

USN 

## Internal Assessment Test 2 – April-2024

Sub:	Internet of Things				Sub Code:	18CS81	Branch:	CSE
Date:	13-04-2024	Duration:	90 mins	Max Marks:	50	Sem / Sec:	VIII (A, B & C)	OBE

Answer any FIVE FULL Questions

							MARKS	CO	RBT
1	Explain i)6LOWPAN ii)Header compression ii)Fragmentation iv)Mesh addressing.						10	CO3	L1
2	Elaborate SCADA protocol translation with a neat diagram.						10	CO3	L2
3	Illustrate the MQTT framework and message format.						10	CO3	L2
4	Explain Hadoop distributed cluster with a neat diagram & writing a file to HDFS .						10	CO4	L2
5(a)	Describe edge streaming analytics with neat Diagram						5	CO4	L2
5(b)	Explain functions of edge analytics processing unit.						5	CO4	L2
6(a)	Justify Prudence model for control hierarchy in IoT						6	CO4	L2
6(b)	Explain OT network characteristics that impact Security.						4	CO4	L2

CI

CCI

HOD

USN 

## Internal Assessment Test 2 – April-2024

Sub:	Internet of Things				Sub Code:	18CS81	Branch:	CSE
Date:	13-04-2024	Duration:	90 mins	Max Marks:	50	Sem / Sec:	VIII (A, B & C)	OBE

Answer any FIVE FULL Questions

							MARKS	CO	RBT
1	Explain i)6LOWPAN ii)Header compression ii)Fragmentation iv)Mesh addressing.						10	CO3	L1
2	Elaborate SCADA protocol translation with a neat diagram.						10	CO3	L2
3	Illustrate the MQTT framework and message format.						10	CO3	L2
4	Explain Hadoop distributed cluster with a neat diagram & writing a file to HDFS .						10	CO4	L2
5(a)	Describe edge streaming analytics with neat Diagram						5	CO4	L2
5(b)	Explain functions of edge analytics processing unit.						5	CO4	L2
6(a)	Justify Prudence model for control hierarchy in IoT						6	CO4	L2
6(b)	Explain OT network characteristics that impact Security.						4	CO4	L2

CI

CCI

HOD

## PO Mapping

Course Outcomes			Modu les covere d	P O 1	P O 2	P O 3	P O 4	P O 5	P O 6	P O 7	P O 8	P O 9	P O 10	P O 11	P O 12	P S O 1	P S O 2	P S O 3	P S O 4	
CO1	Interpret the impact and challenges posed by IoT networks leading to new architectural models.	L2	1	3	2	2	-	-	2	-	-	-	-	-	-	-	-	-	-	3
CO2	Compare and contrast the deployment of smart objects and the technologies to connect them to network.	L2	2	3	2	2	-	-	2	-	-	-	-	-	-	-	-	-	-	3
CO3	Appraise the role of IoT protocols for efficient network communication.	L2	3	3	2	2	-	-	2	-	-	-	-	-	-	-	-	-	-	3
CO4	Elaborate the need for Data Analytics and Security in IoT.	L2	4	3	2	2	-	-	2	-	-	-	-	-	-	-	-	-	-	3
CO5	Illustrate different sensor technologies for sensing real world entities	L3	,5	3	2	2	-	-	2	-	-	-	-	-	-	-	-	-	-	3

COGNITIVE LEVEL	REVISED BLOOMS TAXONOMY KEYWORDS
L1	List, define, tell, describe, identify, show, label, collect, examine, tabulate, quote, name, who, when, where, etc.
L2	summarize, describe, interpret, contrast, predict, associate, distinguish, estimate, differentiate, discuss, extend
L3	Apply, demonstrate, calculate, complete, illustrate, show, solve, examine, modify, relate, change, classify, experiment, discover.
L4	Analyze, separate, order, explain, connect, classify, arrange, divide, compare, select, explain, infer.
L5	Assess, decide, rank, grade, test, measure, recommend, convince, select, judge, explain, discriminate, support, conclude, compare, summarize.

PROGRAM OUTCOMES (PO), PROGRAM SPECIFIC OUTCOMES (PSO)				CORRELATION LEVELS	
PO1	Engineering knowledge	PO7	Environment and sustainability	0	No Correlation
PO2	Problem analysis	PO8	Ethics	1	Slight/Low
PO3	Design/development of solutions	PO9	Individual and team work	2	Moderate/ Medium
PO4	Conduct investigations of complex problems	PO10	Communication	3	Substantial/ High
PO5	Modern tool usage	PO11	Project management and finance		
PO6	The Engineer and society	PO12	Life-long learning		
PSO1	Develop applications using different stacks of web and programming technologies				
PSO2	Design and develop secure, parallel, distributed, networked, and digital systems				
PSO3	Apply software engineering methods to design, develop, test and manage software systems.				
PSO4	Develop intelligent applications for business and industry				

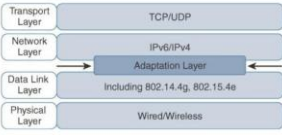
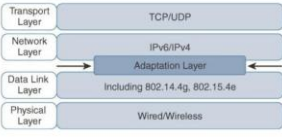
---

Internal Assessment Test 2 – April, 2024

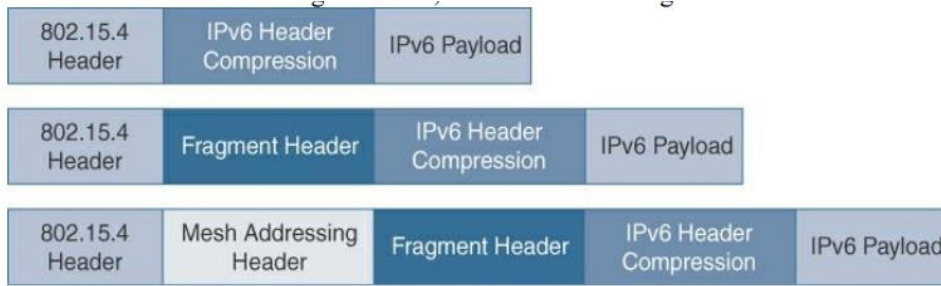
Sub:	Internet of Things	Sub Code:	18CS81	Branch:	CSE
Date:	13-04-2024	Duration:	90 mins	Max Marks:	50
		Sem / Sec:	VIII (A, B & C)		OBE

Answer any FIVE FULL Questions

MAR KS	CO	RBT
--------	----	-----

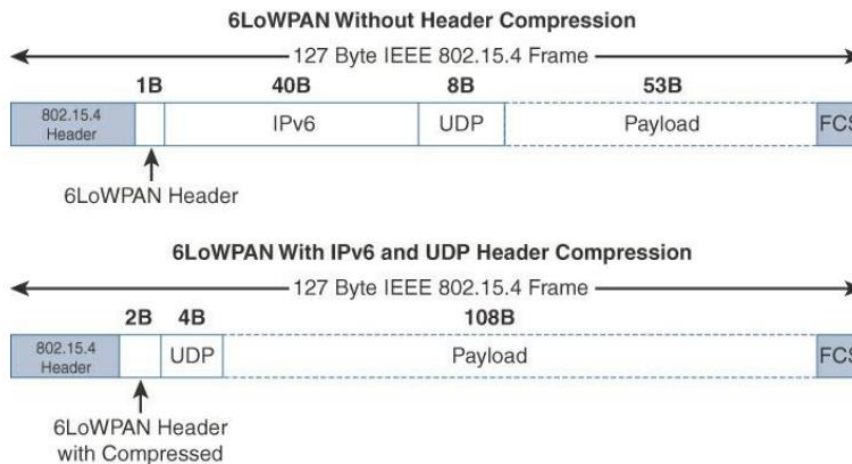
<b>1</b>	<p>Explain the need for IP optimization for the following 6LOWPAN i)Header compression ii)Fragmentation iii)Mesh addressing.</p>  <p><b>ANS :</b></p> <p>Optimizing IP for IoT Using an Adaptation Layer, it highlights the TCP/IP layers where optimization is applied.</p>  <p>From 6LoWPAN to 6Lo • In the IP architecture, the transport of IP packets over any given Layer 1 (PHY) and Layer 2 (MAC) protocol must be defined and documented. The model for packaging IP into lower-layer protocols is often referred to as an adaptation layer. • IP adaptation layers are typically defined by an IETF working group and released as a Request for Comments (RFC). • For example, RFC 864 describes how an IPv4 packet gets encapsulated over an Ethernet frame, and RFC 2464 describes how the same function is performed for an IPv6 packet. • The main examples of adaptation layers optimized for constrained nodes or “things” are the ones under the 6LoWPAN working group and its successor, the 6Lo working group. Comparison of an IoT Protocol Stack Utilizing 6LoWPAN and an IP Protocol Stack</p> <div style="display: flex; justify-content: space-around; align-items: flex-start;"> <div style="text-align: center;"> <p><b>IP Protocol Stack</b></p> <table border="1" style="border-collapse: collapse; text-align: center;"> <tr><td colspan="2">HTTP</td><td colspan="2">RTP</td></tr> <tr><td>TCP</td><td>UDP</td><td colspan="2">ICMP</td></tr> <tr><td colspan="4">IP</td></tr> <tr><td colspan="4">Ethernet MAC</td></tr> <tr><td colspan="4">Ethernet PHY</td></tr> </table> </div> <div style="text-align: center;"> <p><b>IoT Protocol Stack with 6LoWPAN Adaptation Layer</b></p> <table border="1" style="border-collapse: collapse; text-align: center;"> <tr><td colspan="2">Application Protocols</td></tr> <tr><td>UDP</td><td>ICMP</td></tr> <tr><td colspan="2">IPv6</td></tr> <tr><td colspan="2">LoWPAN</td></tr> <tr><td colspan="2">IEEE 802.15.4 MAC</td></tr> <tr><td colspan="2">IEEE 802.15.4 PHY</td></tr> </table> </div> </div>	HTTP		RTP		TCP	UDP	ICMP		IP				Ethernet MAC				Ethernet PHY				Application Protocols		UDP	ICMP	IPv6		LoWPAN		IEEE 802.15.4 MAC		IEEE 802.15.4 PHY	
HTTP		RTP																															
TCP	UDP	ICMP																															
IP																																	
Ethernet MAC																																	
Ethernet PHY																																	
Application Protocols																																	
UDP	ICMP																																
IPv6																																	
LoWPAN																																	
IEEE 802.15.4 MAC																																	
IEEE 802.15.4 PHY																																	

6LoWPAN Header Stacks, shows the sub headers related to compression, fragmentation, and mesh addressing.



### Header Compression

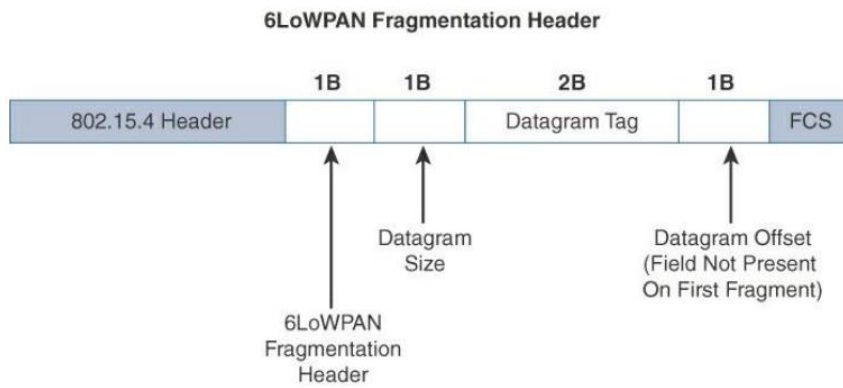
- IPv6 header compression for 6LoWPAN was defined initially in RFC 4944 and subsequently updated by RFC 6282. This capability shrinks the size of IPv6's 40-byte headers and User Datagram Protocol's (UDP's) 8-byte headers down as low as 6 bytes combined in some cases.
- Header compression for 6LoWPAN is only defined for an IPv6 header and not IPv4. The 6LoWPAN protocol does not support IPv4, and, in fact, there is no standardized IPv4 adaptation layer for IEEE 802.15.4.
- 6LoWPAN header compression is stateless, and conceptually it is not too complicated.



- 6LoWPAN frame without any header compression enabled: The full 40-byte IPv6 header and 8-byte UDP header are visible. The 6LoWPAN header is only a single byte in this case.
- Uncompressed IPv6 and UDP headers leave only 53 bytes of data payload out of the 127-byte maximum frame size in the case of IEEE 802.15.4.
- Frame where header compression has been enabled for a best-case scenario. The 6LoWPAN header increases to 2 bytes to accommodate the compressed IPv6 header, and UDP has been reduced in half, to 4 bytes from 8.

### → Fragmentation

- The maximum transmission unit (MTU) for an IPv6 network must be at least 1280 bytes. The term MTU defines the size of the largest protocol data unit that can be passed. For IEEE 802.15.4, 127 bytes is the MTU.

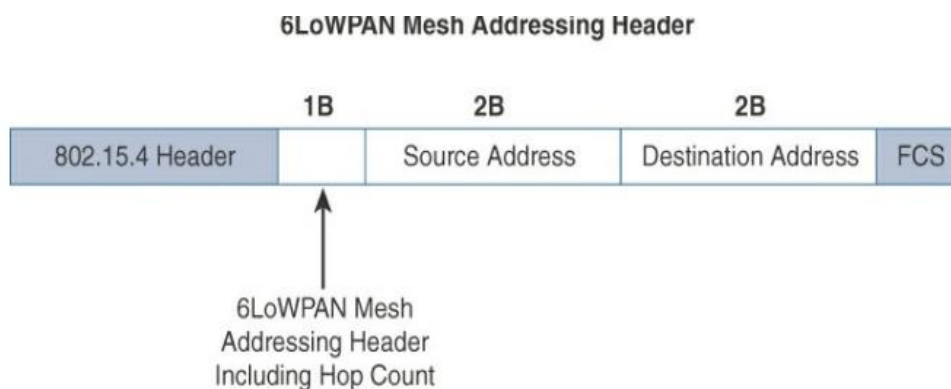


The 6LoWPAN fragmentation header field itself uses a unique bit value to identify that the subsequent fields behind it are fragment fields as opposed to another capability, such as header compression.

- In the fragmentation header for an IPv6 payload being only 4 bytes long. The remainder of the fragments have a 5-byte header field so that the appropriate offset can be specified.

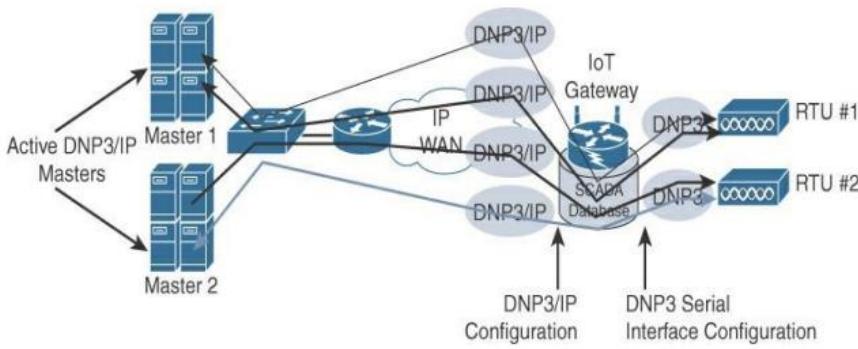
### Mesh Addressing

- The purpose of the 6LoWPAN mesh addressing function is to forward packets over multiple hops. Three fields are defined for this header: Hop Limit, Source Address, and Destination Address.
- The IPv6 hop limit field, the hop limit for mesh addressing also provides an upper limit on how many times the frame can be forwarded. Each hop decrements this value by 1 as it is forwarded. Once the value hits 0, it is dropped and no longer forwarded.
- The Source Address and Destination Address fields for mesh addressing are IEEE 802.15.4 addresses indicating the endpoints of an IP hop.



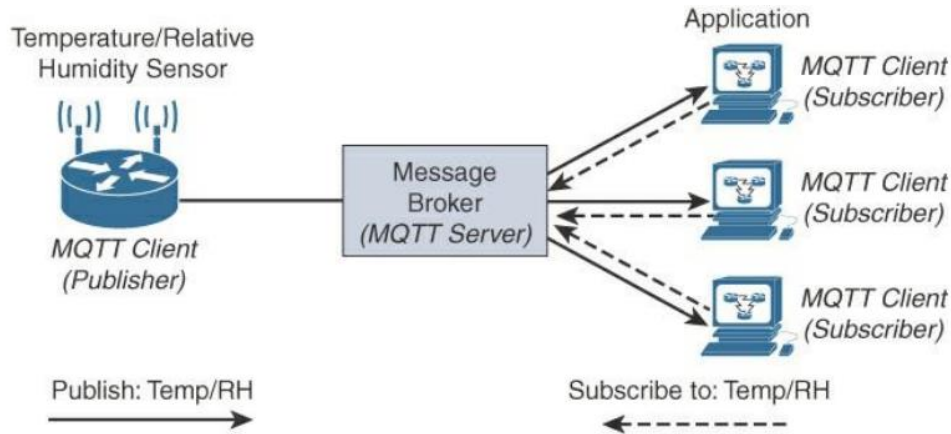
Note that the mesh addressing header is used in a single IP subnet and is a Layer 2 type of routing known as mesh-under.

- Mesh-Under Versus Mesh-Over Routing - For network technologies such as IEEE 802.15.4, IEEE 802.15.4g, and IEEE 1901.2a that support mesh topologies and operate at the physical and data link layers, two main

	<p>options exist for establishing reachability and forwarding packets. o With the first option, mesh-under, the routing of packets is handled at the 6LoWPAN adaptation layer. o The other option, known as “mesh-over” or “route-over,” utilizes IP routing for getting packets to their destination</p>			
<p>2</p>	<p>Elaborate SCADA protocol translation with a neat diagram.</p> <p><b>Ans</b></p> <p>→ SCADA(supervisory control and data acquisition) –</p> <ul style="list-style-type: none"> <li>• Combined with the fact that IP is the de facto standard for computer networking in general, older protocols that connected sensors and actuators have evolved and adapted themselves to utilize IP.</li> <li>• A prime example of this evolution is supervisory control and data acquisition (SCADA). Designed decades ago, SCADA is an automation control system that was initially implemented without IP over serial links, before being adapted to Ethernet and IPv4.</li> </ul> <p>→ A Little Background on SCADA</p> <ul style="list-style-type: none"> <li>– o At a high level, SCADA systems collect sensor data and telemetry from remote devices, while also providing the ability to control them.</li> <li>o Used in today’s networks, SCADA systems allow global, real-time, data-driven decisions to be made about how to improve business processes.</li> </ul> <p>→ SCADA Protocol Translation</p> <ul style="list-style-type: none"> <li>• <b><u>DNP3 Protocol Translation</u></b></li> </ul>  <p>The above figure shows two serially connected DNP3 RTUs and two master applications supporting DNP3 over IP that control and pull data from the RTUs.</p> <ul style="list-style-type: none"> <li>• The IoT gateway in this figure performs a protocol translation function that enables communication between the RTUs and servers, despite the fact that a serial connection is present on one side and an IP connection is used on the other.</li> <li>• By running protocol translation, the IoT gateway connected to the RTUs is implementing a computing function close to the edge of the network. Adding computing functions close to the edge helps scale distributed intelligence in IoT networks.</li> <li>• This can be accomplished by offering computing resources on IoT gateways or routers, as shown in this protocol translation example.</li> </ul>	<p>10</p>	<p>CO3</p>	<p>L2</p>
<p>3</p>	<p>Illustrate the framework and message format of the protocol which is reliable, lightweight &amp; cost-effective to monitor and control a large number of sensors and their data from a central server location especially for the oil and gas industry.</p> <p><b>Ans</b></p> <p>Message Queuing Telemetry Transport (MQTT)</p> <ul style="list-style-type: none"> <li>• At the end of the 1990s, engineers from IBM and Arcom (acquired in 2006 by Eurotech) were looking for a reliable, lightweight, and cost-effective protocol to monitor and control a large number of sensors and their</li> </ul>	<p>10</p>	<p>CO3</p>	<p>L3</p>



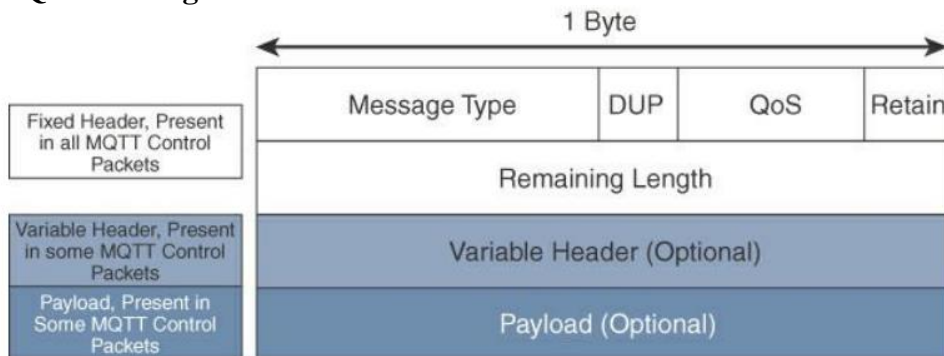
data from a central server location, as typically used by the oil and gas industries.



An MQTT client can act as a publisher to send data (or resource information) to an MQTT server acting as an MQTT message broker.

- The MQTT client on the left side is a temperature (Temp) and relative humidity (RH) sensor that publishes its Temp/RH data.
- The MQTT server (or message broker) accepts the network connection along with application messages, such as Temp/RH data, from the publishers. It also handles the subscription and unsubscription process and pushes the application data to MQTT clients acting as subscribers.
- The application on the right side is an MQTT client that is a subscriber to the Temp/RH data being generated by the publisher or sensor on the left.
- This model, where subscribers express a desire to receive information from publishers, is well known. A great example is the collaboration and social networking application Twitter.

#### MQTT Message Format



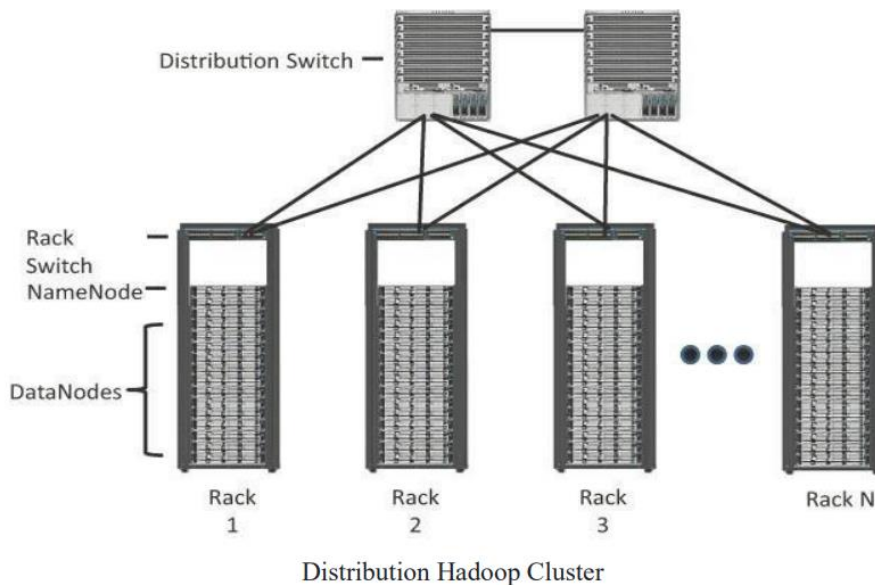
4 Explain Hadoop distributed cluster with a neat diagram & writing a file to HDFS. Hadoop Hadoop is the most recent entrant into the data management market, but it is arguably the most popular choice as a data repository and processing engine. Hadoop was originally developed as a result of projects at Google and Yahoo!, and the original intent for Hadoop was to index millions of websites and quickly return search results for open source search engines. the project had two key elements:  
 Hadoop Distributed File System (HDFS): A system for storing data across multiple nodes  
 MapReduce: A distributed processing engine that splits a large task into smaller ones that can be run in parallel

10

CO4

L2





Both MapReduce and HDFS take advantage of this distributed architecture to store and process massive amounts of data and are thus able to leverage resources from all nodes in the cluster.

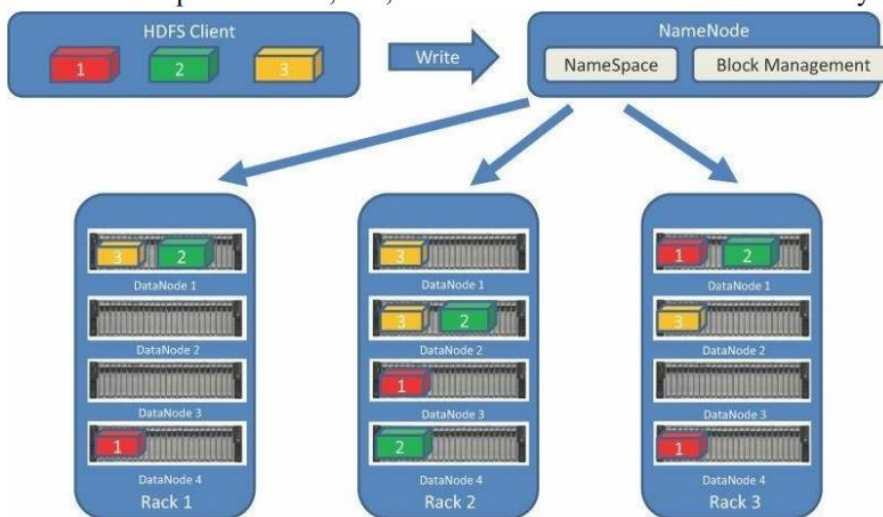
For HDFS, this capability is handled by specialized nodes in the cluster, including NameNodes and DataNodes

**NameNodes:** These are a critical piece in data adds, moves, deletes, and reads on HDFS. They coordinate where the data is stored, and maintain a map of where each block of data is stored and where it is replicated.

**DataNodes:** These are the servers where the data is stored at the direction of the NameNode.

- o It is common to have many DataNodes in a Hadoop cluster to store the data.

- o Data blocks are distributed across several nodes and often are replicated three, four, or more times across nodes for redundancy.



MapReduce leverages a similar model to batch process the data stored on the cluster nodes.

5(a)

Describe edge streaming analytics with neat Diagram

**Ans**

Analyzing a massive volume of time-sensitive IoT data in a centralized cloud is often not ideal.

The key values of edge streaming analytics include the following:

5

CO4

L2

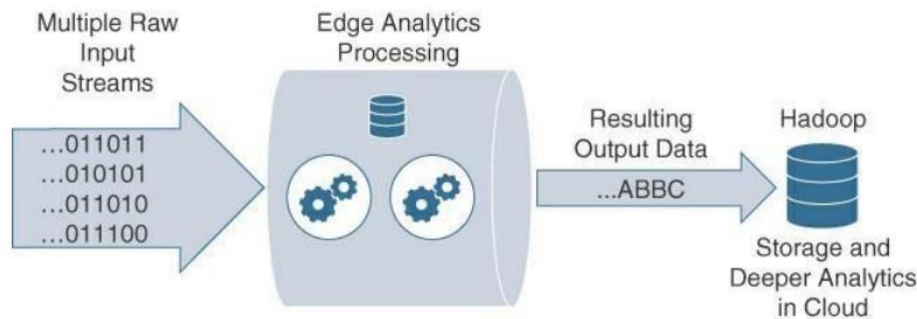
**Reducing data at the edge:** The aggregate data generated by IoT devices is generally in proportion to the number of devices. The scale of these devices is likely to be huge, and so is the quantity of data they generate. Passing all this data to the cloud is inefficient and is unnecessarily expensive in terms of bandwidth and network infrastructure.

**Analysis and response at the edge:** Some data is useful only at the edge (such as a factory control feedback system). In cases such as this, the data is best analyzed and acted upon where it is generated.

**Time sensitivity:** When timely response to data is required, passing data to the cloud for future processing results in unacceptable latency. Edge analytics allows immediate responses to changing conditions.

5(b)

Explain functions of edge analytics processing unit.  
 To perform analytics at the edge, data needs to be viewed as real-time flows. Streaming analytics at the edge can be broken down into three simple stages:  
 Raw input data  
 Analytics processing unit (APU)  
 Output streams



Edge Analytics Processing Unit

In order to perform analysis in real-time, the APU needs to perform the following functions:

**Filter:** The streaming data generated by IoT endpoints is likely to be very large, and most of it is irrelevant. For example, a sensor may simply poll on a regular basis to confirm that it is still reachable. This information is not really relevant and can be mostly ignored. The filtering function identifies the information that is considered important.

**Transform:** In the data warehousing world, Extract, Transform, and Load (ETL) operations are used to manipulate the data structure into a form that can be used for other purposes. Analogous to data warehouse ETL operations, in streaming analytics, once the data is filtered, it needs to be formatted for processing.

**Time:** As the real-time streaming data flows, a timing context needs to be established. This could be to correlated average temperature readings from sensors on a minute-by-minute basis

5

CO4

L2

Defining Streams and Windows

2016-01-08 04:05:06	Sensor_5	23.45
2016-01-08 04:06:45	Sensor_3	27.22
2016-01-08 04:06:54	Sensor_3	26.89
2016-01-08 04:07:07	Sensor_2	25.01
2016-01-08 04:07:33	Sensor_5	23.00
2016-01-08 04:08:10	Sensor_5	23.02
2016-01-08 04:09:01	Sensor_2	25.02

2016-01-08 04:07:00	Sensor_5	23.45
2016-01-08 04:07:00	Sensor_3	27.06
2016-01-08 04:08:00	Sensor_5	23.00
2016-01-08 04:08:00	Sensor_3	27.06
2016-01-08 04:08:00	Sensor_2	25.01
2016-01-08 04:09:00	Sensor_5	23.01
2016-01-08 04:09:00	Sensor_2	25.01

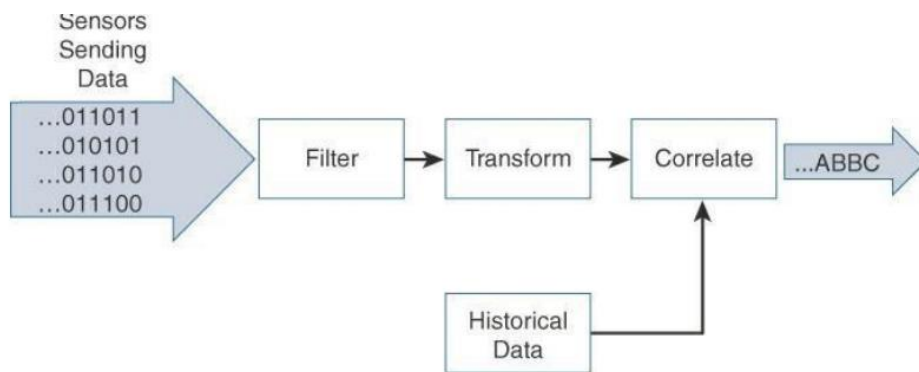
  

```

CREATE STREAM Temp (
  ts TIMESTAMP CQTIME USER,
  device TEXT,
  temp NUMERIC(15,2)
);

SELECT cq_close(*), device, avg (temp)
FROM Temp <VISIBLE '2 min' ADVANCE '1 min'>
GROUP BY device;
    
```

**Correlate:** Streaming data analytics becomes most useful when multiple data streams are combined from different types of sensors. For example, in a hospital, several vital signs are measured for patients, including body temperature, blood pressure, heart rate, and respiratory rate



Correlating Data Streams with Historical Data

**Match patterns:** Once the data streams are properly cleaned, transformed, and correlated with other live streams as well as historical data sets, pattern matching operations are used to gain deeper insights to the data

**Improve business intelligence:** Ultimately, the value of edge analytics is in the improvements to business intelligence that were not previously available.

6(a) Justify Prudure model for control hierarchy in IoT  
**Ans**

The Purdue Model for Control Hierarchy

Regardless of where a security threat arises, it must be consistently and unequivocally treated. IT information is typically used to make business decisions, such as those in process optimization, whereas OT information is instead characteristically leveraged to make physical decisions, such as closing a valve, increasing pressure, and so on.

Enterprise Zone	Enterprise Network	Level 5
	Business Planning and Logistics Network	Level 4
DMZ	Demilitarized Zone — Shared Access	
Operations Support	Operations and Control	Level 3
	Supervisory Control	Level 2
	Process Control / SCADA Zone	Basic Control
Process		Level 0
Safety	Safety-Critical	

The Logical Framework Based on the Purdue Model for Control Hierarchy

6

CO4

L2

	<p>This model identifies levels of operations and defines each level. The enterprise and operational domains are separated into different zones and kept in strict isolation via an industrial demilitarized zone (DMZ):</p> <p>Enterprise zone Level 5: Enterprise network: Corporate-level applications such as Enterprise Resource Planning (ERP), Customer Relationship Management (CRM), document management, and services such as Internet access and VPN entry from the outside world exist at this level</p> <p>Level 4: Business planning and logistics network: The IT services exist at this level and may include scheduling systems, material flow applications, optimization and planning systems, and local IT services such as phone, email, printing, and security monitoring</p> <p>Industrial demilitarized zone DMZ: The DMZ provides a buffer zone where services and data can be shared between the operational and enterprise zones. It also allows for easy segmentation of organizational control. By default, no traffic should traverse the DMZ; everything should originate from or terminate on this area.</p> <p>Operational zone Level 3: Operations and control: This level includes the functions involved in managing the workflows to produce the desired end products and for monitoring and controlling the entire operational system. This could include production scheduling, reliability assurance, system wide control optimization, security management, network management, and potentially other required IT services, such as DHCP, DNS, and timing.</p> <p>Level 2: Supervisory control: This level includes zone control rooms, controller status, control system network/application administration, and other control-related applications, such as human- machine interface (HMI) and historian</p> <p>Level 1: Basic control: At this level, controllers and IEDs, dedicated HMIs, and other applications may talk to each other to run part or all of the control function</p> <p>Level 0: Process: This is where devices such as sensors and actuators and machines such as drives, motors, and robots communicate with controllers or IEDs.</p> <p>Safety zone Safety-critical: This level includes devices, sensors, and other equipment used to manage the safety functions of the control system</p> <p>One of the key advantages of designing an industrial network in structured levels, as with the Purdue model, is that it allows security to be correctly applied at each level and between levels</p>			
6(b)	<p>Explain OT network characteristics that impact Security. Ans</p>	4	CO4	L2

While IT and OT networks are beginning to converge, they still maintain many divergent characteristics in terms of how they operate and the traffic they handle. These differences influence how they are treated in the context of a security strategy. For example, compare the nature of how traffic flows across IT and OT networks:

**IT networks:**

In an IT environment, there are many diverse data flows. The communication data flows that emanate from a typical IT endpoint travel relatively far. They frequently traverse the network through layers of switches and eventually make their way to a set of local or remote servers, which they may connect to directly. Data in the form of email, file transfers, or print services will likely all make its way to the central data center, where it is responded to, or triggers actions in more local services, such as a printer. In the case of email or web browsing, the endpoint initiates actions that leave the confines of the enterprise network and potentially travel around the earth

**OT networks:**

By comparison, in an OT environment (Levels 0–3), there are typically two types of operational traffic. The first is local traffic that may be contained within a specific package or area to provide local monitoring and closed-loop control. This is the traffic that is used for real-time (or near-real-time) processes and does not need to leave the process control levels. The second type of traffic is used for monitoring and control of areas or zones or the overall system. SCADA traffic is a good example of this, where information about remote devices or summary information from a function is shared at a system level so that operators can understand how the overall system, or parts of it, are operating. They can then implement appropriate control commands based on this information.

