USN | | | | | | | | | | |

Internal Assessment Test 1 – March 2019

Sub:	Internet of Things Technology					Sub Code:	15CS81	Branch:	CSE	
Date:	/4/2019	Duration:	90 min's	Max Marks:	50	Sem / Sec:	VIII A, B and C		OBE	

Answer any FIVE FULL Questions

		MARKS	CO	RBT
1 (a)	Explain ZigBee and ZigBee IP protocols Mention the drawback of Zigbee compared to ZigBee IP	[10]	CO2	L2
2 (a)	Explain LoRaWAN protocol with respect to layers, MAC frame headers and security	[10]	CO2	L2
3 (a)	List any FIVE key advantages of Internet Protocol Also, describe the need for optimization of IP for IoT	[10]	CO3	L1
4 (a)	How to optimize IP for IoT? Explain using 6LoWPAN protocol	[10]	CO3	L2
5 (a)	Write a short note on RPL and SCADA protocols	[10]	CO3	L2
6(a)	Distinguish between MQTT and CoAP protocols Also analyze message format for each of them	[10]	CO3	L3
7(a)	Write a short note on (i) IEEE 802 11ah (ii) NB-IoT	[10]	CO3	L2

USN | | | | | | | | | | |

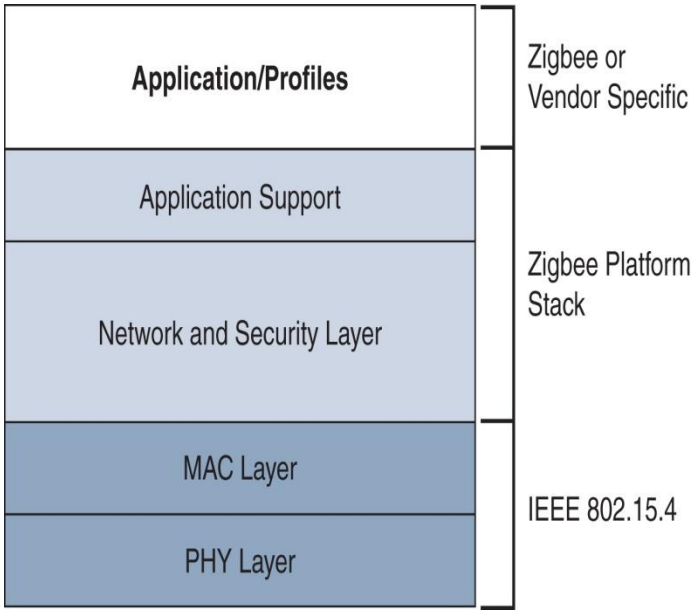
Internal Assessment Test 1 – September 2018

Sub:	Internet of Things Technology					Sub Code:	15CS81	Branch:	CSE	
Date:	/3/2019	Duration:	90 min's	Max Marks:	50	Sem / Sec:	VIII A, B and C		OBE	

Answer any FIVE FULL Questions

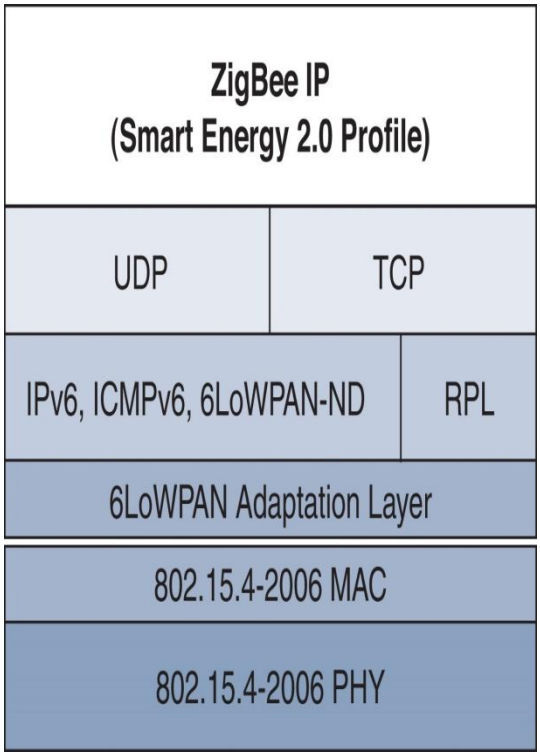
		MARKS	CO	RBT
1 (a)	Explain ZigBee and ZigBee IP protocols Mention the drawback of Zigbee compared to ZigBee IP	[10]	CO2	L2
2 (a)	Explain LoRaWAN protocol with respect to layers, MAC frame headers and security	[10]	CO2	L2
3 (a)	List any FIVE key advantages of Internet Protocol Also, describe the need for optimization of IP for IoT	[10]	CO3	L1
4 (a)	How to optimize IP for IoT? Explain using 6LoWPAN protocol	[10]	CO3	L2
5 (a)	Write a short note on RPL and SCADA protocols	[10]	CO3	L2
6(a)	Distinguish between MQTT and CoAP protocols Also analyze message format for each of them	[10]	CO3	L3
7(a)	Write a short note on (i) IEEE 802 11ah (ii) NB-IoT	[10]	CO3	L2

1. Explain ZigBee and ZigBee IP protocols Mention the drawback of Zigbee compared to ZigBee IP



Zigbee is a wireless technology developed as an open global standard to address the unique needs of low-cost, low-power wireless IoT networks The Zigbee standard operates on the IEEE 802 15 4 physical radio specification and operates in unlicensed bands including 2 4 GHz, 900 MHz and 868 MHz

Zigbee is an IEEE 802 15 4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios, such as for home automation, medical device data collection, and other low-power low-bandwidth needs, designed for small scale projects which need wireless connection Hence, Zigbee is a low-power, low data rate, and close proximity (i e , personal area) wireless ad hoc network The technology defined by the Zigbee specification is intended to be simpler and less expensive than other wireless personal area networks (WPANs), such as Bluetooth or more general wireless networking such as Wi-Fi Applications include wireless light switches, home energy monitors, traffic management systems, and other consumer and industrial equipment that requires short-range low-rate wireless data transfer Its low power consumption limits transmission distances to 10–100 meters line-of-sight, depending on power output and environmental characteristics Zigbee devices can transmit data over long distances by passing data through a mesh network of intermediate devices to reach more distant ones Zigbee is typically used in low data rate applications that require long battery life and secure networking (Zigbee networks are secured by 128 bit symmetric encryption keys) Zigbee has a defined rate of 250 kbit/s, best suited for intermittent data transmissions from a sensor or input device Zigbee was conceived in 1998, standardized in 2003, and revised in 2006 The name refers to the waggle dance of honey bees after their return to the beehive

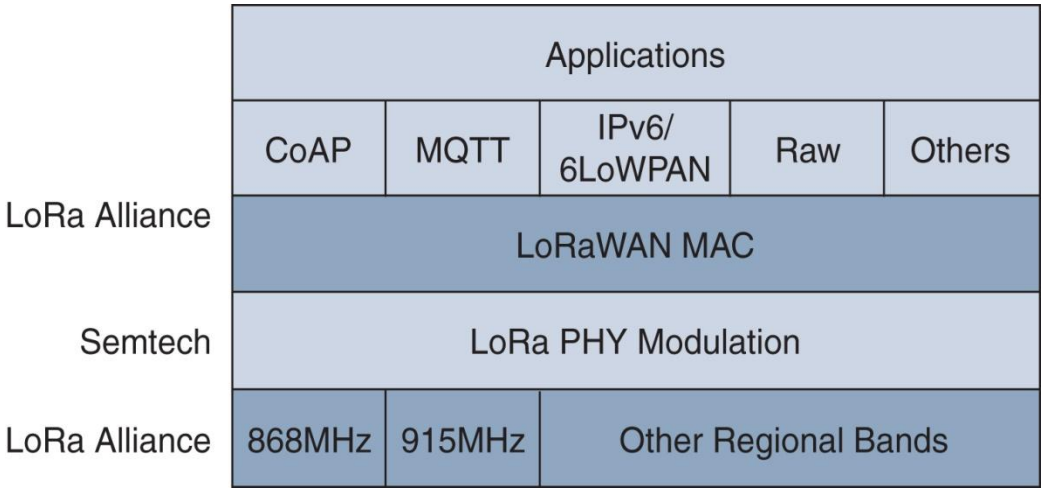


The main functions of the network layer are to enable the correct use of the MAC sublayer and provide a suitable interface for use by the next upper layer, namely the application layer Its capabilities and structure are those typically associated to such network layers, including routing The Network Layer 's function is exactly as it sounds It deals with network functions such as connecting, disconnecting, and setting up networks It will add a network, allocate addresses, and add/remove certain devices This layer makes use of star, mesh and tree topologies It adds an interface to the application layer On the one hand, the data entity creates and manages network layer data units from the payload of the application-layer and performs routing according to the current topology On the other hand, there is the layer control, which is used to handle configuration of new devices and establish new networks: it can determine whether a neighboring device belongs to the network and discovers new neighbors and routers The control can also detect the presence of a receiver, which allows direct communication and MAC synchronization The routing protocol used by the network layer is AODV [33] In AODV, to find the destination device, AODV broadcasts out a route request to all of its neighbors The neighbors then broadcast the request to their neighbors and onward until the destination is reached Once the destination is reached, it sends its route reply via unicast transmission following the lowest cost path back to the source Once the source receives the reply, it will update its routing table for the destination address of the next hop in the path and the path cost Application layer The application layer is the highest-level layer defined by the specification and is the effective interface of the Zigbee system to its end users It comprises the majority of components added by the Zigbee specification: both ZDO and its management procedures,

together with application objects defined by the manufacturer, are considered part of this layer This layer binds tables, sends messages between bound devices, manages group addresses, reassembles packets and also transports data It is responsible for providing service to Zigbee device profiles Main components The ZDO (Zigbee Device Object), a protocol in the Zigbee protocol stack, is responsible for overall device management, security keys, and policies It is responsible for defining the role of a device as either coordinator or end device, as mentioned above, but also for the discovery of new (one-hop) devices on the network and the identification of their offered services It may then go on to establish secure links with external devices and reply to binding requests accordingly The application support sublayer (APS) is the other main standard component of the layer, and as such it offers a well-defined interface and control services It works as a bridge between the network layer and the other elements of the application layer: it keeps up-to-date binding tables in the form of a database, which can be used to find appropriate devices depending on the services that are needed and those the different devices offer As the union between both specified layers, it also routes messages across the layers of the protocol stack

2. Explain LoRaWAN protocol with respect to layers, MAC frame headers and security

LoRa (Long Range) is a patented digital wireless data communication technology developed by Cycleo of Grenoble, France, and acquired by Semtech in 2012LoRa is a long-range wireless communication protocol that competes against other low-power wide-area network (LPWAN) wireless such as narrowband IoT (NB IoT) or LTE Cat M1 Compared to those, LoRa achieves its extremely long range connectivity, possible 10km+, by trading off data rate Because its data rates are below 50kbps and because LoRa is limited by duty cycle and other restrictions, it is suitable in practice for non-real time applications in which one can tolerate delay

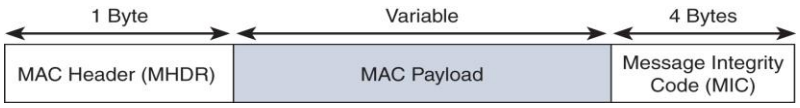


oRa uses license-free sub-gigahertz radio frequency bands like 169 MHz, 433 MHz, 868 MHz (Europe) and 915 MHz (North America) LoRa enables long-range transmissions (more than 10

km in rural areas) with low power consumption [4] The technology is presented in two parts: LoRa, the physical layer and LoRaWAN (Long Range Wide Area Network), the upper layers

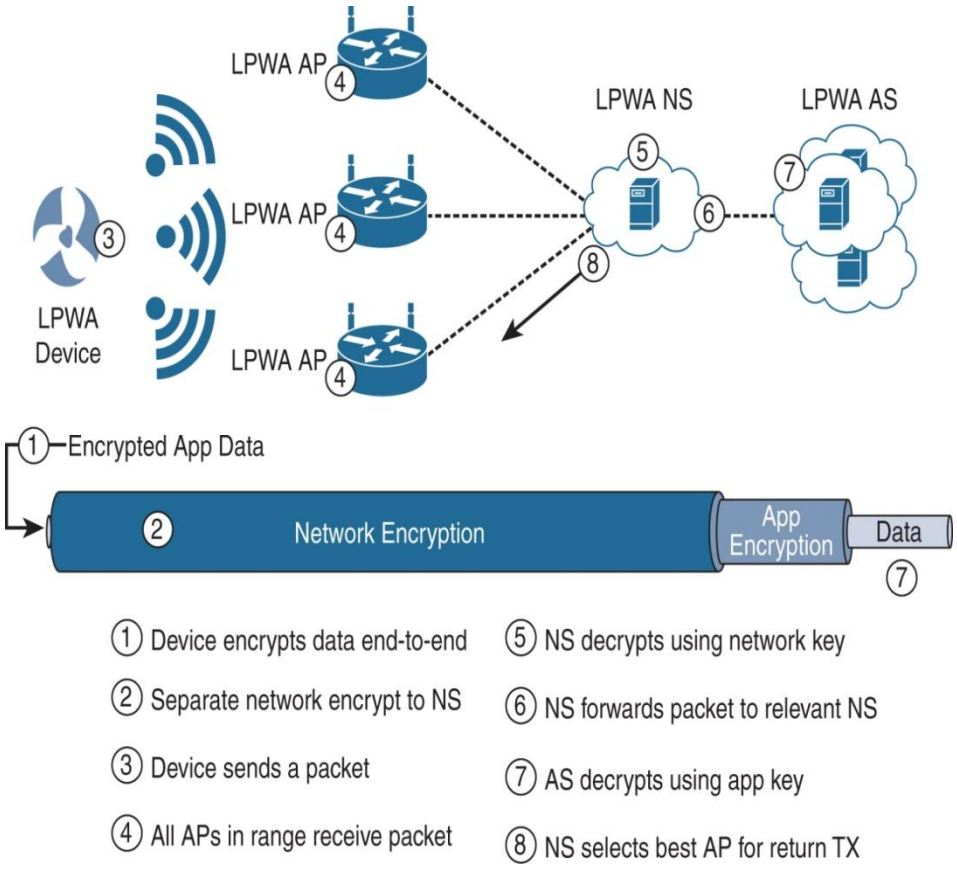
LoRa is a spread spectrum modulation technique derived from chirp spread spectrum (CSS) technology, and is the first low-cost implementation of chirp spread spectrum for commercial usage [5] In January 2018, new LoRa chipsets were announced, with reduced power consumption, increased transmission power, and reduced size compared to older generation [6] LoRa devices have geolocation capabilities used for triangulating positions of devices via timestamps from gateways [7] LoRa and LoRaWAN permit long-range connectivity for Internet of Things (IoT) devices in different types of industries [8]

Figure 4.16 - High-Level LoRaWAN MAC Frame Format



LoRa PHY The LoRa physical layer protocol is proprietary; therefore, there is no freely available official documentation However, several people have analyzed it and documented their findings and Semtech has provided an overview of the modulation and other relevant technical specifications [9][10] LoRa uses a proprietary spread spectrum modulation that is similar to and a derivative of Chirp Spread Spectrum modulation (CSS) [11] This allows LoRa to trade off data rate for sensitivity with a fixed channel bandwidth by selecting the amount of spread used (a selectable radio parameter from 7 to 12) This spreading factor determines the data rate and dictates the sensitivity of a radio In addition, LoRa uses Forward Error Correction coding to improve reselience against interference LoRa's high range is characterized by extremely high wireless link budgets, around 155 dB to 170 dB [12] LoRaWAN Since LoRa defines the lower physical layer, the upper networking layers were lacking LoRaWAN was developed to define the upper layers of the network LoRaWAN is a media access control (MAC) layer protocol but acts mainly as a network layer protocol for managing communication between LPWAN gateways and end-node devices as a routing protocol, maintained by the LoRa Alliance Version 1 0 of the LoRaWAN specification was released in June 2015 [13]

LoRaWAN defines the communication protocol and system architecture for the network, while the LoRa physical layer enables the long-range communication link LoRaWAN is also responsible for managing the communication frequencies, data rate, and power for all devices [14] Devices in the network are asynchronous and transmit when they have data available to send Data transmitted by an end-node device is received by multiple gateways, which forward the data packets to a centralized network server [15] The network server filters duplicate packets, performs security checks, and manages the network [16] Data is then forwarded to application servers [17] The technology shows high reliability for the moderate load, however, it has some performance issues related to sending acknowledgements [18]



3. List any FIVE key advantages of Internet Protocol Also, describe the need for optimization of IP for IoT

   Advantages of IP

   a. Open and standards based
   b. Versatile
   c. Ubiquitous
   d. Scalable
   e. Manageable and highly secure
   f. Stable and resilient
   g. Consumers marker adoption

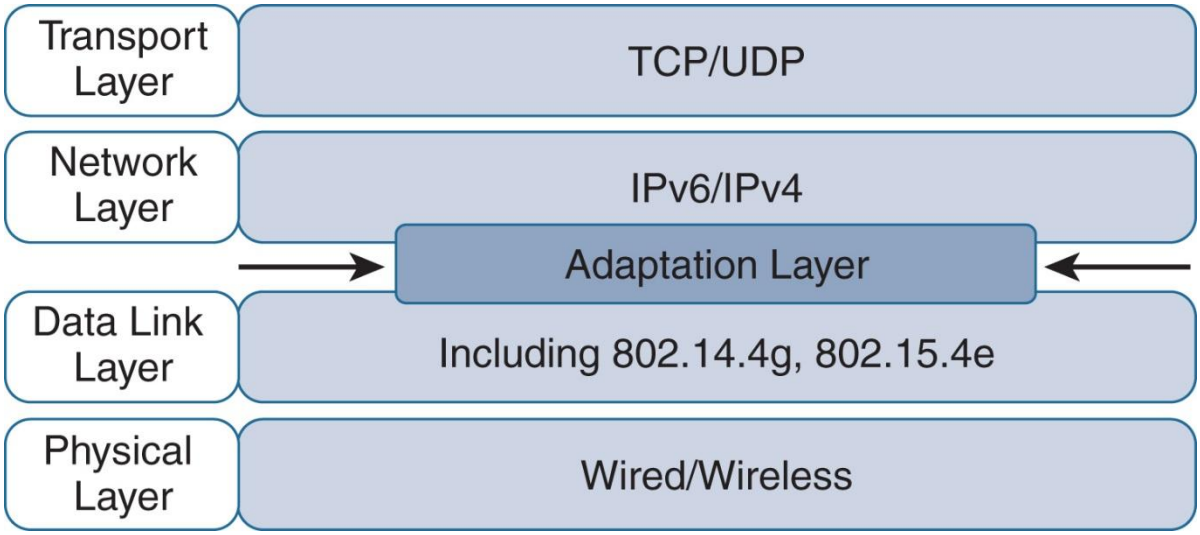
h. The innovation factor

Need for Optimization:

I. Constrained nodes
II. constrained networks
III. IP versions

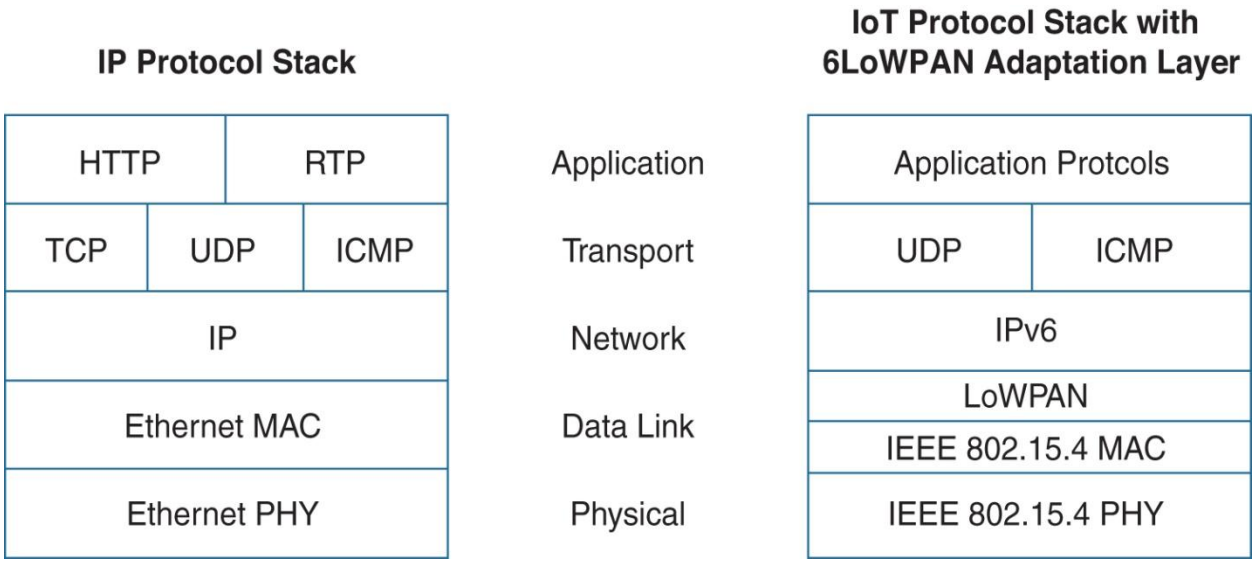
4. How to optimize IP for IoT? Explain using 6LoWPAN protocol

Optimizing IP for IoT Using an Adaptation Layer

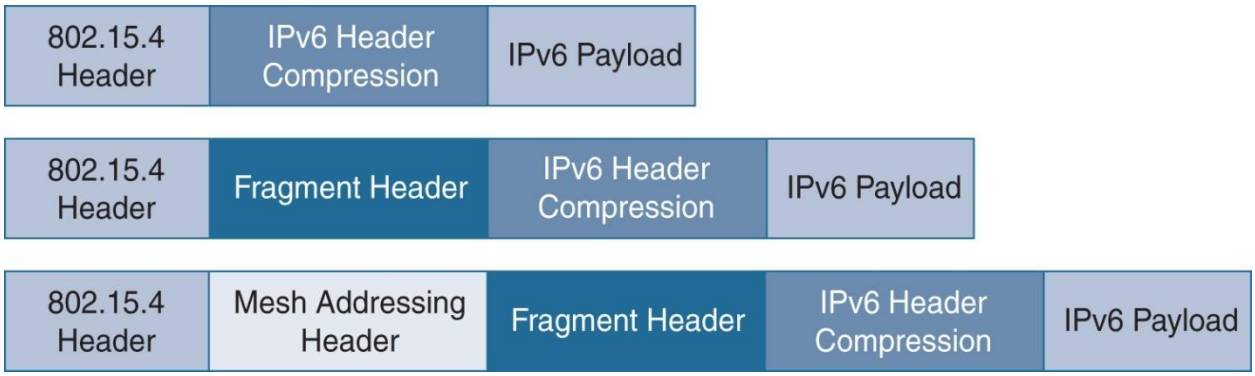


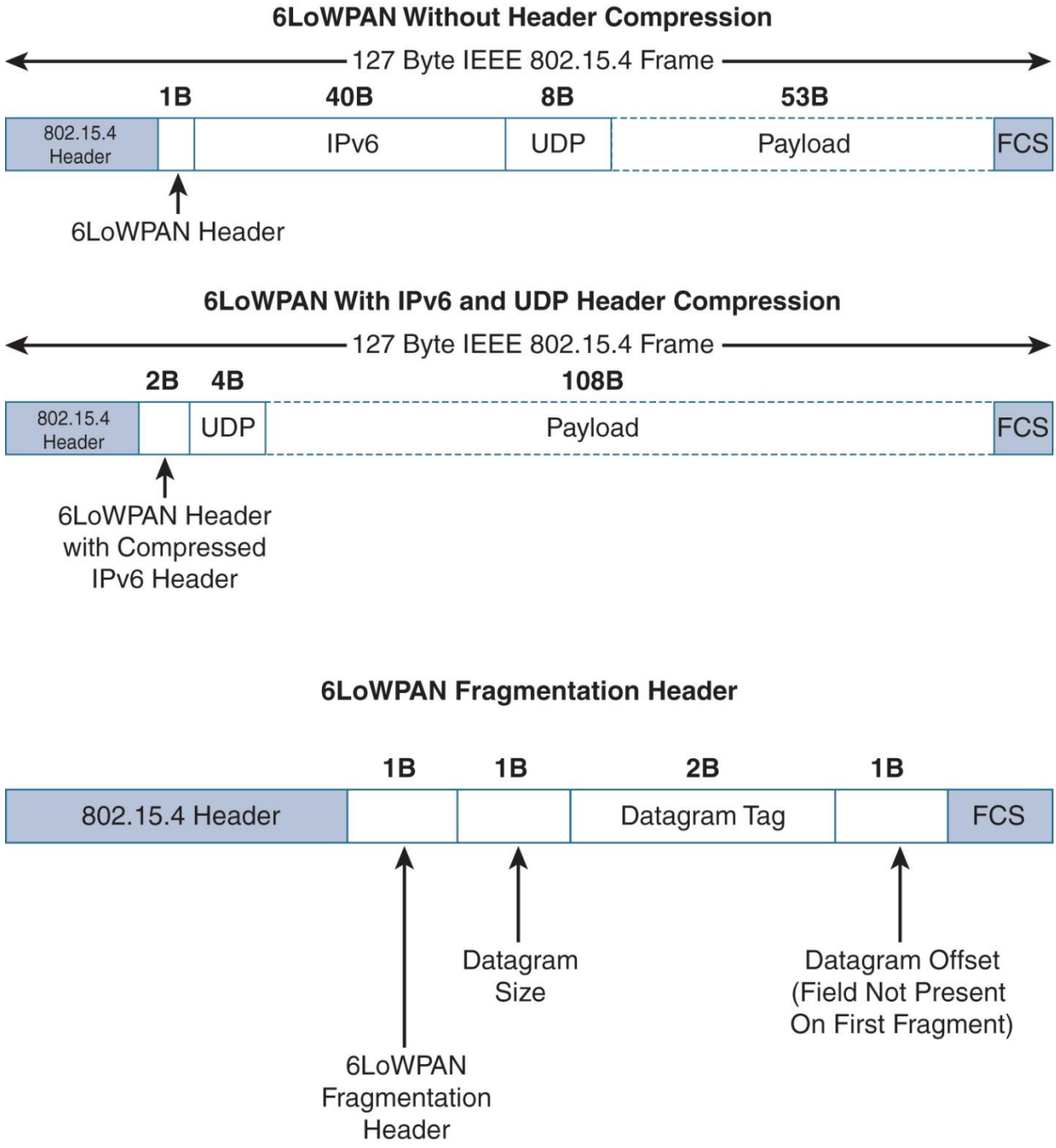
6LoWPAN is an acronym of IPv6 over Low-Power Wireless Personal Area Networks 6LoWPAN is the name of a concluded working group in the Internet area of the IETF The 6LoWPAN concept originated from the idea that "the Internet Protocol could and should be applied even to the smallest devices," and that low-power devices with limited processing capabilities should be able to participate in the Internet of Things [4] The 6LoWPAN group has defined encapsulation and header compression mechanisms that allow IPv6 packets to be sent and received over IEEE 802 15 4 based networks IPv4 and IPv6 are the work horses for data delivery for local-area networks, metropolitan area networks, and wide-area networks such as the Internet Likewise, IEEE 802 15 4 devices provide sensing communication-ability in the wireless domain The inherent natures of the two networks though, are different The base specification developed by the 6LoWPAN IETF group is RFC 4944 (updated by RFC 6282 with header compression, and by RFC 6775 with neighbor discovery optimizations) The problem statement document is RFC 4919 IPv6 over Bluetooth Low Energy (BLE) is defined in RFC 7668

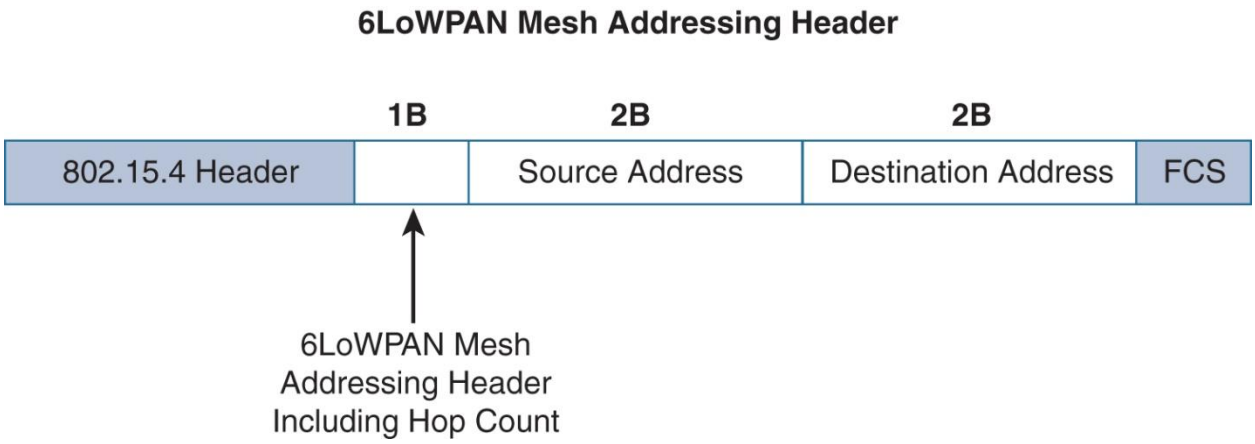
Comparison of an IoT Protocol Stack Utilizing 6LoWPAN and an IP Protocol Stack



6LoWPAN Header Stacks




6LoWPAN Without Header Compression
127 Byte IEEE 802.15.4 Frame
1B
40B
8B
53B
802.15.4 Header
IPv6
UDP
Payload
FCS
6LoWPAN Header
6LoWPAN With IPv6 and UDP Header Compression
127 Byte IEEE 802.15.4 Frame
2B
4B
108B
802.15.4 Header
UDP
Payload
FCS
6LoWPAN Header with Compressed IPv6 Header
6LoWPAN Fragmentation Header
1B
1B
2B
1B
802.15.4 Header
Datagram Tag
FCS
Datagram Size
Datagram Offset (Field Not Present On First Fragment)
6LoWPAN Fragmentation Header



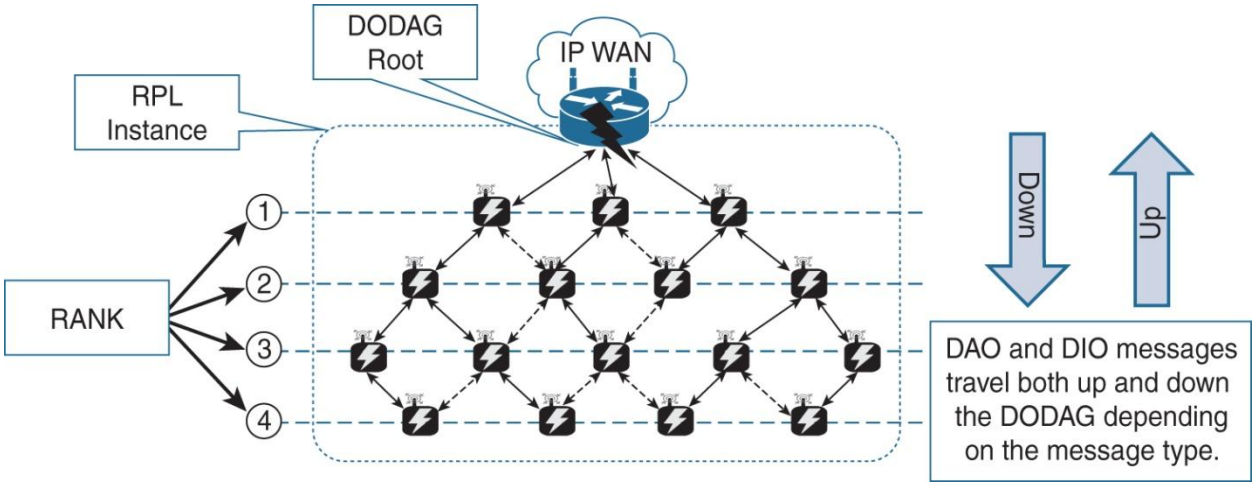
As with all link-layer mappings of IP, RFC4944 provides a number of functions Beyond the usual differences between L2 and L3 networks, mapping from the IPv6 network to the IEEE 802 15 4 network poses additional design challenges (see RFC 4919 for an overview) Adapting the packet sizes of the two networks IPv6 requires the maximum transmission unit (MTU) to be at least 1280 octets In contrast, IEEE 802 15 4's standard packet size is 127 octets A maximum frame overhead of 25 octets spares 102 octets at the media access control layer An optional but highly recommended security feature at the link layer poses an additional overhead For example, 21 octets are consumed for AES-CCM-128 leaving only 81 octets for upper layers Address resolution IPv6 nodes are assigned 128 bit IP addresses in a hierarchical manner, through an arbitrary length network prefix IEEE 802 15 4 devices may use either of IEEE 64 bit extended addresses or, after an association event, 16 bit addresses that are unique within a PAN There is also a PAN-ID for a group of physically collocated IEEE 802 15 4 devices Differing device designs IEEE 802 15 4 devices are intentionally constrained in form factor to reduce costs (allowing for large-scale network of many devices), reduce power consumption (allowing battery powered devices) and allow flexibility of installation (e g small devices for body-worn networks) On the other hand, wired nodes in the IP domain are not constrained in this way; they can be larger and make use of mains power supplies Differing focus on parameter optimization IPv6 nodes are geared towards attaining high speeds Algorithms and protocols implemented at the higher layers such as TCP kernel of the TCP/IP are optimized to handle typical network problems such as congestion In IEEE 802 15 4-compliant devices, energy conservation and code-size optimization remain at the top of the agenda Adaptation layer for interoperability and packet formats An adaptation mechanism to allow interoperability between IPv6 domain and the IEEE 802 15 4 can best be viewed as a layer problem Identifying the functionality of this layer and defining newer packet formats, if needed, is an enticing research area RFC 4944 proposes an adaptation layer to allow the transmission of IPv6 datagrams over IEEE 802 15 4 networks Addressing management mechanisms The management of addresses for devices that communicate across the two dissimilar domains of IPv6 and IEEE 802 15 4 is cumbersome, if not exhaustingly complex Routing

considerations and protocols for mesh topologies in 6LoWPAN Routing per se is a two phased problem that is being considered for low-power IP networking: Mesh routing in the personal area network (PAN) space The routability of packets between the IPv6 domain and the PAN domain Several routing protocol have been proposed by the 6LoWPAN community such as LOAD,[9] DYMO-LOW,[10] HI-LOW [11] However, only two routing protocols are currently legitimate for large-scale deployments: LOADng[12] standardized by the ITU under the recommendation ITU-T G 9903 and RPL[13] standardized by the IETF ROLL working group [14] Device and service discovery Since IP-enabled devices may require the formation of ad hoc networks, the current state of neighboring devices and the services hosted by such devices will need to be known IPv6 neighbour discovery extensions is an internet draft proposed as a contribution in this area Security IEEE 802 15 4 nodes can operate in either secure mode or non-secure mode Two security modes are defined in the specification in order to achieve different security objectives: Access Control List (ACL) and Secure mode

5. Write a short note on RPL and SCADA protocols

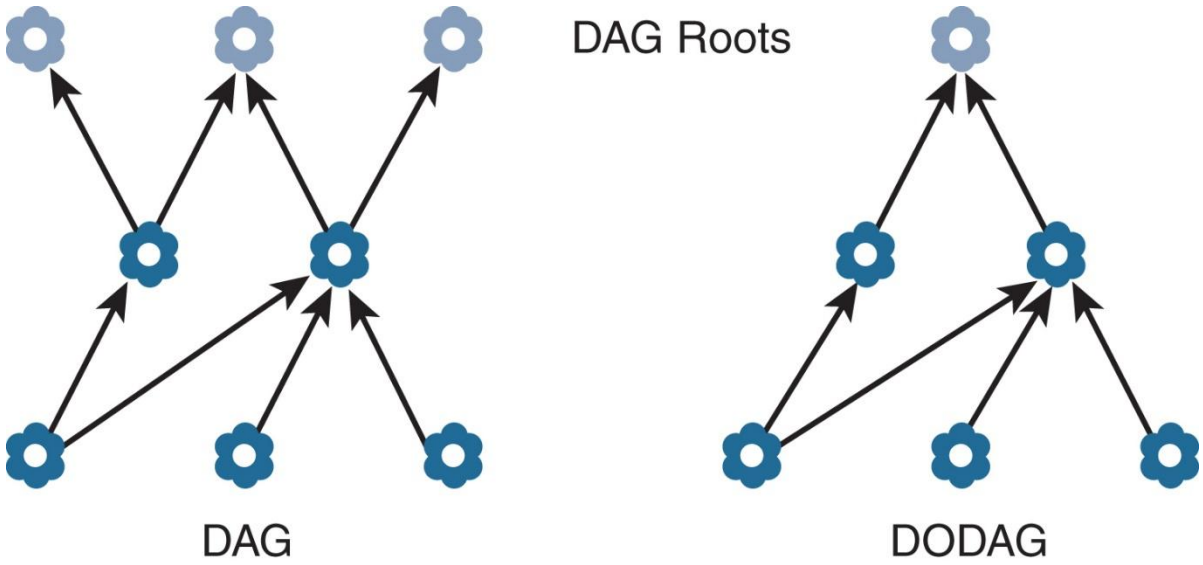
RPL:

RPL (Routing Protocol for Low-Power and Lossy Networks) is a routing protocol for wireless networks with low power consumption and generally susceptible to packet loss It is a proactive protocol based on distance vectors and opera on IEEE 802 15 4 , optimized for multi-hop and many-to-one communication, but also supports one-to-one messages This protocol is specified in RFC 6550 with special applications in RFCs 5867, 5826, 5673 and 5548 RPL can support a wide variety of link layers, including those with limitations, with potential losses or that are used in devices with limited resources This protocol can quickly create network routes, share routing knowledge and adapt the topology in an efficient way



RPL creates a topology similar to a tree (DAG or directed acyclic graph) Each node within the network has an assigned rank (Rank), which increases as the teams move away from the

root node (DODAG) The nodes resend packets using the lowest range as the route selection criteria



Three types of packages are defined ICMPv6: DIS (information request DODAG): Used to request information from nearby DODAG, analogous to router request messages used to discover existing networks DIO (object of information of the DAG): Message that shares information from the DAG, sent in response to DIS messages, as well as used periodically to refresh the information of the nodes on the topology of the network DAO (object of update to the destination): Sent in the direction of the DODAG, it is a message sent by the teams to update the information of their "parent" nodes throughout the DAG Implementation of the RPL protocol The implementation of the RPL protocol occurs in wireless sensors and networks, the most used operating system for its implementation is Contiki which is a small open source operating system developed for use in a number of small systems ranging from 8-bit computers to integrated systems on microcontrollers, including sensor network nodes

SCADA:

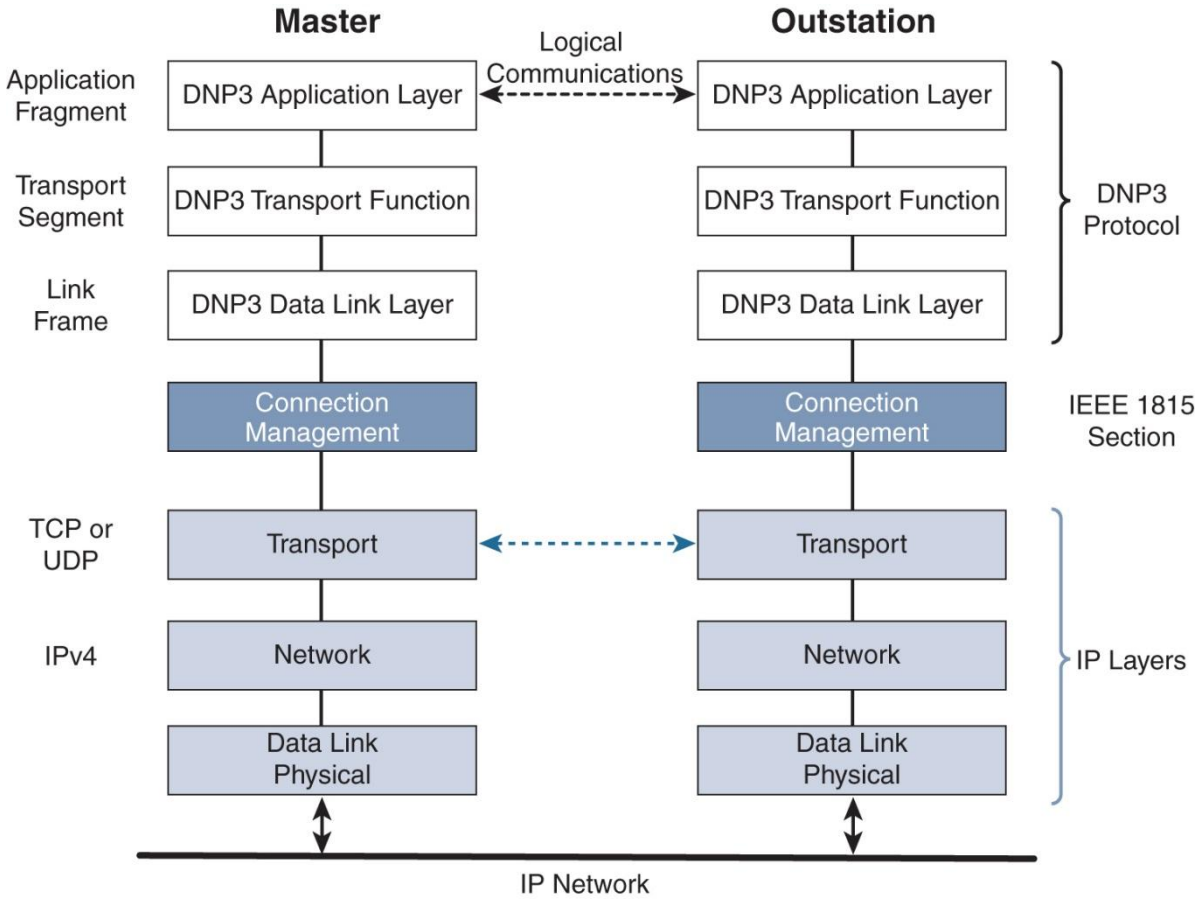
Supervisory control and data acquisition (SCADA) is a system of software and hardware elements that allows industrial organizations to:

- Control industrial processes locally or at remote locations
- Monitor, gather, and process real-time data
- Directly interact with devices such as sensors, valves, pumps, motors, and more through human-machine interface (HMI) software
- Record events into a log file

SCADA systems are crucial for industrial organizations since they help to maintain efficiency, process data for smarter decisions, and communicate system issues to help mitigate downtime

The basic SCADA architecture begins with programmable logic controllers (PLCs) or remote terminal units (RTUs) PLCs and RTUs are microcomputers that communicate with an array of objects such as factory machines, HMIs, sensors, and end devices, and then route the information from those objects to computers with SCADA software The SCADA software processes, distributes, and displays the data, helping operators and other employees analyze the data and make important decisions

For example, the SCADA system quickly notifies an operator that a batch of product is showing a high incidence of errors The operator pauses the operation and views the SCADA system data via an HMI to determine the cause of the issue The operator reviews the data and discovers that Machine 4 was malfunctioning The SCADA system's ability to notify the operator of an issue helps him to resolve it and prevent further loss of product



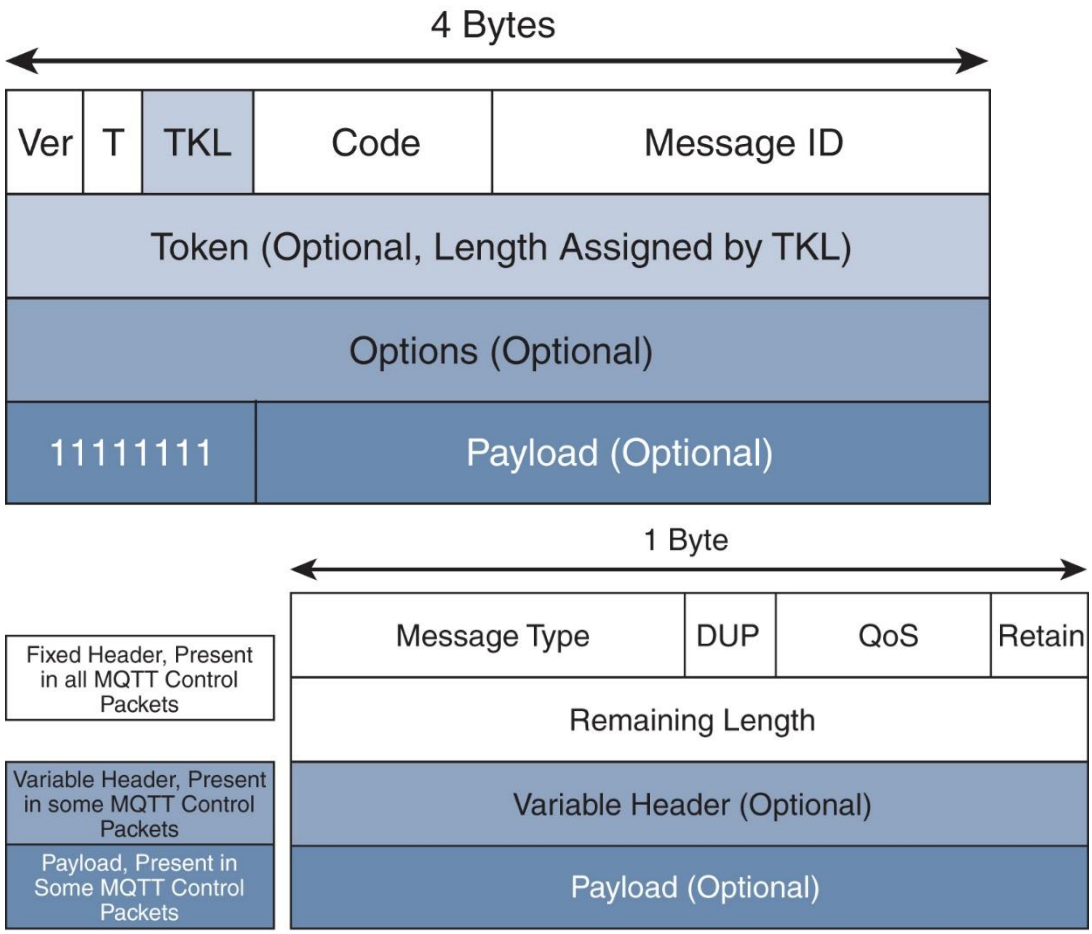
DNP3 is a communications protocol used in SCADA and remote monitoring systems It is widely used because it is an open protocol, meaning any manufacturer can develop DNP3 equipment that is compatible with other DNP3 equipment

DNP3 is typically used for communication between central Masters and Remotes In a typical network, the Remotes gather status information from mission critical gear Any time there is an alarm, that information is pushed up to the Master via DNP3 for appropriate action

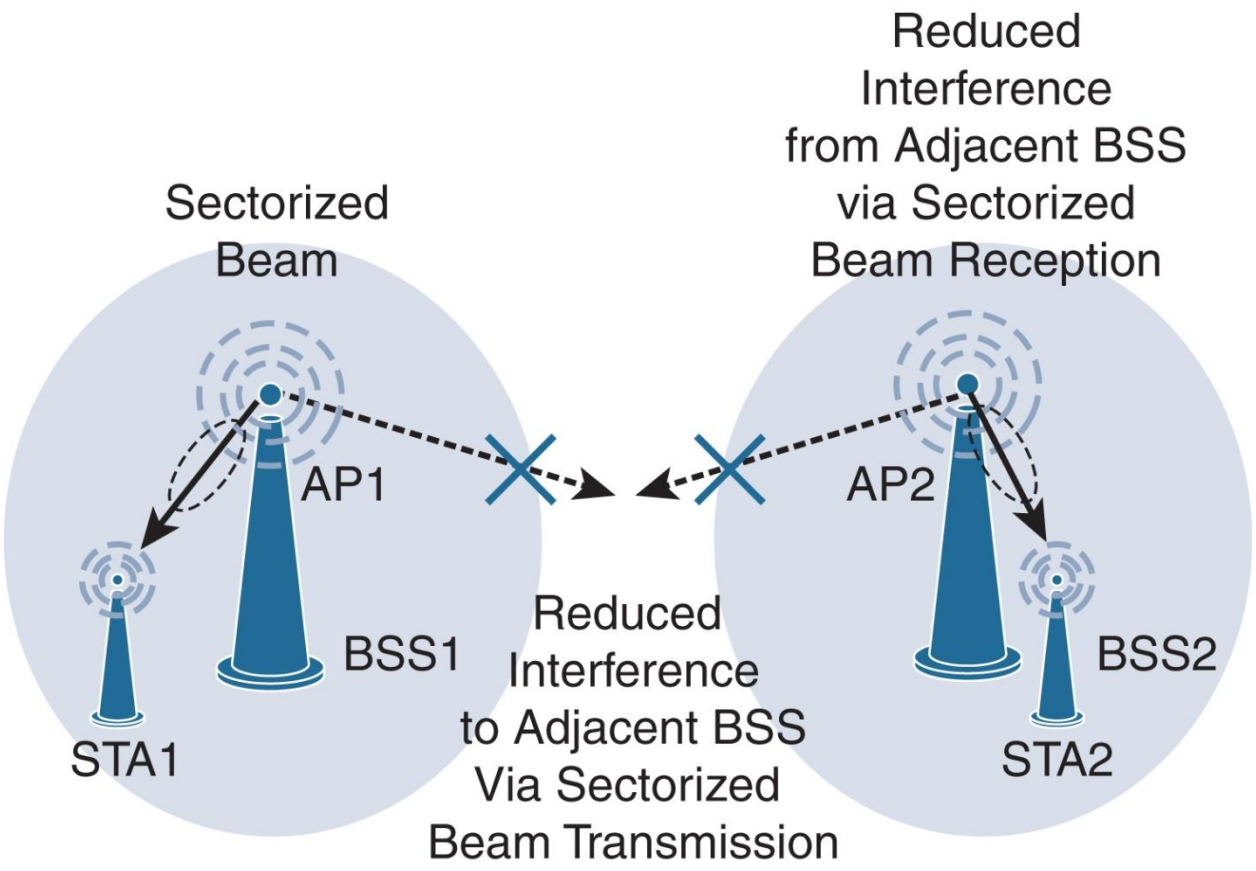
6. Distinguish between MQTT and CoAP protocols Also analyze message format for each of them

Table 6-3 *Comparison Between CoAP and MQTT*

Factor	CoAP	MQTT
Main transport protocol	UDP	TCP
Typical messaging	Request/response	Publish/subscribe
Effectiveness in LLNs	Excellent	Low/fair (Implementations pairing UDP with MQTT are better for LLNs.)
Security	DTLS	SSL/TLS
Communication model	One-to-one	many-to-many
Strengths	Lightweight and fast, with low overhead, and suitable for constrained networks; uses a RESTful model that is easy to code to; easy to parse and process for constrained devices; support for multicasting; asynchronous and synchronous messages	TCP and multiple QoS options provide robust communications; simple management and scalability using a broker architecture
Weaknesses	Not as reliable as TCP-based MQTT, so the application must ensure reliability.	Higher overhead for constrained devices and networks; TCP connections can drain low-power devices; no multicasting support



7. Write a short note on (i) IEEE 802 11ah (ii) NB-IoT



IEEE 802 11ah is a Wi-Fi standard that has been designed to utilize the sub one GHz licence free ISM bands The radio propagation at these frequencies means that the signals are able to travel greater distances and this opens up opportunities for uses with the Internet of Things where sensors and control nodes may be located further apart The bands at these frequencies are much smaller than the 2,4GHz and 5GHz bands normally used for Wi-Fi and this limits the data rates that can be pushed over the links To accommodate the different aspects of sub GHz Wi-Fi a new physical layer and MAC has been developed to enable communications in these frequencies, albeit at a lower speed than that which is achievable for the main stream very high speed Wi-Fi variants IEEE 802 11ah sub GHz Wi-Fi basics The IEEE 802 11ah standard is aimed at providing a global Wireless LAN, WLAN standard that operates within the unlicensed ISM, Industrial, Scientific, and Medical, bands that are available below 1 GHz In this way IEEE 802 11ah will allow Wi-Fi-enabled devices to gain access for short-term transmissions in these frequency bands that are currently much less congested In addition to gaining access to additional spectrum, the use of 802 11ah will provide improved coverage range because of the propagating characteristics of these frequencies This will open the applications of available to IEEE 802 11ah users to new opportunities including wide area based sensor networks, sensor backhaul systems and potential Wi-Fi off-loading ISM bands available There are several ISM bands that are available for use by IEEE 802 11ah that exist below 1GHz These are not globally available, but suitable bands do appear in most areas of the globe ISM ALLOCATIONS APPLICABLE FOR IEEE 802 11AH COUNTRY BAND LIMITS (MHZ) China 755 - 787 Europe 863 - 868 Japan 916 5 - 927 5 Korea 917 5 - 923 5 Singapore

866 - 869 & 920 - 925 USA 902 - 928 802 11ah channelization IEEE 802 11ah sub GHz Wi-Fi defines the channels based upon the spectrum that is available in a given country The basic channel width is 1MHz, although it is possible to bond two adjacent channels together to form a 2 MHz channel to provide higher data throughput capability Wider channels are available, the widest in the US being 16 MHz for the 902 - 928 MHz ISM band Again this uses the same channel bonding method adopted for 802 11n and 11ac Channel widths of 1, 2, 4, 8, and 16 MHz can be used Other countries have different spectrum allocations and accordingly the channels are on different frequencies, but the same basic methods are used, obviously with different limitations on the maximum number of channels that can be bonded together