Module 2

PROTOCOLS IN IOT INFRASTRUCTURE

Messaging protocols

Messaging protocols are used to sent data/message to and from the cloud for IoT application.

1. MQTT
2. AMQP
3. DDS
4. XMPP
5. CoAP

1.MQTT

- Message queuing telemetry transport protocol
- Light weight publish/subscribe messaging transport protocol for transporting message between iot devices.
- This protocol typically runs over TCP/IP
  It can operate on top of other networking protocol.so they provide ordered ,loseless,bidirectional connection
- There is a third component called a message brocker,handles the communication between publisher & subscriber

Components

MQTT CLIENT:-

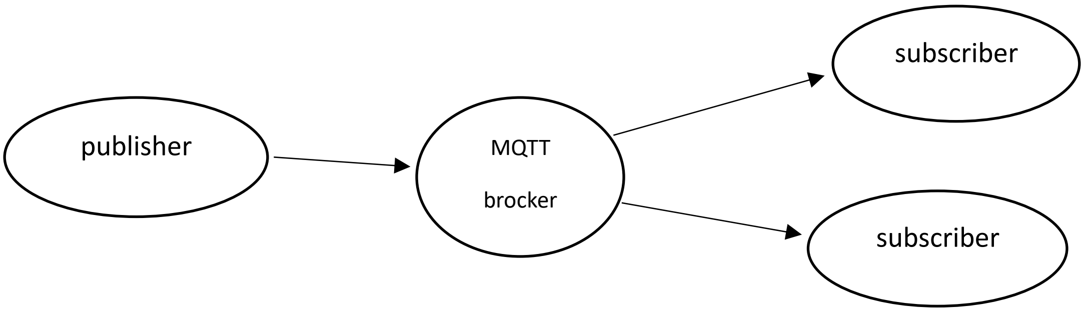
- if the client sending message,it act as a publisher,if it receiving message it act as a receiver
- Basically any device that communicatr using MQTT over a n/w can be called an MQTT client

MQTT BROCKER:-

- it is the backend system which coordinates message between the different clients.
- It also receiving & filtering messages,identifying clients subscribed to each message & sending the msg
- Authorizing & authenticating MQTT clients,handles missed msg.

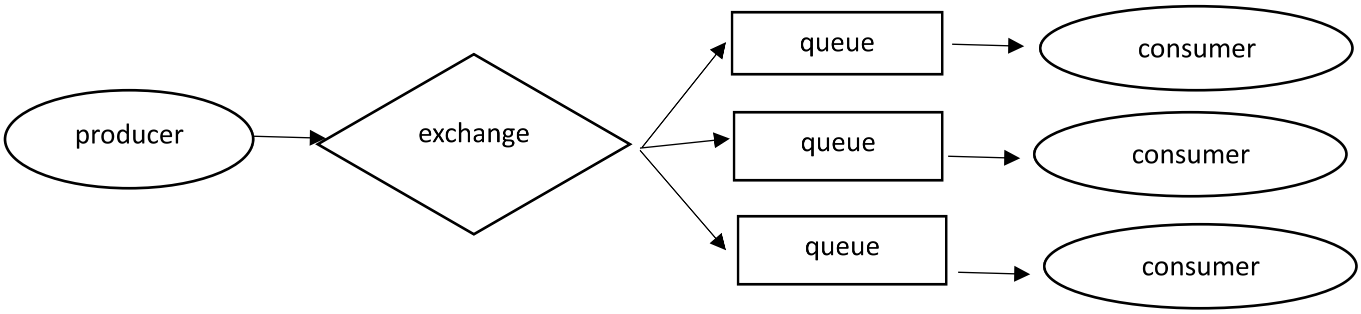
MQTT CONNECTION:-

- Clients and brockers begin communicating by using an MQTT connection
- Client initiate the connection by sending a CONNECT msg to the MQTT brocker.
- The brocker confirms that a connection has been established by responding with CONNACK msg.



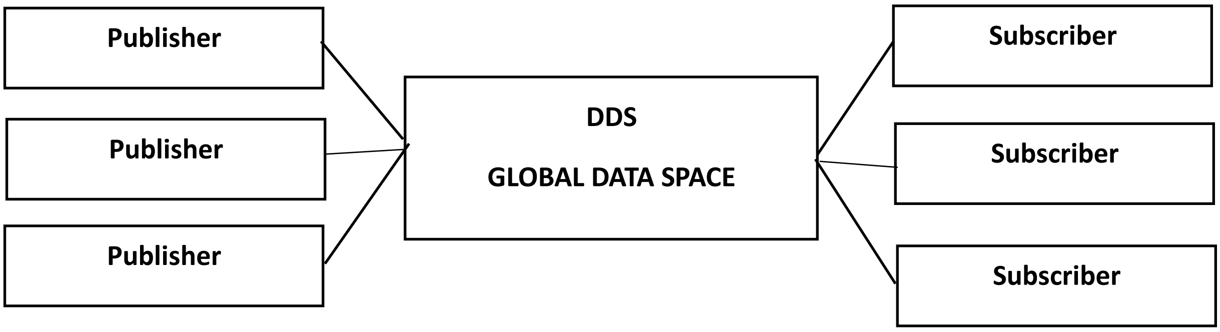
2.AMQP

- Advanced message queuing protocol
- Open protocol used asynchronous message queuing
- The publisher create the message and the consumer take them up and process them
- Publisher send message to a exchange and consumer get message from queue or the queue pushes the to the consumer
- It is similar to HTTP
- It is based on Client – Server architecture
- It is a one-to-one communication protocol
- It uses GET/PUT/DELETE methods.
- Layers of CoAP Application Request –
- Response Messages UDP
- CoAP is a two layer protocol
- The lower layer is the message layer
- The upper layer is called Request – Response layer



- CoAP supports four types of messages:
 1. **Confirmable (CON)** – In this type, an acknowledgment should be send after receiving the message. When there is a timeout, a reset (RST) message will be sent.
 2. **Non-Confirmable(NON)-** In this type an ID will be send as part of the message. No acknowledgement is send by the receiver.
 3. **Acknowledgement (ACK)** – Used to send acknowledgment
 4. **Reset (RST)** – Used to initiate reset when time out occur.

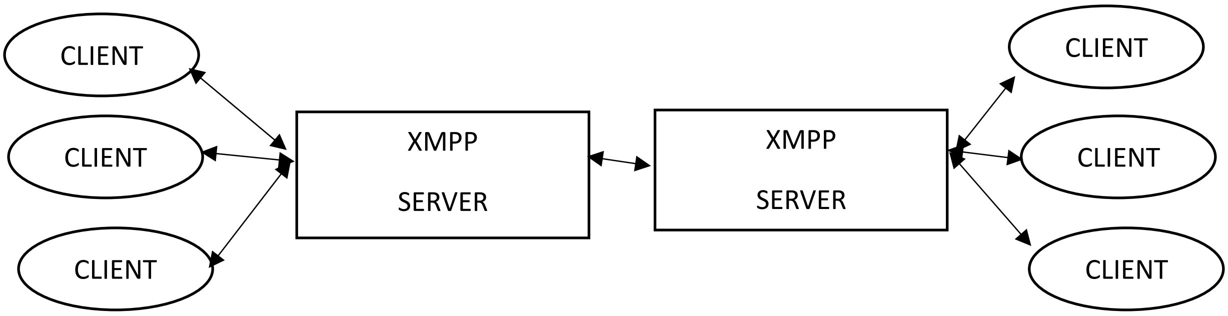
3.DDS



- It uses brockerless architecture.
- It is used for M2M(Machine to Machine)communication
- It enables data exchange via publish-subscribe methodology
- It uses multicasting to bring high quality of service to application

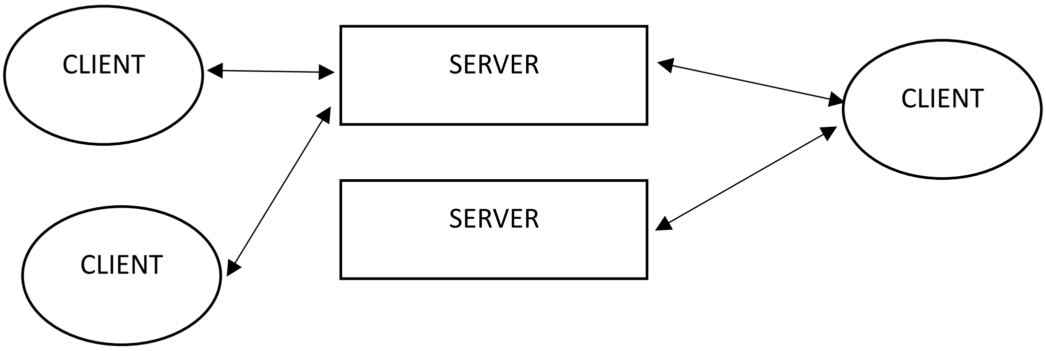
- Direct connection of devices
- The publisher and subscribers can join or leave the GDS at any point in time
- Subscriptions are matched by taking into account the topics with details like name,datatype etc
- All the subscriptions are dynamically matched and the data flows from publisher to subscriber.

4.XMPP



- Extensible messaging presence protocol.
- X-Extensible.XMPP is a open source project which can be changed or extended according to the need.
- It is commonly used for instant message purpose like video call,voice call chat.
- M-XMPP designed for sending messages in real time.it has very efficient push mechanism compared to other
- P-it determine whether you are online/offline it indicates the state
- P-a set of standard that allow system to communicate with each other.

5.CoAP



- Constrained application protocol
- It is a specialized web transfer protocol for use with constained node and network.
- It is used for machine to machine application
- It is basically a client-server IOT protocol where the client makes a request and server sends back a response

COAP	MQTT
• Constrained application protocol • For communication it uses a request-response prototype • It uses Asynchronous and Synchronous messaging • It uses Datagram protocol(UDP) • Header size 4 byte • It will give label to the message • It has a secured system	• Message query telemetry transport • For communication it uses Publish-subscriber prototype • It uses only asynchronous message • It uses TCP • Header size 2 byte • It does not have • Very secure

TRANSPORT PROTOCOLS

Two important transport protocol for IoT infrastructure are,

1. BLE (Bluetooth Low Energy)

2. Li-Fi (Light Fidelity)

BLE (Bluetooth Low Energy)

➢ It is a wireless protocol for connecting devices

➢ It is low power

➢ It is low cost

➢ Used for connecting IoT devices

➢ It uses 2.4GHz ISM band

➢ It is introduced in the Bluetooth 4.0 version.

➢ It is implemented in most of the smartphones.

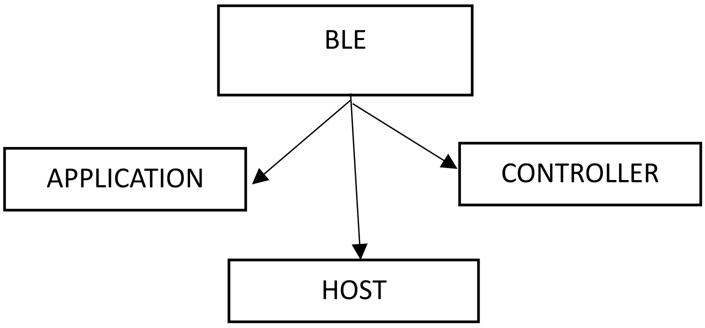
➢ It is supported by most of the Operating Systems.

Architecture of BLE BLE has 3 components:

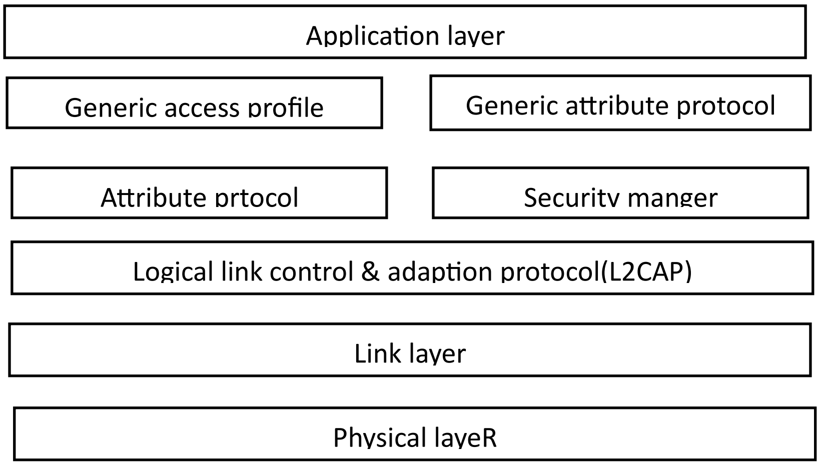
1. Application - It represent all applications

2. Host - It is responsible for connection establishment

3. Controller – It takes care of data transmission and control



BLE Protocol Stack



Application layer

Generic access profile

Generic attribute protocol

Attribute prtocol

Security manger

Logical link control & adaption protocol(L2CAP)

Link layer

Physical layeR

Controller : Controller has two layers:

1. Link layer
2. Physical layer

Link Layer:

- It defines packet structure and control.

Physical Layer:

- It handles data transmission.
- Modulation and demodulation.
- Analog to digital and digital to analog conversion

Host :

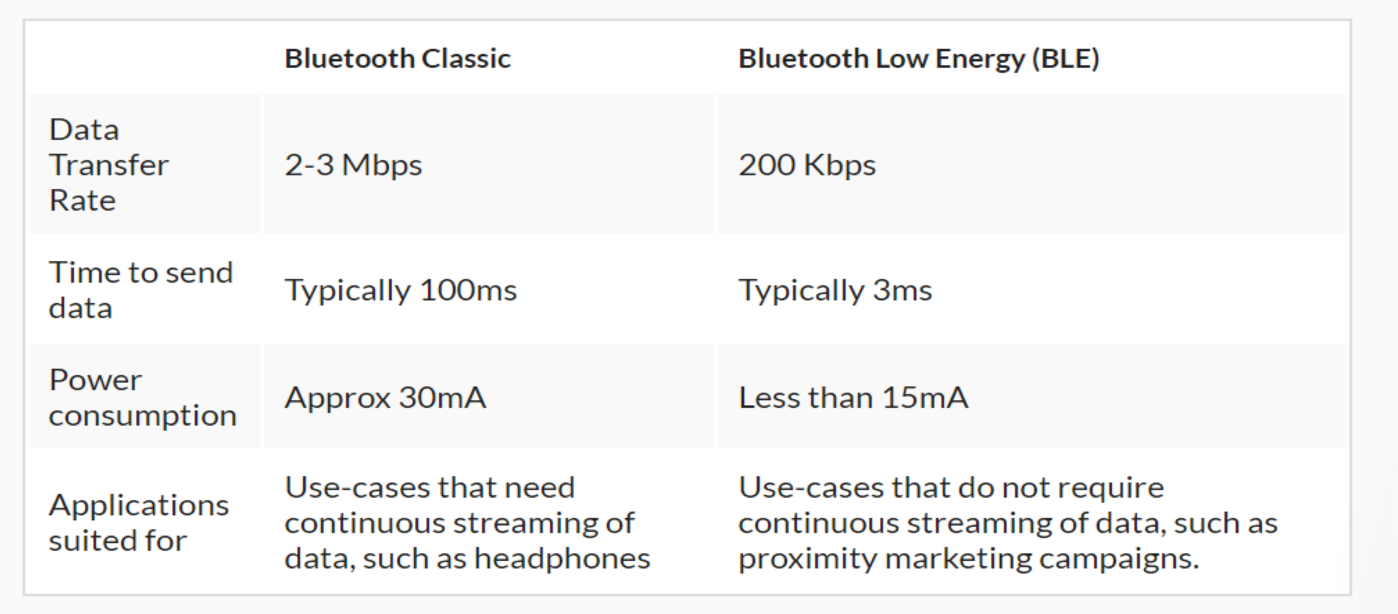
Host contains 5 layers:

1. Generic Access Profile (GAP)
    - It handles device discovery, connection establishment and management.
2. Generic Attribute Profile (GATT)
    - It defines the guidelines for data read/write .
3. Attribute Protocol (ATT)
    - It defines the protocol for accessing data.
4. Logical Link Control and Adaptation Protocol (L2CAP)
    - It is responsible for fragmentation and reassembly of data. o It also do multiplexing and demultiplexing of channels.
5. Security Manager (SM)
    - It manages pairing, authentication and encryption

Application : - Application layer is responsible for User interface (UI) and Application logic

BLE Device connection

- The peripheral device broadcast advertising data.
- The central device scan for advertising data.
- If any advertising message is found, central devise send scan request.
- On receiving the scan request, the peripheral device send response.
- Now connection is established and data can be send between central and peripheral devices.



	Bluetooth Classic	Bluetooth Low Energy (BLE)
Data Transfer Rate	2-3 Mbps	200 Kbps
Time to send data	Typically 100ms	Typically 3ms
Power consumption	Approx 30mA	Less than 15mA
Applications suited for	Use-cases that need continuous streaming of data, such as headphones	Use-cases that do not require continuous streaming of data, such as proximity marketing campaigns.

connection topology in BLE

Star Network

Star topology is the easiest topology in the three kinds of network structures. It consists of one central node and several peripheral nodes

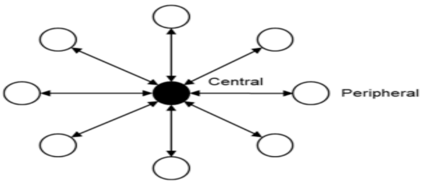


Figure 1. Star Network

Mesh topology

In mesh networks, each device is connected to one or more of the other devices. There is no clear role definition that parallels central/peripheral

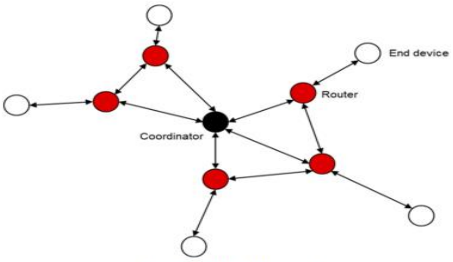


Figure 2. Mesh Network

Tree Structure Network

Compared to mesh routing rules, the tree structure network routing rules are much simpler. This means the hardware and software requirements are lower than for a mesh network. This makes the tree structure network easier to achieve. Compared to the star network, the tree structure network can connect more nodes.

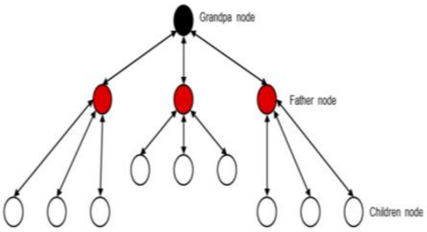
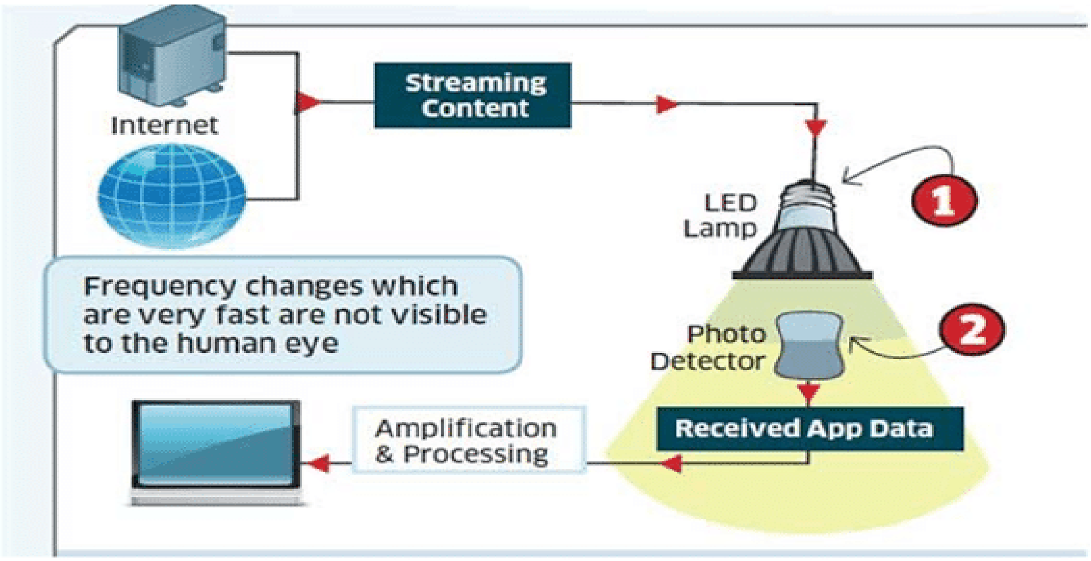


Figure 3. Tree Structure Network

Li-Fi Technology

- Li-Fi means Light Fidelity
- Li-Fi is the transmission of data through light.
- Light source like LED bulb is used as transmitter.
- Change in the intensity of light is considered as binary zero and one.
- Changing the brightness occur very fast and human eye can not able to detect it


Internet
Streaming Content
LED Lamp
1
Frequency changes which are very fast are not visible to the human eye
Photo Detector
2
Received App Data
Amplification & Processing

Li-Fi Working Transmitter:

• The streaming data is given to the LED lamp driver.

• The lamp driver changes the intensity of the lamp according to the binary value of the data.

• This happens very fast and human eyes can not really feel or see this.

Li-Fi Working Receiver:

• The receiver contains a photo diode which detects the change in intensity of the light and generate electric current.
• After amplification and processing, the data is forwarded to the receiver.

Li-Fi Advantages

• Hight data transfer rate – 224Gbps

• Hight security

• Low power consumption

• Less harmful to humans

• High efficiency Li-Fi Disadvantages

• Light can't pass through objects.

• Short range

• Interference from sunlight or external bulbs.

• Always requires light as medium.

• Challenges of how the receiving device will transmit back to transmitter

Disadvantages of Li-Fi

- Speed and range affected by the intensity of light
- High initial setup cost
- Presence of light is essential
- Not penetrate through wall

IPv4 – Internet Protocol - Version 4

- An IP address is a unique identification for a node connected to a network.

- Networks using TCP/IP uses this address to route messages.

- IP address has two versions – IPv4 and IPv6

- IPv4 address is 4 bytes or 32 bit long.

- It can be represented as binary or dotted decimal notation format.

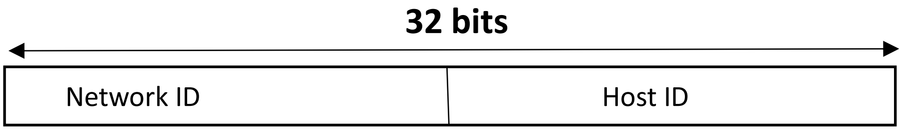
- Example: 172.16.0. **1**

IP Address Classes

- An IP address has two sections:

1. Net Id – Used to identify network.

2. Host Id – Used to identify host.



IP Address Classes

- IP address are classified into 5 classes:

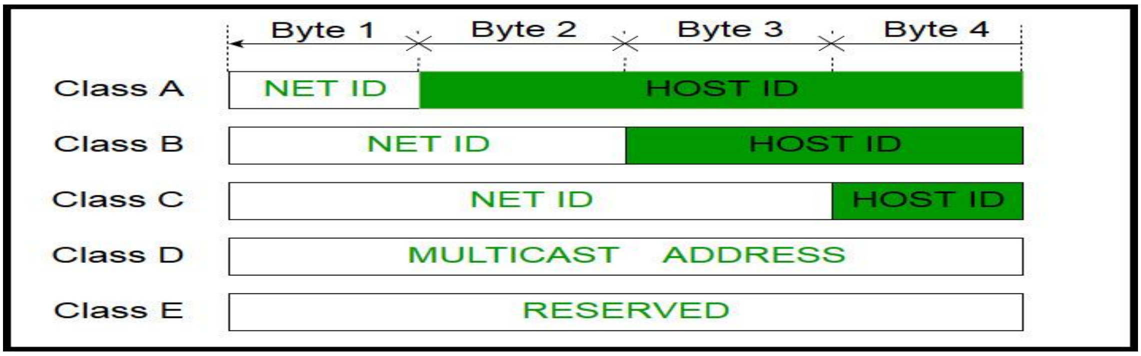
1. Class A

2. Class B

3. Class C

4. Class D

5. Class E



1.Class A (1.0.0.0 to 126.0.0.0):

- The first bit in a Class A address is always "0."

- These addresses were used for large networks, such as universities and major corporations.

- Class A addresses provide a very large number of host addresses (approximately 16 million) in each network.

2. Class B (128.0.0.0 to 191.255.0.0):

- The first two bits in a Class B address are "10."

- Class B addresses were typically used by medium-sized organizations and businesses.

- Each Class B network can have around 65,000 host addresses.

3.Class C (192.0.0.0 to 223.255.255.0):

- The first three bits in a Class C address are "110."
- Class C addresses were designed for smaller networks, such as small businesses.
- Each Class C network can support approximately 254 host addresses.

4. Class D (224.0.0.0 to 239.255.255.255):

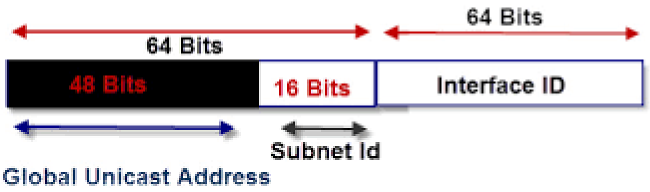
- Class D addresses are reserved for multicast groups, which allow for one-to-many or many-to-many communication.
- These addresses are not assigned to individual hosts or networks.

6. **Class E (224.0.0.0 to 239.255.255.255):**

- Class E addresses are reserved for experimental purposes and should not be used in regular networks.

IPv6– Internet Protocol - Version 6

- IPv6, is a network layer protocol used for communication over the Internet.
- It is the successor to IPv4. • It was developed to overcome the address limitations of IPv4.



IPv6 Address Structure

Features of IPv6

1. Expanded address space: IPv6 uses 128-bit addresses, which provides a larger address space.

2. Address Format: IPv6 addresses are represented as eight groups of four hexadecimal digits separated by colons (2001: 0db8 : 85a3 : 0000 : 0000 : 8a2e : 0370 : 7334)

3. Simplified Header: The IPv6 header is simpler and more efficient than the IPv4 header.

4. Autoconfiguration: IPv6 includes features for automatic address assignment and network configuration.

5. Improved Security: IPv6 includes built-in support for IPsec (Internet Protocol Security).

6. Multicasting: IPv6 has built-in support for multicast communication

IPV4	IPV6
• 32 bit length •	• 128 bit •
• It support manual & DHCP address configuration •	• It support auto & renumbering address configuration •
• Address format is dotted decimal notation	• Address format is hexadecimal notation
• Both routers & the sending host fragment packets	• Routers do not support packet fragmentation.sending host fragments packets
• Header include checksum	• Header does not include a checksum
• Header include options	• Optional data is supported as extension header
• Checksum field is available in IPV4 header	• No checksum field in ipv6 header

3.**URI and URL**

URI	URL
URI is an acronym for a Uniform Resource Identifier.	URL is an acronym for a Uniform Resource Locator.
URI identifies a resource and differentiates it from others by using a name, location, or both.	URL identifies the web address or location of a unique resource.
URI contains components like a scheme, authority, path, and query.	URL has similar components to a URI, but its authority consists of a domain name and port.
URI is usually used in XML, tag library files, and other files, such as JSTL and XSTL.	URL is mainly for searching web pages on the internet.
URI scheme can be a protocol, a specification, or a designation like HTTP, file, or data.	URL scheme is a protocol, such as HTTP and HTTPS.