1. **Explain the IoT Components?**

1) Sensors/Devices

2) Connectivity

3) Data Processing

4)User Interface

**1) Sensors/Devices**

• Sensors or devices are a key component that helps you to collect live data from the surrounding environment.

• All this data may have various levels of complexities.

• It could be a simple temperature monitoring sensor, or it may be in the form of the video feed.

**2) Connectivity**

• All the collected data is sent to a cloud infrastructure.

• The sensors should be connected to the cloud using various mediums of communications.

• These communication mediums include mobile or satellite networks, Bluetooth, WI-FI, WAN, etc.

**3) Data Processing**

• Once that data is collected, and it gets to the cloud, the software performs processing on the gathered data.

• This process can be just checking the temperature, reading on devices like AC or heaters.

• However, it can sometimes also be very complex like identifying objects, using computer vision on video.

**4)User Interface**

• The information needs to be available to the end-user in some way which can be achieved by triggering alarms on their phones or sending them notification through email or text message.

o The user sometimes might need an interface which actively checks their IoT system.

• For example, the user has a camera installed in his home. He wants to access video recording and all the feeds with the help of a web server.

**2.What is IOT and Explain the Characteristics of IoT ?**

The Internet of Things (IoT) is a system of interrelated computing devices, mechanical and digital machines, objects, animals or people that are provided with unique identifiers and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

**Characteristics of IoT:**

**Connectivity**

Connectivity entitles the internet of things by bringing together everyday objects. With everything in IoT devices and hardware, with sensors and other electronics and connected hardware and control systems there need to be a connection between various levels. It provides hardware accessibility and compatibility in the things with this connectivity, and new market opportunities for the intent of things can be created by the networking of smart appliances.

**Intelligence**

The Intelligence in IoT is only concerned with the interaction between devices, while user and device interaction is achieved by standard input methods and graphical user interfaces.

**Dynamic Nature**

The most important part of IoT is gathering data from its environment, which is achieved with the dynamic changes that take place around the devices. In addition to the context of devices including temperature, location, and speed and the number of devices also changes dynamically with a person, place, and time.

**Security**

IoT devices are vulnerable to security threats. There is a high level of transparency and privacy issues with IoT. For creating a security paradigm, it is important to secure the endpoints, networks, and data that are transferred across all of them.

**Sensing**

The sensing information is the analog input from the physical world, but it can provide a rich understanding of the complex world.

**Heterogeneity**

IoT architecture must support direct network connectivity between heterogeneous networks. The requirement of heterogeneous networks in IoT is scalabilities, modularity, extensibility, and interoperability.

**Enormous Scale**

the enormous scale of IoT in the estimated report where it expressed that 5.5 million new things will get connected every day and 6.4 billion connected devices will be in use worldwide in 2016, which is up by 30% from 2015. The report also forecast that the number of connected devices will reach 20.8 billion by 2020

**3.Explain the IoT Applications & Domains?**

• Smart Thermostats

• Connected Cars

• Activity Trackers

• Parking Sensors

• Connect Health

• Smart City

**4.Explain the difference between IoT and M2M?**

* **Communication Protocols**
* M2M and IoT can differ in how the communication between the machines or devices happens.
* M2M uses either proprietary or non-IP based communication protocols for communication within the M2M area networks.
* **Machines in M2M vs Things in IoT**
  + The "Things" in IoT refers to physical objects that have unique identifiers and can sense and communicate with their external environment (and user applications) or their internal physical states.
  + M2M systems, in contrast to IoT, typically have homogeneous machine types within an M2M area network.
* **Hardware vs Software Emphasis**
  + While the emphasis of M2M is more on hardware with embedded modules, the emphasis of IoT is more on software.
* **Data Collection & Analysis**
  + M2M data is collected in point solutions and often in on-premises storage infrastructure.
  + In contrast to M2M, the data in IoT is collected in the cloud (can be public, private or hybrid cloud).
* **Applications**
  + M2M data is collected in point solutions and can be accessed by on-premises applications such as diagnosis applications, service management applications, and on- premisis enterprise applications.
  + IoT data is collected in the cloud and can be accessed by cloud applications such as analytics applications, enterprise applications, remote diagnosis and management applications, etc.

**5.Write a short note on the Limitation of SNMP.**

**LIMITATIONS** :

* SNMP is stateless in nature and each SNMP request contains all the information required to process the request. The application needs to be intelligent to manage the device.
* SNMP is a connectionless protocol which uses UDP as the transport protocol, making it unreliable as there is no support for acknowledgement of requests.
* MIBs often lack writable objects without which device configuration is not possible using SNMP.
* It is difficult to differentiate between configuration and state data in MIBs.
* Retrieving the current configuration from a device can be difficult with SNMP.
* Earlier versions of SNMP did not have strong security features

**SNMP SECURITY** :

* Lacks authentication. Vulnerable to the variety of security threats.
* Vulnerable to masquerading, modification of information, time modifications, message sequencing and disclosures.
* Message sequence and timing modifications occurs when an entity who is unauthorized reorders, delays, or copies and later replays a message generated by an authorized entity.

**6.What are the IoT Enabling Technologies and Challenges in IoT?**

**IoT(internet of things) enabling technologies:**

* Wireless Sensor Network
* Cloud Computing
* Big Data Analytics
* Communications Protocols
* Embedded System

1. **Wireless Sensor Network(WSN)** : A WSN comprises distributed devices with sensors which are used to monitor the environmental and physical conditions. A wireless sensor network consists of end nodes, routers and coordinators. End nodes have several sensors attached to them where the data is passed to a coordinator with the help of routers. The coordinator also acts as the gateway that connects WSN to the internet.

• Weather monitoring system

• Indoor air quality monitoring system

• Soil moisture monitoring system

• Surveillance system

• Health monitoring system

1. **Cloud Computing** : It provides us the means by which we can access applications as utilities over the internet. Cloud means something which is present in remote locations. With Cloud computing, users can access any resources from anywhere like databases, webservers, storage, any device, and any software over the internet.

**characteristics** –

• Broad network access

• On demand self-services

• Rapid scalability

• Measured service

• Pay-per-use

1. **Big Data Analytics :** It refers to the method of studying massive volumes of data or big data. Collection of data whose volume, velocity or variety is simply too massive and tough to store, control, process and examine the data using traditional databases. Big data is gathered from a variety of sources including social network videos, digital images, sensors and sales transaction records. Several steps involved in analyzing big data

• Data cleaning

• Processing

• Visualization

**Examples** –

• Bank transactions

• Data generated by IoT systems for location and tracking of vehicles

• E-commerce and in Big-Basket

• Health and fitness data generated by IoT system such as a fitness bands

1. **Communications Protocols :** They are the backbone of IoT systems and enable network connectivity and linking to applications. Communication protocols allow devices to exchange data over the network. Multiple protocols often describe different aspects of a single communication. A group of protocols designed to work together is known as a protocol suite; when implemented in software they are a protocol stack.

They are used in

• Data encoding

• Addressing schemes

**5. Embedded Systems :** It is a combination of hardware and software used to perform special tasks. It includes microcontroller and microprocessor memory, networking units (Ethernet Wi-Fi adapters), input output units (display keyword etc. ) and storage devices (flash memory). It collects the data and sends it to the internet. Embedded systems used in **Examples** –

• Digital camera

• DVD player, music player

• Industrial robots

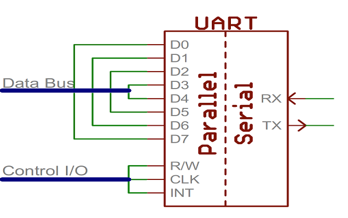
• Wireless Routers etc

**Challenges of Internet of Things (IoT)**

* Insufficient testing and updating
* Concern regarding data security and privacy
* Software complexity
* Data volumes and interpretation
* Integration with AI and automation
* Devices require a constant power supply which is difficult
* Interaction and short-range communication

**7.Explain the UART and SPI?**

Universal Asynchronous Receiver/Transmitter Hardware that translates between parallel and serial forms Commonly used in conjunction with communication standards such as EIA, RS-232, RS-422 or RS-485.



**Protocol**

Each character is sent as

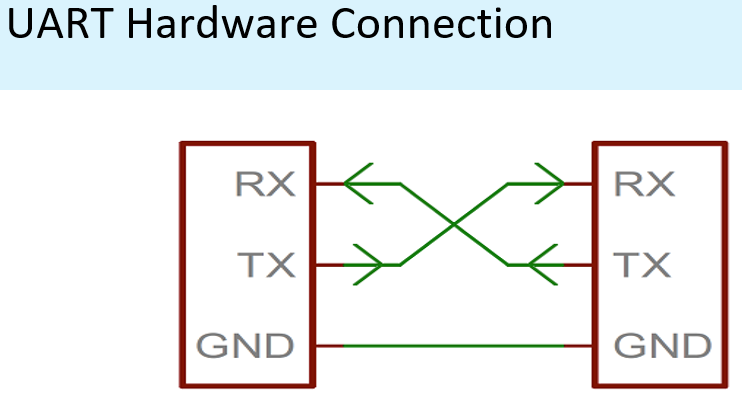
a logic *low* **start** bit

a configurable number of data bits (usually 7 or 8, sometimes 5)

an optional parity bit

*one or more logic high* **stop** bits

with a particular bit timing (“baud”)



**Security Risks for using UART**

Internet of Things (IoT) devices may support UART to send and transmit signals wirelessly. Manufacturers install UART interfaces on IoT boards to review serial console logs and complete any debug activity required. Since UART interacts with IoT devices, it is possible for hackers to infiltrate the UART shell and root shell. Shells manage user interaction with a computing system through an input-output interface. Hence, we have to take UART Security into consideration

If a cybercriminal gains access to the root shell, they can cause detriment to an organization. For example, hackers may:

* Infiltrate and reverse engineer firmware to see how to exploit it further
* Gain access to sensitive information such as certificates or API keys
* Examine communication protocols for vulnerabilities
* Target user devices, including company users and clients

**Serial Peripheral Interconnect (SPI)**

Another kind of serial protocol in embedded systems (proposed by Motorola)

Four-wire protocol

**SCLK — Serial Clock**

**MOSI/SIMO — Master Output, Slave Input**

**MISO/SOMI — Master Input, Slave Output**

**SS — Slave Select**

Single master device and with one or more slave devices

Higher throughput than I2C and can do “stream transfers”

No arbitration required

But

Requires more pins

Has no hardware flow control

No slave acknowledgment (master could be talking to thin air and not even know it)

**What is SPI?**

Serial Bus protocol

Fast, Easy to use, Simple

Everyone supports it

**SPI Basics**

A communication protocol using 4 wires Also known as a 4 wire bus Used to communicate across small distances Multiple Slaves, Single Master Synchronized.

**SPI Capabilities**

Always Full Duplex Communicating in two directions at the same time Transmission need not be meaningful Multiple Mbps transmission speed Transfers data in 4 to 16 bit characters Multiple slaves Daisy-chaining possible.

**SPI Protocol**

Wires:

* Master Out Slave In (MOSI)
* Master In Slave Out (MISO)
* System Clock (SCLK)
* Slave Select 1…N

Master Set Slave Select low

Master Generates Clock

Shift registers shift in and out data

**8.Describe the Simple Network Management Protocol (SNMP)?**

A Protocol that Facilitates the exchange of management information between network devices.

it was developed To **control and monitor status** of network devices.

it beneficial Enables network administrators to: Manage network performance ,Find and solve network problems, Plan for network growth.

**SNMP Basic Components**

SNMP is a well-known and widely used network management protocol that allows monitoring and configuration of network devices such as routers, switches, servers, printers, etc.

Network Management station

Collects and stores management information, and makes this information available to NMS using SNMP Could be a work station or PC

Network Management System (NMS)

Executes applications that monitor and control managed devices

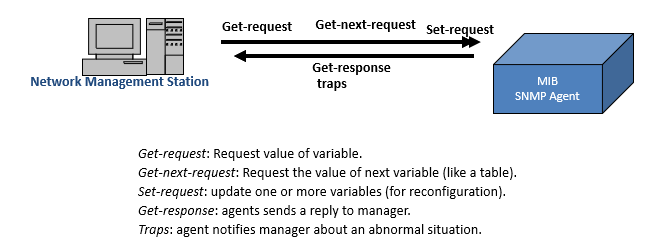
Agent

A network-management software module that resides in a managed device

Management Information Base (MIB)

Used by both the manager and the agent to store and exchange management information.

**How SNMP Works**

****

**9.Describe IoT Levels and Deployment Techniques.**

An IoT system comprises of the following components:

**• Device**: An IoT device allows identification, remote sensing, actuating and remote monitoring capabilities. You learned about various examples of IoT devices in section

**• Resource:** Resources are software components on the IoT device for accessing, processing, and storing sensor information, or controlling actuators connected to the device. Resources also include the software components that enable network access for the device.

**• Controller Service:** Controller service is a native service that runs on the device and interacts with the web services. Controller service sends data from the device to the web service and receives commands from the application (via web services) for controlling the device.

**• Database:** Database can be either local or in the cloud and stores the data generated by the IoT device.

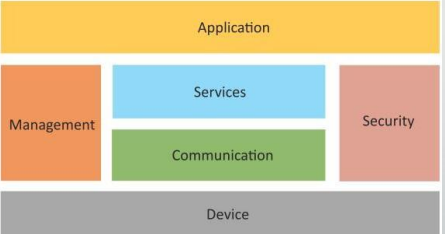
**• Web Service:** Web services serve as a link between the IoT device, application, database and analysis components. Web service can be either implemented using HTTP and REST principles (REST service) or using WebSocket protocol (WebSocket service).

**• Analysis Component**: The Analysis Component is responsible for analyzing the IoT data and generate results in a form which are easy for the user to understand.   
**• Application:** IoT applications provide an interface that the users can use to control and monitor various aspects of the IoT system. Applications also allow users to view the system status and view the processed data.

**10.Explain the Logical Design of IoT**

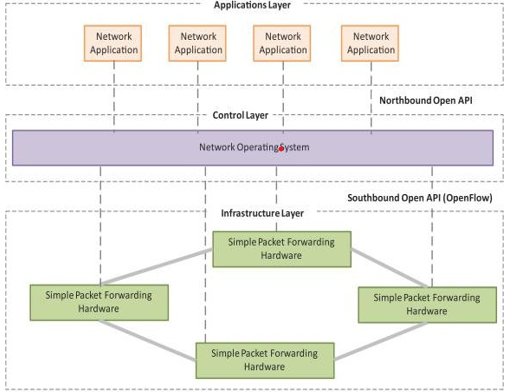
• Logical design of an IoT system refers to an abstract representation of the entities and processes without going into the low-level specifics of the implementation.

• An IoT system comprises of a number of functional blocks that provide the system the capabilities for identification, sensing, actuation, communication, and management

****

**11.Describe Software Defined Networking (SDN) with a diagram.**

* Software-Defined Networking (SDN) is a networking architecture that separates the control plane from the data plane and centralizes the network controller.
* Software-based SDN controllers maintain a unified view of the network and make confi guration, management and provisioning simpler.
* The underlying infrastructure in SDN uses simple packet forwarding hardware as opposed to specialized hardware in conventional networks.

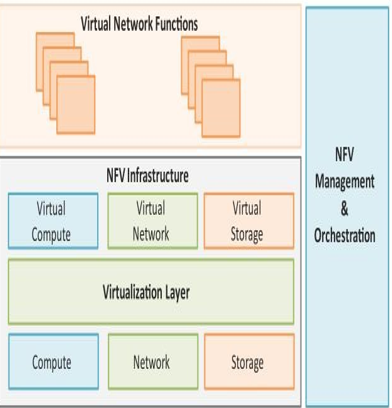


**Key elements of SDN**

* Centralized Network Controller
  + With decoupled control and data planes and centralized network controller, the network administrators can rapidly configure the network.
* Programmable Open APIs
  + SDN architecture supports programmable open APIs for interface between the SDN application and control layers
* Standard Communication Interface (OpenFlow)
  + SDN architecture uses a standard communication interface between the control and infrastructure layers (Southbound interface).
  + OpenFlow, which is defined by the Open Networking Foundation (ONF) is the broadly accepted SDN protocol for the Southbound interface.

**12.Explain the Network Function Virtualization (NFV) with a neat diagram.**

* Network Function Virtualization (NFV) is a technology that leverages virtualization to consolidate the heterogeneous network devices onto industry standard high volume servers, switches and storage.
* NFV is complementary to SDN as NFV can provide the infrastructure on which SDN can run.

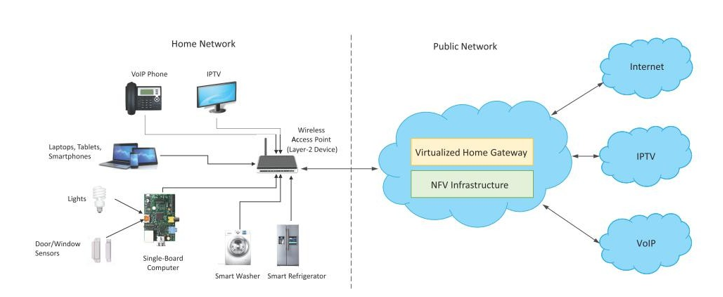


**Key elements of NFV**

* Virtualized Network Function (VNF):
  + VNF is a software implementation of a network function which is capable of running over the NFV Infrastructure (NFVI).
* NFV Infrastructure (NFVI):
  + NFVI includes compute, network and storage resources that are virtualized.
* NFV Management and Orchestration:
  + NFV Management and Orchestration focuses on all virtualization-specific management tasks and covers the orchestration and life-cycle management of physical and/or software resources that support the infrastructure virtualization, and the life-cycle management of VNFs.

**NFV Use Case**

* NFV can be used to virtualize the Home Gateway. The NFV infrastructure in the cloud hosts a virtualized Home Gateway. The virtualized gateway provides private IP addresses to the devices in the home. The virtualized gateway also connects to network services such as VoIP and IPTV.



**13. Explain Simple Network Management Protocol (SNMP)?**

Ans. Simple Network Management Protocol (SNMP) is a protocol that is used to manage and monitor devices on a network. It allows a network administrator to remotely retrieve information about a device, as well as to make configuration changes to the device.

SNMP consists of three main components:

1. Management stations: These are the computers that are used by network administrators to manage and monitor the devices on the network. Management stations run SNMP management software that allows them to communicate with the devices using SNMP.
2. Agents: These are the software programs that run on the devices being managed and monitored. Agents are responsible for collecting information about the device and making it available to the management stations via SNMP.
3. Management information base (MIB): This is a database of information about the device that is made available to the management stations via SNMP. The MIB includes details about the device's hardware and software configuration, as well as information about its current status and performance.

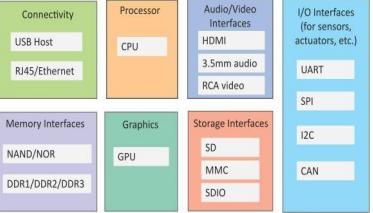
SNMP is a widely used protocol in networking and is supported by a wide range of devices, including routers, switches, servers, and printers. It is a simple and efficient way to manage and monitor devices on a network, and allows network administrators to quickly and easily identify and troubleshoot problems on the network.

**14. Explain the Physical Design of IoT?**

The "Things" in IoT usually refers to IoT devices which have unique identities and can perform remote sensing, actuating and monitoring capabilities.

IoT devices can:

* Exchange data with other connected devices and applications (directly or indirectly), or
* Collect data from other devices and process the data locally or
* Send the data to centralized servers or cloud-based application back-ends for processing the data, or
* Perform some tasks locally and other tasks within the IoT infrastructure, based on temporal and space constraints.



• “Physical” components / capabilities – Sensors / Actuators – Compute, store, communicate data

• An IoT device may consist of several interfaces for connections to other devices, both wired and wireless.

• I/O interfaces for sensors

• Interfaces for Internet connectivity

• Memory and storage interfaces

• Audio/video interfaces.