"Please note that these files may not be up to date. However, the questions will help you understand the exam format and typical question patterns."

## Question: 1

Assume that a large enterprise needs to deploy a WLAN to provide wireless access for both employees and guests. However, guest data may pose security threats on the network. Which of the following networking modes is applicable to this scenario?

A. Navi WAC Networking
B. Leader AP networking
C. Mesh networking
D. Fat AP networking

**Answer: A**

Explanation:

Navi WAC networking is a networking mode that uses a WLAN Access Controller (WAC) to manage and control APs. It can provide different authentication and security policies for different user groups, such as employees and guests. Guest data is isolated from the internal network to prevent security threats.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100064352/9aadccc0/navi-wac-networking

## Question: 2

Which of the following methods are used in IPsec to ensure secure transmission of service data on the network through encryption and authentication?

A. The receiver verifies the identity of the sender.
B. The receiver rejects old or duplicate packets in order to prevent attacks initiated by malicious users who resend sniffed packets,
C. The sender verifies the identity of the receiver.
D. Data integrity is verified.

**Answer: AD**

Explanation:

IPsec uses authentication headers (AHs) and encapsulating security payloads (ESPs) to ensure secure transmission of service data on the network. AHs provide authentication and integrity verification for the sender and the receiver, while ESPs provide encryption and optional authentication for the data. Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/ipsec

## Question: 3

Either of the two APs that have established a mesh connection can send a Mesh Peering Close frame to the other AP to tear down the mesh connection.

A. True
B. False

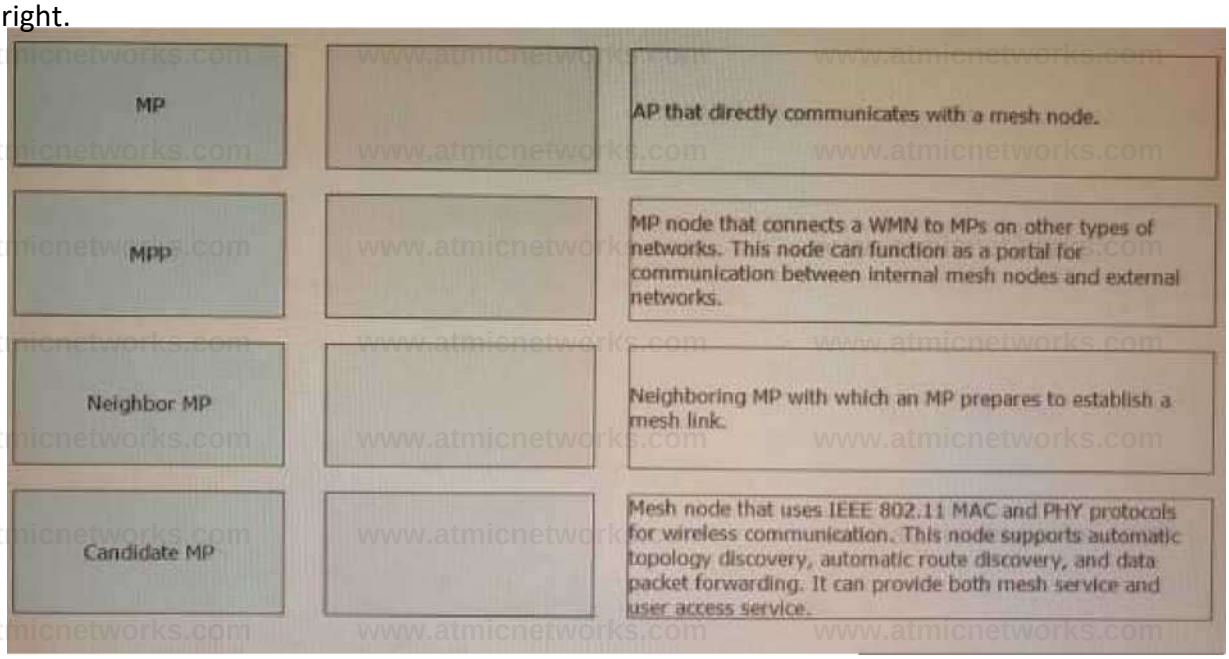
**Answer: A**

Explanation:

A mesh connection can be torn down by either of the two APs that have established it by sending a Mesh Peering Close frame to the other AP. This frame indicates that the sender no longer wants to maintain the mesh connection.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/mesh- networking

## Question: 4

DRAG DROP
In mesh networking, APs have different roles. Drag the AP roles on the left to the role descriptions on the right.




**Answer:**

Explanation:
MP: Mesh node that uses IEEE 802.11 MAC and PHY protocols for wireless communication. This node supports automatic topology discovery, automatic route discovery, and data packet forwarding. It can provide both mesh

service and user access service1.

MPP: MP node that connects a WMN to MPs on other types of networks. This node can function as a portal for communication between internal mesh nodes and external networks1.

Neighbor MP: Neighboring MP with which an MP prepares to establish a mesh link1.

Candidate MP: AP that directly communicates with a mesh node2.

https://support.huawei.com/enterprise/en/doc/EDOC1100064365/90f2391e/configuration- examples-for-mesh 2:

https://support.huawei.com/enterprise/en/doc/EDOC1100169459/8d79210e/configuring-wireless- mesh-networking

## Question: 5

In a VRRP HSB scenario, ifthe VRRP preemption delay is set to a small value, which of the following problems may occur after a master/backup switchover? (Select All that apply)

A. The batch backup process cannot be started.
B. A master/backup switchback is triggered too quickly.
C. Backup information is incomplete.
D. Service data on the master and backup WACs is lost.

**Answer: BC**

Explanation:

According to the Huawei documents and resources, the VRRP preemption delay is the time that an AC waits before preempting another AC with a lower priority. If the VRRP preemption delay is set to a small value, the following problems may occur after a master/backup switchover:

B. A master/backup switchback is triggered too quickly. If the master AC recovers soon after a switchover, it may preempt the backup AC again and become the master AC. This may cause frequent switchovers and affect network stability1.

C. Backup information is incomplete. If the backup AC takes over services from the master AC too quickly, it may not have received all the data synchronized from the master AC through HSB. This may cause service interruption or data loss2.

Therefore, B and C are the correct answers. Reference: 1: https://support.huawei.com/enterprise/en/doc/EDOC1100064368/80fc2ebd/example-for- configuring-vrrp-hsb 2: https://support.huawei.com/enterprise/en/doc/EDOC1100096325/1a753937/vrrp-hsb-configuration

## Question: 6

The display sync-configuration compare command is executed on the backup WAC in HSB to check wireless configuration synchronization. Based on the command output, which of the following statements are true? (Select All that apply)

```
<WAC> display sync-configuration compare
<WAC>— /tmp/master-comm on-cfg.cfg
+++ /tmp/backup-common-cfg.cfg
@@ -214,59 +214,6 @@
  forward-mode tunnel
  service-vlan vlan-Id 102
```

```
    ssid-proflle 2
-  vap-profile name 2
-  forward-mode tunnel
-  service-vlan vlan-id 102
- ssid-profile IR2D
+ vap-profile name 3
+ forward-mode tunnel
+ service-vlan vlan-id 102
+ ssid-profile 3
@@ -287,70 +234,21 @@
```

A. This command is used to check whether the public configurations on two WACs are consistent after wireless configuration synchronization.
B. The configuration of ssid-profile 2 exists on both the master and backup WACs.
C. The configuration of vap-profile name 3 exists on the master WAC but not on the backup WAC.
D. The configuration of vap-profile name 2 exists on the backup WAC but not on the master WAC.

**Answer: AC**

Explanation:

The display sync-configuration compare command is used to check whether the public configurations on two WACs are consistent after wireless configuration synchronization. The command output shows the differences between the configurations on the master and backup WACs. In this case, the configuration of vap-profile name 3 exists on the master WAC but not on the backup WAC.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/display-sync-configuration-compare

## Question: 7

In a dual-link backup scenario, the active/standby link switchover mode is set to priority. When the active link recovers, the AP detects that the original active link has a higher priority and triggers a switchback. How many Echo intervals does the AP wait for before switching back to the original primary WAC?

A. 20
B. 10
C. 15
D. 5

**Answer: C**

Explanation:

In a dual-link backup scenario, when the active link recovers, the AP waits for 15 Echo intervals before switching back to the original primary WAC. This prevents frequent link switchovers caused by unstable links.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/dual-link-

backup

## Question: 8

In a dual-link HSB scenario, after an AP sets up CAPWAP links with the active and standby WACs, which of the following types of packets does the AP periodically send to the WACs to detect link status?

A. DTLS
B. Join
C. Echo
D. Keepalive

**Answer: C**

Explanation:

In a dual-link HSB scenario, after an AP sets up CAPWAP links with the active and standby WACs, the AP periodically sends Echo packets to the WACs to detect link status. The Echo packets are sent every 30 seconds by default.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/dual-link-hsb

## Question: 9

Which of the followings is not a roaming optimization solution?

A. Proactive roaming
B. Smart roaming
C. Fast roaming using PMK caching
D. 802.11r roaming

**Answer: B**

Explanation:

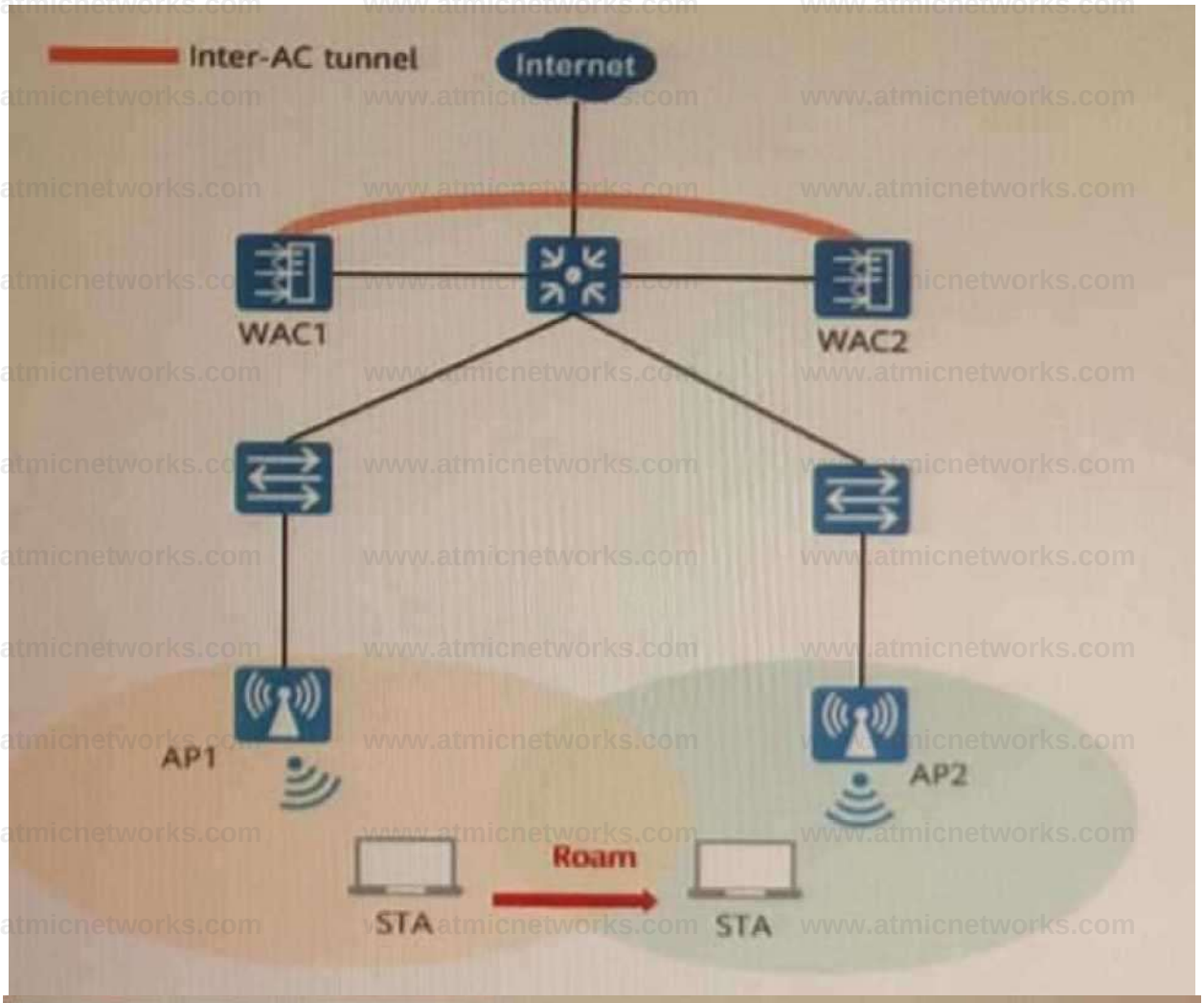
Smart roaming is not a roaming optimization solution, but a feature that allows an AP to automatically adjust its transmit power based on signal strength and interference level. The other

options are all roaming optimization solutions that can reduce roaming latency and packet loss. Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/smart-roaming

## Question: 10

DRAG DROP

802. 11r fast roaming (over-the-air) is enabled on the WLAN shown in the figure. A STA roams from AP1 to AP2. Sort the steps in chronological order during the 802.11r fast roaming process between WACs.




| | | |
|---|---|---|
| The STA initiates an 802.11 FT authentication request to AP2. | | 1 |
| The STA accesses the network through AP1. | | 2 |
| AP2 starts the reassociation timer, and sends an 802.11 FT authentication response to the STA. | | 3 |
| The STA generates and installs a PTK based on the information contained in the response frame. | | 4 |
| The STA sends a reassociation request to AP2. | | 5 |
| AP2 generates and installs a PTK according to PMK-R1 and information contained in the request frame. | | 6 |
| After receiving the reassociation request, AP2 disables the reassociation timer, and then sends a reassociation response to the STA. | | 7 |
| The STA receives the response frame of AP2. The roaming process is complete. | | 8 |

**Answer:**

Explanation:

According to the Huawei documents and resources, the chronological order during the 802.11r fast roaming

process between WACs is as follows:

2. The STA accesses the network through API. This is the initial association process before roaming.

1.The STA initiates an 802.11 FT authentication request to AP2. This is the first step of the roaming process when the STA moves to a new AP.

3. AP2 starts the reassociation timer, and sends an 802.11 FT authentication response to the ST

A. This is the second step of the roaming process when AP2 responds to the STA's request and sets a timer for reassociation.

4. The STA generates and installs a P TK based on the information contained in the response frame. This is the third step of the roaming process when the STA derives a new pairwise key for encryption. 5.The STA sends a reassociation request to AP2. This is the fourth step of the roaming process when the STA requests to reassociate with AP2.

6. AP2 generates and installs a PTK according to PMK-RI and information contained in the request frame. This is the fifth step of the roaming process when AP2 derives the same pairwise key as the STA.

7. After receiving the reassociation request, AP2 disables the reassociation timer, and then sends a reassociation reg onse to the STA. This is the sixth step of the roaming process when AP2 confirms the reassociation with the STA and stops the timer.

8. The STA receives the response frame of AP2. The roaming process is complete. This is the final step of the roaming process when the STA completes the handover to AP2.

Therefore, 2, 1, 3, 4, 5, 6, 7, 8 is the correct answer. Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100169459/8d79210e/configuring-wireless- mesh-networking

## Question: 11

In Huawei's smart roaming solution, which of the following methods can be used by a WAC to discover and maintain neighboring AP entries of STAs? (Select All that Apply)

A. The WAC obtains such entries using 802. 11v.
B. The AP listens to the Probe frames sent by STAs.
C. The AP periodically and proactively scans neighboring APs of STAs.
D. STAs proactively report neighboring AP information.

**Answer: BC**

Explanation:

In Huawei's smart roaming solution, the WAC can discover and maintain neighboring AP entries of STAs by using two methods: passive listening and active scanning. Passive listening means that the AP listens to the Probe frames sent by STAs and reports them to the WAC. Active scanning means that the AP periodically and proactively scans neighboring APs of STAs and reports them to the WAC. Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/smart-roaming

## Question: 12

Which of the following statements about the home agent are true? (Select All that Apply)

A. The home agent communicates with the gateway on the STAs1 home network at Layer 2.
B. The home agent communicates with the gateway on the STAs' home network at Layer 3.
C. A home AP can function as a home agent of STAs.

D. A home WAC can function as a home agent of STAs.

**Answer: BD**

Explanation:

The home agent is a device that communicates with the gateway on the STAs' home network at Layer 3 and maintains the binding entries of STAs' home addresses and care-of addresses. A home WAC can function as a home agent of STAs, while a home AP cannot.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/mobile-ip

## Question: 13

Which of the following types of non-Wi-R devices can be identified by Huawei APs? (Select All that Apply)

A. Bluetooth device
B. ZigBee device
C. Game controller
D. 2.4 GHz wireless video and audio transmitter

**Answer: ABD**

Explanation:

Huawei APs can identify non-Wi-Fi devices that operate in the 2.4 GHz frequency band, such as Bluetooth devices, ZigBee devices, game controllers, wireless video and audio transmitters, microwave ovens, cordless phones, and baby monitors.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/non-wi-fi- device-identification

## Question: 14

Which of the following advantages does BSS coloring provide in Wi-Fi 6? (Select All that Apply)

A. Higher packet rate on the air interface
B. Enhanced encryption on the air interface
C. More efficient channel use
D. Higher concurrency in high-density scenarios

**Answer: ACD**

Explanation:

BSS coloring is a feature introduced in Wi-Fi 6 that assigns different colors to different BSSs to reduce co-channel interference. BSS coloring provides the following advantages:

Higher packet rate on the air interface: BSS coloring reduces collisions between packets from different BSSs on the same channel, improving packet transmission efficiency.

More efficient channel use: BSS coloring allows spatial reuse of channels by different BSSs, increasing channel utilization.

Higher concurrency in high-density scenarios: BSS coloring reduces interference among neighboring APs and improves network performance in high-density scenarios.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/bss-coloring

## Question: 15

An AP may preferentially use the BTM mode to steer some STAs. With which of the following protocols are such STAs compliant?

A. 802.11k
B. 802.11i
C. 802.11r
D. 802.11v

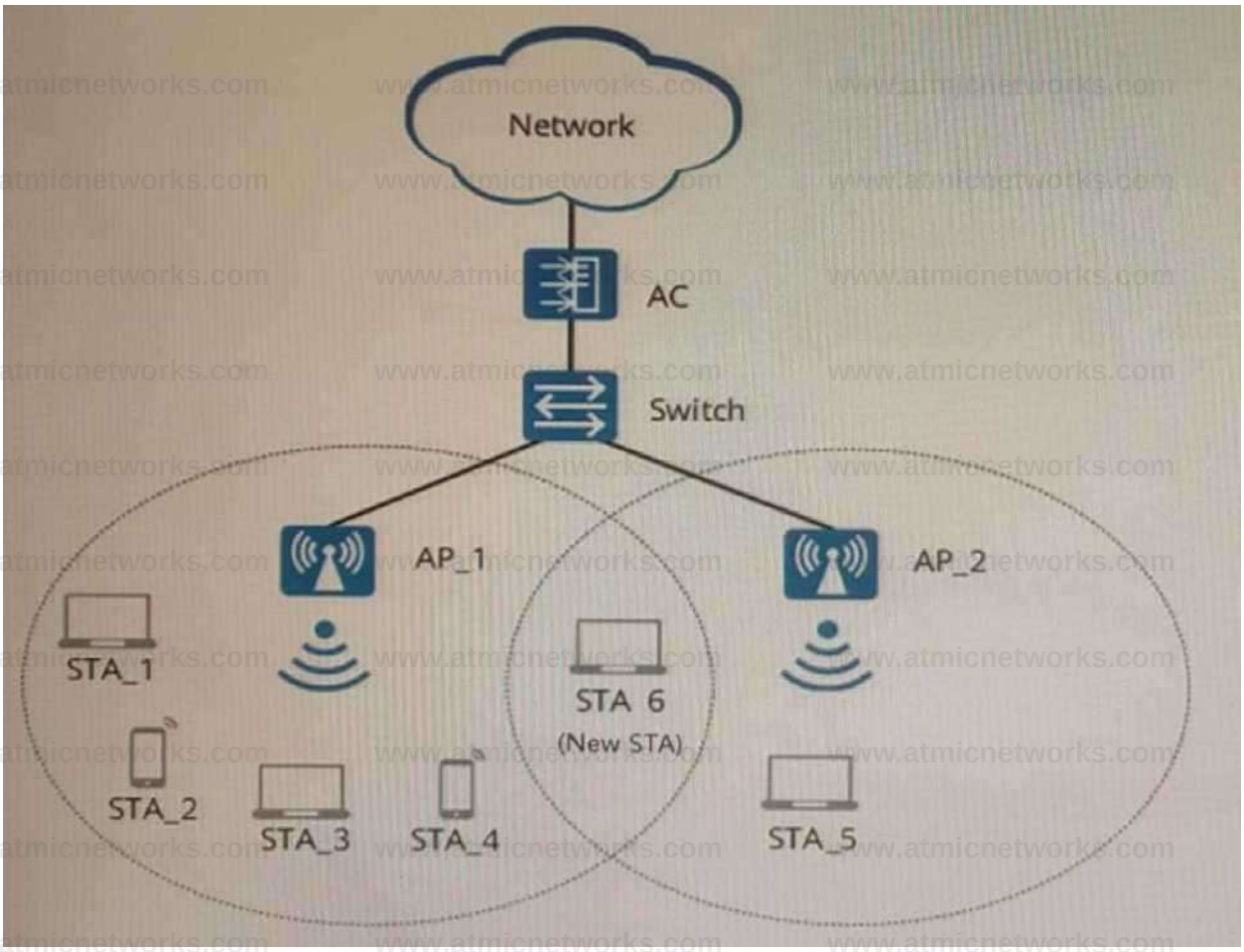
**Answer: D**

Explanation:

An AP may preferentially use the BTM mode to steer some STAs that are compliant with 802.11v protocol. BTM stands for BSS Transition Management, which is a feature defined in 802.11v protocol that allows an AP to send a request to a STA to switch to another BSS.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/btm

## Question: 16

As shown in the figure, STA_1 through STA_4 are associated with AP_1, and STA_5 is associated with AP_2. Assuming that the load balancing threshold is 2, the load difference threshold is 25%, and API and AP2 support a maximum of 10 STAs, which of the following statements are true? (Select All that Apply)




A. The load percentage of AP_1 is 40%, and that of AP_2 is 10%.
B. The load balancing mechanism needs to be enabled. Then some STAs are steered from AP_1 to AP 2.
C. If load balancing is performed, the load percentage of AP_1 changes to 30%.
D. The minimum load percentage is 10%, which is greater than the load difference threshold. Therefore, load balancing needs to be enabled.

**Answer: AB**

Explanation:

The load percentage of an AP is calculated by dividing the number of associated STAs by the maximum number of STAs supported by the AP. In this case, the load percentage of AP_1 is 4/10 = 40%, and that of AP_2 is 1/10 = 10%. The load balancing mechanism needs to be enabled to balance the load between AP_1 and AP_2. Then some STAs are steered from AP_1 to AP_2 based on the load balancing threshold and the load difference threshold.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/load- balancing

## Question: 17

In a multicast solution, there must be reachable unlcast routes between multicast sources and receivers.

A. True
B. False

**Answer: A**

Explanation:

In a multicast solution, there must be reachable unicast routes between multicast sources and receivers, because multicast routing protocols use unicast routing information to build multicast forwarding trees.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/multicast

## Question: 18

After multicast-to-unicast conversion is enabled on an AP's air interface, which of the followings is the destination MAC address of multicast packets sent over the air interface?

A. Multicast MAC address
B. MAC address of the multicast source
C. Broadcast MAC address
D. MAC address of a STA

**Answer: D**

Explanation:

After multicast-to-unicast conversion is enabled on an AP’s air interface, the destination MAC address of multicast packets sent over the air interface is changed to the MAC address of a STA that has joined the multicast group. This improves the transmission efficiency and reliability of multicast packets.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/multicast-to-unicast-conversion

## Question: 19

To enable WPA3-incapable ST As to access a WPA3-conflgured network, the WI-FI Alliance defines the WPA3 transition mode in which WPA3 and WPA2 can coexist for a period of time in the future. This mode applies only to WPA3-Enterprise, not to WPA3-Personal.

A. True
B. False

**Answer: B**

Explanation:

The WPA3 transition mode applies to both WPA3-Enterprise and WPA3-Personal. In this mode, WPA3 and WPA2 can coexist for a period of time in the future to enable WPA3-incapable STAs to access a WPA3-configured network.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/wpa3-transition-mode

## Question: 20

Which of the following statements correctly arranges matching modes used by URL filtering in descending order of priority?

A. Exact matching > Prefix matching > Suffix matching > Keyword matching
B. Exact matching > Suffix matching > Keyword matching > Suffix matching
C. Exact matching > Suffix matching > Prefix matching > Keyword matching
D. Exact matching > Keyword matching > Suffix matching > Prefix matching

**Answer: C**

Explanation:

URL filtering supports four matching modes: exact matching, suffix matching, prefix matching, and keyword matching. The priority order of these modes is as follows:
Exact matching: The highest priority. An exact match means that a URL entered by a user is exactly the same as a URL in a blacklist or whitelist.
Suffix matching: The second highest priority. A suffix match means that a URL entered by a user ends with a suffix in a blacklist or whitelist.
Prefix matching: The third highest priority. A prefix match means that a URL entered by a user starts with a prefix in a blacklist or whitelist.
Keyword matching: The lowest priority. A keyword match means that a URL entered by a user contains a keyword in a blacklist or whitelist.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/url-filtering

## Question: 21

WPA3 has the following advantages over WPA and WPA2: supports WPA3-SAE, provides a more secure handshake protocol, enhances the algorithm strength, and supports Suite A cryptography.

A. True
B. False

**Answer: A**

Explanation:

WPA3 has the following advantages over WPA and WPA2:
Supports WPA3-SAE, which provides more secure authentication and key management than PSK.
Provides a more secure handshake protocol than 802.11i, which can resist offline dictionary attacks and protect forward secrecy.
Enhances the algorithm strength from AES-128 to AES-192 or AES-256.
Supports Suite A cryptography, which provides higher security levels for government or military networks.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/wpa3

## Question: 22

Which of the following statements about attack defense is true?

A. Defense against flood attacks can be used to defend against Ping of Death attacks.

B. Attack defense allows APs to analyze the contents and behaviors of incoming packets on ports to determine whether packets have attack characteristics. The APs then take defense measures on the packets that have attack characteristics.

C. Attack defense can defend against spoofing packet attacks, malformed packet attacks, fragmentation attacks, and flood attacks.

D. Fragmentation attack defense enables a device to detect packet fragments in real time and discard or rate-limit them to protect the device.

**Answer: B**

Explanation:

Attack defense is a feature that allows APs to analyze the contents and behaviors of incoming packets on ports to determine whether packets have attack characteristics. The APs then take defense measures on the packets that have attack characteristics, such as discarding them or limiting their rate. Attack defense can defend against spoofing packet attacks, malformed packet attacks, fragmentation attacks, and flood attacks.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/attack-defense

## Question: 23

In 802. IX authentication using port-based access control, once a user is authenticated successfully on a port, subsequent users on this port can access the network without authentication. When the authenticated user goes offline, all other users are denied access to the network.

A. True

B. False

**Answer: A**

Explanation:

According to the Huawei documents and resources, 802.1X authentication using port-based access control is a method that allows only one user to access the network through a port at a time. If a user is authenticated successfully on a port, subsequent users on this port can access the network without authentication. When the authenticated user goes offline, all other users are denied access to the network1. Therefore, A is the correct answer. Reference: 1: https://support.huawei.com/enterprise/en/doc/EDOC1100086527

## Question: 24

Which of the following are typical 802. IX authentication modes? (Select All that apply)

A. EAP termination

B. EAP relay

C. EAP-TLS

D. EAP-MD5

**Answer: AB**

Explanation:

According to the Huawei documents and resources, EAP termination and EAP relay are typical 802.1X authentication modes between the access device and authentication server. In EAP termination mode, the access device terminates EAP packets and encapsulates them into RADIUS packets. In EAP relay mode, the access device directly encapsulates the received EAP packets into RADIUS using EAP over RADIUS (EAPoR) packets2. Therefore, A and B are the correct answers. Reference: 2: https://support.huawei.com/enterprise/en/doc/EDOC1100086527

## Question: 25

Huawei Agile Cloud Authentication (HACA) supports only IMaster NCE-Campus as the HACA server.

A. True
8. False

**Answer: B**

Explanation:

According to the Huawei documents and resources, Huawei Agile Cloud Authentication (HACA) supports iMaster NCE-Campus as well as Agile Controller-Campus as the HACA server. HACA is an authentication method that allows users to access a network without entering user names or passwords3. Therefore, B is the correct answer. Reference: 3: https://support.huawei.com/enterprise/en/doc/EDOC1100086527

## Question: 26

Which of the following statements about EAP relay and EAP termination are false? (Select All that apply)

A. In EAP termination mode, an access device encapsulates EAP packets sent by an 802. IX client Into RADIUS packets, without processing the data in the EAP packets.
B. In EAP relay mode, an access device extracts information from EAP packets, encapsulates the information into RADIUS packets, and sends the RADIUS packets to an authentication server.

C. In EAP termination mode, an access device extracts client authentication information from the EAP packets sent by a client and encapsulates the information using the standard RADIUS protocol. The access device supports only the EAP MD5-Challenge authentication method.
D. The EAP termination mode simplifies the processing on an access device and supports various authentication methods. However, this mode requires an authentication server to support EAP and have high processing capability.

**Answer: AD**

Explanation:

A. In EAP termination mode, an access device encapsulates EAP packets sent by an 802. IX client Into RADIUS packets, without processing the data in the EAP packets. This statement is false because in EAP termination mode, an access device extracts information from EAP packets, encapsulates the information into RADIUS packets, and sends the RADIUS packets to an authentication server2.

D. The EAP termination mode simplifies the processing on an access device and supports various authentication methods. However, this mode requires an authentication server to support EAP and have high processing capability.

This statement is false because it describes the EAP relay mode, not the EAP termination mode2.

Therefore, A and D are the correct answers. Reference: 2: https://support.huawei.com/enterprise/en/doc/EDOC1100086527

## Question: 27

Which of the following encapsulation formats are used for EAP termination in 802.1X authentication? (Select All that apply)

A. EAP-TLS
B. EAPoL
C. EAPoR
D. EAP

**Answer: BC**

Explanation:

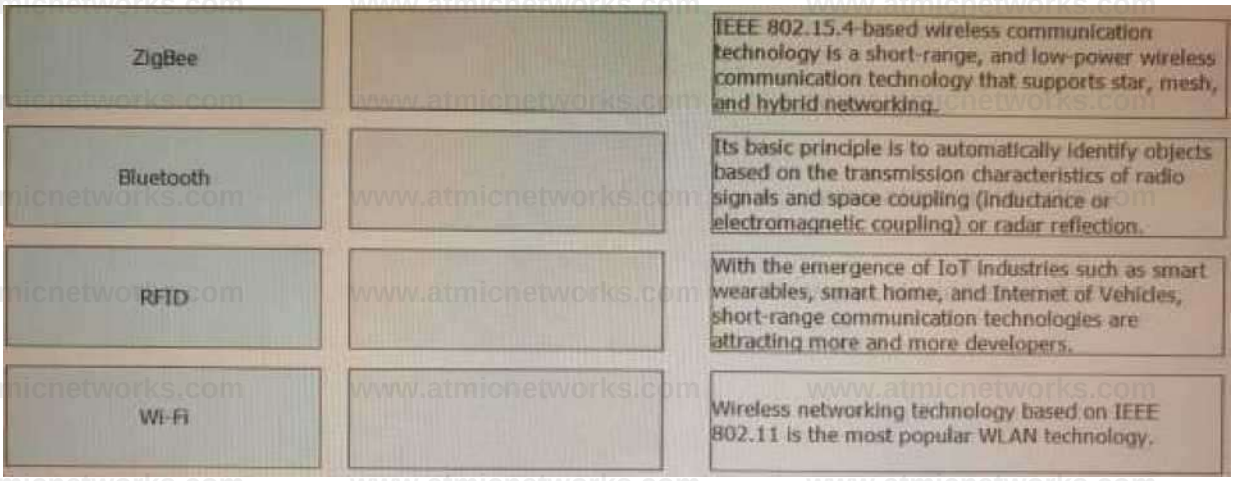
According to the Huawei documents and resources, the encapsulation formats used for EAP termination in 802.1X authentication are as follows:

B. EAPoL: The client and access device exchange information using EAPoL packets across the LAN2.
C. EAPoR: The access device directly encapsulates the received EAP packets into RADIUS using EAP over RADIUS (EAPoR) packets2.

Therefore, B and C are the correct answers. Reference: 2: https://support.huawei.com/enterprise/en/doc/EDOC1100086527

## Question: 28

DRAG DROP
Drag the short-range wireless IoT technologies on the left to their corresponding descriptions on the right.




**Answer:**

Explanation:

According to the Huawei documents and resources, the definitions of the short-range wireless IoT technologies are as follows:

ZigBee: IEEE 802.15.4-based wireless communication technology is a short-range, and low-power wireless communication technology that supports star, mesh, and hybrid networking.

Bluetooth: With the emergence of IoT industries such as smart wearables, smart home, and Internet of Vehicles, short-range communication technologies are attracting more and more developers.

REID: Its basic principle is to automatically identify objects based on the transmission characteristics of radio signals and space coupling (inductance or electromagnetic coupling) or radar reflection.

Wi-Fi: Wireless networking technology based on IEEE 802.11 is the most popular WLAN technology.

Therefore, ZigBee - 1, Bluetooth - 3, REID - 2, Wi-Fi - 4 is the correct answer. Reference: :

https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/zigbee :

https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/bluetooth :

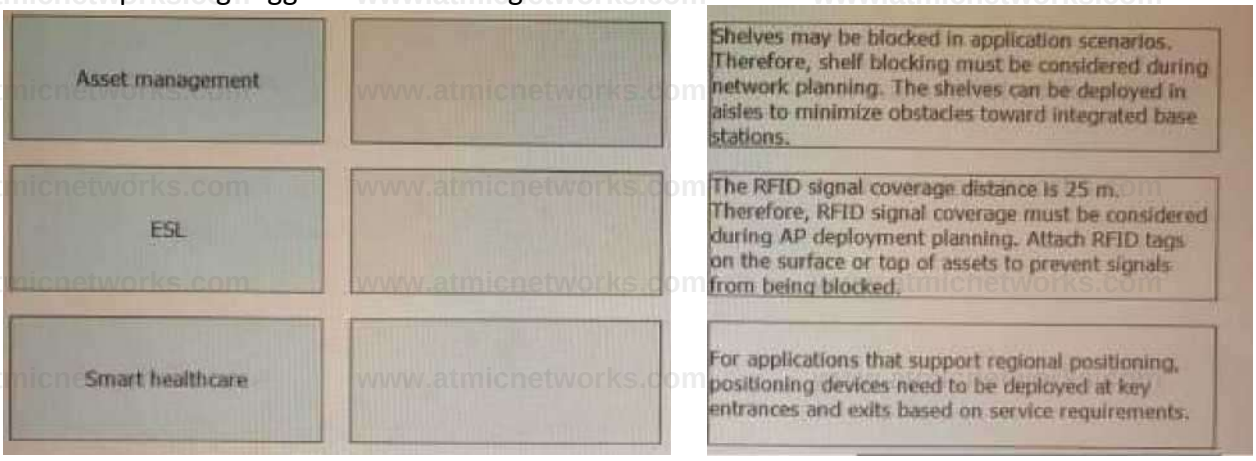
https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/rfid :

https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/wi-fi

## Question: 29

DRAG DROP

Differentiated network planning needs to be performed to meet requirements of different IoT services in Huawei's CloudCampus IoT solutions. Drag the solutions on the left to their corresponding network planning suggestions on the right.




**Answer:**

Explanation:

According to the Huawei documents and resources, the network planning suggestions for the solutions are as follows:

Asset management: The RFID signal coverage distance is 25 m. Therefore, RFID signal coverage must be considered during AP deployment planning. Attach RFID tags on the surface or top of assets to prevent signals from being blocked.

ESL: Shelves may be blocked in application scenarios. Therefore, shelf blocking must be considered during network planning. The shelves can be deployed in aisles to minimize obstacles toward integrated base stations.

Smart healthcare: For applications that support regional positioning, positioning devices need to be deployed at key entrances and exits based on service requirements.

Therefore, Asset management - 2, ESL - 1, Smart healthcare - 3 is the correct answer. Reference: : https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/asset-management : https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/esl : https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/smart-healthcare

## Question: 30

Which of the following components is not included In a typical RFID system?

A. Information processing platform
B. RFID tag
C. Router
D. RFID reader

**Answer: C**

Explanation:

A router is not included in a typical RFID system. A typical RFID system consists of three components: RFID tag, RFID reader, and information processing platform. The RFID tag is attached to the object to be identified, the RFID reader communicates with the tag and reads its information, and the information processing platform processes and stores the data collected by the reader.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/rfid

## Question: 31

DRAG DROP

Drag the Huawei's wireless positioning solutions on the left to their corresponding features and application scenarios on the right.


Runs based on the built In Bluetooth module of an AP, which can be Implemented on either the network side or terminal side

W1 R terminal positioning

Provides high positioning accuracy, and Is applicable to scenarios that require high accuracy, such as intelligent manufacturing, warehousing logistics, and mechanical manufacturing.

performs network-side positioning generally based on the RSS1, tout provides low positioning accuracy This method applies to (scenarios such as precision marketing and customer flow analysis in shopping malls.

Runs based on the built in Bluetooth module of an AP. The AP reports data to a positioning engine for location resolution. This positioning technology provides low positioning accuracy and applies to asset positioning and personnel positioning scenarios

**Answer:**

Explanation:

According to the Huawei documents and resources, the features and application scenarios of the wireless positioning solutions are as follows:

Wi-Fi terminal positioning: Performs network-side positioning generally based on the RSSI, but provides low positioning accuracy. This method applies to scenarios such as precision marketing and customer flow analysis in shopping malls.

Bluetooth tag positioning: Runs based on the built-in Bluetooth module of an AP. The AP reports data to a positioning engine for location resolution. This positioning technology provides low positioning accuracy and applies to asset positioning and personnel positioning scenarios.

UWB positioning: Provides high positioning accuracy, and is applicable to scenarios that require high accuracy, such as intelligent manufacturing, warehousing logistics, and mechanical manufacturing. Bluetooth terminal positioning: Runs based on the built-in Bluetooth module of an AP, which can be implemented on either the network side or terminal side.

Therefore, Wi-Fi terminal positioning - 3, Bluetooth tag positioning - 4, UWB positioning - 2, Bluetooth terminal positioning - 1 is the correct answer. Reference: :

https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/wi-fi-terminal- positioning :

https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/bluetooth-tag- positioning :

https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/uwb- positioning :

https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/bluetooth-terminal- positioning

## Question: 32

Satellite positioning can achieve high positioning accuracy in both indoor and outdoor scenarios.

A. True
B. False

**Answer: B**

Explanation:

Satellite positioning can achieve high positioning accuracy in outdoor scenarios, but not in indoor scenarios. This is because satellite signals are easily blocked or interfered by buildings, walls, ceilings, and other obstacles in indoor environments.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/satellite- positioning

## Question: 33

Which of the following statements about fingerprint-based positioning technology are true? (Select All that Apply)

A. The positioning engine generates a virtual fingerprint library through calculations based on the AP deployment and environment information.
B. Terminals learn from each other to form a fingerprint library that can be shared.
C. APs collect surrounding environment information to form a fingerprint library.
D. The fingerprint map is obtained through onsite information collection.

**Answer: AD**

Explanation:

Fingerprint-based positioning technology is a method that uses the signal strength or phase difference of wireless signals to locate objects. There are two types of fingerprint-based positioning technology: virtual fingerprint-based positioning and real fingerprint-based positioning. In virtual fingerprint-based positioning, the positioning engine generates a virtual fingerprint library through calculations based on the AP deployment and environment information. In real fingerprint-based positioning, the fingerprint map is obtained through onsite information collection.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/fingerprint-based-positioning-technology

## Question: 34

Which of the followings is an IPv6 multicast address?

A. 2222::11
B. FF02::18C
C. FE80:: A
D. FC00::1

**Answer: B**

Explanation:

FF02::18C is an IPv6 multicast address. An IPv6 multicast address starts with FF and identifies a group of interfaces that belong to the same multicast group. The other options are not IPv6 multicast addresses. 2222::11 is an IPv6 unicast address, FE80::A is an IPv6 link-local address, and FC00::1 is an IPv6 unique local address.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/ipv6-multicast-addresses

## Question: 35

Which of the following parameters can be allocated to clients In DHCPv6 stateful autoconflguratlon? (Select All that Apply)

A. IPv6 address

B. PD prefix
C. SNTP server address
D. DNS server address

**Answer: ABD**

Explanation:

In DHCPv6 stateful autoconfiguration, a client obtains an IPv6 address, a PD prefix (if required), and other configuration parameters (such as DNS server address) from a DHCPv6 server.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/dhcpv6-stateful-autoconfiguration

## Question: 36

Which of the fallowings is not an IPv6 address type?

A. Multicast address
B. Unicast address
C. Broadcast address
D. Anycast address

**Answer: C**

Explanation:

Broadcast address is not an IPv6 address type. IPv6 does not support broadcast addressing, but uses multicast addressing instead. The other options are valid IPv6 address types. Unicast address identifies a single interface, multicast address identifies a group of interfaces, and anycast address identifies multiple interfaces but delivers packets to only one of them.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/ipv6-address-types

## Question: 37

When a STA roams from API to AP2 at Layer 2, AP2 notifies its neighbors of from this STA is encapsulated in a tunnel and sent to API for forwarding.

A. True
B. False

**Answer: B**

Explanation:

When a STA roams from AP1 to AP2 at Layer 2, AP2 notifies its neighbors of the MAC address learned from this STA. The MAC address is not encapsulated in a tunnel and sent to AP1 for forwarding. Instead, AP1 deletes the MAC address entry of the STA and releases the IP address lease.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/layer-2-roaming

## Question: 38

Which of the following statements about the access layer design are true when Huawei's CloudCampus Solution is applied to small and midsize campus networks? (Select All that Apply)

A. In the mini-store scenario, APs and egress devices must be deployed if Wi-Fi coverage is required. APs cannot directly connect to egress links and do not support NAT.

B. When selecting a switch, ensure that the following condition is met; Number of connected APs x AP power ^ Power provided by the PoE switch. Therefore, select PoE switches with a proper power supply based on the AP model and quantity.

C. Select appropriate models of access switches based on whether PoE support is required and how many APs need to access the network.

D. For relatively large networks in midsize shopping malls, supermarkets, and primary/secondary education campuses, it is recommended that stack networking be used at the access layer. If a single device can provide sufficient access capacity for downstream terminals, single-device networking can be used at the access layer. If the upstream devices of access-layer devices are stacked, it is recommended that Eth-Trunks be used to connect to such upstream devices. If more APs need to be deployed, use the PoE switch to increase the number of APs to be connected.

**Answer: BC**

Explanation:

A is false because in the mini-store scenario, APs can directly connect to egress links and support NAT if Wi-Fi coverage is required. There is no need to deploy egress devices separately.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/access-layer-design

## Question: 39

Which of the following key factors is used by the CloudCampus cloud management platform to determine the tenant to which a device belongs?

A. Device ESN
B. Device IP address
C. Device MAC address
D. Device model

**Answer: A**

Explanation:

The device ESN (Electronic Serial Number) is a unique identifier that is used by the CloudCampus cloud management platform to determine the tenant to which a device belongs. The device ESN is bound to a tenant when a device is added to the platform.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/device-esn

## Question: 40

On a campus network, which of the following problems may occur when you manually create a static VXLAN tunnel? (Select All that Apply)

A. Although the static VXLAN tunnel mode supports the distributed gateway scenario, the configuration involves a heavy workload and is complex to adjust.
B. A static VXLAN tunnel uses related protocols on the control plane, consuming device resources.
C. If N devices need to establish VXLAN tunnels, you need to manually configure the ingress replication list up to N x (N-l)/2 times.
D. Remote MAC addresses can be learned only through data flooding.

**Answer: AC**

Explanation:

B is false because a static VXLAN tunnel does not use any protocols on the control plane, saving device resources.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/static-vxlan- tunnel

## Question: 41

Which of the following user access authentication modes are supported In Huawel's CloudCampus Solution? (Select All that Apply)

A. 802. IX authentication
B. MAC address authentication
C. Portal authentication

**Answer: ABC**

Explanation:

Huawei's CloudCampus Solution supports three user access authentication modes: 802.1X authentication, MAC address authentication, and Portal authentication.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/user-access-authentication-modes

## Question: 42

Which of the following statements about VXLAN is false?

A. A Layer 2 VXLAN gateway forwards traffic to a VXLAN network and can also be used for Intrasubnet communication on the same VXLAN network.
B. Layer 2 and Layer 3 VXLAN gateways must maintain VBDIF interfaces. Otherwise, users cannot communicate with each other through these interfaces.
C. A VBDIF interface is a logical interface created based on a BD. It is similar to a VLANIF interface on a traditional network.
D. A Layer 3 VXLAN gateway is used for inter-subnet communication on a VXLAN network and communication with external non-VXLAN networks.

**Answer: B**

Explanation:

B is false because only Layer 3 VXLAN gateways need to maintain VBDIF interfaces for inter-subnet communication on a VXLAN network or communication with external non-VXLAN networks. Layer 2 VXLAN gateways do not need VBDIF interfaces.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/vxlan-gateway

## Question: 43

Master NCE-CampusInsight analyzes network issues during correlation analysis of poor-QoE clients, including coverage, interference throughput, and hardware issues.

A. True

B. False

**Answer: A**

Explanation:

iMaster NCE-CampusInsight analyzes network issues during correlation analysis of poor-QoE clients, including coverage, interference, throughput, and hardware issues. It also provides suggestions for network optimization based on the analysis results.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/correlation-analysis-of-poor-qoe-clients

## Question: 44

Which of the following statements are true about data collection of IMaster NCE-CampusInslght? (Select All that Apply)

A. iMaster NCE-CampusInsight uses telemetry to Implement efficient data collection.

B. Calculated data can be displayed on iMaster NCE-CampusInsight only after a license Is loaded on the device management page.

C. To collect data from WLAN devices, ensure that WACs can communicate with the southbound IP address of iMaster NCE-CampusInsight. APs do not need to communicate with the southbound IP address of iMaster NCE-CampusInsight.

D. The UTC time of iMaster NCE-CampusInsight must be the same as that of its managed devices.

**Answer: AC**

Explanation:

B is false because calculated data can be displayed on iMaster NCE-CampusInsight without loading a license on the device management page. The license only affects the number of devices that can be managed by iMaster NCE-CampusInsight.

D is false because the UTC time of iMaster NCE-CampusInsight does not need to be the same as that of its managed

devices. However, it is recommended that they use the same time zone to avoid confusion.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/data-collection

## Question: 45

With protocol trace, iMaster NCE-CampusInsight displays protocol-level Interaction details at the phases for wireless users. (Enter the acronyms in capital letters.)

**Answer: AP, WAC, and AC**

Explanation:

With protocol trace, iMaster NCE-CampusInsight displays protocol-level interaction details at the AP, WAC, and AC phases for wireless users.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/protocol-trace

## Question: 46

Which of the following may be the reason why no data Is displayed on the telemetry management page of IMaster NCE-CampusInsight? (Select All that Apply)

A. The network connecting devices and iMaster NCE-CampusInsight Is faulty.
B. Telemetry data reporting is not configured on devices according to the configuration guide.
C. No license file is imported.
D. Devices are not added to iMaster NCE-CampusInsight.
E. The UTC time of devices is inconsistent with that of iMaster NCE-CampusInsight.

**Answer: ABD**

Explanation:

C is false because the license file only affects the number of devices that can be managed by iMaster NCE-CampusInsight, not the data display.

E is false because the UTC time of devices does not need to be consistent with that of iMaster NCE-CampusInsight.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/data-display

## Question: 47

iMaster NCE-CampusInsight provides Intelligent radio calibration for high-load APs to increase the frequency bandwidth. This function applies to both 5 GHz and 2.4 GHz frequency bands.

A. True
B. False

**Answer: B**

Explanation:

iMaster NCE-CampusInsight provides intelligent radio calibration for high-load APs to increase the frequency bandwidth. However, this function applies only to the 5 GHz frequency band, not to the 2.4 GHz frequency band.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/intelligent- radio-calibration

## Question: 48

Master NCE-CampusInsight can comprehensively record and analyze Interference. Which of the following parameters are recorded? (Select All that Apply)

A. Recommended channels
B. Interference fulfillment rate
C. Interference strength
D. Number of interference SSIDs
E. Air interface congestion fulfillment rate

**Answer: ACD**

Explanation:

B and E are not parameters recorded by iMaster NCE-CampusInsight for interference analysis. The other options are parameters recorded by iMaster NCE-CampusInsight to comprehensively record and analyze interference.
Reference:
https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/interference-analysis

## Question: 49

To which of the following scenarios is radio calibration applicable?

A. Enterprise office scenario
B. Rail transportation scenario
C. High-density scenario
D. WDS or mesh backhaul scenario

**Answer: C**

Explanation:

Radio calibration is applicable to high-density scenarios where a large number of users access the network simultaneously and require high bandwidth, such as stadiums, exhibition halls, and conference centers. Radio calibration can improve user experience by increasing the frequency bandwidth for high-load APs.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/radio- calibration

## Question: 50

Which of the following tools are commonly used for WLAN network planning, acceptance, or health evaluation? (Select All that Apply)

A. WLAN Planner
B. iMaster NCE-CampusInsight
C. eDesk
D. CloudCampus APP

**Answer: ABD**

Explanation:

C is not a tool commonly used for WLAN network planning, acceptance, or health evaluation. eDesk is a tool for remote fault diagnosis and rectification on WLAN networks.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/wlan-planner https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/imaster-nce-campusinsight
https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/cloudcampus-app

## Question: 51

iMaster NCE-CampusInsight comprehensively analyzes WLAN client access, displays success rates and time consumption of association, ---------- , and DHCP. It also provides issue analysis and optimization suggestions. (Enter lowercase letters.)

**Answer: authentication**

Explanation:

iMaster NCE-CampusInsight comprehensively analyzes WLAN client access, displays success rates and time consumption of association, authentication, and DHCP. It also provides issue analysis and optimization suggestions.
Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/client- access-analysis

## Question: 52

Which of the following items is not involved in the HLD phase?

A. Capacity planning
B. Network design
C. AP position planning
D. Deployment planning

**Answer: C**

Explanation:

According to the Huawei documents and resources, the HLD phase is the high-level design phase of a WLAN project. It involves the following items:

Capacity planning: Determines the number and types of devices required for the WLAN network based on the customer's requirements and network scale.

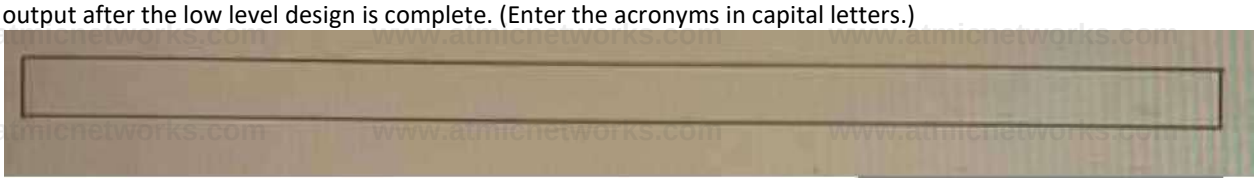
Network design: Designs the network topology, IP addressing scheme, VLAN division, security policies, and other network parameters for the WLAN network.

Deployment planning: Plans the deployment sequence, schedule, resources, and risks for the WLAN project.

AP position planning is not involved in the HLD phase. It is part of the LLD phase, which is the low- level design phase of a WLAN project. It involves the detailed design of AP positions, antenna types, channel allocation, power adjustment, and other wireless parameters for the WLAN network. Therefore, C is the correct answer. Reference: : https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/wlan-project-design

## Question: 53

During a project lifecycle, the document needs to be output after the high level design be output after the low level design is complete. (Enter the acronyms in capital letters.)



**Answer: ATP**

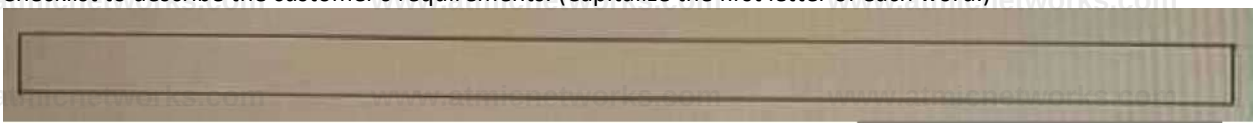
Explanation:

ATP stands for Acceptance Test Plan, which is a document that needs to be output after the low level design is complete. The ATP describes the acceptance criteria and test cases for the project.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/atp

## Question: 54

In the early phase of a project, after the project requirements are clarified, the project owner should Checklist to describe the customer's requirements. (Capitalize the first letter of each word.)



**Answer: Customer Requirement Specification**

Explanation:

Customer Requirement Specification (CRS) is a document that needs to be output after the project requirements are clarified. The CRS describes the customer's requirements in detail and serves as the basis for subsequent project design and delivery.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/crs

## Question: 55

Which of the following statements are true about the WLAN site survey In different typical scenarios? (Select All that Apply)

A. In a classroom scenario. If the walls are made of reinforced concrete, the signal attenuation Is high. In this case, you are advised to test the attenuation during the site survey. Additionally, pay attention to the locations of ELV

rooms in the teaching building.

B. In an office scenario, the load-bearing columns and partitions affect the signal coverage. If an integrated ceiling is used, deploy APs near maintenance entrances. If a metal ceiling is used, mount APs on the ceiling or wall.

C. In a ward-round scenario, high requirements are posed on the coverage field strength, roaming effect, and bandwidth. Determine the interference of medical equipment and the areas where Wi-Fi signals are not allowed.

D. In a stadium scenario, the onsite environment is complex and cabling is difficult. Therefore, confirm with the property management company about ELV rooms and cabling. If the transmission distance is too long, consider deploying more switches. During the survey, focus on the interference between APs and AP mounting modes.

**Answer: ABCD**

Explanation:

Only: All statements are true about the WLAN site survey in different typical scenarios.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/wlan-site- survey

## Question: 56

When calculating the number of APs, you can divide the total required bandwidth by the maximum bandwidth of a single AP.

A. True

B. False

**Answer: B**

Explanation:

When calculating the number of APs, you cannot simply divide the total required bandwidth by the maximum bandwidth of a single AP. You also need to consider other factors such as signal coverage area, user density, interference level, and application type.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/calculation- of-the-number-of-aps

## Question: 57

Which of the following statements about WLAN roaming and signal strength Is false?

A. Smart roaming can be enabled on the WAC to help ST As roam and associate with APs with better signals.

B. Generally, a STA roams when it detects that the signal strength is less than -75 dBm.

C. STAs can roam between WACs in dual-link HSB mode.

D. In most cases, the signal strength of a STA should range from -45 dBm to -65 dBm.

**Answer: B**

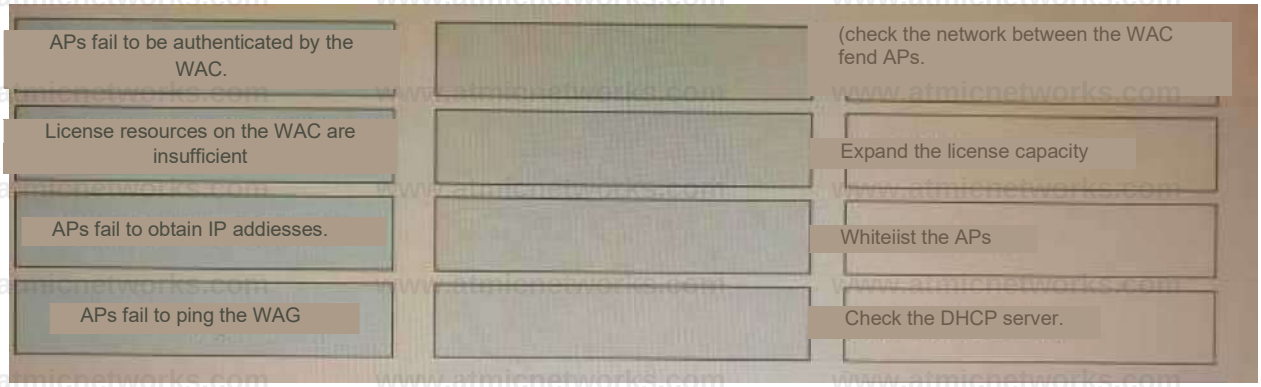
Explanation:

B is false because generally, a STA roams when it detects that the signal strength is less than -70 dBm or -65 dBm, not -75 dBm.

Reference: https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/wlan-roaming-and-signal-strength

## Question: 58

DRAG DROP
Drag the reasons for AP onboarding failures on the left to the corresponding troubleshooting operations on the right.




## Answer:

Explanation:
According to the Huawei documents and resources, the troubleshooting operations for the AP onboarding failures are as follows:
APS fail to be authenticated by the WAC: Whitelist the APS. The WAC can authenticate APs based on

their MAC addresses or SNs. If an AP is not whitelisted on the WAC, it cannot be authenticated and onboarded.
License resources on the WAC are insufficient: Expand the license capacity. The WAC can manage a limited number of APs based on its license. If the license resources are insufficient, some APs cannot be onboarded.
APS fail to obtain IP addresses: Check the DHCP server. The APs need to obtain IP addresses from a DHCP server before they can communicate with the WAC. If the DHCP server is not configured or reachable, the APs cannot obtain IP addresses and onboard.
APS fail to ping the WAC: Check the network between the WAC and APS. The APs need to ping the WAC to discover its IP address and establish a CAPWAP tunnel. If there is a network problem between the WAC and APs, such as incorrect VLAN configuration or firewall blocking, the APs cannot ping the WAC and onboard.
Therefore, APS fail to be authenticated by the WAC - c, License resources on the WAC are insufficient - b, APS fail to obtain IP addresses - d, APS fail to ping the WAC - a is the correct answer. Reference: : https://support.huawei.com/enterprise/en/doc/EDOC1100158948/9a0d5c37/ap-onboarding- failures

## Question: 59

After the HTTP domain name is entered in a browser, the user Is not redirected to the Portal URL.
Which of the followings is the possible cause for this failure? (Select All that Apply)

A. The DNS server IP address is not added to the authentication-free rule.
B. The URL template is incorrectly configured.
C. HTTPS redirection is disabled.
D. The web server is incorrectly configured.

**Answer: ABD**

Explanation:

C is false because HTTPS redirection is not required for Portal authentication to work properly.

Reference:
https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/troubleshooting-portal-authentication-failures

## Question: 60

Which of the following configurations may cause ST As to experience a slow Internet connection? (Select All that Apply)

A. QoS CAR is configured in the traffic profile.
B. Radio 1 of APs is disabled.
C. TKIP encryption is configured, causing a low link setup rate.
D. Rate limiting is configured in the SSID profile.

**Answer: ACD**

Explanation:
B is false because disabling radio 1 of APs does not affect the Internet connection speed of STAs that use radio 2.
Reference:
https://support.huawei.com/enterprise/en/doc/EDOC1100058940/8a8f1c9b/troubleshooting-slow- internet-connection