PassQueen
a.k.a dumpsqueen.com

Certified Wireless IoT Solutions Administrator

CWNP CWISA-102

Version Demo

Total Demo Questions: 8

Total Premium Questions: 84

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, IoT Fundamentals	5
Topic 2, IoT Technologies	22
Topic 3, IoT Connectivity	28
Topic 4, IoT Security	12
Topic 5, IoT Solutions	17
Total	84

QUESTION NO: 1

What is the primary difference between LoRa and LoRaWAN?

A. LoRa is the modulation method and LoRaWAN implements the higher network layers

B. LoRa Is used for communicating across the Internet and LoRaWAN is used only on the local link

C. LoRa uses RF and LoRaWAN uses light-based communications

D. LoRaWAN is the Physical Layer and LoRa is the Transport Layer

ANSWER: A

Explanation:

LoRa is the modulation method and LoRaWAN implements the higher network layers is correct because the two terms describe complementary, but distinct, parts of a wireless IoT solution. LoRa is Semtech's proprietary physical-layer radio technology based on chirp spread spectrum modulation. Its characteristics, including long communication range, robust reception at low signal levels, and low power consumption, make it well suited to battery-operated sensors and other IoT endpoints. LoRa itself describes how information is carried over the RF link; it does not by itself define a complete interoperable network architecture.

LoRaWAN is the open networking specification designed to use LoRa radio links in wide-area IoT deployments. It defines the MAC-layer behavior and the surrounding architecture, including the relationships among end devices, gateways, network servers, and application servers. The specification also addresses device activation, addressing, message handling, security keys, and bidirectional communications. In practical terms, a LoRaWAN device transmits using the LoRa physical layer, while LoRaWAN supplies the standardized rules that allow those transmissions to participate in a managed, scalable network. See the LoRa Alliance overview of LoRaWAN and Semtech's LoRa technology overview.

QUESTION NO: 2

What process, used for security in wireless solutions, is defined as the encoding of information to prevent readability by unauthorized users?

A. Access Control

B. Authentication

C. Encryption

D. Authorization

ANSWER: C

Explanation:

Encryption is the process of encoding readable data, known as plaintext, into an unreadable form, known as ciphertext, so that unauthorized parties cannot understand it. A cryptographic algorithm and key perform this transformation; an authorized recipient with the appropriate key can decrypt the ciphertext and restore the original information. In wireless IoT solutions, encryption is essential because radio transmissions can potentially be received by devices outside the intended communication path. Proper encryption protects the confidentiality of information while it is transmitted over the air and, where implemented, while stored on endpoints or supporting systems. Wi-Fi security technologies use encryption as part of their protection mechanisms. For example, WPA3 provides modern Wi-Fi security protections, and its Personal mode uses SAE to establish secure credentials and protect communications. Encryption is also a foundational security control for IoT deployments because sensitive telemetry, commands, identities, and configuration data may traverse networks that are not physically contained. The National Institute of Standards and Technology describes cryptography as transforming data so that only authorized entities can access or understand protected information. See the NIST Cryptographic Standards and Guidelines and the Wi-Fi Alliance security overview.

QUESTION NO: 3

A Wi-Fi enabled weight scale is an example of what kind of health IoT device?

A. implantable

B. wearable

C. non-wearable

D. injectable

ANSWER: C

Explanation:

non-wearable is correct because a Wi-Fi-enabled weight scale is used externally and is not attached to, worn on, injected into, or surgically placed within a person's body. The scale collects a biometric measurement—typically body weight, and sometimes related metrics such as body-mass index or body-composition estimates—and transmits that information through Wi-Fi to an application, cloud service, or health-management platform. This makes it a connected health IoT endpoint, but its physical mode of use places it in the non-wearable category. Non-wearable health IoT devices commonly include connected scales, blood-pressure cuffs, thermometers, and other equipment that a person uses periodically rather than continuously wearing. The Wi-Fi connection enables the scale to synchronize readings automatically, making longitudinal data available for personal wellness tracking or, where appropriate, remote health monitoring. The U.S. Food and Drug Administration describes wireless medical devices as devices that use wireless technology to communicate information, a concept that includes connected measurement equipment used in health contexts. NIST also provides guidance on securing IoT devices, including connected devices that collect and transmit potentially sensitive data. See the FDA wireless medical devices overview and NIST Cybersecurity for IoT Program.

QUESTION NO: 4

What is an important acceptance agreement to achieve in the final customer meeting for a wireless IoT deployment?

A. Stakeholder acceptance

B. Support for wearable IoT solutions

C. Scope definition

D. Power supply provisioning

ANSWER: A

Explanation:

Stakeholder acceptance is the essential agreement to obtain during the final customer meeting because it formally confirms that the wireless IoT deployment meets the customer's agreed requirements and is ready to transition from project delivery into operational use. This acceptance should reflect that the relevant customer stakeholders have reviewed the delivered solution, validation results, documentation, and any agreed handover materials. Their approval establishes a clear completion point for the implementation and records the customer's willingness to assume ownership of the solution and its ongoing operation.

For a wireless IoT deployment, this is particularly important because successful handover involves more than confirming that devices connect to the network. The customer needs confidence that the implemented system supports the intended business outcomes, that operational responsibilities are understood, and that the deployment has been accepted according to defined criteria. Formal stakeholder acceptance also supports good project governance by documenting approval, closing delivery activities, and providing an agreed basis for support and lifecycle management. CWNP's CWISA credential focuses on planning, deploying, validating, and administering wireless IoT solutions, all of which culminate in a successful customer handover. See the CWNP CWISA certification overview and the CWISA-102 exam overview.

QUESTION NO: 5

An MQTT publisher reports the current state of a loading-bay door only when that state changes. A dashboard subscriber must display the latest known state immediately after it connects, even if the door state has not changed recently. What MQTT feature should be used?

A. A retained message

B. A clean session

C. A Quality of Service 0 message

D. A wildcard subscription

ANSWER: A

Explanation:

A retained message is correct because the broker stores the most recent retained message for a topic and sends it to a new subscriber when that subscriber subscribes to the topic. This makes retained messages appropriate for publishing current state values, such as whether a door is open or closed. A persistent session preserves subscriptions and queued qualifying messages for a client, but it does not by itself establish a current state value for every new subscriber. Quality of Service levels address delivery handling rather than state retention.

QUESTION NO: 6

How is ASK modulation different from FSK modulation?

A. ASK varies the amplitude of the signal while FSK shifts its frequency

B. FSK is more sensitive to noise than ASK

C. ASK does not work at high frequencies

D. ASK can carry more data than FSK

ANSWER: A

Explanation:

ASK varies the amplitude of the signal while FSK shifts its frequency. Both are digital modulation methods: they encode digital symbols by changing a property of an RF carrier. With amplitude-shift keying, the carrier's amplitude is switched between defined levels—for example, a higher amplitude for one binary state and a lower or absent amplitude for the other. With frequency-shift keying, the transmitter instead uses discrete carrier frequencies to represent the states, such as one frequency for a binary zero and another for a binary one.

This distinction is fundamental when identifying a modulation scheme in an IoT wireless design or when interpreting a radio's signal behavior. The defining characteristic is the carrier parameter that changes during symbol transmission: amplitude for ASK and frequency for FSK. These techniques can be implemented in several forms, including binary variants, but the basic relationship remains the same. Frequency modulation methods are commonly used by low-power radio systems because information can be recovered from frequency transitions rather than solely from received signal strength. For further technical background, see the Analog Devices introduction to modulation and the ETSI SRD radio standard.

QUESTION NO: 7

What consideration is found in PtMP systems that is not found in PtP systems?

A. Interference avoidance

B. SINR optimization

C. Airtime management

D. Frequency selection

ANSWER: C

Explanation:

Airtime management is the distinct consideration in a point-to-multipoint (PtMP) wireless deployment because one central radio must coordinate medium access for multiple associated or connected remote stations. Every station competes for use of the same RF channel, and the usable capacity is shared rather than dedicated to a single peer. The design therefore needs to account for how transmission opportunities are allocated, how much airtime slower or weaker stations consume, and whether important traffic receives timely service when many stations contend for the medium.

Effective airtime management can involve scheduling methods such as TDMA, airtime fairness policies, traffic prioritization, and client-capacity planning. These mechanisms help maintain predictable performance and prevent a small number of inefficient transmissions from disproportionately reducing service available to the rest of the PtMP population. This is especially significant in wireless IoT designs, where numerous endpoints may report through one infrastructure radio and may have differing latency, reliability, and throughput needs.

A point-to-point link has only two endpoints on the link, so it does not require the same multi-client airtime-sharing and scheduling consideration. Cisco's discussion of wireless medium access provides background on contention and shared-medium operation: Cisco 802.11ac WLAN Deployment Guide. See also the Wi-Fi Alliance overview of Wi-Fi's shared radio medium: Wi-Fi CERTIFIED 6.

QUESTION NO: 8

You have been asked to consider smart building opportunities for your organization. Which one of these is a benefit of smart building technology?

A. Increased vacation time for building managers

B. Improved operational efficiency

C. Reduced design and construction costs

D. Faster Wi-Fi connectivity

ANSWER: B

Explanation:

Improved operational efficiency is a core benefit of smart building technology. Smart buildings integrate connected sensors, controls, automation platforms, and analytics to collect operational data and use it to make building systems more responsive. For example, occupancy and environmental sensors can inform HVAC, lighting, and ventilation controls so that energy and resources are used according to actual conditions rather than fixed schedules. This helps facility teams reduce waste while maintaining occupant comfort and appropriate indoor environmental conditions.

Operational data also supports proactive facilities management. Monitoring equipment status, performance trends, and fault conditions enables teams to identify maintenance needs earlier, prioritize work effectively, and reduce unplanned downtime. Space-use data can likewise help an organization understand how rooms and common areas are being used, supporting better allocation of workplace resources. These capabilities make day-to-day building operation more measurable, adaptable, and efficient. The U.S. Department of Energy describes building controls as an important means of optimizing building energy use and operations, while NIST outlines how IoT systems provide sensing, connectivity, and data-driven capabilities applicable to smart environments. See the U.S. Department of Energy's Building Controls overview and NIST's Cyber-Physical Systems and Internet of Things resources.