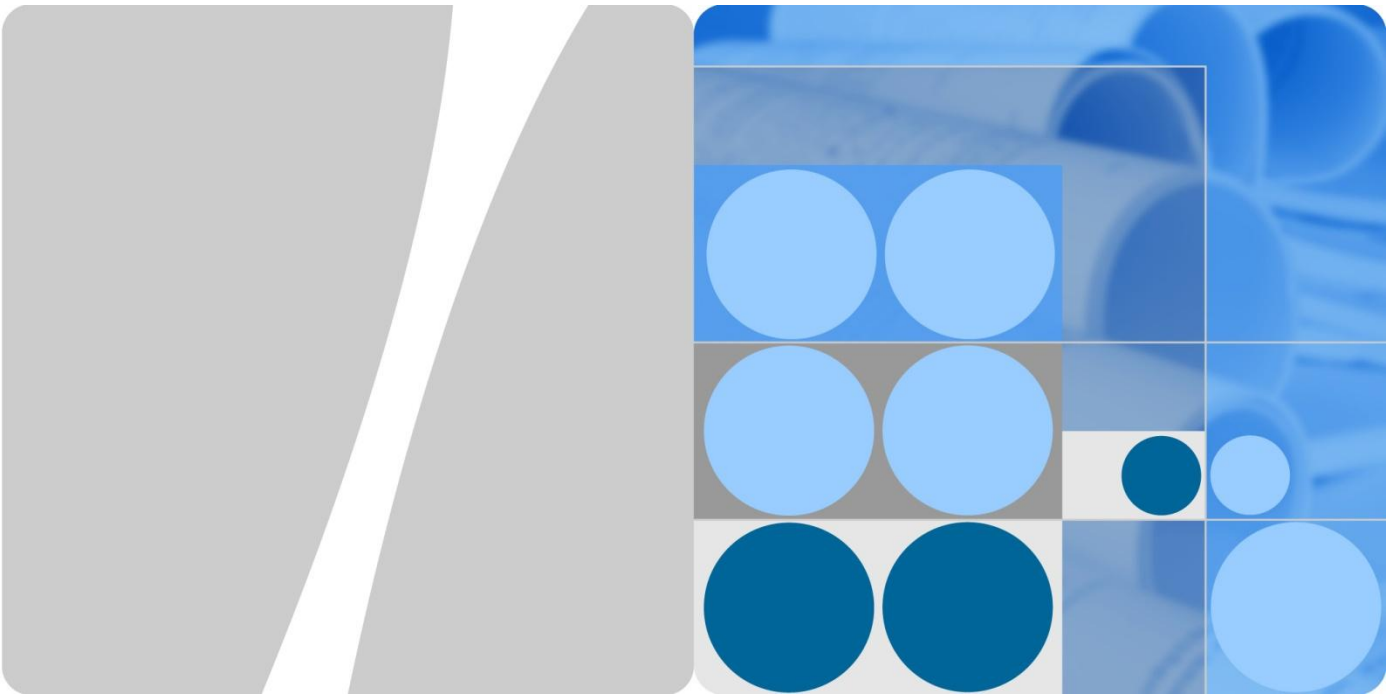


WLAN Inter-AC Roaming Technology White Paper

Issue 1.0

Date 2014-04-23

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions


and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://www.huawei.com

Email: support@huawei.com

Tel: 0755-28560000 4008302118

Fax: 0755-28560111

About This Document

Keywords

WLAN, AC, roaming

Abstract

WLAN roaming technology ensures that users can move freely within the WLAN signal coverage, services are not interrupted, and user experience is not affected. Users roam between different AP coverage areas. In the AP/AC infrastructure WLAN structure, two APs before and after roaming may be managed by different ACs as the wireless network scale becomes larger. Therefore, inter-AC roaming is required.

Abbreviations

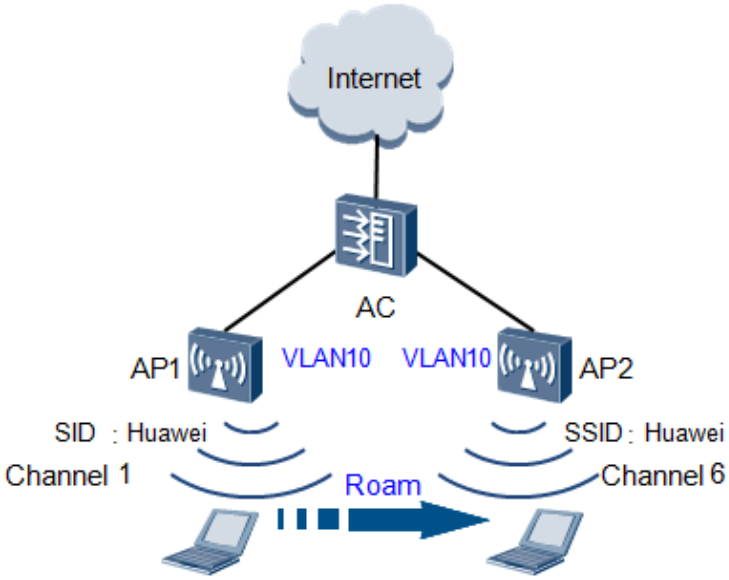
Abbreviation	Full Name
STA	Station
AP	Access point
SSID	Service set identifier
BSSID	Basic service set identifier
CAPWAP	Control and provisioning of wireless access points

Contents

1 Background

WLAN roaming allows a STA to move from an AP to another AP in the same ESS on a WLAN network with nonstop service transmission. As shown in Figure 1-1, a STA is first connected to AP1, moves from the signal coverage area of AP1 to that of AP2, and then is connected to AP2. During this process, the STA IP address remains unchanged and services are not interrupted. This is called roaming.

Figure 1-1 WLAN roaming process



In the roaming process, user services are not interrupted. If the STA disconnects from AP1 and gets online on AP2 after a certain period, services of the STA are interrupted. This process is not a roaming process.Nonstop

service transmission is ideal. Actually, a small number of packets are lost during roaming in the following scenarios:

- The signal is weak or coverage hole exists in the signal overlapping area of two APs.
- The STA needs to switch scan channels to discover a new AP.
- The STA needs to switch the connection relationship between the original and new APs.
- The STA needs to perform key negotiation or be reauthenticated after connecting to a new AP.

WLAN roaming ensures uninterrupted service experience and prevents service delay by reducing packet loss during roaming. The following paragraphs describe measures taken to minimize packet loss.

WLAN roaming allows only user movement within the same ESS. If a STA is first associated with the SSID Huawei and then with another SSID, the STA is not roaming because the STA requires re-association and re-authentication, and needs to obtain an IP address again. In this process, STA service transmission is interrupted.

On a small network, all APs are managed by one AC. When users are roaming between APs, the status information of all STAs is managed by the same AC. Inter-AP roaming does not require synchronization between AC devices in advance, which is easy to implement. However, multiple ACs are deployed on a large network. STA status information needs to be synchronized between ACs in advance or queried in real time. Smooth inter-AC roaming must be implemented to ensure normal STA traffic forwarding after roaming. In this way, a wider range of wireless overage can be provided and customer requirements be met.

2 Technology Implementation

2.1 Basic Concepts

2.1.1 Home and Foreign

- HAC: home AC, indicating the AC that a STA is associated with the first time.
- HAP: home AP, indicating the AP that a STA is associated with the first time.
- FAC: foreign AC, indicates the current AC that a STA is associated with after roaming.
- FAP: foreign AP, indicates the current AP that a STA is associated with after roaming.

A user may roam multiple times consecutively. The HAC and HAP are fixed, but the FAC and FAP change with each roaming.

2.1.2 Intra-AC Roaming and Inter-AC Roaming

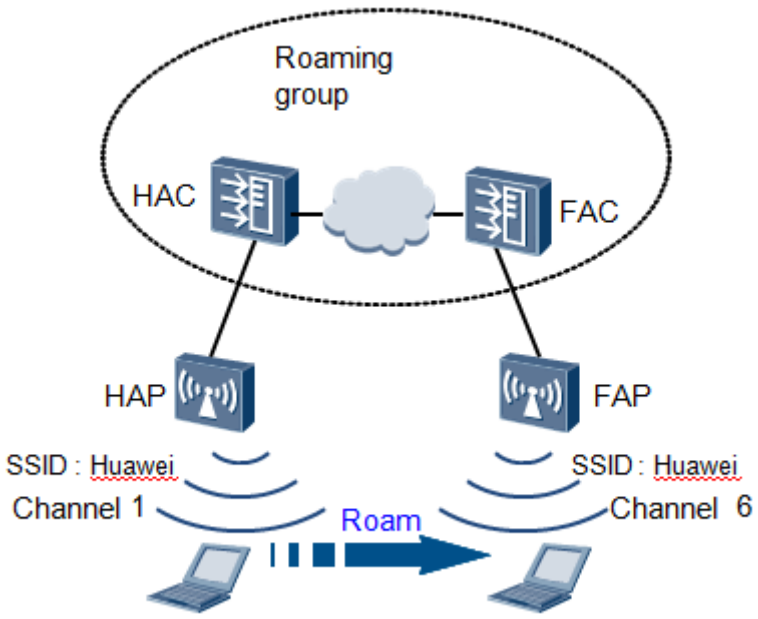
- Intra-AC roaming

  If the HAC and FAC during roaming are the same AC, it is an intra-AC roaming.

- Inter-AC roaming

  If the HAC and FAC during roaming are not the same AC, it is an inter-AC roaming. That is, the APs associated with the STA before and after the roaming are managed by different ACs, as shown in Figure 2-1.

Figure 2-1 Inter-AC roaming



On some large-scale WLAN networks, there are a large number of APs and therefore it is impossible to use one AC to manage all the APs. Usually, multiple ACs manage these APs. Inter-AC roaming must be supported to ensure that users can roam freely between any APs. In this scenario, the APs associated with the STA before and after the roaming are managed by different ACs.

Intra-AC roaming can be regarded as a special case of inter-AC roaming, in which the HAC and FAC are the same AC.

- Home agent

  A home agent can implement Layer 2 communication with the gateway of a user's home network. To ensure that the user can still access the home network after roaming, user traffic needs to be forwarded through a tunnel to the home agent, and then transmitted by the home agent. One end of the tunnel is the FAP, and the other is the home agent. The home agent functions as a transit station. Currently, the HAP or HAC works as the home agent.

- Tunnel between ACs

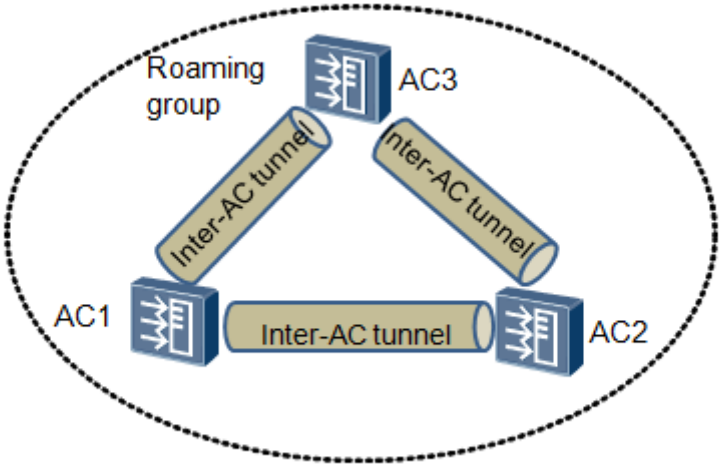
  To support inter-AC roaming, some user information needs to be exchanged between ACs, and user traffic also needs to be forwarded. Therefore, a tunnel is set up between the ACs to manage packets and forward data.

  The tunnel is created using the CAPWAP protocol, and is the same as an AP-AC CAPWAP link.

- Roaming group

Obviously, inter-AC roaming cannot be supported between any two ACs on the network. After an AC group is created manually, the ACs belong to the same group can support inter-AC roaming. This group is called roaming group, as shown in Figure 2-2. An AC tunnel is set up between every two ACs in the same roaming group, forming a full-mesh connection.

Figure 2-2 Roaming group



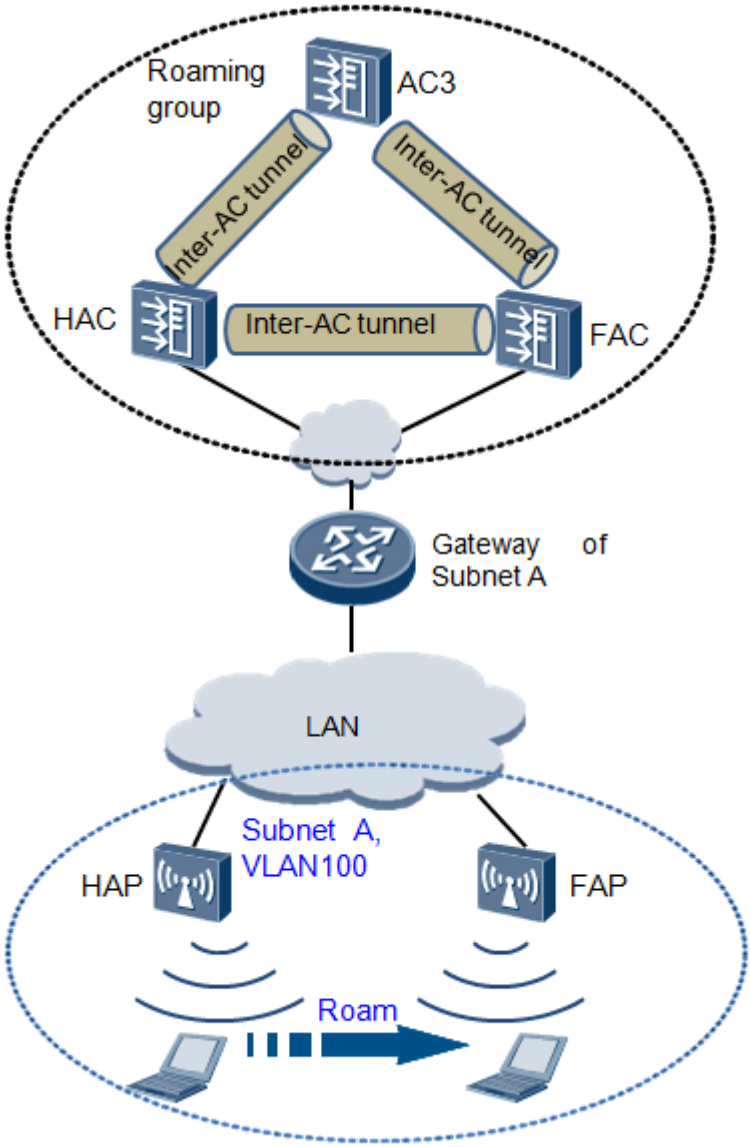
Note: All the AC in the same roaming group share home AC information of current online users.

2.1.3 Layer 2 Roaming and Layer 3 Roaming

- Layer 2 roaming

  In Layer 2 roaming, a STA roams within the same subnet. For example, the APs associated with the STA before and after roaming belong to service VLAN 100.

Figure 2-3 Layer 2 roaming

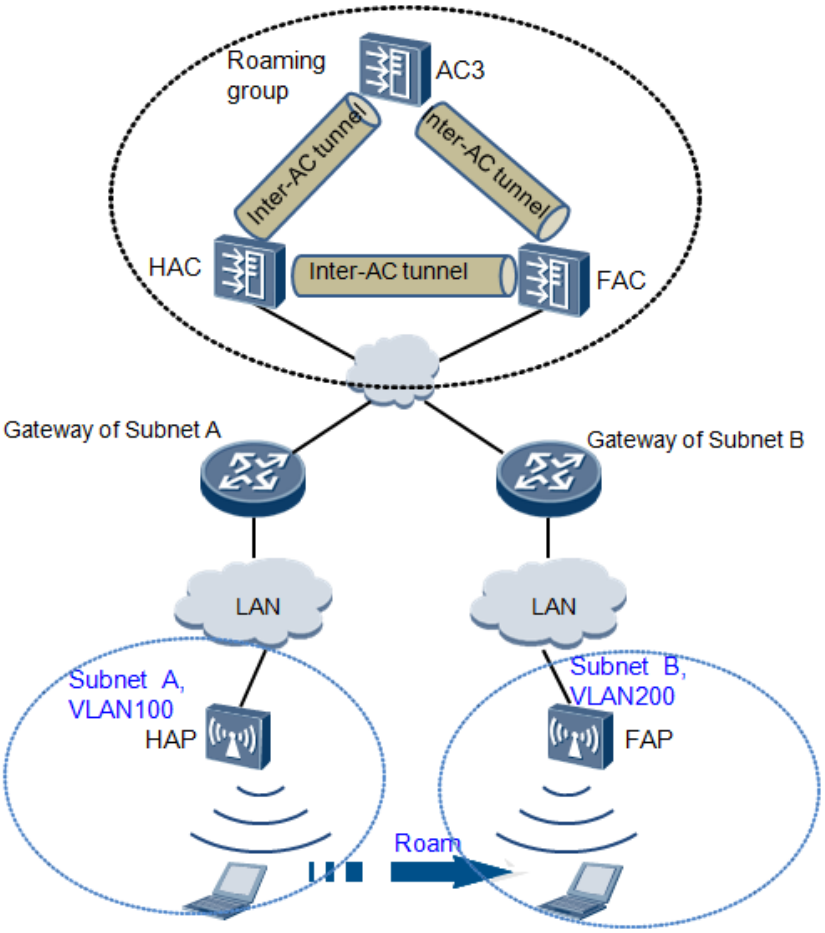


Note: In actual network planning, two APs in the same subnet cannot be managed by different ACs, and therefore Layer 2 roaming across ACs is impossible. However, after the AC pool feature is introduced, the two APs in the same subnet may be managed by different ACs due to the different online time. The AP that goes online later may connect to another AC because of some special reasons.

- Layer 3 roaming

  In Layer 3 roaming, a STA roams in different subnets. For example, the AP associated with the STA before roaming belongs to service VLAN 100 and network segment 100.1.1.X; the AP associated with the STA after roaming belongs to service VLAN 200 and network segment 200.1.1.X.

Figure 2-4 Layer 3 roaming



2.1.4 Fast Roaming and Non-Fast Roaming

- Fast roaming

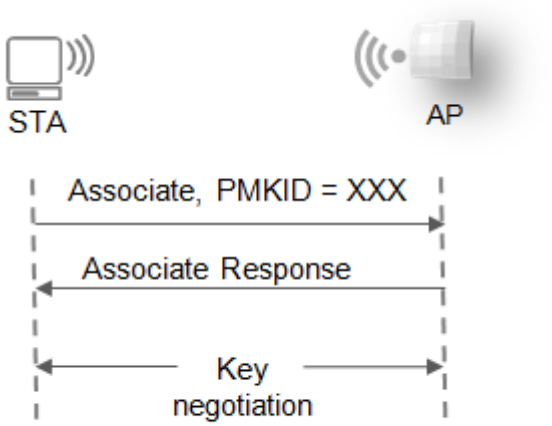
  When a STA is associated with a new AP and performs 802.1x re-authentication, packets may be lost during roaming. The authentication takes a long time, during which services are interrupted. To prevent long-time 802.1x authentication during each roaming, the PMKs obtained by the STA in the previous roaming processes can be saved on the AC. When the association/re-association request is received from the STA, the PMKs saved on the AC are used to match the PMKID carried in the request. If they match each other, the user can go online without authentication. This technology is called opportunistic key caching (OKC).

The preceding roaming mode is called fast roaming, which does not require authentication and significantly reduces the service interruption time (from more than 300 ms to less than 100 ms) during roaming.

The fast roaming process is as follows:

1. The AC saves the PMKs obtained by the STA in the previous several authentication processes.
2. The STA sends the (Re)-Associate request containing the PMKID.
3. After receiving the (Re)-Associate request, the AC compares the PMKID with the saved PMKs. As long as one PMK can match the PMKID, 802.1X authentication is skipped and the AC uses the PMK to negotiate with the STA.

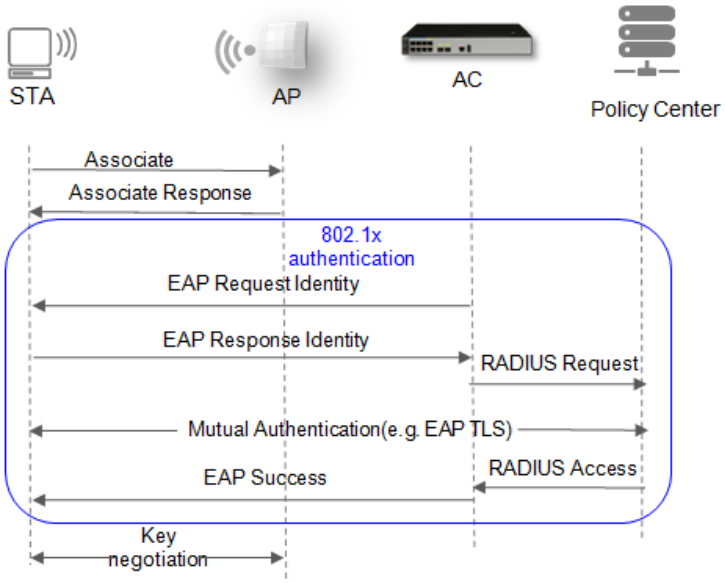
Figure 2-5 Fast roaming process



- Non-fast roaming

  Compared with the fast roaming process, 802.1x authentication is used in the non-fast roaming process, as shown in Figure 2-6.

Figure 2-6 Non-fast roaming process

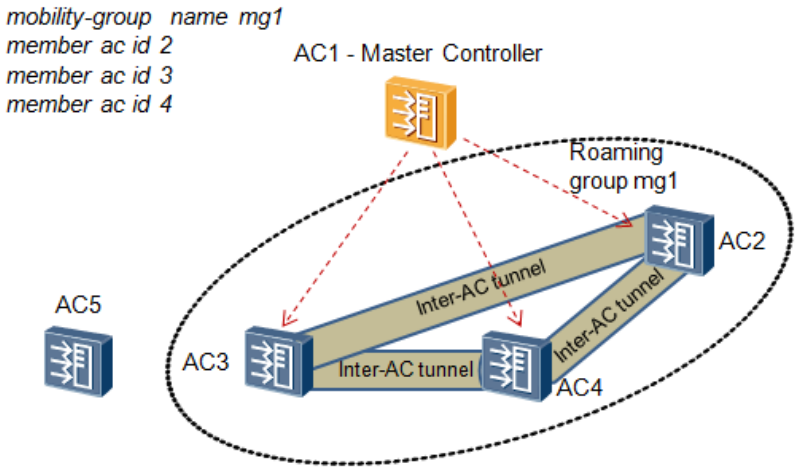


2.2 Configuration Roadmap

By default, intra-AC roaming and fast roaming can be supported without any additional configuration.

To support inter-AC roaming, configure a roaming group. As roaming group configuration involves multiple ACs, the centralized configuration solution is used to simplify the configuration: Select an AC as the Master Controller from multiple ACs, configure a roaming group on the Master Controller, and add member ACs to the roaming group. Deliver the configuration information of the roaming group and its members to each AC.

Figure 2-7 Roaming group configuration



Note:

- The Master Controller is specified for each member AC using the **master-controller {ip ipv4-address | ipv6 ipv6-address}** command.
- Configure the mapping between AC IDs and AC IP addresses on the Master Controller.

Create a roaming group on the Master Controller, and add member ACs. Deliver the roaming group configuration to each member AC. After receiving the configuration, the member ACs in the group automatically set up tunnels with each other to exchange user information and forward user traffic during user roaming.

- Each AC must specify one Master Controller. The Master Controller has the Master Controller role enabled and ACs manually added and managed.
- The Master Controller manages the ACs similarly as an AC manages APs. The Master Controller is also delivered to each managed AC through CAPWAP signaling that is transmitted using CAPWAP control tunnels.
- Master Controller is a logical role, which can be taken over by any AC. An AC functioning as the Master Controller can join a roaming group or not. If the AC functioning as the Master Controller needs to be added to a roaming group, the AC must be added to the roaming group by the Master Controller. As shown in the preceding figure, the **member ac id 1** command is used to add AC1 to the roaming group **mg1**.

Currently, the Master Controller only supports centralized roaming group configuration. Other configurations such as AP and radio configurations still need to be performed on each AC.

2.3 Information Synchronization and Roaming Judgment Between ACs

2.3.1 STA Information Synchronization Between ACs

When a user goes online, the AC associated with the user is queried to obtain user data.

Each AC must save online status of all users on all ACs in the same roaming group, so that a user's current AC can be quickly confirmed. The online state of a user is a bitmap (each AC corresponds to a bit), which records the ACs through which the user goes online.

STA Connection and Disconnection Notification

To ensure that each AC can obtain users' online status in real time, ACs in a roaming group need to be instructed to update online status when users in this group get online or offline, and ACs join or leave the roaming group.

- Connection notification

After a user is connected to an AC, the AC sends a user online notification message to other ACs in the same group. Other ACs receive the message and then set the bit corresponding to the connected AC to 1 in the online status bitmap.

- Disconnection notification

After a user is disconnected from an AC and the AC determines to permanently delete the user data, the AC sends a user offline notification message to other ACs in the same group. After receiving the message, other ACs set the bit corresponding to the connected AC to 0 in the online status bitmap. If the user is offline on all the ACs, the user status information is deleted.

AC Roaming Group Change

- An AC member is added to a roaming group.
- When a new AC joins a roaming group or an AC changes from fault state to normal state, other ACs synchronize the user's online status to the new AC at a time.
  - When an AC joins a roaming group, other ACs in the same group notify the new AC of the current online user status in batches.
  - When the CAPWAP link between two ACs is recovered, the ACs notify each other of the current online user status in batches.
- An AC member is deleted from a roaming group.
  - An AC leaves a roaming group.

    The user online status is deleted in batches when an AC leaves a roaming group.

    Other ACs set the bit corresponding to the leaving AC to 0 in the online status bitmap of all users. In addition, the ACs log out the

users who have roamed from the leaving AC over Layer 3 and reconnect to the users.

The leaving AC sets the bits corresponding to other ACs to 0 in the user online status bitmap, log out the users who have roamed from other ACs over Layer 3, and reconnect to the users.

- The tunnel between ACs is Down.

  The user online status flag of the peer AC is cleared, and the users who have roamed from the peer AC over are forced offline and go online again.

- A roaming group is deleted.

  Each AC in the roaming group is forced to leave the roaming group.

AP Connection and Disconnection

When an AP goes online, STA connection is not involved; therefore, no special processing is required. However, when an AP goes offline, all the STAs associated with the AP are forced offline. At the same time, other ACs in the roaming group are notified of the disconnections. VAP is another virtual logical entity of an AP, which is set by an administrator. Once a VAP is deleted, all users associated with the VAP are forced offline. The STA synchronization action is the same as that of AP disconnection.

- When the users associated with an AP or VAP go offline, other ACs are instructed to clear the user online status flag.

  Each HAC records the HVAP of users who perform Layer 3 roaming from the HVAP. If the HAP or HVAP is deleted, a notification message about Layer 3 roaming user disconnection is sent to other ACs. The message contains the BSSID of the deleted HVAP and the MAC addresses of these users. After receiving the message, other ACs determine that these users roamed from the specified HVAP over Layer 3 and force the users offline. The users then reconnect to ACs. (Note: It seems that the users for which the roaming tunnel is terminated only at ACs should not be forced offline. However, the ACs cannot determine whether the roaming tunnel for the user is still terminated at the ACs after the AP/VAP is deleted. Therefore, these users are also forced offline.)

- ACs reset user online status for APs, and the tunnels between APs and ACs are Down.

  When the users associated with an AP go offline, other ACs are instructed to clear the user online status flag.

  The forwarding entries of the users who perform Layer 3 roaming from the AP and for whom the tunnel is connected to the AP are deleted.

  A notification message about the AP-AC tunnel Down event is sent to other ACs. The message contains the BSSIDs of all current VAPs on the AP. After receiving the message, other ACs check local online user entries and forces these users offline. The users then reconnect to ACs.

Other Configuration Modification

- Modifying VAP VLAN configuration

A notification message for modifying VAP VLAN configuration is sent to other ACs. The message contains the VAP BSSID and new VLAN configuration. After receiving the message, other ACs check entries of local online users who perform Layer 3 roaming from the VAP. If the VLAN configuration has been modified, other ACs force these users offline and the users reconnect to ACs.

- Modifying the VAP forwarding mode

  A notification message for modifying the VAP forwarding mode is sent to other ACs. The message contains the VAP BSSID. After receiving the message, other ACs check entries of local online users who perform Layer 3 roaming from the VAP and force these users offline. The users then reconnect to ACs.

- Modifying the VAP home agent

  If the local forwarding mode is configured for the VAP, a notification message for modifying the VAP home agent is sent to other ACs. The message contains the VAP BSSID. After receiving the message, other ACs check entries of local online users who perform Layer 3 roaming from the VAP and force these users offline. The users then reconnect to ACs.

Information Synchronization Reliability

The system uses timeout retransmission and periodical synchronization to improve reliability of user information synchronization between ACs.

- As messages between ACs may be lost, user information synchronization may fail. This may result in problems such as inconsistency of user data on two ACs and user entry leakage. Therefore, transmission acknowledgement and timeout retransmission mechanisms are used in information synchronization between ACs.
- Each AC periodically synchronizes the list of current local online users to other ACs. A 10s timer is started on each AC, which scans the online user table and synchronizes 400 users at an interval. The remaining online users are synchronized in the next interval. If an AC supports a maximum of 32000 users, it takes about 15 minutes to complete the synchronization.

2.3.2 Roaming Judgment and Connection Process

After receiving an association/reassociation request, an AC regards it as a roaming request to process as long as the user entry already exists. The process is as follows:

1. Each AC saves a bitmap for each STA to record the ACs through which the STA goes online. Each AC corresponds to one bit in the bitmap. Normally, the STA goes online only through one AC. When data synchronization is abnormal, multiple ACs may be recorded.
2. After receiving a STA's association/reassociation request, the AC checks whether the STA already exists in the roaming group. If so, the AC considers that the STA is roaming; if no, the AC considers STA online. A STA can send a request to:

- All ACs
- AC to which the STA is connected
- AC to which the STA is connected and AC with the current AP address configured

  If the STA sends a request to all ACs, a lot of messages may be transmitted in the network. If the STA sends a request to the connected AC and AC with the current AP address configured, the AP MAC address needs to be synchronized between ACs. This is more complex and not cost-effective (only slightly reduces the possibility of mistakenly considering roaming as online). It is recommended that the STA should send a request to the connected AC. The AC checks the online AC bitmap in the local STA entries, and sends a message to all current online ACs to synchronize user data.

3. After the requested AC/HAC receives the data synchronization request, it checks whether the STA has gone online through the AC/HAC. If the STA uses the fast roaming method, the AC/HAC checks whether the PMKID/BKID is matched. If so, the AC/HAC obtains and sends user data to the requesting AC. (Note: BKID is a field in WAPI authentication, which is similar to PMKID.
4. If the requesting AC does not receive any correct response after the request times out, the AC considers that the STA is online. As long as the AC receives one correct response, it considers that the STA is roaming.
5. If the AC considers that the STA is roaming but receives a reassociation request or an association request containing the Current AP Address field, the AC instructs the AP to forge the current AP address to force the STA offline.

2.4 Traffic Forwarding Model

2.4.1 Layer 2 Roaming

A STA is still in the original subnet after Layer 2 roaming, so the FAP/FAC traffic forwarding for Layer 2 roaming users is the same as that for a common new online user. The user traffic is directly forwarded on the local FAP/FAC network, and does not need to be forwarded by the tunnel to the home agent.

Figure 2-8 Traffic forwarding in the case of Layer 2 roaming + local forwarding

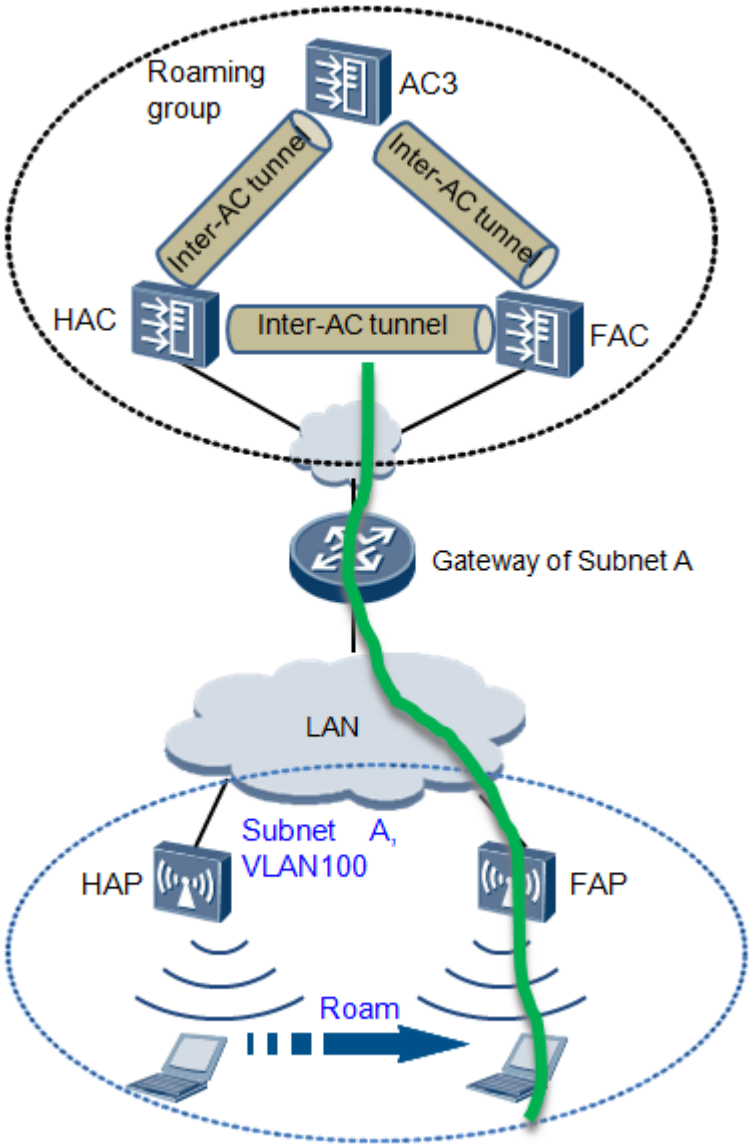
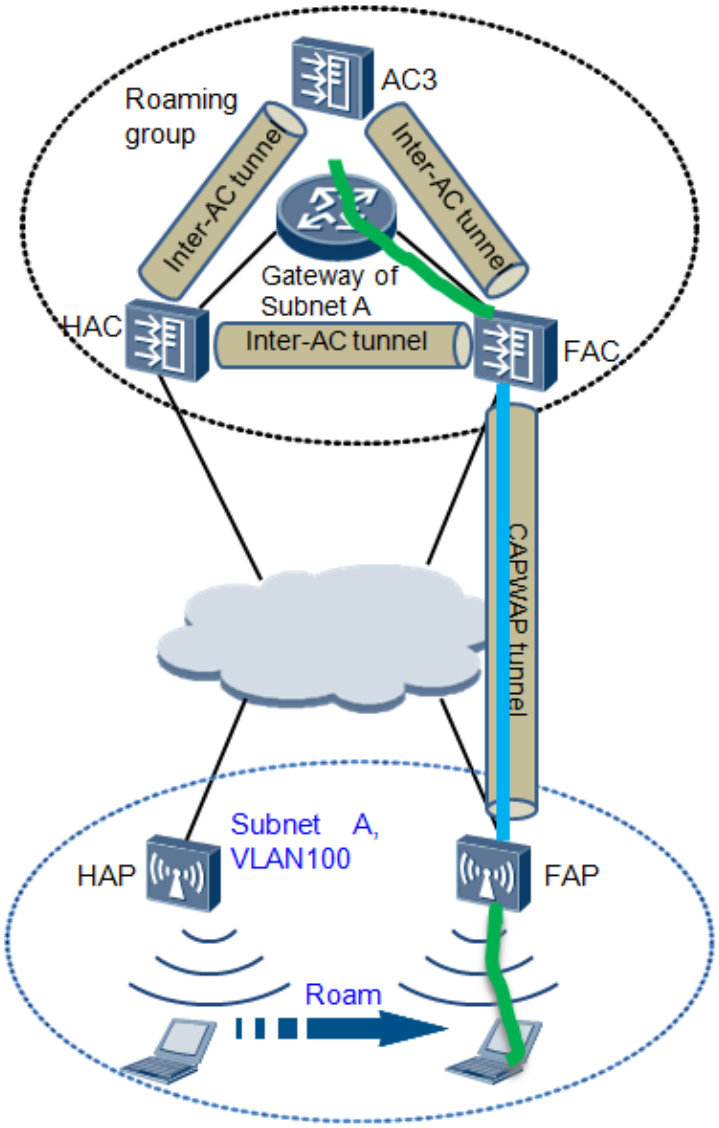


Figure 2-9 Traffic forwarding in the case of Layer 2 roaming + centralized forwarding



2.4.2 Layer 3 Roaming

Unicast Packet Forwarding

After a STA performs Layer 3 roaming, it leaves the original subnet. To allow the STA to access the network, the user traffic needs to be transferred back to the home agent through the tunnel and then be transmitted by the home agent. In addition, packets sent from the network side to the STA are first transmitted

to the home agent and then forwarded by the home agent through the tunnel to the FAP.

A HAC or HAP can be specified as the home agent based on the following rules:

1. If centralized forwarding is used for a STA on the HAP, the HAC is fixed as the home agent because it can be assumed that the user gateway is accessed through the HAC. In this case, the tunnel between the FAP and home agent actually includes two parts: the tunnel between the FAP and FAC, and the tunnel between the FAC and HAC. For users who perform Layer 3 roaming from other subnets to the local subnet, packets are forwarded through the CAPWAP tunnel between the FAP and FAC, regardless of whether centralized forwarding is configured on the FAP.
2. If local forwarding is used for the STA on the HAP, the HAP or HAC can be configured as the home agent.

- By default, the HAP functions as the home agent. In this case, the tunnel between the FAP and home agent actually includes three parts: the tunnel between the FAP and FAC, the tunnel between the FAC and HAC, and the tunnel between the HAC and HAP. For users who perform Layer 3 roaming from the local subnet to other subnets, packets are forwarded through the CAPWAP tunnel between the HAP and HAC, regardless of whether centralized forwarding is configured on the HAP.
- If the HAC can access the user gateway (for example, the HAC and gateway can access each other at Layer 2) or the HAC is the user gateway, the HAC can be configured as the home agent. The HAC with higher capabilities can reduce the burden on the HAP and shorten the length of the tunnel from the FAP to the home agent to improve forwarding efficiency.

Assume that the HAP performs local forwarding for the STA and the HAP is configured as the home agent. 0 shows the unicast packet forwarding path of Layer 3 roaming STAs.

In the uplink direction, the process is as follows:

1. The STA sends a packet from the air interface.
2. The FAP receives the packet from the STA and forwards it to the FAC through the CAPWAP tunnel between the FAP and FAC.
3. The FAC forwards the packet to the HAC through the inter-AC tunnel between the FAC and HAC.
4. The HAC forwards the packet to the HAP through the CAPWAP tunnel between the HAC and HAP.
5. The HAP properly forwards the packet to the user gateway.

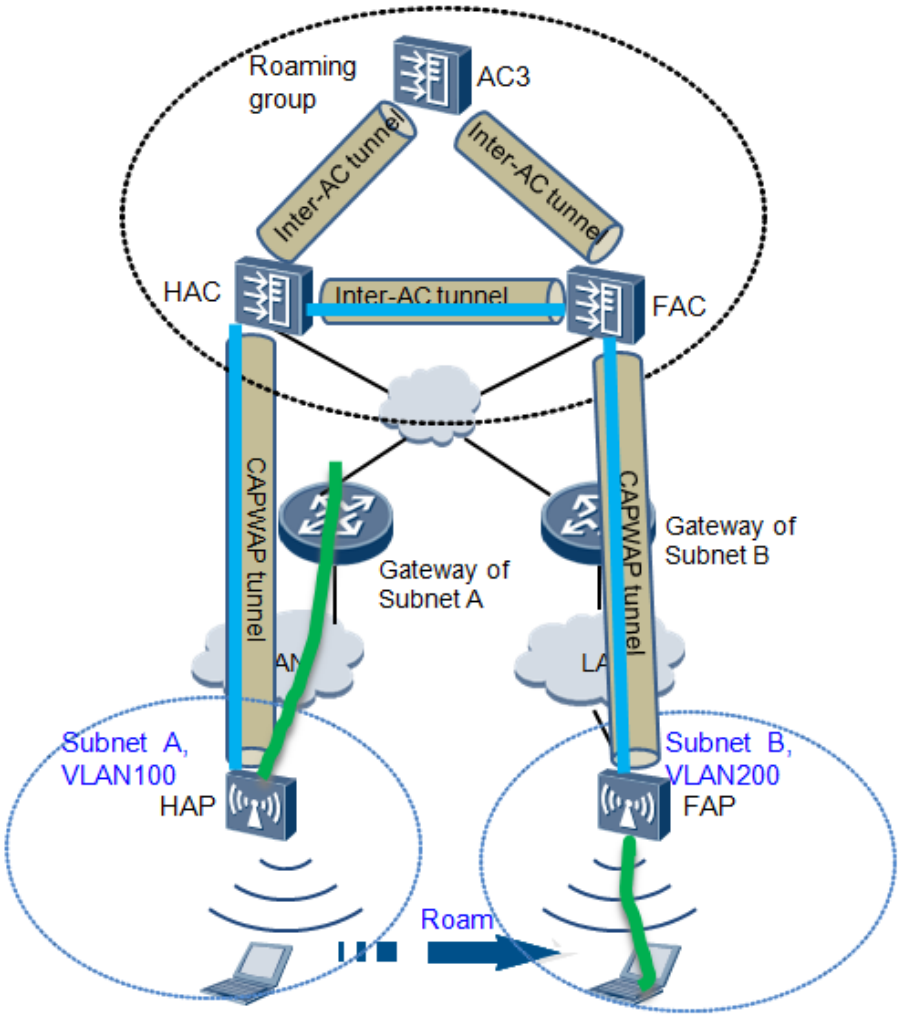
The forwarding path in the downlink direction is opposite to that in the uplink direction. In the downlink direction, the process is as follows:

1. The HAP receives a packet to be sent to a roaming user from the network side or air interface, and forwards it to the HAC through the CAPWAP tunnel between the HAP and HAC.
2. The HAC forwards the packet to the FAC through the inter-AC tunnel between the HAC and FAC.

3. The FAC forwards the packet to the FAP through the CAPWAP tunnel between the FAC and FAP.
4. The FAP forwards the packet to the STA through the air interface.

The packet forwarding mode in intra-AC roaming is the same as that in inter-AC roaming. However, in intra-AC roaming, the HAC and FAC overlap and the inter-AC tunnel between the HAC and FAC does not exist.

Figure 2-10 Local forwarding scenario and data forwarding path in which the HAP functions as the home agent



Assume that local forwarding is used for the STA on the HAP and the HAC is configured as the home agent. Figure 2-11 shows the unicast packet forwarding path of Layer 3 roaming users. (This scenario does not have step 4

in the uplink direction and step1 in the downlink direction compared with the scenario in which the HAP is configured as the home agent.)

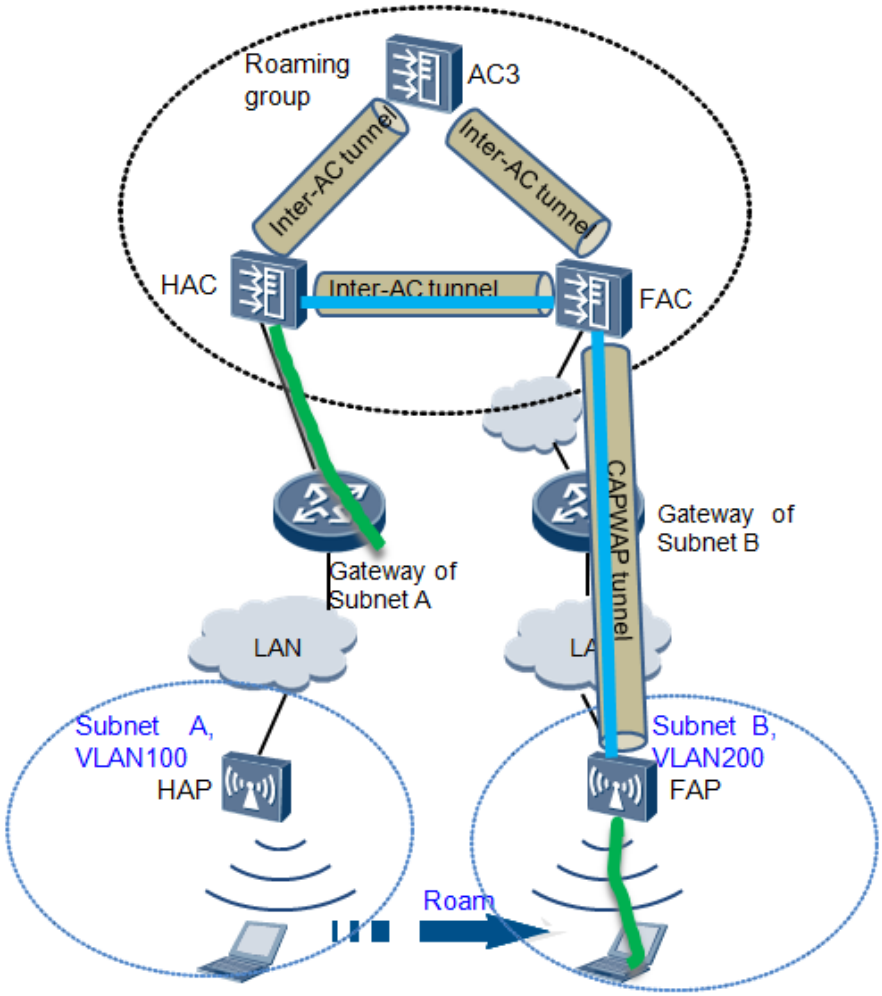
In the uplink direction, the process is as follows:

1. The STA sends a packet through the air interface.
2. The FAP receives the packet from the STA and forwards it to the FAC through the CAPWAP tunnel between the FAP and FAC.
3. The FAC forwards the packet to the HAC through the inter-AC tunnel between the FAC and HAC.
4. The HAC properly forwards the packet to the user gateway.

The forwarding path in the downlink direction is opposite to that in the uplink direction. In the downlink direction, the process is as follows:

1. The HAC receives a packet to be sent to a roaming user from the network side, and forwards it to the FAC through the inter-AC tunnel between the HAC and FAC.
2. The FAC forwards the packet to the FAP through the CAPWAP tunnel between the FAC and FAP.
3. The FAP forwards the packet to the STA through the air interface.

Figure 2-11 Local forwarding scenario and data forwarding path in which the HAC functions as the home agent



In this example, centralized forwarding is used for the STA on the HAP. Figure 2-12 shows the unicast packet forwarding path of Layer 3 roaming users. (This path is the same as the forwarding path in the scenario where local forwarding is used and the HAP is configured as the home agent.)

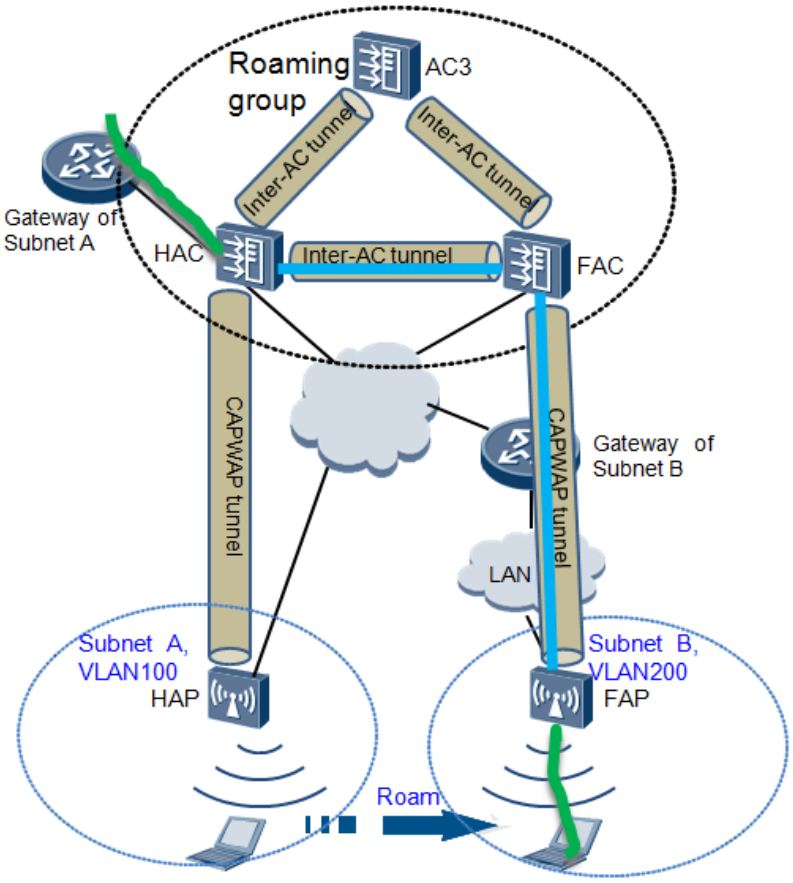
In the uplink direction, the process is as follows:

1. The STA sends a packet through the air interface.
2. The FAP receives the packet from the STA and forwards it to the FAC through the CAPWAP tunnel between the FAP and FAC.
3. The FAC forwards the packet to the HAC through the inter-AC tunnel between the FAC and HAC.
4. The HAC properly forwards the packet to the user gateway.

The forwarding path in the downlink direction is opposite to that in the uplink direction. In the downlink direction, the process is as follows:

1. The HAC receives a packet to be sent to a roaming user from the network side, and forwards it to the FAC through the inter-AC tunnel between the HAC and FAC.
2. The FAC forwards the packet to the FAP through the CAPWAP tunnel between the FAC and FAP.
3. The FAP forwards the packet to the STA through the air interface.

Figure 2-12 Centralized forwarding scenario and data forwarding path in which the HAC functions as the home agent



Broadcast Packet Forwarding

The forwarding mode of uplink broadcast packets from STAs to the network side is the same as that of unicast packets.

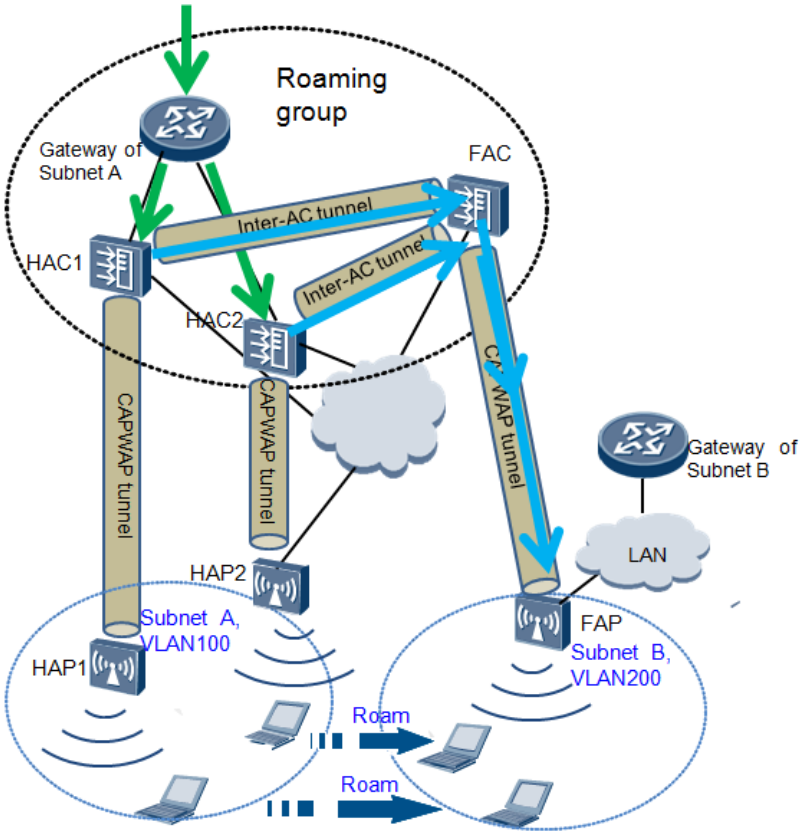
The downlink broadcast and multicast packets from the network side to STAs need to be processed specially. Traffic of Layer 3 roaming users needs to be

forwarded through the tunnel between the FAP and home agent, which puts forward a tunnel convergence issue.

As shown in 5, there are two ACs: HAC1 and HAC2, each having a STA that performs Layer 3 roaming to the FAC. In this example, two STAs on the HAP both use the centralized forwarding mode and are configured in the same subnet Subnet A.

1. When the network side sends a broadcast packet, the packet is broadcast to HAC1 and HAC2.
2. HAC1 and HAC2 detect that they have a STA roaming to the FAC. To allow the roaming STAs to receive the broadcast packet, HAC1 and HAC2 send the broadcast packet to the FAC through the inter-AC tunnel between them and FAC.
3. Therefore, the FAC receives two identical broadcast packets and forwards them to the FAP through the tunnel between the FAC and FAP.
4. The FAP receives two identical broadcast packets and broadcasts them to the STA over the air interface.
5. The STA receives two identical broadcast packets.

Figure 2-13 Tunnel convergence for downlink broadcast/multicast packets in Layer 3 roaming scenario



There are tunnels between one FAP and multiple home agents. If each home agent receives a broadcast/multicast packet and sends it to the FAP through a tunnel, the FAP will receive multiple copies of the same broadcast/multicast packet. Finally, the STA receives multiple copies of the same broadcast/multicast packet.

To prevent tunnel convergence, process downlink broadcast/multicast packets according to the following rules:

- Discarding unknown unicast packets (do not pass through the roaming tunnel) in the roaming tunnel ingress of the HAC
- Transmitting ARP, ND, DHCP, and mDNS packets through the roaming tunnel of the HAC, and discarding other broadcast/multicast packets (do not pass through the roaming tunnel)
- Converting broadcast/multicast packets that are transparently transmitted to the FAC to unicast packets (destined to the roaming user of the source tunnel), and sending them to the FAP
- Forwarding packets to the roaming STA by the FAP

Multicast Packet Forwarding

Tunnel convergence also occurs in multicast and broadcast packet forwarding. Use the processing rules mentioned in the previous part. Downlink multicast packets arrive at the HAC and do not pass through tunnels. In this case, roaming users across ACs cannot receive multicast data from the home network, and online multicast services are interrupted.

To solve this problem, the FAP sends an IGMP General Query message packet to a roaming STA, so that the STA sends an IGMP join message to the network. The FAP directly forwards the uplink multicast packet of the roaming STA in the roaming destination. Therefore, multicast forwarding entries of the roaming network are updated by the IGMP join message, and the multicast flow is transmitted to the FAP and finally sent to the roaming STA.

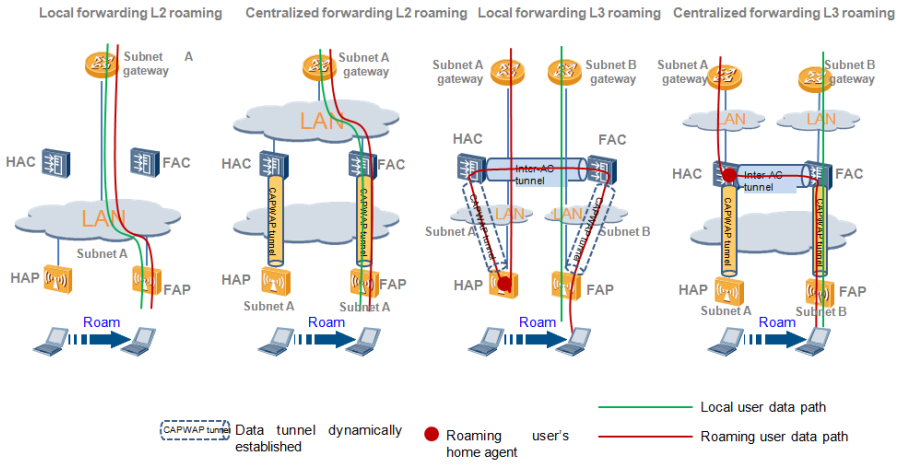
Currently, the FAP supports the IGMP snooping function for roaming STAs. After receiving the multicast flow, the FAP converts it to the unicast flow and forwards the unicast flow to the specified roaming STA.

Note: It takes a certain time to update the upper-layer multicast tree, so multicast flow may be interrupted during roaming for a time period. If the FAP in the roaming destination has received the multicast flow, the interruption time is greatly shortened.

2.4.3 Roaming Forwarding Model

There are four scenarios of inter-AC roaming according to the forwarding model and whether roaming is performed across Layer 3.

Figure 2-14 Basic forwarding model of four inter-AC roaming scenarios

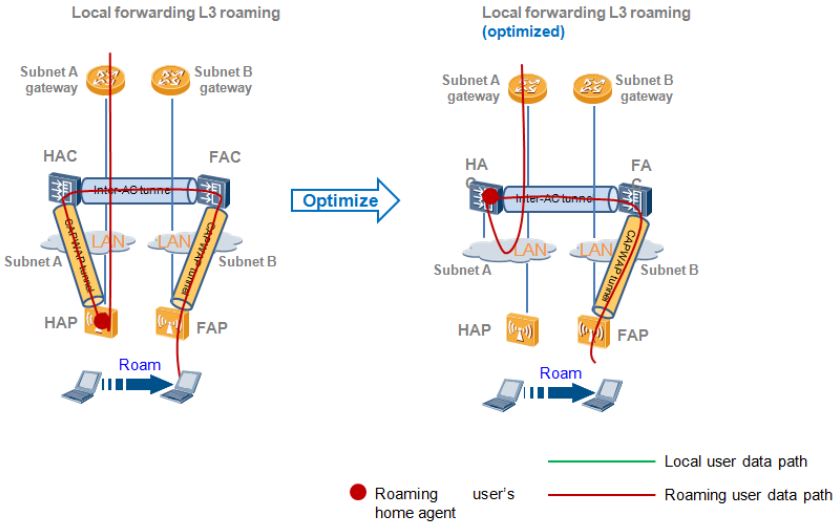


The first and third scenarios use the local forwarding mode; therefore, the AC and AP only need to be reachable at Layer 3, and Layer 2 or Layer 3 networking can be used between the AC and AP. As the AC is not located in the data forwarding path, the networking between the AC and AP is not shown in the preceding figure.

The difference between Layer 2 and Layer 3 roaming lies in whether the two APs before and after roaming access the same STA service subnet by default.

In the local forwarding Layer 3 roaming scenario, when the HAC and HAP are located in the same subnet, the HAC can be configured as the home agent. This optimizes the forwarding path.

Figure 2-15 Optimization of inter-AC Layer 3 roaming



Note: The prerequisite for optimization is that Layer 2 networking is used between the HAC and HAP. Optimization cannot be enabled in cross-Layer 3 networking.

In the forwarding model, MAC address learning is not performed for packets from roaming tunnels; the FAP/FAC does not forward uplink broadcast and unicast packets from roaming users based on destination IP addresses but specifies roaming tunnels for the packets to pass through. The FAP forwards uplink multicast packets in the roaming area.

Downlink unknown unicast packets are directly discarded on the HAC; downlink ARP/ND/DHCP/mDNS packets pass through roaming tunnels and are converted into unicast packets on the FAC.

2.5 Identification of Layer 2 Roaming and Layer 3 Roaming

Layer 2 and Layer 3 roaming have quite different forwarding behaviors, so identifying Layer 2 and Layer 3 roaming is important.

To differentiate Layer 2 roaming from Layer 3 roaming, check whether a user is roaming in the same subnet. Assume that the default service VLAN (service VLAN configured by the ESS) of the VAP on the AP can represent the networking.

- If the HAP and FAP have the same service VLAN configured, they are in the same subnet and the STA performs Layer 2 roaming between them.
- If the HAP and FAP have different service VLANs configured, they are in different subnets and the STA performs Layer 3 roaming between them.

The actual VLAN used by the user is ignored, for example, the authorization VLAN delivered by an authentication server. The authorization VLAN can be different from the service VLAN, but support on the authorization VLAN should be the same on the devices in the same subnet. For example, if the HAP supports the authorization VLAN, the FAP should also support it. Therefore, Layer 2 or Layer 3 roaming of a STA only depends on whether the HAP and FAP are in the same subnet, not whether the authorization VLAN is the same as the service VLAN.

The preceding assumptions are reasonable in most application scenarios. However, in some large networks, two subnets may use the same VLAN ID. For example, the network segments 10.11.104.x and 192.168.1.x both use VLAN 100. In this case, whether the HAP and FAP are in the same subnet can be determined only according to the VLAN.

Therefore, the ESS has a VLAN mobility group (Layer 2 roaming domain in the VLAN) configured. The HAP and FAP are in the same subnet only when they have the same VLAN and same VLAN mobility group.

The rule for determining Layer 2 or Layer 3 roaming is as follows:

If the HAP and FAP have the same service VLAN and Layer 2 roaming domain (VLAN mobility group) configured in the ESS of a roaming user, the user performs Layer 2 roaming. If the service VLANs and Layer 2 roaming domains are different, the user performs Layer 3 roaming.

3 Benefits to Customers

Compared with a traditional wired network, the biggest advantage of a WLAN is that a STA can move freely within the WLAN coverage without the restriction of physical media locations, and services are not affected during the movement. In an ESS, multiple APs are required to cover a large area. A STA always needs to move from one AP signal coverage to another during its movement. Accordingly, the STA can obtain services from the new AP only after the association is switched from the original AP to the new AP. WLAN roaming technology ensures that user services are not interrupted during the association switchover, minimizes the packet loss, and provides stable and smooth user service experience during the roaming process.

WLAN roaming has the following advantages:

- Ensures that the IP address remains unchanged after a STA roams.

  Application protocol packets are transmitted using IP addresses and TCP/UDP connections. STAs' IP addresses must remain unchanged after WLAN roaming so that the TCP/UDP connections established for the STAs are not interrupted.
- Ensures that a STA can still access its first connected network (called home network) and the services that the STA can use remain unchanged. The STA can access the home network when roaming any place, and the service layer cannot detect the roaming.
- Prevents packet loss during data transmission in roaming and provides good user experience.

WLAN roaming technology ensures that users can move freely within the WLAN signal coverage, services are not interrupted, and user experience is not affected.

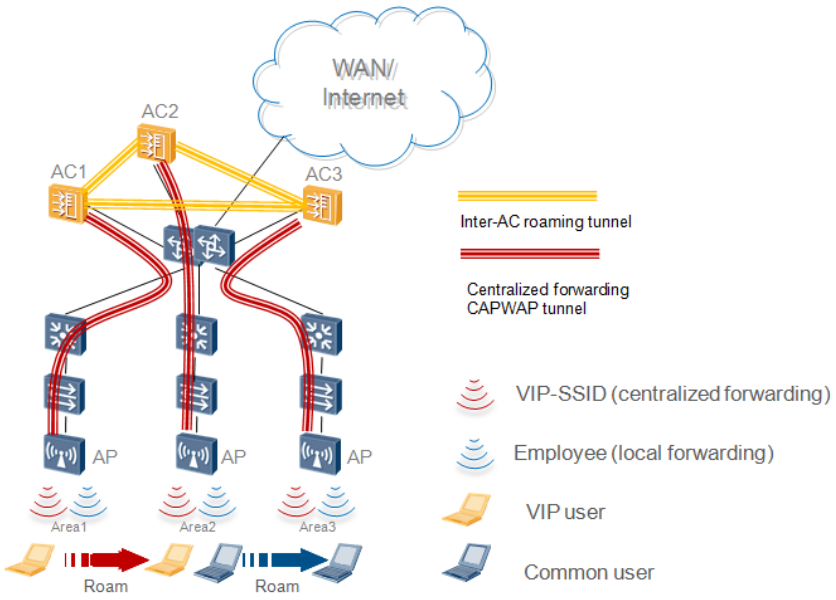
In the single-AC infrastructure WLAN architecture, all APs are managed by the same AC. When a user is roaming between APs, the status information is managed by the same AC. When the network scale grows, multiple ACs are deployed. Huawei uses technologies such as inter-AC information synchronization and dynamic roaming tunnel after roaming to implement smooth inter-AC roaming, meeting customer requirements of radio coverage and roaming in wider areas.

4 Typical Application Scenarios

4.1 Core-Layer Roaming Solution

In large-scale enterprises, the network scale is large and multiple ACs need to be deployed to cover different areas. The demand on inter-AC roaming is put forward because enterprise personnel need to perform inter-area roaming. Figure 4-1 shows a typical WLAN networking scenario for a large-scale enterprise.

Figure 4-1 Core-layer inter-AC roaming solution

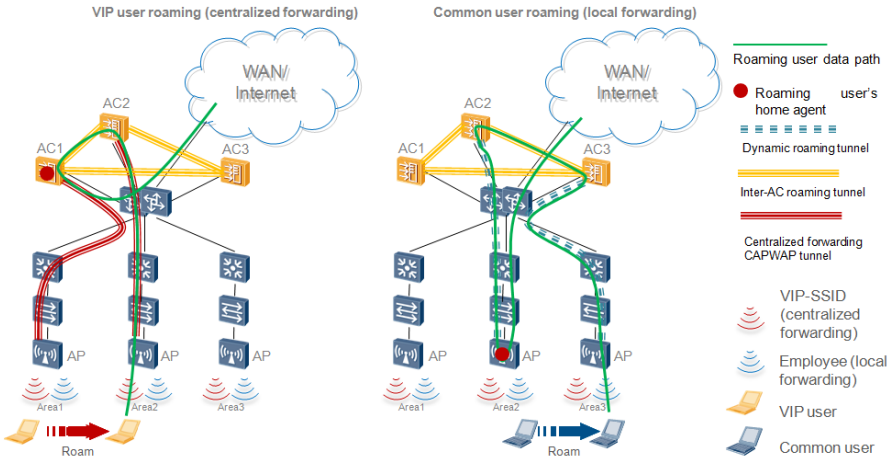


Multiple WLAN AC devices are deployed besides the enterprise's core devices for access and management of WLAN AP devices. Two WLAN services are deployed in the network: one used for wireless access of enterprise employees and the other for wireless access of VIP users.

- For wireless access of employees, local forwarding is used and user data is directly forwarded in the enterprise intranet after entering the WLAN APs.
- For wireless access of VIP users, centralized forwarding is used and all data is transmitted through the centralized forwarding CAPWAP tunnel between the APs and AC and forwarded by the AC.

Inter-AC roaming is supported for both employees and VIP users. Figure 4-2 shows the inter-AC roaming process of wireless users in different forwarding modes.

Figure 4-2 Core-layer inter-AC roaming solution using different forwarding modes

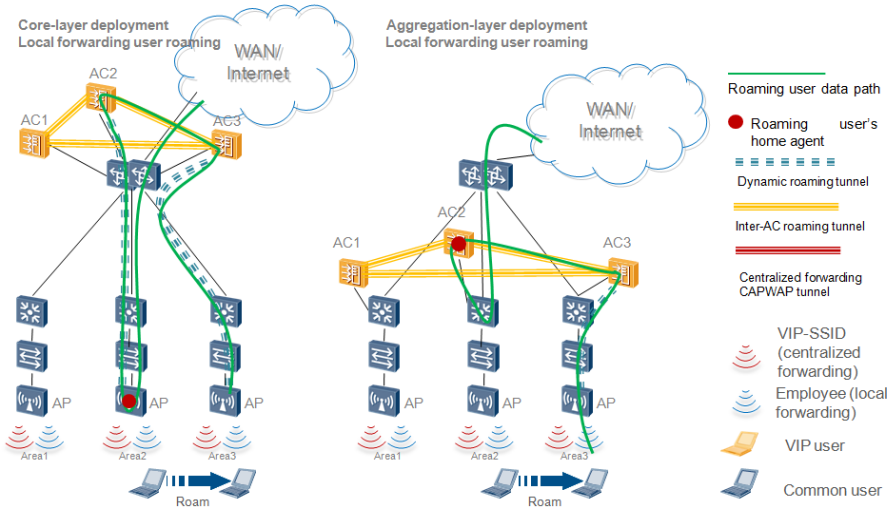


- For VIP users in centralized forwarding mode, when a wireless user roams to another AC area, home AC1 is the roaming user's home agent and the uplink/downlink user traffic is transmitted on home AC1. The downlink traffic enters the inter-AC roaming tunnel on AC1, and then reaches the roaming user through the centralized forwarding tunnel between AC2 and AP2. The uplink traffic also needs to be sent back to home AC1 through the inter-AC tunnel to complete the subsequent forwarding.
- For employees in local forwarding mode, when a wireless user roams to another AC area, home AP2 is the roaming user's home agent and the uplink/downlink user traffic is transmitted on home AP2. The system automatically sets up a dynamic roaming tunnel for the roaming user, although the user uses the local forwarding mode and there is no fixed centralized forwarding CAPWAP tunnel between the AC and APs. The downlink traffic enters the roaming tunnel between AP2 and AC2 on AP2, and then reaches the roaming user through the inter-AC roaming tunnel and the roaming tunnel between AC3 and AP3. The uplink traffic enters the roaming tunnel on AP3, and arrives at the home AP2 out of the tunnel to complete the subsequent forwarding.

4.2 Aggregation-Layer Roaming Solution

The enterprise may deploy a WLAN AC at the aggregation layer. The WLAN AC and its managed APs are available at Layer 2, and the VIP user forwarding models for centralized forwarding are the same. For wireless roaming users in local forwarding mode, the home agent of the roaming users can be changed to the WLAN AC to optimize the forwarding path, as shown in Figure 4-3.

Figure 4-3 Core-layer and aggregation-layer inter-AC roaming solutions



By default, the roaming users' home AP (HAP) is configured as the home agent. If the administrator determines that the WLAN HAC and HAP are located in the same L2 network, the HAC can be configured as the home agent using the following commands:

home-agent { ac | ap }

The AC or AP is configured as the home agent.

undo home-agent

The default home agent (AP) is restored.