1. What is MQTT primarily used for?

a) Video streaming
b) Real-time communication between IoT devices
c) Online gaming
d) File sharing

Answer: b) Real-time communication between IoT devices

Explanation: MQTT (Message Queuing Telemetry Transport) is a lightweight messaging protocol designed for reliable, efficient communication between IoT devices, making it ideal for applications where bandwidth and resources are limited.

2. Which of the following is NOT a MQTT method?

a) CONNECT
b) PUBLISH
c) UPDATE
d) SUBSCRIBE

Answer: c) UPDATE

Explanation: The MQTT protocol primarily consists of methods like CONNECT, PUBLISH, and SUBSCRIBE for establishing connections, publishing messages, and subscribing to topics, respectively. UPDATE is not a standard MQTT method.

3. What are topics in MQTT used for?

a) Identifying devices in a network
b) Filtering messages
c) Establishing secure connections
d) Synchronizing time between devices

Answer: b) Filtering messages

Explanation: MQTT topics are hierarchical strings used to filter and route messages between publishers and subscribers. Subscribers can specify topics they're interested in, and publishers can publish messages to specific topics, allowing for efficient message distribution.

4. Which protocol is known for its lightweight communication in IoT networks and is often used as an alternative to MQTT?

a) TCP
b) HTTP
c) CoAP
d) UDP

Answer: c) CoAP (Constrained Application Protocol)

Explanation: CoAP is designed for the resource-constrained Internet of Things (IoT) devices and networks. It provides a lightweight communication protocol suitable for constrained environments, similar to MQTT.

5. What is the primary communication model used in CoAP?

a) Point-to-Point

b) Publish-Subscribe
c) Request-Response
d) Peer-to-Peer

Answer: c) Request-Response

Explanation: CoAP primarily follows a Request-Response model, where clients make requests to servers, and servers respond to those requests. This model is common in many IoT scenarios where devices need to exchange data in a client-server fashion.

6. Which protocol is commonly used for real-time messaging and presence information exchange?

a) XMPP (Extensible Messaging and Presence Protocol)
b) SMTP (Simple Mail Transfer Protocol)
c) FTP (File Transfer Protocol)
d) SSH (Secure Shell)

Answer: a) XMPP (Extensible Messaging and Presence Protocol)

Explanation: XMPP is a communication protocol for message-oriented middleware based on XML (Extensible Markup Language). It is commonly used for real-time messaging, presence information, and contact list maintenance.

7. What are the key features of AMQP (Advanced Message Queuing Protocol)?

a) Lightweight and suitable for IoT devices
b) Designed for real-time video streaming

c) Supports reliable message delivery and queuing
d) Primarily used for web browsing

Answer: c) Supports reliable message delivery and queuing

Explanation: AMQP is an open standard application layer protocol for message-oriented middleware. Its key features include reliable message delivery, queuing, routing, and security mechanisms, making it suitable for various messaging scenarios.

8. Which of the following is NOT a frame type in AMQP?

a) Header
b) Body
c) Control
d) Method

Answer: c) Control

Explanation: In AMQP, frames are used to encapsulate different types of data. The frame types include Header, Body, and Method. “Control” is not a standard frame type in AMQP.

9. What is SMQTT?

a) Secure MQTT, an encrypted version of MQTT
b) Simple MQTT, a lightweight variant of MQTT
c) Scalable MQTT, designed for large-scale IoT deployments
d) Streamlined MQTT, optimized for low-latency communication

Answer: b) Simple MQTT, a lightweight variant of MQTT

Explanation: SMQTT stands for Simple MQTT, which is a lightweight variant of the MQTT protocol designed for simplicity and efficiency in communication, particularly in resource-constrained environments.

10. Which protocol is known for its efficiency in constrained networks and is often used in scenarios where bandwidth and resources are limited?

a) HTTP
b) FTP
c) CoAP
d) SMTP

Answer: c) CoAP (Constrained Application Protocol)

Explanation: CoAP is specifically designed for constrained networks and devices, offering a lightweight communication protocol suitable for IoT applications where bandwidth and resources are limited.

Related posts:

1. Introduction to Information Security
2. Introduction to Information Security MCQ
3. Introduction to Information Security MCQ
4. Symmetric Key Cryptography MCQ
5. Asymmetric Key Cryptography MCQ
6. Authentication & Integrity MCQ

7. E-mail, IP and Web Security MCQ