



HAL
open science

Huawei HCIA-IoT v. 2.5 Evaluation Questions

Michel Bakni

► **To cite this version:**

Michel Bakni. Huawei HCIA-IoT v. 2.5 Evaluation Questions. Engineering school. Huawei HCIA-IoT v. 2.5, Bidart, France. 2023, pp.157. hal-03189245v2

HAL Id: hal-03189245

<https://hal.science/hal-03189245v2>

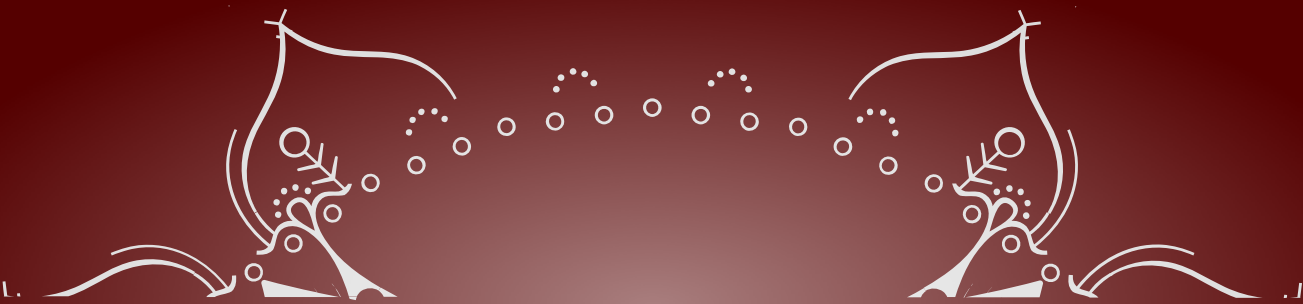
Submitted on 10 Sep 2023

HAL is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



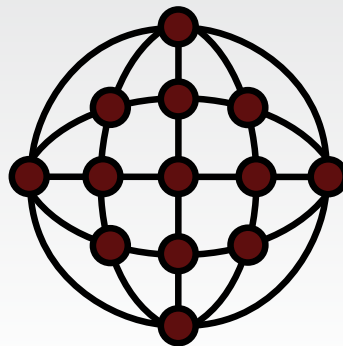
Distributed under a Creative Commons Attribution| 4.0 International License



Huawei HCIA-IoT v. 2.5: Evaluation Questions



IoT
Internet of things



Michel Bakni

2023

2nd Ed.

**Enlarged &
Carefully revised**

Huawei HCIA-IoT v. 2.5

Evaluation Questions

**Supported
with Illustrations**

&

Definitions of Abbreviations

Michel BAKNI

September 2023

2^{ed} Edition

Enlarged & Carefully Revised

Title: Huawei HCIA-IoT v. 2.5 Evaluation Questions
Author: Michel BAKNI **Author ISNI:** 0000 0005 0354 6620
Year: 2023 **Edition:** 2
Cover design: Zeina KHOURY
ISBN: 978-2-9576887-2-2 **DOI:** 10.6084/m9.figshare.22337185

HUAWEI is a trademark of Huawei Technologies Co., Ltd.

Copyright notice

This work is licensed under Creative Commons Attribution 4.0 International (CC BY 4.0)

You are free to:

Share — copy and redistribute the material in any medium or format

Adapt — remix, transform, and build upon the material

for any purpose, even commercially.

The licensor cannot revoke these freedoms as long as you follow the license terms:

Attribution — You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

No additional restrictions — You may not apply legal terms or technological measures that legally restrict others from doing anything the license permits.

Read the text of the full license Creative Commons Attribution 4.0 International on the following link: <https://creativecommons.org/licenses/by/4.0/legalcode>



For more information on the Huawei copyright policies, and the use of the word HUAWEI in the title: <https://consumer.huawei.com/en/legal/intellectual-property/huawei-trademark-policy/>

The font used in this document is Calibri. It is a copyrighted property for Microsoft. It is embedded from a Microsoft word 365 application that is not for home, student, or non-commercial use.

Application license ID: EWW_15cd13b2-4549-42f8-9d2f-00d8bd8e0e9f_ca421d4c3fbc11eecd

The illustrations used in this book are created by the author. They are all licensed under CC BY-SA Version 4.0

2^{ed} Edition Preface

Gladly, two years after the first edition was issued, we come back with a more comprehensive version of this booklet: "Huawei HCIA-IoT v. 2.5 Evaluation Questions". In this edition, we adopted several pedagogical enhancements to make the book one of the best tools available for students preparing to pass the HCIA-IoT v. 2.5 exam.

Over the last two years, I have received several emails from professors and students all around the world, with dozens of recommendations, notes, and corrections. I am grateful for them all, they were useful in creating a better and solid version of the learning material. So, after you read this work, feel free to share your ideas back on how you think this booklet can be better realized.

Compared to the 1st edition, this edition includes several enhancements. Mainly, we added a new section for each chapter, to include multiple-choice questions that have more than one correct answer. Furthermore, we extended the abbreviation section by adding definitions to clarify the meaning. We also added a small section with several illustrations, we believe, based on our experience teaching the course, that they are useful for students to enlarge their general understanding.

As I always do, I insist that this is not an exam dump, and it should never be treated as such. Instead, this is an auxiliary material created to help students prepare for the exam, and it is not enough for the students, by all means, to the pass official exam if used alone with no suitable preparation.

Finally, I would like to thank Pallavi Malhotra, Director of the Huawei Talent Alliance in the Western European Region for her nice words and support. I met Mme. Malhotra in Barcelona last year, at the UNESCO 3rd World Higher Education Conference (WHEC2022), where I presented the manuscript to her, and she was very encouraging and supportive of this non-profit initiative. I would also like to thank my professor, Mr. Octavian CUREA, for helping to structure the document, thus, it became in its current form.

Bayonne

19-03-2023

1st Edition Preface

This document is oriented towards students preparing for the exam of Huawei Certified Information and communication technology Associate (HCIA-IoT) v. 2.5. The main idea of this booklet is to provide students with an evaluation tool for their understanding of the course content. This booklet is not an exam dump, and it should never be handled like that. HCIA-IoT is a course provided by Huawei. It focuses on the Internet of things explaining the technologies used to support it, such as 5G and NB-IoT. It also introduces Huawei products and solutions in this domain.

The structure of this document follows the chapters of the course. For each chapter, there are two groups of questions: True or false and multiple choices questions. Additionally, the booklet includes a table for abbreviations used in this course in alphabetical order.

I recommend the following steps to maximize the benefits of this document (Figure1):

1. Read the targeted chapter from the course support.
2. Try to answer the questions associated with the targeted chapter in this document.
 - a. If you succeed (more than 90% of answers are correct), go forward for the next chapter.
 - b. If not, go backward and study the targeted chapter with more careful.

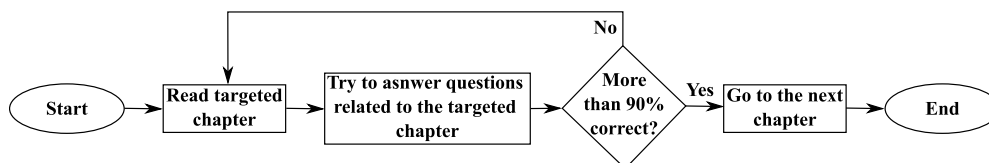


Figure 1: Flow chart explaining a proposed mechanism to address this booklet.

I had the chance to work with Huawei in France in February and March 2021. In this period, I prepared this document. Unfortunately, the spread of COVID-19 was at its highest rates. The course had to follow very strict instructions of the local authorities. However, we were able to touch physical materials and develop several labs using IoT Huawei developer kit.

Paris

15-03-2021

Attention: Studying this document only is not enough to pass the official exam.

Contents at a Glance

Changes to Edition 1:	8
Chapter 1. IoT development history and Overview	9
Chapter 2. IoT Industry Applications and Solutions	18
Chapter 3. IoT Security Technologies	26
Chapter 4. Overview of Common IoT Communications Technologies	35
Chapter 5. NB-IoT Communication Technologies and Solutions	46
Chapter 6. 5G Communications Technologies and Solutions	55
Chapter 7&8. Huawei IoT Gateways (Industrial + Home)	63
Chapter 9. IoT Platform	73
Chapter 10. IoT Platform Secondary Development	85
Chapter 11. IoT OS	95
Chapter 12. Sensing Layer Development	102
Chapter 13. AT Commands for Communication Modules	112
Answers	115
Appendix I: Abbreviations	127
Appendix II: Reference images	154
Author Biography	156

Changes to Edition 1:

- Adding a third section for each chapter containing multiple-choice questions with more than one correct answer. The objective is to comply with the approved examination system.
- Adding a new section with 5 reference images.
- Adding definitions for the acronyms in the abbreviations section.
- Change the font used from the copyrighted Times new roman to Calibri, which is licensed free.
- Re-numbering the chapters in accordance with the numbering used in the official course.
- Correct minor typos and misspellings.
- Adding colored cover.
- Adding ISBN.
- Adding 2nd author's preface.
- Adding the author's biography at the end of the booklet.

Chapter 1. IoT development history and Overview

A. Mark the followings True or False?

1. The Trojan room coffee pot of the computer laboratory in Cambridge University is an example of an IoT solution.
2. ITU referred to the IoT concept at the world summit on the information society in 2005.
3. NB-IoT is developed for 5G technologies.
4. The first 3GPP standard for the 5G is Release-16.
5. VR glasses, body fat scales, smart locks, and smart speakers are examples of industry-related IoT products.
6. Smart agriculture is an example of industry-related IoT products.
7. IoT is an Internet where all things are interconnected.
8. IoT requires moving from the internet of things to the internet of people.
9. IoT model includes 4 layers.
10. In the IoT model, the platform layer collects information and process signals.
11. Huawei IoT solution architecture is 1+2+1.
12. Huawei cloud IoT platform is open, pre-integrated and access-dependent.
13. Bluetooth is an example of communication protocols used by IoT applications.
14. Fully open smart ONT requires a bit rate up to 1 Gbit/s.
15. In the IoT model, device management and security maintenance are performed by the platform.
16. Huawei IoT Solution Architecture 1+2+1 means: one IoT access method, two platforms, and one IoT operating system.
17. Huawei LiteOS features low power consumption, small size, and quick response.
18. NB-IoT stands for NearBand Internet of Things.
19. Huawei LiteOS features a basic kernel size less than 20 kB.
20. 5G Architecture supports both NFV and SDN.
21. IoT is a technology designed based on internet technologies.

22. IoT is a data service technology.
23. Huawei provides a full stack solution to meet IoT requirements.
24. The network layer is the layer of things.
25. The top layer of the Huawei's full stack IoT solution is the platform layer.
26. The platform layer is equivalent to a communication medium between the sensing layer and the network layer.
27. The application layer is oriented to costumers.
28. The platform layer in the IoT solution is divided into two sublayers, the lower sublayer is called service enablement layer.
29. According to the Huawei IoT solution, there are two network access modes.
30. NB-IoT is an IoT solution of Huawei.

B. Choose the correct answer, there is only one correct answer for each question:

1. Which of the followings is considered the oldest known mention of IoT:
 - A. Bill Gates book (the road ahead)
 - B. ITU internet reports.
 - C. Trojan room coffee pot
 - D. Hannover messe

2. In which release of the 3GPP the NB-IoT standard was frozen?
 - A. 13
 - B. 14
 - C. 15
 - D. 16

3. Which of the followings Chinese mobile operator(s) was(were) the first 5G network(s) commercially used?
 - A. China Telecom
 - B. China Mobile
 - C. China Unicom
 - D. All of them

4. In which quarter of 2019, the 5G networks were employed in China for public commercial use?
 - A. First
 - B. Second
 - C. Third
 - D. Fourth

5. Development of IoT industry is driven by:
 - A. Consumers
 - B. Policies
 - C. Industry
 - D. All of them

6. One of the followings is not a policy-driven application of the IoT industry:
 - A. Firefighting
 - B. Smart agriculture
 - C. Parking
 - D. Street lightning

7. One of the followings is consumption-driven application of the IoT industry:
- A. Smart speaker
 - B. Public utilities
 - C. Security system integration
 - D. Internet of Vehicles
8. Which of the followings is industry-driven application of the IoT industry?
- A. Smart agriculture
 - B. Smart logistics
 - C. IoV
 - D. All of them
9. From 1999 to 2013, the term “connected objects” was used to describe:
- A. Smart wearable devices
 - B. Smart home utilities
 - C. Things in the radio frequency domain
 - D. Industrial devices and applications
10. How many layers are there in the IoT model?
- A. 2
 - B. 3
 - C. 4
 - D. 5
11. Which of the followings layer of the IoT model provides data presentation and customer interaction services?
- A. Application layer
 - B. Platform layer
 - C. Network layer
 - D. Device layer
12. One of the followings is not a component of the platform layer in the IoT model:
- A. Cloud data center
 - B. Operations platform
 - C. IoT gateways
 - D. Security maintenance

13. Which of the followings is a network layer technology in the IoT model?
- A. GPRS
 - B. NB-IoT
 - C. 4G
 - D. All of them
14. One of the followings is not an example of an IoT applications:
- A. Smart home
 - B. Huawei LiteOS
 - C. Safe city
 - D. IoV
15. Which of the following solutions for the IoT model architecture is proposed by Huawei?
- A. 1+2+1
 - B. 2+1+1
 - C. 2+1+2
 - D. 1+1+2
16. The adapted Huawei IoT architecture includes:
- A. Two IoT platform, two access methods and one IoT operating system
 - B. One IoT platform, two access methods and one IoT operating system
 - C. One IoT platform, two access methods and two IoT operating system
 - D. None of them
17. One of the followings is not an example of protocols used in the NB-IoT end-to-end solution:
- A. HTTP
 - B. MQTT
 - C. ICMP
 - D. CoAP

18. One of the followings is not an example of devices used in the NB-IoT end-to-end solution:

- A. MCUs
- B. Modules
- C. NB-IoT chipsets
- D. HTTP

19. Which of the following connectivities is required in a smart home using ONT technology?

- A. 1 Mbit/s
- B. 1 Gbit/s
- C. 1 Tbit/s
- D. None of them

20. HUAWEI CLOUD IoT platform is:

- A. Open
- B. Pre-integrated
- C. Service-oriented
- D. All of them

C. Choose the correct answer, there are multiple correct answers for each question:

1. Which of the followings are considered as IoT application classes?
 - A. Policy-driven
 - B. Agriculture-driven
 - C. Industry-driven
 - D. Application-driven

2. Which of the followings are considered as policy-driven applications?
 - A. Smart cities
 - B. Smart logistics
 - C. IoV
 - D. Smart speakers
 - E. Smart streetlamp

3. Which of the followings are not considered as industry-driven applications?
 - A. IoV
 - B. VR devices
 - C. Smart bands
 - D. Smart logistics

4. Which of the followings are true about IoT?
 - A. The essence of IoT is an Internet
 - B. IoT aims to help connect all things together
 - C. Mobile phone, computer, and air conditions are examples of things in IoT
 - D. IoT is a technology designed based on internet technologies.

5. Choose layers that belongs to the IoT stack model?
 - A. Application
 - B. Transport
 - C. Link
 - D. Network
 - E. Sensing

6. Which of the following layers are included in the Huawei's full-stack IoT solution?
- A. Application
 - B. Platform
 - C. Network
 - D. Sensing
7. Which of the followings are not included in the sensing layer?
- A. Sensors
 - B. Chipsets
 - C. Applications
 - D. Gateways
 - E. Modules
8. Which of the following technologies are used in the network layer?
- A. GPRS
 - B. NB-IoT
 - C. Huawei LiteOS
 - D. IoV
9. Which of the following are taking place in the sensing layer?
- A. Collecting data
 - B. Presenting data
 - C. Storing data
 - D. Processing signals
 - E. Sending data to the platform
10. Which of the followings are parts of the Huawei's IoT solution?
- A. HUAWEI CLOUD IoT platform
 - B. HUAWEI APPLICATION
 - C. HUAWEI LiteOS
 - D. HUAWEI network solutions
11. Which of the followings are sublayers of the platform layer?
- A. Service enablement layer
 - B. Access and transmission layer
 - C. Information collecting layer
 - D. Connectivity management layer

12. Which of the following functionalities are provided by the platform layer?

- A. Authentication
- B. Network access management
- C. IoT device management
- D. Providing services to applications
- E. Data collecting

13. "N+1" architecture means:

- A. The Operating system has only one kernel
- B. There are N modes to access the network
- C. There are N+1 layers
- D. There are N pieces of middleware

14. Which of the followings are solutions provided by/supported at the network layer?

- A. 5G
- B. NB-IoT
- C. Smart gateway
- D. Huawei LiteOS

Chapter 2. IoT Industry Applications and Solutions

A. Mark the followings True or False?

1. Traffic management is a common problem in modern cities.
2. Environmental sanitation is not included in the city management scenario.
3. Device management in the smart city solution includes: 2G/3G/4G, fixed and NB-IoT accesses.
4. Smart streetlamp services do not include charging bills.
5. Smart manhole cover solution can provide real-time monitoring.
6. Security management is a common problem in campus management.
7. Power consumption management is not covered in the smart campus solution.
8. In the campus solution, facial recognition can be used to manage visitors.
9. NB-IoT is a common technology used to manage security in smart campus solution.
10. AMI stands for Advanced Metering Interface.
11. Randomness is a characteristic in the desired AMI solution.
12. V2X includes V2N, V2I, V2P, and V2V.
13. DRIS consists of V2X server and V2X edge.
14. DRIS and HUD can be integrated in an IoV solution.
15. DRIS stands for Driver Road Infrastructure Service.
16. It is not necessary in an ICT-based production system of smart manufacturing to include intelligent sensing technologies.
17. In 5IABCDE, E stands for Encryption.
18. 5IABCDE includes five emerging technologies.
19. Block chain is included in 5IABCDE.
20. AIoT stands for Advanced Internet of Things.
21. In future, IoT solutions that do not integrate AI capability will become increasingly less competitive.
22. The whole process of electrical power supply consists of 6 steps.

23. Currently, the main power stations are thermal, nuclear and hydropower.
24. The major difference between a smart grid and a traditional grid is that the smart grid establishes by unidirectional information flows between power generation and consumption.
25. IoV is a part of IoT.
26. Huawei's smart grid solution is called AMI.
27. The development of IoV is divided into 4 phases.
28. Safety is a challenge in the IoV scenario.
29. Power grid development differs by country and region.
30. A combination of AI, edge computing and IoT is needed in the low-latency scenarios.

B. Check the correct answer, there is only one correct answer for each question:

1. One of the followings is not a common problem in modern cities:
 - A. Visitor management
 - B. Parking management
 - C. Streetlamp management
 - D. Manhole cover management
2. Smart city solution includes:
 - A. 2G/3G/4G and fixed access
 - B. NB-IoT access
 - C. None of them
 - D. Both of them
3. One of the followings is not in the application layer for smart firefighter solution:
 - A. Alarm handling
 - B. Remote muting
 - C. Traffic broadcast
 - D. Device self-check
4. One of the followings is not used in the smart parking solution:
 - A. NB-IoT modules
 - B. Huawei IoT platform
 - C. IoT agent
 - D. RRU + Antenna
5. Which of the followings protocol(s) is(are) used in the network layer in the smart firefighting solution?
 - A. SNMP
 - B. HTTP
 - C. CoAP
 - D. All of them
6. Which of the followings is a common problem in a traditional campus?
 - A. Lack of sensing
 - B. Visitor management
 - C. None of them
 - D. Both of them

7. In a smart campus solution, facial recognition uses one of the followings:
- A. Video- assisted alarm acknowledgment
 - B. Intelligent pre-event warning
 - C. System linkage handling
 - D. Blacklist-based surveillance
8. One of the followings is not used in the power consumption management in the smart campus solution:
- A. Temperature/humidity sensor
 - B. Geo-magnetic vehicle detector
 - C. Intelligent switch/motion sensor
 - D. Smart electricity/water meter
9. Electrical power supply system does not include:
- A. Power generation
 - B. Power transformation
 - C. Power distribution
 - D. Power storage
10. Which of the followings is(are) a character(s) of traditional grid?
- A. Simultaneity
 - B. Integration
 - C. Integration
 - D. All of them
11. In the AMI solution, one of the followings is not used in the field area network:
- A. LTE
 - B. Microwave
 - C. Zigbee
 - D. Wireless LAN
12. In the AMI solution, NAN stands for:
- A. Node Area Network
 - B. Neighborhood Area Network
 - C. NB-IoT Area Network
 - D. None of them

13. One of the followings is not used as a device in the smart AMI solution:
- A. Three-phase prepaid meter
 - B. Wireless smoke sensor
 - C. Single-phase prepaid meter
 - D. Data concentrator unit
14. Which of the followings is not a connection name in IoV environment?
- A. V2V
 - B. V2N
 - C. V2I
 - D. V2E
15. One of the followings is not considered as a vehicle device in IoV solution:
- A. T-Box
 - B. Rearview mirror
 - C. Cabinet meter
 - D. Vehicle-mounted screen
16. Which of the followings is not a part of the seven-emerging technologies?
- A. 4G
 - B. 5G
 - C. IoT
 - D. AI
17. "B" in 5IABCDE stands for:
- A. Big data
 - B. Block chain
 - C. 5G
 - D. None of them
18. AI does not include:
- A. Speech recognition
 - B. Image recognition
 - C. Edge computing
 - D. Natural language processing

19. AIoT includes:

- A. Edge computing
- B. Image recognition
- C. Block chain technologies
- D. Hybrid networking

20. Digital twin includes:

- A. Physical products
- B. Virtual products
- C. Both of them
- D. None of them

C. Choose the correct answer, there are multiple correct answers for each question:

1. Which of the followings are common problems in cities?
 - A. Load balance
 - B. Parking problems
 - C. Manhole cover management
 - D. Visitor management
 - E. Streetlamp problems

2. Nowadays, in cities, sanitation management is:
 - A. Outdated
 - B. Disordered
 - C. Low
 - D. Slow

3. Which of the followings are challenges to the streetlamp management in cities?
 - A. Illegal parking
 - B. Maintenance
 - C. Utilization of all position resource
 - D. Meter reading
 - E. Solar eclipses

4. Which of the followings are common problems in campus?
 - A. Visitor management
 - B. Power management
 - C. Traffic management
 - D. Mainly managed by people

5. Which of the followings are not steps in the electrical power supply?
 - A. Reception
 - B. Generation
 - C. Transformation
 - D. Storing
 - E. Consumption

6. Which of the followings are common problems in traditional electrical grid?
- A. Linelose rate
 - B. Cost
 - C. Full connectivity
 - D. Load balancing
 - E. Meter reading
7. Currently, the main power stations are:
- A. Thermal
 - B. Nuclear
 - C. Hydropower
 - D. Solar
8. Which of the followings are technologies used to handle IoV problems?
- A. V2X
 - B. UBI
 - C. AMI
 - D. DRIS
9. Which of the followings technologies are part of 5IABCDE?
- A. 5G
 - B. AI
 - C. AMI
 - D. Digital twin
 - E. Big data
10. Which of the followings are not true about 5IABCDE?
- A. 5G is used in the network layer
 - B. "B" in 5IABCDE stands for Big data
 - C. AI is used to process data in the platform layer
 - D. 5IABCDE includes 5 emerging technologies

Chapter 3. IoT Security Technologies

A. Mark the followings True or False?

1. The Tesla incident is classified as a DDoS attack.
2. In the Tesla incident, the network layer of the IoT architecture was attacked.
3. DDoS stands for Distributed Denial of Service.
4. Data interception and tampering is not considered as a security threat.
5. API attacks are categorized as a pipe threat.
6. Pipe detection, cloud-cloud synergy and trusted device authentication are effective means to resolve security threats.
7. Huawei IoT security system provides security to data, access and devices.
8. In the Huawei IoT security system, digital signature process includes the use of RSA2048 or SHA256.
9. In the Huawei IoT security system, the use of digital signature includes generation of public and private keys.
10. In the Huawei IoT security system, the signature verification is provided by the terminal device.
11. During the last two decades, the attackers' capability level has increased.
12. Password guessing is an example of IoT attacks.
13. DoS, phishing and encryption are examples of network attacks.
14. In recent days, requirements on attackers' capabilities are low.
15. As requirements on attackers' capabilities are decreasing, attackers' capability level is decreasing as well.
16. AI-based attacks and ransomware viruses are examples of attack tools developed in the 2010s.
17. 3T+1M means 3 security tires and 1 management layer.
18. Anti-DDoS and signaling storms are part of the pipe security.
19. A priority-based system is an anti-DDoS tool.

20. The two-factor authentication can include: certificate and password.
21. The Huawei security solution is focused on LPWA and loV.
22. IoT devices can run advanced encryption system despite of power supply restrictions.
23. IoT security issues occur on the sensing layer only, this is because devices are vulnerable targets.
24. Huawei provides security applications for all layers in the IoT architecture.
25. Authentication is used at the platform layer.
26. FOTA digital signature takes place at the sensing layer.
27. IPSec and L2PT are examples of security technologies used at the network layer.
28. FOTA digital signature are used to ensure that each device is connected to the platform.
29. E2E authentication is used to defend against DDoS attack.
30. In the priority-based message classification, low priority packets are discarded first.

B. Check the correct answer, there is only one correct answer for each question:

1. In Tesla incident, the hackers attack the:
 - A. Inter-vehicles connections
 - B. In-vehicle system
 - C. Vehicle-gateway interconnection
 - D. All of them

2. In the context of Mirai malware attack, “Zombies” refer to:
 - A. Network cameras
 - B. Digital video recorders
 - C. Intelligent routers
 - D. All of them

3. One of the followings is not categorized as application threat for the LPWA security:
 - A. Invalid security access control
 - B. Incorrect security configurations
 - C. API attacks
 - D. Sensitive information leakage

4. Which of the followings is not a security threat to the IoV system?
 - A. DDoS attacks/signaling storms
 - B. API attacks
 - C. T-Box communication security threats
 - D. Bluetooth vulnerabilities

5. Trust key attacks are LPWA security threat, they fill into one of the following categories:
 - A. Application
 - B. Platform
 - C. Network (pipe)
 - D. Device

6. Which of the followings is device security threat?
 - A. Unencrypted transmission
 - B. Checking of damaged devices
 - C. None of them
 - D. Both of them

-
7. During the last two decades, as the network attack technologies become more sophisticated, the requirements on attackers' capabilities:
- A. Raised up
 - B. Stayed the same
 - C. Dropped down
 - D. Become also sophisticated
8. Which of the following tools is(are) used to attack IoT networks?
- A. APT attacks
 - B. AI-based attacks
 - C. Ransomware viruses
 - D. All of them
9. Which of the following architectures does Huawei IoT security adopt?
- A. 3T+1M
 - B. 1T+3M
 - C. 3T+2M
 - D. 3T+3M
10. Which of the followings is(are) included in the IoT security solution?
- A. Data security
 - B. Access security
 - C. Device security
 - D. All of them
11. One of the followings is not included in the Huawei IoT defense of big data security:
- A. Machine learning
 - B. Anti-DDoS
 - C. Threat response
 - D. Attack detection
12. Implementation of FOTA digital signature includes using of the following algorithm(s):
- A. RSA2048
 - B. SHA256
 - C. Both of them
 - D. None of them

13. The digital signature operation includes the use of:

- A. Two public keys
- B. Two private keys
- C. One public and one private keys
- D. Only a private key

14. Pipe security mechanism for IoT solution includes:

- A. Anti-DDoS
- B. Firmware validity
- C. Both of them
- D. None of them

15. A priority-based mechanism against anti-DDoS includes:

- A. Congestion management
- B. Delay access mechanism
- C. Both of them
- D. None of them

16. In the digital signature algorithm, the signature creation is done at the:

- A. Core of the network
- B. Terminal devices
- C. Gateway
- D. Cloud

17. One of the followings is not an attack tool:

- A. Password cracking
- B. Encryption
- C. Password guessing
- D. Phishing

18. Which of the followings is not used in the two-factor authentication?

- A. Certification
- B. SMS
- C. Digital signature
- D. Password

19. In the bicycle sharing scenario, which of the following mechanism(s) is(are) used?

- A. One-way authentication
- B. Dual authentication
- C. Both of them
- D. None of them

20. In the context of bicycle sharing scenario, "DICE" stands for:

- A. Device Identifier Composition Engine
- B. Digital Identifier Composition Engine
- C. Digital Identifier Center Engine
- D. Digital Interconnection Composition Engine

C. Choose the correct answer, there are multiple correct answers for each question:

1. Which of the followings are examples of attacks on the IoT technology?
 - A. IoV
 - B. DDoS
 - C. Data transmission
 - D. Data tampering
 - E. Physical damage

2. Which of the followings are true about Nanjing environmental protection bureau incident?
 - A. The incident was form of DDoS
 - B. Encryption and integrity protection where not carried out during data transmission
 - C. Hackers control a large number of devices to attack a server
 - D. The incident occurred at the network layer of IoT

3. In which layers of IoT model security issues occurs?
 - A. Sensing
 - B. Network
 - C. Platform
 - D. Application

4. IoT security threats often target devices because?
 - A. Devices cannot run advanced encryption system
 - B. Network technologies become increasingly advanced
 - C. Attackers need to master a lot of knowledge to launch the attack
 - D. Devices are vulnerable to physical damage

5. Which of the followings are true about IoT security?
- A. IoT Security threats often target devices
 - B. Attackers need to master a lot of knowledge to launch the attack
 - C. IoT security issues occurs on all layers of the IoT model
 - D. Attackers can launch attacks with limited communications technologies
6. Which of the followings are true about “3T+1M”?
- A. “T” stands for tire
 - B. Cloud, pipe and device layers are included
 - C. 1M means unified security O&M at each layer
 - D. M stands for maintenance
7. For which of the following layers, Huawei provides security applications?
- A. Application
 - B. Platform
 - C. Network
 - D. Sensing
8. Which of the following security technologies are used at network layer?
- A. FOTA
 - B. IPSec
 - C. L2PT
 - D. E2E authentication
 - E. DDoS
9. FOTA Digital Signature ensures:
- A. Validity of the firmware
 - B. Confidentiality of the firmware
 - C. Integrity of the firmware
 - D. Privacy of the firmware

10. Which of the following technologies are used to protect IoT against security threats?

- A. L2PT
- B. FOTA Digital Signature
- C. DDoS
- D. DTLS+
- E. IPSec

Chapter 4. Overview of Common IoT Communications Technologies

A. Mark the followings True or False?

1. Ethernet uses CSMA/CA to detect collisions.
2. FE stands for Fast Ethernet.
3. Micro-B is a USB port Type.
4. The bit rate of USB 4.0 can go up to 40 Gbit/s.
5. In M-Bus technology, the power supply capability of the bus is 10 A.
6. Bluetooth includes three types: BR/EDR, BLE and BLF.
7. Wi-Fi can use 2.4 GHz UHF or 5 GHz SHF ISM radio frequency bands.
8. GPRS bit rate is 9.6 kbps.
9. UMTS is categorized as 2.5G.
10. IMT-Advanced is the official name of 4G.
11. LTE UE category 1 supports a downlink bit rate up to 10 Mbit/s.
12. 5G application scenarios are eMBB, mMTC and URLLC.
13. Commercial use of the 5G started in 2020.
14. NB-IoT is categorized as LPWA communication technology.
15. SigFox bit rate is 1000 bit/s.
16. 3G, 4G and 5G are considered high-rate and long-range technologies.
17. Smart meter reading scenarios can use small-packet and ultra-long-range technology such as 3G.
18. Wi-Fi and Bluetooth are considered high-rate and short-range technologies.
19. NB-IoT and LoRa are low bit rate connection technologies.
20. Z-Wave coverage can extend to 1 km.
21. RS-232, RS-485 and USB are serial communication ports.
22. RS-485 is an upgraded version of RS-232.
23. M-Bus cannot power devices remotely, and there is a need to install power cable.
24. PLC can be used only in near-end scenarios where the voltage does not change.
25. Z-Wave is similar to ZigBee, but ZigBee is more reliable.

26. Over a 2G network, it is possible to make video calls, and watch TV programs on smart phones.
27. Over a 3G network, it is possible to make calls and send SMS.
28. In the IoT field, LTE category 1 UEs are widely used.
29. eMBB is closely related to IoT scenarios, while mMTC and URLLC are closely related to users.
30. NB-IoT can be directly deployed in the existing cellular networks.

B. Check the correct answer, there is only one correct answer for each question:

1. One of the followings is not a wired communication technology:
 - A. Ethernet
 - B. LTE
 - C. PLC
 - D. USB
2. One of the followings is not a wireless communication technology:
 - A. Wi-Fi
 - B. Zigbee
 - C. LoRa
 - D. RS-232
3. Which of the followings is not considered as a cellular mobile network technology?
 - A. UMTS
 - B. GSM
 - C. PLC
 - D. LTE
4. Which of the followings is(are) considered as short-range wireless communication technology(ies)?
 - A. Wi-Fi
 - B. Zigbee
 - C. Bluetooth
 - D. All of them
5. LTE-Advanced Pro belongs to:
 - A. 2G
 - B. 3G
 - C. 4G
 - D. 5G
6. One of the followings is not a 3G technology:
 - A. UMTS
 - B. GPRS
 - C. HSPA
 - D. HSPA+

7. GSM bit rate is in the range of:
- A. kbit/s
 - B. Mbit/s
 - C. Gbit/s
 - D. Tbit/s
8. 5G connection density is:
- A. 10^4 connections/km²
 - B. 10^5 connections/km²
 - C. 10^6 connections/km²
 - D. 10^7 connections/km²
9. 5G supports mobility at the speed of:
- A. 200 km/h
 - B. 300 km/h
 - C. 400 km/h
 - D. 500 km/h
10. One of the followings is not a 3G technology:
- A. FDMA
 - B. TD-SCDMA
 - C. CDMA2000
 - D. WCDMA
11. AR, VR and MR are supported in the:
- A. 3G
 - B. 4G
 - C. 5G
 - D. All of them
12. In which of the following LPWA technology, the coverage can extend to 50 km?
- A. SigFox
 - B. LoRa
 - C. NB-IoT
 - D. eMTC

13. The bandwidth used for LPWA NB-IoT is:

- A. 180 MHz
- B. 180 kHz
- C. 18 MHz
- D. 18 kHz

14. LPWA NB-IoT supports mobility scenarios with a speed less than:

- A. 80 km/h
- B. 100 km/h
- C. 200 km/h
- D. 500 km/h

15. eMTC was developed by:

- A. Nokia
- B. Ericsson
- C. Huawei
- D. None of them

16. Which of the followings has the lowest typical transmission rate?

- A. SigFox
- B. LoRa
- C. NB-IoT
- D. eMTC

17. Video surveillance requires:

- A. Low data rate and high bandwidth
- B. High data rate and high bandwidth
- C. High data rate and low bandwidth
- D. Low data rate and low bandwidth

18. Smart meter applications require:

- A. High data rate
- B. High bandwidth
- C. None of them
- D. Both of them

19. Which of the followings requires 5G?

- A. Video surveillance
- B. IoV
- C. None of them
- D. Both of them

20. Small packet and short-range technologies include:

- A. eMTC
- B. LoRa
- C. Z-Wave
- D. SigFox

C. Choose the correct answer, there are multiple correct answers for each question:

1. Which of the followings are wired communication technologies?
 - A. Ethernet
 - B. USB
 - C. LoRa
 - D. M-Bus
 - E. RS-232

2. Which of the followings are true about CSMA/CD?
 - A. It is used with wired and wireless technologies
 - B. It is used with USB
 - C. Once a collision is detected, data transmission stops immediately
 - D. A station is required to detect collision.

3. Which of the followings are not true about RS-232 and RS-485?
 - A. RS-485 is limited to 20 m
 - B. RS-232 is one-to-one communication technology
 - C. RS-232 uses balance transmission mode
 - D. RS-485 has transmission rate of 10 Mbit/s

4. Which of the followings are true about USB?
 - A. Serial
 - B. Scalable
 - C. High-speed
 - D. Easy to use

5. Which of the followings are not a type of USB port?
 - A. Type-A
 - B. Type-B
 - C. Micro B
 - D. Type-D

- E. Micro D
6. Which of the followings are considered short-range wireless communication technologies?
- A. 5G
B. Bluetooth
C. SigFox
D. WiFi
E. eMTC
7. Which of the followings are true about Bluetooth?
- A. It is used for ranges from about 10 cm to 10 m
B. Bluetooth 5.0 supports a transmission rate up to 3 Mbit/s
C. BR/EDR supports only point-to-point communications
D. BLE is not suitable for low-energy scenario
8. Which of the followings are not true about WiFi?
- A. It is used to access internet from homes
B. It uses 2.4 GHz and 5 GHz frequency bands
C. WiFi 6 is the most current standard, it supports a transmission rate up to 9.6 kbit/s
D. WiFi is long-range communication technology.
9. Which of the followings are true about Z-Wave?
- A. It is similar to ZigBee but more reliable
B. It has 2 transmission rates: 9.6 kbit/s and 40 kbit/s
C. It is not open-source
D. It uses 2.4 GHz frequency band

10. Which of the followings are true about ZigBee?

- A. It features low consumption
- B. Its transmission rate is 9.6 kbit/s
- C. Low-cost
- D. It allows direct data transmission between devices
- E. Difficult to maintain

11. Which of the followings are not cellular mobile communication technologies?

- A. WCDMA
- B. 5G
- C. LoRa
- D. SigFox
- E. HSPA+

12. Which of the followings are true about 2G?

- A. It is a digital system
- B. It supports making calls and send SMSs
- C. It is also called GSM
- D. It has a transmission rate of Mbit/s

13. Which of the followings are standards for 3G networks?

- A. CDMA2000
- B. WCDMA
- C. TD-SCDMA
- D. HSPA+

14. Which of the followings are considered LPWA communication technologies?

- A. SigFox
- B. LoRa
- C. GPRS
- D. eMTC
- E. NB-IoT

15. Which of the followings are true about 4G?

- A. HSPA+ is a 4G technology
- B. 4G is required to transmit HD videos
- C. Module chips for devices at different categories have different prices
- D. Different category means different transmission rate on the uplink only

16. Which of the followings are true about category 1 UE?

- A. It is widely used in IoT field
- B. It belongs to 4G
- C. It supports a downlink up to 10 Mbit/s
- D. It is a cost-effective solution

17. Which of the followings are considered to be 5G application scenarios?

- A. eMBB
- B. URLLC
- C. mMTC
- D. eMTC

18. Which of the followings are true about SigFox?

- A. It is suitable for low throughput project
- B. It can maintain stable data communication with less transmission power
- C. It is a wired communication technology
- D. It is trusted for data storage and information security
- E. It is LPWA communication technology

19. Which of the followings are true about NB-IoT?

- A. It is LPWA communication technology
- B. It needs 180 kHz of bandwidth
- C. It has a bit rate less than 250 kbit/s
- D. It can be deployed in existing cellular network

20. Which of the followings are true about LoRaWAN?

- A. It is a cellular communication technology
- B. It runs on unlicensed frequency band
- C. It is an ultra-long-range wireless solution
- D. It has a high bit rate

Chapter 5. NB-IoT Communication Technologies and Solutions

A. Mark the followings True or False?

1. NB-IoT and NR can coexist.
2. The industry recognizes NB-IoT evolution and agrees to incorporate it into the overall 5G plan.
3. NB-IoT bandwidth is 200 kHz.
4. NB-IoT downlink has 12 subcarriers each is 15kHz.
5. OFDMA is an evolution of OFDM that combines it with FDMA.
6. NB-IoT technology supports massive connections, but it consumes remarkable amount of energy.
7. PSM stands for Power Sleeping Mode.
8. In NB-IoT technology, PSM consumes the most amount of energy.
9. NB-IoT uses retransmission over the air interface and ultra-narrow bandwidth to provide an extra gain of over 20 dB compared with GSM.
10. NB-IoT is based on cellular networks and coexists with other networks of this type.
11. NB-IoT standalone deployment is only based on LTE.
12. NB-IoT supports three deployment modes.
13. NB-IoT on the Boudica 150 chip supports full duplex channel.
14. DRX period can be 1.28, 2.56, 5.12 or 10.24s, and it is determined by the operator's network.
15. The maximum eDRX period is 2.92 hours.
16. An IoT device can be in the dormant state for up to 99% of the total time.
17. PSM maximum period is 200 hours.
18. Because NB-IoT uses repeated transmission, the downlink gain increased by 12 dB and the uplink gain increased by 9 dB.
19. NB-IoT is a wide coverage technology.
20. NB-IoT is not an example of LPWA communication technologies.

21. NB-IoT networks provide very slow transmission rate.
22. Before the emergence of NB-IoT, there were no LPWA networks.
23. IoT device needs frequency with weak penetration.
24. All NB-IoT networks are deployed on sub-GHz frequency band.
25. All NB-IoT networks are based on 4G LTE networks.
26. Boudica 120 supports sub-GHz band and mobility introduced in R14.
27. NB-IoT is designed for much lower data rate than 4G.
28. NB-IoT cannot be deployed in the in-band or guard band of the LTE system.
29. Boudica 150 chip has 2 antennas.
30. DRX is not suitable for IoT devices because it consumes too much power.

B. Check the correct answer, there is only one correct answer for each question:

1. LPWA stands for:
 - A. Long-Power Wide-Area
 - B. Low-Power Wide-Area
 - C. Large-Power Wide-Area
 - D. Low-Person Wide-Area
2. Power transmission gain in the basic version of LPWA was:
 - A. 20 dB
 - B. 10 dB
 - C. 5 dB
 - D. 25 dB
3. NB-IoT and NR technologies:
 - A. Work separately only
 - B. Can coexist
 - C. Interfere with each other
 - D. None of them
4. Boudica 150 chip supports:
 - A. Multicast
 - B. Downlink: 21.2 kbps,
uplink: 15.6 kbps
 - C. Positioning
 - D. All of them
5. One of the followings is not true about Boudica 120, it:
 - A. Supports paging
 - B. Has 20 dB coverage enhancement
 - C. Supports IP only
 - D. Supports single tone
6. At the physical layer of NB-IoT, the bandwidth is:
 - A. 150 kHz
 - B. 180 kHz
 - C. 120 kHz
 - D. 200 kHz

7. At the physical layer of NB-IoT, uplink technology is:
- A. OFDMA
 - B. SC-FDMA
 - C. TDMA
 - D. CDMA
8. One of the followings is not an NB-IoT feature:
- A. Ultra-low cost
 - B. Massive connections
 - C. Ultra-high-power consumption
 - D. Ultra-wide coverage
9. NB-IoT deployment mode(s) is(are):
- A. Standalone
 - B. Guard band
 - C. In-band
 - D. All of them
10. Standalone deployment mode is used with:
- A. GSM
 - B. UTMS
 - C. LTE
 - D. All of them
11. Kirin 4G chip supports:
- A. Broadband
 - B. High bit rate
 - C. Full duplex
 - D. All of them
12. PSM consumption pattern can last up to:
- A. 300 hours
 - B. 210 hours
 - C. 310 hours
 - D. 350 hours

13. Deep coverage solution provides gain increasing by:
- A. 5 dB
 - B. 11 dB
 - C. 20 dB
 - D. 25 dB
14. NB-IoT gain in the repeated transmission is:
- A. Decreased both in the uplink and downlink
 - B. Increased both in the uplink and downlink
 - C. Increased in the uplink only
 - D. Increased in the downlink only
15. Which of the followings technologies has the highest maximum coupling loss?
- A. LTE
 - B. GPRS
 - C. NB-IoT
 - D. GSM
16. NB-IoT increases battery life to be:
- A. 5 years
 - B. 7 years
 - C. 10 years
 - D. 12 years
17. Which of the followings is the number of connections per cells supported by NB-IoT?
- A. 5000
 - B. 50 000
 - C. 100 000
 - D. 150 000
18. One of the followings is not true about NB-IoT:
- A. Evolution is based on the live network
 - B. Operator-level reliability
 - C. High security
 - D. Local roaming

19. NB-IoT solution architecture includes:

- A. 3 layers
- B. 4 layers
- C. 5 layers
- D. None of them

20. Which of the following solutions can include NB-IoT?

- A. Smart parking
- B. Shared bikes
- C. Smart streetlamp
- D. All of them

C. Choose the correct answer, there are multiple correct answers for each question:

1. Which of the followings are true about NB-IoT?
 - A. It was proposed by Huawei and Vodafone
 - B. It evolved out of NB-M2M
 - C. It was part of 5G plan from the beginning
 - D. The current NB-IoT does not support access to 5G networks
 - E. NB-IoT provides very slow transmission rate

2. IoT devices:
 - A. Are typically widely separated
 - B. Need to run on limited power
 - C. Need to transmit small amount of data
 - D. Need frequency with strong penetration

3. Which of the followings are true about NB-IoT deployment?
 - A. Most operators deploy NB-IoT on the sub-GHz frequency band
 - B. It can be deployed on 1800 MHz
 - C. Both 3G station and 4G station can be upgraded to function as NB-IoT station
 - D. It cannot be deployed on 2G network

4. Which of the followings are true about Huawei NB-IoT chips?
 - A. Huawei launched Boudica 120 and Boudica 140 and Boudica 150 chips
 - B. Boudica 120 is compatible with R13
 - C. Boudica 150 is compatible with R14
 - D. Boudica 120 supports sub-GHz frequency band and mobility

5. In which of the following applications NB-IoT is involved?
- A. Water meters
 - B. Streetlamp
 - C. Gas meters
 - D. Smart parking
6. Which of the followings are true about NB-IoT?
- A. It is a narrowband system
 - B. The system bandwidth is 200 kHz
 - C. It has a high bit rate
 - D. It uses OFDMA and SC-CDMA
7. NB-IoT deployment modes are:
- A. Out-band
 - B. Standalone
 - C. Guard band
 - D. In-band
8. Which of the following technologies are supported by ultra-low power consumption NB-IoT?
- A. DRX
 - B. eDRX
 - C. PTW
 - D. PSM
9. Which of the followings are true about eDRX?
- A. It introduced the paging time window
 - B. Within each PWT, an IoT device make 3 paging attempts.
 - C. An eDRX cycle can be up to 310 days
 - D. eDRX are suitable for all IoT scenarios

10. Which of the followings are true about the traffic model of IoT devices?

- A. Devices do not require high quality communication
- B. Devices usually send long data packets
- C. Latency is a major issue
- D. It includes large number of devices

Chapter 6.5G Communications Technologies and Solutions

A. Mark the followings True or False?

1. NR stands for New Reality.
2. Massive MIMO supports 64 transmitter antennas and 64 for receivers.
3. Release 15 is the first 3GPP standard dedicated for 5G.
4. In 5G, E2E latency is 10 ms.
5. Compared to the 4G technology, latency in 5G is 30 to 50 times less.
6. The throughput of 5G can go up to 10 Mbps.
7. Compared to the 4G technology, throughput in 5G is 100 times higher.
8. 5G can support a number of connections per km² up to 1 million.
9. Compared to the 4G technology, 5G supports 1000 times the number of connections.
10. 4G and 5G supports slicing.
11. IMT-Advanced is another name for 5G.
12. SDN stands for Software-Driven Networking.
13. NSA can coexist with SA.
14. eNB stands for evolved NodeB.
15. 5G New Radio can be full duplex or half duplex.
16. 5G New Radio supports Massive MIMO.
17. Sub-3 GHz means lower than 3000 MHz and C-band covers 3000 - 6000 MHz.
18. 5G New Radio extends to the visible light band.
19. In 5G, URLLC scenarios need ultra-high reliability and ultra-low latency services.
20. VR, AR and MR are examples of eMBB scenarios.
21. The 4G era saw only two standards: LTE TDD and LTE FDD.
22. Release 16 make the complete version of 5G, it was released in 2017.
23. With NFV being used, the same hardware can be allocated to different users.
24. In 5G, control plan and data plan are not separated. Thus, traffic control is simple.

25. In addition to the time and frequency domains, the space domain is also multiplexed to improve the throughput.
26. 3G uses the 1.8 GHz bands, 4G uses the 2.6 GHz band and 5G directly jumps to the C band (3.4 to 3.6 GHz).
27. 5G supports M-MIMO on the transmitter and receiver. Thus, multiple antennas are located on the receiver only.
28. 5G deployment is a hybrid networking approach that combines high and low frequency bands.
29. With MR, no glasses are needed.
30. The recognition of NB-IoT is an important step to incorporating massive connections into 5G.

B. Check the correct answer, there is only one correct answer for each question:

1. 3GPP process of the 5G standardization started in:
 - A. Release 14
 - B. Release 15
 - C. Release 16
 - D. Release 17

2. Which of the followings standard(s) can benefit from the 5G?
 - A. WiMax
 - B. WCDMA
 - C. LTE
 - D. All of them

3. One of the followings is not true about the 5G, it provides:
 - A. Global unified standardization
 - B. Global roaming
 - C. Massive connections
 - D. Bit rate up to 1Tbit/s

4. Compared to LTE, the throughput of the 5G is:
 - A. 10 times greater
 - B. 100 times greater
 - C. 1000 times greater
 - D. None of them

5. Compared to LTE, the number of connections of 5G is:
 - A. The same
 - B. 10 times greater
 - C. 100 times greater
 - D. 1000 times greater

6. In 5G, the latency is around:
 - A. 0.1 msec
 - B. 1 msec
 - C. 10 msec
 - D. 100 msec

13. Which of the followings multiplexing technologies does massive MIMO use?
- A. Spatial
 - B. Time
 - C. Code
 - D. Frequency
14. One of the followings is not true about the 5G frequency bands:
- A. C-band is mainly used for capacity expansion
 - B. 5G can use bands above 6 GHz
 - C. 28 GHz band can be used for industrial purposes
 - D. Visible light bands are supported
15. One of the followings is not true about the sub-6 GHz, it is used for:
- A. Higher bit rate
 - B. Coverage
 - C. Mobility
 - D. Connectivity
16. Which of the followings is not true about 5G full spectrum?
- A. Sub-6 GHz low frequency bands serve as the core spectrum
 - B. High frequency bands are supplementary
 - C. Sub-6 GHz is used for higher rate
 - D. C-band is mainly used for capacity expansion
17. eMBB stands for:
- A. Enhanced Mobile BroadBand
 - B. Evolved Mobile BroadBand
 - C. Electronic Mobile BroadBand
 - D. Enhanced Mobile BaseBand

18. Which one of the followings is not a reality-based technology?

- A. Virtual Reality
- B. Augmented Reality
- C. Supported Reality
- D. Mixed Reality

19. URLLC scenarios require:

- A. Ultra-low reliability and ultra-low latency
- B. Ultra-high reliability and ultra-low latency
- C. Ultra-low reliability and ultra-high latency
- D. Ultra-high reliability and ultra-high latency

20. Which of the followings 5G application scenario(s) is(are) defined by ITU?

- A. eMBB
- B. mMTC
- C. URLLC
- D. All of them

C. Choose the correct answer, there are multiple correct answers for each question:

1. Which of the followings are true about 5G?
 - A. First standard was released in 2017
 - B. First standard was Release 14
 - C. 5G is covered by Release 15 and Release 16
 - D. Release 15 is the complete version of 5G

2. Which of the followings are considered 5G indicators?
 - A. 10 Gbit/s
 - B. 1 ms latency
 - C. $10^6/\text{km}^2$ connections
 - D. Slice-based network architecture

3. Which of the followings are key technologies in network slicing?
 - A. NFV
 - B. NSA
 - C. EPC
 - D. SDN

4. Which of the followings are true about 5G networking modes?
 - A. There are two modes
 - B. 5G can co-exist with 4G
 - C. 5G UE connects with eNodeB while 4G UE connects with gNodeB
 - D. NGC is another name of network core in 5G

5. Which of the followings are considered as technical features of 5G?
 - A. Control plane and user plane are separated from each other
 - B. Edge Mobile Computing (EDC)
 - C. Function reconstruction
 - D. Network slicing

6. Which of the followings are characteristics of 5G new radio?
- A. M-MIMO
 - B. CDMA
 - C. F-OFDM
 - D. Half duplex
 - E. Polar coding
7. Over which of the following frequency bands 5G can operate?
- A. C-band
 - B. Sub-GHz band
 - C. ISM band
 - D. mmWave band
8. Which of the followings are 5G scenarios are sensitive to latency?
- A. Remote surgery
 - B. Autonomous driving
 - C. VR
 - D. MR
9. Which of the followings 5G scenarios require ultra-high transmission rates?
- A. VR
 - B. MR
 - C. AR
 - D. NB-IoT
 - E. Remote surgery
10. Which of the followings are considered 5G application dimensions?
- A. eMBB
 - B. mMTC
 - C. eMTC
 - D. URLLC

Chapter 7&8. Huawei IoT Gateways (Industrial + Home)

A. Mark the followings True or False?

1. Industrial-grade design requirements include the need of the gateway to be dustproof and waterproof.
2. Enterprise routers temperature range is -40°C to +70°C.
3. Industrial IoT gateway sets in-between the network and the cloud.
4. Industrial IoT gateway includes extensive interfaces and protocols.
5. Industrial IoT gateway uses edge computing to reduce latency.
6. Edge computing reference architecture covers 4 domains: application, data, cloud and device.
7. The reliability of the star topology is high.
8. Huawei RF networking technology is based on the bus topology.
9. Bus topology is simple and easy to expand.
10. Ring topology is easy to expand.
11. The topology of the future home network will be star.
12. A smart home network runs over a baseband connection.
13. AP stands for Access Point.
14. Huawei HiLink allows two connection modes: direct hardware and cloud-based.
15. STB stands for Set Tree Box.
16. Smart home devices can use PLC.
17. Security surveillance is one application of the smart home scenario.
18. Huawei HiLink ecosystem connection includes modules, SDK and routers.
19. HiLink SDK is used to connect the smart home application to the cloud.
20. Wi-Fi, ZigBee, Z-Wave and Bluetooth are examples of wireless communication technologies supported by the smart home gateway.
21. IoT gateway serves as a bridge between sensing layer and the platform layer.
22. In IoT edge computing has its own architecture.

23. In edge computing, after the data is processed, the gateway still needs to notify the central node that the data has been processed.
24. In edge computing, the device domain is equivalent to the platform layer in the IoT model.
25. In the ring topology, path selection is complex.
26. Mesh topology can significantly increase the network bandwidth.
27. In home environment, 80% of devices are expected to use WiFi in the future.
28. Intelligent O&M and smart ONT are key services of a smart home gateway.
29. A driver is a program that must be installed to enable communication between the hardware of two nodes.
30. Huawei OpenLife solution imports and integrates hardware vendors and service/application content for operators.

B. Check the correct answer, there is only one correct answer for each question:

1. Which of the followings is not true about industrial-grade routers? they are:
 - A. Designed to work in temperature:
-40°C to +70°C
 - B. Dustproof
 - C. Waterproof
 - D. Weak against electromagnetic interference

2. Industrial IoT gateways sit in-between:
 - A. Network and terminal devices
 - B. Network and application
 - C. Application and terminal devices
 - D. None of them

3. Which of the followings is(are) a core-benefit of edge computing?
 - A. Real-time services
 - B. Data aggregation
 - C. Processing at the edge
 - D. All of them

4. One of the followings is not distributed in the network by edge computing technologies:
 - A. Computing
 - B. Storage
 - C. Coverage
 - D. Security

5. How many domains are considered in the edge computing architecture?
 - A. 3
 - B. 4
 - C. 5
 - D. 6

6. One of the followings is not true about star topology, it is/has:
- A. Easy control
 - B. Low cost
 - C. Simple structure
 - D. Short latency
7. Which of the followings is true about the star topology?
- A. Low cost
 - B. High reliability
 - C. High network latency
 - D. Poor resource sharing capability
8. Which of the followings is not true about the ring topology?
- A. Closed
 - B. Difficult to extend
 - C. High reliability
 - D. Difficult to locate faulty nodes
9. Which of the followings is not true about the bus topology?
- A. Complex structure
 - B. Easy to expand
 - C. Difficult to locate faulty nodes
 - D. Small number of cables are linked
10. Which of the followings is not true about the mesh topology?
- A. Rapid deployment
 - B. Resilient to damage
 - C. Has a control center
 - D. No preset infrastructure
11. Which of the followings topologies is adopted by Huawei RF technology?
- A. Mesh
 - B. Bus
 - C. Star
 - D. Ring

12. Nowadays, home network topology is:

- A. Star
- B. Mesh
- C. Ring
- D. Bus

13. Which of the followings is not true about future IoT home networks? it:

- A. Requires accessing broadband connection
- B. Uses fiber optics
- C. Has a mesh topology
- D. Has a low-processing ability

14. Which of the followings is not a device used in the IoT home network?

- A. STB
- B. Smart gateway
- C. NodeB
- D. Wi-Fi repeater

15. Which of the followings technology(ies) can be used to extend Wi-Fi coverage in the IoT home network?

- A. PLC
- B. Wireless repeater
- C. Ethernet AP
- D. All of them

16. In the smart ONT solution, which of the following technology is not used inside homes?

- A. USB dongle
- B. ZigBee
- C. Z-Wave
- D. LTE

17. In the Huawei smart home solution, the plug-in download service is provided by:

- A. The smart terminal devices
- B. The open platform
- C. The smart gateway
- D. Control and management applications

18. Which of the followings is not true about Huawei HiLink platform? it is:

- A. Open
- B. Simple to use
- C. Jointly constructed
- D. Expensive

19. Which of the followings is(are) part(s) of the Huawei HiLink access?

- A. HiLink module
- B. HiLink SDK
- C. HiLink router
- D. All of them

20. How many connection modes are supported in the Huawei HiLink solution?

- A. 2
- B. 3
- C. 4
- D. 5

C. Choose the correct answer, there are multiple correct answers for each question:

1. Which of the followings are considered challenges faced by IoT in the industrial field?
 - A. Diversity of protocols
 - B. Harsh environment
 - C. Cyber security
 - D. Complex O&M
 - E. Diversity of platforms

2. Which of the followings are true about edge computing?
 - A. Low latency
 - B. High latency
 - C. Greater user privacy
 - D. Low cost
 - E. High cost

3. Which of the followings are names of domains in the edge computing architecture?
 - A. Device
 - B. Platform
 - C. Sensing
 - D. Data
 - E. Application

4. Which of the followings are not true about star topology?
 - A. Hard to implement
 - B. Low cost
 - C. Heavy installation workload
 - D. Easy fault diagnosis
 - E. Potential bottle neck

5. Which of the followings are true about ring topology?
 - A. Difficult to expand
 - B. Hard to use
 - C. High reliability
 - D. Hard to locate faulty nodes

6. Which of the followings are names of the mesh topology?
- A. Multihop
 - B. Multipoint-to-multipoint
 - C. Multicast
 - D. Multithread
7. Which of the followings are disadvantages of the bus topology?
- A. The entire network will shut down if there is a break in the main cable
 - B. Terminators are required at both ends of the main cable
 - C. Difficult to identify the root cause of network shutdowns
 - D. The transmission speed slows when a large number of devices are added to the network
 - E. Suitable for small networks
8. Which of the followings are true about mesh topology?
- A. It does not rely on reset infrastructure
 - B. Temporarily networking
 - C. Rapid deployment
 - D. Resilient to damage
9. Which of the followings are true about home network development?
- A. In the nineteenth, home networks had point-to-point structure
 - B. A typical home network in 2022 has a star structure
 - C. A typical home network in 2022 has a bus structure
 - D. All future networks are expected to evolved towards mesh structure

10. Which of the following solutions does Huawei propose for WiFi coverage distance in homes?
- A. Ethernet AP
 - B. PLC (modem)
 - C. ZigBee
 - D. Wireless repeater
11. Which of the followings are considered types of smart gateway plug-ins?
- A. Driver
 - B. Agent
 - C. SDK
 - D. AP
 - E. Application
12. Which of the following technologies, a smart gateway is expected to support?
- A. WiFi
 - B. LoRa
 - C. Z-Wave
 - D. ZigBee
 - E. Bluetooth
13. Which of the following connection methods are available for HiLink ecosystem?
- A. HiLink module
 - B. HiLink SDK
 - C. HiLink switches
 - D. HiLink routers
14. Which of the followings are access method to Huawei HiLink platform?
- A. Connect through hardware
 - B. Connect through software
 - C. Connect through firmware
 - D. Connect through cloud

15. Huawei HiLink platform is:

- A. Open
- B. Shared
- C. Easy to use
- D. Secure
- E. Reliable

Chapter 9. IoT Platform

A. Mark the followings True or False?

1. An IoT platform requires: device access decoupling, security and reliability.
2. Decimal data are accepted format in HUAWEI CLOUD IoT platform.
3. HUAWEI CLOUD IoT platform uses LwM2M and MQTT to access devices.
4. HUAWEI CLOUD IoT platform is multi-network access, this means devices can connect to the platform directly, through gateways or edge devices.
5. Devices that use property protocols based on TCP/UDP can connect to the IoT platform by using CIGs deployed on the cloud.
6. HTTP is an asynchronous protocol.
7. HTTP is a heavyweight protocol with many headers and rules; thus, it is not suitable for restricted networks.
8. CoAP is based on HTTP.
9. CIG stands for Carrier Interworking Gateway.
10. Device management includes device registration and activation.
11. IoT platform has three ways to deliver commands: Immediate, delayed and synchronic deliveries.
12. In time-based triggers, actions can be set based on specific events.
13. In the IoT platform, firmware and software upgrades for devices are achieved through FOTA and SOTA respectively.
14. In the IoT platform, hardware upgrade is called "Hardware-Over-The-Air".
15. HUAWEI CLOUD uses Identity and Access Management for application registration authentication.
16. Multi-temperature data management maximizes processing efficiency.
17. Multi-temperature management classifies data into two classes: hot and cold.
18. HUAWEI CLOUD IoT is access agnostic.
19. The IoT platform has its own security strategies, it includes one for each of the followings: device, networking, service, data storage and access security.

20. The IoT platform cloud-based architecture is flexible but not scalable.
21. Traditional internet standards are not suitable for the IoT.
22. IoT agent provides SDKs, but cannot support APIs independent of underlying resources.
23. Device management means carriers can manage all sensor nodes at the bottom layer, obtain information about each node, and implement remote control.
24. A complete IoT solution consists of the IoT platform, devices, and applications.
25. IoT device access services include global SIM.
26. The cookies mechanism in HTTP is used to address the fact that the protocol is stateless.
27. HTTP is a lightweight protocol; thus, it is suitable for IoT networks.
28. CoAP is based on HTTP and uses TCP.
29. CoAP is suitable for devices that uses sleep/ wakeup mechanism.
30. Devices need to connect to the platform, then, they can be registered.
31. NB-IoT devices that receives commands from the platform using delayed delivery must be set to PSM.
32. Temperature-based actions uses event-based triggers.
33. In OTA, the software upgrade protocol is PCP.
34. Batch operations apply to the scenarios where the same operation is to be performed on a large number of devices.
35. IAM token is valid for 48 hours.
36. In any given push message, the IoT platform functions as a client and the application functions as the server.
37. Multi-temperature data management minimize processing efficiency.
38. Timestamps are example of key data that are collected on a regular basis.
39. Global SIM link provides cellular networks, and not NB-IoT, connections for IoT devices.
40. In the data processing field, edge computing is derived from cloud computing.

B. Check the correct answer, there is only one correct answer for each question:

1. One of the followings is not a requirement for IoT platform:
 - A. Device access decoupling
 - B. Coverage
 - C. Security
 - D. Reliability

2. How many sublayers are there in the functional architecture of the Huawei IoT platform?
 - A. 2
 - B. 3
 - C. 4
 - D. 5

3. Which of the followings is(are) an accepted data format(s) for Huawei IoT platform?
 - A. JSON only
 - B. Binary only
 - C. None of them
 - D. Both of them

4. One of the followings is not a category of an IoT device access service:
 - A. Device connectivity
 - B. Data forwarding
 - C. IoT Edge
 - D. Application integration

5. One of the followings is not true about the IoT device access in the Huawei platform, it supports:
 - A. Multiple access modes
 - B. Multi-network access
 - C. Multi-protocol access
 - D. Multiplexing modes

6. If the HTTP client first message has the sequence field set to X, the ACK field in the server response will be set to:
- A. X
 - B. X-1
 - C. X+1
 - D. None of them
7. Which of the followings is not true about HTTP? it is:
- A. Stateless
 - B. Asynchronous
 - C. Heavy weight
 - D. Not suitable for restricted network
8. If MQTT is used, how many message(s) is(are) to be exchanged between the client and the server before sending the first publish message?
- A. 1
 - B. 2
 - C. 3
 - D. 4
9. CoAP stands for:
- A. Constrained Access Point
 - B. Constrained Application Protocol
 - C. Coverage Application Protocol
 - D. None of them
10. Which of the followings is not a typical IoT protocol?
- A. CoAP
 - B. HTTP
 - C. MQTT
 - D. FBB

11. Devices that do not use TCP/IP protocol stack:

- A. Cannot connect to the IoT platform
- B. Use a gateway with an integrated IoT device SDK
- C. Use a gateway with an integrated IoT device tiny SDK
- D. None of them

12. IoT device SDK does not support:

- A. C
- B. R
- C. Java
- D. C#

13. Which of the followings is(are) used by the IoT platform to deliver commands?

- A. Delayed delivery
- B. Synchronous delivery
- C. None of them
- D. Both of them

14. Which of the followings is(are) supported trigger(s) in the IoT platform?

- A. Time-based
- B. Event-based
- C. Data-based
- D. All of them

15. Which of the followings is true about the IoT platform? it supports:

- A. Hardware upgrade only
- B. Hardware and software upgrades
- C. Firmware upgrade only
- D. Software and firmware upgrades

16. One of the followings is not true about IoT data:

- A. Huge volume
- B. High quality
- C. Low value density
- D. High time sensitivity

17. How many data categorizations are included in the Multi-temperature management?

- A. 2
- B. 3
- C. 4
- D. 5

18. Which of the followings is the correct sequence for managing warm data?

- A. Cleansing, storage, analysis, visualization
- B. Storage, cleansing, analysis, visualization
- C. Analysis, storage, cleansing, visualization
- D. Visualization, analysis, storage, cleansing

19. One of the followings is not a common IoT data problem:

- A. Duplicate data
- B. High-quality data
- C. Format differences
- D. Noise interference

20. Which of the followings is(are) character(s) of Huawei cloud IoT platform?

- A. Access agnostic
- B. Scalable
- C. None of them
- D. Both of them

C. Choose the correct answer, there are multiple correct answers for each question:

1. Which of the followings are true about ecosystem and platform?
 - A. A platform is based on an open ecosystem
 - B. An enterprise that builds a platform is the platform owner
 - C. In the IoT platform model, platform participants can collaborate with each other
 - D. Enterprises in the ecosystem can collaborate with each other

2. Which of the followings are major changes facing IoT industry?
 - A. Long rollout period
 - B. Too many standards
 - C. Lack of applications
 - D. Difficult network selection

3. Which of the followings are requirements for an IoT platform?
 - A. Security
 - B. Reliability
 - C. Device access decoupling
 - D. Capability openness

4. Which of the followings are devices at the IoT device layer?
 - A. Smart devices
 - B. Intellectual hardware
 - C. Home gateways
 - D. Industrial gateways
 - E. IoT agents

5. Which of the followings are functions provided by device connectivity layer?
 - A. Device management
 - B. Open applications and APIs
 - C. Transmission protocol adaption
 - D. Lightweight authentication
 - E. Data management and openness

6. IoT provides the following functions:
- A. Device fleet access
 - B. Unidirectional communication between devices and the cloud
 - C. Over-The-Air upgrades
 - D. Device linkage rules
7. Which of the followings are true about HTTP?
- A. It is a network-layer protocol
 - B. It is stateful
 - C. It is a synchronization protocol
 - D. It uses three-way handshake
 - E. It is a lightweight protocol
8. Which of the followings are true about MQTT?
- A. It is simple and lightweight
 - B. It is synchronization protocol
 - C. It supports reliable message transmission
 - D. It supports real time message notifications
 - E. The message can be short as for 4 bytes
9. Which of the followings are not true about CoAP?
- A. The header is compressed
 - B. It uses TCP to provide message retransmission
 - C. Strong real time support
 - D. It suits smart parking applications

10. Which of the followings are true about device registration and access authentication?
- A. They are required to ensure that devices connected to the platform are secure and reliable
 - B. Devices need to connect to the platform before registration
 - C. Devices are authenticated when they try to connect to the platform
 - D. They are parts of data forwarding
11. Which of the followings are status in the device command status transition?
- A. PENDING
 - B. EXPIRED
 - C. CANCELED
 - D. SENT
12. Which of the followings are triggers of device linkage rules?
- A. Time-based
 - B. Data-based
 - C. Application-based
 - D. Event-based
 - E. Energy-based
13. Which of the followings are interfaces that can be used to upgrade firmware or software?
- A. LwM2M
 - B. CoAP
 - C. HTTP
 - D. PCP
14. Which of the followings are considered batch operations?
- A. Device registration
 - B. Command delivery
 - C. Location upload
 - D. Device configuration
 - E. Software and firmware upgrades

15. Which of the followings are included in the data forwarding process?
- A. FOTA
 - B. DIS
 - C. DMS
 - D. OBS
 - E. SOTA
16. Which of the followings are included in the application registration authentication?
- A. IAM
 - B. Applications
 - C. Users
 - D. Platform
17. After authentication is done, which of the followings are part of subscribe/ push process?
- A. An application calls the subscription API
 - B. The platform pushes a message
 - C. A device updates its details
 - D. A token is obtained
18. Which of the followings are characteristics for IoT data?
- A. High quality
 - B. Huge volume
 - C. High density
 - D. High time sensitivity
19. Which of the followings are common data problems in the IoT?
- A. No value
 - B. Abnormal transition
 - C. Duplicated data
 - D. Format differences
 - E. Noise interfere

20. Which of the followings are features of IoT studio?

- A. Quick build
- B. Low cost
- C. Small size
- D. Easy O&M

21. Which of the followings are challenges related to the global SIM link?

- A. Difficult deployment
- B. Difficulties in scalability
- C. Difficulties in reliability
- D. Difficult card management

22. Reliability in HUAWEI CLOUD platform covers:

- A. System
- B. Network
- C. Service
- D. Module
- E. Application

23. Which of the followings are true about edge computing?

- A. It is a concept
- B. It is derived from cloud computing
- C. The edge cannot clean data
- D. The edge and the cloud are connected through network

24. Which of the followings are characteristics of Huawei IoT platform?

- A. Reliable
- B. Secure
- C. Access agnostic
- D. Open
- E. Scalable

25. Data cleaning in edge computing includes:

- A. Filtering
- B. Decoupling
- C. Deduplication
- D. Aggregation

Chapter 10. IoT Platform Secondary Development

A. Mark the followings True or False?

1. Product development includes product management, model developing and online debugging.
2. The codec is also called “profile”.
3. The profile describes what a device is, what it can do and how to control it.
4. Only data that is matched with the product model is saved on the IoT platform.
5. The codec decodes binary data reported by application into JSON format that can be read by the devices.
6. NB-IoT devices have high requirements on power consumption, that is why their application layer data uses JSON format.
7. Graphical codec development is recommended.
8. GET action is used to create a resource on the server.
9. PUT action is used to update resources on the server.
10. In an API message, path parameter includes the path part in the URL.
11. In an API message, the body parameter is used after the question mark (?) in the URL.
12. Application access authentication is achieved by exchanging messages with the platform's IAM.
13. The status code in the response message of the querying device is 203.
14. Creating a device requires registering it in the cloud first and then binding it.
15. All developments on the device side can be achieved using MQTT and CoAP/LwM2M.
16. IoTDA stands for Internet of Things Data Analytics.
17. Authentication for devices using LwM2M over CoAP is not possible.
18. Authentication for devices is possible using Native MQTT or MQTTS.
19. When deleting a device successfully, the returned code is 204.
20. Querying device messages is achieved using the PUT method.

21. Product details uniquely identify the product model.
22. When developing a product model, it is possible to import models in an Excel files.
23. “.txt” files can be imported to develop a product model.
24. Raw device data passes to data parsing without codec conversion.
25. URI request has the following format: {URI-scheme} :// {resource-path} / {Endpoint} ? {query-string}.
26. Applications must be authenticated by the IAN service to obtain tokens to integrate functions such as device management.
27. In the token authentication, the validity of a token is 24 hours.
28. An HTTP status code is a group of digits ranging from 1xx to 4xx.
29. The platform authenticates application and devices in the same way.
30. Status code 204 means no content, it is used as a response to a delete request.

B. Check the correct answer, there is only one correct answer for each question:

1. Which of the following is not true about the product model?
 - A. It is also called “profile”
 - B. It defines the properties of a device
 - C. It is created using codes
 - D. It defines what can a device do

2. A product model includes:
 - A. Product details
 - B. Service capabilities
 - C. None of them
 - D. Both of them

3. Which of the following is not done by the codec?
 - A. Encodes binary data into JSON format
 - B. Decodes data in JSON format into binary data
 - C. None of them
 - D. Both of them

4. Which of the following is not true about codec development? it is:
 - A. Graphical
 - B. Written using C++
 - C. Offline
 - D. Script-based

5. Which of the following cannot be performed by application-side API?
 - A. View the application access address on the console
 - B. Report binary data
 - C. Create and manage products
 - D. Deliver commands, properties and messages

6. One of the following is not an API action:
- A. ADD
 - B. GET
 - C. PUT
 - D. DELETE
7. Which of the following is not a parameter used in the API messages?
- A. Path
 - B. Data
 - C. Header
 - D. Query
8. Which of the following methods is used by the application access authentication?
- A. POST
 - B. GET
 - C. PUT
 - D. DELETE
9. What is the status code in the response of the application access authentication?
- A. 200
 - B. 201
 - C. 202
 - D. 203
10. PUT Method is used to:
- A. Application access authentication
 - B. Querying device messages
 - C. Create a device
 - D. Modify device information
11. Which of the following device development method is not supported by Huawei cloud IoT?
- A. Certified sensor
 - B. Certified module
 - C. Certified MCU
 - D. LiteOS

12. Which of the following device development methods is supported by Huawei cloud IoT?
- A. Certified sensor
 - B. Certified module
 - C. Certified MCU
 - D. LiteOS
13. Common development on the device side requires the use of:
- A. Certified MCU and communications module
 - B. MCU/single-chip microcomputer only
 - C. MCU/single-chip microcomputer and communications module
 - D. Certified MCU only
14. Immediate delivery of MQTT device messages is achieved using:
- A. IoT device
 - B. IoT platform
 - C. IoT application
 - D. All of them
15. Which of the following is true about device property reporting in JSON format?
- A. It requires a codec
 - B. It does not require a codec
 - C. It is not possible
 - D. None of them
16. Which of the following protocol(s) can be used for authentication for devices?
- A. Native MQTT
 - B. LwM2M over CoAP
 - C. MQTTS
 - D. All of them
17. When deleting a device successfully, the returned code is:
- A. 201
 - B. 202
 - C. 203
 - D. 204

18. In which of the following API operation(s) a token is returned?

- A. Application access authentication
- B. Device creating
- C. None of them
- D. Both of them

19. IAM service is only used when:

- A. Creating a device
- B. Authenticating application access
- C. Deleting a device
- D. None of them

20. Which of the following device development method is used if the device includes an SDK Tiny?

- A. Certified MCU
- B. Gateway
- C. Common
- D. LiteOS

C. Choose the correct answer, there are multiple correct answers for each question:

1. The process of using IoTDA includes:
 - A. Product development
 - B. Development on the device site
 - C. Development on the application site
 - D. Routine management

2. Which of the followings are included in the service capability of the product model?
 - A. Properties
 - B. Commands
 - C. Commands parameters
 - D. Protocols

3. Which of the followings are included in the product details of the product model?
 - A. Commands
 - B. Commands parameters
 - C. Services
 - D. Device type
 - E. Protocol

4. Which of the followings are methods for developing product models?
 - A. Importing reset models
 - B. Uploading a profile
 - C. Importing models in Excel file
 - D. Customizing functions

5. Codec can be developed using:
 - A. Online development
 - B. Offline development
 - C. Graphical development
 - D. Network development

6. Which of the followings are true about codec?
- A. It decodes binary data reported by devices
 - B. It decodes binary data reported by applications
 - C. It supports graphical development
 - D. It decodes commands to Json format
7. Which of the followings are command delivery methods supported by HUAWEI CLOUD IoT platform?
- A. Immediate delivery of LwM2M/CoAP commands
 - B. Delayed delivery of LwM2M/CoAP commands
 - C. Immediate delivery of MQTT commands
 - D. Delayed delivery of MQTT commands
8. Which of the followings are parts of the request URI?
- A. URI scheme
 - B. Endpoint
 - C. Resource-path
 - D. Query-string
 - E. URL
9. Which of the followings are HTTP request methods?
- A. GET
 - B. SET
 - C. PUT
 - D. INSERT
 - E. DELETE

10. Which of the followings are API authentication method supported by HUAWEI CLOUD IoT platform?

- A. Token authentication
- B. AK/SK authentication
- C. Native MQTT authentication
- D. LwM2M over CoAP authentication

11. Which of the followings are not API operations?

- A. Creating a device
- B. Querying a device
- C. Disabling a device
- D. Decoupling a device
- E. Modifying device information

12. Which of the followings are API operation?

- A. Creating a device
- B. Querying a device
- C. Modifying device information
- D. Querying device messages
- E. Deleting a device

13. Which of the followings are not development mode on the device side?

- A. Certified MCU development
- B. Certified module development
- C. Certified OS development
- D. Certified device development
- E. LiteOS development

14. Which of the followings are true about development on the device side?

- A. Supporting TCP/IP protocol stack has no influence on the communication with the platform
- B. MQTT is the first choice for IoT communication
- C. There are 6 development modes on the development side
- D. Developers must use the IoT device SDK to connect devices to the platform over MQTTS

15. Device authentication can be performed using:

- A. Native MQTT
- B. MQTT
- C. Token
- D. LwM2M over CoAP

Chapter 11. IoT OS

A. Mark the followings True or False?

1. OS is a computer program that manages hardware, software and firmware resources.
2. DOS and windows are examples of programming language handlers.
3. Peripherals hardware includes external memory, input devices and output devices.
4. Internal memory includes RAM, REM and ROM.
5. CPU stands for Central Programming Unit.
6. Punched tapes are examples of the manual operation system.
7. Multi-job batch processing OS developed to time-sharing OS.
8. Time-sharing OS is an operating system that implements a specific function within a defined time frame.
9. In single-job batch processing OS, programs are loaded into the memory and executed individually.
10. Network OS developed after distributed OS.
11. IoT OS can operate in networks where the number of connections might grow up to reach a limit of 10 billion.
12. Open-source Huawei LiteOS entered the IoT field in 2015.
13. High requirements on performance and power consumption for videos are two challenges facing the IoT OS.
14. Smart terminals need to meet three standards: smart connections, smart networking and smart management.
15. Huawei LiteOS includes multiple kernels and one middleware.
16. OS evolves over a long period of time.
17. The second-generation of OS also known as real-time systems.
18. There are three aspects of smartness: intelligent management, intelligent connectivity and intelligent network.

19. Enable users to capture low-quality videos with low power consumption is a challenge to the IoT OS.
20. Huawei LiteOS is used in the consumer field and industry because scenarios of this field have common requirements.

B. Check the correct answer, there is only one correct answer for each question:

1. The OS manages and controls all resources of:
 - A. Software and hardware
 - B. Software only
 - C. Hardware only
 - D. Firmware

2. CPU includes:
 - A. Input devices
 - B. Output devices
 - C. None of them
 - D. Both of them

3. One of the following is not a peripherals hardware in the microcomputer system:
 - A. CD-ROM
 - B. Keyboard
 - C. Printer
 - D. ROM

4. ALU is included within:
 - A. CPU
 - B. RAM
 - C. ROM
 - D. CD-ROM

5. DOS is a(n):
 - A. Central processing unit
 - B. Operating system
 - C. Output device
 - D. Main memory

6. One of the following is not an operating system type:
 - A. Patch OS
 - B. Time-sharing OS
 - C. Complex OS
 - D. Real-time OS

7. Time-sharing OS developed to:
- A. Real-Time OS
 - B. Network OS
 - C. Distributed OS
 - D. Multi-job OS
8. IoT OS should be able to handle connections up to:
- A. 1 billion
 - B. 10 billion
 - C. 100 billion
 - D. None of them
9. Which of the following hardware technology(ies) is(are) supported by the IoT OS?
- A. DSP
 - B. MIPS
 - C. FPGA
 - D. All of them
10. Which of the following is not a challenge to the IoT terminal development?
- A. Multi-sensor coordination that is complex to manage
 - B. High requirements on performance
 - C. Power consumption for videos
 - D. Various IoT platform
11. How many kernel(s) does Huawei LiteOS includes?
- A. 1
 - B. 2
 - C. 3
 - D. 4
12. Which of the following is true about security in the Huawei LiteOS? it is implemented:
- A. In the kernel layer
 - B. In the middleware layer
 - C. Across model's layers
 - D. In the open API layer only

13. Huawei LiteOS became open to consumers on:

- A. 2010
- B. 2011
- C. 2012
- D. 2013

14. In which year Huawei LiteOS entered the IoT field?

- A. 2014
- B. 2015
- C. 2017
- D. 2018

15. Which of the following solution(s) implement Huawei LiteOS?

- A. Smart home
- B. Smart water meter
- C. Smart parking
- D. All of them

C. Choose the correct answer, there are multiple correct answers for each question:

1. Which of the followings are true about the modern computer system?
 - A. It is divided into two parts: hardware and software
 - B. The software is divided into two parts: system and application
 - C. The hardware is divided into two parts: host and peripherals
 - D. The host contains devices such as keyboard.

2. Which of the followings are true about OS?
 - A. OS is a program that manages all software and hardware resources
 - B. OS has a short service life
 - C. OS provide a complex model for user programs
 - D. Only with an OS, the user can run program

3. Which of the followings are types of OS?
 - A. Batch-processing
 - B. Time-sharing
 - C. Real-time
 - D. Distributed

4. Real-time systems are classified to:
 - A. Soft real time system
 - B. Hard real time system
 - C. Distributed real time system
 - D. Fast real time system

5. Which of the followings are challenges facing IoT terminal development?
 - A. Different chipsets
 - B. Different architectures
 - C. Different protocols
 - D. Different applications

6. When developing IoT OS, which of the followings are aspects of smartness?
- A. Intelligent management
 - B. Intelligent application
 - C. Intelligent platform
 - D. Intelligent connectivity
 - E. Intelligent networking
7. Which of the followings are true about LiteOS?
- A. It is an open-source OS
 - B. It uses “1+N” architecture
 - C. It includes “1+N” middleware
 - D. Kernels can be added or removed
8. Which of the followings are challenges to IoT OS?
- A. There are many types of IoT terminals
 - B. Terminals use different communication protocols
 - C. Capturing high-quality videos with low power consumption
 - D. Current terminals are smart

Chapter 12. Sensing Layer Development

A. Mark the followings True or False?

1. All programs process computer data through a simple set of instructions.
2. To implement multiple functions, a register is used.
3. MOV is a common ARM instruction, it is used to transfer data from memory to register.
4. There are two types of instruction sets in today's typical architecture: RISC and CISC.
5. Standard MPUs have a system clock speed of 3 GHz.
6. RAM stores data running in the program, it will disappear after the power goes off.
7. ROM data is lost after the power is off.
8. An interface connects an internal device to an MCU.
9. ADC stands for Analog-to-Digital Converter
10. An interrupt is the process where the CPU stops to execute a new program.
11. In terms of basic sensing functions, there are 5 types of sensing elements.
12. RTD stands for Resistance Temperature Detector.
13. A photoelectric sensor converts electrical signals into optical signals.
14. Huawei LiteOS provides one single memory management algorithm: the static memory allocation.
15. An interrupt can be deleted.
16. The message queue provides an asynchronous processing mechanism.
17. An event is not associated with a task.
18. A semaphore is used only to enable tasks to access system resources synchronously.
19. A mutex is a special binary queue.
20. The system clock is also referred to as time scale or tick.

21. While implementing multiple functions in the circuits, a multiplexer must be added to properly select each one.
22. An instruction set is the smallest functional unit.
23. CISC is used to reduce the complexity of RISC CPU.
24. RISC instruction can be interrupted.
25. System bus connects all hardware parts together for data communication.
26. Task scheduling mechanism is based on priorities.
27. Dynamic memory allocation is not suitable for users with high memory resource requirement.
28. Although interrupts have priorities, if multiple interrupts occur at the same time, they are served simultaneously.
29. Mutex is also called binary semaphore.
30. Timers can be classified into software, firmware and hardware timers.

B. Check the correct answer, there is only one correct answer for each question:

1. Which of the following elements is used to record previous results and subsequent instructions?
 - A. Multiplexer
 - B. Register
 - C. Mux
 - D. None of them

2. LDR ARM instructions is used to:
 - A. Addition
 - B. Subtraction
 - C. Data transfer from memory to register
 - D. Exclusive OR

3. Standard MPUs have a system clock speed of:
 - A. 3 MHz
 - B. 300 MHz
 - C. 3 GHz
 - D. 300 GHz

4. Standard MCUs have a system clock speed that ranges between 10 and 100:
 - A. kHz
 - B. MHz
 - C. GHz
 - D. None of them

5. The system bus in the MCU architecture includes:
 - A. Control bus
 - B. Address bus
 - C. Data bus
 - D. All of them

6. Under which of the following senses the chemical sensor is classified?
 - A. Vision sense
 - B. Auditory sense
 - C. Taste sense
 - D. Olfactory sense

7. In terms of basic sensing functions, which of the following is not a type of senses?
- A. Color
 - B. Taste
 - C. Touch
 - D. Magnet
8. How many classes are used to classify temperature sensors?
- A. 2
 - B. 3
 - C. 4
 - D. 5
9. Which of the following is not a type of heart rate sensor?
- A. Piezoelectric
 - B. Photoelectric
 - C. Piezoresistive
 - D. Photoresistive
10. The process where the CPU stops to execute a new program is called:
- A. Task
 - B. Allocation
 - C. Interrupt
 - D. None of them
11. A task can be:
- A. Created
 - B. Deleted
 - C. Delayed
 - D. All of them
12. One of the following is not a disadvantage of the dynamic memory use:
- A. High performance overheads
 - B. Fragments in the memory pool
 - C. Memory is wasted if there are many small blocks
 - D. Large blocks are cost-effective

13. An interrupt can be:

- A. Deleted
- B. Delayed
- C. None of them
- D. All of them

14. Which of the following is not an inter-task communication?

- A. Queue
- B. Stack
- C. Semaphore
- D. Mutex

15. Which of the following is not true about events?

- A. It is a synchronization inter-task communication
- B. It involves data transmission
- C. Events are independent from each other.
- D. An event is not associated with a task

16. When the number of tasks accessing the same resource reaches the maximum, the semaphore:

- A. Blocks other tasks from accessing the resource
- B. Release all resources
- C. Execute all the tasks
- D. All of them

17. How many statuses does the mutex have?

- A. 2
- B. 3
- C. 4
- D. 5

18. A mutex is locked when:

- A. Two tasks are competing on it
- B. A task owns it
- C. None of them
- D. Both of them

19. Huawei LiteOS provides:

- A. Hardware timers
- B. Software timers
- C. Firmware timers
- D. All of them

20. Which of the following is true about Huawei LiteOS kernel features?

- A. Low power consumption
- B. Strong performance
- C. Ultra-small kernel of less than 6 kB
- D. All of them

C. Choose the correct answer, there are multiple correct answers for each question:

1. Which of the followings are true about instruction set?
 - A. Instructions are a unit of computer language used to design programs
 - B. RISC is designed to reduce complexity of CISC CPU
 - C. CISC run faster than RISC
 - D. The number of instructions in the CISC exceeds that in the RISC

2. Which of the followings are operated by CISC?
 - A. Memory
 - B. Register
 - C. Arithmetic unit
 - D. Input/Output interface

3. Which of the followings are true about processing unit?
 - A. Microcontroller is also called CPU
 - B. CPU contains MPU-memory-Input/Output devices
 - C. Processing unit can be divided into microprocessors and microcontrollers
 - D. The clock frequency of MPU is relatively high compared to CPU

4. Which of the followings are considered as types of sensors?
 - A. Photoelectric
 - B. Temperature
 - C. Acceleration
 - D. Heart rate

5. Which of the followings are true about sensing technologies?
 - A. Sensors collect analog signals
 - B. Some sensors contain DAC module
 - C. Precision of the sensor determine the accuracy of data collect
 - D. There are five types of sensors

6. Which of the following components are included in the Huawei LiteOS kernel?
- A. Task management
 - B. Event management
 - C. Memory management
 - D. Time management
7. Which of the followings are true about tasks?
- A. They are the smallest running unit of an OS
 - B. Each task is dependent
 - C. They are processed following sequence
 - D. Task scheduling mechanism is based on priorities
 - E. There are a total of 32 priorities for tasks
8. Which of the followings are true about memory?
- A. The memory management module is responsible for initializing, allocating and releasing memory
 - B. Memory management is classified to static and dynamic
 - C. Static memory is more cost-effective for users who requires large memory resources
 - D. Fragments are generated in static memory management
9. Which of the followings are true about interrupts?
- A. When it happens, CPU stops to execute new program.
 - B. Interrupts have priorities
 - C. Interrupt is not an instant trigger
 - D. Interrupt is used to synchronize tasks

10. Which of the followings are considered inter-task communication of the LiteOS?

- A. Queue
- B. Event
- C. Semaphore
- D. Mutex

11. Which of the followings are true about Queue?

- A. It is a data structure
- B. It can function as a buffer
- C. It is a special type of semaphore
- D. It is used to implement exclusive access to critical resources

12. Which of the followings are true about events?

- A. Data transmissions occur between them
- B. An event is like a condition for triggering a task
- C. LiteOS uses 32-bit variable to indicate an event
- D. Only 31 event type can be set

13. Which of the followings are true about the semaphore?

- A. It is a data structure
- B. Semaphore is a special type of mutex
- C. It is used to implement synchronization between tasks
- D. It is used to implement exclusive access to critical resources

14. Which of the followings are true about mutex?

- A. It is a special type of semaphore
- B. It is also called "Binary semaphore"
- C. It is used to exclusively occupy shared resources
- D. It has only two states

15. Which of the followings are true about timers?

- A. They are used to generate interrupts
- B. They are classified into software, firmware and hardware timers
- C. It is used to synchronize tasks
- D. The number of hardware timers are limited by hardware

Chapter 13. AT Commands for Communication Modules

A. Mark the followings True or False?

1. AT commands are sent from DTE to DCE.
2. After a TE sends an AT command to an MT, the MT sends back the response.
3. AT commands stands for ATtraction commands.
4. PUT command is a category of AT commands.
5. Execution commands can be written with or without parameters.
6. Set command is used to display valid parameter values set by other AT commands.
7. AT+<x>=P1 is the syntax of a read command.
8. Execution command is used to instruct a module to execute a specific function.
9. AT+<x>=? is the syntax of a read command.
10. AT+<x>=<...> is not a valid syntax of the AT commands.

B. Check the correct answer, there is only one correct answer for each question:

1. AT commands stands for:
 - A. ATtention commands
 - B. Adapter Terminal commands
 - C. Adapter Technical commands
 - D. ATtraction commands
2. AT commands are:
 - A. Sent from terminal equipment
 - B. Sent to a terminal equipment
 - C. Sent from a mobile terminal
 - D. All of them
3. AT commands are used within:
 - A. NB-IoT networks only
 - B. Wi-Fi networks only
 - C. NB-IoT and Wi-Fi networks
 - D. Bluetooth networks only
4. How many categories are there for AT commands?
 - A. 2
 - B. 3
 - C. 4
 - D. 5
5. AT command type "=XX" is used to:
 - A. Display valid parameter values set by other AT commands
 - B. Set the attributes carried in the AT command
 - C. Query attributes set by other AT commands
 - D. Instruct a module to execute a specific function
6. Read command is referred to as:
 - A. "=XX"
 - B. "=?"
 - C. "?"
 - D. Null

7. AT execution command is used to:
- A. Display valid parameter values set by other AT commands
 - B. Set the attributes carried in the AT command
 - C. Query attributes set by other AT commands
 - D. Instruct a module to execute a specific function
8. Which of the following AT commands can be used with and without parameters?
- A. Set
 - B. Test
 - C. Read
 - D. Execution
9. For which of the following commands the syntax "AT+<x>=?" is used?
- A. Set
 - B. Test
 - C. Read
 - D. Execution
10. "AT+CGSN" is an example for a:
- A. Set command
 - B. Test command
 - C. Execution command with parameters
 - D. Execution command without parameters

Answers

Chapter 1. IoT development history and Overview

A. True or False questions

- | | | | | |
|-----------|-----------|-----------|-----------|-----------|
| 1. False | 2. True | 3. False | 4. True | 5. False |
| 6. True | 7. True | 8. False | 9. True | 10. False |
| 11. True | 12. False | 13. False | 14. True | 15. True |
| 16. False | 17. True | 18. False | 19. False | 20. True |
| 21. True | 22. True | 23. True | 24. False | 25. True |
| 26. False | 27. True | 28. False | 29. True | 30. True |

B. Multiple choices questions (One correct answer)

- | | | | | |
|-------|-------|-------|-------|-------|
| 1. C | 2. A | 3. D | 4. D | 5. D |
| 6. B | 7. A | 8. D | 9. C | 10. C |
| 11. A | 12. C | 13. D | 14. B | 15. A |
| 16. B | 17. C | 18. D | 19. B | 20. D |

C. Multiple choices questions (Several correct answers)

- | | | | | |
|------------|-------------|----------|---------------|-------------|
| 1. A, C | 2. A, E | 3. B, C | 4. A, B, C, D | 5. A, D, E |
| 6. B, C, D | 7. C, D | 8. A, B | 9. A, D, E | 10. A, C, D |
| 11. A, D | 12. A, C, D | 13. A, D | 14. A, B, C | |

Chapter 2. IoT Industry Applications and Solutions

A. True or False questions

- | | | | | |
|-----------|-----------|-----------|-----------|-----------|
| 1. True | 2. False | 3. True | 4. False | 5. True |
| 6. True | 7. False | 8. True | 9. False | 10. False |
| 11. False | 12. True | 13. True | 14. True | 15. False |
| 16. False | 17. False | 18. False | 19. True | 20. False |
| 21. True | 22. True | 23. True | 24. False | 25. True |
| 26. True | 27. False | 28. True | 29. True | 30. False |

D. Multiple choices questions (One correct answer)

- | | | | | |
|-------|-------|-------|-------|-------|
| 1. A | 2. D | 3. C | 4. D | 5. A |
| 6. D | 7. D | 8. B | 9. D | 10. D |
| 11. C | 12. B | 13. B | 14. D | 15. C |
| 16. A | 17. B | 18. C | 19. C | 20. C |

E. Multiple choices questions (Several correct answers)

- | | | | | |
|---------------|---------------|------------|------------|----------|
| 1. B, C, E | 2. A, B, C, D | 3. B, C, E | 4. A, B, D | 5. A, D |
| 6. A, B, D, E | 7. A, B, C | 8. A, B, D | 9. A, B, E | 10. B, D |

Chapter 3. IoT Security Technologies

A. True or False questions

- | | | | | |
|----------|-----------|-----------|-----------|-----------|
| 1. False | 2. False | 3. True | 4. False | 5. False |
| 6. True | 7. True | 8. False | 9. True | 10. False |
| 11. True | 12. False | 13. False | 14. True | 15. False |
| 16. True | 17. False | 18. True | 19. True | 20. True |
| 21. True | 22. False | 23. False | 24. False | 25. True |
| 26. True | 27. True | 28. False | 29. False | 30. True |

B. Multiple choices questions (One correct answer)

- | | | | | |
|-------|-------|-------|-------|-------|
| 1. B | 2. D | 3. C | 4. A | 5. D |
| 6. B | 7. C | 8. D | 9. A | 10. D |
| 11. B | 12. C | 13. C | 14. A | 15. C |
| 16. B | 17. B | 18. C | 19. B | 20. A |

C. Multiple choices questions (Several correct answers)

- | | | | | |
|------------|------------|---------------|---------|----------------|
| 1. B, D, E | 2. B, D | 3. A, B, C, D | 4. A, D | 5. A, C, D |
| 6. B, C, D | 7. B, C, D | 8. B, C | 9. A, C | 10. A, B, D, E |

Chapter 4. Overview of common IoT communication Technologies

A. True or False questions

- | | | | | |
|-----------|-----------|-----------|-----------|-----------|
| 1. False | 2. True | 3. True | 4. True | 5. False |
| 6. False | 7. True | 8. False | 9. False | 10. True |
| 11. True | 12. True | 13. False | 14. True | 15. False |
| 16. False | 17. False | 18. True | 19. True | 20. False |
| 21. True | 22. True | 23. False | 24. True | 25. False |
| 26. False | 27. True | 28. True | 29. False | 30. True |

B. Multiple choices questions (One correct answer)

- | | | | | |
|-------|-------|-------|-------|-------|
| 1. B | 2. D | 3. C | 4. D | 5. C |
| 6. B | 7. A | 8. C | 9. D | 10. A |
| 11. C | 12. A | 13. B | 14. A | 15. B |
| 16. A | 17. B | 18. C | 19. B | 20. C |

C. Multiple choices questions (Several correct answers)

- | | | | | |
|----------------|-------------|----------------|----------------|----------------|
| 1. A, B, D, E | 2. C, D | 3. A, C | 4. A, B, C, D | 5. D, E |
| 6. B, D | 7. A, B, C | 8. C, D | 9. A, B, C | 10. A, C, D, E |
| 11. C, D | 12. A, B, C | 13. A, B, C, D | 14. A, B, D, E | 15. B, C |
| 16. A, B, C, D | 17. A, B, C | 18. A, B, E | 19. A, B, C, D | 20. B, C |

Chapter 5. NB-IoT Communication Technologies and Solutions**A. True or False questions**

- | | | | | |
|-----------|-----------|-----------|-----------|-----------|
| 1. True | 2. True | 3. False | 4. True | 5. True |
| 6. False | 7. False | 8. False | 9. True | 10. True |
| 11. False | 12. True | 13. False | 14. True | 15. True |
| 16. True | 17. False | 18. False | 19. True | 20. False |
| 21. True | 22. True | 23. False | 24. False | 25. False |
| 26. False | 27. True | 28. True | 29. False | 30. True |

B. Multiple choices questions (One correct answer)

- | | | | | |
|-------|-------|-------|-------|-------|
| 1. B | 2. A | 3. B | 4. D | 5. C |
| 6. B | 7. B | 8. C | 9. D | 10. D |
| 11. D | 12. C | 13. B | 14. B | 15. C |
| 16. C | 17. B | 18. D | 19. B | 20. D |

C. Multiple choices questions (Several correct answers)

- | | | | | |
|---------------|---------------|------------|---------|---------------|
| 1. A, B, D, E | 2. A, B, C, D | 3. A, B, C | 4. B, C | 5. A, B, C, D |
| 6. A, D | 7. B, C, D | 8. B, D | 9. A, B | 10. A, D |

Chapter 6. 5G Communications Technologies and Solutions**A. True or False questions**

- | | | | | |
|-----------|-----------|-----------|-----------|-----------|
| 1. False | 2. True | 3. True | 4. False | 5. True |
| 6. False | 7. True | 8. True | 9. False | 10. False |
| 11. False | 12. False | 13. True | 14. True | 15. False |
| 16. True | 17. True | 18. False | 19. True | 20. True |
| 21. True | 22. False | 23. True | 24. False | 25. True |
| 26. True | 27. False | 28. True | 29. True | 30. True |

B. Multiple choices questions (One correct answer)

- | | | | | |
|-------|-------|-------|-------|-------|
| 1. B | 2. D | 3. D | 4. B | 5. C |
| 6. B | 7. D | 8. C | 9. D | 10. B |
| 11. D | 12. D | 13. A | 14. D | 15. A |
| 16. C | 17. A | 18. C | 19. B | 20. D |

C. Multiple choices questions (Several correct answers)

- | | | | | |
|------------|---------------|---------|------------|---------------|
| 1. A, C | 2. A, B, C, D | 3. A, D | 4. A, B, D | 5. A, B, C, D |
| 6. A, C, E | 7. A, D | 8. A, B | 9. A, B, C | 10. A, B, D |

Chapter 7&8: Huawei IoT Gateways (Industrial + Home)**A. True or False questions**

- | | | | | |
|-----------|-----------|----------|-----------|-----------|
| 1. True | 2. False | 3. False | 4. True | 5. True |
| 6. False | 7. False | 8. False | 9. True | 10. False |
| 11. False | 12. False | 13. True | 14. True | 15. False |
| 16. True | 17. True | 18. True | 19. False | 20. True |
| 21. True | 22. True | 23. True | 24. False | 25. False |
| 26. True | 27. True | 28. True | 29. False | 30. True |

B. Multiple choices questions (One correct answer)

- | | | | | |
|-------|-------|-------|-------|-------|
| 1. D | 2. A | 3. D | 4. C | 5. B |
| 6. B | 7. D | 8. C | 9. A | 10. C |
| 11. A | 12. A | 13. D | 14. C | 15. D |
| 16. D | 17. B | 18. D | 19. D | 20. A |

C. Multiple choices questions (Several correct answers)

- | | | | | |
|---------------|----------------|---------------|------------|-------------------|
| 1. A, B, C, D | 2. A, C, D | 3. A, D, E | 4. A, B | 5. A, D |
| 6. A, B | 7. A, B, C, D | 8. A, B, C, D | 9. A, B, D | 10. A, B, D |
| 11. A, B, E | 12. A, C, D, E | 13. A, B, D | 14. A, D | 15. A, B, C, D, E |

Chapter 9. IoT Platform**A. True or False questions**

- | | | | | |
|-----------|-----------|-----------|-----------|-----------|
| 1. True | 2. False | 3. True | 4. False | 5. True |
| 6. False | 7. True | 8. True | 9. False | 10. True |
| 11. False | 12. False | 13. True | 14. False | 15. True |
| 16. True | 17. False | 18. True | 19. True | 20. False |
| 21. True | 22. False | 23. True | 24. True | 25. False |
| 26. True | 27. False | 28. False | 29. True | 30. False |
| 31. True | 32. False | 33. True | 34. True | 35. False |
| 36. True | 37. False | 38. True | 39. False | 40. True |

B. Multiple choices questions (One correct answer)

- | | | | | |
|-------|-------|-------|-------|-------|
| 1. C | 2. D | 3. D | 4. C | 5. D |
| 6. C | 7. B | 8. D | 9. B | 10. D |
| 11. B | 12. B | 13. A | 14. D | 15. D |
| 16. B | 17. B | 18. A | 19. B | 20. D |

C. Multiple choices questions (Several correct answers)

- | | | | | |
|----------------|----------------|---------------|-------------------|-------------|
| 1. B, C, D | 2. A, B, D | 3. A, B, C, D | 4. A, B, E | 5. A, C, D |
| 6. A, C, D | 7. C, D | 8. A, C, D | 9. B, C | 10. A, C |
| 11. A, B, C, D | 12. A, B, D | 13. A, D | 14. A, B, C, D, E | 15. B, C, D |
| 16. A, B, D | 17. A, B, C | 18. B, D | 19. A, B, C, D, E | 20. A, B, D |
| 21. A, D | 22. A, B, C, D | 23. A, B, D | 24. A, B, C, D, E | 25. A, C, D |

Chapter 10. IoT Platform Secondary Development**A. True or False questions**

- | | | | | |
|-----------|-----------|-----------|-----------|-----------|
| 1. True | 2. False | 3. True | 4. True | 5. False |
| 6. False | 7. True | 8. False | 9. True | 10. True |
| 11. False | 12. True | 13. False | 14. True | 15. True |
| 16. False | 17. False | 18. True | 19. True | 20. False |
| 21. True | 22. True | 23. False | 24. False | 25. False |
| 26. True | 27. True | 28. False | 29. False | 30. True |

B. Multiple choices questions (One correct answer)

- | | | | | |
|-------|-------|-------|-------|-------|
| 1. C | 2. D | 3. C | 4. B | 5. B |
| 6. A | 7. B | 8. A | 9. B | 10. D |
| 11. A | 12. A | 13. C | 14. C | 15. B |
| 16. D | 17. D | 18. A | 19. B | 20. C |

C. Multiple choices questions (Several correct answers)

- | | | | | |
|---------------|-------------------|---------------|---------------|-------------|
| 1. A, B, C, D | 2. A, B, C | 3. D, E | 4. A, B, C, D | 5. B, C |
| 6. A, C | 7. A, B, C, D | 8. A, B, C, D | 9. A, C, E | 10. A, B |
| 11. C, D | 12. A, B, C, D, E | 13. C, D | 14. B, C | 15. A, B, D |

Chapter 11.IoT OS**D. True or False questions**

- | | | | | |
|-----------|-----------|----------|-----------|-----------|
| 1. False | 2. False | 3. True | 4. False | 5. False |
| 6. True | 7. True | 8. False | 9. True | 10. False |
| 11. False | 12. True | 13. True | 14. True | 15. False |
| 16. True | 17. False | 18. True | 19. False | 20. True |

A. Multiple choices questions (One correct answer)

- | | | | | |
|-------|-------|-------|-------|-------|
| 1. A | 2. C | 3. D | 4. A | 5. B |
| 6. C | 7. A | 8. C | 9. D | 10. D |
| 11. A | 12. C | 13. C | 14. B | 15. D |

B. Multiple choices questions (Several correct answers)

- | | | | | |
|---------------|---------|---------------|---------|------------|
| 1. A, B, C, D | 2. A, D | 3. A, B, C, D | 4. A, B | 5. A, B, C |
| 6. A, D, E | 7. A, B | 8. A, B, C | | |

Chapter 12.Sensing Layer Development**A. True or False questions**

- | | | | | |
|-----------|-----------|-----------|-----------|-----------|
| 1. True | 2. False | 3. False | 4. True | 5. True |
| 6. True | 7. False | 8. False | 9. True | 10. True |
| 11. False | 12. True | 13. False | 14. False | 15. False |
| 16. True | 17. True | 18. False | 19. False | 20. True |
| 21. True | 22. False | 23. False | 24. True | 25. True |
| 26. True | 27. False | 28. False | 29. True | 30. False |

B. Multiple choices questions (One correct answer)

- | | | | | |
|-------|-------|-------|-------|-------|
| 1. B | 2. C | 3. C | 4. B | 5. D |
| 6. C | 7. C | 8. A | 9. D | 10. C |
| 11. D | 12. D | 13. C | 14. B | 15. B |
| 16. A | 17. A | 18. B | 19. B | 20. D |

C. Multiple choices questions (Several correct answers)

- | | | | | |
|------------|-------------|----------|----------------|----------------|
| 1. A, B | 2. A, B, C | 3. C, D | 4. A, B, C, D | 5. A, B, C |
| 6. A, C, D | 7. A, D, E | 8. A, B | 9. A, B, C | 10. A, B, C, D |
| 11. A, B | 12. B, C, D | 13. C, D | 14. A, B, C, D | 15. A, D |

Chapter 13.AT Commands for Communication Modules**A. True or False questions**

- | | | | | |
|----------|----------|----------|----------|-----------|
| 1. True | 2. True | 3. False | 4. False | 5. True |
| 6. False | 7. False | 8. True | 9. False | 10. False |

D. Multiple choices questions (One correct answer)

- | | | | | |
|------|------|------|------|-------|
| 1. A | 2. A | 3. C | 4. D | 5. B |
| 6. C | 7. D | 8. D | 9. B | 10. D |

Appendix I: Abbreviations

Abb. (Full name): Definition

#

3GPP (3rd Generation Partnership Project): A consortium with seven standards organizations that develop telecommunication protocols for cellular networks.

A

ADC (Analog-to-Digital Converter): An electrical system that transforms a signal from an analog form into a digital one.

AGC (Automated Guided Cart): A type of AGV, specialized for moving traditional carts by being positioned underneath them.

AGV (Automated Guided Vehicle): A robot that follows marker lines on the floor using different technologies for navigation.

AIoT (Artificial Intelligence and Internet of Things): A combination of artificial intelligence technologies with the internet of things infrastructure to enhance the performance of the two.

AK/SK (Access Key/ Secret Key): security credentials used to authenticate users identities and to authorize specific resources or rights to them.

ALU (Arithmetic and Logic Unit): A combinational digital electronic circuit that executes arithmetic operations on binary-coded integers, such as addition and multiplication, and bitwise operations on binary numbers, such as AND and shifting. ALU is used to build more complex units such as central processing unit (CPU) and graphics processing unit (GPU).

AMI (Advanced Metering Infrastructure): A two-way integrated system that provides communication between utilities and customers. It consists of smart meters, telecommunications networks, and data management software.

AP (Access Point): A data-link layer networking hardware device that permits wireless devices to connect to a wired network.

API (Application Programming Interface): A software interface that allows for two or more programs to communicate in a way that one is offering a service to the others.

APT (Advanced Persistent Threat): A state, or non-state, threat actor, usually a group of hackers or specialists that stealthily obtained unauthorized network access and stays around undetected for a considerable time.

AR (Augmented Reality): A real-world system that provides a compound of real and virtual worlds as well as human real-time interaction. AR technologies are implemented in the physical world, with information or objects added virtually.

AT command (Attention command): A text-based set of instructions used to control a modem. Originally, it was developed by Dennis Hayes in 1981.

B

B2B (Business-to-Business): A commercial transaction between business entities carried out by professional staff and usually includes negotiation.

B2C (Business-to-Consumer): A direct commercial transaction between a business entity and its customers aiming for selling products by passing any type of middlemen.

B2H (Business-to-Human): A commercial transaction between a business entity and customers aiming for selling products based on individual needs.

BLE (Bluetooth Low Energy): An energy-aware variation of Bluetooth that defines a wireless personal area network.

BR (Basic Rate): The Bluetooth classical signaling mode, it streams data over 79 channels in the 2.4 GHz unlicensed ISM frequency band.

BRAS (Broadband Remote Access Server): A device that sits at the edge of an ISP's core network, it routes traffic to and from broadband remote access devices.

BSC (Base Station Controller): A 2G device that is responsible for handling traffic and signaling between a user equipment and the network switches. .

BSD (Berkeley Software Distribution): A discontinued OS built on Research Unix, developed and distributed by the Computer Systems Research Group at the University of California, Berkeley.

BSS: it can be:

- **(Basic Service Set)**: A topology mode in WiFi where the network includes WiFi-supporting devices and one access point used to link the devices with each other and with the Wired LAN.
- **(Business Support System)**: A set of business elements used by the telecommunications service provider to run its business operations towards customers.

BTS (Base Transceiver Station): A hardware device that handles the wireless communication between the user equipment and the rest of the cellular network.

C

CA: it can be:

- **(Certificate Authority)**: A structure that keeps and signs digital certificates. A digital signature proves the ownership of a public key.
- **(Carrier Aggregation)**: A wireless communication technology that allows for per-user multiple frequency blocks assignment resulting in increased bit rate

CAN (Controller Area Network): A standard vehicle bus that allows internal communications between microcontrollers and other onboard devices without the need for a host computer.

CDMA (Code-Division Multiple Access): A channel access method used in shared-medium networks. By assigning a unique code to users and implementing a spread spectrum technology, CDMA allows many users to share a frequency band at the same time with no interference.

CIG (Cloud Interworking Gateway): A gateway that sits between the application and the platform to integrate any on-premise or third party systems with the platform solutions.

CISC (Complex Instruction Set Computer): A computer architecture used to define instructions that includes multi-step operations or involve several low-level operations.

CoAP (Constrained Application Protocol): An application-layer telecommunication protocol for devices limited in terms of hardware or energy. CoAP is described in RFC 7252

CPE (Customer-Premises Equipment): A terminal device owned by the service provider but located at the subscriber side, it connects to the distribution infrastructure provided by the telecommunication service.

CPU (Central Processing Unit): An electronic circuit that executes instructions of the programs. It performs basic arithmetic and logical operations as well as handling the input/output of the computing system.

CRM (Customer Relationship Management): Studying the interactions between an organization and its customers using data analysis tools.

CS (Cloud Stream): A stream computing system that is distributed, and real-time. It is major characteristics low latency, high throughput, and high reliability.

CSMA/CD (Carrier Sense Multiple Access with Collision Detection): A medium access control method for LAN used in Ethernet technologies prior to 2011. When CSMA/CD is used, no device transmits data if the shared medium is already occupied.

D

DAC (Digital-to-Analog Converter): An electrical system that transforms a signal from a digital form into an analog one.

DAG (Directed Acyclic Graph): A Directed Acyclic Graph: a directed graph, consists of vertices and edges that do not form loops.

DC: it can be:

- **(Data Center):** A space dedicated to host computer systems and its components.
- **(Dual Connectivity):** A technology that allows 4G and 5G to operate at the same time.

DCE (Data Circuit Equipment): A signal converter and an interfacing device that sits in between the transmission medium and a Data Terminal Equipment.

DDoS (Distributed Denial-of-service): A cyber-attack occurs when multiple machines are operating together to attack one target.

DICE (Device Identifier Composition Engine): A hardware or software techniques for cryptographic operations.

DIS (Data Ingestion Service): A service for collect, process, and distribute real-time streaming data.

DMS (Distributed Message Service): A message middleware service based on distributed clustering technology. It provides reliable, scalable, fully managed queues for storing messages.

DOS (Disk Operation System): An umbrella term for a group of text-based operating systems that were common in the eighties and nineties.

DRAM (Dynamic Random-Access Memory): A semiconductor-based variation of RAM that uses capacitive memory cells to store each bit, thus, unlike SRAM, DRAM does need continuous refresh to keep its contents.

DRIS (Digital Road Infrastructure Solution): A set of digital technologies used to create smarter and interactive roads, this include road infrastructure and logistics services as well as smart vehicles

DRX (Discontinuous Reception): An energy-aware communication mode used by wireless devices to extend the expected duration of service. The device periodically enters the sleep phase where the energy consumption drops down to its minimum.

DSL (Digital Subscriber Line): A set of wired telecommunication technologies used to connect to the internet over the traditional telephone lines.

DSP (Digital Signal Processor): A specific type of digital processor used to execute instructions designed for signal processing operations such as those performed on the samples of a continuous variable of time or frequencies.

DSRC (Dedicated Short-Range Communications): A short-range wireless telecommunication technology, designed to be used in devices mounted inside vehicles. The technology was standardized by European Committee for Standardization in EN 12253 and EN 12253 as well as ISO in ISO 14906.

DTE (Data Terminal Equipment): An end device that Receives data from users, delivers data, and vice versa.

DTLS (Datagram Transport Layer Security): An application-layer protocol that is used to secure data between communicating applications. It is suitable for the UDP scenarios because it is able to overcome lost or reordered datagram situations. DTLS was originally described in RFC 4347, and later in RFC 6347 and RFC 9147.

DTLS+ (Datagram Transport Layer Security Plus): An Extended version of DTLS, developed to answer the IoT needs in terms of reducing the number of messages exchanged between the client and the server and prolonging battery life.

E

E2E (End-To-End): A design concept in the Internet that requires application-specific features such as intelligence, reliability, and security to reside at the end nodes and not in the network itself.

ECC (Edge Computing Consortium): A cooperative industrial platform that promotes open cooperation in ICT fields for Edge computing. As for 2022, the consortium includes six dominated IT entities notably ARM, Huawei and Intel.

ECU (Electronic Control Unit): An embedded system used to control at least one electrical system, or subsystem, in a motor vehicle.

EDR (Enhanced Data Rate): A signaling mode for Bluetooth, introduced in version 2.0. It supports a bit rate up to 3 Mbit/s.

eDRX (extended Discontinuous Reception): An IoT extension for DRX in which sleep time lasts longer to reduce power consumption.

EIA (Electronic Industries Alliance): A former American trade organization was founded in 1924 and seized operation in 2011. EIA was engaged in developing industry standards to ensure compatibility and interchangeability for products of different manufacturers.

eMBB (enhanced Mobile BroadBand): A main application domain in 5G. eMBB supports scenarios where higher throughput is required such as Mixed reality.

eMTC (enhanced Machine Type Communication): A technology standard developed by 3GPP and introduced in 2016. It defines low-power wide-area network for machine-to-machine and IoT applications.

eNB (evolved NodeB): A hardware device that handles the wireless communication between the user equipment and the LTE network. It corresponds to Node B in UMTS and to BTS in GSM.

EPC: it can be:

- **(Electronic Power Control)**: an engine management system with a computer-driven ignition. EPC helps recognize computerized system issues and draws the driver's attention when need mechanical intervention is needed.
- **(Evolved Packet Core)**: A network architecture used in the 4G LTE network. Unlike 2G and 3G networks where voice and data are processed separately, EPC provides converged framework for processing voice and data.

EPP (Enhanced Parallel Port): A de-facto standard for the parallel port that was later standardized by IEEE in the late 1990s under the codename IEEE 1284. EPP defines a method for high bitrate bi-directional parallel communication between a computer and peripheral devices.

eSIM (Embedded Subscriber Identity Module): A variation of the SIM card that is embedded programmably into another physical device.

ESS (Extended Service Set): A topology mode in WiFi where the network includes WiFi-supporting devices and two or more APs appears to devices as a single AP with large coverage.

ETC (Electronic Toll Collection): Electronic Toll Collection: A wireless payment system used to automatically collect fees from vehicles. A small device is fixed inside the vehicle, the device is to be detected and a bill is charged, when the vehicle crosses detection technologies such as a toll bridge, or a toll tunnel.

ETSI (European Telecommunications Standards Institute): an independent non-profit standardization organization founded in 1988. ETSI supports the development and testing of global technical standards of information and communication technologies.

E-UTRAN (Evolved Universal Terrestrial Radio Access Network): A network architecture for the air interface in the 4G LTE network, it includes eNodeBs and UEs.

F

FAN (Field Area Network): A spatial-based type of data network that covers a large number of devices spread throughout a given geographical area.

FBB (Fixed BroadBand): An umbrella term used to describe a set of high-speed, uni- or bidirectional connectivity technologies available for public use of at least 256 Kbit/s.

FDM (Frequency Division Multiplexing): A medium-sharing technique where the total bandwidth in the communication medium is divided into a number of non-overlapping frequency channels, each of which can be assigned later to a user of the telecommunication system to exchange data over it.

FDMA (Frequency Division Multiple Access): An FDM-based channel access method used in shared-medium networks. When used, each user is assigned a frequency band in a way that if different users access the channel at the same time, no interference will occur.

FE (Fast Ethernet): Also called IEEE 802.3u, a wired telecommunication technology and a variation of Ethernet. It was introduced in 1995 and has a nominal bit rate of 100 Mbit/s.

F-OFDM (Filtered Orthogonal Frequency Division Multiplexing): A variation of OFDM where the resulted frequency bands can vary in the ranges and the number of subcarriers.

FOTA (Firmware-Over-The-Air): A method of distribute new firmware to a group of devices.

FPGA (Field-Programmable Gate Array): A configurable type of integrated circuit that contains an array of programmable logic blocks and designed to be setup by a customer after the manufacturing process.

FSK (Frequency Shift Keying): A type of digital modulation for analog carrier. In FSK, the frequency of an analog signal carry coded digital data.

FTTB (Fiber-To-The-Building): A variation of the FTTX, where the optical fiber reaches the boundary of the building such as a basement or department store.

FTTH (Fiber-To-The-Home): A variation of the FTTX, where the optical fiber reaches the boundary of the living space such as an office or an apartment.

FTTN (Fiber-To-The-Neighborhood): A variation of the FTTX, where the optical fiber reaches a street cabinet. Usually, a copper cable is used later to reach the premises of the customers.

FTTX (Fiber-To-The-X): An umbrella term for any broadband network architecture that uses optical fiber technologies to provide the local loop, completely or partially, for last mile telecommunications.

FWA (Fixed Wireless Access): An umbrella term for a set radio-based telecommunications technologies used to deliver services to retail end-users.

G

GDPR (General Data Protection Regulation): A regulation in the European Union dedicated to data protection and privacy. It was made by the European Parliament and Council of the European Union on the 14th of April 2016 and implemented on the 25th of May 2018.

GE (Gigabit Ethernet): Also called IEEE 802.3ab, a wired telecommunication technology and a variation of Ethernet. It was introduced in 1999 and has a nominal bit rate of 1 Gbit/s.

GFW (Great FireWall): A set of legal and technical measures in China to regulate access to the Internet locally and to monitor traffic to and from the Internet.

GGSN (Gateway General packet radio service Support Node): A variation of SGSN used in the UMTS mobile network, it is used to route calls outside the mobile network towards other networks such as PSTN.

GIS (Geographic Information system): A geographical database combined with software for managing, analyzing, and visualizing.

GIV (Global Industry Vision): Huawei future vision for an intelligent connected world of industry.

GMSC (Gateway Mobile service Switching Center): A variation of SGSN used in the UMTS mobile network, it is used to route calls outside the mobile network towards other networks such as PSTN.

gNB (next generation NodeB): A hardware device that handles the wireless communication between the user equipment and the 5G network. It corresponds to Node B in UMTS and to eNode B in LTE.

GPRS (General Packet Radio Service): A standard for a digital Cellular mobile network developed by the ETSI in the late 1990s and maintained by 3GPP. From a generation perspective, GPRS is described as 2.5G, it provides data rates of 56–114 kbit/s.

GPS (Global Positioning System): A radionavigation-satellite service provided by the United States Space Force. GPS provides users with geolocation and time information to anywhere near the Earth's surface.

GPU (Graphics Processing Unit): An electronic circuit that is specially designed to accelerate operations related to images and video processing.

GSM (Global System for Mobile Communications): A standard for a 2G digital Cellular mobile network developed by the ETSI in the late 1980s and early 1990s. GSM is suitable for voice calls and SMS; it can provide a bit rate up to 9.6 Kbit/s.

H

HFC (Hybrid Fiber Coaxial): A term used to describe a broadband wired data network that includes both optical fiber and coaxial cable.

HUD (Head-Up Display): An Umbrella term used to describe any see-through display that presents visual data without requiring the users to change the angle of view from their usual viewpoints.

HTTP (HyperText Transfer Protocol): An application-layer protocol allows the transfer of hypermedia information following the request-response method and using the client-server model. The current version is HTTP/3, it was released in 2022 and described in RFC 9114.

HTTPS (HyperText Transfer Protocol Secure): Also called HTTP Over TLS, an extension of HTTP, created in 1994 originally described in RFC 2818 and later in RFC 9110. HTTPS is used to provide secure communication for clients and servers in a data network.

I

IAM (Identity and Access Management): A set of processes forced by an administrative entity to manage the behavior of the users of its information systems. It includes both: Authentication of the user identity, and authorization of access to the entity resources.

ICT (Information and Communication Technology): A term refer to the in integration of a set of information technologies covers any product that send, process, store or receive information electronically in a digital form.

IEEE (Institute of Electrical and Electronics Engineers): Pronounced I-triple-E, a professional non-profit association for electronic and electrical engineering. By creating technical standards, and through conferences and publications, IEEE focus, among many other similar disciplines, on electrical, electronic, computer and telecommunications engineering.

IEF (Intelligent EdgeFabric): An edge computing solution for IoT applications to became able to make use of the Edge instead of sending data to the cloud. It can also provide data analysis and decision-making support.

IETF (Internet Engineering Task Force): A non-profit organization created in 1986. IETF is part of internet society, and it is responsible for creating open standards for Internet technologies.

IDE (Integrated Development Environment): A software package that supports computer programmers in the software development process. Usually, it includes a text editor, a debugger, a compiler, and a GUI builder.

IDPS (Intrusion Detection and Prevention System): Two broad terms used to describe security measures. An intrusion detection system monitors and analyses events on the network searching for possible threats. while an intrusion detection system includes performing the detection as well as the stopping of the detected incidents.

IDS (Intrusion Detection System): See IDPS.

IMEI (International Mobile Equipment Identity): A 15-bit unique identifier allocated by GSM association to valid devices connected to mobile-cellular networks.

IMSI (International Mobile Subscriber Identity): A unique identifier associated with a mobile cellular network used to, internationally, identify users. IESI is defined in the ITU-T Recommendation E.212 and is usually 15 digits long.

Internet (Interconnected networks): A set of non-centralized interconnected data networks. The Internet project started in 1969 in the USA, entered commercial use in 1989, and is the largest data network worldwide. It is considered a pillar of the current civilization.

IoT (Internet of Things): A data network structure that enables physical objects to be connected and exchange data. IoT nodes tend to need low bit rates and to work in with limited conditions in terms of computation and energy.

IoTDA (Internet of Things Device Access): A Basic service of the Huawei cloud IoT platform that enables users to quickly connect hardware devices to the platform and integrate their application.

IoV (Internet of Vehicles): A data network structure that enables smart vehicles to contact and exchange data with one another, and with other objects along the roads.

IP (Internet Protocol): A family of layer 3 protocols used on the internet. It provides the networks with major functions such as Internetworking, addressing, and fragmentation. The family includes two members IPv4 and IPv6.

IPS (Intrusion Detection and Prevention System): See IDPS.

IPv4 (Internet Protocol version 4): A variation of internet protocol standardized in 1981 in RFC 791. Written using the dotted decimal notation, IPv4 defined 32-bit addresses which were not sufficient to contain the Internet growth, thus, it was exhausted in 2011, and is slowly being replaced with IPv6.

IPv6 (Internet Protocol version 6): The major protocol in the internet, it is a variation of internet protocol standardized in 1995 and currently described in RFC 8200. Written using the hexadecimal numeric system, IPv6 defines 128-bit addresses to overcome the execution problem of its predecessor, IPv4.

ISM (Industrial, Scientific and Medical): A set of bands within the radio spectrum that are internationally reserved for, typically, unlicensed operations in the industrial, scientific, and medical domains.

ISO (International Organization for Standardization): A non-governmental international standard organization founded in 1947. It develops standards from technical domains such as electrical engineering, and nontechnical fields such as authority control.

ITS (Intelligent Transportation System): A traffic management application, usually smart, that provide decision-making support for transport networks administrative bodies.

ITU (International Telecommunication Union): A UN agency specialized in information and communication technologies. The organization is created in 1865 and merged into the UN system by 1949. It consists of three sectors: radio, standardization, and development.

ITU-R (International Telecommunication Union - Radiocommunication Sector): A sector of the ITU, created in 1992 to take over the objectives of the International Radio Consultative Committee handling the international spectrum of the radiofrequency and satellite orbit resources.

ITU-T (International Telecommunication Union – Telecommunication standardization sector): A sector of the ITU, created in 1993 to take over the objectives of the International Telegraph and Telephone Consultative Committee handling crating standards for ICT. ITU-T technical committee includes member states, representing of both the private sector and Academia.

IVI (In-Vehicle Infotainment): A set of software and hardware devices located inside the vehicles to provide audio and video output for entertainment purposes.

I/O (Input/Output): Data interfaces of information systems that communicate it with other systems or with physical devices. The input interface receives data entering the system, while the output interface is where the information exits the system.

J

JVM (Java Virtual Machine): A 32-bit open virtual machine developed in 1994 and maintained by Sun Microsystems. JVM is a part of java runtime environment and is mainly used to enable PCs to run Java programs.

L

L2TP (Layer To Tunnelling Protocol): A link-layer tunnelling protocol used in data networks to create tunnels between two terminals, to carry data, usually over heterogeneous Layer 2 networks. L2TP standard was published in 2000 (RFC 2661), the current version is described in RFC 3931.

LAN (Local Area Network): A spatial-based type of data network that covers an area limited to a small-to-medium residence or an office building.

LiFi: Mistakenly thought to come from Light Fidelity. However, there is no clear origin of the name except similarity with WiFi. An umbrella term used to describe a set of technologies that use ultraviolet, infrared, and visible light to wirelessly transmit data. LiFi was standardized in IEEE 802.15.7 which defines different physical layers that support bit rates up to 96 Mbit/s. an umbrella term used to describe a set of technologies that use ultraviolet, infrared, and visible light to wirelessly transmit data. LiFi was standardized in IEEE 802.15.7 which defines different physical layers that support bit rates up to 96 Mbit/s.

LoRa (Long Range): A low-power wide-area wireless proprietary standard for a data network that provides a bit rate of 0.3 kbit/s to 50 kbit/s. LoRa developed in France in 2015.

LPWA (Low-Power Wide-Area): A variation of WAN that is designed to support low-power and low-bit-rate devices.

LTE (Long Term Evolution): A standard for a 4G digital Cellular mobile network developed by the 3GPP in 2008 and is described in Release 8. LTE support only packet switching services and

includes two technologies: Frequency-division duplex and time-division duplex, it can provide a bit rate of around 100 Mbit/s.

LwIP (Lightweight Internet Protocol): An open Internet protocol suite designed to support embedded systems. It was developed in the late 2000s by Adam Dunkels and is maintained by the lwIP developers' group.

LwM2M (Lightweight Machine-To-Machine): An application-layer CoAP-based client-server protocol used for management of IoT devices.

M

M2M (Machine-To-Machine): A type of wired or wireless data communication that directly links two devices.

MAC (Media Access Controller): A sublayer of data link layer in the IEEE 802 LAN/MAN standards responsible for managing the interactions between devices and both wired and wireless telecommunication media.

MBB (Mobile BroadBand): A commercial name for a set of services that provide wireless Internet access through cellular mobile networks.

Mbus (Meter Bus): A wired telecommunication technology developed in the late 1990s by European Committee for Standardization, it is described in EN 13757-2 and EN 13757-3. Mbus is used for a remote meter's reading.

MCL (Maximum Coupling Loss): The maximum conducted power level that a communication system can tolerate before being considered out of service.

MCU (Main Control Unit): Also called a Microcontroller, A tiny-sized computer carried on a single integrated circuit chip. A microcontroller unit includes at least one processor core, different types of memories namely: RAM, ROM and flash, as well as several programmable I/O peripherals.

MDM (Meter Data Management): software that receives, stores, and analyses the data obtained from a smart metering system.

MEC (Multi-access edge computing): formerly mobile edge computing; A network architecture defined by ETSI to add the capabilities of cloud computing at the edge of mobile cellular networks.

MIIT (Ministry of Industry and Information Technology): A ministry in the Chinese government, created in 2008. It is responsible for the regulation and development of the Internet, wireless, broadcasting, communications, production of electronic and information goods as well as the software industry.

MIMO (Multi-Input Multi-Output): The use of multiple antennas in radio telecommunication for multiplying the capacity of the channel and to enable sending and receiving of more than one data signal simultaneously.

MIPS (Microprocessor without Interlocked Pipelined Stages): A set of RISC-based instruction set architectures developed by MIPS Computer Systems in 1985. The current version: Release 6, developed in 2014, supports both 32-bit and 64-bit integers formats.

MME (Mobile Management Entity): The unit of the 4G EPC that is responsible for handling the control signals between the UEs and the rest of the EPC.

M-MIMO (Massive Multi-Input Multi-Output): A variation of MIMO used to improve spectral and energy efficiency. mMIMO implicates the use of a large number of antennas, up to thousands, arranged in a single array.

mMTC (massive Machine-Type Communications): A machine-to-machine communication in wired or wireless data networks where a massive number of devices are exchanging data with minimum or no human intervention.

MMU (Memory Management Unit): An electronic circuit that is designed to handle memory access operations including read and write data as well as translation of virtual address into physical addresses.

MQTT (Message Queuing Telemetry Transport): A lightweight open publish-subscribe machine-to-machine application-layer protocol developed in 1999 and maintained by OASIS. MQTT is used to feed information to large numbers of devices that have limited constrains in term of energy and bit rates.

MPU (MicroProcessor Unit): Also called a processor, for simplicity, a hardware device that performs logical and arithmetical operations. MPU usually incorporates the functionalities of CPU, ALU, MMU, GPU and other computation units.

MR (Mixed Reality): A real-time system that merges reality and virtuality together creating a new hybrid environment.

MRS (MapReduce Service): A big-data solution offered by cloud operators to store, process, and analyse a massive amount of data.

MSA (Multi-Streaming Aggregation): A variation of carrier aggregation developed by 3GPP for the LTE. It is mainly used to enhance data rate in the mobile cellular networks.

MSC (Mobile service Switching Center): A voice-call switch device in GSM. MSC handles also other services provided by the mobile cellular system such as SMS.

MT (Mobile Terminal): a broad term used to describe any telecommunication device, usually portable, that is able to wirelessly connect with a cellular mobile network.

MU-MIMO (Multi-User Multi-Input Multi-Output): A variation of MIMO that includes multiple multi-antenna-equipped terminals communicating with each other.

N

NAN: it can be:

- **(Near-me area network)**: A logical type of data network that includes a group of telecommunication devices located within a certain proximity from each other but not connected to the same data network.
- **(Neighbor Awareness Networking)**: Also called Wi-Fi Aware, A cluster-based network architecture supported by Wi-Fi. When used, devices can discover each other and directly connect with no further need for configuration or additional infrastructure

NB-IoT (NarrowBand Internet of Things): A standard for wireless LPWAN developed by 3GPP and was first described in 2016 in Release 13 for low-cost IoT devices and applications supported in the LTE-Advanced Pro. NB-IoT was later integrated in the 5G.

NB-OFDM (Narrowband Orthogonal Frequency Division Multiplexing): An extension for OFDM, developed to adapt the technology to narrow-band applications where the frequency bands shrink remarkably in terms of range.

NE (Network Element): An SNMP term used to describe a hardware device connected to a data network with an SNMP agent installed on it to perform network management functions requested by the network management systems.

NFC (Near-Field Communication): A broad term used to describe a set of physical-layer telecommunication protocols developed to wirelessly exchange data between devices located at a maximum distance of 4 cm. NFC protocols use an unlicensed ISM frequency band of 13.56 MHz and support bit rates of 106 to 424 kbit/s.

NFV (Network Function Virtualization): A data network architecture based on virtualization technologies to provide hardware-independent networking services.

NGC (Next Generation Core): The architecture of the 5G operator network. It is built to respond to very high demands for bandwidth, a massive number of connections, and ultra-low delay. It also supports several technologies including SDN, NFV and network slicing.

NIST (National Institute of Standards and Technology): An agency of the United States Department of Commerce created in 1901. NIST is active in physical sciences and aims to promote American innovation and industrial competitiveness.

NR (New Radio): A radio access technology developed by 3GPP for the 5G mobile cellular networks. It was first described in Release 15 in 2018.

NMS (Network Management System): A set of applications used to create a framework for network engineers to monitor and analyse key functions of the network to keep its high operational performance.

NSA (Non-StandAlone): A network architecture supported by the 5G in the first deployment phase. NSA enables the 5G network to coexist with other LTE networks and makes use of the 4G core that has been already installed and working, especially handling the 5G control signalling.

O

O2O (Online-To-Offline): A term in digital marketing describes the digital the approaches used to attract consumers from the digital worlds into the physical stores.

OBD (On-Board Diagnostics): A term used to describe a capability in the vehicle's system for self-diagnostic and error reporting.

OBS (OBject storage Service): A service provided by cloud operators offering high reliability and secure data sharing.

OBU (On-Board Unit): Telecommunication device mounted on vehicles and supports DSRC. It is usually used for paying toll as well as intervehicle communication.

OEM (Original Equipment Manufacturer): A broad term used in the automotive and computer industry to refer to the entity that first produced the commercial product, partly or completely.

OFDM (Orthogonal frequency-division multiplexing): An extension of FDM introduced in 1966 by Bell Labs. OFDM includes the use of closely spaced orthogonal subcarriers that have overlapping spectra, the overlapping does not affect the quality of the signals thanks to the orthogonality of the subcarrier.

OFDMA (Orthogonal Frequency Division Multiple Access): An OFDM-based multiple-carrier channel access method used in shared-medium networks. By assigning orthogonal frequency carriers to users, OFDMA allows many users, each using multiple carriers, to share the communication medium at the same time with no interference.

OICT (Operational, Information, and Communications Technologies): An extension term for ICT, it adds operational technologies which are hardware or software used to monitor and control equipment, assets, processes, and events in the industrial domain.

OLT (Optical Line Terminal): A hardware device sits at the service provider endpoint of the optical network to provide both electro-optical conversion operations and optical signal multiplexing.

ONT (Optical Network Terminal): A demultiplexer device at the end of the fiber to obtain customer signals and feed them to its equipment.

OS (Operating System): A set of software responsible for managing computing system resources, both software and hardware.

OSGi (Open Services Gateway initiative): An organization founded in 1999 develops open standards for Java software and services.

OSI (Open Systems Interconnection): A conceptual layer-based model for nodes used in data networks. The model divides the work with network nodes into 7 layers based on functionality. The goal is to achieve the interoperability of communication systems without

taking into account their underlying specifications. The model was first proposed by ISO in 1977 and standardized in ISO 7498.

OSS (Operations Support System): A management system used by telcos to provide functions includes error detection and service provisioning as well as inventory and configuration of their network.

OTA (Over-The-Air): A broad term used to describe a set of methods used to distribute new software, new firmware, update data for a large number of devices or users.

OTN (Optical Transmission Network): A multiplexing system for transport data over optical fibers. It is defined by ITU-T Recommendation G.709 and is able to support up to 400 Gbit/s in 2021.

OTT (Over-The-Top): A subscription-based media service that offers content via cable, broadcast satellite television, or any other platform that provides content distribution over the Internet.

O&M (Operations & Management): A routine works, and any additional activities or actions needed to keep a targeted system operating within functional conditions.

P

PAN (Personal Area Network): A spatial-based type of data network that covers an area within a person's workspace.

PAYD (Pay As You Drive), see UBI.

PCB (Printed Circuit Board): Also called printed wiring board, a hardware structure that consists of a set of conductive and insulating layers. PCB provides a surface to solder electronic components in fixed positions as well as connection media to link these components.

PCI (Programmable Communications Interface), see USART.

PCP (Port Control Protocol): An application-layer protocol used to support NAT in IP hosts. PCP was proposed in 2013 and is standardized in RFC 6887.

PDC (Personal Digital Cellular): An absolute 2G cell mobile network standard, operated in the 1990s and 2000s, but was later phased out to be replaced by 3G and subsequent cellular standards.

PHYD (Pay How You Drive), see UBI.

PLC (Power Line Communication): Also called Power-Line Carrier, a wired communication technology that is based on electric power distribution networks. There are two major standards for PLC: Recommendation G.hn/G.9960, adopted by ITU-T in 2009, and IEEE 1901, developed in 2010 by IEEE.

PKI (Public Key Infrastructure): A system that includes hardware and software dedicated to creating, distributing, storing, and using public keys for digital signatures and encryption.

PMU (Power Monitoring Unit): A measurement hardware device used to access real-time energy parameters of a given device, some PMUs provides a way to store the collected data for later analysis.

PSK (Pre-Shared Key): A feature for low-power devices developed by 3GPP, standardized Release 12 and published in 2015. PSM aims to reduce power consumption in wireless nodes to maximize battery life.

PSM (Power Saving Mode): A feature for low-power devices developed by 3GPP, standardized Release 12 and published in 2015. PSM aims to reduce power consumption in wireless nodes to maximize battery life.

PTW (Paging Time Window): A time parameter set for the eDRX technology, it describes a fixed interval within the eDRX cycle when the network can connect to the UE, if traffic is queued for it.

PV (PhotoVoltaic): A physical phenomenon in which energy delivered by light is converted into an electrical form.

PWB (Printed Wiring Board): see PCB.

Q

QoS (Quality of Service): A set of quantitative measurements of the performance of a data network. Usually, QoS is expressed in terms of packet loss, bit rate, throughput, delay, jitter and other performance parameters.

R

RAM (Random Access Memory): A type of volatile memory used to store digital data in computer systems. Volatility means that the memory loses all its contents if the electrical supply goes off, while random access means the time needed to access data stored in any

address is the same. In RAM, data can be written or read with no limitation in terms of the number of times.

RF (Radio Frequency): A band of frequencies ranges between 20 kHz and 300 GHz. All electronic telecommunication systems use frequencies from the RF band. In the frequency spectrum, the radio band is preceded by the audio band and followed by the infrared.

RFID (Radio-Frequency Identification): A low-cost short-range wireless technology used to exchange data by means of electromagnetic fields. RFID uses tags with predefined information that can be fixed to objects or cards. The tags can be passively and remotely powered and read using a specific reader. RFID is standardized in ISO/IEC 18000.

RISC (Reduced Instruction Set Computer): A computer architecture used to define simple instructions where each instruction performs only one function.

ROM (Read-Only Memory): A type of non-volatile memory used to store digital data in computer systems. Non-volatility means that the memory does not lose its contents if the electrical supply goes off. In ROM, data can be written only one time by the manufacturer and can be electronically modified after that, data can also be read with no limitation in terms of the number of times.

RR (Round-Robin): A method of handling objects such as document or data packets in a circular way where the object starts from a point and pass by different stages or receivers, then return to the starting point.

RRH (Remote Radio Head) see RRU.

RRU (Remote Radio Unit): Also called remote radio head, a wireless hardware device used in several mobile cellular networks to extend the wireless coverage of the network in challenging environments such as rural areas or tunnels.

RS (Recommended Standard): A literal prefix for standard names that were developed by EIA.

RSU (Road-Side Unit): A DSRC-based radio transceiver used wirelessly to communicate with other onboard devices mounted in vehicles such as OBU or ETC.

RTD (Resistance Temperature Detector): Also called resistance thermometer, a family of metal-based sensor devices used to measure temperature up to 500 C.

RTOS (Real Time Operating System): A variation of operating systems dedicated to processing data obtained from real-time applications. Real-time processing means that the time needed to process a task is less than the time lapsed until the next task, of the same type, arrives.

RTU (Remote Terminal Unit): Also called a Remote Telemetry Unit and Remote Telecontrol Unit, a hardware device that includes a CPU and a set of digital and analog input and outputs, it is used to collect telemetry data from the field and transmit it to a control system for purposes of monitoring and analysis.

S

SA (StandAlone): A network architecture supported by the 5G. SA enables the 5G network to operate autonomously with no support from other LTE EPC or eNBs.

SC-FDMA (Single-Carrier Frequency-Division Multiple Access): A FDMA-based single-carrier channel access method used in shared-medium networks. By assigning different users different sets of non-overlapping sub-carriers, SC-FDMA allows many users, each using a single carrier, to share the communication medium at the same time with no interference.

SCMA (Sparse Code Multiple Access): A code-based non-orthogonal channel access method used in shared-medium networks. By assigning a unique code to users and implementing a spread spectrum technology, SCMA allows many users to share a frequency band at the same time with no interference.

SDK (Software Development Kit): A set of one-package installable software tools used to create applications. Usually, an SDK is hardware-specific and includes a text editor, compiler, debugger, and GUI builder.

SDMA (Space Division Multiple Access): A channel access method used in radio telecommunication. When used, parallel spatial sites are created, and the telecommunication system is duplicated within each site. Thus, two users in two sites can be assigned the same frequencies at the same time, and no interference will occur.

SDN (Software-Defined Networking): An architecture developed to simplify the management of data networks. In SDN, the control plane is separated from the data plan and is centralized in a device called a controller. The architecture depends on a protocol called OpenFlow, or

another similar proprietary to allowing the controller to communicate with network devices that include the data plane.

SHA (Secure Hash Algorithm): A board name used to describe a member of the Secure Hash Algorithms family which is developed and maintained by NIST. the family includes SHA-0, SHA-1, SHA-2, and SHA-3. Each of these algorithms uses a cryptographic hash function.

SHF (Super High Frequency): A sub-band in the radio frequencies that ranges from 3 and 30 gigahertz, these frequency values correspond to wavelength from 1 to 10 cm, that is why it is also called the centimetre band. Radar applications run in this range, it includes the following sub-bands: S, C, X, Ku, K, or Ka.

SIM (Subscriber Identity Module): Also called a SIM card, an integrated circuit used in mobile cellular networks to store digital including authentication keys and IDs that uniquely identify a subscriber such as an IMSI assigned from the network operator stored in the card. SIM cards are available in three sizes: full, mini-SIM, and micro-SIM cut-outs.

SMS (Short Message Service): A text messaging service provided by mobile cellular network operators. It was introduced in GSM and is supported by all subsequent systems. In SMS, each message can contain up to 160 alpha-numeric characters.

SNMP (Simple Network Management Protocol): An application-layer protocol used to pass configuration to network devices, and to collect information from them for management purposes. The protocol includes 3 versions, SNMPv1 developed in 1988 and described in 3 three documents: RFC 1065 to RFC 1067, SNMPv2 defined by RFC 1441 in 1993, and SNMPv3 defined in RFC 3411 in 2002.

SOAP (Simple Object Access Protocol): An XML-based application-layer protocol developed, in 1998, for message exchange.

SoC (System-on-a-Chip): An architecture of integrated circuits where all the functions and components of a system are integrated on a single chip.

SOTA (Software-Over-The-Air): Also called Over-the-air programming, A set of methods used to distribute new software, set configuration, or update encryption keys to a group of devices.

SQL (Structure Query Language): A standard domain-specific query language used to handle structured data stored in a relational database management system. The language was first

created by Donald D. Chamberlin and Raymond F. Boyce in 1974 and standardized by ANSI in 1986.

SRAM (Static Random-Access Memory): A variation of RAM that uses flip-flop circuitry to store each bit, thus, unlike DRAM, SRAM does not need a continuous refresh to keep its contents.

STB (Set Top Box): A hardware customer-side device commonly used in the TV industry. STB read the source signal from the cable or the dish antenna and converts it into a format that can be displayed on a display device.

T

TA (Terminal Adapter): A piece of hardware equipment used to connect a terminal device to a data network.

TCP (Transmission Control Protocol): A transport-layer protocol used for reliable exchange of segments within a data network. TCP is a main pillar of the Internet, it was developed in 1974 and standardized in RFC 792.

TDM (Time Division Multiplexing): A medium-sharing technique where the periodic time window used in the communication medium is divided into a number of subsequent timeslots, each of which can be assigned later to a user of the telecommunication system to exchange data over it.

TDMA (Time Division Multiple Access): A TDM-based channel access method used in shared-medium networks. When used, within a periodic time frame, each user is assigned a time slot in a way that if each user accesses the shared medium in its time slot, using the same frequency, no interference will occur.

TE (Terminal Equipment): A broad term used to describe a hardware device located at the end of telecommunication links. It can be a source or destination of packets in data networks.

TLS (Transport Layer Security): A session-layer protocol used to provide security for applications in data networks. TLS provides both block and stream ciphers. TLS was developed in 1999 by IETF and standardized in RFC 2246, the current version is 1.3, it was introduced in 2018 and described in RFC 8446. The protocol is accepted as a successor to Secure Sockets Layer.

TLSF (Two-Level Segregated Fit): A general-purpose dynamic memory allocator designed to answer real-time application requirements. The allocator implements an algorithm that includes two-level indexing to help achieve bounded and fast response time.

TPM (Trusted Platform Module): A standard to implement a dedicated microcontroller, designed to secure hardware by means of integrated cryptographic keys, called a secure crypto processor. It was developed in 2007 by the trusted Computing Group and the first ISO/IEC joint technical committee, it is standardized in ISO/IEC 11889.

TSDB (Time Series Data Base): Time Series Data Base: A variation of databases optimized to store pairs of time and values called times series.

TTM (Time-To-Market): A commercial term used to describe the time needed for a product from being imagined until being ready for sale.

U

UART (Universal Asynchronous Receiver-Transmitter): A wired telecommunication technology that includes asynchronous serial transmission with configurable data format and transmission bit rates.

UBI (Usage-Based Insurance): A dynamic type of vehicle insurance where fees are based on data constantly collected about the vehicle, including distance covered and driver and behavior and excluding vehicle type.

UDP (User Datagram Protocol): A transport-layer protocol used for an unreliable exchange of datagrams within a data network. it was developed in 1980 by David Reed and standardized in RFC 768.

UE (User Equipment): A broad term used in the 3GPP mobile cellular networks terminology to describe an end-user device able to communicate with the network

UHD (Ultra-High Definition): A set of resolutions for display devices that follows the 16:9 aspect ratio. In 2022, it includes two formats: 4K and 8K.

UHF (Ultra-High Frequency): A sub-band in the radio frequencies that ranges from 300 MHz and 3 GHz, these frequency values correspond to wavelength from 1 m to 1 dm, that is why it is also called the decimetre band. Radar applications run in this range, it includes the L and S IEEE sub-bands.

UMTS (Universal Mobile Telecommunications System): A standard for a 3G digital Cellular mobile network was developed by the 3GPP in late 1999 in Release 99. UMTS is suitable for voice calls and for browsing the Internet. Originally, UMTS was designed to provide a bit rate up to 384 kbit/s.

UNB (Ultra-Narrow Band): A broad term used to describe devices or systems that are capable of handling telecommunication radio channel with a very narrow bandwidth, typically 100 Hz.

URI (Uniform Resource Identifier): Uniform Resource Identifier: A sequence of characters used in the web to uniquely identify physical or logical objects such as names and resources. It was defined in 1998 by Tim Berners-Lee in RFC 2396.

URL (Uniform Resource Locator): A specific type of URI used as a reference to identify a resource and its location on the web. It was first defined in 1994 by Tim Berners-Lee in RFC 1738 and is currently maintained by IETF.

URLLC (Ultra-Reliable Low-Latency Communication): A main application domain in 5G. URLLC supports delay-sensitive scenarios where system latency is around 1 ms, such as remote surgery and IoV.

USART (Universal synchronous and asynchronous receiver-transmitter): Also called programmable communications interface, A wired telecommunication technology that includes both synchronous and asynchronous serial transmission with configurable data format and transmission bit rates. Several data links and physical protocols developed to support this technology including SDLC, HDLC, and PPP.

USB (Universal Serial Bus): A set of standards for the terminals of the cables and the physical and data link layer of the OSI model. USB is a family of wired telecommunication technologies that can transmit both power and data, it was first introduced in 1996 as a result of collaboration between enterprises. As for 2022, it can provide a bit rate up to 40 Gbps.

V

V2I (Vehicle-To-Infrastructure): A variation of V2X used to describe a communication link between the vehicle and road infrastructure such as a traffic light.

V2N (Vehicle-To-Network): A variation of V2X used to describe a communication link between the vehicle and the IoV network.

V2P (Vehicle-To-Pedestrian): A variation of V2X used to describe a communication link between the vehicle and walkers or people on foot, the communication can be established with wearable devices held by these entities, or it can be simply a form of echo-reply to detect their physical presence.

V2V (Vehicle-To-Vehicle): A variation of V2X used to describe a communication link between the two vehicles.

V2X (Vehicle-To-Everything): A broad term used to describe a communication link between a vehicle and other entities in the IoV architecture. V2V covers a set of sub-interfaces such as V2V, V2P, and V2N.

VM (Virtual Machine): An emulation that duplicates an OS on another OS. Usually, it is used on hosts to provide different OSs without the need of installing the OS on an independent physical machine.

VR (Virtual Reality): A simulated environment system that provides parallel worlds for entertainment, education, medical and military purposes.

VRP (Versatile Routing Platform): An OS for network devices supported by Huawei.

vSIM (virtual Subscriber Identity Module): virtual Subscriber Identity Module: A technology in mobile devices to virtualize SIM cards in a way that the physical SIM can be totally replaced. The user later can switch between the vSIMs to change the operator via an application with no need to insert or take out physical SIMs.

W

WAN (Wide Area Network): A spatial-based type of data network that covers a large geographical. WANs are usually operated by telcos and can be used to connect widely separated LANs.

WLAN (Wireless Local Area Network): A variation of LAN where connections are all wireless. WLAN is usually based on IEEE 802.11 standards, but it is not limited to it.

WWAN (Wireless Wide Area Network): A variation of WAN where connections are all wireless. Mobile cellular networks, LoRa, and Sigfox are examples of data networks in this category.

Appendix II: Reference images

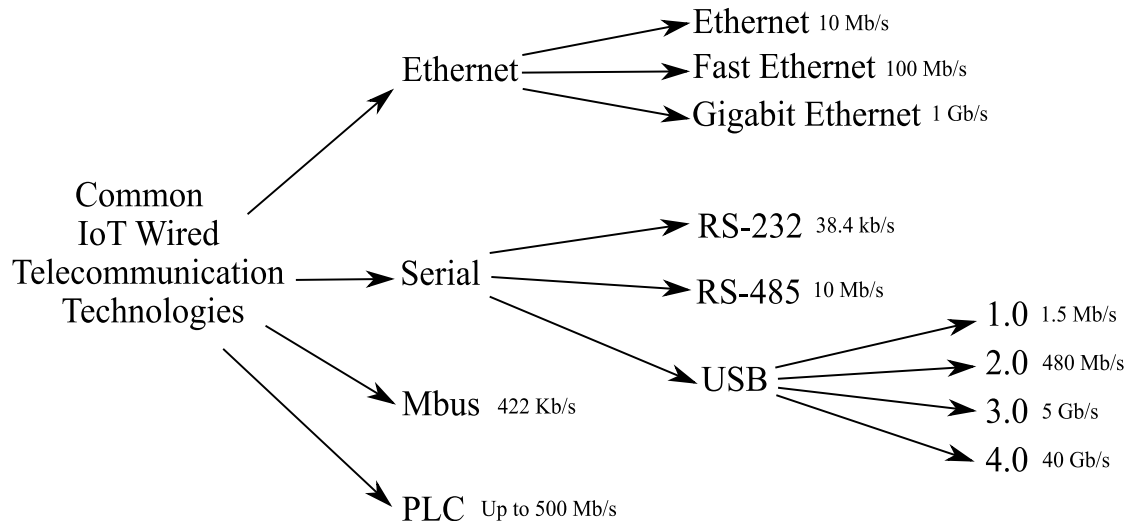


Figure II-1: Common IoT Wired Technologies classification

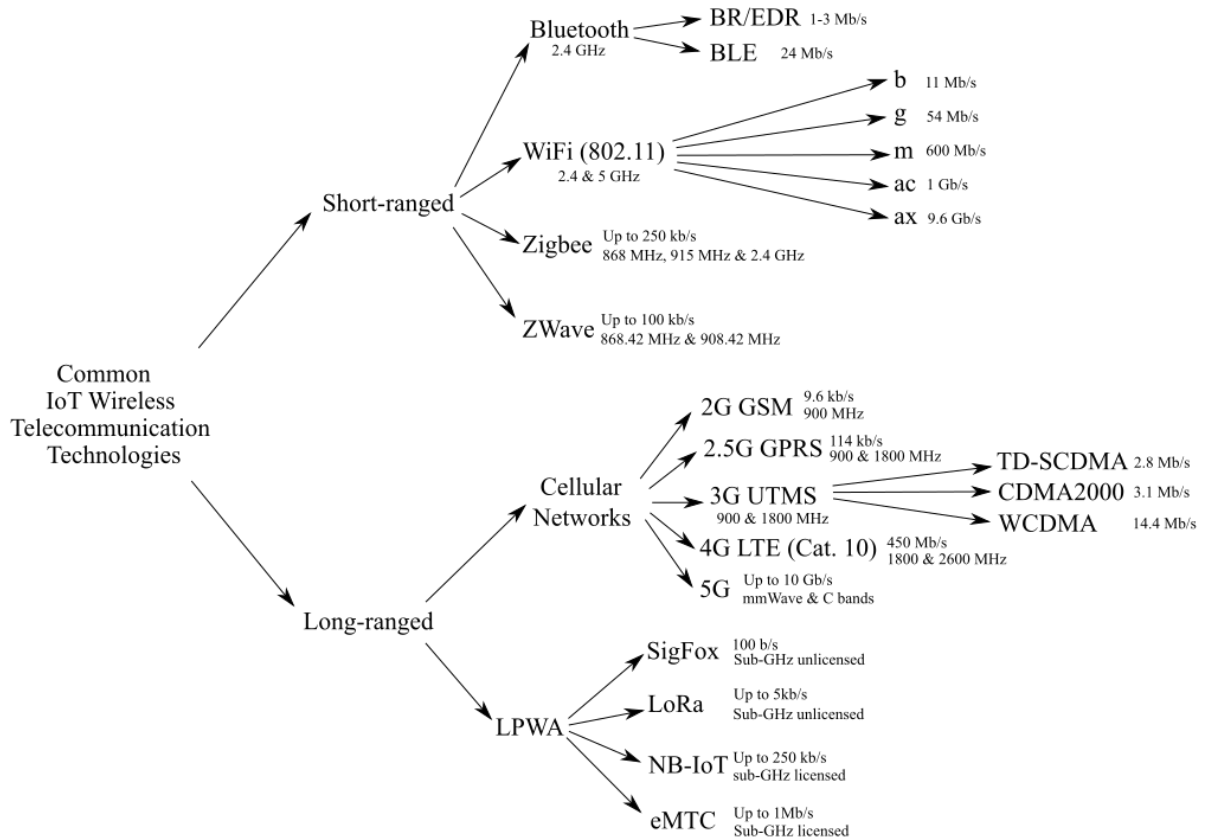


Figure II-2: Common IoT Wireless Technologies classification

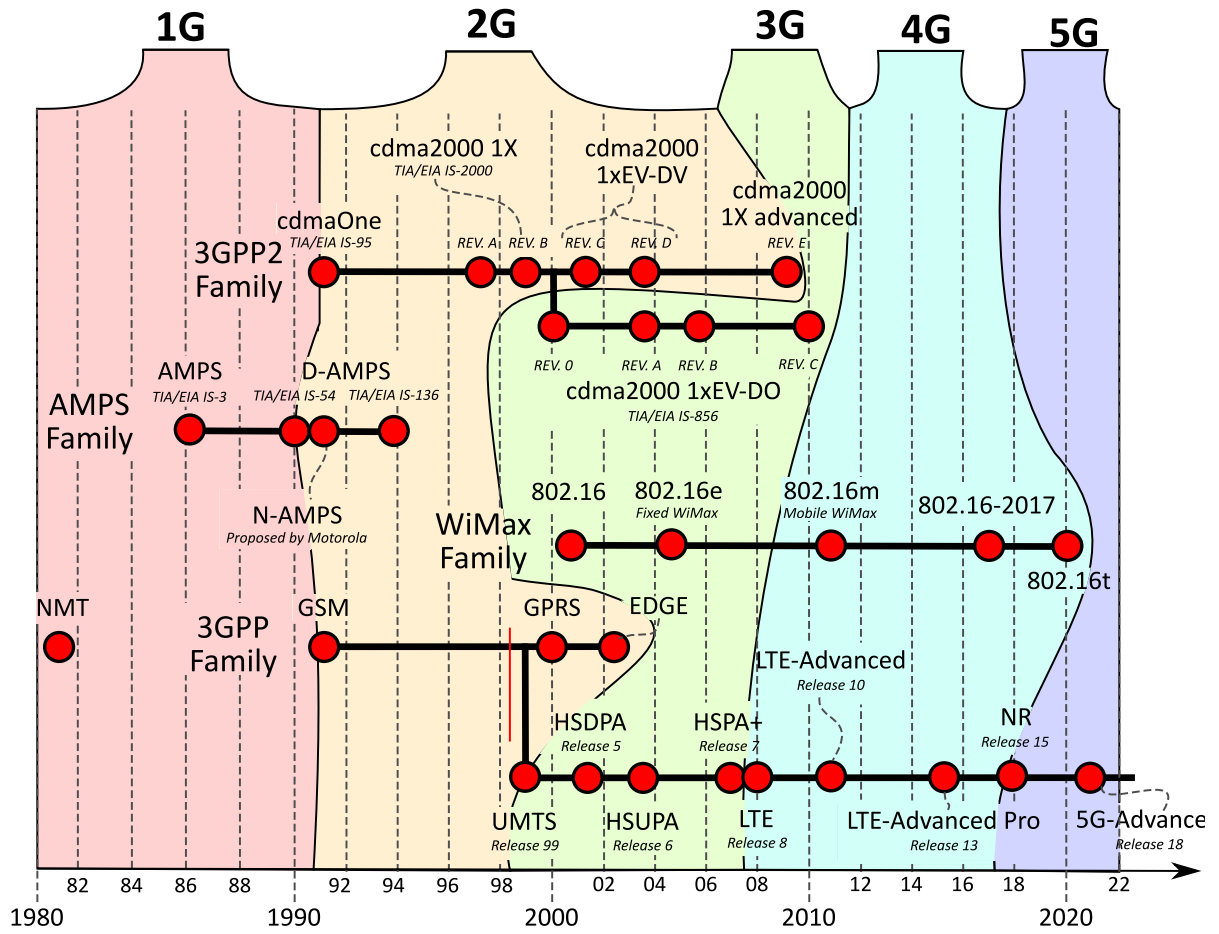


Figure II-3: Timeline for generations of mobile cellular networks

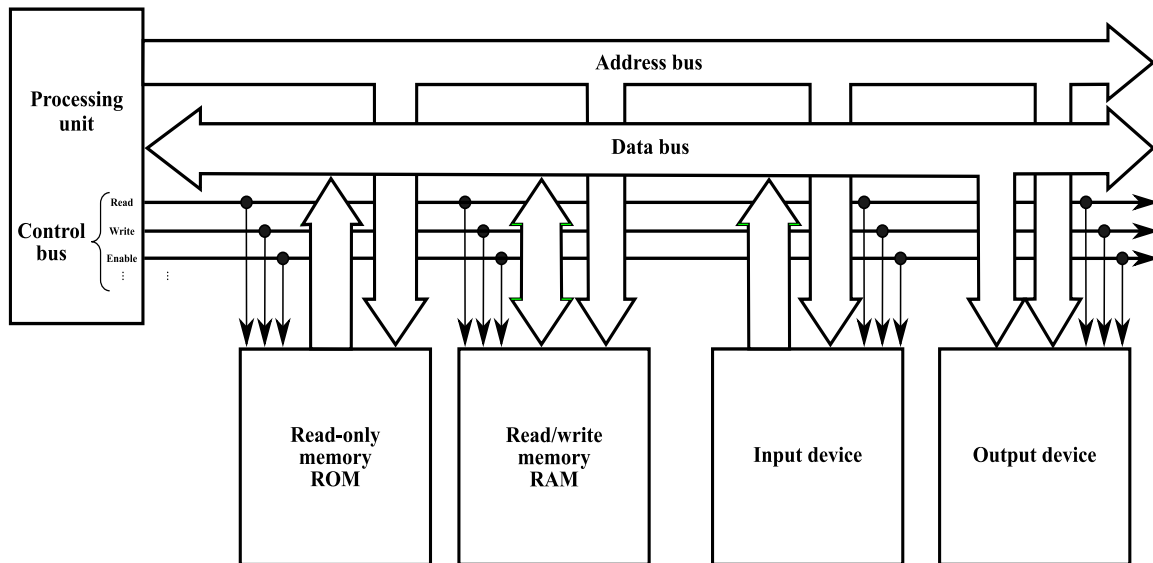


Figure II-4: Schematic diagram for the structure of a modern computing system

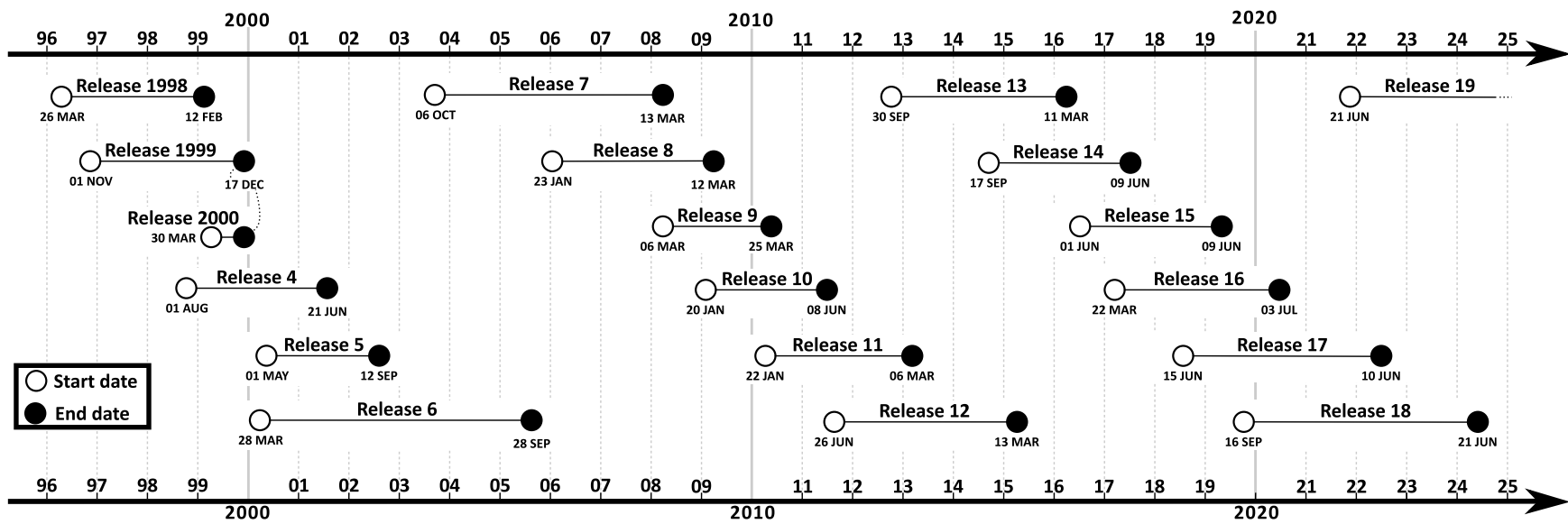
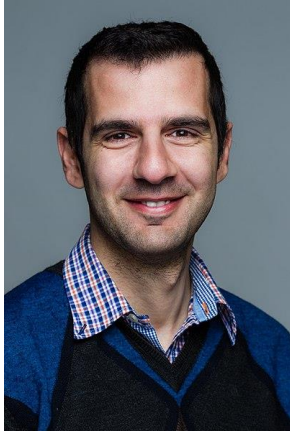


Figure II-5: Timeline of 3GPP releases

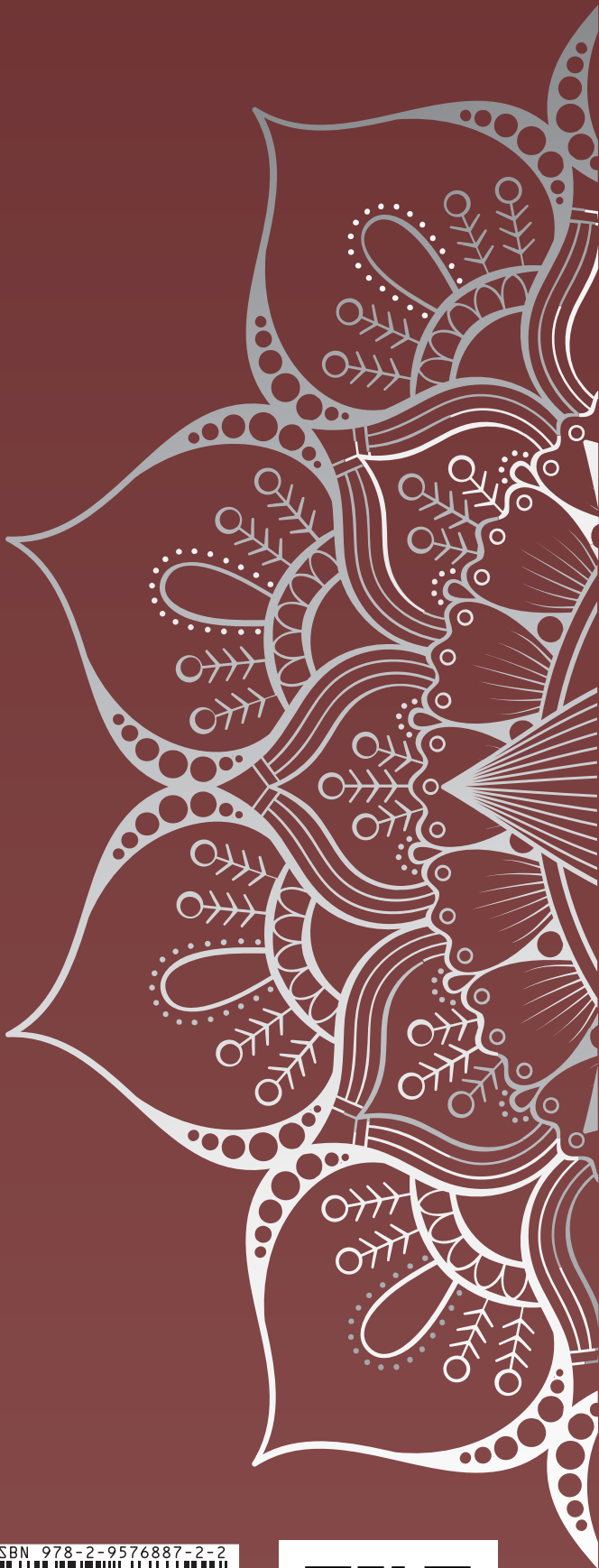
Author Biography



Michel Bakni received the B.S. degree in telecommunication and electronics from Tishreen University, Syria, in 2013 and the M.S. degree from UTBM (French: Université de Technologie de Belfort-Montbéliard), France, in 2017, in mobile and distributed networks. In 2021, He received a Ph.D. degree in electronics from the doctoral school of the University of Bordeaux. His research interests include networking, wireless sensor networks, energy consumption optimization and Internet of Things (IoT).

Author Bibliography

- Fundamentals of Subnetting (2016), hal-02147262.
- The bipolar transistor: The concept and applications (2019), ISBN: 9782957688708, hal-02364351v2.
- Internet Protocol : IPv4 & IPv6 (2022), icn, ISBN:978-2-9576887-1-5, hal-03611066



About this book

This booklet is the second edition of "Huawei HCIA-IoT v. 2.5 Evaluation Questions", it is enhanced based on comments and feedback received from users on the first edition. The booklet is designed to help students and professionals who are preparing for the Huawei HCIA-IoT v. 2.5 certification exam. The booklet includes around 1000 questions in three different categories: True and false, multiple-choice questions with a correct answer, and multiple-choice questions with several correct answers. Additionally, there are two appendixes: one for the abbreviation, enriched with text definitions, and the other for the colored illustrations. Remember always when using this booklet, that it is not an exam dump, but rather a tool to help you prepare for the exam well.

ISBN 978-2-9576887-2-2

