PassQueen
a.k.a dumpsqueen.com

HCIA-IoT V2.5 Exam

Huawei H12-111_V2-5

Version Demo

Total Demo Questions: 23

Total Premium Questions: 235

Buy Premium PDF

https://passqueen.com

support@passqueen.com

Topic Break Down

Topic	No. of Questions
Topic 1, IoT Overview	21
Topic 2, IoT Communication Technology	62
Topic 3, IoT Platforms	31
Topic 4, Huawei IoT Solution	87
Topic 5, IoT Application Development	23
Topic 6, IoT Security	11
Total	235

QUESTION NO: 1

Among the following options, the security technologies suitA, Ble for use on simple end devices are ()? (Multiple choice)

A. PSK

B. VPN

C. Certification

D. Encryption

ANSWER: A C D

Explanation:

PSK, Certification, and Encryption are suitable security technologies for simple IoT end devices because they can provide essential identity and data-protection capabilities with implementations tailored to constrained hardware. A pre-shared key enables a device and platform to authenticate each other using a secret provisioned during manufacturing or onboarding. This approach has relatively low computing and storage requirements, which makes it practical for devices with limited memory, processor performance, and power availability.

Certification supports device identity authentication through device certificates and public-key infrastructure. It enables a platform to identify an individual device rather than relying only on a shared group secret, and can be used with lightweight IoT security protocols and managed certificate lifecycles. Encryption protects the confidentiality of telemetry, commands, configuration data, and credentials while they are transmitted or stored. In practice, lightweight symmetric encryption is especially appropriate on constrained endpoints, while certificate-based mechanisms may be selected where stronger identity management is needed. Huawei IoTDA documentation describes device authentication mechanisms and secure device access in its security guidance; Huawei also documents secure device connectivity in the IoTDA developer guide.

QUESTION NO: 2

OceanConnest provides IoT services to end users.

A. Correct

B. Error .

ANSWER: B

Explanation:

“Error” is correct because OceanConnect is positioned as an IoT platform that connects devices, manages device connectivity and data, and exposes platform capabilities through open interfaces for application developers and industry applications. Its role is to provide the enabling IoT services on which vertical solutions—such as smart city, utilities, transportation, or manufacturing applications—are built. Those applications in turn deliver the user-facing functions and experiences to their respective customers or end users.

In other words, OceanConnect operates as the platform layer in an IoT solution rather than as the direct end-user service layer. It supports common capabilities including device access, device management, data collection, data processing, and integration with applications. This architecture lets solution providers develop services for specific industries without having to build the underlying device-connectivity and management platform themselves. Huawei’s IoT platform documentation describes these device and application enablement functions, while Huawei’s OceanConnect materials identify the platform as a foundation for industry IoT solutions. See Huawei OceanConnect and Huawei Cloud IoT Device Access product documentation.

QUESTION NO: 3

The order to add a whitelist to the AR502EGRc-Lc model gateway is ()?

A. zigbee-network permit-join whitelist longid

B. rf-network permit-join whitelist longid

C. hiplc-network permit-join whitelist longid

D. network permit-join whitelist longid

ANSWER: B

Explanation:

The correct command is **rf-network permit-join whitelist longid**. On the AR502EGRc-Lc, RF-network commissioning and access-control operations are entered in the `rf-network` command context. The `permit-join` portion controls whether devices may join the RF network, while `whitelist` specifies that joining is restricted to an approved-device list. The `longid` parameter identifies a device by its long identifier, which is the identifier used when adding that device to the permitted-join whitelist. This command structure therefore combines the appropriate RF-network command namespace, join-permission operation, whitelist mechanism, and required device-identifier type. Huawei documentation and software resources for enterprise gateways are accessed through the Huawei Enterprise Support portal; select the applicable gateway model and software version before using the related command reference. See the Huawei Enterprise Support portal and Huawei's enterprise router and gateway product resources.

QUESTION NO: 4

Does the Huawei LiteOS Security Framework contain () part? (Multiple choice).

A. Endpoint Security

B. End-cloud security

C. Transmission security

D. Chip security

ANSWER: A B C

Explanation:

Huawei LiteOS applies a layered, end-to-end security approach for IoT deployments. The framework includes endpoint security, which protects the device-side environment through measures such as secure startup, identity authentication, access control, and protection of sensitive assets. It also includes transmission security, ensuring that data exchanged between devices and platform services is protected in transit through authenticated, encrypted communication channels. End-cloud security is the cloud-side component of this security model. It protects IoT platform services, device management, application access, data handling, and the trusted interaction between endpoints and cloud resources. Together, endpoint security, transmission security, and end-cloud security establish the security coverage required across the full IoT data path: from the physical endpoint, across the network, to the cloud platform. This layered model is particularly important because IoT systems combine constrained devices, potentially untrusted networks, and remotely managed cloud services. Huawei describes LiteOS as an IoT operating system designed for connected-device scenarios at Huawei LiteOS. Huawei Cloud's IoT documentation also outlines security capabilities for device-to-cloud IoT services at Huawei Cloud IoT security documentation.

QUESTION NO: 5

What are the main processes of OceanConnect ()? (Multiple choice)

A. Southbound message escalation process

B. Business Issuance Process

C. Northbound registration process .

D. Southbound registration process .

ANSWER: A B C D

Explanation:

OceanConnect's end-to-end operational model includes onboarding applications at the northbound interface, registering devices through the southbound interface, issuing services or business operations toward managed devices, and escalating messages reported from devices to applications. Therefore, "Northbound registration process" is a main process because applications must be registered and authenticated before they can consume platform capabilities and device information. "Southbound registration process" is also fundamental because it establishes device access and registration with the platform through the device-facing side.

"Business Issuance Process" represents the platform-to-device operational path used to deliver service requests, management actions, or commands through the appropriate device connectivity channel. "Southbound message escalation process" represents the reverse reporting path: device-originated data, events, and notifications are received by the platform and forwarded upward for application handling. Together, these processes describe the complete interaction lifecycle between applications, OceanConnect, and connected devices. Huawei's cloud Internet-of-Things documentation describes the platform's device connectivity, management, and application integration capabilities: Huawei Cloud IoT services and Huawei Cloud IoT documentation.

QUESTION NO: 6

In the power industry, the main advantages of using eLTE-IoT to achieve AMI remote meter reading are wide coverage, massive connections, easy to deploy and expand.

A. Correct

B. Error

ANSWER: A

Explanation:

Correct is the right answer. Advanced Metering Infrastructure (AMI) requires a communications network that can reliably connect large numbers of geographically distributed electricity meters, including meters in basements, rural areas, apartment buildings, and other locations where signal penetration is important. Huawei eLTE-IoT is designed for industry private-network IoT scenarios and uses LTE-based radio technology to provide broad-area wireless coverage and reliable connectivity for terminals such as smart meters. Its cellular architecture supports a high density of connected devices, which is essential when a utility must collect readings and status information from a very large meter population. The solution also reduces dependence on extensive wired communication construction: base-station coverage can be planned and expanded as meter deployments grow. This makes network rollout and later capacity expansion more practical for utility AMI projects. In addition to periodic meter-reading data, a utility can use the same wireless infrastructure for operational information and device management, helping support digital grid modernization. Huawei describes eLTE-IoT as an LTE-based solution for vertical-industry IoT connectivity at Huawei eLTE-IoT. The LTE radio foundation is standardized by 3GPP; see 3GPP LTE.

QUESTION NO: 7

NB-IoT system broadband is ()?

A. 3.75kHz

B. 15kHz

C. 180kHz

D. 60kHz

ANSWER: C

Explanation:

The correct value is **180kHz**. NB-IoT is designed as a narrowband cellular IoT radio technology and occupies a 180 kHz carrier, corresponding to the bandwidth of one LTE physical resource block. This compact spectrum requirement is a core reason NB-IoT can support broad coverage, low device complexity, and long battery life for massive numbers of low-throughput devices such as meters, sensors, trackers, and alarms.

In LTE deployments, an NB-IoT carrier can be deployed in three principal ways: stand-alone, within an LTE carrier using unused resource blocks, or in the guard band of an LTE carrier. In each deployment approach, the NB-IoT radio carrier retains its 180 kHz bandwidth. The subcarrier spacing used by particular NB-IoT uplink or downlink transmissions should not be confused with the overall system carrier bandwidth. For example, narrower subcarrier spacings can be used for coverage and device-operation purposes, while the defined NB-IoT carrier itself remains 180 kHz wide.

This specification is reflected in the NB-IoT radio requirements published by 3GPP and ETSI. See 3GPP NB-IoT and ETSI TS 136 101.

QUESTION NO: 8

Adding a task to the task stack before the system runs is no different from adding a task to the task stack after the system runs.

A. Correct

B. Error

ANSWER: B

Explanation:

Error is correct. In Huawei LiteOS, task creation is dependent on the kernel's current initialization and scheduling state, so creating a task before the system starts is not equivalent to creating one after the system is running. During the initialization phase, tasks can be created and placed in the ready queue, but they do not execute until the scheduler is started. This enables an application to establish its initial task set, priorities, stacks, and other resources in a controlled order before multitasking begins.

After the system starts, the scheduler is active. Creating a task may immediately affect scheduling: if the new task is in the ready state and has a higher priority than the currently running task, LiteOS can schedule it promptly. Thus, task creation after startup can cause a context switch and concurrent execution, whereas task creation before startup cannot run the newly created task until scheduler startup. The timing, execution behavior, and scheduling consequences are therefore materially different. Huawei LiteOS task and scheduler source interfaces, including task creation and scheduler initialization, are available in the official Huawei LiteOS repository; related kernel documentation is provided through the LiteOS documentation site.

QUESTION NO: 9

Among the following communication technologies, the frequency band is in the SubG license-free band ()? (Multiple choice)

A. Wifi

B. NB-IoT

C. Sigfox

D. Lora

ANSWER: C D

Explanation:

Sigfox and Lora are both designed for low-power wide-area IoT communications and commonly operate in licence-exempt sub-1 GHz spectrum. "SubG" means frequencies below 1 GHz; the exact band is region-dependent. For example, deployments commonly use 868 MHz in Europe and 902–928 MHz in North America. These lower-frequency bands provide

favorable propagation characteristics for IoT: compared with higher-frequency short-range radio systems, signals can generally travel farther and penetrate buildings and obstacles more effectively at low power. This makes them suitable for battery-powered sensors, metering, tracking, alarms, and similar devices that send relatively small amounts of data intermittently over a wide area.

LoRaWAN regional parameters formally define the channel plans and operating requirements for unlicensed regional ISM bands, including EU868 and US902–928. Sigfox likewise specifies regional radio configurations, including operation in the European 868 MHz and North American 902 MHz licence-exempt bands. Therefore, Sigfox and Lora are the communication technologies in the listed choices that use SubG licence-free spectrum. See the LoRaWAN Regional Parameters and Sigfox Radio Configurations.

QUESTION NO: 10

Regardingthe features of the OceanConnect platform, the following is not under the permission management ()?

A. Access permissions

B. Login certificate

C. Data storage encryption

D. Account sub-permissions

ANSWER: C

Explanation:

Data storage encryption is the correct answer because it is a data-security capability rather than a permission-management capability. Permission management governs identity-based control: it determines which user, account, application, or tenant can authenticate and which platform resources or operations that identity is authorized to access. This type of control is generally implemented through accounts, credentials, roles, policies, and fine-grained authorization.

Data storage encryption instead protects the confidentiality of information while it is stored. It transforms stored data into ciphertext and requires the appropriate cryptographic key to recover readable data. Consequently, encryption remains relevant even after storage media are copied, lost, or accessed outside an expected application path. In a cloud IoT platform architecture, encryption at rest is normally associated with data protection and key-management services, while authorization is associated with identity and access management. Huawei Cloud describes identity and access management as controlling access to cloud resources through users, groups, and permissions: Huawei Cloud IAM User Guide. Huawei Cloud also documents encryption and key management as cryptographic protection services for data: Huawei Cloud Data Encryption Workshop User Guide.

QUESTION NO: 11

In Modbus TCP communication, the default server port number is ()?

A. 80

B. 443

C. 502

D. 1883

ANSWER: C

Explanation:

The correct answer is **502**. Modbus TCP encapsulates Modbus application data in TCP/IP packets, and TCP port 502 is the well-known port assigned for Modbus/TCP communication. An IoT gateway or industrial controller acting as a Modbus TCP client normally establishes a TCP connection to port 502 on the Modbus TCP server.

Port 502 should not be exposed directly to untrusted networks. Industrial deployments should use network segmentation, firewalls, access control, and secure remote-access mechanisms to protect Modbus devices. The Modbus TCP/IP implementation guide is available from Modbus Organization.

QUESTION NO: 12

Common scenarios for issuing control commands in Internet ofVehicle Applications are ()?

(Multiple choice)

A. Lock the car

B. Acquisition module software version

C. Location information query

D. Location information is reported

ANSWER: A B C

Explanation:

In an Internet of Vehicles application, a cloud platform or mobile application issues a command when it needs the vehicle terminal to perform an action or return information in response to a request. “Lock the car” is a typical remote-control command: the platform sends an instruction to the vehicle, and the terminal executes the lock operation and can return an execution result. “Acquisition module software version” is also a valid command scenario because fleet operators commonly query a vehicle device’s software or firmware version for asset inventory, compatibility checking, fault analysis, and upgrade planning. “Location information query” likewise represents a command-driven request for the vehicle terminal to obtain and return its current positioning data. These scenarios all have the essential command pattern of cloud-to-device delivery, followed by device processing and, where applicable, a response. Huawei IoT device-management services support sending commands to devices and receiving command execution results, which is the underlying mechanism used for such vehicle-control and information-query operations. See Huawei Cloud documentation on sending commands to devices and the IoTDA API reference.

QUESTION NO: 13

Among the followingIoT access technologies, the highest power consumption is ()?

A. eMTC

B. LTE-V

C. GPRS

D. NB-IoT

ANSWER: B

Explanation:

LTE-V is the correct choice. In this IoT-access comparison, LTE-V is associated with the highest power consumption because it is intended for vehicle-to-everything communication, including demanding safety and cooperative-driving scenarios. LTE-V devices must support highly reliable, low-latency communication while vehicles are moving at high speed, and may transmit or receive frequent status and awareness messages. This operational profile requires more radio activity and processing capability than technologies optimized primarily for long battery life and small, infrequent IoT messages.

LTE-V is based on cellular vehicle-to-everything capabilities, including direct sidelink communications between vehicles and other road participants or infrastructure. The 3GPP overview of V2X describes these communications as supporting road-safety and advanced driving use cases, which require timely exchange of information in dynamic environments. Such requirements make LTE-V suitable for vehicles, where electrical power is generally available from the vehicle, rather than for ultra-low-power sensors expected to operate for years on a small battery. Therefore, within the technologies listed, LTE-V is

the expected highest-power-consumption access technology. See the 3GPP V2X technology overview and Huawei's LTE-V2X overview for additional context.

QUESTION NO: 14

When the terminal is in PSM (power saving mode), the control instructions issued by the service platform cannot reach the terminal in real time, and the downstream control instructions need to be cached in the operator's ()?

A. Base station

B. Business platform

C. IoT Platform

D. Core network

ANSWER: C

Explanation:

IoT Platform is correct. In Power Saving Mode (PSM), an NB-IoT terminal becomes unreachable for normal mobile-terminated communication in order to minimize energy consumption. The terminal does not continuously monitor paging or maintain an active signaling connection; instead, it becomes reachable again when it performs a scheduled tracking-area update or otherwise resumes communication according to its configured active-time and extended-discontinuous-reception behavior.

Accordingly, a service application can submit a downstream command while the terminal is asleep, but the operator-side IoT platform must retain that command until the device next becomes available. The IoT platform acts as the service-facing capability layer: it accepts application requests, associates them with the target device, manages device connectivity state, and supports deferred delivery of commands. Once the terminal reconnects or wakes at its scheduled opportunity, the platform can forward the cached downlink instruction through the cellular network.

This store-and-forward behavior lets battery-powered IoT devices use long sleep periods without requiring the service platform to repeatedly send commands or maintain direct real-time reachability. PSM operation is specified in 3GPP TS 23.682; see also the GSMA's NB-IoT Deployment Guide.

QUESTION NO: 15

The description of the Northbound app registration direct connection device, incorrect is ()?

A. When registering a direct-attached device, nodeid recommends using the MAC address of the device

B. Register direct-attached device interface, which can be used not only to register direct-attached devices, but also to register non-direct-attached devices .

C. When registering a direct-attached device, there is no timeout setting if timeout is set to 0

D. After registering a direct-attached device interface call, if the binding is not completed within the timeout range, the device registration will be invalidated

ANSWER: B

Explanation:

"Register direct-attached device interface, which can be used not only to register direct-attached devices, but also to register non-direct-attached devices ." is the incorrect statement. In Huawei IoT platform terminology, a directly connected device is a device that communicates with the IoT platform itself, whereas a non-directly connected device is managed through a gateway. These are distinct onboarding and connectivity models. The northbound registration API specifically intended for directly connected devices creates registration information for the direct-device model; it does not also serve as the registration mechanism for gateway-subordinate devices. A non-directly connected device must instead be associated with its gateway using the platform's gateway/subdevice management workflow and corresponding APIs. This separation lets the

platform maintain the correct device topology, route messages through the appropriate connection, and apply the applicable authentication and lifecycle management process. Huawei's IoT documentation describes direct and gateway-mediated device access as separate connection approaches and provides dedicated API guidance for device management. See the Huawei Cloud IoTDA User Guide and the Huawei Cloud IoTDA API Reference.

QUESTION NO: 16

Among the followingoptions, the process initiated by the IoT device has ()? (Multiple choice)

A. Southbound message escalation process

B. Business issuance process

C. Control the message delivery process

D. Southbound Registration Process

ANSWER: A D

Explanation:

The device-initiated interactions are the **Southbound message escalation process** and the **Southbound Registration Process**. In the registration process, an IoT device begins the interaction by connecting to the IoT platform and submitting its identity or authentication information. This allows the platform to recognize the device and establish an authorized communication relationship before normal service traffic is exchanged. Registration is therefore a foundational device-originated operation.

In the southbound message escalation process, the device originates telemetry, status, event, alarm, or other collected data and reports it to the platform. The platform receives this uplink information and can subsequently expose it to applications, rules engines, storage, or operations systems. This direction is device-to-platform, even though "southbound" terminology can vary between translated training materials and platform architecture diagrams. Huawei's IoT Device Access documentation describes device connectivity and message exchange as core device-access functions; see the Huawei Cloud IoT Device Access documentation. MQTT, a common protocol for this communication model, likewise supports a client/device publishing data after establishing a connection, as specified by the MQTT specification.

QUESTION NO: 17

Can the following () business applications be implemented with eLTE-IoT? (Multiple choice).

A. Remote meter reading (meter, water meter)

B. Voicecalls

C. Video backhaul

D. Smart Street Lights

E. Environmental monitoring

ANSWER: A D E

Explanation:

eLTE-IoT is designed for wide-area IoT connectivity where large numbers of distributed devices transmit relatively small amounts of data, require broad coverage, and benefit from low power consumption. "Remote meter reading (meter, water meter)" is a core IoT use case: meters periodically report readings and status information to a utility platform, enabling automated billing, fault detection, and operational visibility without manual collection.

"Smart Street Lights" is also well suited to eLTE-IoT because each lamp controller can report operating state, energy use, and alarms, while receiving commands for switching and dimming. This allows centralized and fine-grained municipal lighting management. "Environmental monitoring" fits the same connectivity model: geographically dispersed sensors can

periodically send measurements such as air quality, temperature, humidity, water level, or pollutant data to a monitoring application.

Huawei describes eLTE-IoT as supporting vertical IoT scenarios that need wide coverage, massive connections, and low-power communications. These capabilities align directly with metering, smart-city lighting, and environmental sensing deployments. See Huawei's eLTE-IoT solution overview and its IoT technology overview.

QUESTION NO: 18

Is the IoT gateway in the () position of the entire IoT solution?

A. Middle layer, downstream aggregation, upstream forwarding.

B. Application layer, providing rich data processing capabilities

C. Perception layer, providing rich sensing data acquisition capabilities

D. Software platform layer, providing rich protocol adaptation capabilities

ANSWER: A

Explanation:

The IoT gateway occupies the middle layer of an end-to-end IoT solution, acting as the bridge between field devices and the upstream IoT platform or application environment. On its downstream side, it connects to and aggregates data from sensors, controllers, and other device-side nodes, often across local or specialized access networks. This aggregation reduces the number of direct cloud connections and provides a controlled point at which device communications can be collected and managed.

On its upstream side, the gateway forwards collected device data to the platform and can receive platform commands for delivery to devices. In practical deployments, it may also perform local protocol conversion, connectivity management, filtering, and edge-side processing before data is transmitted upstream. This placement is fundamental because the gateway links heterogeneous device networks with IP-based platform services while supporting reliable bidirectional communication. Huawei's edge-computing documentation describes edge nodes as providing the connection and local processing layer between devices and cloud services, consistent with this gateway role. See Huawei Cloud Intelligent EdgeFabric overview and Huawei Cloud IoT Device Access product description.

QUESTION NO: 19

The positioning in the refinery can be completed by the positioning of the base station.

A. Correct

B. Error

ANSWER: B

Explanation:

Error is correct because base-station positioning alone is not a generally sufficient positioning solution for a refinery environment. A refinery is a complex industrial site containing dense metal structures, process units, tanks, pipes, and both indoor and outdoor operating areas. These conditions can obstruct, reflect, and attenuate radio signals, reducing the accuracy and reliability that can be obtained from cellular base-station measurements. Industrial positioning must instead be selected according to the required positioning precision, coverage area, device capabilities, and the site radio survey. Depending on the use case, a refinery deployment may combine cellular positioning with GNSS for suitable outdoor areas, or use dedicated short-range technologies such as Bluetooth, Wi-Fi, UWB, or RFID where more precise indoor or asset-level positioning is required. Huawei's IoT portfolio supports connecting and managing diverse devices and networks, while the positioning method remains dependent on the deployment environment and service requirement. This site-specific approach is consistent with industrial IoT design practices and 3GPP positioning architecture, which supports multiple positioning

methods rather than treating cell-based positioning as universally adequate. See Huawei ICT Insights: Intelligent IoT and 3GPP Positioning.

QUESTION NO: 20

Among the following options, which functions can be implemented by an IoT rule engine ()? (Multiple choice)

A. Trigger an alarm when a reported value exceeds a threshold

B. Forward device data to an application server

C. Deliver a command according to a condition

D. Replace the device communication protocol

ANSWER: A B C

Explanation:

A rule engine processes device messages or events against configured conditions and then triggers defined actions. **Triggering an alarm when a reported value exceeds a threshold** is a typical rule because the platform can compare telemetry with a configured limit. **Forwarding device data to an application server** is also correct because rules can route matched data to northbound services. **Delivering a command according to a condition** is correct because a rule can initiate a cloud-to-device action when specified event criteria are met.

Replacing the device communication protocol is not a normal rule-engine function. Protocol adaptation is performed by device-access, gateway, or codec capabilities before business rules process the normalized device data. Huawei Cloud IoTDA documentation describes rules and device-message processing at Huawei Cloud IoTDA User Guide.

QUESTION NO: 21

Can the MobileCam solution be widely referenced in the following (domain)? (Multiple choice)

A. Smart Camera

B. Video doorbell

C. Drone

D. Motion DV

ANSWER: A B C D

Explanation:

Huawei MobileCam is intended as a reusable mobile-video solution for consumer and lightweight intelligent-video devices, rather than being restricted to one camera form factor. Its capabilities are applicable to **Smart Camera** products, which need networked video capture, viewing, management, and intelligent device integration. They also apply to **Video doorbell** devices, where a compact camera endpoint provides event-based video and remote interaction.

The same solution scope includes mobile and wearable imaging scenarios. A **Drone** can use mobile video capabilities for image acquisition, transmission, storage, and user-side viewing, while **Motion DV** devices (sports or action cameras) similarly require portable video capture and mobile connectivity. These product categories share the core characteristics addressed by MobileCam: camera-based media collection, network communication, device management, and delivery of video services to users. Huawei's IoT documentation describes the general device-to-cloud model used by connected smart devices, and Huawei's media documentation provides the related media-service context: Huawei Cloud IoTDA User Guide and Huawei Media Services Overview.

QUESTION NO: 22

Among the following options, which belong to the difficulties currently encountered by the

Internet of Things ( )? (Multiple choice)

A. Multi-sensor collA, Borative management complex

B. High performance and power consumption requirements in video scenarios

C. Complex and diverse communication protocols between terminals

D. Inefficient and difficult to develop voiceprogramming

ANSWER: A B C D

Explanation:

IoT deployments must connect, manage, and derive value from large numbers of heterogeneous devices, which makes multi-sensor collaborative management complex. Sensors can differ in data formats, sampling rates, capabilities, locations, and operational states; coordinating their data and lifecycle management is therefore a significant practical challenge. Video-based IoT scenarios also impose demanding performance and power-consumption requirements because capturing, encoding, transmitting, and sometimes analyzing video requires substantially more compute, bandwidth, storage, and energy than many simple telemetry workloads.

Complex and diverse communication protocols between terminals are another core IoT challenge. Devices may use different wired and wireless access technologies and application protocols, so platforms need interoperability mechanisms, gateways, device adaptation, and unified management. Inefficient and difficult voice programming is likewise relevant where voice interaction is used for device control: robust speech recognition and intent handling must operate reliably despite constrained edge hardware, noisy environments, connectivity variation, and diverse user expressions. Huawei's IoT overview describes the need to connect and manage diverse devices and data, while its IoTDA service documentation highlights protocol adaptation and device connectivity considerations. See Huawei Cloud IoT Device Access and Huawei: What Is IoT?.

QUESTION NO: 23

Huawei LiteOS DeveloperCommunity Provides () Support? (Multiple choice).

A. Kernel code

B. Development documentation

C. Scenario-based SDK

D. Forum

ANSWER: A B C D

Explanation:

Huawei LiteOS developer resources are intended to support the full embedded-IoT development lifecycle. **Kernel code** is provided so developers can obtain, inspect, port, configure, and build the lightweight operating-system components needed for constrained devices. The LiteOS open-source project includes source code and supporting build materials, enabling practical development and adaptation to target hardware. **Development documentation** is also essential support: developers need guidance for platform architecture, APIs, porting, compilation, debugging, and IoT application development.

Scenario-based SDK support helps developers implement common IoT solutions more efficiently by supplying reusable capabilities and examples suited to typical device scenarios. Finally, a **Forum** provides a community channel for technical discussion, issue sharing, experience exchange, and collaboration among developers. Together, these resources combine code access, technical guidance, reusable development assets, and peer/community assistance rather than limiting support to a single tool or document set. The LiteOS project's publicly available source and documentation resources can be reviewed at Huawei LiteOS on GitHub. Huawei's broader open-source commitment and ecosystem information is available through Huawei Open Source.