| **Basis of** | **COAP** | **MQTT** |
| --- | --- | --- |
| **Abbreviation** | Constrained Application Protocol | Message Queuing Telemetry Transport |
| **Communication Type** | It uses Request-Response model. | It uses Publish-Subscribe model |
| **Messaging Mode** | This uses both Asynchronous and Synchronous. | This uses only Asynchronous |
| **Transport layer protocol** | This mainly uses[User Datagram protocol(UDP)](https://www.geeksforgeeks.org/user-datagram-protocol-udp/) | This mainly uses [Transmission Control protocol(TCP)](https://www.geeksforgeeks.org/tcp-ip-model/) |
| **Header size** | It has 4 bytes sized header | It has 2 bytes sized header |
| **RESTful based** | Yes, it uses REST principles | No, it does not uses REST principles |
| **Persistence support** | It does not has such support | It supports and best used for live data communication |
| **Message Labelling** | It provides by adding labels to the messages. | It has no such feature. |
| **Usability/Security** | It is used in Utility area networks and has secured mechanism. | It is used in IoT applications and is secure |
| **Effectiveness** | Effectiveness in LNN is excellent. | Effectiveness in LNN is low. |
| **Communication Model** | Communication model is one-one. | Communication model is many-many. |

**Application layer protocols**

* Application layer protocols in IoT must address some major challenges in IoT's network communications. The data in IoT are more complex than in conventional networking.
* In a simple scenario, a sensor reports a temperature to a local network, which then passes the data to a cloud through the internet.
* Complex scenarios can get as tricky as dialog between multiple machines on a factory floor that selectively power down when environmental sensors report the detection of fire, while a cloud AI system monitors the shutdown and reports the event to multiple external systems.
* The simple scenario includes a single data type and a single message moving in one direction.
* The complex one includes many data types in many messages among many devices that must efficiently exchange the data.
* The hardware itself can vary wildly.

**IMP**

**Write a short note on 6TiSCH add-on:**

* Wireless Sensor Networks (WSNs) have gained interest with the introduction of application areas such as industrial internet, m-Health, and Smart Grid.



* WSNs consist of sensors with wireless capability operating autonomously and reporting data to a central unit.



* To enable low power, high reliability, and deterministic WSNs, 6TiSCH protocol has been proposed which uses Time Slotted Channel Hopping (TSCH) MAC with IPv6 addressing



* Low-power devices utilize TSCH to communicate over a wireless link.



* It is designed for low-power and lossy networks (LLNs) with the main purpose of providing a reliable media access control layer.



* TSCH can be viewed as a combination of Time division multiple access and Frequency-division multiple access mechanisms as it uses diversity in time and frequency to provide reliability to the upper network layers.



**.4 Write a short note on NB- IoT:**

1. Narrowband IoT or NB-IoT is a wireless communication standard for the Internet of Things in its different forms.



1. NB-IoT belongs to the category of low-power wide-area networks (LPWAN), enabling to connect devices that need small amounts of data, low bandwidth, and long battery life.



1. This makes it suitable for a variety of applications and use cases for IoT.



1. NB-IoT applications, typically small data volume amounts need to be infrequently transmitted.



1. NB-IoT (Narrowband-IoT) is a narrowband radio technology for M2M and Internet of Things (IoT) devices and applications requiring wireless transmission over a more extended range at a relatively low cost and using little power for long battery lives.



1. NB-IoT can co-exist with 2G, 3G, and 4G mobile networks.
2. It also benefits from all the security and privacy features of mobile networks, such as support for user identity confidentiality, entity authentication, confidentiality, data integrity, and mobile equipment identification.



1. The first NB-IoT commercial launches have been completed and global roll out is expected for 2017/18



|  |  |  |
| --- | --- | --- |
| **Parameters** | **Arduino** | **Raspberry Pie** |
| Control Unit | The Control Unit of the Arduino is from the ATmega family. | The Control Unit of the Raspberry Pi is from the ARM family. |
| Basis | Arduino works on the basis of a microcontroller. | Raspberry Pi, on the other hand, works on the basis of a microprocessor. |
| Use | The Arduino basically helps in controlling all the electrical components that connect to a system’s circuit board. | The Raspberry Pi primarily computes data and info for producing valuable outputs. It also controls the various components in any given system on the basis of the outcome (of the computation). |
| Structure of Hardware and Software | The Arduino boards have a very simple structure of software and hardware. | The Raspberry Pi boards consist of comparatively complex software and hardware architecture. |
| Type of CPU Architecture | Arduino has an 8-bit architecture. | Raspberry Pi has a 64-bit architecture. |
| RAM Usage | Arduino makes use of very little RAM of about 2 kB (Kilobytes). | Raspberry Pi always requires more RAM than Arduino of about 1 GB (Gigabytes). |
| Processing Speed | Arduino clocks 16 MHz (Megahertz) of processing speed in a system. | The Raspberry Pi clocks 1.4 GHz (Gigahertz) of processing speed in a system. |
| Cost Efficiency | It has a higher cost-efficiency because it is comparatively cheaper. | It has a lower cost-efficiency because it is comparatively more expensive. |
| I/O Drive Strength | The I/O current drive strength in the case of Arduino is higher. | The I/O current drive strength in the case of Raspberry Pi is lower. |
| Power Consumption | Arduino consumes power of about 200 MW (Megawatts). | Raspberry Pi consumes about 700 MW. |

**Q.8 FAIR (Factor Analysis of Information Risk) standard for risk assessment.**

FAIR (Factor Analysis of Information Risk) is a framework for understanding , examining and evaluating information risk.



FAIR is intended to address weaknesses in security practices within organizations.



The framework is designed to allow organizations to address a unified practice in regards to risk; utilize risk assessments and apply them to any asset or object; have an overview of total organizational risk;



challenge determined risks using innovative evaluations; and understand the affects that time and money impact the organization’s overall security profile.

**Scope the analysis**: Define the scope of the analysis, including the assets to be assessed and the risk scenarios to be considered.

**Identify threats**: Identify potential threats that could impact the assets in scope.

**Identify assets**: Identify the assets that could be impacted by the identified threats.

**Identify and assess risk factors:** Identify and assess the various risk factors that could impact the assets, including the likelihood of the event occurring, the impact if it does, and any controls or safeguards that are in place to mitigate the risk.

**Determine the risk**: Use the assessed risk factors to determine the overall risk level for each asset.

**Communicate and monitor:** Communicate the results of the risk assessment to stakeholders and develop a plan to monitor and manage the identified risks.

**Three pros to using FAIR;**

* It is not subject to the limits of ordinary scaling techniques.



* It accounts for the true scientific developing of loss disclosures.
* It contains additional comprehensive definitions of threats, vulnerabilities and risks.



**Three cons to using FAIR;**

* Difficult to use.
* It’s not thoroughly documented as other methods.



* Virtually no access to existing material regarding the methodology

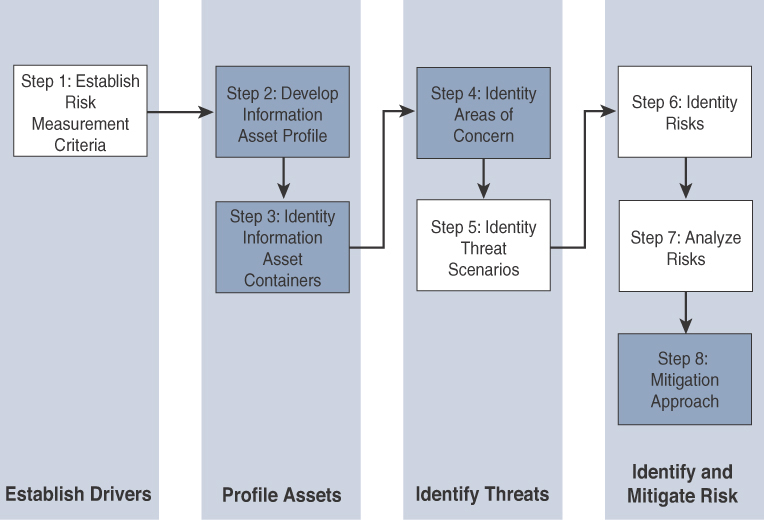
**Explain the OCTAVE risk assessment frameworks with neat diagram.**

* **Risk Assessment Methodologies:**
* OCTAVE **(Operationally Critical Threat, Asset and Vulnerability Evaluation)** tools, techniques, and methods that are used in risk-based information security for strategic assessment and planning.



* OCTAVE considers assets to be people, computer systems, software, hardware, and sensitive private information.



* 
* **Phase:**
* The first step of the **OCTAVE** Allegro methodology is to **establish a risk measurement criterion**. OCTAVE provides a fairly simple means of doing this with an emphasis on impact, value, and measurement.



* The second step is to **develop an information asset profile**. This profile is populated with assets, a prioritization of assets, attributes associated with each asset, including owners, custodians, people, explicit security requirements, and technology assets. It is important to stress the importance of process.



* The third step is to **identify information asset containers**. Roughly speaking, this is the range of transports and possible locations where the information might reside. This references the compute elements and the networks by which they communicate.



* The fourth step is to **identify areas of concern**. At this point, we depart from a data flow, touch, and attribute focus to one where judgments are made through a mapping of security-related attributes to more business-focused use cases.



* fifth step, where **threat scenarios** are identified. This definition means that results from both malevolent and accidental causes are viable threats.



* At the sixth **step risks are identified**. Within OCTAVE, risk is the possibility of an undesired outcome. This is extended to focus on how the organization is impacted.

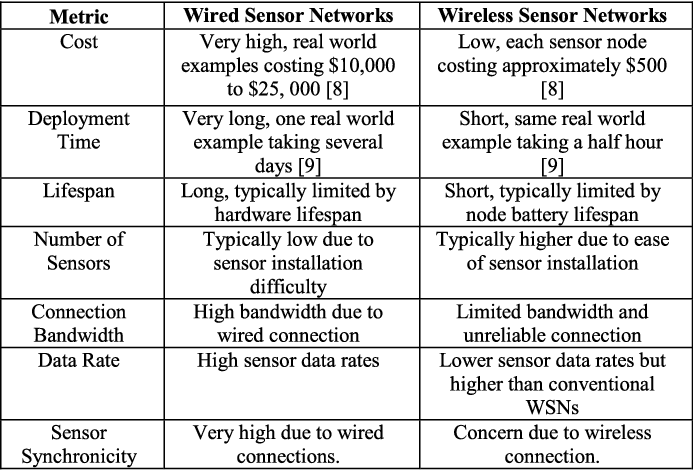


* The seventh step is **risk analysis**, with the effort placed on qualitative evaluation of the impacts of the risk.



* Finally, mitigation is **applied at the eighth step**. There are three outputs or decisions to be taken at this stage. One may be to accept a risk and do nothing, other than document the situation, potential outcomes, and reasons for accepting the risk.





Q. Elaborate Tunneling Legacy SCADA over IP Networks with three scenarios.

**What Is Tunneling:**

* in networking, tunnels are a method for transporting data across a network using protocols that are not supported by that network.
* Tunneling works by encapsulating packets: wrapping packets inside of other packets.
* (Packets are small pieces of data that can be re-assembled at their destination into a larger file.)
* Tunneling is often used in virtual private networks (VPNs). It can also set up efficient and secure connections between networks, enable the usage of unsupported network protocols, and in some cases allow users to bypass firewalls.

**Split Tunneling Scenario:**

* Usually, when a user connects their device to a VPN, all their network traffic goes through
* the VPN tunnel. Split tunneling allows some traffic to go outside of the VPN tunnel.
* In essence, split tunneling lets user devices connect to two networks simultaneously: one public and one private.

**GRE Tunneling Scenario:**

Generic Routing Encapsulation (GRE) is one of several tunneling protocols. GRE encapsulates data packets that use one routing protocol inside the packets of another protocol.

GRE is one way to set up a direct point-to-point connection across a network, for the purpose of simplifying connections between separate networks.

**GRE adds two headers to each packet:** the GRE header and an IP header. The GRE header indicates the protocol type used by the encapsulated packet. The IP header encapsulates the original packet's IP header and payload. Only the routers at each end of the GRE tunnel will reference the original, non-GRE IP header.

**SSH Tunneling Scenario:**

The Secure Shell (SSH) protocol sets up encrypted connections between client and server, and can also be used to set up a secure tunnel. SSH operates at layer 7 of the OSI model, the application layer. By contrast, IPsec, IP-in-IP, and GRE operate at the network layer.

### Q.06 What is Internet Protocol Suite?



* The **Internet** Protocol Suite is also known as a TCP/IP protocol suite or TCP/IP model.
* It is one type of protocol and network model used on the internet.



* It consists of four layers’ application layer, transport layer, internet layer, and the link layer.



* In this networking, the TCP and the IP layers are the most widely used protocols, so that this model named as TCP/IP model or Internet Protocol Suite model.



### The key advantages of the IP suite for the Internet of Things:

As follow

♣**Open and standards-based:**



IP is an open standard which is not vendor specific and can suit IOT applications as IOT requires different devices to work together.

♣**Versatile:**



The layered IP architecture is well provide to cope with any type of physical and data link layers. No single access technology can serve all IOT application, where there are various wired and wireless access technologies which can be used based on the type of the application and IP can cope with any of them.



♣**Ubiquitous:**

IP is the most pervasive protocol when you look at what is supported across the various IoT solutions.



♣**Scalable:**

Millions of private and public IP infrastructure nodes have been operational for years.



**♣Manageable and highly secure:**

IP networks has a well-understood network management and security protocols, mechanisms, and toolsets that are widely available.



**♣Stable and resilient:**

IP has a large and well-established knowledge base and, more importantly, it has been used for years in critical infrastructures, such as financial and Defense networks.



**♣Consumers’ market adoption:**

Access to applications and devices will occur predominantly over broadband and mobile wireless infrastructure. IP is the common protocol that links IoT in the consumer space to these devices.



**♣The innovation factor:**



IP is the underlying protocol for applications ranging from file transfer and e-mail to the World Wide Web, e-commerce, social networking, mobility, and more.

**Q15 What is DNS how does it works**

* + DNS stands for Domain Name System.
  + DNS is a directory service that provides a mapping between the name of a host on the network and its numerical address.
  + DNS is required for the functioning of the internet.
  + Each node in a tree has a domain name, and a full domain name is a sequence of symbols specified by dots.
  + DNS is a service that translates the domain name into IP addresses. This allows the users of networks to utilize user-friendly names when looking for other hosts instead of remembering the IP addresses.
  + For example, suppose the FTP site at EduSoft had an IP address of 132.147.165.50, most people would reach this site by specifying ftp.EduSoft.com. Therefore, the domain name is more reliable than IP address.

**Working of DNS**

* + DNS is a client/server network communication protocol. DNS clients send requests to the. server while DNS servers send responses to the client.
  + Client requests contain a name which is converted into an IP address known as a forward DNS lookups while requests containing an IP address which is converted into a name known as reverse DNS lookups.
  + DNS implements a distributed database to store the name of all the hosts available on the internet.
  + If a client like a web browser sends a request containing a hostname, then a piece of software such as DNS resolver sends a request to the DNS server to obtain the IP address of a hostname. If DNS server does not contain the IP address associated with a hostname, then it forwards the request to another DNS server.
  + If IP address has arrived at the resolver, which in turn completes the request over the internet protocol.

**. What are TCP and UDP Ports? Explain with Example.**

* + TCP is a connection orientated protocol with built in error recovery and re transmission.
  + You can liken a TCP connection to a telephone connection.
  + With a telephone connection you first need to setup the connection by dialing the number, and once the calling party answers you have a both way communications channel.
  + With TCP you set up the connection using the 3 way handshake .
  + A port number is a unique identifier used with an IP address. A port is a 16-bit unsigned integer, and the total number of ports available in the TCP/IP model is 65,535 ports.
  + UDP, the zero port is not available.
  + UDP is a connectionless protocol.
  + You can liken UDP to email or the normal post.
  + With email or a written message you send your message, but have no idea whether or not that message was received.
* Example of port number:192.168.1.100: 7
* In the above case, 192.168.1.100 is an IP address, and 7 is a port number.
  + Ex: the client sends the TCP segment to the well-known port, i.e., 80 of the HTTP protocols.

**Classification of port numbers**

The port numbers are divided into three categories:

* + Well-known ports
  + Registered ports
  + Dynamic ports

**Well-known ports**

The range of well-known port is 0 to 1023. The well-known ports are used with those protocols that serve common applications and services such as HTTP (hypertext transfer protocol), IMAP (Internet Message Access Protocol), SMTP (Simple Mail Transfer Protocol), etc. For example, we want to visit some websites on an internet; then, we use http protocol;

**Registered ports**

The range of registered port is 1024 to 49151. The registered ports are used for the user processes. These processes are individual applications rather than the common applications that have a well-known port.

**Dynamic ports**

The range of dynamic port is 49152 to 65535. Another name of the dynamic port is ephemeral ports. These port numbers