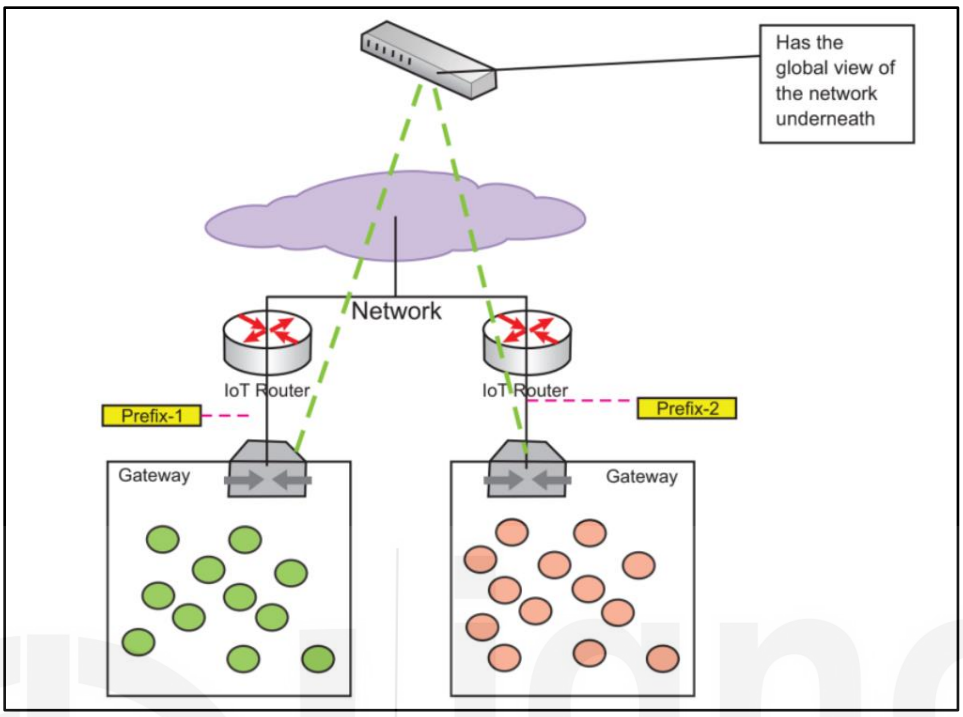

Fig 4: Remote anchor point
(Source: Reference 1)

9.7 MULTIHOMING

The practice of connecting a host to more than one network is called Multihoming. This can increase reliability and performance. Various ways to performmultihoming are –

1. Host multihoming
   In this type of multihoming, a single host can be connected to two or more networks. For example a computer connected to both a local network and awi-fi network.

2. Classical multihoming
   In this type of multihoming, a single network is connected to multiple providers. Edge router communicates with providers using dynamic routing protocols. This protocol can recognize failures and reconfigure routing tables without hosts being aware of it. It requires address space recognized by all providers, hence it is costly.

9.8 IoT IDENTIFICATION AND DATA PROTOCOLS

IoT devices are diverse in their architecture and its use cases can scale from single device deployment to massive cross-platform deployment. There are various types of communication protocols that allow communication between these devices. Some of the protocols are given below.

IPv4

Internet Protocol is a network layer protocol version 4 used to provide addresses to hosts in a network. It is a widely used communication protocol for different kinds of networks. It is a connectionless protocol that makes use of packet switching technology. It is used to give a 32 bit address to a host. It is divided into five classes – A, B, C, D, and E. It can provide upto 4.3 billion addresses only which is not sufficient for an IoT device. It allows data to be encrypted but does not limit access to data hosted on the network.

IPV6

As the total number of addresses provided by IPv4 are not sufficient specially for IoT devices, Internet protocol version 6 or IPv6 is introduced. It is an upgraded version of IPv4. It uses 128 bits to address a host hence anticipates future growth and provides relief from shortage of network addresses. It gives better performance than IPv4. It also ensures privacy and data integrity. It is automatically configured and has built-in support for authentication. Some of the differences between IPv4 and IPv6 are shown in table 2.

Table 2. Differences between IPv4 and IPv6

IPv4	IPv6
Its length is 32 bits	Its length is 128 bits
Possible number of addresses are 2^{32}	Possible number of addresses are 2^{128}
It is represented in dotted decimal notation	It is represented in hexadecimal notation
IPsec is optional	IPsec is compulsory
It supports manual or DHCP configuration	It supports auto-configuration

It supports broadcasting	It supports multicasting

MQTT

Message queuing telemetry transport (MQTT) is a widely used light-weight messaging protocol based on subscription. It is used in conjunction with TCP/IP protocol. It is designed for battery powered devices. Its model is based on Subscriber, Publisher and Broker. Publishers are light weight sensors and subscribers are applications which will receive data from publishers. Subscribers need to subscribe to a topic. Messages updated in a topic are distributed by brokers. Publisher collects the data and sends it to the subscriber through a broker. Broker after receiving messages, filtering and making decisions, sends messages to the subscribers. Brokers also ensure security by authorizing subscribers and publishers. Fig 5 shows the working of MQTT.

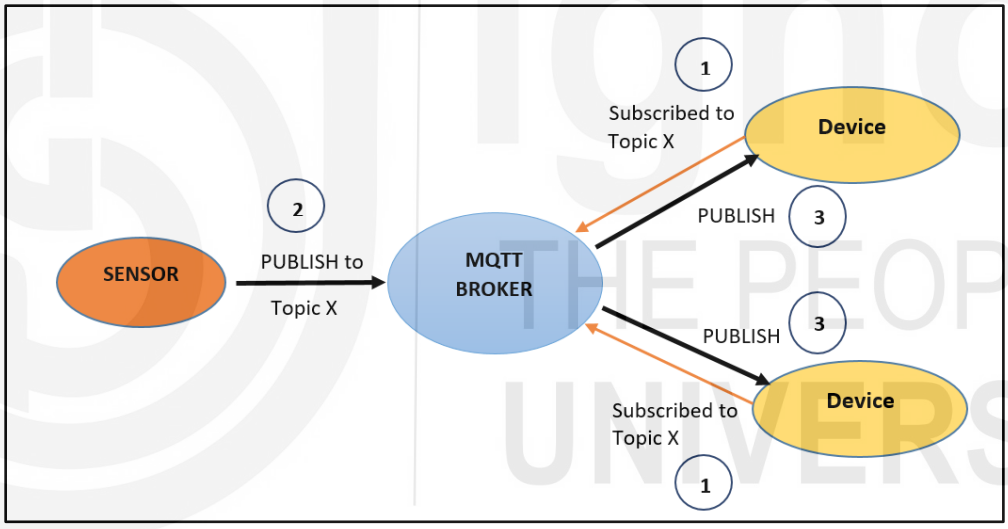

Fig 5: Working of MQTT

CoAP

Constrained Application Protocol (CoAP) is a web transfer protocol used to translate the HTTP model so as to be used with restrictive devices and network environments.It is used for low powered devices. It allows low power sensors to interact with RESTful services. It makes use of UDP for establishing communication between endpoints. It allows data to be transmitted to multiple hosts using low bandwidth.

XMPP

Extensible messaging and presence protocol (XMPP) enables real time exchange of extensible data between network entities. It is a communication protocol based on XML i.e. extensible markup language. It is an open standard hence anyone can implement these services. It also supports M2M communication across a variety of networks. It can be used for instant messaging, multi-party chat, video calls, etc.

AMQP

Advanced message queuing protocol i.e AMQP is an application layer message oriented protocol. It is open standard, efficient, multi-channel, portable and secure. This is fast and also guarantees delivery along with acknowledgement of received messages. It can be used for both point-to-point and publish-subscribe messaging. It is used for messaging in client-server environments. It also supports a multi-client environment and helps servers to handle requests faster.

Need to elaborate more on Protocols?

9.8 CONNECTIVITY TECHNOLOGIES

IoT devices need to be connected in order to work. Various technologies used to establish connections between devices are discussed in this section.

IEEE 802.15.4

It is an IEEE standard protocol used to establish wireless personal area networks (WPAN). It is used for providing low cost, low speed, ubiquitous networks between devices. It is also known as Low-Rate wireless Personal Area Network (LR-WPAN) standard. It makes use of the first two layers (Physical and MAC layers) of the network stack and operates in ISM band. These standards are also used with communication protocols of higher levels like- ZigBee, 6LoWPAN, etc.

6LoWpan

IPV6 over low power wireless personal area network, is a standard for wireless communication. It was the first standard created for IoT. It allows small, limited processing capabilities and low power IoT devices to have direct connectivity with IP based servers on the internet. It also allows IPV6 packets to be transmitted over IEEE 802.15.4 wireless network.

ZigBee

It is a wireless technology based on IEEE 802.15.4 used to address needs of low-power and low-cost IoT devices. It is used to create low cost, low power, low data rate wireless ad-hoc networks. It is resistant to unauthorized reading and communication errors but provides low throughput. It is easy to install, implement and supports a large number of nodes to be connected. It can be used for short range communications only.

NFC

Near Field Communication (NFC) is a protocol used for short distance communication between devices. It is based on RFID technology but has a lower transmission range (of about 10 cm). It is used for identification of documents or objects. It allows contact less transmission of data. It has shorter setup time than Bluetooth and provides better security.

Bluetooth

It is one of the widely used types of wireless PAN used for short range transmission of data. It makes use of short range radio frequency. It provides data rate of appx 2.1 Mbps and operates at 2.45GHz. It is capable of low cost and low power transmission for short distances. Its initial version 1.0 supported upto 732kpbs speed. Its latest version is 5.2 which can work upto 400m range with 2 Mbps data rate.

Z-Wave

It is one of the standards available for wireless networks. It is interoperable and uses low powered radio frequency communication. It is used for connecting to smart devices by consuming low power. These Z-waves devices allow IoT devices to be controlled over the internet. It is generally used for applications like home automation . It supports data rate of upto 100kbps. It also supports encryption and multi-channel.

RFID

Radio frequency identification (RFID) are electronics devices consisting of an antenna and a small chip. This chip is generally capable of carrying data upto 2000 bytes. It is used to give unique identification to an object. Its system is composed of reading device and RFID tags. RFID tags are used to store data and identification information, which is then attached to the object to be tracked. The reader is used to track presence of RFID tag when the object passes through it.

Check your Progress 2

1. What is Gateway prefix ? Why it is needed.
2. State differences between IPv4 and IPv6.
3. Explain any three connectivity technologies.

Need to elaborate more on the above technologies?

9.9 SUMMARY

In this unit M2M and IoTtechnologies are discussed in detail. Machine-to-Machine is a technology that allows connectivity between networking devices. IoT technology expands the concept of M2M by creating large networks of devices in which devices communicate with one another through cloud networking platforms. In order to implement IoT, components involved are – sensors, network, analytics and actions (actuators). Some of the existing IoT identification and data protocols are IPv4, IPv6, MQTT, XMPP, etc. Existing connectivity technologies used for connecting devices are – Bluetooth, Zigbee, 802.15.4, RFID, etc.

References

1. “Internet of Things”, Dr.JeevaJose , 2018, Khanna Book Publishing Co. (P) LTD. ISBN: 978-93-86173-59-1.

Solutions to Check your Progress 1

1. IoT is a network of physical objects , called “Things” , embedded with hardware like - sensors or actuators or software, for exchanging data with other devices over the internet. With the help of this technology, it is possible to connect any kind of device like simple household objects example- kitchen appliances, baby monitors, ACs, TVs, etc.

2. The various differences between IoT and M2M are –

M2M	IoT
Machine 2 Machine	Internet of Things
Point to point connection establishment	Devices are connected through the network and also supports connecting to global cloud networks.
Limited amount of intelligence	Decision making is enabled
Makes use of internet protocols like- HTTP, FTP, etc.	Makes use of traditional communication protocols
Generally may not rely on internet connection	Generally Rely on internet connection
Less scalable	Highly scalable

3. The components involved in the implementation of IoT are –
   a) Sensors - devices that are capable of collecting data from the environment. There are various types of sensors available –temperature sensors, pressure sensors, RFID tags, light intensity detectors, electromagnetic sensors, etc.
   b) Network - Data collected from sensors are passed over the network for computations to the cloud or processing nodes.
   c) Analytics - The process of generating useful insights from the data collected by sensors is called analytics.

a) Action - Information obtained after analytics must be either passed to the user using some user interface, messages, alerts, etc; or may also trigger some actions with the help of actuators.

Solutions to Check your Progress 2

1. Gateways connect IoT LANs and WANs together. It is responsible for forwarding packets between them on the IP layer. Since a large number of devices are connected, address space needs to be conserved. Each connected device needs a unique address. IP addresses allocated to devices within a gateway's jurisdiction are valid only in its domain. Same addresses may be allocated in another gateway's domain. Hence to maintain uniqueness, each gateway is assigned a unique network prefix. It is used for global identification of gateways.

2. Both IPv4 and IPv6 are network layer protocols. Some of the differences are –

IPv4	IPv6
Its length is 32 bits	Its length is 128 bits
Possible number of addresses are 2^{32}	Possible number of addresses are 2^{128}
It is represented in dotted decimal notation	It is represented in hexadecimal notation
IPsec is optional	IPsec is compulsory
It supports manual or DHCP configuration	It supports auto-configuration

3. V
arious connectivity technologies are –

   a) IEEE 802.15.4 - It is an IEEE standard protocol used to establish wireless personal area networks (WPAN). It is used for providing low cost, low speed, ubiquitous networks between devices.
   b) 6LoWpan - IPV6 over low power wireless personal area network, is a standard for wireless communication. It was the first standard created for IoT. It allows small,

limited processing capabilities and low power IoT devices to have direct connectivity with IP based servers on the internet.

c) RFID - Radio frequency identification (RFID) are electronics devices consisting of an antenna and a small chip. This chip is generally capable of carrying data upto 2000 bytes. It is used to give unique identification to an object.