

# WLAN WDS Technology White Paper

Issue        03  
Date         2017-11-21

**Copyright © Huawei Technologies Co., Ltd. 2017. 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://enterprise.huawei.com>

# Change History

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

## Issue 03 (2017-11-21)

This issue is updated based on changes of WLAN devices in V200R005C00. In this issue, dual-link connections are changed to single-link connections.

## Issue 02 (2013-02-28)

This issue is updated based on changes of WLAN devices in V200R002C00 and V200R003C00.

1. Deleted the original section 1.2 "Availability."
2. Modified the section 1.3.1 "P2P Networking and Configuration Notes."
3. Added the note "In V200R003C00, the configuration takes effect immediately."

## Issue 01 (2012-07-15)

This is the first official release.

# WDS Technology White Paper

## Keywords

WDS, bridge, P2P, P2MP

## Abstract

This document describes wireless distribution system (WDS) technology supported by Huawei WLAN devices. WDS technology allows for long-distance wireless connection between networks, enlarges the network coverage, and lowers network deployment costs.

This document provides the WDS working mechanism, networking scenarios, and configuration notes. In addition, the WDS configuration is described.

## Acronyms and Abbreviations

Acronym and Abbreviation	Full Name
WDS	Wireless distribution system
AP	Access point
AC	Access controller
VAP	Virtual access point
WVL	Wireless virtual link
LAN	Local area network
P2P	Point-to-point
P2MP	Point-to-multipoint

---

# Contents

---

<b>1 WDS Technology .....</b>	<b>1</b>
1.1 Overview .....	1
1.2 Technology Description .....	1
1.2.1 WDS .....	1
1.2.2 WDS Setup .....	3
1.3 Configuration Notes.....	5
1.3.1 P2P Networking and Configuration Notes.....	5
1.3.2 P2MP Networking and Configuration Notes .....	6
<b>2 WDS Application .....</b>	<b>8</b>
2.1.1 Indoor WDS Networking.....	9
2.1.2 Outdoor WDS Networking .....	9
2.2 WDS Network Planning .....	11
2.2.1 Transmission Distance Planning.....	11
2.2.2 Network Bandwidth Planning.....	13
<b>3 WDS Configuration Example .....</b>	<b>17</b>
3.1 Networking Requirements.....	17
3.2 Configuration Analysis .....	18
3.3 Configuration Files .....	20

---

## List of Figures

---

<b>Figure 1-1</b> WDS network .....	2
<b>Figure 1-2</b> P2P networking.....	3
<b>Figure 1-3</b> P2MP networking .....	3
<b>Figure 1-4</b> P2P networking.....	5
<b>Figure 1-5</b> P2MP networking .....	6
<b>Figure 2-1</b> APs connecting to an AC through WDS .....	8
<b>Figure 2-2</b> Indoor WDS networking.....	9
<b>Figure 2-3</b> Outdoor WDS networking (1) .....	9
<b>Figure 2-4</b> Outdoor WDS networking (2) .....	10
<b>Figure 2-5</b> Outdoor WDS networking (3) .....	10
<b>Figure 2-6</b> Outdoor WDS networking (4) .....	10
<b>Figure 2-7</b> Outdoor WDS networking (5) .....	11
<b>Figure 2-8</b> Network diagram .....	16
<b>Figure 3-1</b> WLAN WDS network .....	17
<b>Figure 3-2</b> Flowchart for configuring WLAN WDS services.....	20

---

# 1 WDS Technology

---

## 1.1 Overview

### Definition

A wireless distribution system (WDS) connects two or more wired or wireless local area networks (LANs) wirelessly to establish a large network for data communication.

### Purpose

802.11 wireless technology has been widely used on home, SOHO, and enterprise networks. Users can easily access the Internet over WLANs. On a wireless network, APs must connect to the existing wired network to provide wireless network access services for users. To expand the wireless coverage area, APs need to be connected using cables, switches, and power supplies. This increases network costs and prolongs network construction period. In this case, WDS technology can be used to connect APs wirelessly, facilitating WLAN construction in a complex environment.

### Benefits

A WDS uses wireless links to connect two or more independent wired or wireless LANs so that users on these LANs can exchange data with each other. Network deployment and device installation are convenient.

## 1.2 Technology Description

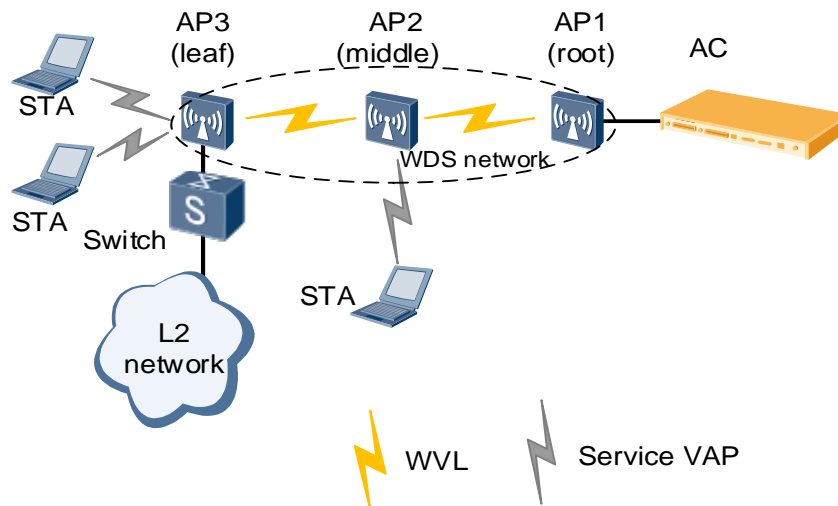
### 1.2.1 WDS

#### Concepts

- On a traditional WLAN, you can create service virtual APs (VAPs) on APs to provide access for wireless stations (STAs). Similarly, on a WDS network, you can create bridge VAPs on APs to provide access for neighboring bridges. The bridges then set up wireless virtual links (WVLs).
  - Bridge: a functional entity on an AP that provides the WDS service

- Service VAP: a WLAN access point that an AP uses to provide the WLAN service for STAs
- Bridge VAP: an access point that an AP uses to set up WVLs with neighboring bridges. A pair of bridge VAPs is created each time. One is called AP bridge and the other one is called STA bridge. The AP bridge provides a wireless access point for the STA bridge.
- WVL: a link between two bridge VAPs on different AP bridges. Service, management, and configuration packets on WDS networks are transmitted over WVLs.
- Depending on an AP's location on a WDS network, a wireless bridge works in root, middle, or leaf mode.
  - Root: The AP functions as a root node to directly connect to an AC using a cable, and functions as an AP bridge to connect to a STA bridge.
  - Middle: The AP functions as a middle node to connect to an AP bridge and a STA bridge. When connecting to an AP bridge, the AP is a STA bridge; when connecting to a STA bridge, the AP is an AP bridge.
  - Leaf: The AP functions as a leaf node to connect to an AP bridge as a STA bridge.
- Wired interfaces of APs on a WDS network can connect to ACs, switches, or hosts. Depending on the AP's location, the wired interface on an AP works in root or endpoint mode.
  - Root interface: connects to an AC.
  - Endpoint interface: connects to a switch or host.

Figure 1-1 WDS network



## WDS Architecture

WDS networking is classified into point-to-point (P2P) mode and point-to-multipoint (P2MP) mode.

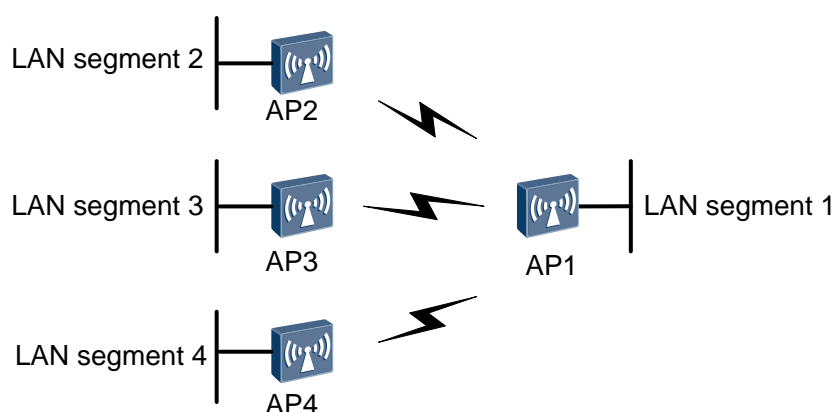
- P2P mode



**Figure 1-2** P2P networking

As shown in Figure 1-2, the WDS uses two APs to implement wireless bridging of LAN segments 1 and 2 so that LAN segments 1 and 2 can communicate with each other. In practice, the peer MAC address can be configured on each AP to determine the bridging link to be set up.

- P2MP mode

**Figure 1-3** P2MP networking

As shown in Figure 1-3, on a P2MP network, AP1 is used as the central AP, and all other APs establish wireless bridge links only with AP1. This implements connection of multiple networks. LAN segments 2, 3, and 4 can only communicate through AP1.

## 1.2.2 WDS Setup

### Setting Up Connections Between Bridges

After wireless bridging is enabled on an AP, a pair of bridge VAPs is automatically created. One is an AP bridge and the other is a STA bridge. The bridge VAPs have only basic parameters configured and are used to set up an initial WVL between APs. The AP connects to the AC through the initial WVL and obtains configurations from the AC. A final WVL is then set up according to the following process. In the process, Bridge A is a STA bridge and bridge B is an AP bridge.

1. The STA bridge detects the AP bridge.

When the channel mode is set to automatic, bridge A broadcasts a probe request packet carrying a specified bridge name (bridge identifier, which is similar to the SSID in the traditional WLAN service) in all channels in turn until it receives a response.

When the channel mode is set to fixed, bridge A broadcasts a probe request packet carrying a specified bridge name in a channel until it receives a response.

2. The AP bridge responds.

After receiving the probe request packet, bridge B checks the packet. If the bridge name in the packet is the same as that of bridge B and the whitelist has no bridge configured (indicating that access of bridge A is not restricted), or the MAC address of the AP connected by bridge A is in the whitelist (indicating that access of bridge A is allowed), bridge B responds to bridge A.

If the bridge name in the packet is different from that of bridge B, or the MAC address of the AP connected by bridge A is not in the whitelist and the whitelist has other bridges configured, bridge B does not respond to bridge A.

3. The STA bridge sends a connection request to the AP bridge.

If bridge B has no authentication policy configured, the two bridges can set up a connection. If bridge B has been configured with an authentication policy and a key, bridge A requests bridge B to perform authentication and authorization.

4. The AP bridge performs authentication on the STA bridge.

If bridge B has no authentication policy configured, the two bridges can set up a connection. If bridge B has been configured with an authentication policy and a key, bridge A requests bridge B to perform authentication and authorization.

5. The bridges maintain the connection.

After the connection is set up, the bridges periodically send messages to each other to maintain the connection. If one end does not respond for a long, the connection is torn down, and the bridges repeat the operations from step 1 to step 4.

6. If the AC delivers new WDS parameters to the bridges, the bridges use the new parameters to perform step 1 to step 5.

## AC Delivers Configurations to Connected APs

An AP enabled with the bridging function discovers and connects to an AC through a wired or wireless bridge interface, and obtains configurations from the AC.

During configuration delivery, the following situations may occur:

- If the AC delivers the configuration with WDS disabled, the AP disables all WDS VAPs, disables automatic discovery, and stops sending connection keepalive packets. In this case, service access parameters can be set, but WDS parameters cannot be set.
- If the AC delivers the configuration with WDS enabled, the AP creates a WDS VAP. WDS parameters can be set. If existing WDS parameters are modified, the bridge needs to rediscover the AC and set up a link.
- If the AP's version does not support the WDS function, the AP notifies the AC that it does not support WDS parameters. The AC still delivers other service parameters, but does not deliver WDS parameters.
- When the WDS-enabled AP receives VAP parameters delivered by the AC that does not support the WDS function, the AP automatically switches the radio to the access mode to accept the VAP parameters.

## Eliminating Loops Using STP

On a P2MP network, loops may occur between bridge links or wired links. To prevent network storms and ensure correct Layer 2 forwarding, enable the Spanning Tree Protocol (STP) function to detect loops.

STP takes effect only on AP wired interfaces and WDS-enabled bridge interfaces. Each WVL on bridge interfaces independently participates in STP interaction and control.

## 1.3 Configuration Notes

### 1.3.1 P2P Networking and Configuration Notes

Figure 1-4 P2P networking

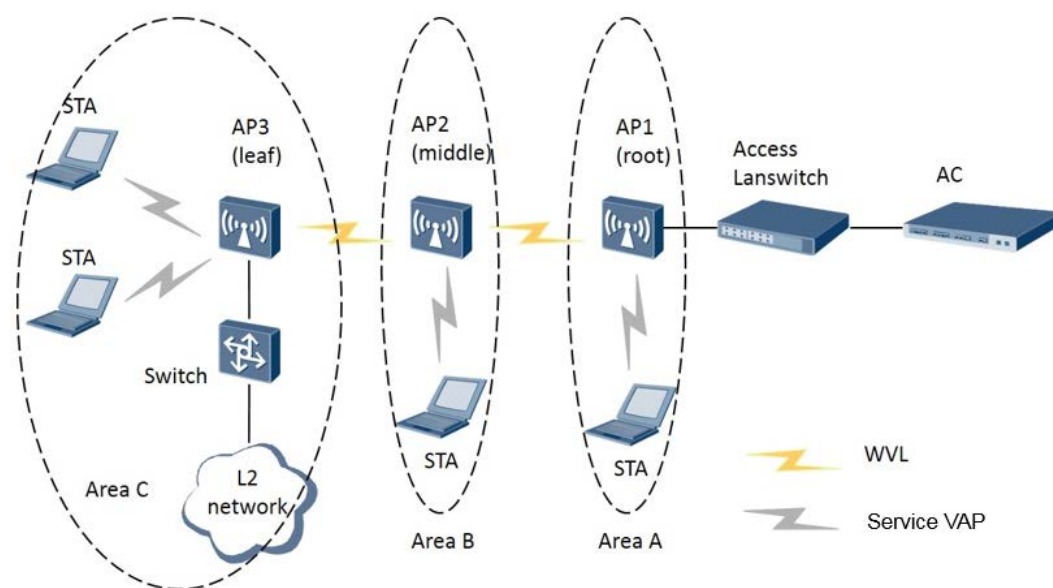


Figure 1-4 shows the WDS P2P topology. The root AP connects to a middle or leaf AP in bridging mode. Dual-band APs are used on the actual network. The APs use the 5 GHz radio for radio backhaul and the 2.4 GHz radio to provide access for STAs.

The configuration notes in P2P networking are as follows:

- Management WDS links and service WDS links must not be in the same VLAN; otherwise, loops will occur. Table 1-1 describes the VLAN configuration plan.

Table 1-1 VLAN configuration plan

Item	Data
VLAN	Management VLAN: 100
	Service VLANs: 101, 102, 103, 104, 105, and 106 <ul style="list-style-type: none"> <li>• Area A: VLAN 101 for wireless services</li> <li>• Area B: VLAN 102 for wireless services</li> <li>• Area C: VLAN 103 for wireless services</li> <li>• Area C: VLANs 104, 105, and 106 on wired interfaces of AP3</li> </ul>

- Management WDS links do not support STP; therefore, other measures must be taken to ensure that no loop will occur on the management links and external network.
- STP can prevent loops between bridges and on the networks connected to AP wired interfaces. The STP cost of Huawei switches (including ACs) complies with 802.1t, while the STP cost of Huawei APs complies with 802.1d. When a Huawei AP is connected to a Huawei switch and STP needs to be enabled for the WDS network, the STP cost on the switch (or AC) must be correctly set; otherwise, the path on the root AP may be blocked. For example, run the following commands to set the STP cost on Huawei S5300:

```
<Quidway> system-view
[Quidway] stp pathcost-standard dot1d-1998
[Quidway] quit
```

- If VAPs 12 through 15 have been configured, change the VAP IDs before enabling WDS.
- The AP must be restarted after WDS is enabled or disabled, the wired interface role is changed, or the management VLAN (including tag/untag and PVID) is changed; otherwise, the configurations do not take effect.



#### NOTE

In V200R003C00, the configurations take effect immediately after being performed.

- To ensure sufficient bandwidth, you are advised to configure no more than three hops. If the first bridge provides 150 Mbit/s throughput on the network shown in Figure 1-4, the throughput is decreased to 20 Mbit/s after the first hop and to 5.7 Mbit/s after the second hop.
- Disable the calibration function in the radio profile to prevent impact of calibration on services. You are advised to configure an independent radio profile for the WDS and add WDS bridges to an independent region.
- The country codes of APs can be changed on the connected ACs. If the country code of a root AP is changed on the connected AC, the country codes of the root AP and leaf APs may be different. In this case, the root AP and leaf APs support different channel sets, and the leaf APs may fail to associate with the root AP. Therefore, ensure that the country codes of all WDS bridge APs are the same.
- Do not change the radio profiles of middle APs or leaf APs.

## 1.3.2 P2MP Networking and Configuration Notes

Figure 1-5 P2MP networking

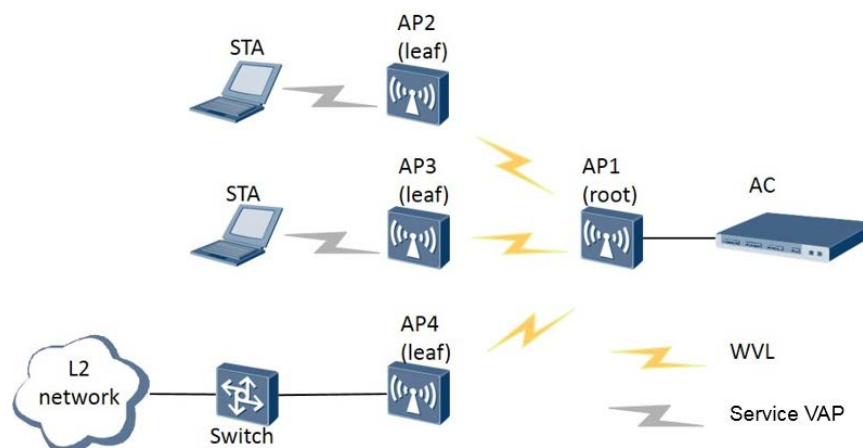


Figure 1-5 shows the P2MP topology. AP1 connects to multiple APs through WDS in bridging mode. Data from AP2, AP3, and AP4 can only be forwarded by AP1.

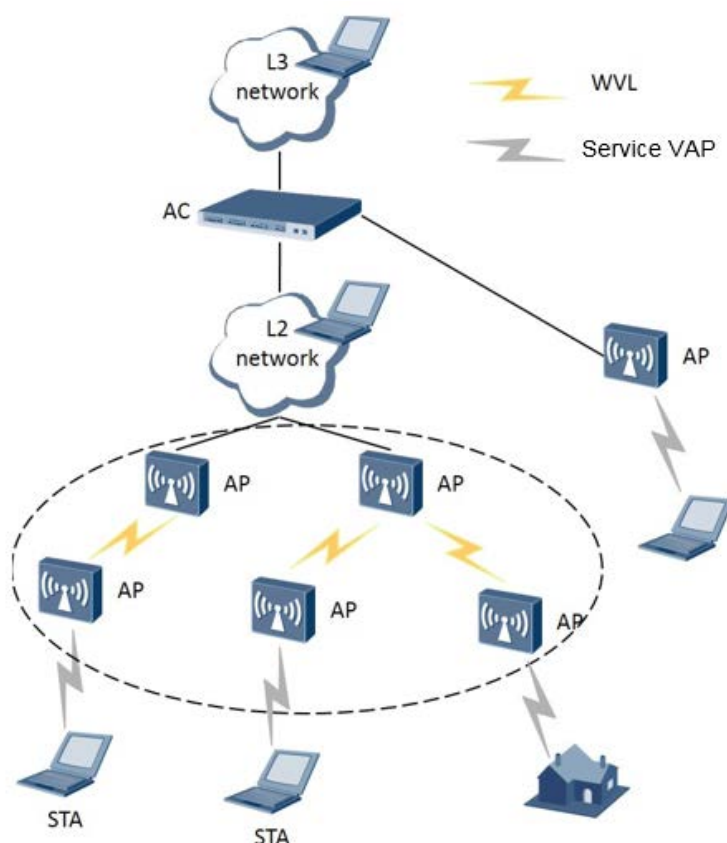
The configuration notes in P2MP networking are as follows:

The configuration notes in P2P networking also apply to P2MP networking because WDS implementation is the same in the two networking modes. However, P2MP networking requires sufficient bandwidth for users. In typical cases, the number of next-hop APs cannot exceed 6.

# 2 WDS Application

The following figure shows how APs connect to an AC through WDS.

**Figure 2-1** APs connecting to an AC through WDS

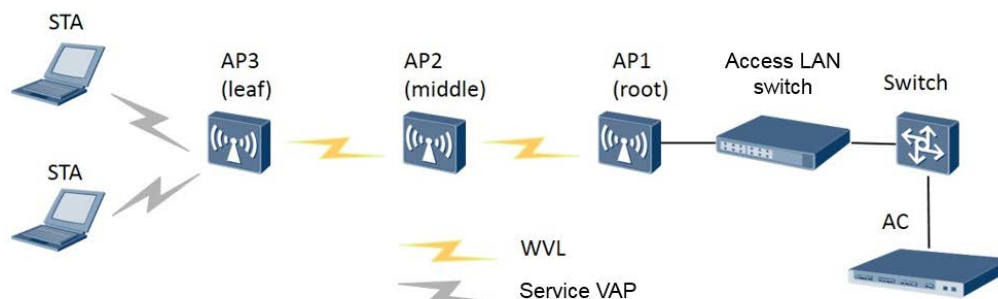


As shown in Figure 2-1, multiple APs are deployed on a WDS network. APs can set up wireless multi-hop connections and connect to the AC wirelessly. STAs are unaware of the differences between traditional WLANs and WDS networks because the only difference between them is the backbone layer.

The following describes typical WDS networking scenarios.

## 2.1.1 Indoor WDS Networking

**Figure 2-2** Indoor WDS networking



The indoor WDS networking shown in Figure 2-3 is applicable to homes, warehouses, subways, and enterprises. As WLAN signals are deteriorated by walls and other obstacles, one AP cannot provide signal coverage for all indoor areas. In this case, WDS technology can be used to connect multiple APs, enlarging signal coverage and reducing cabling costs.

## 2.1.2 Outdoor WDS Networking

In outdoor scenarios, different antennas can be used to enable APs to form a WDS network over dozens of kilometers. WDS technology implements cross-obstacle or cross-area data transmission. This overcomes limitations of wired networks, such as difficult construction, high deployment costs, and poor flexibility. The outdoor WDS networking is applicable to campuses, plantations, mountainous areas, and high buildings.

### TIP

Obstacles in outdoor scenarios are mainly trees and high buildings. The radius of the Earth must be considered if the transmission distance is long. Therefore, select and install antennas based on the site condition.

### Outdoor Scenario (1)

The following figures show the WDS networks that connect LANs of different buildings. For example, Figure 2-3 shows the WDS networking for connecting two LANs that are blocked by obstacles.

**Figure 2-3** Outdoor WDS networking (1)

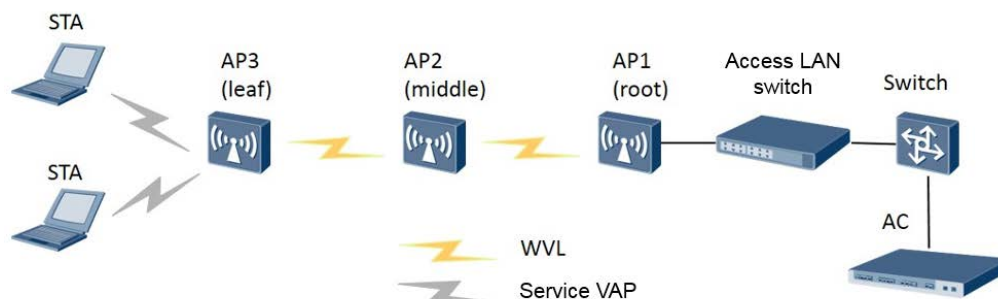


Figure 2-4 Outdoor WDS networking (2)

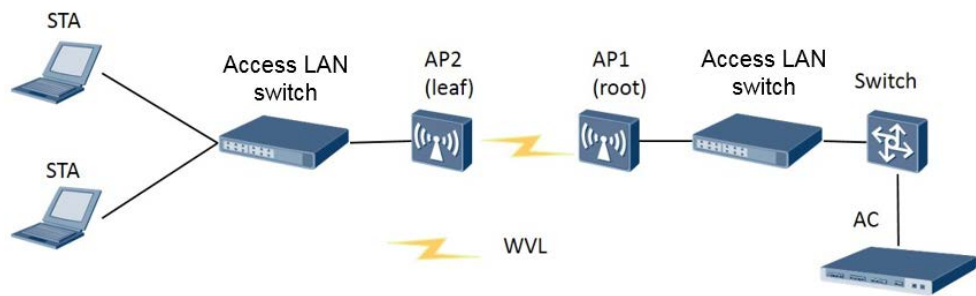
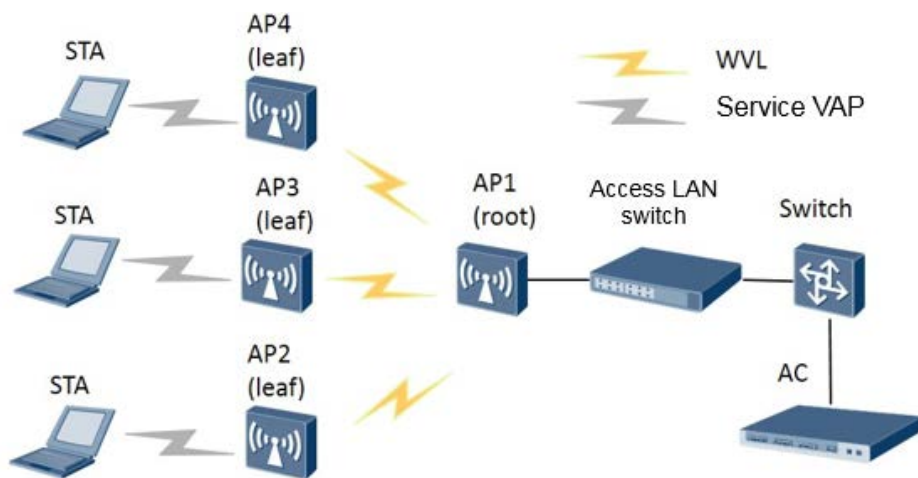


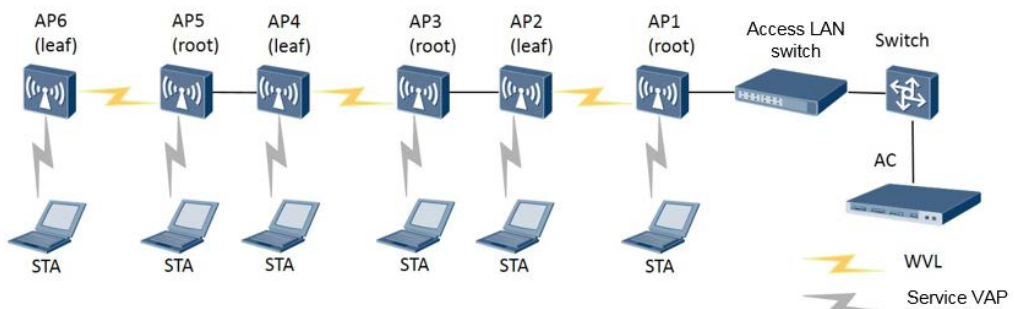
Figure 2-5 Outdoor WDS networking (3)



### Outdoor Scenario (2)

When obstacles exist between networks to be connected or the transmission distance is long, deploy two WDS APs through wired interfaces in back-to-back mode to provide the relay bridging function. This network deployment mode ensures bandwidth of wireless links during long-distance network transmission.

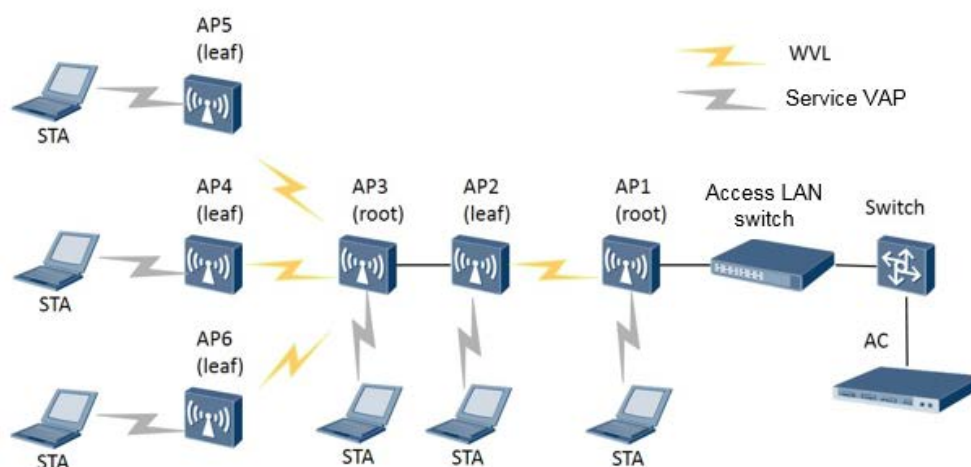
Figure 2-6 Outdoor WDS networking (4)





## Outdoor Scenario (3)

Figure 2-7 Outdoor WDS networking (5)



## 2.2 WDS Network Planning

### 2.2.1 Transmission Distance Planning

#### Signal Attenuation

When APs are used as bridges on a WDS network, at least two APs are connected over several hundred meters to dozens of kilometers. Radio waves will attenuate during long-distance transmission. The following assumes that radio waves are transmitted in free space without reflection, refraction, diffraction, scattering, or absorption. The relationship between the path loss of radio waves and transmission distance is as follows:

$$PL = 32.45 + 20 \times \lg(d_{km}) + 20 \times \lg(f_{MHz})$$

The free space transmission model is the simplest radio transmission model. In this model, the path loss relates only to the transmission distance and frequency of radio waves. The actual transmission environment is more complex, so environmental factor  $n$  must be taken into account. The formula changes into the following:

$$PL = 32.45 + 10 \times n \times \lg(d_{km}) + 20 \times \lg(f_{MHz})$$

The environmental factor  $n$  varies depending on the transmission environment and ranges from 2 to 5. Generally,  $n$  ranges from 4 to 5 in city centers with high-density users, ranges from 3 to 4 in common urban areas, and ranges from 2.5 to 3 in suburb areas.

For example, on a WDS network, two APs are deployed 1 km away from each other and work at the frequency of 5000 MHz. The following assumes that radio waves are transmitted in free space and  $n$  is 2, the pass loss is calculated as follows:

$$PL = 32.45 + 10 \times 2 \times \lg(1) + 20 \times \lg(5000) = 106.4 \text{ dB}$$

The calculation result shows that radio waves attenuate obviously in long-distance transmission. In the actual WDS networking, two connected bridge APs may be dozens of kilometers away from each other. As the transmit power of APs is fixed, the key to ensuring signal quality in long-distance transmission is to select proper antennas.

#### TIP

In real radio environments, it is considered that radio signals are transmitted in free space as long as they are not blocked in the first Fresnel zone. In this way, you can estimate signal attenuation easily.

## Antenna Parameters

Antenna parameters include the gain, lobe width, polarization direction, electrical downward declination angle, and front-to-rear ratio. The antenna gain and lobe width affect wireless network performance the most.

- **Antenna gain:** ratio of the power produced by an antenna from a far-field source on the antenna's beam axis to the power produced by a hypothetical lossless isotropic antenna, which is equally sensitive to signals from all directions.
- **Lobe width:** angle of the sector formed by radio waves. An antenna transmits radio waves of different strengths in different directions, so the lobe width is defined as the angle between two directions with 3 dB power lower than the maximum transmit power.

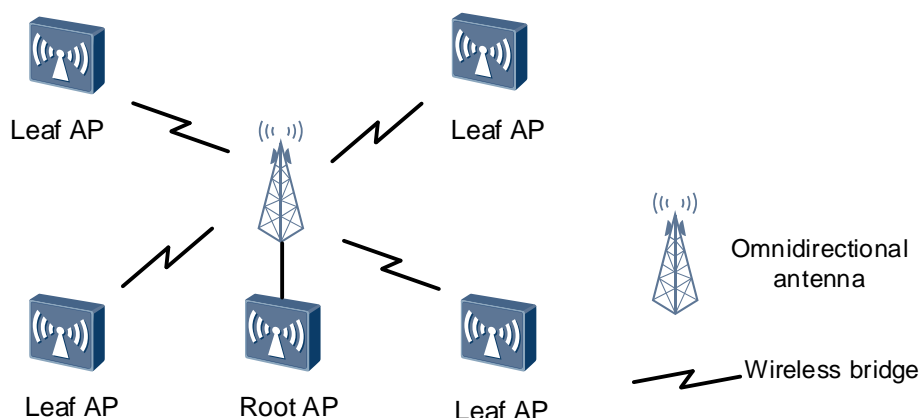
In normal cases, when the antenna gain increases, the lobe width decreases and radiant energy transmitted by the antenna is more concentrated.

## Antenna Type

Depending on the signal radiation on horizontal or vertical planes, antennas are classified into omnidirectional antennas and directional antennas.

- **Omnidirectional antenna:** Signals from an omnidirectional antenna are evenly distributed 360 degrees around the central point. The lobe width of an omnidirectional antenna is 360 degrees, but its antenna gain is low.

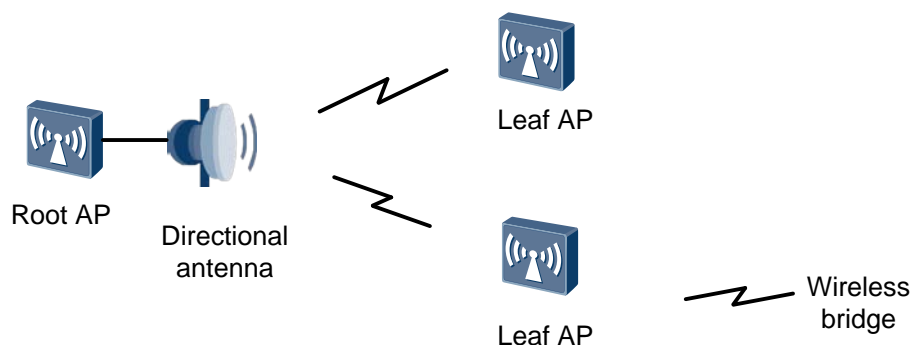
On a WDS network, omnidirectional antennas are used upon a short transmission distance, a large coverage angle, and a large number of APs. In the P2MP networking, an omnidirectional antenna can be used on the root AP to connect to the leaf APs around the root AP.



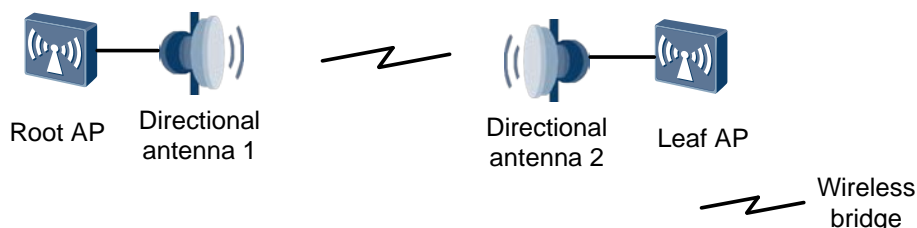
- **Directional antenna:** Signals from a directional antenna radiate in a certain angle. Directional antennas can concentrate energy and transmit signals to a specified direction.

Therefore, using directional antennas is a good choice when a few remote linked devices exist or the linked devices are concentrated in a certain angle.

On a P2MP WDS network, pay attention to the lobe width of directional antennas. The angle between an antenna and its linked device must be smaller than the lobe width of the antenna. The linked device must be within the antenna coverage. As shown in the following figure, the root AP uses a directional antenna to connect to two leaf APs. The two leaf APs must be located within the coverage area of the directional antenna.



On a P2P WDS network, directional antennas with a small lobe width are recommended, because they can improve the transmission distance and signal quality. Directional antennas with a small lobe width have a high antenna gain and can concentrate energy in a narrow range.



The following figure shows the appearances of typical antennas. For details about antenna types and parameters, see the *WLAN V2R1 Antennas*.



## 2.2.2 Network Bandwidth Planning

On a wireless network, as the transmission distance increases, signal attenuation increases and the effective bandwidth decreases. Table 2-1 and Table 2-2 list the effective bandwidth values mapping different antenna gains in P2P bridge mode. The two WDS APs use antennas with the same gain.

**Table 2-1** Transmission bandwidth in different distances in P2P bridge mode (HT20)

Frequency Band	Environment	Antenna Gain	Bandwidth Within Different Distances in HT20 Mode (Mbit/s)					
			0.2 km	0.5 km	1 km	2 km	5 km	10 km
5 GHz	Urban areas	11 dBi	80	55	30	6	/	/
		15 dBi	80	80	60	30	/	/
		18 dBi	80	80	80	50	12	/
		21 dBi	80	80	80	80	32	10
	Countryside or suburb areas	11 dBi	80	80	80	45	8	/
		15 dBi	80	80	80	48	10	/
		18 dBi	80	80	80	80	30	8
		21 dBi	80	80	80	80	50	27

**Table 2-2** Transmission bandwidth in different distances in P2P bridge mode (HT40)

Frequency Band	Environment	Antenna Gain	Bandwidth Within Different Distances in HT40 Mode (Mbit/s)					
			0.2 km	0.5 km	1 km	2 km	5 km	10 km
5 GHz	Urban areas	11 dBi	160	90	45	/	/	/
		15 dBi	160	160	95	45	/	/
		18 dBi	160	160	160	80	15	/
		21 dBi	160	160	160	135	50	/
	Countryside or suburb areas	11 dBi	160	160	135	65	/	/
		15 dBi	160	160	160	70	/	/
		18 dBi	160	160	160	120	45	/
		21 dBi	160	160	160	160	80	40

In P2MP networking, if WDS APs are deployed far from each other, they may become hidden stations to each other. (If base stations A and C simultaneously send signals to base station B because base station C does not know that base station A is sending information to base station B, signal conflict occurs. As a result, signals sent to base station B are all lost. In this situation, base stations A and C are hidden stations to each other.) Due to competition among P2MP bridges, transmission bandwidth in P2MP networking is much lower than that in P2P networking when the transmission distance is the same. Table 2-3 lists the reference values of transmission bandwidth under various P2MP configurations.

**Table 2-3** Factors affecting P2MP bridge performance

P2MP	Impact Coefficient		Bandwidth Impact Factor	
	Hidden STA	Multi-User Competition	P	MP
1	N/A	N/A	1	1
2	0.6	0.95	0.57	0.285
3	0.6	0.9	0.54	0.18
4	0.6	0.9	0.54	0.135
5	0.6	0.8	0.48	0.096
6	0.6	0.8	0.48	0.08

The following provides an example:

According to the performance indicators of a network bridge (see the appendix), when bridges are deployed in P2P networking in a rural area, work on the 5 GHz band, and use antennas with a gain of 18 dBi, the maximum bandwidth within a distance of 2 km is 80 Mbit/s. When the same APs are deployed in P2MP networking (M equals 3) in the same scenario, the maximum bandwidth on each node is calculated as follows using the impact factors:

Effective bandwidth on the root node = 80 Mbit/s x 0.54 = 43.2 Mbit/s

Effective bandwidth on the leaf node = 80 Mbit/s x 0.18 = 14.4 Mbit/s

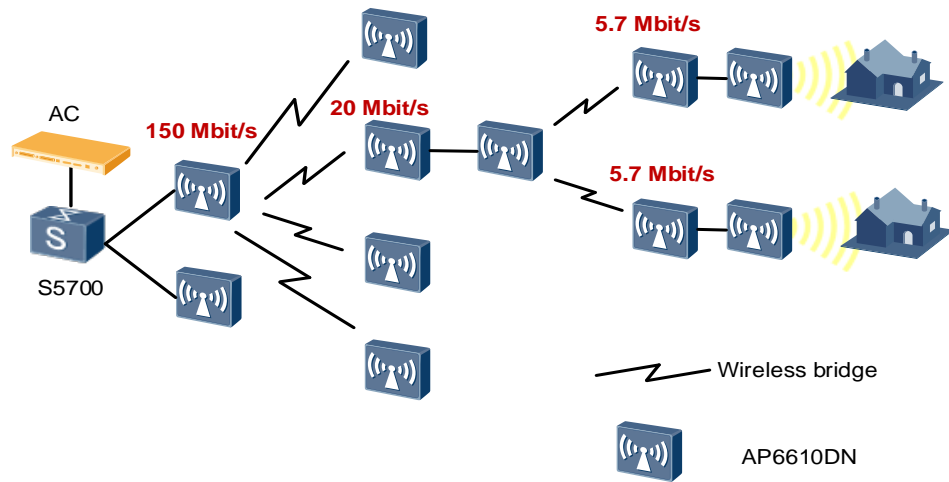
Compared to P2P networking, the total link bandwidth of bridges reduces from 80 Mbit/s to 43.2 Mbit/s in P2MP networking (M equals 3). The bandwidth on each link is only 14.4 Mbit/s in P2MP networking (M equals 3). This example proves that the maximum bandwidth in P2MP networking is much lower than that in P2P networking. Therefore, when deploying bridges in P2MP networking, ensure that the bandwidth is sufficient for user access.

## Bandwidth Planning Example

To bridge digital divide, a local government plans to build a wireless network for local plantations. This network will provide Internet access services in the plantations, covering 310,000 household users. Users in the plantations are common users. Each plantation has about 300 to 400 households. If each household has five users, the total number of users in a village is about 1750. The number of concurrent users accounts for 30% of the total. There are no special requirements for network bandwidth. Approximately 100 households share 10 Mbit/s bandwidth, so a total ingress bandwidth of 40 Mbit/s can meet the requirement in a village.

Each plantation can use an AC to manage APs and support wireless roaming. More than 100 AP6610DN outdoor dual-band APs are deployed in each plantation. An AP6610DN supports the 2.4 GHz and 5 GHz frequency bands and can work as a wireless bridge device. The AP6610DN complies with IEEE 802.11a/b/g/n and provides both wireless transmission and coverage. The following figure shows the network diagram.

**Figure 2-8** Network diagram



If the first bridge provides 150 Mbit/s bandwidth on the network, the bandwidth is decreased to 20 Mbit after the first hop and to 5.7 Mbit after the second hop. As 100 users share 10 Mbit/s bandwidth, 5.7 Mbit bandwidth is sufficient for 20 users.

# 3 WDS Configuration Example

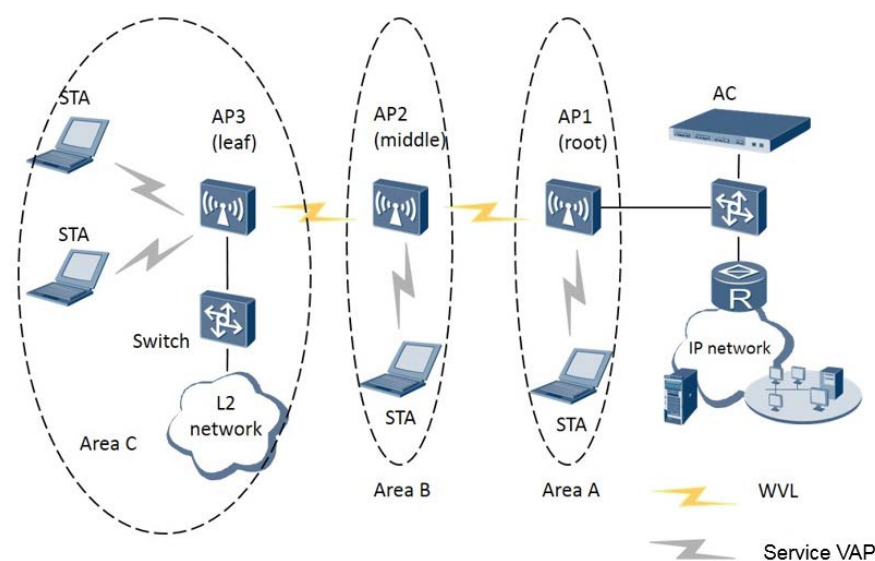
## 3.1 Networking Requirements

An enterprise plans to provide WLAN access services for its customers and employees in three areas. To lower cabling costs, the enterprise uses WDS technology to connect APs in areas B and C to the AC wirelessly.

Figure 3-1 shows the WLAN WDS network topology.

- The AC6605 is used.
- The AC functions as a DHCP server to assign IP addresses to APs and STAs in each area.
- AP1 connects to the AC in wired mode, provides WLAN services for area A, and connects to AP2 as a bridge.
- AP2 connects to the AC through a wireless bridge (AP1), provides WLAN services for area B, and connects to AP3 as a bridge.
- AP3 connects to the AC through a wireless bridge (AP2), provides WLAN services for area C, and connects to a Layer 2 network through a wired interface.

**Figure 3-1** WLAN WDS network



## 3.2 Configuration Analysis

When configuring WDS, ensure that the management WVL and service WVLs are in different VLANs; otherwise, loops will occur. Table 3-1 describes the VLAN configuration plan.

**Table 3-1** VLAN configuration plan

Item	Configuration
Management VLAN	Management VLAN: 100
Service VLAN	Service VLANs: 101, 102, 103, 104, 105, and 106 Area A: VLAN 101 for WLAN services Area B: VLAN 102 for WLAN services Area C: VLAN 103 for WLAN services and VLANs 104, 105, and 106 on the wired interface of AP3

Before performing the tasks in this example, ensure that the radios on AP1, AP2, and AP3 are not configured with service VAPs with WLAN IDs of 13, 14, 15, or 16.

After data is planned, configure the WDS. Perform the following operations to configure a bridge VAP:

- Step 1** Configure a radio profile and bind a WMM profile to it. The bridges use 5 GHz radios, but the default radio type in the radio profile is 802.11b/g, which does not support 5 GHz radios. Therefore, the radio type in the radio profile must be changed.

```
[AC]wlan
[AC-wlan-view]radio-profile name aaa
[AC-wlan-radio-prof-aaa]wmm-profile name aaa
[AC-wlan-radio-prof-aaa]radio-type 80211an
Warning: Modify the Radio type may cause some parameters of Radio resume default
value, are you sure to continue?[Y/N]:y
[AC-wlan-radio-prof-aaa]quit
```

- Step 2** Configure bridge whitelists for the APs, and add neighbors of each AP to the whitelists. The whitelists prevent leaf APs from directly connecting to the root AP without connecting to middle APs.

Configure a bridge whitelist for AP1.

```
[AC-wlan-view]bridge-whitelist name ap1
[AC-wlan-br-whitelist-ap1]peer ap 5489-9845-9573
[AC-wlan-br-whitelist-ap1]quit
Configure the bridge whitelist for AP2.
[AC-wlan-view]bridge-whitelist name ap2
[AC-wlan-br-whitelist-ap2]peer ap 0025-9e12-6667
[AC-wlan-br-whitelist-ap2]peer ap 80fb-0689-81c3
[AC-wlan-br-whitelist-ap2]quit
```

Configure a bridge whitelist for AP3.

```
[AC-wlan-view]bridge-whitelist name ap3
[AC-wlan-br-whitelist-ap3]peer ap 5489-9845-9573
[AC-wlan-br-whitelist-ap3]quit
```



- Step 3** Configure radios on each AP. Enable the 5 GHz bridge, set the bridge mode, and bind the bridge whitelists to the radios.

Configure AP1 as a root AP.

```
[AC-wlan-view]ap 1 radio 1
[AC-wlan-radio-1/1]radio-profile name aaa
Warning: Modify the Radio type may cause some parameters of Radio resume default
value, are you sure to continue?[Y/N]:y
[AC-wlan-radio-1/1]bridge enable mode root
Info: This action will take effect after resetting ap.
[AC-wlan-radio-1/1]bridge-whitelist name ap1
[AC-wlan-radio-1/1]quit
[AC-wlan-view]
```

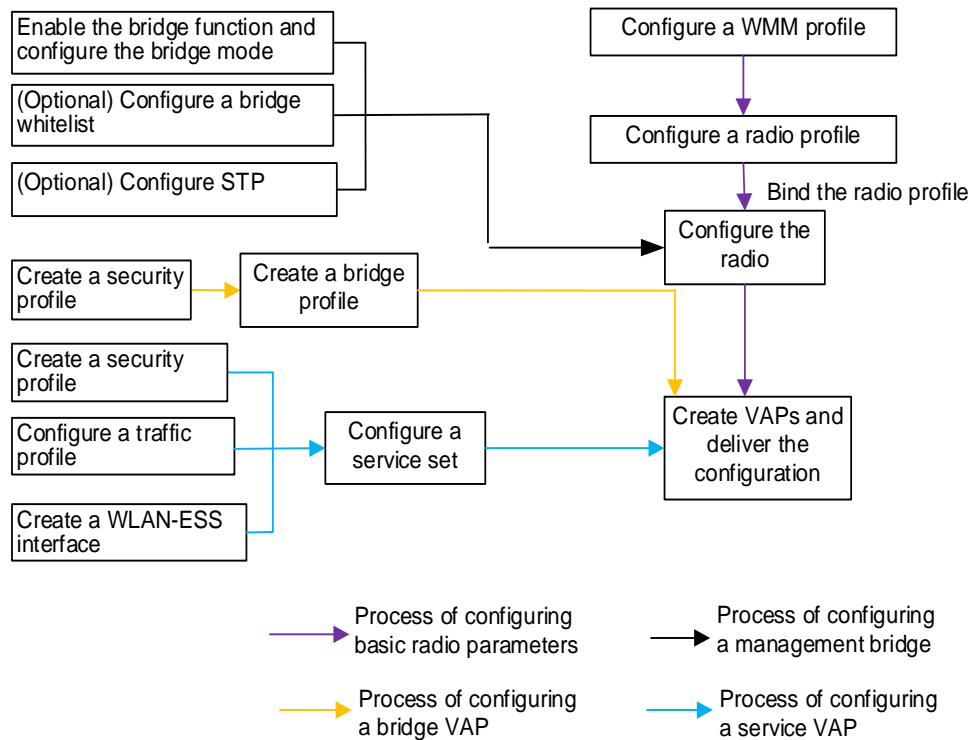
Configure AP2 as a middle AP.

```
[AC-wlan-view]ap 2 radio 1
[AC-wlan-radio-2/1]radio-profile name aaa
Warning: Modify the Radio type may cause some parameters of Radio resume default
value, are you sure to continue?[Y/N]:y
[AC-wlan-radio-2/1]bridge enable mode middle
Info: This action will take effect after resetting ap.
[AC-wlan-radio-2/1]bridge-whitelist name ap2
[AC-wlan-radio-2/1]quit
[AC-wlan-view]
```

Configure AP3 as a leaf AP.

```
[AC-wlan-view]ap 3 radio 1
[AC-wlan-radio-3/1]radio-profile name aaa
Warning: Modify the Radio type may cause some parameters of Radio resume default
value, are you sure to continue?[Y/N]:y
[AC-wlan-radio-3/1]bridge enable mode leaf
Info: This action will take effect after resetting ap.
[AC-wlan-radio-3/1]bridge-whitelist name ap3
[AC-wlan-radio-3/1]quit
[AC-wlan-view]
```

- Step 4** Configure a bridge profile. After a security profile is created, create a bridge profile and bind the bridge profile to the radio profile to create a bridge VAP.
- Step 5** Configure service sets for AP1, AP2, and AP3, and bind the service sets to the radio profile to create a service VAP.
- Step 6** Deliver the created bridge VAP and service VAP to the APs.

**Figure 3-2** Flowchart for configuring WLAN WDS services

----End

### 3.3 Configuration Files

- Switch configuration file

```

#
vlan batch 100 to 106
#
interface GigabitEthernet0/0/1
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 106
#
interface GigabitEthernet0/0/2
port link-type trunk
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 106
#

```

- AC configuration file

```

#
vlan batch 100 to 106
#
wlan ac-global carrier id ctc ac id 1
#

```

```
dhcp enable
#
interface Vlanif100
 ip address 192.168.10.1 255.255.255.0
 dhcp select interface
#
interface Vlanif101
 ip address 192.168.1.1 255.255.255.0
 dhcp select interface
#
interface Vlanif102
 ip address 192.168.2.1 255.255.255.0
 dhcp select interface
#
interface Vlanif103
 ip address 192.168.3.1 255.255.255.0
 dhcp select interface
#
interface XGigabitEthernet0/0/1
 port link-type trunk
 port trunk allow-pass vlan 100 to 106
#
interface Wlan-Ess1
 port hybrid pvid vlan 101
 port hybrid untagged vlan 101
 dhcp enable
#
interface Wlan-Ess2
 port hybrid untagged vlan 102
 dhcp enable
#
interface Wlan-Ess3
 port hybrid untagged vlan 103
 dhcp enable
#
wlan
 wlan ac source interface vlanif100
 ap-region id 101
 ap-region id 102
 ap-region id 103
 ap-auth-mode no-auth
 ap id 1 type-id 19 mac 0025-9e12-6667
 region-id 101
 ap id 2 type-id 19 mac 5489-9845-9573
 region-id 102
 ap id 3 type-id 19 mac 80fb-0689-81c3
 region-id 103
 lineate-port stp enable
 lineate-port mode endpoint
 lineate-port pvid vlan 104
 lineate-port user-isolate enable
 lineate-port vlan tagged 105
 lineate-port vlan untagged 106
 wmm-profile name wp01 id 0
 traffic-profile name tp01 id 0
```

```
security-profile name sp01 id 0
security-policy wpa2
wpa2 authentication-method psk pass-phrase 12345678 encryption-method ccmp
service-set name ss01 id 0
wlan-ess 1
ssid ChinaSer01
traffic-profile id 0
security-profile id 0
service-vlan 101
service-set name ss02 id 1
wlan-ess 2
ssid ChinaSer02
traffic-profile id 0
security-profile id 0
service-vlan 102
service-set name ss03 id 2
wlan-ess 3
ssid ChinaSer03
traffic-profile id 0
security-profile id 0
service-vlan 103
bridge-profile name bp01 id 0
bridge-name ChinaNet01
security-profile id 0
vlan tagged 100 to 106
radio-profile name rp01 id 0
wmm-profile id 1
radio-profile name rp02 id 1
radio-type 80211an
wmm-profile id 1
bridge-whitelist name bw01 id 0
peer ap mac 5489-9845-9573
bridge-whitelist name bw02 id 1
peer ap mac 80fb-0689-81c3
peer ap mac 0025-9e12-6667
ap 1 radio 0
radio-profile id 0
service-set id 0 wlan 1
ap 1 radio 1
radio-profile id 2
bridge enable mode root
bridge whitelist enable
bridge-whitelist id 0
service-set id 0 wlan 1
bridge-profile id 0
ap 2 radio 0
radio-profile id 0
service-set id 0 wlan 1
ap 2 radio 1
radio-profile id 2
bridge enable mode middle
bridge whitelist enable
bridge-whitelist id 1
bridge-profile id 0
ap 3 radio 0
```

```
radio-profile id 0
service-set id 0 wlan 1
ap 3 radio 1
radio-profile id 2
bridge enable mode leaf
bridge whitelist enable
bridge-whitelist id 0
bridge-profile id 0
#
return
```