

**AC6605 Access Controller
V200R001C00**

Dual-Link Backup White Paper

Issue **01**
Date **2012-05-30**

Copyright © Huawei Technologies Co., Ltd. 2012. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of 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

About This Document

Purpose

This document describes the dual-link backup technology of the AC6605. The dual-link backup technology provides high reliability between important network nodes to ensure service availability.

This document covers the mechanism and networking modes of dual-link backup supported by the AC6605, and provides configuration examples for typical dual-link backup applications.






Intended Audience

This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
 DANGER	Alerts you to a high risk hazard that could, if not avoided, result in serious injury or death.
 WARNING	Alerts you to a medium or low risk hazard that could, if not avoided, result in moderate or minor injury.
 CAUTION	Alerts you to a potentially hazardous situation that could, if not avoided, result in equipment damage, data loss, performance deterioration, or unanticipated results.
 TIP	Provides a tip that may help you solve a problem or save time.
 NOTE	Provides additional information to emphasize or supplement important points in the main text.

Change History

Changes between document issues are cumulative. The latest document issue contains all the changes made in earlier issues.

Issue 01 (2012-05-30)

This is the first formal issue.

Contents

About This Document	ii
1 Dual-Link Backup	1
1.1 Introduction to Dual-Link Backup.....	1
1.2 Availability	2
1.3 Principles	2
1.3.1 Dual-Link Backup Mechanism.....	2
1.3.2 AP Login Process.....	3
1.3.3 STA Login Process.....	6
1.3.4 Active/Standby Switchover and Revertive Switchover	6
1.3.5 Loop Prevention in VLANs.....	7
1.3.6 Dual-Link Backup in Layer 2 Networking and Configuration Notes	10
1.3.7 Dual-Link Backup in Layer 3 Networking and Configuration Notes	18
1.4 Applications	29
1.4.1 Direct Forwarding in Layer 3 Chain Networking.....	29
1.4.2 Tunnel Forwarding in Layer 2 Branched Networking.....	33

1 Dual-Link Backup

About This Chapter

- 1.1 Introduction to
- 1.2 Availability
- 1.3 Principles
- 1.4 Applications

1.1 Introduction to Dual-Link Backup

Definition

Dual-link backup is implemented by deploying a standby AC at the same layer as the active AC. The standby AC has the same configuration as the active AC. When the active AC fails, the backup AC starts to manage services quickly.

Purpose

An AC usually controls thousands of APs and tens of thousands of STAs; therefore, the AC must be highly reliable. Configuring dual-link backup can ensure stable service operating on a WLAN network.

Benefits

The dual-link backup technology provides high reliability between important network nodes to ensure service availability.

1.2 Availability

Version Support

Product	Product Version
AC6605	V200R001C00

Constraints

Dual-link backup has the following constraints:

- The active and standby ACs must have the same WLAN service configuration.
- APs must be able to communicate with both the active and standby ACs. When APs communicate with the ACs through a Layer 2 network, APs must belong to the same VLAN as the ACs, and AP IP addresses must be on the same network segment as AC IP addresses.
- If the active AC functions as a DHCP server to allocate IP addresses to APs, configure static IP addresses for APs or configure an IP address pool only on the active AC. If you need to configure IP address pools on both ACs, ensure that the IP address pools on the two ACs do not overlap. Otherwise, IP address conflicts may occur.
- The ACs cannot allocate IP addresses to STAs or work as gateways for STAs.

1.3 Principles

1.3.1 Dual-Link Backup Mechanism

Dual-link backup is enabled on active and standby ACs so that APs can establish Control and Provisioning of Wireless Access Points (CAPWAP) tunnels with both ACs. The status of an AP is displayed as normal on the active AC and displayed as standby on the standby AC. When both the active and standby ACs are working properly, only the active AC manages services of APs and delivers configurations to the APs.

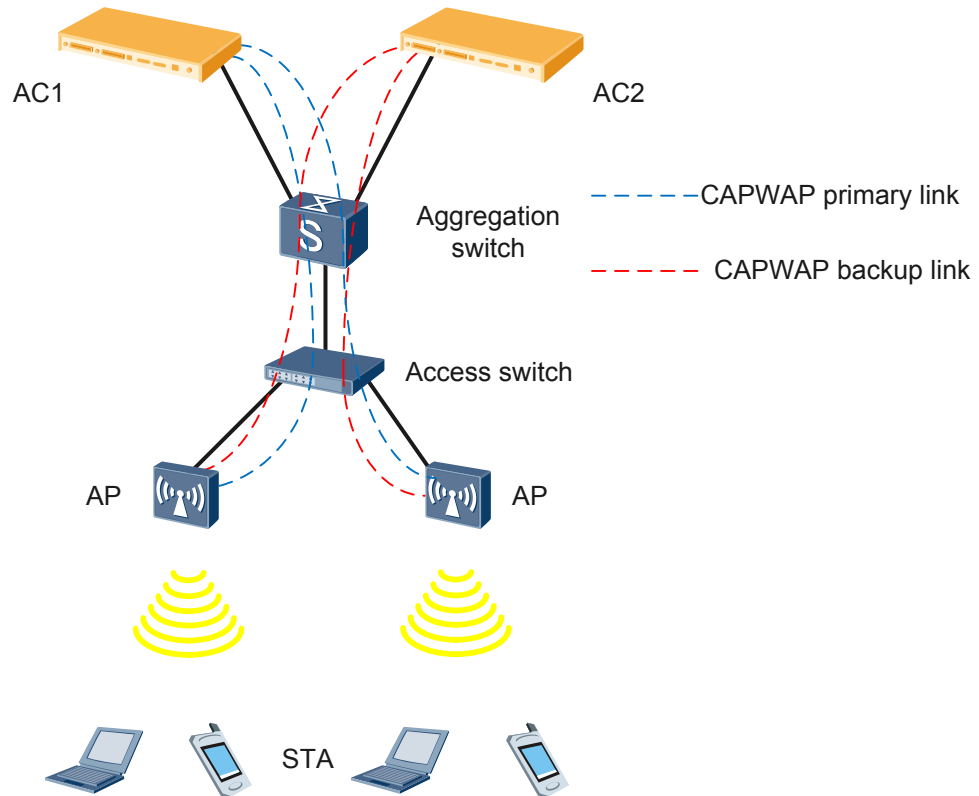
An AP sends Echo packets to monitor the status of the links connected to the ACs. When the active AC is unavailable because of an AC fault or network failure, an AP detects that the link connected to the active AC is Down, and the AP status on the standby AC changes from standby to normal. The standby AC then delivers configurations to the AP and manages services of the AP.

When the AP detects that the link connected to the active AC recovers, it switches service traffic back to the active AC within 500 seconds if revertive switching is enabled. After the switchover, the AP status is displayed as normal on the active AC and displayed as standby on the standby AC. If revertive switching is disabled, the AP still sends service traffic to the standby AC.

As shown in Figure 1-1, the APs set up CAPWAP tunnels with the active AC (AC1) and standby AC (AC2) simultaneously when they go online. The APs and ACs exchange handshake packets to monitor the link status. When the APs detect that the links connected to AC1 fail, they switch service traffic to AC2. As they have established CAPWAP tunnels with AC2, service switching time is reduced. However, users need to go online again after the

switchover. Users that were authenticated using open system or WEP authentication do not need to go online again.

Figure 1-1 Dual-link backup



Impact of an active/standby switchover on services is as follows:

- During an active/standby switchover, services are interrupted for a period because an AP needs to detect the failure of primary link using CAPWAP heartbeat packets. The service interruption time is determined by the heartbeat interval (3s to 300s) and number of detection attempts (2 to 120). Users cannot use Internet services, but they are still online and do not need to be reauthenticated after the switchover is complete. The AP status on the standby AC changes from standby to normal after the AP detects a failure on the primary link.
- When traffic is switched back from the standby AC to the active AC, services are not affected because both the primary link and backup link are working properly. Users are still online and do not need to be reauthenticated after the switchover is complete.

1.3.2 AP Login Process

After an AP is powered on, it uses DHCP to obtain its own IP address and IP addresses of the active and standby ACs. The AP then discovers the ACs and establishes primary and backup links with the ACs to implement dual-link backup.

If neither of the active and standby ACs is used as a DHCP server, you only need to set Option 43 to IP addresses of the active and standby ACs on the DHCP server and do not need to consider the IP address lease. The following describes the AP login process when an AC functions as a DHCP server.

Obtaining IP Addresses on a Layer 2 Network

1. An AP broadcasts a DHCP Discovery packet with Option 60 as Huawei AP.
2. The two ACs receive the DHCP Discovery packet and both reply with a DHCP Offer packet.
3. After receiving the two DHCP Offer packets, in the Discovery phase, the AP sends Discover Request messages to both ACs. As long as the ACs are working properly, they will return Discover Response messages to the AP. The Discover Response messages contain the dual-link backup flag, priorities, workload, and IP addresses of the ACs. After receiving the Discover Response messages, the AP compares information in the packets and selects an AC as the DHCP server, and then sends a DHCP Request packet to the selected AC.
4. The selected AC sends a DHCP ACK packet to the AP. In the DHCP ACK packet, the Option 43 field contains the IP addresses of the two ACs, and the Option 51 field contains a long IP address lease. (The 32-bit Option 51 field can specify the longest lease of 136 years.)
5. After receiving the DHCP ACK packet, the AP obtains its own IP address and IP addresses of the active and standby ACs. The IP address lease is very long so that the AP does not need to extend the lease. If no Option 43 is configured on the ACs, the AP can broadcast a DHCP Request to discover ACs.

Obtaining IP Addresses on a Layer 3 Network

1. An AP broadcasts a DHCP Discovery packet with Option 60 as Huawei AP.
2. A DHCP relay agent is deployed between the ACs and APs, and the primary and secondary DHCP servers are configured on the active and standby ACs. The DHCP relay agent sends a DHCP Discovery packet to the active AC (in active/standby mode) or to both the ACs (in load balancing mode).
3. If the DHCP relay agent works in active/standby mode, the active AC receives the DHCP Discovery packet and replies with a DHCP Offer packet. If the DHCP relay agent works in load balancing mode, both ACs receive the DHCP Discovery packet and reply with a DHCP Offer packet.
4. The DHCP relay agent forwards the DHCP Offer packets to the AP.
5. After receiving the two DHCP Offer packets, in the Discovery phase, the AP sends Discover Request messages to both ACs. As long as the ACs are working properly, they will return Discover Response messages to the AP. The Discover Response messages contain the dual-link backup flag, priorities, workload, and IP addresses of the ACs. After receiving the Discover Response messages, the AP compares information in the packets and selects an AC as the DHCP server, and then sends a DHCP Request packet to the selected AC.
6. The DHCP relay agent forwards the DHCP Request packet to the selected AC.
7. The selected AC sends a DHCP ACK packet to the AP. In the DHCP ACK packet, the Option 43 field contains the IP addresses of the two ACs, and the Option 51 field contains a long IP address lease. (The 32-bit Option 51 field can specify the longest lease of 136 years.)
8. The DHCP relay agent forwards the DHCP ACK packet to the AP.
9. After receiving the DHCP ACK packet, the AP obtains its own IP address and IP addresses of the active and standby ACs. The IP address lease is very long so that the AP does not need to extend the lease.

The AP then discovers ACs and set up tunnels with the ACs.

Setting Up the First Tunnel

1. After the AP obtains its own IP address and IP addresses of the two ACs, it sends a Discover Request packet to both ACs to discover ACs. If the AP obtains only its own IP address, it broadcast a Discover Request packet to discover ACs.
2. If the ACs are working properly, they send a Discover Response packet with the dual-link backup flag, workload, and priority to the AP.
3. After receiving the Discover Response packets, the AP compares the priorities and IP addresses of the ACs to select an AC and establishes a CAPWAP tunnel with the selected AC. The AC with a smaller priority value becomes the active AC. If the ACs have the same priority value, the AC with a lower workload becomes the active AC. If their workloads are also the same, the AC with smaller IP address becomes the active AC.

 **NOTE**

If an AC fails to return a Discover Response packet, the AP selects the other AC to set up the CAPWAP tunnel. The tunnel set up first may not be the primary tunnel. The AP will determine the primary and backup tunnels after it successfully establishes tunnels with both the two ACs.

4. The subsequent negotiation and configuration delivery processes are the same as those for setting up a single CAPWAP tunnel.
5. After the tunnel is set up, the AC delivers configurations to the AP. When the AP works, STAs can go online and use network services.

Setting Up the Second Tunnel with the Other AC

1. The AP determines to set up a CAPWAP tunnel with the other AC only when the Discover Response packet sent by the first AC contains the dual-link backup flag. The AP starts to set up the second tunnel after the first AC has delivered configurations to the AP. This avoids repeated configuration delivery.
2. If the AP has obtained the other AC's IP address, it sends a unicast Discover Request packet to this AC, and then sends a broadcast Discover Request packet to discover ACs. If the AP has not obtained the other AC's IP address, it sends a broadcast Discover Request to discover ACs. The AC that has set up a CAPWAP tunnel with the AP ignores the Discover Request packet.
3. If the AC is working properly, it returns a Discover Response packet containing the dual-link backup flag and priority to the AP.
4. The AP knows that the dual-link backup function is enabled after receiving the Discover Response packet, and saves the priority of the AC.

 **NOTE**

The second AC will not become the active AC even if it has a higher priority than the first one. The AP switches traffic to this AC only after it sets up a CAPWAP tunnel with the AC.

5. The AP sends a Join Request packet, notifying the AC that the configurations have been delivered. The AC will not deliver configurations to the AP after receiving the Join Request packet.
6. After the tunnel is set up, the AP compares the priorities and IP addresses of the two ACs and determines the active and standby ACs. The AP performs a revertive switchover if the second AC becomes the active AC.

1.3.3 STA Login Process

Association Authentication

STA association authentication is performed by the active AC, and the standby AC does not save STA information. After an active/standby switchover, the new active AC synchronizes STA information from APs through CAPWAP tunnels.

IP Address Allocation

When STA addresses are allocated by an AC, STAs face two issues: address conflicts and address lease extension. In addition, STAs cannot be allocated static IP addresses because they connect to wireless networks randomly.

Two solutions are available to address the two issues:

- (Recommended) Deploy an independent DHCP server to allocate IP addresses to STAs.
- Deploy DHCP servers on the ACs and configure non-overlapping IP address pools on the ACs. Set the lease of IP addresses to the longest time STAs may stay online, for example, seven days. The non-overlapping IP address pools on the ACs prevent IP address conflicts. Because most STAs go offline before their IP addresses expire, STAs do not need to extend their IP address leases. There is a very low probability that an STA stays online for a long time and extends its IP address lease during an active/standby switchover. This low probability is acceptable.

Additionally, the ACs cannot function as gateways for STAs. If an AC functions as the gateway for STAs, the gateway IP address changes after a switchover. However, STAs cannot change the gateway IP address, causing service interruption.

Data Forwarding

Data of STAs is forwarded in either of the following modes:

Direct forwarding: Data of STAs is forwarded by APs locally.

Tunnel forwarding: Data of STAs is forwarded by the active AC. After an active/standby switchover, data of STAs is sent to the new active AC for forwarding.

1.3.4 Active/Standby Switchover and Revertive Switchover

Active/Standby Switchover

After an AP sets up tunnels with the active and standby ACs, it sends Echo packets to monitor the tunnel status. The Echo packets contain the primary/secondary status of tunnels. When an AP detects that the primary tunnel fails, the AP sends an Echo packet to the standby AC to trigger an active/standby switchover. The failed tunnel then becomes the secondary tunnel, and the original secondary tunnel becomes the primary tunnel. The Echo packet sent from the AP to the standby AC contains the primary link flag. After receiving this Echo message, the standby AC changes to active state and sets the AP status to normal. The AP then send service data to the new active AC. The AP periodically sends Discovery Request packets to check whether the failed link recovers.

Revertive Switchover

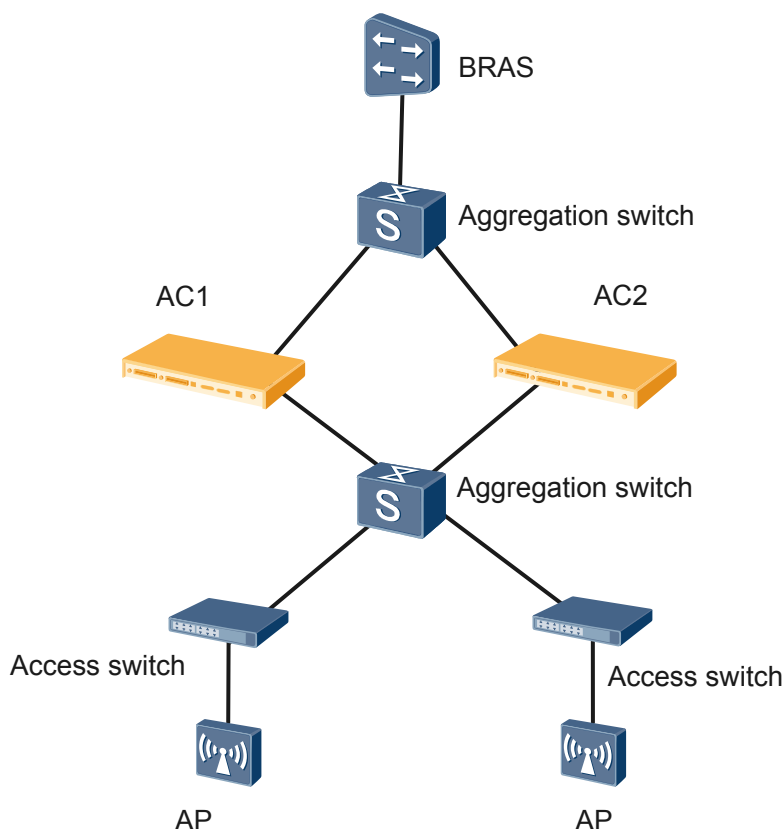
After the original active AC recovers and the AP sets up a CAPWAP tunnel with this AC, the AP triggers a revertive switchover after a delay time to avoid frequent switchovers caused by network flapping. The delay time is fixed at 500 seconds, which is 20 times the Echo interval. When the delay expires, the AP sends an Echo packet to request the ACs to carry out a revertive switchover. Additionally, the AP transfers STA data to the new active AC.

1.3.5 Loop Prevention in VLANs

As shown in Figure 1-2, AC1 and AC2 work in dual-link backup mode to manage APs. The APs obtain IP addresses and service configurations from the ACs. The BRAS allocates IP addresses to STAs and works as the gateway for STAs. Data packets from STAs are forwarded to the active AC through a CAPWAP tunnel and forwarded to the BRAS by the AC at Layer 2. The BRAS forwards the data packets to the upstream network at Layer 3.

In this networking, the ACs must be configured with the management VLAN of APs, service VLANs of STAs, and management VLANs of the aggregation switch and access switches (PoE switches).

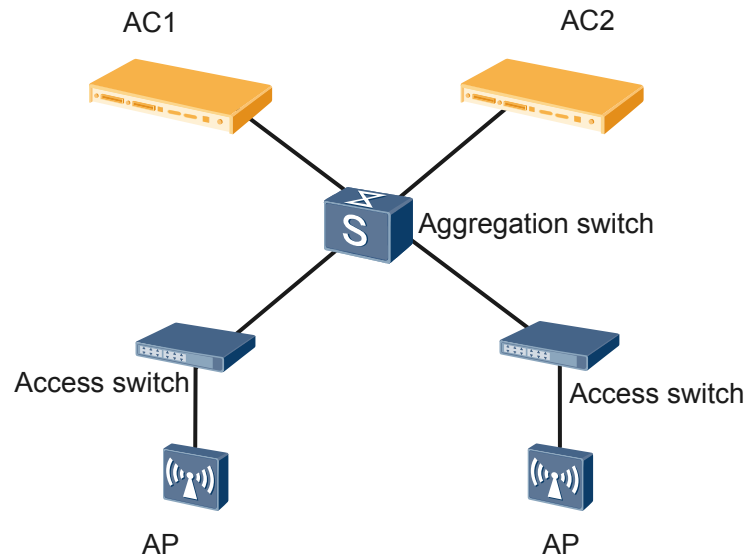
Figure 1-2 Networking of dual-link backup in Layer 2 chain networking



- Management VLAN of APs, service VLANs of STAs, and management VLANs of switches are different.

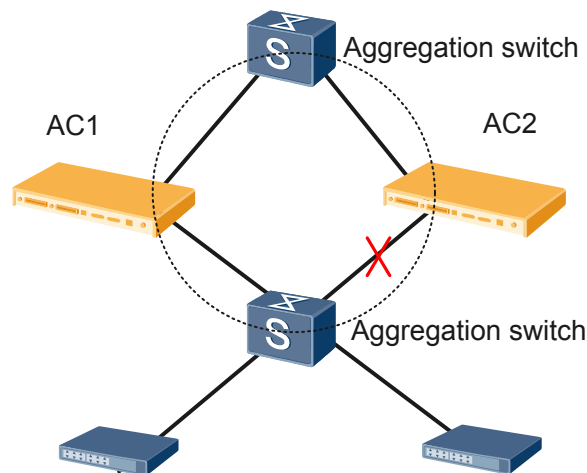
The management VLAN of the APs only needs to be configured on the ACs and downstream switches, as shown in Figure 1-3. Therefore, no loop will be formed in the VLAN.

Figure 1-3 No loop in the management VLAN of APs



Management VLANs of the aggregation switches and access switches must be configured on the two aggregation switches and ACs; therefore, a loop is formed, as shown in Figure 1-4. To prevent packet looping, enable MSTP or configure port isolation on the ACs or aggregation switches. MSTP is recommended.

Figure 1-4 Loop in management VLANs of aggregation and access switches



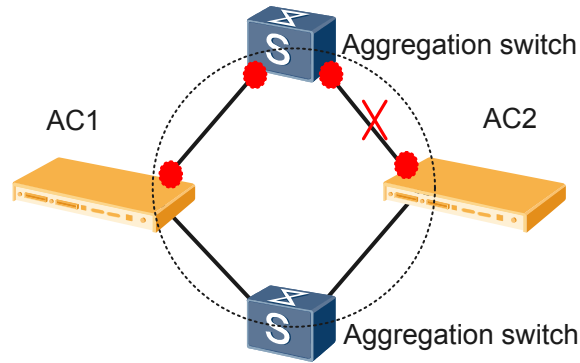
Service VLANs of STAs also need to be configured on the two aggregation switches and ACs, causing loops. Similarly, enabling MSTP or configuring port isolation can prevent loops in these VLANs. Because there are many service VLANs of STAs, MSTP is recommended so that service VLANs can be mapped to an MST instance.

- APs use the same VLAN as switches or STAs.

If the AP management VLAN is the same as a VLAN of switches or STAs, a loop occurs in this VLAN. To prevent loops in this VLAN, enable MSTP (recommended) or configure port

isolation on the ACs or aggregation switches. When using MSTP to prevent loops, ensure that the blocked port is one of ports between the ACs and upstream aggregation switches (the four ports marked red in Figure 1-5).

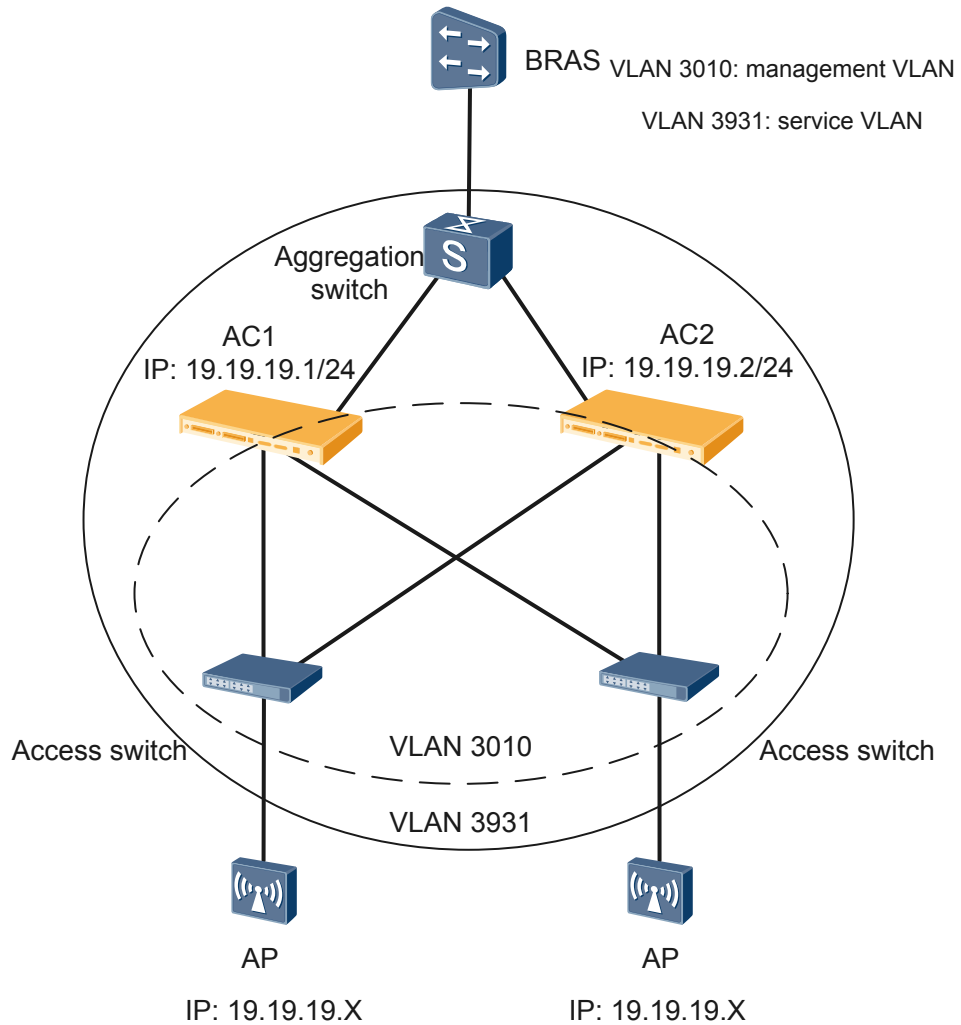
Figure 1-5 Loop formed when AP management VLAN is the same as a VLAN of switches or STAs



1.3.6 Dual-Link Backup in Layer 2 Networking and Configuration Notes

Layer 2 Chain Networking (Direct Forwarding)

Figure 1-6 Dual-link backup in Layer 2 chain networking (direct forwarding)



As shown in Figure 1-6, the ACs are deployed between an aggregation switch and two access switches on a Layer 2 network. Data packets from STAs are forwarded in direct mode. AC1 is the active AC, and AC2 is the standby AC.

The configuration notes in this networking are as follows:

- Configure the same AC ID and carrier ID for AC1 and AC2. Otherwise, after the active AC fails, services cannot be switched to the standby AC because BSSIDs of the two ACs are different. Run the following commands:

```
[AC6605_AC1] wlan ac-global ac id 999 carrier id ctc  
[AC6605_AC2] wlan ac-global ac id 999 carrier id ctc
```

The ACs must deliver the same VAP to an AP. Manually add offline APs to AC1 and AC2. It is recommended that the same AP ID be configured for an AP on AC1 and AC2. Run the following commands:

```
AC6605_AC1] wlan
[AC6605_AC1-wlan-view] ap id 0 ap-type WA601 mac 0025-9876-2633 sn A0928182
[AC6605_AC2] wlan
[AC6605_AC2-wlan-view] ap id 0 ap-type WA601 mac 0025-9876-2633 sn A0928182
```

- To prevent IP address conflicts, ensure that the IP address pools configured for APs on AC1 and AC2 do not overlap each other.

Configure an IP address pool for APs on AC1.

```
[AC6605_AC1] ip pool ap-active
[AC6605_AC1-ip-pool-ap-active] gateway-list 19.19.19.1
[AC6605_AC1-ip-pool-ap-active] network 19.19.19.0 mask 255.255.255.0
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 19.19.19.2
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 19.19.19.151 19.19.19.254
[AC6605_AC1-ip-pool-ap-active] option 43 sub-option 3 ascii HuaweiAC-19.19.19.1,
19.19.19.2 ///This configuration is optical in Layer 2 networking but is
recommended.
```

Configure an IP address pool for APs on AC2.

```
[AC6605_AC2] ip pool ap-standby
[AC6605_AC2-ip-pool-ap-standby] gateway-list 19.19.19.2
[AC6605_AC2-ip-pool-ap-standby] network 19.19.19.0 mask 255.255.255.0
[AC6605_AC2-ip-pool-ap-standby] excluded-ip-address 19.19.19.1
[AC6605_AC2-ip-pool-ap-standby] excluded-ip-address 19.19.19.3 19.19.19.150
[AC6605_AC2-ip-pool-ap-standby] option 43 sub-option 3 ascii HuaweiAC-19.19.19.1,
19.19.19.2 ///This configuration is optical in Layer 2 networking but is
recommended.
```

You can also manually assign IP addresses for APs in a batch. If this method is used, you do not need to specify the IP address range in the address pools, but you still need to configure an IP address pool and enable the DHCP server on each AC.

- Manually perform the same service configurations on the ACs. Inconsistent service configurations on the ACs will cause service switching failures.
- To prevent network storms caused by loops on the Layer 2 network, configure port isolation on AC interfaces connected to the aggregation switch or enable MSTP on the aggregation switch.

Configure port isolation on AC1.

```
[AC6605_LSW1] port-isolate mode l2
[AC6605_LSW1] interface GigabitEthernet 0/0/1
[AC6605_LSW1-GigabitEthernet0/0/1] port-isolate enable
[AC6605_LSW1] interface GigabitEthernet 0/0/2
[AC6605_LSW1-GigabitEthernet0/0/2] port-isolate enable
```

Configure port isolation on AC2.

```
[AC6605_LSW2] port-isolate mode l2
[AC6605_LSW2] interface GigabitEthernet 0/0/1
[AC6605_LSW2-GigabitEthernet0/0/1] port-isolate enable
[AC6605_LSW2] interface GigabitEthernet 0/0/2
[AC6605_LSW2-GigabitEthernet0/0/2] port-isolate enable
```

It is recommended that MSTP be enabled on the aggregation switch to prevent loops. For details on how to enable MSTP on the aggregation switch, see the configuration guide of the switch.

- In Layer 2 networking, the ACs can use only IP addresses of VLANIF interfaces as their source IP addresses to communicate with APs. In Layer 3 networking, the ACs can also use loopback addresses as source IP addresses.

- Enable the dual-link backup function on AC1 and AC2 and set a priority for each AC. Run the following commands:

```
[AC6605_AC1] wlan
[AC6605_AC1-wlan-view] wlan ac protect enable protect-ac 19.19.19.2 priority 0
[AC6605_AC2] wlan
[AC6605_AC2-wlan-view] wlan ac protect enable protect-ac 19.19.19.1 priority 7
```

- In the preceding commands, **protect-ac** specifies the IP address of the standby AC. Set this parameter to the other AC's IP address on each AC. The active AC must have a higher priority than the standby AC. The value 0 indicates the highest priority, and the value 7 indicates the lowest priority. A smaller value indicates a higher priority. Run the **display wlan ac protect** command to check the AC priorities.

```
[AC6605_AC1] display wlan ac protect
```

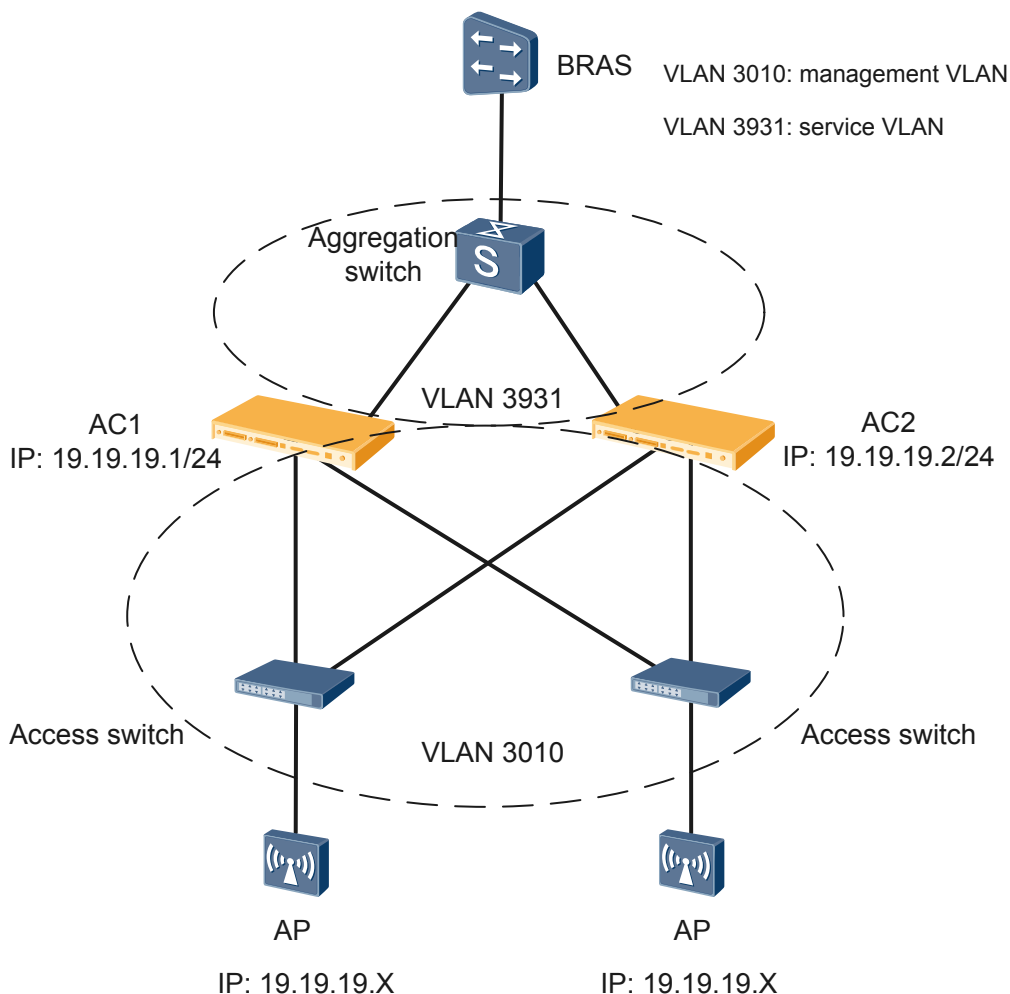
```
-----
Protect state   : enable
Protect AC     : 19.19.19.2
Priority        : 0
Protect restore : enable
-----
```

```
[AC6605_AC2] display wlan ac protect
```

```
-----
Protect state   : enable
Protect AC     : 19.19.19.1
Priority        : 7
Protect restore : enable
-----
```

Layer 2 Chain Networking (Tunnel Forwarding)

Figure 1-7 Dual-link backup in Layer 2 chain networking (tunnel forwarding)



As shown in Figure 1-7, the ACs are deployed between an aggregation switch and two access switches. Data packets from STAs are forwarded through tunnels. AC1 is the active AC, and AC2 is the standby AC.

The configuration notes in this networking are as follows:

- Configure the same AC ID and carrier ID for AC1 and AC2. Otherwise, after the active AC fails, services cannot be switched to the standby AC because BSSIDs of the two ACs are different. Run the following commands:

```
[AC6605_AC1] wlan ac-global ac id 999 carrier id ctc  
[AC6605_AC2] wlan ac-global ac id 999 carrier id ctc
```

- The ACs must deliver the same VAP to an AP. Manually add offline APs to AC1 and AC2. It is recommended that the same AP ID be configured for an AP on AC1 and AC2. Run the following commands:

```
[AC6605_AC1] wlan  
[AC6605_AC1-wlan-view] ap id 0 ap-type WA601 mac 0025-9876-2633 sn A0928182  
[AC6605_AC2] wlan
```

```
[AC6605_AC2-wlan-view] ap id 0 ap-type WA601 mac 0025-9876-2633 sn A0928182
```

- Before enabling dual-link backup, complete the tunnel configuration and commit the configuration on AC1 and AC2. If you enable dual-link backup before committing the tunnel configuration, the configuration cannot be committed on the standby AC. As a result, services cannot be switched to the standby AC after an active/standby switchover.
- To prevent IP address conflicts, ensure that the IP address pools configured for APs on AC1 and AC2 do not overlap each other.

Configure an IP address pool for APs on AC1.

```
[AC6605_AC1] ip pool ap-active
[AC6605_AC1-ip-pool-ap-active] gateway-list 19.19.19.1
[AC6605_AC1-ip-pool-ap-active] network 19.19.19.0 mask 255.255.255.0
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 19.19.19.2
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 19.19.19.151 19.19.19.254
[AC6605_AC1-ip-pool-ap-active] option 43 sub-option 3 ascii HuaweiAC-19.19.19.1,
19.19.19.2 //This configuration is optical in Layer 2 networking but is recommended.
```

Configure an IP address pool for APs on AC2.

```
[AC6605_AC2] ip pool ap-standby
[AC6605_AC2-ip-pool-ap-standby] gateway-list 19.19.19.2
[AC6605_AC2-ip-pool-ap-standby] network 19.19.19.0 mask 255.255.255.0
[AC6605_AC2-ip-pool-ap-standby] excluded-ip-address 19.19.19.1
[AC6605_AC2-ip-pool-ap-standby] excluded-ip-address 19.19.19.3 19.19.19.150
[AC6605_AC2-ip-pool-ap-standby] option 43 sub-option 3 ascii HuaweiAC-19.19.19.1,
19.19.19.2 ///This configuration is optical in Layer 2 networking but is recommended.
```

You can also manually assign IP addresses for APs in a batch. If this method is used, you do not need to specify the IP address range in the address pools, but you still need to configure an IP address pool and enable the DHCP server on each AC.

- Manually perform the same service configurations on the ACs. Inconsistent service configurations on the ACs will cause service switching failures.
- To prevent network storms caused by loops on the Layer 2 network, configure port isolation on AC interfaces connected to the aggregation switch or enable MSTP on the aggregation switch.

Configure port isolation on AC1.

```
[AC6605_LSW1]port-isolate mode l2
[AC6605_LSW1] interface GigabitEthernet 0/0/1
[AC6605_LSW1-GigabitEthernet0/0/1] port-isolate enable
[AC6605_LSW1] interface GigabitEthernet 0/0/2
[AC6605_LSW1-GigabitEthernet0/0/2] port-isolate enable
```

Configure port isolation on AC2.

```
[AC6605_LSW2]port-isolate mode l2
[AC6605_LSW2] interface GigabitEthernet 0/0/1
[AC6605_LSW2-GigabitEthernet0/0/1] port-isolate enable
[AC6605_LSW2] interface GigabitEthernet 0/0/2
[AC6605_LSW2-GigabitEthernet0/0/2] port-isolate enable
```

It is recommended that MSTP be enabled on the aggregation switch to prevent loops. For details on how to enable MSTP on the aggregation switch, see the configuration guide of the switch.

- In Layer 2 networking, the ACs can use only IP addresses of VLANIF interfaces as their source IP addresses to communicate with APs. In Layer 3 networking, the ACs can also use loopback addresses as source IP addresses.

- Enable the dual-link backup function on AC1 and AC2 and set a priority for each AC. Run the following commands:

```
[AC6605_AC1] wlan
[AC6605_AC1-wlan-view] wlan ac protect enable protect-ac 19.19.19.2 priority 0
[AC6605_AC2] wlan
[AC6605_AC2-wlan-view] wlan ac protect enable protect-ac 19.19.19.1 priority 7
```

In the preceding commands, **protect-ac** specifies the IP address of the standby AC. Set this parameter to the other AC's IP address on each AC. The active AC must have a higher priority than the standby AC. The value 0 indicates the highest priority, and the value 7 indicates the lowest priority. A smaller value indicates a higher priority. Run the **display wlan ac protect** command to check the AC priorities.

```
[AC6605_AC1] display wlan ac protect
```

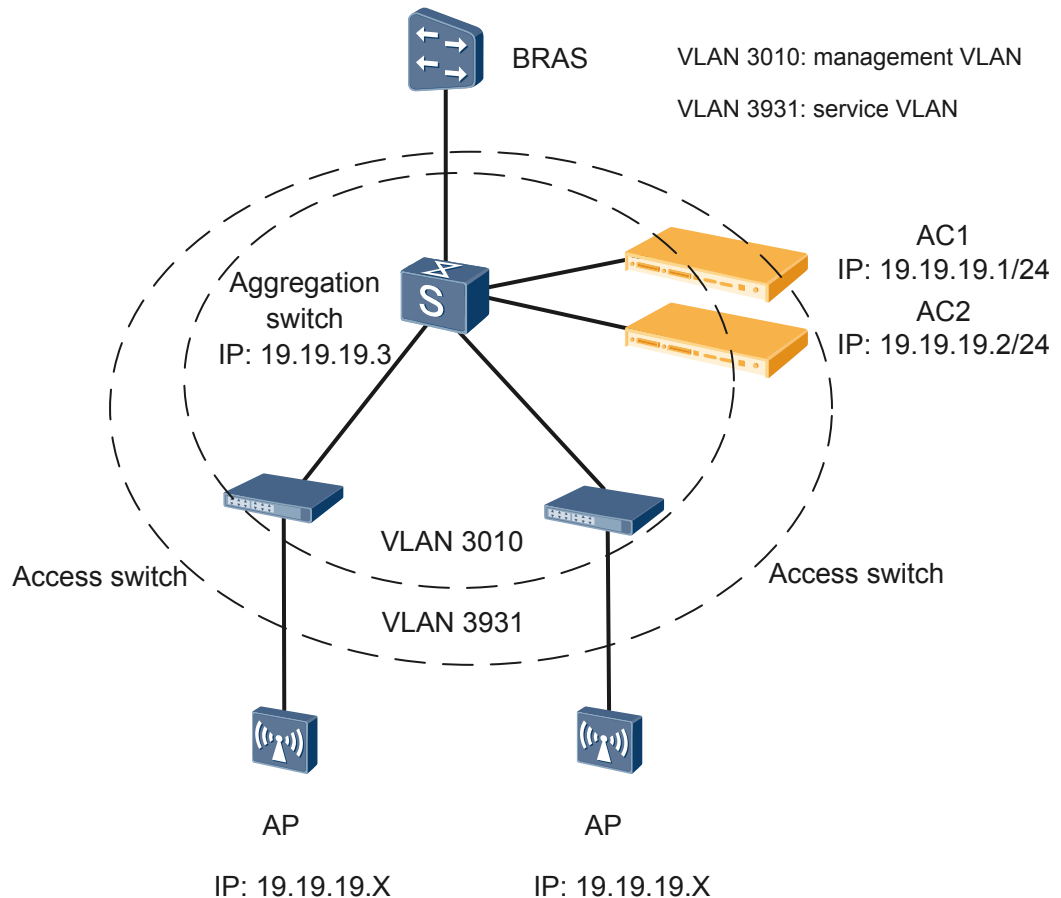
```
-----
Protect state   : enable
Protect AC     : 19.19.19.2
Priority        : 0
Protect restore : enable
-----
```

```
[AC6605_AC2] display wlan ac protect
```

```
-----
Protect state   : enable
Protect AC     : 19.19.19.1
Priority        : 7
Protect restore : enable
-----
```

Layer 2 Branched Networking (Direct Forwarding)

Figure 1-8 dual-link backup in Layer 2 branched networking (direct forwarding)



As shown in Figure 1-8, the ACs are only connected to an aggregation switch on a Layer 2 network. Data packets from STAs are forwarded in direct mode. AC1 is the active AC, and AC2 is the standby AC.

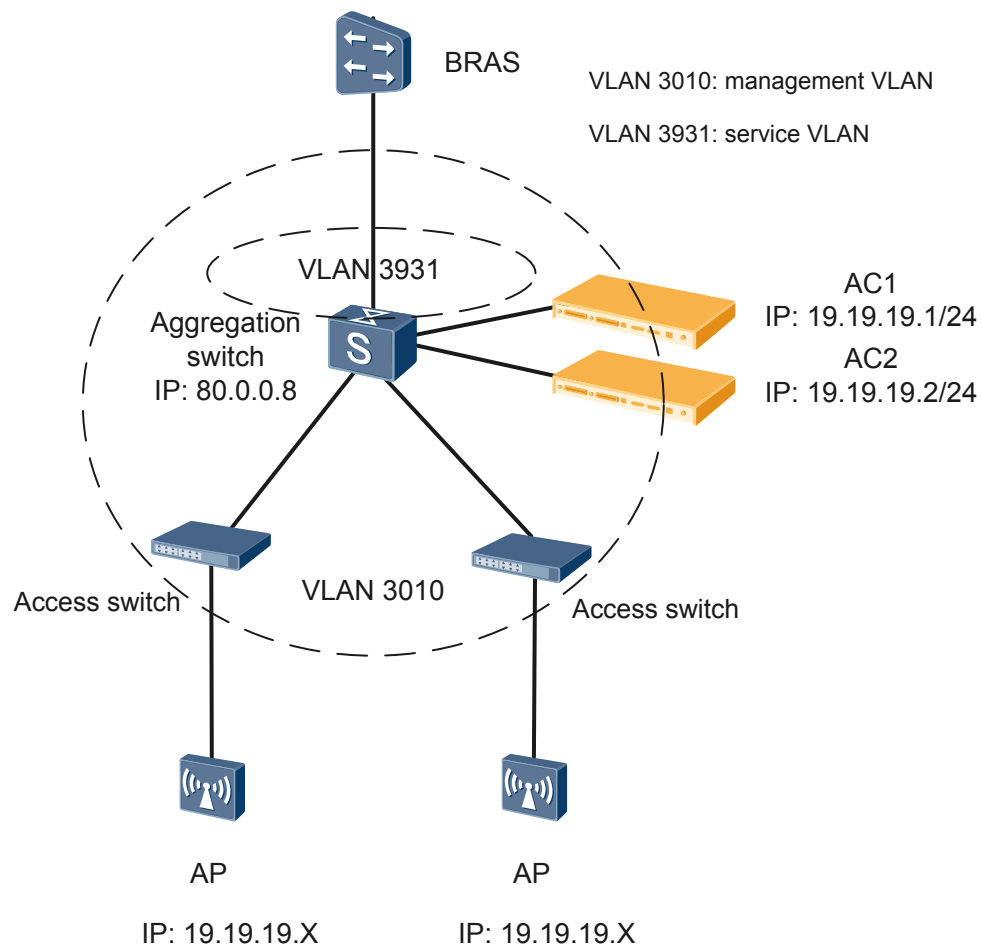
The configuration notes in this networking are as follows:

The configuration notes are the same as those in Layer 2 chain networking (direct forwarding).

In addition, the BRAS interface connected to the aggregation switch must work at Layer 2 to ensure Layer 2 communication between the ACs and APs. For the BRAS configuration, see the configuration guide of the BRAS.

Layer 2 Branched Networking (Tunnel Forwarding)

Figure 1-9 Dual-link backup in Layer 2 branched networking (tunnel forwarding)



As shown in Figure 1-9, the ACs are only connected to an aggregation switch. Data packets from STAs are forwarded through tunnels. AC1 is the active AC, and AC2 is the standby AC.

The configuration notes in this networking are as follows:

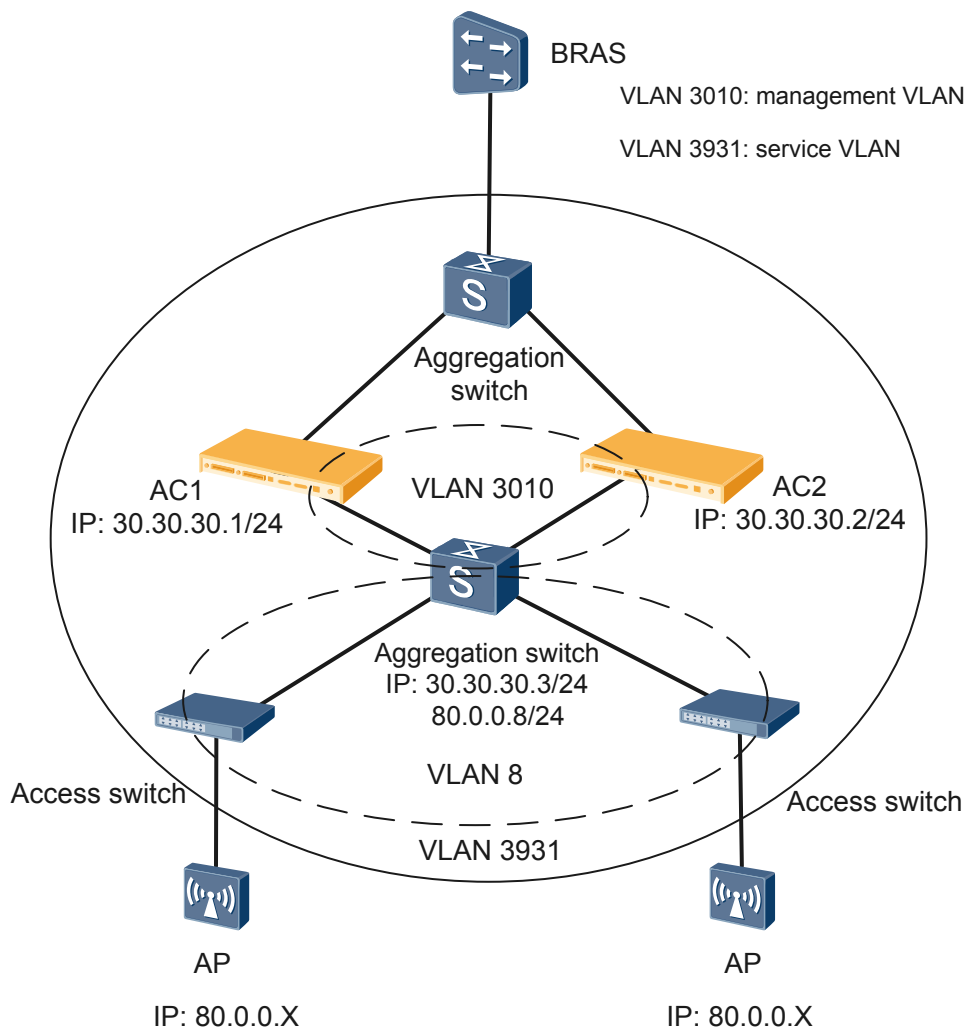
The configuration notes are the same as those in Layer 2 chain networking (tunnel forwarding).

In addition, the BRAS interface connected to the aggregation switch must work at Layer 2 to ensure Layer 2 communication between the ACs and APs. For the BRAS configuration, see the configuration guide of the BRAS.

1.3.7 Dual-Link Backup in Layer 3 Networking and Configuration Notes

Layer 3 Chain Networking (Direct Forwarding)

Figure 1-10 Dual-link backup in Layer 3 chain networking (direct forwarding)



As shown in Figure 1-10, the ACs are deployed between two aggregation switches on a Layer 3 network. Data packets from STAs are forwarded in direct mode. AC1 is the active AC, and AC2 is the standby AC.

The configuration notes in this networking are as follows:

- Configure the same AC ID and carrier ID for AC1 and AC2. Otherwise, after the active AC fails, services cannot be switched to the standby AC because BSSIDs of the two ACs are different. Run the following commands:

```
[AC6605_AC1] wlan ac-global ac id 999 carrier id ctc  
[AC6605_AC2] wlan ac-global ac id 999 carrier id ctc
```

- The ACs must deliver the same VAP to an AP. Manually add offline APs to AC1 and AC2. It is recommended that the same AP ID be configured for an AP on AC1 and AC2. Run the following commands:

```
[AC6605_AC1] wlan
[AC6605_AC1-wlan-view] ap id 0 ap-type WA601 mac 0025-9876-2633 sn A0928182
[AC6605_AC2] wlan
[AC6605_AC2-wlan-view] ap id 0 ap-type WA601 mac 0025-9876-2633 sn A0928182
```

- Configure DHCP proxy on the downstream aggregation switch and specify IP addresses of AC1 and AC2 as the DHCP server IP addresses. This configuration enables APs to obtain IP addresses from the ACs through the aggregation switch.

```
dhcp relay server-ip 30.30.30.1
dhcp relay server-ip 30.30.30.2
```

The dhcp-relay command syntax differs on different switch models. For details about this command, see the command reference of the aggregation switch. The aggregation switch must support at least two DHCP server addresses for the DHCP relay agent.

- In this example, configure a route to network segment 80.0.0.0 of the aggregation switch on each AC. Run the following commands:

```
[AC6605_AC1] ip route-static 80.0.0.0 255.255.255.0 30.30.30.3
[AC6605_AC2] ip route-static 80.0.0.0 255.255.255.0 30.30.30.3
```

The DHCP Offer packets sent from an AC can reach the APs only when the AC has a route to the network segment 80.0.0.0.

- To prevent IP address conflicts, ensure that the IP address pools configured for APs on AC1 and AC2 do not overlap each other.

Configure an IP address pool for APs on AC1.

```
[AC6605_AC1] ip pool ap-active
[AC6605_AC1-ip-pool-ap-active] gateway-list 80.0.0.8
[AC6605_AC1-ip-pool-ap-active] network 80.0.0.0 mask 255.255.255.0
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 80.0.0.1 80.0.0.7
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 80.0.0.9 80.0.0.19
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 80.0.0.101 80.0.0.254
[AC6605_AC1-ip-pool-ap-active] option 43 sub-option 3 ascii
HuaweiAC-30.30.30.1,30.30.30.2 //This configuration is mandatory in Layer 3
networking.
```

Configure an IP address pool for APs on AC2.

```
[AC6605_AC2] ip pool ap-active
[AC6605_AC2-ip-pool-ap-active] gateway-list 80.0.0.8
[AC6605_AC2-ip-pool-ap-active] network 80.0.0.0 mask 255.255.255.0
[AC6605_AC2-ip-pool-ap-active] excluded-ip-address 80.0.0.1 80.0.0.7
[AC6605_AC2-ip-pool-ap-active] excluded-ip-address 80.0.0.9 80.0.0.100
[AC6605_AC2-ip-pool-ap-active] excluded-ip-address 80.0.0.201 80.0.0.254
[AC6605_AC2-ip-pool-ap-active] option 43 sub-option 3 ascii
HuaweiAC-30.30.30.1,30.30.30.2 ///This configuration is mandatory in Layer 3
networking.
```

You can also manually assign IP addresses for APs in a batch. If this method is used, you do not need to specify the IP address range in the address pools, but you still need to configure an IP address pool and enable the DHCP server on each AC.

- Manually perform the same service configurations on the ACs. Inconsistent service configurations on the ACs will cause service switching failures.
- In Layer 3 networking, AC1 and AC2 can use loopback IP addresses as source IP addresses to communicate with APs. Source IP addresses of the ACs can be located on

different network segments. The DHCP function must be enabled on VLANIF interfaces instead of the loopback interfaces to allocate IP addresses to APs.

- Enable the dual-link backup function on AC1 and AC2 and set a priority for each AC. Run the following commands:

```
[AC6605_AC1] wlan
[AC6605_AC1-wlan-view] wlan ac protect enable protect-ac 30.30.30.2 priority 0
[AC6605_AC2] wlan
[AC6605_AC2-wlan-view] wlan ac protect enable protect-ac 30.30.30.1 priority 7
```

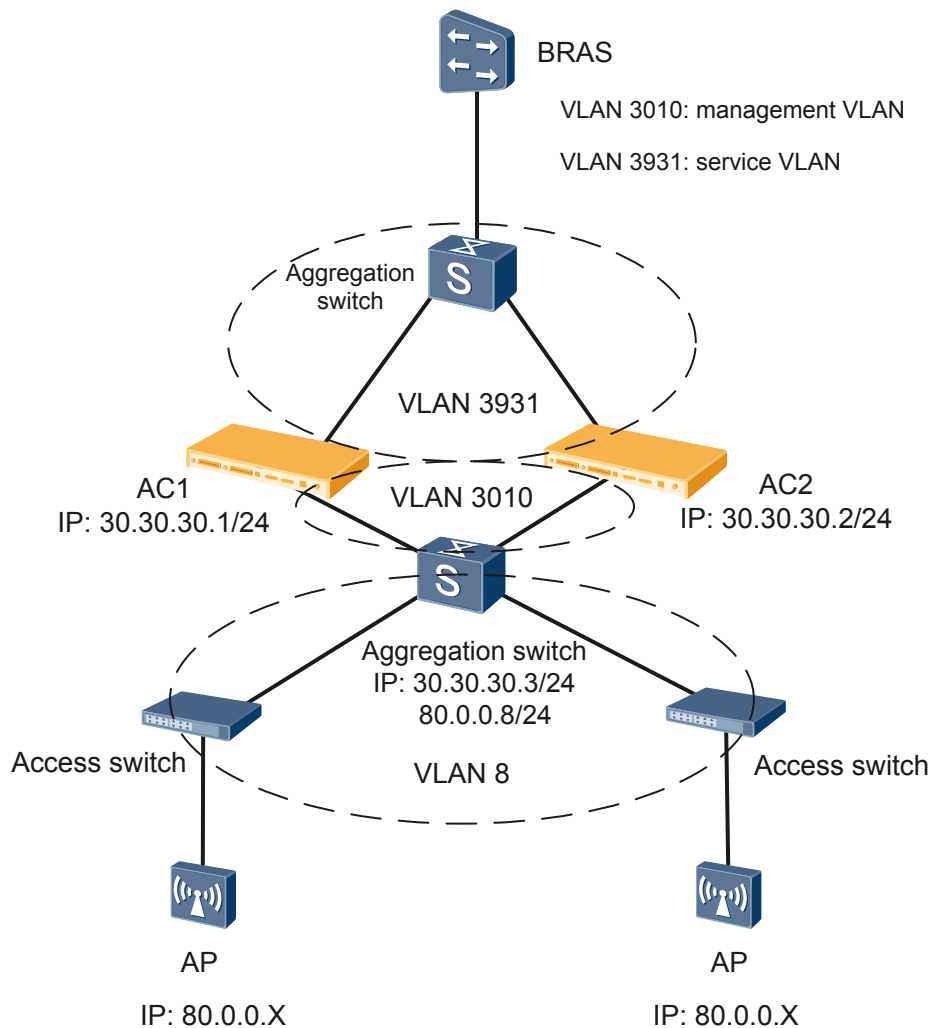
In the preceding commands, **protect-ac** specifies the IP address of the standby AC. Set this parameter to the other AC's IP address on each AC. The active AC must have a higher priority than the standby AC. The value 0 indicates the highest priority, and the value 7 indicates the lowest priority. A smaller value indicates a higher priority. Run the **display wlan ac protect** command to check the AC priorities.

```
[AC6605_AC1] display wlan ac protect
-----
Protect state   : enable
Protect AC     : 30.30.30.2
Priority        : 0
Protect restore : enable
-----

[AC6605_AC2] display wlan ac protect
-----
Protect state   : enable
Protect AC     : 30.30.30.1
Priority        : 7
Protect restore : enable
-----
```

Layer 3 Chain Networking (Tunnel Forwarding)

Figure 1-11 Dual-link backup in Layer 3 chain networking (tunnel forwarding)



As shown in Figure 1-11, the ACs are deployed between two aggregation switches on a Layer 3 network. Data packets from STAs are forwarded through tunnels. AC1 is the active AC, and AC2 is the standby AC.

The configuration notes in this networking are as follows:

- Configure the same AC ID and carrier ID for AC1 and AC2. Otherwise, after the active AC fails, services cannot be switched to the standby AC because BSSIDs of the two ACs are different. Run the following commands:

```
[AC6605_AC1] wlan ac-global ac id 999 carrier id ctc  
[AC6605_AC2] wlan ac-global ac id 999 carrier id ctc
```

- The ACs must deliver the same VAP to an AP. Manually add offline APs to AC1 and AC2. It is recommended that the same AP ID be configured for an AP on AC1 and AC2. Run the following commands:

```
[AC6605_AC1] wlan  
[AC6605_AC1-wlan-view] ap id 0 ap-type WA601 mac 0025-9876-2633 sn A0928182
```

```
[AC6605_AC2] wlan
[AC6605_AC2-wlan-view] ap id 0 ap-type WA601 mac 0025-9876-2633 sn A0928182
```

- Before enabling dual-link backup, complete the tunnel configuration and commit the configuration on AC1 and AC2. If you enable dual-link backup before committing the tunnel configuration, the configuration cannot be committed on the standby AC. As a result, services cannot be switched to the standby AC after an active/standby switchover.
- Configure DHCP proxy on the downstream aggregation switch and specify IP addresses of AC1 and AC2 as the DHCP server IP addresses. This configuration enables APs to obtain IP addresses from the ACs through the aggregation switch.

```
dhcp relay server-ip 30.30.30.1
dhcp relay server-ip 30.30.30.2
```

The dhcp-relay command syntax differs on different switch models. For details about this command, see the command reference of the aggregation switch. The aggregation switch must support at least two DHCP server addresses for the DHCP relay agent.

- In this example, configure a route to network segment 80.0.0.0 of the aggregation switch on each AC. Run the following commands:

```
[AC6605_AC1] ip route-static 80.0.0.0 255.255.255.0 30.30.30.3
[AC6605_AC2] ip route-static 80.0.0.0 255.255.255.0 30.30.30.3
```

The DHCP Offer packets sent from an AC can reach the APs only when the AC has a route to the network segment 80.0.0.0.

- To prevent IP address conflicts, ensure that the IP address pools configured for APs on AC1 and AC2 do not overlap each other.

Configure an IP address pool for APs on AC1.

```
[AC6605_AC1] ip pool ap-active
[AC6605_AC1-ip-pool-ap-active] gateway-list 80.0.0.8
[AC6605_AC1-ip-pool-ap-active] network 80.0.0.0 mask 255.255.255.0
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 80.0.0.1 80.0.0.7
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 80.0.0.9 80.0.0.19
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 80.0.0.101 80.0.0.254

[AC6605_AC1-ip-pool-ap-active] option 43 sub-option 3 ascii
HuaweiAC-30.30.30.1,30.30.30.2 //This configuration is mandatory in Layer 3
networking.
```

Configure an IP address pool for APs on AC2.

```
[AC6605_AC2] ip pool ap-active
[AC6605_AC2-ip-pool-ap-active] gateway-list 80.0.0.8
[AC6605_AC2-ip-pool-ap-active] network 80.0.0.0 mask 255.255.255.0
[AC6605_AC2-ip-pool-ap-active] excluded-ip-address 80.0.0.1 80.0.0.7
[AC6605_AC2-ip-pool-ap-active] excluded-ip-address 80.0.0.9 80.0.0.100
[AC6605_AC2-ip-pool-ap-active] excluded-ip-address 80.0.0.201 80.0.0.254

[AC6605_AC2-ip-pool-ap-active] option 43 sub-option 3 ascii
HuaweiAC-30.30.30.1,30.30.30.2 ///This configuration is mandatory in Layer 3
networking.
```

You can also manually assign IP addresses for APs in a batch. If this method is used, you do not need to specify the IP address range in the address pools, but you still need to configure an IP address pool and enable the DHCP server on each AC.

- Manually perform the same service configurations on the ACs. Inconsistent service configurations on the ACs will cause service switching failures.
- In Layer 3 networking, AC1 and AC2 can use loopback IP addresses as source IP addresses to communicate with APs. Source IP addresses of the ACs can be located on

different network segments. The DHCP function must be enabled on VLANIF interfaces instead of the loopback interfaces to allocate IP addresses to APs.

- Enable the dual-link backup function on AC1 and AC2 and set a priority for each AC. Run the following commands:

```
[AC6605_AC1] wlan
[AC6605_AC1-wlan-view] wlan ac protect enable protect-ac 30.30.30.2 priority 0
[AC6605_AC2] wlan
[AC6605_AC2-wlan-view] wlan ac protect enable protect-ac 30.30.30.1 priority 7
```

In the preceding commands, **protect-ac** specifies the IP address of the standby AC. Set this parameter to the other AC's IP address on each AC. The active AC must have a higher priority than the standby AC. The value 0 indicates the highest priority, and the value 7 indicates the lowest priority. A smaller value indicates a higher priority. Run the **display wlan ac protect** command to check the AC priorities.

```
[AC6605_AC1] display wlan ac protect
```

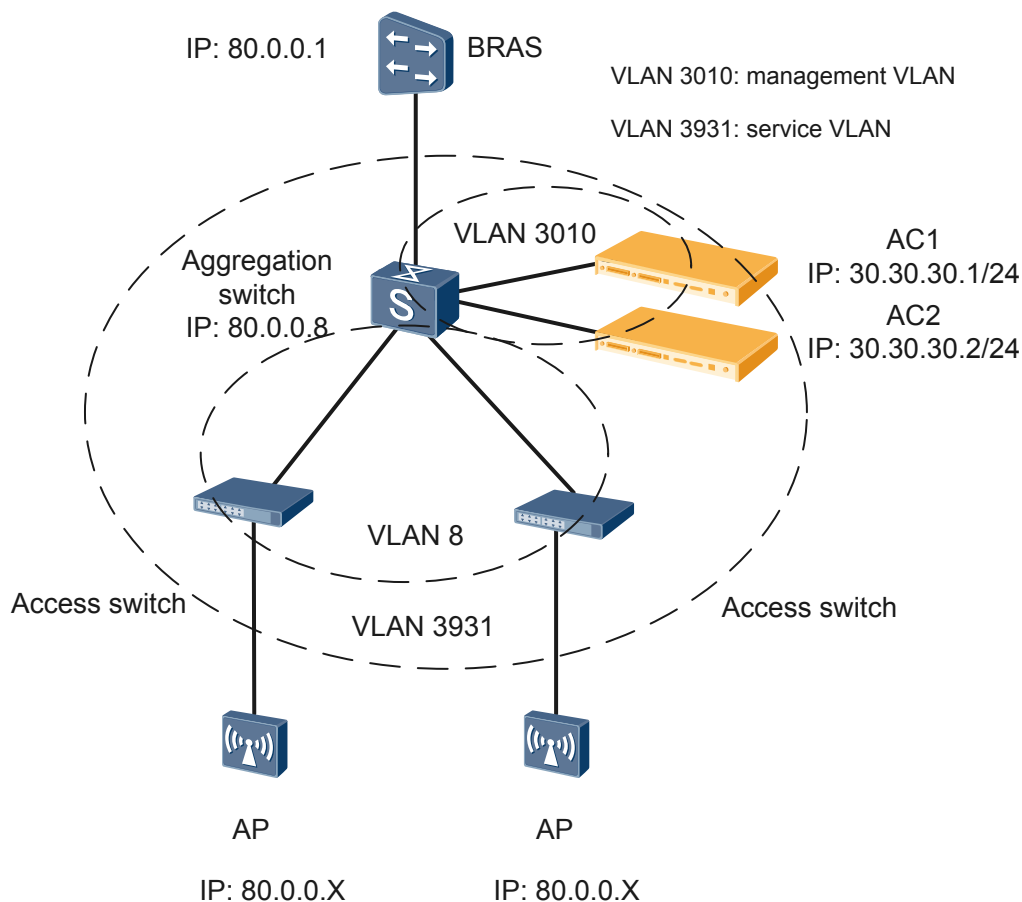
```
-----
Protect state   : enable
Protect AC     : 30.30.30.2
Priority        : 0
Protect restore : enable
-----
```

```
[AC6605_AC2] display wlan ac protect
```

```
-----
Protect state   : enable
Protect AC     : 30.30.30.1
Priority        : 7
Protect restore : enable
-----
```

Layer 3 Branched Networking (Direct Forwarding)

Figure 1-12 Dual-link backup in Layer 3 branched networking (direct forwarding)



As shown in Figure 1-12, the ACs are only connected to an aggregation switch on a Layer 3 network. Data packets from STAs are forwarded in direct mode. AC1 is the active AC, and AC2 is the standby AC.

The configuration notes in this networking are as follows:

- Configure the same AC ID and carrier ID for AC1 and AC2. Otherwise, after the active AC fails, services cannot be switched to the standby AC because BSSIDs of the two ACs are different. Run the following commands:

```
[AC6605_AC1] wlan ac-global ac id 999 carrier id ctc
[AC6605_AC2] wlan ac-global ac id 999 carrier id ctc
```

- The ACs must deliver the same VAP to an AP. Manually add offline APs to AC1 and AC2. It is recommended that the same AP ID be configured for an AP on AC1 and AC2. Run the following commands:

```
[AC6605_AC1] wlan
[AC6605_AC1-wlan-view] ap id 0 ap-type WA601 mac 0025-9876-2633 sn A0928182
[AC6605_AC2] wlan
[AC6605_AC2-wlan-view] ap id 0 ap-type WA601 mac 0025-9876-2633 sn A0928182
```

- Configure DHCP proxy on the downstream aggregation switch and specify IP addresses of AC1 and AC2 as the DHCP server IP addresses. This configuration enables APs to obtain IP addresses from the ACs through the aggregation switch.

```
dhcp relay server-ip 30.30.30.1  
dhcp relay server-ip 30.30.30.2
```

The `dhcp-relay` command syntax differs on different switch models. For details about this command, see the command reference of the aggregation switch. The aggregation switch must support at least two DHCP server addresses for the DHCP relay agent. The DHCP relay function can also be configured on the BRAS. For details about the configuration method, see the command reference of the BRAS.

- In this example, configure a route to network segment 80.0.0.0 of the aggregation switch on each AC. Run the following commands:

```
[AC6605_AC1] ip route-static 80.0.0.0 255.255.255.0 30.30.30.3  
[AC6605_AC2] ip route-static 80.0.0.0 255.255.255.0 30.30.30.3
```

The DHCP Offer packets sent from an AC can reach the APs only when the AC has a route to the network segment 80.0.0.0.

- To prevent IP address conflicts, ensure that the IP address pools configured for APs on AC1 and AC2 do not overlap each other.

Configure an IP address pool for APs on AC1.

```
[AC6605_AC1] ip pool ap-active  
[AC6605_AC1-ip-pool-ap-active] gateway-list 80.0.0.8  
[AC6605_AC1-ip-pool-ap-active] network 80.0.0.0 mask 255.255.255.0  
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 80.0.0.1 80.0.0.7  
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 80.0.0.9 80.0.0.19  
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 80.0.0.101 80.0.0.254
```

```
[AC6605_AC1-ip-pool-ap-active] option 43 sub-option 3 ascii  
HuaweiAC-30.30.30.1,30.30.30.2 //This configuration is mandatory in Layer 3  
networking.
```

Configure an IP address pool for APs on AC2.

```
[AC6605_AC2] ip pool ap-active  
[AC6605_AC2-ip-pool-ap-active] gateway-list 80.0.0.8  
[AC6605_AC2-ip-pool-ap-active] network 80.0.0.0 mask 255.255.255.0  
[AC6605_AC2-ip-pool-ap-active] excluded-ip-address 80.0.0.1 80.0.0.7  
[AC6605_AC2-ip-pool-ap-active] excluded-ip-address 80.0.0.9 80.0.0.100  
[AC6605_AC2-ip-pool-ap-active] excluded-ip-address 80.0.0.201 80.0.0.254
```

```
[AC6605_AC2-ip-pool-ap-active] option 43 sub-option 3 ascii  
HuaweiAC-30.30.30.1,30.30.30.2 ///This configuration is mandatory in Layer 3  
networking.
```

You can also manually assign IP addresses for APs in a batch. If this method is used, you do not need to specify the IP address range in the address pools, but you still need to configure an IP address pool and enable the DHCP server on each AC.

- Manually perform the same service configurations on the ACs. Inconsistent service configurations on the ACs will cause service switching failures.
- In Layer 3 networking, AC1 and AC2 can use loopback IP addresses as source IP addresses to communicate with APs. Source IP addresses of the ACs can be located on different network segments. The DHCP function must be enabled on VLANIF interfaces instead of the loopback interfaces to allocate IP addresses to APs.
- Enable the dual-link backup function on AC1 and AC2 and set a priority for each AC. Run the following commands:

```
[AC6605_AC1] wlan
```

```
[AC6605_AC1-wlan-view] wlan ac protect enable protect-ac 30.30.30.2 priority 0
[AC6605_AC2] wlan
[AC6605_AC2-wlan-view] wlan ac protect enable protect-ac 30.30.30.1 priority 7
```

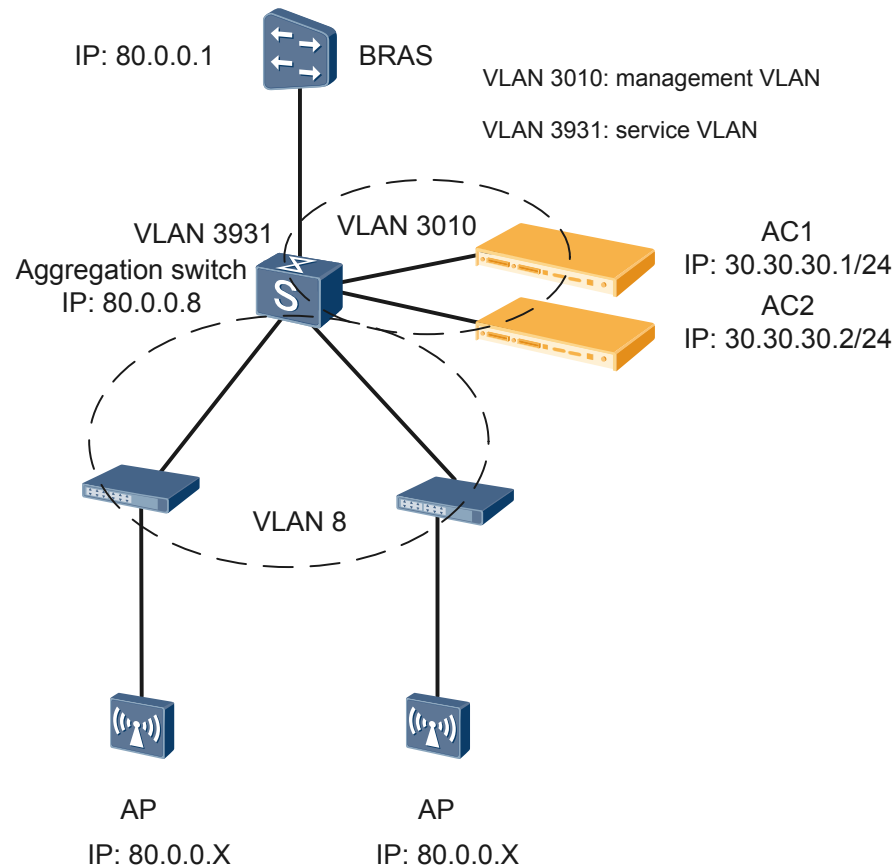
In the preceding commands, **protect-ac** specifies the IP address of the standby AC. Set this parameter to the other AC's IP address on each AC. The active AC must have a higher priority than the standby AC. The value 0 indicates the highest priority, and the value 7 indicates the lowest priority. A smaller value indicates a higher priority. Run the **display wlan ac protect** command to check the AC priorities.

```
[AC6605_AC1] display wlan ac protect
-----
Protect state   : enable
Protect AC     : 30.30.30.2
Priority        : 0
Protect restore : enable
-----

[AC6605_AC2] display wlan ac protect
-----
Protect state   : enable
Protect AC     : 30.30.30.1
Priority        : 7
Protect restore : enable
-----
```

Layer 3 Branched Networking (Tunnel Forwarding)

Figure 1-13 Dual-link backup in Layer 3 branched networking (tunnel forwarding)



As shown in Figure 1-13, the ACs are deployed between two aggregation switches on a Layer 3 network. Data packets from STAs are forwarded through tunnels. AC1 is the active AC, and AC2 is the standby AC.

The configuration notes in this networking are as follows:

- Configure the same AC ID and carrier ID for AC1 and AC2. Otherwise, after the active AC fails, services cannot be switched to the standby AC because BSSIDs of the two ACs are different. Run the following commands:

```
[AC6605_AC1] wlan ac-global ac id 999 carrier id ctc  
[AC6605_AC2] wlan ac-global ac id 999 carrier id ctc
```

- The ACs must deliver the same VAP to an AP. Manually add offline APs to AC1 and AC2. It is recommended that the same AP ID be configured for an AP on AC1 and AC2. Run the following commands:

```
[AC6605_AC1] wlan  
[AC6605_AC1-wlan-view] ap id 0 ap-type WA601 mac 0025-9876-2633 sn A0928182  
[AC6605_AC2] wlan  
[AC6605_AC2-wlan-view] ap id 0 ap-type WA601 mac 0025-9876-2633 sn A0928182
```

- Before enabling dual-link backup, complete the tunnel configuration and commit the configuration on AC1 and AC2. If you enable dual-link backup before committing the

tunnel configuration, the configuration cannot be committed on the standby AC. As a result, the tunnel interface cannot be enabled and therefore services cannot be switched to the standby AC after an active/standby switchover.

- Configure DHCP proxy on the downstream aggregation switch and specify IP addresses of AC1 and AC2 as the DHCP server IP addresses. This configuration enables APs to obtain IP addresses from the ACs through the aggregation switch.

```
dhcp relay server-ip 30.30.30.1
dhcp relay server-ip 30.30.30.2
```

The dhcp-relay command syntax differs on different switch models. For details about this command, see the command reference of the aggregation switch. The aggregation switch must support at least two DHCP server addresses for the DHCP relay agent. The DHCP relay function can also be configured on the BRAS. For details about the configuration method, see the command reference of the BRAS.

- In this example, configure a route to network segment 80.0.0.0 of the aggregation switch on each AC. Run the following commands:

```
[AC6605_AC1] ip route-static 80.0.0.0 255.255.255.0 30.30.30.3
[AC6605_AC2] ip route-static 80.0.0.0 255.255.255.0 30.30.30.3
```

The DHCP Offer packets sent from an AC can reach the APs only when the AC has a route to the network segment 80.0.0.0.

- To prevent IP address conflicts, ensure that the IP address pools configured for APs on AC1 and AC2 do not overlap each other.

Configure an IP address pool for APs on AC1.

```
[AC6605_AC1] ip pool ap-active
[AC6605_AC1-ip-pool-ap-active] gateway-list 80.0.0.8
[AC6605_AC1-ip-pool-ap-active] network 80.0.0.0 mask 255.255.255.0
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 80.0.0.1 80.0.0.7
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 80.0.0.9 80.0.0.19
[AC6605_AC1-ip-pool-ap-active] excluded-ip-address 80.0.0.101 80.0.0.254
[AC6605_AC1-ip-pool-ap-active] option 43 sub-option 3 ascii
HuaweiAC-30.30.30.1,30.30.30.2 //This configuration is mandatory in Layer 3
networking.
```

Configure an IP address pool for APs on AC2.

```
[AC6605_AC2] ip pool ap-active
[AC6605_AC2-ip-pool-ap-active] gateway-list 80.0.0.8
[AC6605_AC2-ip-pool-ap-active] network 80.0.0.0 mask 255.255.255.0
[AC6605_AC2-ip-pool-ap-active] excluded-ip-address 80.0.0.1 80.0.0.7
[AC6605_AC2-ip-pool-ap-active] excluded-ip-address 80.0.0.9 80.0.0.100
[AC6605_AC2-ip-pool-ap-active] excluded-ip-address 80.0.0.201 80.0.0.254
[AC6605_AC2-ip-pool-ap-active] option 43 sub-option 3 ascii
HuaweiAC-30.30.30.1,30.30.30.2 ///This configuration is mandatory in Layer 3
networking.
```

You can also manually assign IP addresses for APs in a batch. If this method is used, you do not need to specify the IP address range in the address pools, but you still need to configure an IP address pool and enable the DHCP server on each AC.

- Manually perform the same service configurations on the ACs. Inconsistent service configurations on the ACs will cause service switching failures.
- In Layer 3 networking, AC1 and AC2 can use loopback IP addresses as source IP addresses to communicate with APs. Source IP addresses of the ACs can be located on different network segments. The DHCP function must be enabled on VLANIF interfaces instead of the loopback interfaces to allocate IP addresses to APs.

- Enable the dual-link backup function on AC1 and AC2 and set a priority for each AC. Run the following commands:

```
[AC6605_AC1] wlan
[AC6605_AC1-wlan-view] wlan ac protect enable protect-ac 30.30.30.2 priority 0
[AC6605_AC2] wlan
[AC6605_AC2-wlan-view] wlan ac protect enable protect-ac 30.30.30.1 priority 7
```

In the preceding commands, **protect-ac** specifies the IP address of the standby AC. Set this parameter to the other AC's IP address on each AC. The active AC must have a higher priority than the standby AC. The value 0 indicates the highest priority, and the value 7 indicates the lowest priority. A smaller value indicates a higher priority. Run the **display wlan ac protect** command to check the AC priorities.

```
[AC6605_AC1] display wlan ac protect
```

```
-----
Protect state   : enable
Protect AC     : 30.30.30.2
Priority       : 0
Protect restore : enable
-----
```

```
[AC6605_AC2] display wlan ac protect
```

```
-----
Protect state   : enable
Protect AC     : 30.30.30.1
Priority       : 7
Protect restore : enable
-----
```

1.4 Applications

1.4.1 Direct Forwarding in Layer 3 Chain Networking

As shown in Figure 1-14, two ACs are deployed in a Layer 3 chain networking and work in dual-link backup mode to improve network reliability and ensure stable wireless services. Data packets from STAs are directly forwarded. This networking mode simplifies the network architecture and applies to large-scale WLANs where APs are deployed in a centralized manner. An AC manages APs in multiple LANs but does not belong to any of the LANs.

AC1 is the active AC, and AC2 is the standby AC. It is recommended that you manually add offline APs to the ACs. Perform the same service configurations (including user authentication configuration) on the two ACs.

Configuration on the ACs is as follows:

- Configure management VLAN 3010 and service VLAN 3931 for APs. Set the management IP address of AC1 to 30.30.30.1, and management IP address of AC2 to 30.30.30.2. Enable DHCP on AC1 and AC2.
- Configure the same carrier ID for the ACs. Enable dual-link backup and configure IP addresses and priorities for the ACs. Ensure that the active AC has a higher priority (smaller priority value) than the standby AC.
- Configure non-overlapping IP address pools on the ACs. In this example, the IP address pool on AC1 contains IP addresses 40.40.40.3 to 40.40.40.100, IP address pool on AC2 contains IP addresses on AC2 is 40.40.40.101 to 40.40.40.254. Set the gateway address

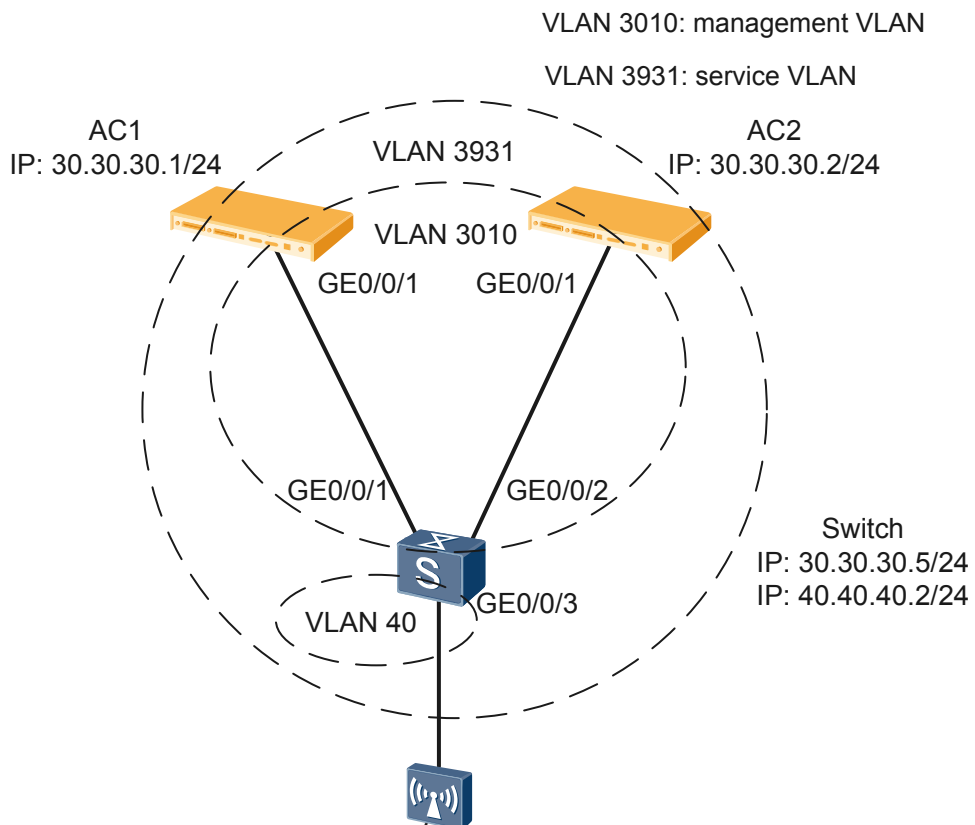
of the IP address pools to 40.40.40.2, which is the IP address of VLANIF40. (Interfaces between the switch and AP belong to VLAN 40).

- Configure the Option 43 field with the IP addresses of the active and standby ACs. Configure static routes from the ACs to the switch.

Configuration on the switch is as follows:

- Create VLANs 40, 3010, and 3931. Assign IP address 40.40.40.2 to VLANIF40 and assign IP address 30.30.30.5 to VLANIF 3010. The switch uses the IP address of VLANIF40 to communicate with APs. VLAN 3010 is the management VLAN of APs.
- Enable DHCP relay and specify IP addresses of the two ACs as the DHCP server addresses for the DHCP relay agent.
- Set the default VLAN of GigabitEthernet 0/0/1 and GigabitEthernet 0/0/2 to VLAN 3010, and configure the two interfaces to allow VLAN40, VLAN 3010 and VLAN 3931. Set the default VLAN of GigabitEthernet 0/0/3 to VLAN 40 and configure the interface to all VLANs.

Figure 1-14 Dual-link backup in Layer 3 chain networking (direct forwarding)



Wireless-side configuration file of AC1

```
#
sysname AC1
#
vlan batch 40 3010 3931
#
```

```
wlan ac-global carrier id cmcc ac id 999
#
dhcp enable
#
ip pool ap
gateway-list 40.40.40.2
network 40.40.40.0 mask 255.255.255.0
excluded-ip-address 40.40.40.1
excluded-ip-address 40.40.40.101 40.40.40.254
option 43 ascii HuaweiAC-30.30.30.1,30.30.30.2
#
interface Vlanif3010
ip address 30.30.30.1 255.255.255.0
dhcp select interface
#
interface XGigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 40 3010 3931
#
ip route-static 40.40.40.0 255.255.255.0 30.30.30.5
#
wlan
wlan ac source interface Vlanif3010
wlan ac protect enable protect-ac 30.30.30.2
#
return
```

Wired-side configuration file of AC1

```
#
sysname lsw_AC1
#
vlan batch 40 3010 3931
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 3010
port trunk allow-pass vlan 40 3010 3931
#
interface XGigabitEthernet0/0/27
port link-type trunk
port trunk allow-pass vlan 40 3010 3931
#
return
```

Wireless-side configuration file of AC2

```
#
sysname AC2
#
vlan batch 40 3010 3931
#
wlan ac-global carrier id cmcc ac id 999
#
dhcp enable
#
ip pool ap
```

```
gateway-list 40.40.40.2
network 40.40.40.0 mask 255.255.255.0
excluded-ip-address 40.40.40.1
excluded-ip-address 40.40.40.3 40.40.40.100
option 43 ascii HuaweiAC-30.30.30.1,30.30.30.2
#
interface Vlanif3010
ip address 30.30.30.2 255.255.255.0
dhcp select interface
#
interface XGigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 40 3010 3931
#
ip route-static 40.40.40.0 255.255.255.0 30.30.30.5
#
wlan
wlan ac source interface Vlanif3010
wlan ac protect enable protect-ac 30.30.30.1 priority 7
#
return
```

Wired-side configuration file of AC2

```
#
sysname lsw_AC2
#
vlan batch 40 3010 3931
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 3010
port trunk allow-pass vlan 40 3010 3931
#
interface XGigabitEthernet0/0/27
port link-type trunk
port trunk allow-pass vlan 40 3010 3931
#
return
```

Configuration file of the switch

```
#
sysname Quidway
#
vlan batch 40 3010 3931
#
interface Vlanif40
ip address 40.40.40.2 255.255.255.0
dhcp select relay
dhcp relay server-ip 30.30.30.1
dhcp relay server-ip 30.30.30.2
dhcp relay information enable
#
interface Vlanif3010
ip address 30.30.30.5 255.255.255.0
#
```

```
interface GigabitEthernet0/0/1
  description connect to active AC
  port link-type trunk
  port trunk pvid vlan 3010
  port trunk allow-pass vlan 40 3010 3931
#
interface GigabitEthernet0/0/2
  description connect to standby AC
  port link-type trunk
  port trunk pvid vlan 3010
  port trunk allow-pass vlan 40 3010 3931
#
interface GigabitEthernet0/0/3
  description connect to AP
  port link-type trunk
  port trunk pvid vlan 40
  port trunk allow-pass vlan 2 to 4094
#
return
```

The preceding configuration files show the basic configurations used for dual-link backup in Layer 3 chain networking. You can configure services on the ACs and the switch after completing the preceding configurations.

1.4.2 Tunnel Forwarding in Layer 2 Branched Networking

As shown in Figure 1-15, two ACs are deployed in a Layer 2 branched networking and work dual-link backup mode to improve network reliability and ensure stable wireless services. Data packets from STAs are forwarded through tunnels. This networking applies to WLAN networks where ACs are deployed close to each other and APs are distributed dispersedly. The ACs belong to the same LAN as APs, and IP addresses of ACs and APs are on the same network segment. This networking does not require high AC performance.

AC1 is the active AC, and AC2 is the standby AC. It is recommended that you manually add offline APs to the ACs. Perform the same service configurations (including user authentication configuration) on the two ACs. Before enabling dual-link backup, complete the tunnel configuration and commit the configuration on AC1 and AC2. If you enable dual-link backup before committing the tunnel configuration, the configuration cannot be committed on the standby AC. As a result, the tunnel interface cannot be enabled and therefore services cannot be switched to the standby AC after an active/standby switchover.

Configuration on the ACs is as follows:

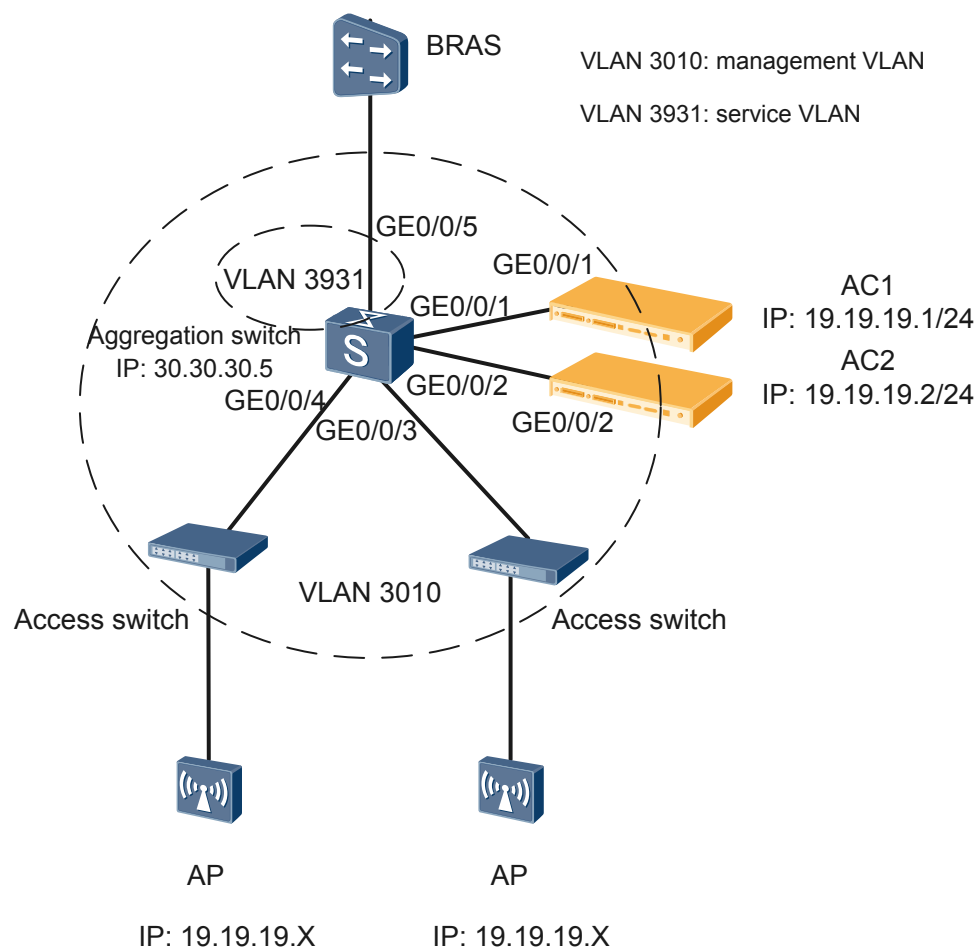
- Configure management VLAN 3010 and service VLAN 3931 for APs. Set the management IP address of AC1 to 19.19.19.1, and management IP address of AC2 to 19.19.19.2. Enable DHCP on AC1 and AC2.
- Configure the same carrier ID for the ACs. Set the data forwarding mode to tunnel forwarding. Enable dual-link backup and configure IP addresses and priorities for the ACs. Ensure that the active AC has a higher priority (smaller priority value) than the standby AC.
- Configure non-overlapping IP address pools on the ACs. In this example, the IP address pool on AC1 contains IP addresses 19.19.19.3 to 19.19.19.100, and the IP address pool on AC2 contains IP addresses 19.19.19.101 to 19.19.19.254. Set the gateway address of the IP address pool on AC1 to 19.19.19.1, and set the gateway address of the IP address pool on AC2 to 19.19.19.2.

- Configure the Option 43 field with the IP addresses of the active and standby ACs, and configure the Option 60 field to identify Huawei APs. Option 43 and Option 60 are optional in Layer 2 networking.

Configuration on the aggregation switch is as follows:

- Configure VLAN 3010 and VLAN 3931, and assign IP address 30.30.30.5 to VLANIF 3010. VLAN 3010 is the management VLAN of APs, and VLAN 3931 is the service VLAN of APs.
- Set the default VLAN of GigabitEthernet 0/0/1, GigabitEthernet 0/0/2, GigabitEthernet 0/0/3, GigabitEthernet 0/0/4, and GigabitEthernet 0/0/5 to VLAN 3010. Configure interfaces GigabitEthernet 0/0/1 through GigabitEthernet 0/0/4 to allow VLAN 3010, and configure GigabitEthernet 0/0/5 to allow VLAN 3010 and VLAN 3931.

Figure 1-15 Dual-link backup in Layer 3 branched networking (tunnel forwarding)



Wireless-side configuration file of AC1

```
#
sysname AC1
#
vlan batch 3010 3931
#
```

```
wlan ac-global carrier id cmcc ac id 999
#
dhcp enable
#
ip pool ap
gateway-list 19.19.19.1
network 19.19.19.0 mask 255.255.255.0
excluded-ip-address 19.19.19.2
excluded-ip-address 19.19.19.101 19.19.19.254
option 43 ascii HuaweiAC-19.19.19.1,19.19.19.2
interface Vlanif3010
ip address 19.19.19.1 255.255.255.0
dhcp select interface
#
interface XGigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 3010 3931
#
wlan
wlan ac source interface Vlanif3010
wlan ac protect enable protect-ac 19.19.19.2
service-set name set1 id 1
forward-mode tunnel
service-vlan 3931
#
return
```

Wired-side configuration file of AC1

```
#
sysname lsw_AC1
#
vlan batch 3010 3931
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 3010
port trunk allow-pass vlan 3010
#
interface XGigabitEthernet0/0/27
port link-type trunk
port trunk allow-pass vlan 3010 3931
#
return
```

Wireless-side configuration file of AC2

```
#
sysname AC2
#
vlan batch 3010 3931
#
wlan ac-global carrier id cmcc ac id 999
#
dhcp enable
#
ip pool ap
```



```
gateway-list 19.19.19.2
network 19.19.19.0 mask 255.255.255.0
excluded-ip-address 19.19.19.1
excluded-ip-address 19.19.19.3 19.19.19.100
option 43 ascii HuaweiAC-19.19.19.1,19.19.19.2
interface Vlanif3010
ip address 19.19.19.2 255.255.255.0
dhcp select interface
#
interface XGigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 3010 3931
#
wlan
wlan ac source interface Vlanif3010
wlan ac protect enable protect-ac 19.19.19.1 priority 7
service-set name set1 id 1
forward-mode tunnel
service-vlan 3931
#
return
```

Wired-side configuration file of AC2

```
#
sysname lsw_AC1
#
vlan batch 3010 3931
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 3010
port trunk allow-pass vlan 3010
#
interface XGigabitEthernet0/0/27
port link-type trunk
port trunk allow-pass vlan 3010 3931
#
return
```

Configuration file of the aggregation switch

```
#
sysname LSW
#
vlan batch 3010 3931
#
interface Vlanif3931
ip address 30.30.30.5 255.255.255.0
#
interface GigabitEthernet0/0/1
description connect to active AC
port link-type trunk
port trunk pvid vlan 3010
port trunk allow-pass vlan 3010
#
interface GigabitEthernet0/0/2
```

```
description connect to standby AC
port link-type trunk
port trunk pvid vlan 3010
port trunk allow-pass vlan 3010
#
interface GigabitEthernet0/0/3
description connect to AP
port link-type trunk
port trunk pvid vlan 3010
port trunk allow-pass vlan 3010
#
interface GigabitEthernet0/0/4
description connect to AP
port link-type trunk
port trunk pvid vlan 3010
port trunk allow-pass vlan 3010
#
interface GigabitEthernet0/0/5
description connect to BRAS
port link-type trunk
port trunk pvid vlan 3931
port trunk allow-pass vlan 3010 3931
#
return
```

The preceding configuration files show the basic configurations used for dual-link backup in Layer 2 branched networking. You can configure services on the ACs and switches after completing the preceding configurations.