T.Y. BSC. (CS): Sem. V (Elective I)

Architecting of IoT

Mumbai University Examination Paper Solution: Nov-22

Q.P. Code:13324

Q1. Attempt All

(a) Multiple choice Questions **[10]**

I. Which domain defines the architecture view of IoT?
- A. Solution domain
- B. Problem domain
- C. system domain
- D. M2M domain

Ans: D. M2M domain

II. Which protocol among the following belongs to the transport layer?
- A. IPv4
- B. DHCP
- C. TCP
- D. CoAP

Ans: C. TCP

III. Z-Wave Network is very efficient, this is because of the _____ protocol it used?
- A. session
- B. Routing
- C. transport
- D. network

Ans: D. network

IV. _____ are a way of limiting the amount of electricity going through a circuit.
- A. resistor
- B. switch
- C. hub
- D. repeater

Ans: A. resistor

V. CoAP has four messaging modes: confirmable, non-confirmable, _____ separate.
- A. protecting
- B. viewing
- C. messaging
- D. piggyback

Ans: D. piggyback

muquestionpapers.com

VI. IoT security management includes _____.

A. Protocol abstraction
B. Simple and fast installation
C. Security with hardware
D. Data storage

Ans: C. Security with hardware

VII. The _____ is the next domain in the WAN-MAN-LAN hierarchy.

A. PAN
B. SAN
C. DAN
D. AAN

Ans: A. PAN

VIII. PPP protocol is also known as _____ Protocol

A. People to people protocol
B. Point to Point
C. Physical to Physical
D. Person to Person

Ans: B. Point to Point

IX. System design and deployment view is a part of _____.

A. Solution domain
B. Analysis domain
C. Functional view
D. Operational view

Ans: D. Operational view

X. In AMQP- the broker is divided into two main components: exchange and _____.

A. queues
B. Devices
C. work
D. delete

Ans: A. queues

(b) Fill in the blanks (underwater, 64, simplex, protocol abstraction, Full-duplex, 128, MAC, Security) [5]

1. In Full duplex communication mode, communication occurs from sender to receiver and receiver to sender at same time.
2. IoT Gateway must provide protocol abstraction.
3. CARP is a distributed routing protocol designed for underwater Communication.
4. IEEE 802.15.4 is the most common used for IoT standard for MAC.
5. IPv6 is 128-bit protocol.

muquestionpapers.com

2. Attempt any three of the following **[15]**

Q2(a) Define the term M2M and discuss its Evolution **(5)**

Ans. 1. M2M, or Machine-to-Machine, refers to the automated communication and interaction between devices or machines without human intervention.

2. This allows machines to exchange data, information, and instructions, enabling seamless connectivity and coordination within various applications and industries.

Evolution of M2M:

- Early Telemetry: M2M's origins can be traced back to the early 20th century when basic telemetry systems were used to remotely monitor and control devices. These early applications were limited to simple sensors and communication technologies like radio and telegraph.
- Emergence of IoT: The term "Internet of Things" gained popularity in the late 1990s and early 2000s, describing a broader vision of interconnected devices and objects with the ability to collect, exchange, and analyze data. IoT expanded the M2M paradigm beyond traditional machine-to-machine interactions and incorporated smart devices, wearables, and more.
- Cloud Computing and Analytics: With the availability of cloud computing and advanced data analytics, M2M capabilities were enhanced. Cloud-based services enabled devices to store and process data, making it easier to manage and access information from anywhere. Data analytics provided valuable insights from the vast amounts of data generated by M2M devices, enabling better decision-making and optimizations.
- Industrial IoT (IoT) and AI Integration: The IoT applied M2M technologies to industrial settings, revolutionizing sectors like manufacturing, energy, and healthcare. Integration of AI and machine learning into M2M systems allowed devices to become smarter and more autonomous, making intelligent decisions without constant human supervision.

3. Overall, M2M's evolution has been driven by advancements in communication technology, computing power, and data analysis, leading to its integration into various industries and the widespread adoption of the Internet of Things.

muquestionpapers.com

Q2(b) What is an Iot Architectural view? discuss reference architecture for an system solution **(5)**

Ans. 1. An IoT (Internet of Things) architectural view refers to the high-level representation of the components, relationships, and interactions within an IoT system.

2. It provides a structured approach to designing and implementing IoT solutions, ensuring scalability, interoperability, and security.

3. The IoT architecture view typically consists of various layers that handle data acquisition, communication, processing, and application interfaces.

4. A reference architecture for an IoT system solution outlines a standardized blueprint or model that serves as a starting point for designing specific IoT applications.

5. It offers best practices and guidelines for building reliable and efficient IoT solutions. Here are the key aspects of a reference architecture for an IoT system solution:

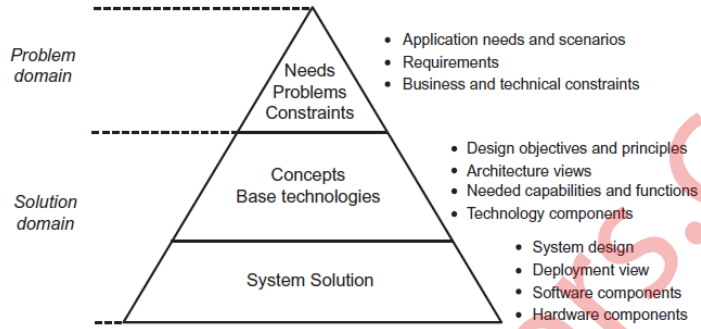
- **Device Layer:** The device layer includes physical IoT devices such as sensors, actuators, and controllers. These devices gather data from the physical world and interact with it through actuators. The reference architecture should cover device management, data collection, and connectivity protocols at this layer.
- **Connectivity Layer:** The connectivity layer facilitates the communication between IoT devices and the central platform. It involves technologies like Wi-Fi, Bluetooth, Zigbee, cellular networks, and Lora WAN. The reference architecture should address communication protocols, data encryption, and authentication methods.
- **Cloud Platform:** The cloud platform serves as the core of the IoT solution, where data from devices is processed, stored, and analysed. It includes data processing engines, databases, and storage solutions. The reference architecture should focus on data management, real-time processing, and scalability.
- **Application Layer:** The application layer provides the user interface and application programming interfaces (APIs) for accessing and interacting with the IoT system. It allows users and other applications to extract valuable insights from the processed data. The reference architecture should cover API design, security, and data visualization.
- **Security and Privacy:** Security is a critical aspect of IoT solutions. The reference architecture should include measures like authentication, authorization, encryption, and secure data transmission to protect against cyber threats and ensure user privacy.

muquestionpapers.com

Q2(c) State and Explain Problem and Solution domain portioning with an example **(5)**

Ans. 1. Problem and solution domain partitioning is a systematic approach to dividing a complex problem into smaller, manageable parts.

2. It helps in understanding and solving the problem more effectively by breaking it down into distinct areas of concern.



4. The problem domain establishes the foundation for the subsequent solutions. It is common to partition the architecture work and solution work into two domains, each focusing on specific issues of relevance at the different levels of abstraction

5. The top level of the triangle is referred to here as the “problem domain” (“domain model” in software engineering). These constraints can be technical, like limited power availability in wireless sensor nodes, or non-technical, like constraints coming from legislation or business.

6. The lower level is referred to as the solution domain. This is where design objectives and principles are established, conceptual views are refined, required functions are identified, and where logical partitions of functionality and information are described.

7. Problem Domain: Designing a Smart Agriculture System.

- Partition 1: Environmental Sensing and Data Collection
- Partition 2: Crop Monitoring and Irrigation Control
- Partition 3: Pest and Disease Detection

8. Solution Domain: Developing an IoT-based Home Security System.

- Partition 1: Device Integration and Control
- Partition 2: User Interface and Mobile App Development
- Partition 3: Video Surveillance and Motion Detection

muquestionpapers.com

Q2(d) Elaborate on Network Application Registration Process **(5)**

Ans. 1. The network application registration process is an essential step in establishing communication between network-connected devices and services.

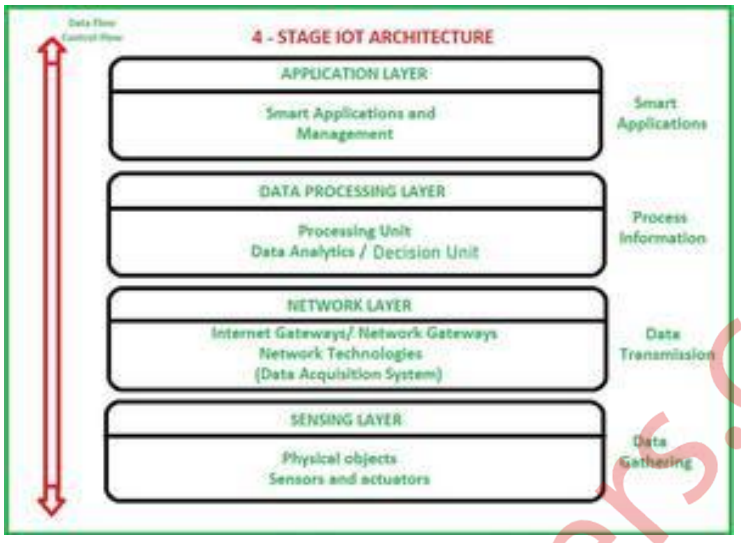
2. It allows applications or devices to announce their presence and capabilities to the network, enabling other devices or services to discover and interact with them. Below is an elaboration of the network application registration process:

- Application Discovery: The registration process begins with an application or device broadcasting its presence on the network. This can be done through various means, such as sending out a multicast message or using specific protocols like m DNS (Multicast DNS) or SSDP (Simple Service Discovery Protocol).
- Network Service Directory: Upon receiving the broadcast message, devices or services interested in discovering applications subscribe to a network service directory or registry. This directory maintains a list of registered applications and their associated information. It acts as a centralized or distributed repository where applications can register and other devices can query for available services.
- Application Registration: The application or device that wants to be discoverable on the network initiates the registration process. It sends a registration message to the network service directory, providing details about its identity, functionality, and supported services.
- Updating and Expiration: To ensure the accuracy and relevance of the network service directory, registered applications regularly update their information. This update process allows devices to notify the directory of any changes, such as IP address updates or service availability status.
- Application Discovery and Interaction: Once an application is successfully registered in the network service directory, other devices or services can discover it by querying the directory.

muquestionpapers.com

Q2(e) Describe with neat labelled diagram, IoT Device Architecture. (5)

Ans.



1. Sensors and Actuators: At the core of an IoT device, there are sensors that collect real-world data (e.g., temperature, humidity, motion) and actuators that allow the device to perform actions (e.g., turning on a motor, activating a display).
2. Microcontroller or Microprocessor: The microcontroller or microprocessor is the brain of the IoT device. It processes data from sensors, controls actuators, and manages device functions. It may also include memory, input/output (I/O) interfaces, and communication modules.
3. Connectivity Module: This component enables the IoT device to communicate with other devices or the cloud. It may include Wi-Fi, Bluetooth, Zigbee, LoRaWAN, cellular, or other communication protocols, depending on the device's connectivity requirements.
4. Power Supply: IoT devices can be powered by batteries, wired connections, or energy harvesting methods. The power supply ensures the device has sufficient energy to operate.
5. Security Module: IoT devices must be secure to protect data and prevent unauthorized access. The security module includes encryption, authentication, and other security mechanisms to safeguard the device and its communication.
6. Operating System (OS) or Firmware: The device's OS or firmware provides the necessary software to run applications, manage hardware resources, and ensure smooth operations.
7. Application Software: This layer includes the specific applications or functionalities

muquestionpapers.com

that make the IoT device useful for its intended purpose. For example, a smart thermostat application for temperature control or a health monitoring application for a wearable device.

8. Cloud Connectivity: Some IoT devices interact with cloud services for data storage, analytics, and remote control. The cloud connectivity allows the device to send and receive data from the cloud server.
9. User Interface (UI): In devices with user interaction, a user interface, such as an LED display, touchscreen, or buttons, allows users to interact with the device and view information.

Q2(f) How do smart cities work? List and explain its different application (5)

Ans. 1. IoT-enabled smart cities leverage the power of the Internet of Things (IoT) to create connected and data-driven urban environments.

2. IoT devices and sensors are deployed throughout the city to collect real-time data, which is then analyzed and used to improve various aspects of urban life. Here are different applications of how IoT smart cities work:

3. Smart Traffic Management: IoT sensors embedded in roads and traffic lights monitor traffic flow and congestion in real-time. This data is sent to a central management system that can optimize traffic signal timings, reroute vehicles, and provide dynamic traffic updates to drivers. Smart traffic management helps reduce congestion, shorten commute times, and improve overall transportation efficiency.

4. Environmental Monitoring: IoT sensors are deployed to monitor air quality, noise levels, temperature, and other environmental factors across the city. This data is collected and analyzed to identify pollution hotspots and trends. City officials can take data-driven actions to improve air quality, plan urban green spaces, and mitigate the impact of climate change.

5. Smart Waste Management: IoT sensors in waste bins monitor the fill levels and send real-time data to waste management teams. This data helps optimize waste collection routes, reducing unnecessary trips and associated carbon emissions. Additionally, smart waste management encourages recycling by providing feedback to citizens about their recycling habits.

6. Public Safety and Security: IoT-enabled surveillance cameras, connected streetlights, and smart sensors enhance public safety in smart cities. These devices can detect unusual

muquestionpapers.com

activities, monitor crowd density during events, and provide real-time data to law enforcement. These applications aid in rapid response to emergencies and help ensure a safer urban environment.

6. Energy Efficiency and Smart Grids: IoT devices are used to monitor and control energy usage in buildings, streetlights, and public infrastructure. Smart grids optimize energy distribution, reduce wastage, and integrate renewable energy sources like solar and wind power. This results in reduced energy consumption and a more sustainable energy infrastructure.

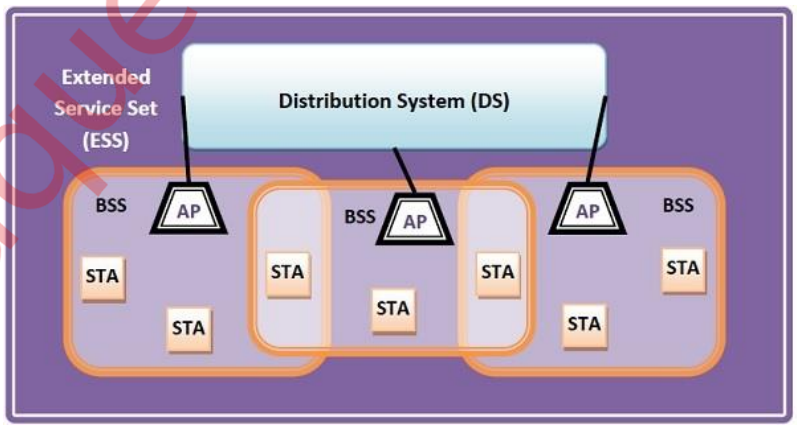
7. Citizen Engagement and Smart Services: Smart cities use IoT-powered mobile applications and online platforms to engage with citizens. These platforms provide access to various public services, such as online bill payment, reporting issues, and participating in city governance. Data analytics and citizen feedback enable the city administration to make data-driven decisions and deliver improved services.

Q3. Attempt any three of the following **[15]**

Q3(a) Discuss 802.11 protocol architecture in brief **(5)**

Ans. 1. IEEE 802.11 standard, popularly known as Wi-Fi, lays down the architecture and specifications of wireless LANs (WLANs).

2. Wi-Fi or WLAN uses high-frequency radio waves instead of cables for connecting the devices in LAN. Users connected by WLANs can move around within the area of network coverage.



3. The components of an IEEE 802.11 architecture are as follows −

muquestionpapers.com

- **Stations (STA)** − Stations comprises of all devices and equipment that are connected to the wireless LAN. A station can be of two types−
    - Wireless Access Point (WAP) − WAPs or simply access points (AP) are generally wireless routers that form the base stations or access.
    - Client. Clients are workstations, computers, laptops, printers, smartphones, etc.
- Each station has a wireless network interface controller.
- **Basic Service Set (BSS)** − A basic service set is a group of stations communicating at the physical layer level. BSS can be of two categories depending upon the mode of operation−
    - Infrastructure BSS − Here, the devices communicate with other devices through access points.
    - Independent BSS − Here, the devices communicate in a peer-to-peer basis in an ad hoc manner.
- **Extended Service Set (ESS)** − It is a set of all connected BSS.
- **Distribution System (DS)** − It connects access points in ESS.

4. Advantages of IEEE 802.11:

- The IEEE 802.11 is easy to installation.
- It has higher frequency range.
- It has efficient coding technique.
- The IEEE 802.11 has reduced wiring expense.

6. Disadvantages of IEEE 802.11:
    - It has traffic disruptions.
    - Network security and the maintenance needed to stay secured.
    - It is required periodic maintenance

Q3(b) Justify the WLAN? Describe its advantages. (5)

Ans. 1. The need for WLAN (Wireless Local Area Network) arises from the increasing demand for wireless connectivity and mobility in various environments, including homes, offices, public spaces, and industrial settings.

2. WLANs provide several advantages over traditional wired networks, making them essential in modern communication scenarios. Here are some justifications for the need of WLAN:

- Mobility and Flexibility: WLAN allows users to connect to the network without being physically tethered to a specific location. It enables users to move freely within the coverage area, making it ideal for mobile devices such as laptops, smartphones, and tablets.

muquestionpapers.com

- Rapid Deployment: Setting up a WLAN is generally quicker and more cost-effective than installing a wired network. There is no need for extensive cabling, making WLANs particularly suitable for temporary setups, event venues, and areas with difficult physical infrastructure.
- Scalability: WLANs can easily accommodate additional devices without the need for major infrastructure changes. As the number of connected devices grows, WLANs can be expanded by adding access points to provide broader coverage and support more users.
- Improved Connectivity: WLANs offer seamless connectivity, allowing devices to switch between access points without interruption (roaming). This feature ensures continuous network access as users move throughout the coverage area.
- Internet of Things (IoT) Integration: With the proliferation of IoT devices, WLANs play a crucial role in connecting and managing various smart devices in homes, industries, and public spaces. WLANs provide the necessary infrastructure for IoT devices to communicate and share data wirelessly.
- Cost-Efficient for Remote Locations: In remote or hard-to-reach areas where laying wired infrastructure is challenging, WLANs provide a cost-effective alternative for delivering internet connectivity and network access.
- Disaster Recovery and Redundancy: WLANs can serve as a backup or redundant network in case of wired network failures or during disaster recovery scenarios.
- Easy Integration with Wired Networks: WLANs can be integrated with existing wired networks, allowing devices to access resources and services regardless of their connection type.

Q3(c) Define and state the following terms **(5)**

a. BSS

b. **ESS**

Ans. a. Basic Service Set (BSS): Basic Service Set (BSS), as name suggests, is a group or set of all stations that communicate with each together. Here, stations are considered as computers or components connected to wired network.

Advantages of BSS:

- Simplicity: A BSS is a simple and cost-effective way to provide wireless connectivity for a small area, such as a home or office.

muquestionpapers.com

- Easy to set up: Setting up a BSS is straightforward, as it only requires a single Access Point (AP) and a set of client devices.
- Easier to manage: A BSS is easier to manage than an ESS, as there is only one AP to configure and maintain.

Disadvantages of BSS:

- Limited coverage: A BSS has limited coverage, typically ranging from a few meters to a few hundred meters.
- Limited scalability: A BSS is not scalable beyond a certain point, as adding more users or devices can cause congestion and slow down the network.

Extended Service Set (ESS): Extended Service Set (ESS), as name suggests, is a group of BSSs or one or more interconnected BSS along with their wired network.

Advantages of ESS:

- Scalability: An ESS can be scaled to cover a much larger area by interconnecting multiple BSSs.
- Greater coverage: An ESS can provide coverage over a large area, such as a campus or an entire building.

Disadvantages of ESS:

- Complexity: An ESS is more complex than a BSS, as it requires multiple APs and a central controller.
- Higher cost: An ESS can be more expensive to set up and maintain than a BSS, due to the need for multiple APs and a central controller.

Q3(d) What is BLE? How does it differ from the standard Bluetooth (5)

Ans. 1. BLE stands for Bluetooth Low Energy, which is a wireless communication technology designed for low-power, short-range data transmission between devices.

2. It is a subset of the standard Bluetooth technology, and while it shares many similarities with classic Bluetooth, it also has some key differences. Here's a comparison between BLE and standard Bluetooth:

- Power Consumption:
    - BLE: One of the most significant advantages of BLE is its low power consumption. It is specifically designed to operate in energy-constrained

muquestionpapers.com

devices like wearables, sensors, and IoT devices. BLE's power-efficient operation allows these devices to run for extended periods using small batteries or even harvested energy.

    - Standard Bluetooth: Classic Bluetooth consumes more power compared to BLE, making it less suitable for battery-operated devices that require long-term usage without frequent battery replacements.

- Data Transfer Rate:
    - BLE: BLE offers a lower data transfer rate compared to standard Bluetooth. Its data throughput is optimized for transmitting small packets of data, typically in the range of a few kilobits per second.
    - Standard Bluetooth: Classic Bluetooth supports higher data transfer rates, making it more suitable for applications that require more extensive data exchanges, such as audio streaming or file transfers.
- Range:
    - BLE: Bluetooth Low Energy is designed for short-range communication, typically within a range of a few meters to tens of meters. This limited range ensures a lower power requirement for wireless communication.
    - Standard Bluetooth: Classic Bluetooth offers a more extended range, typically up to 100 meters, making it suitable for applications that require communication over longer distances.
- Compatibility:
    - BLE: BLE is backward compatible with Bluetooth 4.0 and later versions, ensuring that devices supporting Bluetooth Low Energy can communicate with devices using standard Bluetooth if needed.
    - Standard Bluetooth: Classic Bluetooth devices are not backward compatible with BLE, as the hardware and communication protocols are different.

3. Bluetooth Low Energy (BLE) is a low-power, short-range communication technology designed for energy-efficient applications, while standard Bluetooth is better suited for data-intensive tasks and longer-range communication. Each technology serves different use cases based on their power requirements, data transfer rates, and application compatibility.

muquestionpapers.com

Q3(e) Compare between passive and active RFID with the help of Dash7 network (5)

Ans. 1. Passive and Active RFID are two different types of RFID (Radio Frequency Identification) technologies that operate within the Dash7 network.

2. Dash7 is a wireless sensor networking protocol designed for long-range and low-power communication. Let's compare Passive and Active RFID in the context of the Dash7 network:

- Power Source:
  - Passive RFID: Passive RFID tags do not have their power source. They are powered by the radio frequency energy emitted by the reader (or interrogator) during communication. These tags are relatively simple and cost-effective but have limited read range and cannot initiate communication on their own.
  - Active RFID: Active RFID tags have their power source, typically a battery. They can actively transmit signals and initiate communication independently, providing longer read ranges and more reliable communication.
- Read Range:
  - Passive RFID: Due to their reliance on energy from the reader, passive RFID tags have a shorter read range compared to active tags. Typically, they have a read range of a few meters, making them suitable for close-proximity identification.
  - Active RFID: Active RFID tags, with their own power source, can achieve read ranges of tens to hundreds of meters, enabling longer-range identification and tracking capabilities.
- Communication Speed:
  - Passive RFID: Passive RFID communication is relatively slower, as the tags need to wait for energy from the reader to power up and respond. This can result in slower data transfer rates.
  - Active RFID: Active RFID tags can transmit data faster as they have a constant power source and can initiate communication immediately.
- Complexity and Cost:
  - Passive RFID: Passive RFID tags are simpler and less expensive to manufacture compared to active tags since they do not require a power source. They are often used for cost-sensitive applications.
  - Active RFID: Active RFID tags are more complex and relatively more expensive due to the inclusion of a power source. They are used in applications that require longer read ranges and higher data transfer rates.

3. In the Dash7 network, both passive and active RFID technologies can be integrated to create a versatile ecosystem that caters to different use cases and requirements. Passive RFID is more

muquestionpapers.com

suitable for low-cost and short-range applications, while active RFID provides extended read range and continuous communication for more demanding scenarios.

Q3(f) How do Dash7 components communicate with each other? Explain in detail (5)

Ans. 1. Dash7 components communicate with each other through the Dash7 protocol, a wireless sensor networking technology designed for long-range, low-power communication.
2. The communication process involves several layers in the protocol stack, ensuring efficient data exchange and network management.

3. Here's a detailed explanation of how Dash7 components communicate:

- Physical Layer (PHY): The communication begins at the Physical Layer, where radio signals are transmitted and received between Dash7 components. The PHY layer defines the modulation scheme, channel access method, data rates, and error-checking mechanisms for reliable data transmission over the wireless medium.
- Medium Access Control (MAC) Layer: The Medium Access Control Layer governs access to the shared wireless medium and handles data link layer functions. Dash7 uses a unique channel access method known as Time Slotted Channel Hopping (TSCH). In TSCH, time is divided into fixed-length slots, and devices synchronize their schedules to hop between channels at specific times. This approach minimizes interference and ensures efficient use of the available spectrum.
- Frame Format: Data exchanged between Dash7 components is encapsulated into frames with a specific structure. These frames include fields for synchronization, addressing, data payload, and error-checking. The frame format allows devices to identify the source and destination, extract data, and verify the integrity of received frames.
- Network and Transport Layers: Dash7 follows a 3-layered stack for network communication: Application Layer: The application layer defines the messages and data exchanged between Dash7 devices for specific use cases. It determines how sensors, tags, and readers interact with each other to perform various tasks.
- Transport Layer: The transport layer handles end-to-end communication and data flow control between Dash7 devices. It ensures that data is delivered reliably and in the correct order.
- Network Layer: The network layer manages device addressing, routing, and network topology. It ensures that Dash7 devices can find each other within the

muquestionpapers.com

network and supports routing messages between devices when needed.

Overall, Dash7 components communicate through a combination of radio frequency communication, time-slotted channel hopping, and a layered protocol stack that manages various aspects of data exchange, network management, and device association. This communication approach allows Dash7 to provide long-range, low-power connectivity suitable for various IoT and sensor networking applications.

Q4. Attempt any three of the following **[15]**

Q4(a) Distinguish between TCP and UDP **(5)**

Ans.

Basis	Transmission Control Protocol (TCP)	User Datagram Protocol (UDP)
Type of Service	TCP is a connection-oriented protocol. Connection orientation means that the communicating devices should establish a connection before transmitting data and should close the connection after transmitting the data.	UDP is the Datagram-oriented protocol. This is because there is no overhead for opening a connection, maintaining a connection, or terminating a connection. UDP is efficient for broadcast and multicast types of network transmission.
Reliability	TCP is reliable as it guarantees the delivery of data to the destination router.	The delivery of data to the destination cannot be guaranteed in UDP.
Error checking mechanism	TCP provides extensive error-checking mechanisms. It is because it provides flow control and acknowledgment of data.	UDP has only the basic error-checking mechanism using checksums.
Speed	TCP is comparatively slower than UDP.	UDP is faster, simpler, and more efficient than TCP.

muquestionpapers.com

Retransmission	Retransmission of lost packets is possible in TCP, but not in UDP.	There is no retransmission of lost packets in the User Datagram Protocol (UDP).
Header Length	TCP has a (20-60) bytes variable length header.	UDP has an 8 bytes fixed-length header.
Protocols	TCP is used by HTTP, HTTPs, FTP, SMTP and Telnet.	UDP is used by DNS, DHCP, TFTP, SNMP, RIP, and VoIP.
Stream Type	The TCP connection is a byte stream.	UDP connection is a message stream.
Overhead	Low but higher than UDP.	Very low.

Q4(b) List and explain characteristics of Stream Control Transmission Protocol (5)

Ans. 1. Stream Control Transmission Protocol (SCTP) is a transport layer protocol designed to provide reliable, message-oriented communication between applications.

2. SCTP offers several key characteristics that make it suitable for various use cases. Here are five important characteristics of SCTP:

- Message-Oriented Communication: SCTP operates in a message-oriented manner, which means it sends messages as discrete units rather than a continuous stream of bytes like TCP.
- Reliable Data Transfer: SCTP guarantees reliable data delivery, similar to TCP. It uses acknowledgment mechanisms and retransmissions to ensure that all sent data reaches the destination without errors or omissions.
- Multi-Homing Support: One of the unique features of SCTP is its ability to support multiple network paths between two endpoints. This concept is known as multi-homing. It allows SCTP to maintain multiple IP addresses for each endpoint, providing fault tolerance and increased network redundancy. If one path fails, SCTP can automatically switch to an alternate path, enhancing the protocol's robustness.
- Flow and Congestion Control: SCTP incorporates flow and congestion control mechanisms to optimize data transfer across the network. Flow control prevents the receiver from being overwhelmed with data by allowing it to indicate its buffer's

muquestionpapers.com

capacity. Congestion control helps manage network congestion by adjusting the sending rate based on network conditions, ensuring efficient data transmission without causing network bottlenecks.

3. Overall, SCTP is a versatile transport protocol with features that cater to various communication requirements, making it suitable for a wide range of applications, including voice over IP (VoIP), real-time multimedia, and signaling protocols in telecommunications networks.

Q4(c) Define the term Congestion control. Explain in brief Datagram Congestion Control Protocol. (5)

Ans. 1. Congestion Control: Congestion control is a crucial mechanism employed in computer networks to manage and prevent network congestion. Network congestion occurs when the demand for network resources (bandwidth, buffer space) exceeds the available capacity, leading to degraded performance, packet loss, and increased delays.

2. Datagram Congestion Control Protocol (DCCP): Datagram Congestion Control Protocol (DCCP) is a transport layer protocol that provides congestion control for connectionless protocols, such as User Datagram Protocol (UDP).

3. DCCP combines the benefits of UDP's connectionless nature with the advantages of congestion control mechanisms typically associated with connection-oriented protocols like TCP.

4. Key Features of DCCP:

- Unordered and Reliable Mode: DCCP supports both ordered and unordered delivery of data. In unordered mode, data packets may arrive out of order at the receiver, but the protocol ensures they are received reliably, meaning they are not lost or corrupted during transmission.
- Congestion Control: The primary purpose of DCCP is to provide congestion control. It includes congestion control mechanisms that help prevent network congestion by adapting the transmission rate based on the network's congestion level
- Explicit Congestion Notification (ECN): DCCP utilizes Explicit Congestion Notification (ECN), a technique where routers along the network path can mark packets to indicate network congestion. This way, DCCP can react to congestion more efficiently and reduce its transmission rate proactively.

muquestionpapers.com

Q4(d)Illustrate the working of Extensible Messaging Presence Protocol. (5)

Ans. 1. The Extensible Messaging Presence Protocol (XMPP) is a communication protocol used for real-time messaging, presence information, and other application-specific extensions.

2. It is designed to enable instant messaging, presence tracking, and other real-time communication features. XMPP follows a client-server architecture and is often used for chat applications, social networking platforms, and Internet of Things (IoT) applications.

- Discovery and Authentication:
  - XMPP client performs a DNS SRV query to find the domain of the XMPP server.
  - Client establishes a TCP connection with the server on port 5222 (or the alternative port from DNS SRV).
  - Authentication occurs using mechanisms like SASL.
- Session Establishment:
  - Upon successful authentication, the XMPP server establishes a session with the client.
  - This session allows the exchange of XML stanzas between the client and server.
- Presence Exchange:
  - Users share their presence information, e.g., available, away, busy, offline, etc.
  - The client sends "presence" stanzas to the server to indicate the user's current status.
  - The server relays this information to the user's contacts.
- Messaging:
  - To send messages, the client sends "message" stanzas to the server, specifying the recipient and message content.
  - The server routes the message to the appropriate recipient(s) based on their presence and routing rules.

muquestionpapers.com

Q4(e) Discuss in brief about the Broadband Forum. (5)

Ans. 1. The Broadband Forum is a non-profit industry organization dedicated to developing and promoting broadband technologies and standards.

2. It was established in 1994 and has since played a significant role in shaping the evolution of broadband networks worldwide.

3. Here are key points about the Broadband Forum:

- Standardization and Specifications: The Broadband Forum brings together service providers, equipment manufacturers, system integrators, and other stakeholders to develop and publish open broadband standards and specifications. These standards cover various aspects of broadband technology, including access networks, management, interoperability, and Quality of Service (QoS).
- Working Groups and Projects: The organization operates through various working groups and projects, each focusing on specific aspects of broadband technology. These working groups collaborate to address emerging challenges and opportunities in the broadband industry, contributing to the development of new technologies and solutions.
- Interoperability and Certification Programs: The Broadband Forum promotes interoperability among different vendors' broadband equipment and systems. It conducts interoperability testing and certification programs to ensure that products from different manufacturers can work seamlessly together. This approach reduces deployment risks and encourages market competition.
- Broadband Ecosystem Collaboration: The Broadband Forum acts as a platform for fostering collaboration and knowledge sharing among its members and the broader broadband ecosystem. It organizes conferences, workshops, and webinars to facilitate discussions on industry trends, best practices, and technical advancements.

muquestionpapers.com

Q4(f) Identify different transport layer protocols. Explain UDP with its key point (5)

Ans. 1. Different transport layer protocols include:

a) Transmission Control Protocol (TCP): TCP is a connection-oriented protocol that provides reliable and ordered delivery of data between applications. It ensures that data packets are delivered without errors and in the correct order. TCP establishes a connection before data transmission and uses acknowledgment and retransmission mechanisms to guarantee data delivery.

b) User Datagram Protocol (UDP): UDP is a connectionless protocol that provides best-effort delivery of data between applications. Unlike TCP, UDP does not establish a connection before transmitting data and does not guarantee reliable delivery. It is often used in applications where real-time data transmission is crucial, and some packet loss can be tolerated.

Explanation of UDP with key points:

- Connectionless: UDP does not require a prior connection setup before sending data. Applications can simply send datagrams (small packets) without any handshake or connection establishment.
- No Reliability: UDP does not guarantee reliable data delivery. It does not use acknowledgment or retransmission mechanisms like TCP. Once a UDP packet is sent, there is no assurance that it will reach its destination, and there is no mechanism to recover lost packets.
- Low Overhead: UDP has a lower overhead compared to TCP since it does not involve the complex connection establishment and reliability mechanisms. This makes it faster and more efficient for certain types of applications.
- Best Effort Delivery: UDP follows a "best-effort delivery" approach. It means that the protocol will make an attempt to deliver the data, but it won't ensure that it reaches the destination. If any packets are lost during transmission, UDP does not attempt to recover or retransmit them.
- Suitable for Real-time Applications: UDP is commonly used in real-time applications, such as video streaming, online gaming, VoIP (Voice over Internet Protocol), and DNS (Domain Name System) queries.

muquestionpapers.com

Q5. Attempt any Five of the following **[15]**

Q5(a) Elaborate on CRUD? Discuss its advantages and disadvantages **(3)**

Ans: 1. CRUD stands for Create, Read, Update, and Delete. It represents the four basic operations used to manage data in database systems and applications.

2. Advantages of CRUD:

a) Simplicity: CRUD operations provide a straightforward and easy-to-understand approach to interact with data. This simplicity makes it easier for developers to implement and maintain data-related functionalities.

b) Standardization: The CRUD operations offer a standardized way of dealing with data, which promotes consistency across applications. Developers and users can expect a uniform experience when working with different systems.

c) User-Friendly: CRUD forms the basis of many user interfaces, making applications more intuitive for users. The operations map well to typical user actions, such as creating new records, viewing details, updating information, or removing unwanted data.

3. Disadvantages of CRUD:

a) Limited Functionality: While CRUD covers fundamental data operations, it may not handle more complex database interactions efficiently. Additional custom logic might be required for specialized actions or handling complex relationships between data.

b) Security Concerns: CRUD operations, if not properly secured, can lead to potential security vulnerabilities. Unauthorized users might gain access to sensitive data or perform unauthorized changes, leading to data breaches or integrity issues.

c) Performance Constraints: CRUD operations can become less efficient with large datasets, especially if proper indexing and optimization are not in place. As the data volume grows, performance issues may arise, affecting the overall system responsiveness.

muquestionpapers.com

Q5(b) Differentiate between unicast and multicast addresses. **(3)**

Ans.

Sr.No.	Unicast	Multicast
Communication model	One-to-one.	One-to-many.
Network efficiency	Less efficient	More efficient
Bandwidth	Higher bandwidth	Lower bandwidth
Applications	Suitable for applications that require secure and reliable data transfer, such as email and file transfer	Suitable for applications that require high-bandwidth data transfer to multiple recipients, such as multimedia streaming and online gaming
Protocols	Supported by most networking protocols, including TCP and UDP	Supported by the IP multicast protocol
Addressing	Uses the recipient's unique address or IP address	Uses a multicast group address

Q5(c) Discuss Multipath TCP with its key point. **(3)**

Ans. 1. Multipath TCP (MPTCP) is an extension of the traditional TCP (Transmission Control Protocol) that allows a single connection to use multiple network paths simultaneously.

2. Its key points are:

a) Path Aggregation: MPTCP enables data to be transmitted over multiple network paths concurrently. It combines the bandwidth and reliability of these paths, effectively aggregating their capacities, leading to improved performance and better resource utilization.

b) Resilience and Robustness: MPTCP enhances the resilience of data transmission by

muquestionpapers.com

distributing data across multiple paths. If one path becomes congested or fails, the other paths can continue to transmit data, providing better network reliability and fault tolerance.

c) Seamless Handover: MPTCP is designed to handle seamless handover between different network interfaces, such as switching from Wi-Fi to cellular data or from one Wi-Fi network to another. This enables uninterrupted data transfer as devices move between different network environments.

d) Overall, Multipath TCP is a significant advancement in TCP technology, as it allows for more efficient and reliable data transmission in modern network scenarios where devices may have multiple network interfaces and connectivity options available. It is especially beneficial in mobile and wireless environments, where network conditions can change frequently

Q5(d)Explain an example of CEP- Complex Event Processing (3)

Ans. 1. Complex Event Processing (CEP) is a technique used in information systems to analyze and process streams of events in real-time to identify patterns or complex events.

2. These events can be generated from various sources, such as sensors, applications, databases, or other data streams. CEP enables organizations to gain actionable insights and respond to critical situations promptly.

3. Example of CEP - Smart Traffic Management:

- In a smart traffic management system, CEP can be used to process real-time data from various sources, such as traffic cameras, vehicle sensors, GPS devices, and weather reports, to optimize traffic flow and improve overall transportation efficiency.
- Event Detection: CEP can identify complex events such as traffic congestion, accidents, sudden changes in weather conditions, or a high number of vehicles entering a specific area.
- Real-time Response: Once complex events are detected, the smart traffic management system can trigger real-time responses, such as adjusting traffic signal timings, rerouting traffic, or notifying emergency services and commuters about incidents or alternative routes.
- Pattern Analysis: CEP can analyze patterns of traffic behavior over time, identifying recurring traffic bottlenecks, peak hours, or areas prone to accidents. This data can

muquestionpapers.com

be used to plan infrastructure improvements and optimize traffic management strategies.

Q5(e)Compare between TCP and UDP **(3)**

Ans. 1 Comparison between TCP and UDP:

1. Connection-oriented vs. Connectionless: TCP (Transmission Control Protocol) is a connection-oriented protocol, meaning it establishes a reliable and ordered connection before transmitting data. UDP (User Datagram Protocol), on the other hand, is connectionless and does not require prior connection setup before sending data.
2. Reliability: TCP guarantees reliable data delivery by using acknowledgment and retransmission mechanisms. It ensures that data packets are delivered without errors and in the correct order. UDP, being connectionless, does not provide reliability or guarantee that data will be delivered.
3. Overhead: TCP has higher overhead compared to UDP. It involves more complex connection establishment and maintenance mechanisms, as well as error recovery features. UDP has lower overhead since it does not involve connection setup or reliability mechanisms.
4. In summary, TCP offers reliable, ordered data delivery with higher overhead due to its connection-oriented nature, while UDP is connectionless, providing lower overhead but no reliability guarantees. The choice between TCP and UDP depends on the specific requirements of the application or use case, balancing factors such as data integrity, speed, and resource efficiency.

Q5(f)Define the following terms: **(3)**

1. **Computer Network**
2. **Internet of Things**

Ans. 1.) Computer Network:

- A computer network refers to a collection of interconnected computers and other devices that can communicate with each other and share resources. It allows data, information, and resources to be transmitted and accessed across the network, enabling users to communicate, collaborate, and share data seamlessly.
- Computer networks can be local area networks (LANs) within a limited

muquestionpapers.com

geographical area, such as an office or home, or wide area networks (WANs) that span larger geographical distances, connecting multiple LANs or even global networks like the internet.

b.) Internet of Things (IoT):

- The Internet of Things (IoT) is a concept that involves connecting everyday physical objects or devices to the internet and enabling them to collect, exchange, and process data autonomously without requiring human intervention. These "smart" devices can range from household appliances, wearable devices, industrial machines, vehicles, and more.
- IoT devices are equipped with sensors, actuators, and communication technologies that allow them to interact with the environment and other devices over the internet.
- IoT aims to create a network of interconnected devices that can enhance automation, improve data-driven decision-making, and enable new applications and services for various industries and daily life activities.

Q5(g)What is NAT? List its uses. (3)

Ans. 1. NAT stands for Network Address Translation. It is a technique used in computer networking to map private IP addresses used within a local network to a single public IP address that can be used for communication with devices outside the local network, such as the internet.

2.NAT plays a crucial role in conserving the limited number of public IP addresses available and enhancing the security of local networks.

- Uses of NAT:
- IP Address Conservation: NAT allows multiple devices within a private local network to share a single public IP address. This helps conserve public IP address space, as only one public IP address is required for an entire network of devices.
- Internet Access for Private Networks: NAT enables devices within a private network, which uses non-routable private IP addresses, to access the internet using the single public IP address provided by the network's router or gateway. It acts as a mediator between the private network and the internet.
- Enhanced Security: NAT provides a level of security by hiding the actual IP addresses of devices within the local network from external networks. When devices

muquestionpapers.com

send data to external servers, their private IP addresses are replaced by the router's public IP address, making it difficult for external sources to directly initiate communication with devices within the private network. This process adds a layer of obscurity and protection to the local network.

Q5(h)Determine functions of HTTP? (3)

Ans. 1. HTTP (Hypertext Transfer Protocol) is the foundation of data communication on the World Wide Web.

2. It is an application layer protocol that governs the communication between web clients (such as web browsers) and web servers. The functions of HTTP include:

3. Web Page Retrieval: The primary function of HTTP is to retrieve web resources, particularly web pages, from web servers. When a user requests a web page by entering a URL in a web browser, the browser sends an HTTP request to the server, and the server responds with the requested web page.

4. Stateless Communication: HTTP operates in a stateless manner, which means each request from a client to a server is independent and carries no knowledge of previous requests. This simplicity makes HTTP scalable and allows for easy load balancing in server clusters.

5. Request Methods: HTTP supports various request methods (verbs) that specify the action to be performed on the server's resource. Common HTTP methods include GET (retrieve a resource), POST (submit data to be processed), PUT (update a resource), DELETE (remove a resource), and more. Each method serves different purposes for manipulating resources.

muquestionpapers.com