Scheme of Evaluation

Internal Assessment Test 2 – March.2023

Sub:	Internet of Things							Code:	18CS81
Date:	15/04/2023	Duration:	90mins	Max Marks:	50	Sem:	VIII	Branch:	ISE

Note: Answer Any Five Questions

Question #	Description	Marks Distribution	Max Marks
1	• IEE.802.15.4 IoT access technology.	10M	10 M
2	• Describe LoRAWAN architecture and its MAC frame format..	10 M	10 M
3	• Design a 6LoWPAN protocol header compression and fragmentation	10M	10 M
4	• Illustrate the routing protocol for low power and lossy networks with a neat diagram	10M	10 M
5	• Explain key advantages of IP suite for IoT. • Describe the raw tunneling of SCADA using different scenarios	5M 5M	10 M
6	• Discuss the following with neat diagram I)COAP II)MQTT • Define DAG.	9M 1M	10 M

Internal Assessment Test 2 – March.2023

Sub:	Internet of Things							Code:	18CS81
Date:	15/04/2023	Duration:	90mins	Max Marks:	50	Sem:	VIII	Branch:	ISE

Note: Answer Any Five Questions

1. Explain IEE.802.15.4 IoT access technology.

- IEEE 802.15.4 or IEEE 802.15 Task Group 4 defines low-data-rate PHY and MAC layer specifications for wireless personal area networks (WPAN).
- The IEEE 802.15.4 PHY and MAC layers are the foundations for several networking protocol stacks.
- IEEE 802.15.4 is a wireless access technology for low-cost and low-data-rate devices that are powered or run on batteries.
- IEEE 802.15.4 is commonly found in the following types of deployments:
- Home and building automation
- Automotive networks
- Industrial wireless sensor networks
- Interactive toys and remote controls
- Criticisms of IEEE 802.15.4 often focus on its MAC reliability, unbounded latency, and susceptibility to interference and multipath fading
- Some of the most well-known protocol stacks based on 802.15.4 are highlighted in Table 4-2.

Protocol	Description
ZigBee	Promoted through the ZigBee Alliance, ZigBee defines upper-layer components (network through application) as well as application profiles. Common profiles include building automation, home automation, and healthcare. ZigBee also defines device object functions, such as device role, device discovery, network join, and security. For more information on ZigBee, see the ZigBee Alliance webpage, at www.zigbee.org. ZigBee is also discussed in more detail later in the next Section.
6LoWPAN	6LoWPAN is an IPv6 adaptation layer defined by the IETF 6LoWPAN working group that describes how to transport IPv6 packets over IEEE 802.15.4 layers. RFCs document header compression and IPv6 enhancements to cope with the specific details of IEEE 802.15.4. (For more

ZigBee IP	An evolution of the ZigBee protocol stack, ZigBee IP adopts the 6LoWPAN adaptation layer, IPv6 network layer, and RPL routing protocol. In addition, it offers improvements to IP security. ZigBee IP is discussed in more detail later in this chapter.
ISA100.11a	ISA100.11a is developed by the International Society of Automation (ISA) as "Wireless Systems for Industrial Automation: Process Control and Related Applications." It is based on IEEE 802.15.4-2006, and specifications were published in 2010 and then as IEC 62734. The network and transport layers are based on IETF 6LoWPAN, IPv6, and UDP standards.
WirelessHART	WirelessHART, promoted by the HART Communication Foundation, is a protocol stack that offers a time-synchronized, self-organizing, and self-healing mesh architecture, leveraging IEEE 802.15.4-2006 over the 2.4 GHz frequency band. A good white paper on WirelessHART can be found at http://www.emerson.com/resource/blob/system-engineering-guidelines-iec-62591-wirelesshart--data-79900.pdf
Thread	Constructed on top of IETF 6LoWPAN/IPv6, Thread is a protocol stack for a secure and reliable mesh network to connect and control products in the home. Specifications are defined and published by the Thread Group at www.threadgroup.org.

2. Describe LoRAWAN architecture and its MAC frame format.

- **LoRaWAN:** Unlicensed-band Low Power Wide Area technology.

Standardization and Alliances:

- LoRa was a physical layer, or Layer 1, modulation that was developed by a French company named Cycleo.
- Its Optimized for long-range, 2-way communications and low power consumption

The technology evolved from Layer 1 to a broader scope through the creation of the LoRa Alliance.

MAC Layer Format

- LoRaWAN messages, have a

PHY payload = 1-byte MAC header + variable-byte MAC payload + 4 bytes MIC

- The MAC payload size depends on the frequency band and the data rate.
-

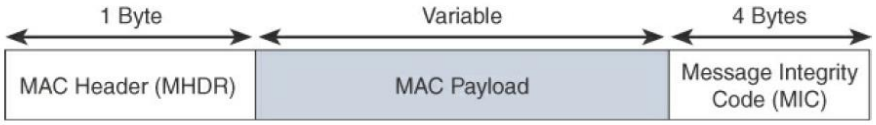


Figure 4-16 High-Level LoRaWAN MAC Frame Format

- LoRaWAN utilizes six MAC message types.
- LoRaWAN devices use join request and join accept messages for over-the-air (OTA) activation and joining the network.
- The other message types are unconfirmed data up/down and confirmed data up/down.
- A "confirmed" message is one that must be acknowledged, and "unconfirmed" signifies that the end device does not need to acknowledge.
- Uplink messages are sent from endpoints to the network server.
- Downlink messages flow from the network server to a single endpoint and are relayed by only a single gateway

LoRaWAN endpoints are uniquely addressable through a variety of methods.

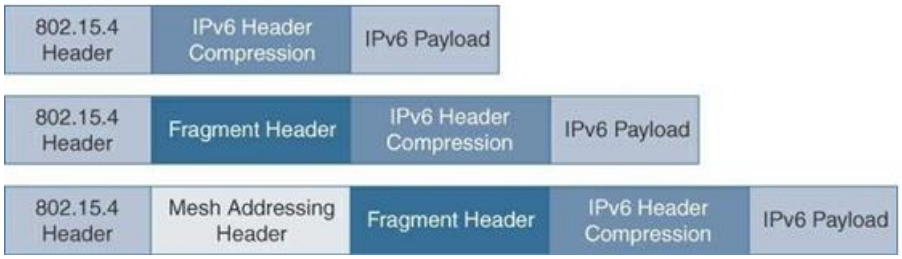
- An endpoint can have a global end device ID or DevEUI represented as an IEEE EUI-64 address.

- An endpoint can have a global application ID or AppEUI represented as an IEEE EUI-64 address that uniquely identifies the application provider.
- In a LoRaWAN network, endpoints are also known by their end device address, known as a DevAddr, a 32-bit address.
- DevAddr= 7 bits network identifier (NwkID) + 25 bits network address (NwkAddr)

3. Design a 6LoWPAN protocol header compression and fragmentation.

- 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***.

Figure shows some examples of typical 6LoWPAN header stacks



Header Compression:

- It shrinks IPv6's 40-byte headers and UDP's 8- byte headers to **6 bytes** in some cases.
- Figure highlights an example that shows the amount of reduction that is possible with 6LoWPAN header compression.

4. Illustrate the routing protocol for low power and lossy networks with a neat diagram

- RPL is based on the concept of a directed acyclic graph (DAG).
- A DAG is a directed graph where no cycles exist.
- All of the edges are arranged in paths oriented toward and terminating at one or more root nodes.
- Figure shows a basic DAG
-

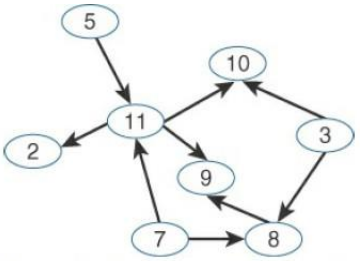
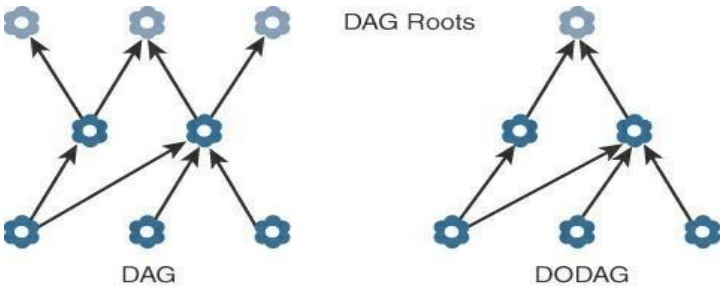


Figure 5-8 Example of a Directed Acyclic Graph (DAG)

- A basic RPL process involves building a destination-oriented directed acyclic graph (DODAG).
- A DODAG is a DAG rooted to 1 destination.
- In RPL, this destination occurs at a border router known as the DODAG root.
- Figure compares a DAG and a DODAG.
- From figure a DAG has multiple roots, whereas the DODAG has just one.



- As illustrated in Figure DAO and DIO messages move both up and down the DODAG, depending on the exact message type.

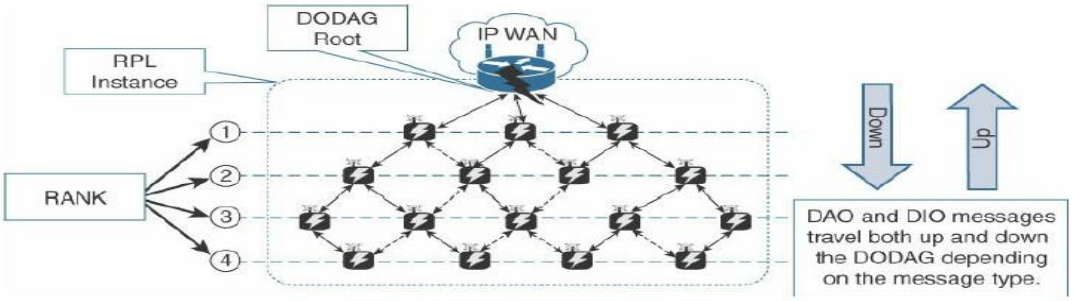


Figure 5-10 RPL Overview

Objective Function (OF)

- It defines how metrics are used to select routes and establish a node's rank
- Whenever a node establishes its rank, it simply sets the rank to the current Minimum Expected Number of Transmissions (METX) among its parents.

Rank

- The rank is a rough approximation of how "close" a node is to the root.
- It helps avoid routing loops and the count-to-infinity problem.
- Nodes can only increase their rank when receiving a DIO message with a larger version number.

5 (a) Explain key advantages of IP suite for IoT.

- Key Advantages of IP :
- Open and standards-based
- Versatile
- Ubiquitous
- Scalable
- Manageable and highly secure
- Stable and resilient
- Consumers' market adoption
- The innovation factor

B) Describe the raw tunneling of SCADA using different scenarios

Supervisory Control and Data Acquisition (SCADA)

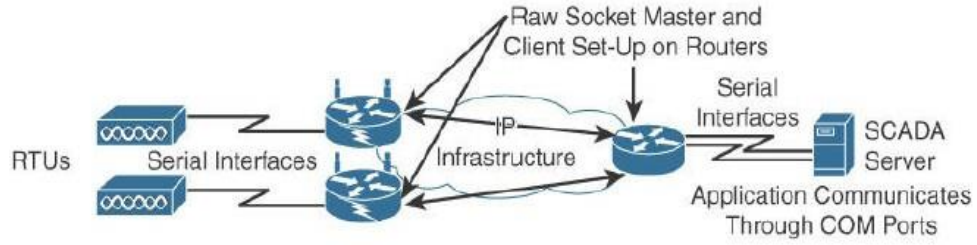
- Its Automation control system, implemented without IP over serial links.
- SCADA systems collect sensor data and telemetry from remote devices, while also providing the ability to control them.
- SCADA networks can be found across various industries.

SCADA commonly uses certain protocols for communications between devices and applications

- Transport of the original serial protocol over IP can be achieved either by tunneling using raw sockets over TCP or UDP or by installing an intermediate device.
- Intermediate device may perform protocol translation between the serial protocol version and its IP implementation.
- A raw socket connection simply denotes that the serial data is being packaged directly into a TCP or UDP transport.

- A socket in this instance is a standard application programming interface (API) composed of an IP address and a TCP or UDP port that is used to access network devices over an IP network.
- Figures next detail raw socket scenarios for a legacy SCADA server trying to communicate with remote serial devices.
- Both the SCADA server and the remote terminal units (RTUs) have a direct serial connection to their respective routers.
- The routers terminate the serial connections at both ends of the link and use raw socket encapsulation to transport the serial payload over the IP network.

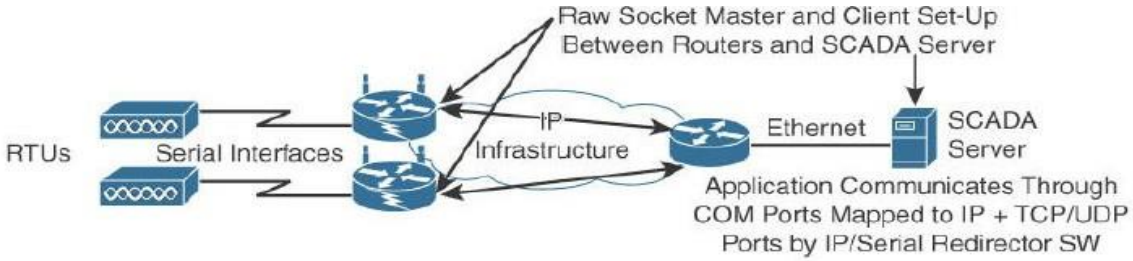
NOTE: An RTU is a multipurpose device used to monitor and control various systems, applications, and devices managing automation



Scenario A: Raw Socket between Routers – no change on SCADA server

- **A piece of software is installed on the SCADA server that maps the serial COM ports to IP ports.**
- **This software is commonly referred to as an IP/serial redirector.**

The IP/serial redirector in essence terminates the serial connection of the SCADA server and converts it to a TCP/IP port using a raw socket connection



Scenario B: Raw Socket between Router and SCADA Server – no SCADA application change on server but IP/Serial Redirector software and Ethernet interface to be added

6 a) Discuss the following with neat diagram I)COAP II)MQTT

- The CoAP messaging model is primarily designed to facilitate the exchange of messages over UDP between endpoints, including the secure transport protocol Datagram Transport Layer Security (DTLS).
- CoAP message format, delivers low overhead while decreasing parsing complexity.
- It allows CoAP to deliver low overhead, which is critical for constrained networks, while also being easy to parse and process for constrained devices.

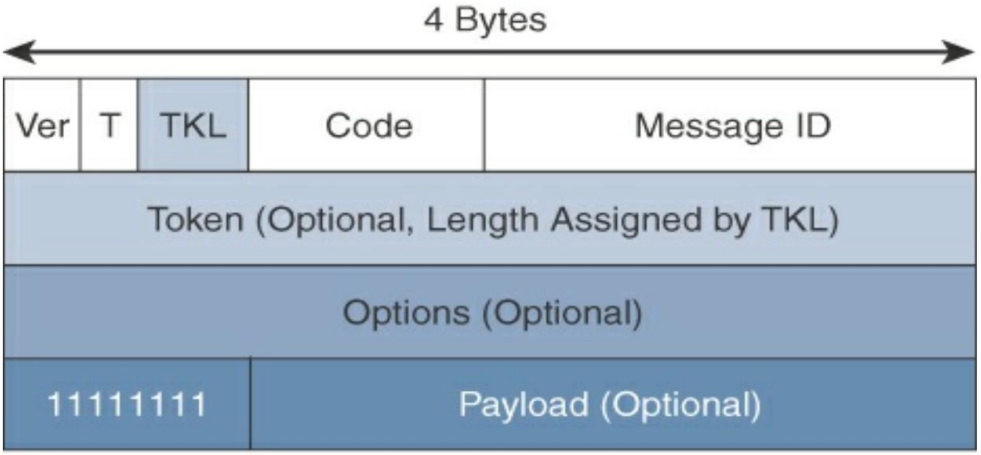


Figure 6-7 CoAP Message Format

ii)MQTT

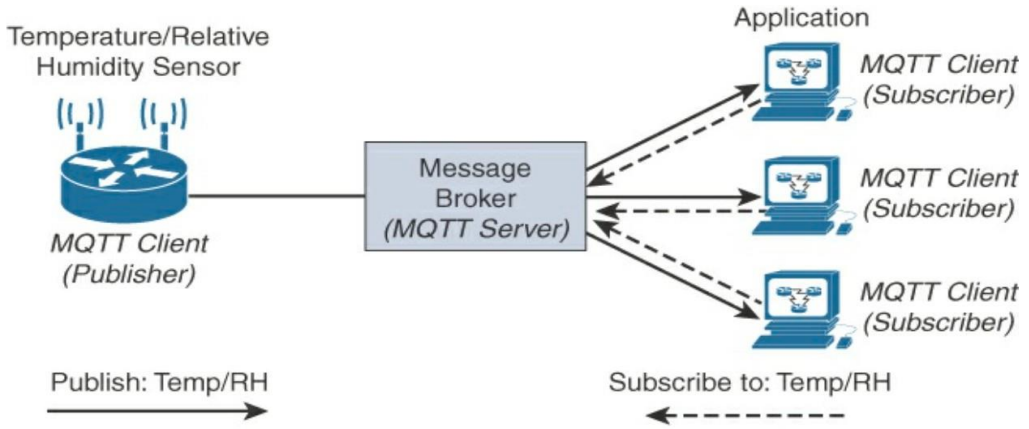


Figure 6-10 MQTT Publish/Subscribe Framework

6 b) Define DAG.

A DAG is a directed graph where no cycles exist.