

Mesh Technology White Paper

Issue 01
Date 2013-05-10

Copyright © Huawei Technologies Co., Ltd. 2013. 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>

About This Document

Overview

This document describes mesh technology used on wireless access devices. Mesh technology can implement long-distance wireless connections between networks, expand network coverage area, and reduce network deployment costs.

This document describes mesh implementation principles, networking scenarios, and configuration notes, and provides mesh configuration examples.





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	Indicates a hazard with a high level or medium level of risk which, if not avoided, could result in death or serious injury.
 WARNING	Indicates a hazard with a low level of risk which, if not avoided, could result in minor or moderate injury.
 CAUTION	Indicates a potentially hazardous situation that, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results.
 TIP	Provides a tip that may help you solve a problem or save your time.

Symbol	Description
 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 (2013-05-10)

This issue is the first official release.

Contents

About This Document	ii
1 Mesh Technology	1
1.1 Introduction to Mesh Technology	1
1.2 Availability	2
1.3 Principles.....	2
1.3.1 Introduction to Mesh	2
1.3.2 Mesh Establishment Process	6
2 Mesh Applications	10
2.1 Typical Application Scenarios.....	11
2.1.1 Indoor WMN.....	11
2.1.2 Outdoor WMN	12
2.2 Mesh Networking Planning.....	12
2.2.1 Mesh Backhaul Layer Planning	12
2.2.2 Mesh Transmission Distance Planning	15
3 Typical Mesh Configuration Examples	18
3.1 Networking Requirements.....	18
3.2 Configuration Notes	19
3.3 Configuration Procedure	19
3.4 Configuration Files.....	26
A Abbreviations	30

1 Mesh Technology

About This Chapter

- 1.1 Introduction to Mesh Technology
- 1.2 Availability
- 1.3 Principles

1.1 Introduction to Mesh Technology

Definition

A wireless mesh network (WMN) is a communications network that consists of multiple wirelessly connected access points (APs) in a mesh topology and connects to a wired network through a portal node. Nodes on a WMN can automatically establish the ad-hoc topology and maintain mesh connectivity. Additionally, these nodes can automatically establish a wireless multi-hop network, providing a cost-effective last-mile broadband access solution.

Purpose

On a traditional wireless local area network (WLAN), each wireless station (STA) connects to the WLAN through a wireless link established with an AP, forming a basic service set (BSS).

Before communicating with each other, STAs must connect to a fixed AP. This network structure is called single-hop network.

STAs can communicate with only APs, and APs must connect to a wired network. This requirement confines the WLAN coverage. Currently, WLANs using a centralized topology apply only to a few scenarios, and APs must connect to a wired network through fixed lines.

As a technological innovation of traditional WLAN, WMN expands the application range of WLAN from hotspots to hot areas and reduces dependence on wired networks. A WMN is multi-hop network. The biggest difference between a WMN and a traditional single-hop network is that APs on a WMN forward wireless signals while providing user access. Multiple APs build a mesh topology where signals are routed from one AP to another AP and finally transmitted through the AP connected to a fixed line to a wired network.

Benefits

A WMN saves cables required between mesh nodes while providing path redundancy and rerouting functions as a distributed network. When a new AP is added to a WMN, the AP can automatically connect to the WMN and determine the optimal multi-hop transmission path after being powered on. When a new AP is moved from a WMN, the WMN can automatically discover the topology change and adjust communication routes to obtain the optimal transmission path.

1.2 Availability

Product Support

Table 1-1 Product and version

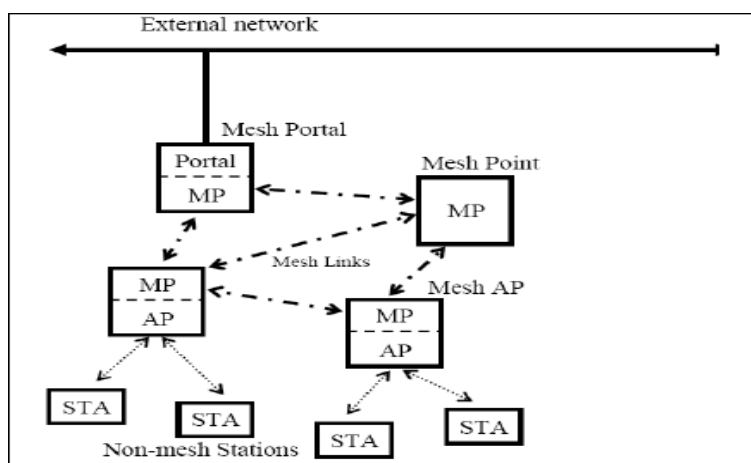
Product	Model	Version
AC	AC6605	V200R003C00
	AC6005-8/AC6005-8-PWR	V200R003C00
AP	AP6010DN/SN, AP6510DN, AP6610DN, WA615DN, WA655DN, AP3010DN, AP5010SN/DN, AP7110SN/DN	V200R003C00

1.3 Principles

1.3.1 Introduction to Mesh

Concepts

Figure 1-1 Mesh node roles (802.11s)



On a traditional WLAN, service virtual access points (VAPs) are created on APs to provide access for wireless STAs. On a WMN, APs establish the ad-hoc topology and are assigned the following roles based on their functions on the WMN:

- Mesh point (MP): a mesh-capable node that uses IEEE 802.11 MAC and physical layer protocols for wireless communication. This node supports automatic topology discovery, automatic route discovery, and data packet forwarding.
- Mesh point portal (MPP): an MP that connects to a WMN or another type of network. This node has the portal function and enables mesh nodes to communicate with external networks.
- Mesh AP (MAP): an MP that supports the AP function and provides access for STAs.



NOTE

In V200R003C00, the mesh configurations of an MP and MPP are different but the mesh configurations of an MP and MAP are the same. If the mesh function is enabled on an AP and an access VAP is created on the AP, the AP is an MAP.

If the mesh function is enabled on an AP but no access VAP is created on the AP, the AP is an MP. Because there may be a large load on an MPP, no access VAP is created on an MPP. In the following sections, MPs are the APs that support the mesh function without differentiating the AP role.

On a WMN, mesh links are established through the Mesh Peering Management (MPM) protocol.

- Neighboring MP: an MP that directly communicates with another MP.
- Mesh link: a wireless link established between two neighboring MPs through a connection management protocol.
- Peer MP: a neighboring MP that has established a mesh link with an MP. Not all neighboring MPs are peer MPs.
- Mesh path: a wireless path comprising a series of mesh links between the source MP and destination MP.

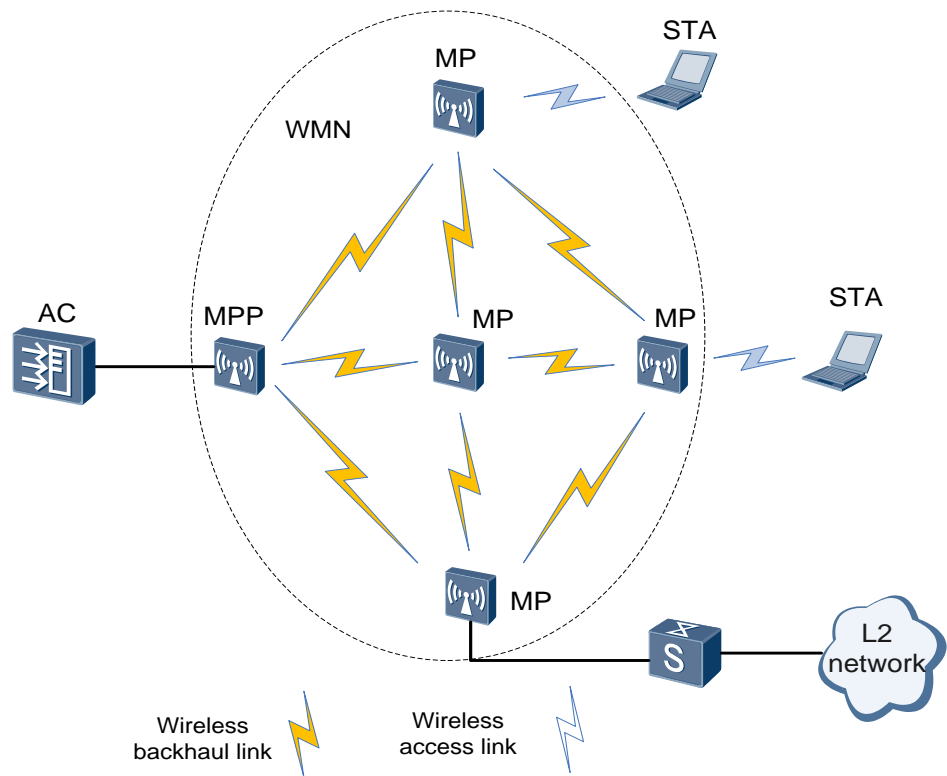
A WMN is a fully meshed WLAN. On a WMN, multiple mesh paths are available between any source and destination, and the transmission quality of these mesh paths varies according to the surrounding environment. Therefore, WMNs must support routing protocols to ensure that data frames are transmitted along the optimal path.

- Mesh gateway: an MPP that connects a WMN to another type of network.
- Mesh proxy: an MAP that enables a STA to connect to a WMN and then to a distribution system (DS).
- Mesh route: a route that is learned through routing management packets sent and forwarded by MPs on a WMN. A mesh route contains information about multiple next hops used for route forwarding.

Two VAP types are available on a mesh node: backhaul VAP and service VAP.

- Backhaul VAP: discovers neighboring MPs, establishes mesh links, backhauls data, and forwards routing management frames on a backhaul link to establish the route topology between mesh nodes. Only one backhaul VAP can be created on a radio.
- Service VAP: provides access for STAs. Multiple service VAPs can be created on a radio.

Figure 1-2 WLAN deployed using mesh technology



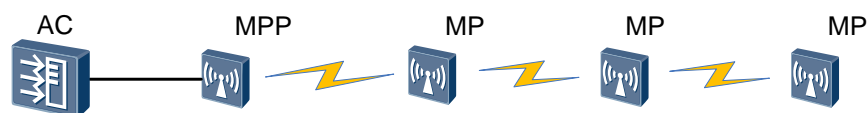
Mesh Network Architecture

Wireless mesh networking is mainly classified into three modes:

- Linear networking

In linear networking, you can preconfigure a neighbor for a node to connect to. 802.11s packets converted from 802.3 packets can be transmitted over links established between MPs and then transmitted over wireless links.

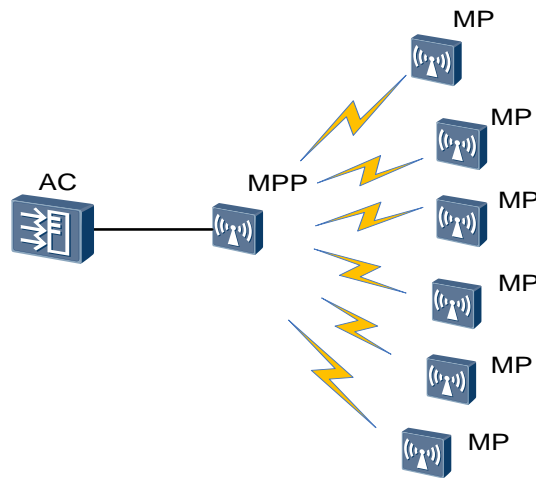
Figure 1-3 Linear networking



- Star networking

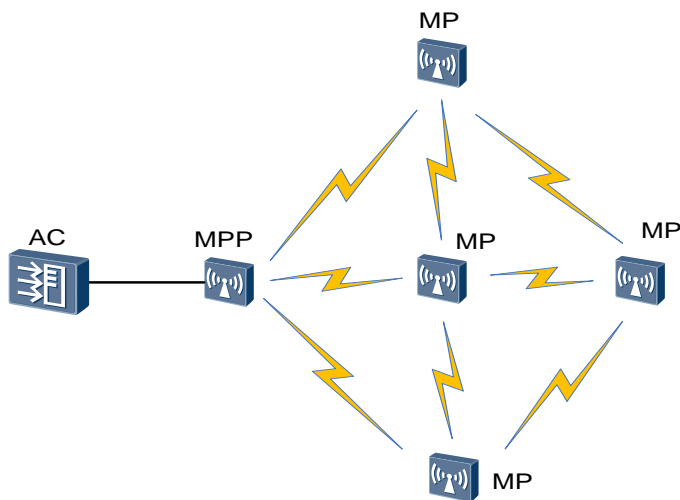
In star networking, all MPs depend on an MPP for data forwarding. All LAN data is transmitted through the MPP.

Figure 1-4 Star networking



- Mesh networking
In mesh networking, a redundant link is available when a mesh link becomes faulty. However, this networking will cause network loops. You can use mesh routing to selectively block redundant links to eliminate loops.

Figure 1-5 Mesh networking

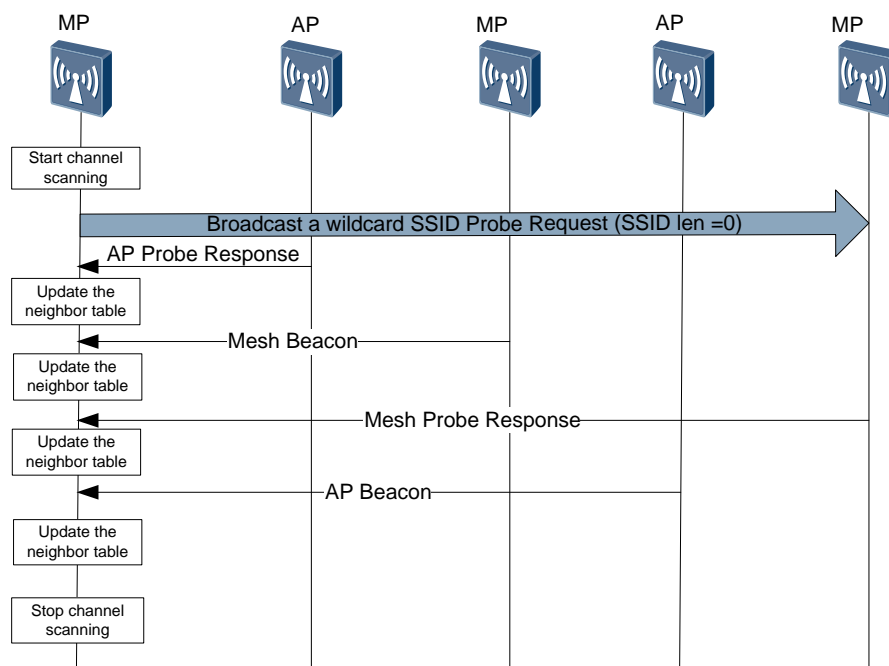


1.3.2 Mesh Establishment Process

Mesh Link Establishment

Mesh link establishment is a process of discovering a mesh neighbor. Mesh neighbor discovery is the first step to establish a WMN. An MP actively sends a Mesh Probe Request frame or passively listens on the Mesh Beacon frames sent from neighboring MPs to collect neighboring MP information. A Beacon or Probe frame contains information including the mesh ID, mesh configuration, and security capability.

Figure 1-6 Obtaining neighboring MP information in a specified channel through active scanning and passive scanning



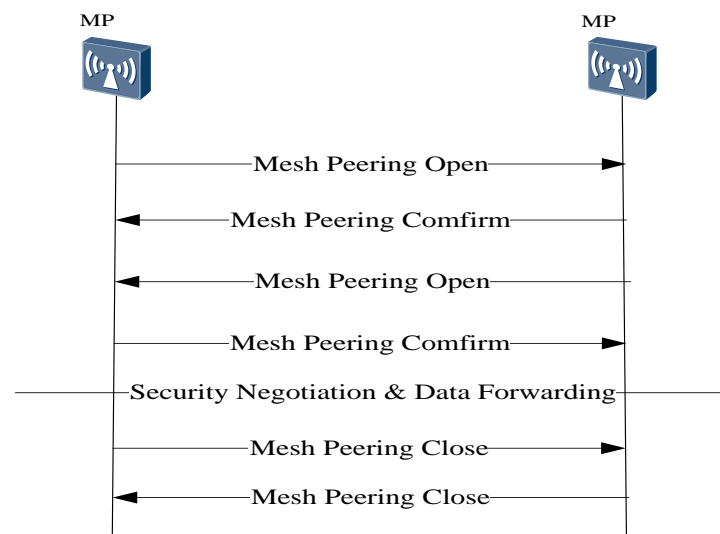
After mesh neighbor discovery is complete, mesh link establishment and teardown need to be performed. Mesh link establishment and teardown are implemented using three types of Mesh Action frames: Mesh Peering Open, Mesh Peering Confirm, and Mesh Peering Close frames.

Two MPs exchange Mesh Peering Open, Mesh Peering Confirm, and Mesh Peering Close frames twice to establish a mesh link. To ensure that a mesh link is successfully established, the two MPs must use the same mesh profile.

After a mesh link is established, the two MPs must perform subsequent authentication and security negotiation to establish an encrypted security link. The two MPs then can forward mesh data over the mesh link.

Either of the two MPs that establish a mesh link can send a Mesh Peering Close frame to the other MP to tear down the mesh link. The Mesh Peering Close frame contains the link teardown reason indicated by a reason code. After receiving the Mesh Peering Close frame, the other MP needs to respond with a Mesh Peering Close frame.

Figure 1-7 Mesh link establishment and teardown



Mesh Path Establishment

On a WMN, multiple mesh paths are available between any source and destination, and the transmission quality of these mesh paths varies according to the surrounding environment. Mesh routing algorithms ensure that data frames are always transmitted along the optimal mesh path. Mesh path establishment involves the following routing management frames:

- Root Announcement (RANN) frame: announces the presence of an MPP.
When a node is configured as an MPP, it periodically broadcasts a RANN frame.
- Proxy Update (PU) frames
A PU frame contains information about the STA associating with the MAP. An MAP sends a PU frame to each MPP in the gateway list periodically or when the MAP detects changes of its associated STA. By exchanging PU frames, an MP learns which mesh node is the proxy of STAs on a WMN.
- Route Request (RREQ) and Route Reply (RREP) frames
The source MP broadcasts a RREQ frame to establish a route to the destination MP. The destination replies with a RREP frame after receiving a RREQ frame.

When there are multiple next hops to the destination MP, static route selection and dynamic route selection are available:

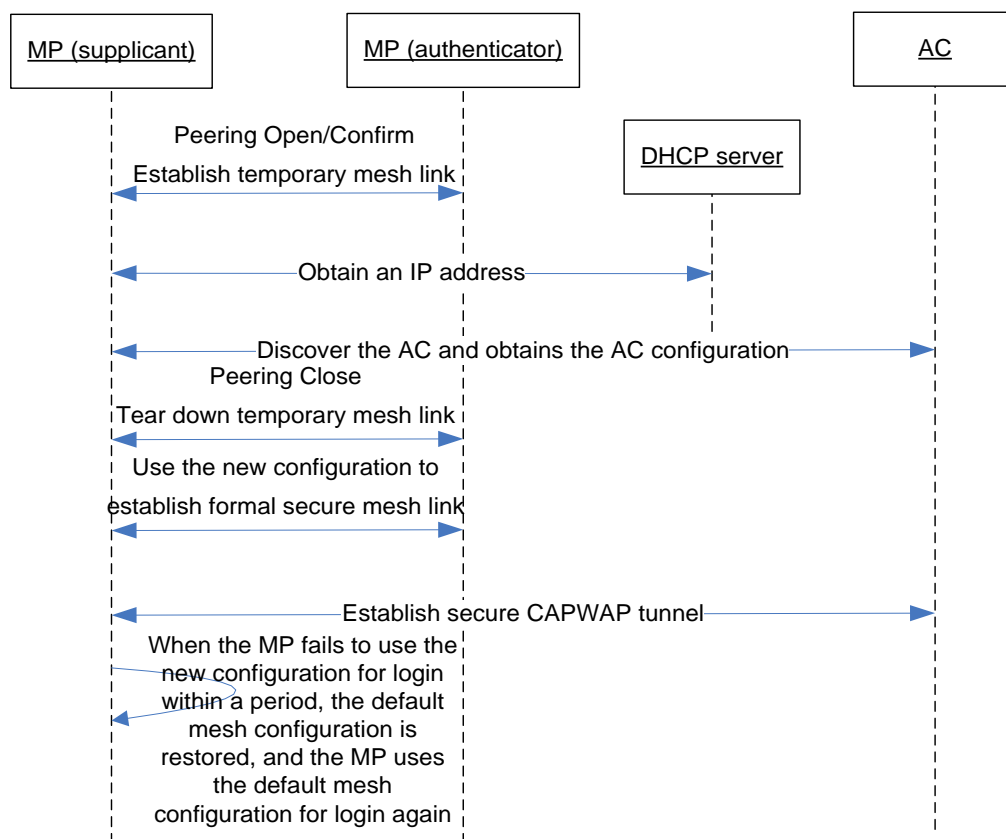
- In static route selection, the path with the minimum hops from the source node to the destination node is selected to construct the forwarding topology.
- In dynamic route selection, route forwarding policies are selected based on the expected transmission time (ETT) that dynamically reflects mesh path quality. The ETT is calculated based on packet loss ratio, packet length, and bandwidth. Paths with smaller ETT are selected to implement dynamic optimal path selection and load balancing between MPs.

Login of Mesh Nodes to an AC

The mesh feature supports the zero touch configuration function. This function allows you to perform a few MP offline management configurations on the AC without having to log in to

MPs to perform any configuration. MPs then can connect to the AC. This function facilitates the deployment of a large number of MPs. During the zero touch configuration, a mesh node automatically discovers and associates with the AC and obtains the configuration of a WMN from the AC.

Figure 1-8 Login using zero touch configuration



The process of MP login using zero touch configuration is as follows:

- Step 2** A new MP scans neighboring MPs, selects a neighboring MP that has associated with the AC as a peer MP, exchanges Mesh Peering Open and Mesh Peering Confirm frames with the peer MP using the default configuration, and establishes a temporary insecure mesh link with the peer MP. The Mesh Beacon and Mesh Probe Response frames sent by a neighboring MP carry the flag indicating whether the neighboring MP has associated with the AC. A new MP selects only the neighboring MP that has associated with the AC to establish a mesh link.
- Step 3** The new MP obtains an IP address from the DHCP server through the mesh link and completes the network configuration.
- Step 4** The new MP discovers and associates with the AC through the mesh link and obtains the mesh configuration and other configuration.
- Step 5** After the new MP obtains the new configuration, it sends a Mesh Peering Close frame to tear down the temporary insecure mesh link.

Step 6 The new MP exchanges Mesh Peering Open and Mesh Peering Confirm frames with the peer MP using the new mesh configuration and performs MAC address authentication and four-way handshake to negotiate the key required for communication between peers. The new MP then establishes a formal secure mesh link with the peer MP and re-establishes a secure CAPWAP tunnel with the AC.

----End

When the new MP fails to use the new mesh configuration for login within a specified period, the default mesh configuration is restored and the whole login process starts from step 1 until the MP establishes a secure CAPWAP tunnel with the AC using the new mesh configuration.

During configuration delivery, the following situations may occur:

- If the AC delivers the radio without mesh enabled, the MP disables backhaul VAPs, stops automatic discovery, and stops sending Keepalive packets. Service access parameters can be set, but mesh parameters cannot be set.
- If the AC delivers the radio with mesh enabled, the MP receives the mesh parameters set on the AC. If the original mesh parameters are modified, the MP uses the new mesh configuration to discover neighboring MPs and establish a mesh link with a neighboring MP.
- If the MP's version does not support the mesh function, the MP notifies the AC that it does not support mesh parameters. The AC still delivers other service parameters, but does not deliver mesh parameters.
- When the mesh-enabled MP receives VAP parameters delivered by the AC that does not support the mesh function, the MP automatically switches the radio to access mode to accept the VAP parameters.

Eliminating Mesh Network Loops

A WMN uses a mesh topology with redundant links between MPs. The following measures are defined to prevent broadcast storms:

- Time to live (TTL) check: A mesh frame contains the TTL field. After an MP receives a mesh frame, the MP reduces the TTL field of the frame by 1. If the TTL field of the frame becomes 0, the MP discards the frame. Otherwise, the MP forwards the frame.
- Duplicate frame detection: An MP checks the sequence number field in a mesh frame to determine whether a duplicate frame is received. An MP needs to maintain a table with <mesh source address, mesh Sequence Number> entries. These entries are generated based on the information in the recently received frames. If a received frame matches this table, the frame is a duplicate frame and is discarded. Otherwise, the frame is forwarded.

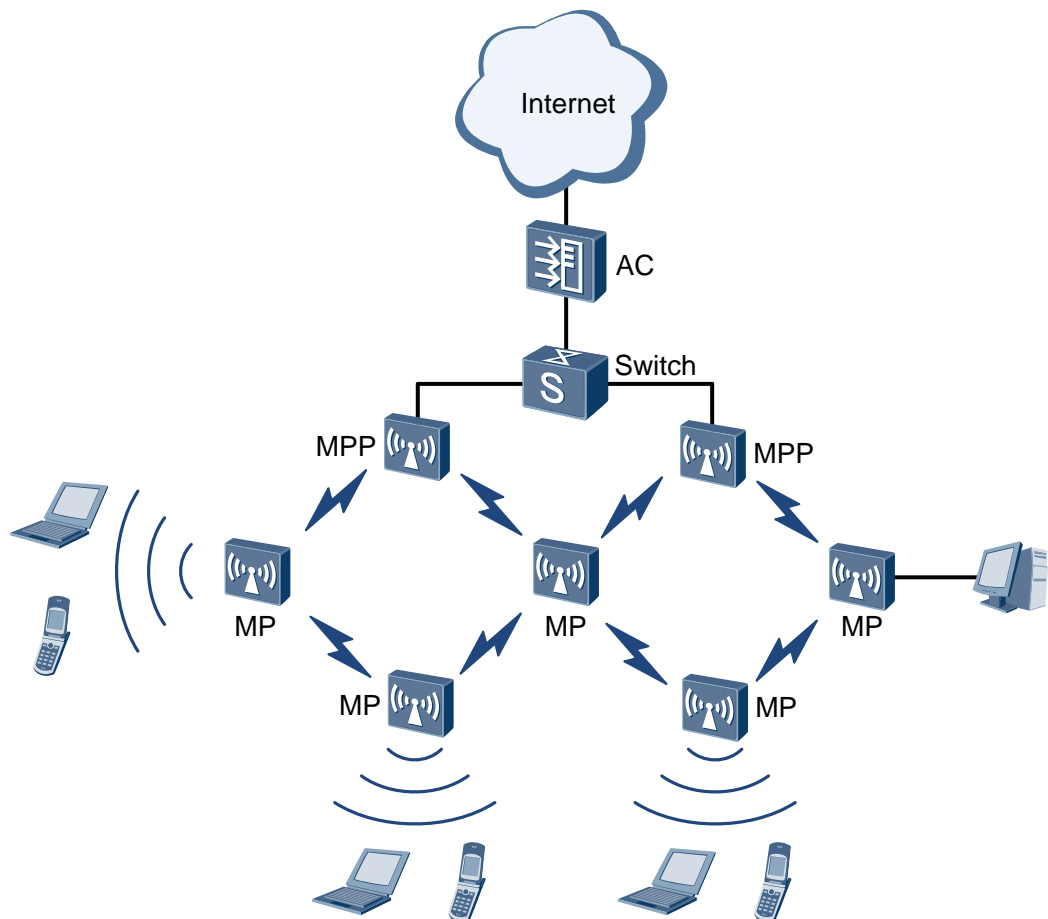


NOTE

Currently, spanning tree protocol packets cannot be transparently transmitted on a WMN. When a WMN with multiple MPPs, ensure that no loop exists between LANs and WMNs.

2 Mesh Applications

Figure 2-1 Mesh clients accessing the Internet through a WMN

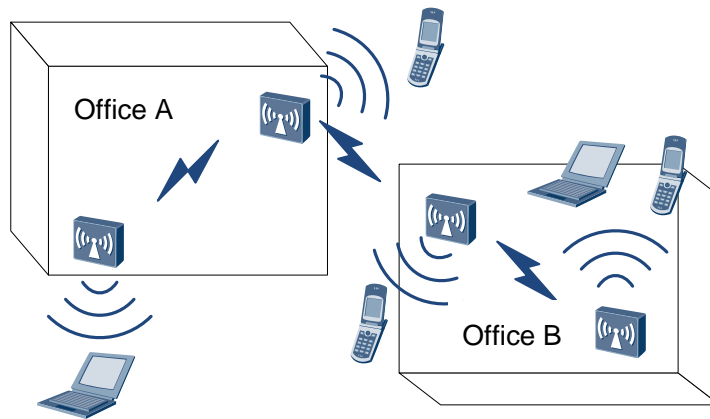


As shown in Figure 2-1, a WMN connects multiple MPs so that MPs can establish wireless multi-hop connections and wirelessly connect to the AC. Users are unaware of the differences between traditional WLAN and WMN because the only difference between them is the backbone layer. The following describes typical application scenarios of mesh technology.

2.1 Typical Application Scenarios

2.1.1 Indoor WMN

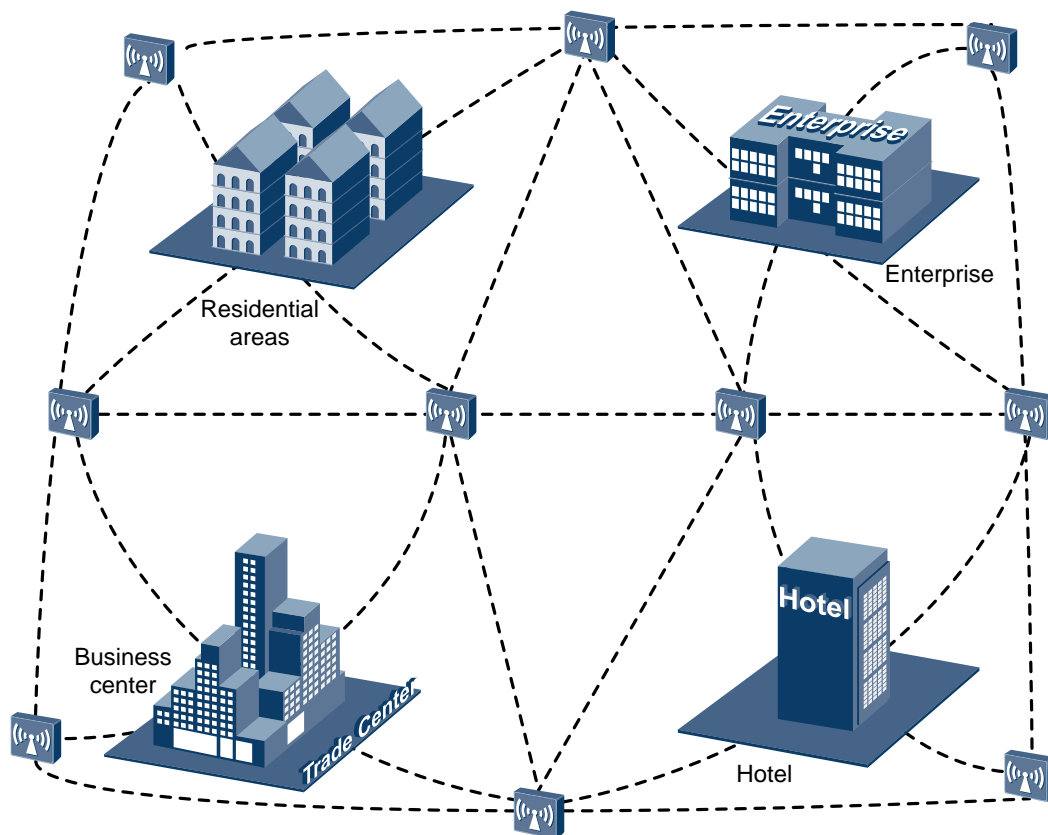
Figure 2-2 Indoor WMN networking



In homes, warehouses, subways, and office buildings, WLAN signals attenuate when they penetrate walls or other obstacles. Coverage holes exist when there is only one MP deployed. Indoor WMN networking can solve this problem. This networking expands the wireless network coverage and saves cabling costs. Figure 2-2 shows the indoor WMN networking.

2.1.2 Outdoor WMN

Figure 2-3 Outdoor WMN networking



In an outdoor WMN, two MPs can interconnect over dozens of kilometers. Mesh technology can implement data transmission across office buildings or areas. It overcomes the limitations of wired networks such as difficult deployment, high deployment costs, and low flexibility. Therefore, outdoor WMN networking applies to campus, plantations, mountain areas, and high buildings.

 **TIP**

Outdoor obstacles include trees and high buildings. The radian of the Earth must be considered for long-distance transmission. Select and install antennas based on site requirements.

2.2 Mesh Networking Planning

2.2.1 Mesh Backhaul Layer Planning

The mesh backhaul layer backhauls user data to the DS and forwards data from the DS to access users. Mesh backhaul layer planning determines the mesh topology and forwarding capability.

Gateway Deployment

Gateway deployment determines the MPP deployment positions on a WMN. Generally, a candidate list is made to specify the places to deploy MPPs, such as buildings and poles. MPPs are deployed in the places under optimal line of sight (LOS) condition in the candidate list.

Backhaul Topology

Typical backhaul topologies are shown in "Mesh Network Architecture" in section 1.3.1 "Introduction to Mesh". These topologies can be used as basic modules to build WMNs and apply to various mesh networking scenarios. The following describes the factors considered in backhaul topology planning:

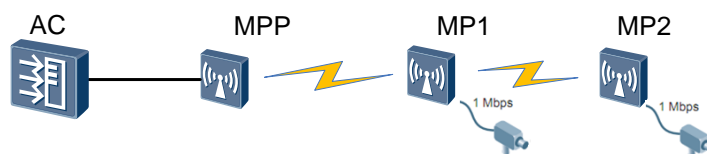
- **Maximum number of hops**
In a linear topology, if each MP uses multiple backhaul radios and transmits uplink traffic and downlink traffic on different channels, each hop has the same throughput. Currently, APs are single-band or dual-band APs. The best deployment method is to use a 2.4-GHz radio as an access radio and use a 5-GHz radio as a backhaul radio, forming single-band backhaul. In this scenario, the typical performance calculation formula is $1/N$ (N specifies the number of hops). This formula shows that performance is inversely proportional to the number of hops. In this case, a maximum number of four hops are recommended.
- **Maximum number of mesh nodes**
It is recommended that you deploy no more than 50 mesh nodes on a WMN and deploy 10 MPs per square kilometer. (The actual data needs to be verified). If more mesh nodes are required, divide the coverage area into smaller areas and increase the number of MPPs.
- **Maximum number of MPs allowed to connect to an MPP**

The number of MPs connecting to an MPP determines the throughput of users accessing wired networks. If many MPs connect to an MPP and users on the MPs use bandwidth-consuming backhaul services such as video surveillance, the MPP is likely to become the bottleneck of the WMN. Therefore, during network planning, control the number of MPs and users connecting to an MPP, increase the number of MPPs, and reserve sufficient bandwidth for potential services. You are not advised to start access VAPs on an MPP.

Backhaul Capability

- Backhaul channel selection
To ensure a higher throughput and better user experience, 5-GHz channels with better radio quality are often used as backhaul channels. During zero touch configuration of an MP, you must manually configure a backhaul channel on the AC.
- HT40 and HT20 selection
At the backhaul layer, 5-GHz radios are often used, so the HT40 mode is recommended to provide a higher backhaul rate. At the access layer, many handheld devices do not support the HT40 mode, and the HT40 mode is seldom used on 2.4-GHz radios. Therefore, the HT20 mode is often used at the access layer.
- Dynamic frequency selection (DFS)
If the backhaul channel is a DFS channel, channel switching occurs when radar signals are detected. Then user services may be interrupted for a long period. Therefore, do not use DFS channels as backhaul channels.
- MPP selection and backhaul layer performance deterioration in the case of a single channel

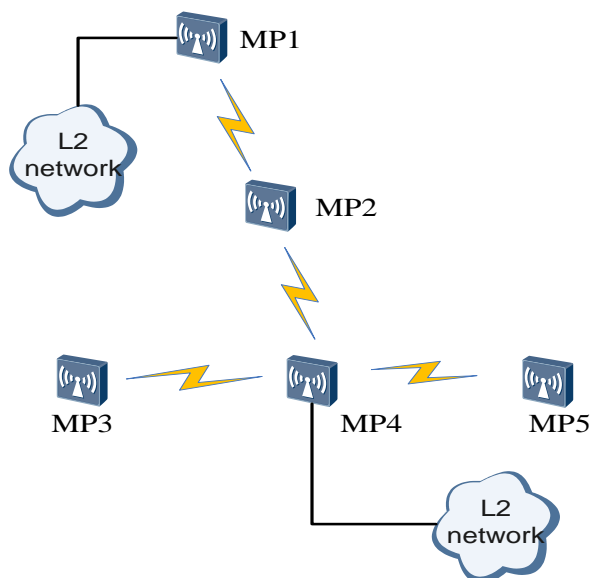
Figure 2-4 Backhaul layer performance deterioration model in the case of a single channel



In the scenario shown in Figure 2-4, all the MPs use the same 5-GHz channel, there is no interference signal in the surroundings, and all the MPs reside in the same collision area. Assume that the backhaul bandwidth of one hop is C Mbit/s and the number of hops is N . MP1 and MP2 each connect to a monitoring probe that generates fixed traffic of 1 Mbit/s. In this backhaul model, the 5-GHz channel is used once when traffic on MP1 needs to be transmitted to the AC, and the 5-GHz channel is used twice when traffic on MP2 needs to be transmitted to the AC. Therefore, the following formulas are available: The throughput peak value of each node is C/N ; the average MP throughput is $2C/(N*(N+1))$ (N indicates the total number of hops); the performance deterioration of the system is $(100 - 200/(N+1))\%$.

According to the preceding formulas, a higher throughput can be achieved on the network shown in Figure 2-5 if MP4 is an MPP and MP1 is not.

Figure 2-5 Backhaul layer performance deterioration analysis in the case of a single channel



2.2.2 Mesh Transmission Distance Planning

Signal Attenuation

During WDN networking, at least two MPs need to interconnect over a distance of several hundred meters or dozens of kilometers. Radio waves will attenuate during long-distance transmission. Assuming that radio waves are transmitted in a free space without reflection, refraction, diffraction, scattering, or absorption, the relationship between the path loss (PL) of radio waves and transmission distance is as follows:

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

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

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

The environmental factor n varies according to transmission environment and ranges from 2 to 5. Generally, n ranges from 4 to 5 in city centers with high user densities, ranges from 3 to 4 in common urban areas, and ranges from 2.5 to 3 in suburbs.

In a WMN networking, two MPs are deployed 1 km away from each other and work at a frequency of 5000 MHz. Assuming that radio waves are transmitted in a free space and n is 2, the PL is calculated as follows:

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

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

 **TIP**

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

Antenna Parameters

Antenna parameters include gain, lobe width, polarization direction, electrical downtilt, and front-to-rear ratio. The antenna gain and lobe width are the most parameters that determine the wireless network performance.

- **Antenna gain:** ratio of the power produced by the 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 transmit radio waves of different strengths in different directions, so lobe width is defined as the angle between two directions with 3 dB power lower than the maximum transmit power.

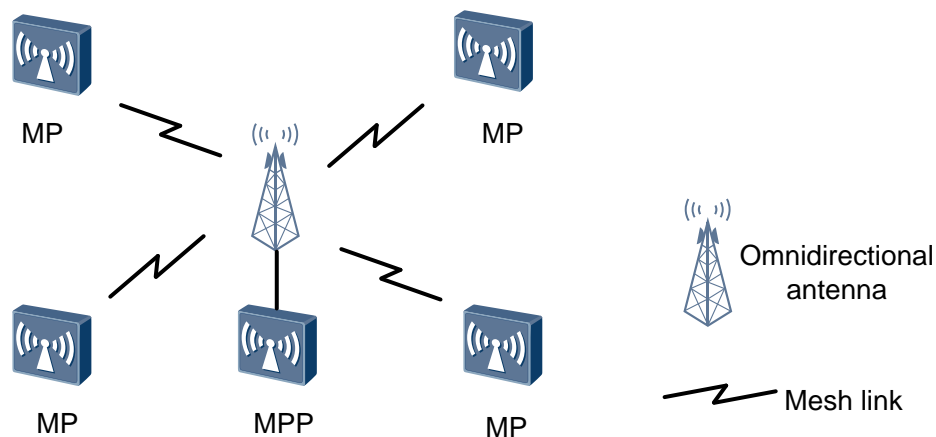
Generally, when the antenna gain increases, the lobe width decreases and radiant energy transmitted by the antenna is more concentrated.

Antenna Selection

Antennas are classified into omnidirectional antennas and directional antennas based on the signal radiation in horizontal or vertical planes.

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

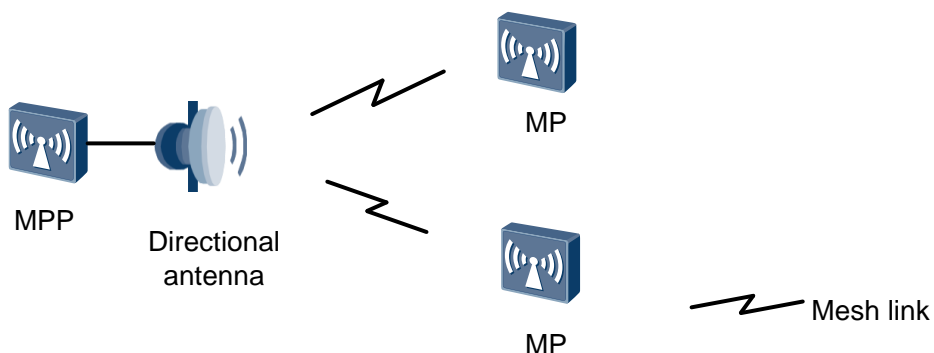
Omnidirectional antennas can be used for mesh links when many linked devices are deployed close to each other and distributed in a wide-angle range. The following figure shows a usage scenario of omnidirectional antennas. In this P2MP networking, an omnidirectional antenna can be used on the MPP to connect the MPs around the MPP.



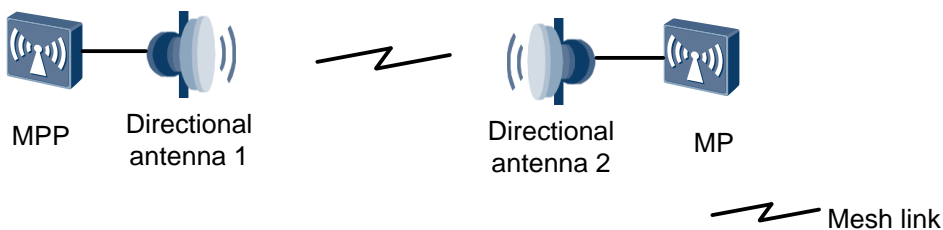
- **Directional antenna:** Signals from a directional antenna radiate in a certain angle. Directional antennas can concentrate energy and transmit signals to a specified direction. Therefore, directional antenna is a good choice when there are a few linked devices or the linked devices are concentrated in a certain angle.

In a P2MP WMN networking, pay attention to the lobe width when selecting directional antennas. The angle formed by the linked devices and antenna cannot exceed the lobe

width of the antenna so that the linked device is in the coverage area of the antenna. As shown in the following figure, the MPP uses a directional antenna to connect two MPs. The two MPs must be within the coverage area of the directional antenna.



In a P2P WMN networking, 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 networking.



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



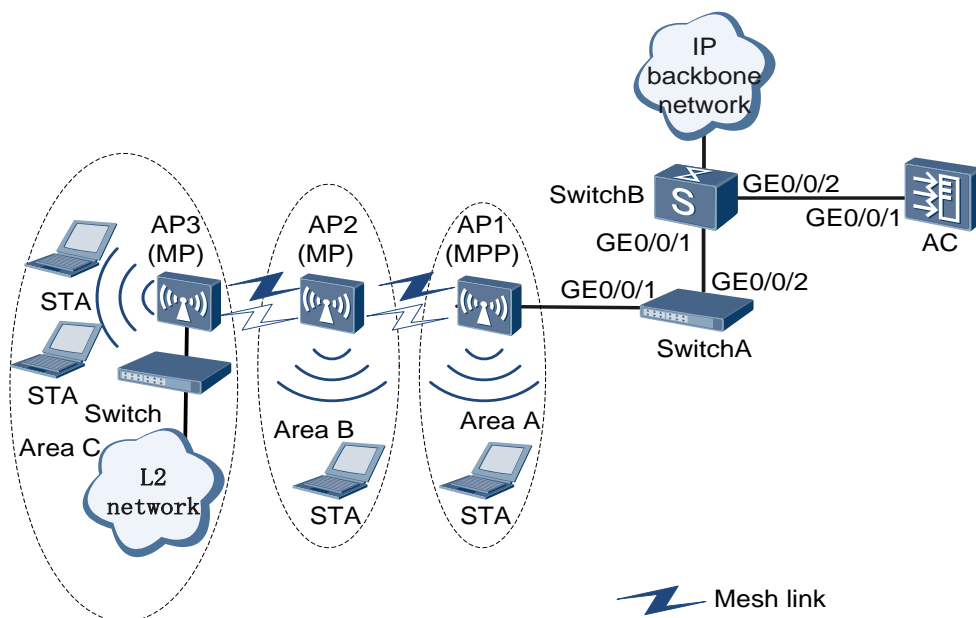
3 Typical Mesh Configuration Examples

3.1 Networking Requirements

To allow customers and employees to access the Internet wirelessly and reduce cabling costs, a company uses mesh technology for networking. Figure 3-1 shows the networking topology. In Figure 3-1:

- The AC6605 provides the AC function.
- The AC functions as a DHCP server to allocate IP addresses to MPs and STAs.
- The MPP connects to the AC in wired mode and functions as the gateway of the WMN.
- MPs 1 to 4 wirelessly connect to the MPP and form a WMN. MP3 and MP4 provide the wireless access function, and MP4 accesses a Layer 2 wired network.

Figure 3-1 Diagram of configuring the WLAN mesh service



3.2 Configuration Notes

- VAP15 on a 2.4-GHz radio and VAP31 on a 5-GHz radio are used as backhaul VAPs. If VAP15 and VAP31 have been configured and the mesh function is required, delete the configured VAP15 and VAP31, and then configure VAP15 and VAP31 as backhaul VAPs.
- To ensure sufficient service bandwidth, deploy no more than 50 MPs on the entire network and no more than four hops.
- Disable the calibration function in the radio profile to prevent impact of calibration on services. It is recommended that you configure an independent radio profile for the mesh function and add the MPs on the WMN to an independent region.
- You can change the country code on an AC. If you change the country code of an MPP on an AC, the country codes of the MPP and MPs may be different. In this case, the MPP and MPs support different channel sets, and MPs may fail to associate with the MPP. To prevent this problem, ensure that all the nodes on a WMN have the same country codes.
- The mesh function and WDS function are mutually exclusive and cannot be configured together.
- The HT20 mode and HT40plus/minus mode support different channel sets. You are advised to use the HT20 mode for user access and use the HT40 mode for data backhaul and ensure that devices on both sides use the same HT40plus/minus mode. Otherwise, the two devices cannot establish a mesh link.

3.3 Configuration Procedure

The following table lists AP roles and MAC addresses.

AP	Role	MAC Address
AP1	MPP	0046-4b59-1ee0
AP2	MP	0046-4b59-1d20
AP3	MP	0046-4b59-1d40

1. Connect AP1 to the AC.

Configure SwitchA. Add GE0/0/1 of SwitchA to management VLAN 100, set the PVID to VLAN 100, and configure GE0/0/1 and GE0/0/2 to allow packets from VLANs 100 to 106 to pass through.

 **NOTE**

You are advised to configure port isolation on GE0/0/1 that connects SwitchA to AP1. If port isolation is not configured, unnecessary packets are broadcast in the VLANs or WLAN users connected to different APs can communicate with each other at Layer 2.

```
<Huawei> system-view
[Huawei] sysname SwitchA
[SwitchA] vlan batch 100 to 103
[SwitchA] interface gigabitEthernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] port link-type trunk
```



```
[SwitchA-GigabitEthernet0/0/1] port trunk pvid vlan 100
[SwitchA-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 103
[SwitchA-GigabitEthernet0/0/1] port-isolate enable
[SwitchA-GigabitEthernet0/0/1] quit
[SwitchA] interface gigabitEthernet 0/0/2
[SwitchA-GigabitEthernet0/0/2] port link-type trunk
[SwitchA-GigabitEthernet0/0/2] port trunk allow-pass vlan 100 to 103
[SwitchA-GigabitEthernet0/0/2] quit
```

Configure SwitchB. Configure GE0/0/1 to allow packets from VLAN 100 to VLAN 103 to pass through and GE0/0/2 to allow packets from VLAN 100 to pass through.

```
<Huawei> system-view
[Huawei] sysname SwitchB
[SwitchB] vlan batch 100 to 103
[SwitchB] interface gigabitEthernet 0/0/1
[SwitchB-GigabitEthernet0/0/1] port link-type trunk
[SwitchB-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 103
[SwitchB-GigabitEthernet0/0/1] quit
[SwitchB] interface gigabitEthernet 0/0/2
[SwitchB-GigabitEthernet0/0/2] port link-type trunk
[SwitchB-GigabitEthernet0/0/2] port trunk allow-pass vlan 100
[SwitchB-GigabitEthernet0/0/2] quit
```

Configure GE0/0/1 that connects the AC to SwitchB to allow packets from VLAN 100 to VLAN 103 to pass through.

```
<Huawei> system-view
[Huawei] sysname AC
[AC] vlan batch 100 to 103
[AC] interface gigabitEthernet 0/0/1
[AC-GigabitEthernet0/0/1] port link-type trunk
[AC-GigabitEthernet0/0/1] lineate-port vlan untagged 101 to 103
[AC-GigabitEthernet0/0/1] quit
```

2. Configure SwitchB to assign IP addresses to STAs and the AC to assign IP addresses to APs.

Configure SwitchB as a DHCP server to assign IP addresses to STAs from IP address pools on VLANIF interfaces.

```
[SwitchB] dhcp enable
[SwitchB] interface vlanif 101
[SwitchB-Vlanif101] ip address 192.168.1.1 24
[SwitchB-Vlanif101] dhcp select interface
[SwitchB-Vlanif101] quit
[SwitchB] interface vlanif 102
[SwitchB-Vlanif102] ip address 192.168.2.1 24
[SwitchB-Vlanif102] dhcp select interface
[SwitchB-Vlanif102] quit
[SwitchB] interface vlanif 103
[SwitchB-Vlanif103] ip address 192.168.3.1 24
[SwitchB-Vlanif103] dhcp select interface
[SwitchB-Vlanif103] quit
```

Enable DHCP on the AC and configure the AC to assign IP addresses to APs from an IP address pool on a VLANIF interface.

```
[AC] dhcp enable
[AC] interface vlanif 100
[AC-Vlanif100] ip address 192.168.10.1 24
[AC-Vlanif100] dhcp select interface
[AC-Vlanif100] quit
```

3. Configure AC system parameters.

Configure the country code.

```
[AC] wlan ac-global country-code cn
Warning: Committing configuration may cause service interruption,continue?[Y/N]
] y
```

Configure the AC ID and carrier ID.

```
[AC] wlan ac-global ac id 1 carrier id ctc
```

Configure the source interface.

```
[AC] wlan
[AC-wlan-view] wlan ac source interface vlanif 100
```

4. Manage APs on the AC.

Set AP authentication mode to MAC address authentication.

```
[AC-wlan-view] ap-auth-mode mac-auth
```

Add APs offline.

```
[AC-wlan-view] ap id 1 ap-type AP6010DN-AGN mac 0046-4b59-1ee0
[AC-wlan-ap-1] quit
[AC-wlan-view] ap id 2 ap-type AP6010DN-AGN mac 0046-4b59-1d20
[AC-wlan-ap-2] quit
[AC-wlan-view] ap id 3 ap-type AP6010DN-AGN mac 0046-4b59-1d40
[AC-wlan-ap-3] quit
```

Configure the Ethernet interfaces that connect APs to SwitchA to allow packets from VLAN 101 to pass through.



NOTE

If MPP Ethernet interfaces are not configured to allow packets carrying service VLAN tags to pass through, communication fails.

```
[AC] wlan
[AC-wlan-view] ap id 1
[AC-wlan-ap-1] lineate-port vlan tagged 101 to 103
[AC-wlan-ap-1] quit
[AC-wlan-view] quit
```

Create AP regions 101, 102, and 103.

```
[AC-wlan-view] ap-region id 101
[AC-wlan-ap-region-101] quit
```

```
[AC-wlan-view] ap-region id 102
[AC-wlan-ap-region-102] quit
[AC-wlan-view] ap-region id 103
[AC-wlan-ap-region-103] quit
```

Add AP1 to AP region 101, AP2 to AP region 102, and AP3 to AP region 103.

```
[AC-wlan-view] ap id 1
[AC-wlan-ap-1] region-id 101
[AC-wlan-ap-1] quit
[AC-wlan-view] ap id 2
[AC-wlan-ap-2] region-id 102
[AC-wlan-ap-2] quit
[AC-wlan-view] ap id 3
[AC-wlan-ap-3] region-id 103
[AC-wlan-ap-3] quit
```

5. Configure mesh parameters.

Create a WMM profile named **wp01** and retain the default settings in the profile.

```
[AC-wlan-view] wmm-profile name wp01 id 1
[AC-wlan-wmm-prof-wp01] quit
```

Create a radio profile named **rp02**. Set the radio type to 802.11an, GI mode to short GI, the channel mode to manual, and the DTIM interval to 1, and retain the default settings of the other parameters in the profile. Bind the radio profile to WMM profile **wp01**.

```
[AC-wlan-view] radio-profile name rp02 id 1
[AC-wlan-radio-prof-rp02] wmm-profile name wp01
[AC-wlan-radio-prof-rp02] radio-type 80211an
Warning: Modify the Radio type may cause some parameters of Radio resume default
t value, are you sure to continue?[Y/N]:y
[AC-wlan-radio-prof-rp02] 80211n guard-interval-mode short
[AC-wlan-radio-prof-rp02] channel-mode fixed
[AC-wlan-radio-prof-rp02] dtim-interval 1
[AC-wlan-radio-prof-rp02] quit
```

Create a mesh whitelist named **mesh01**.

```
[AC-wlan-view] mesh-whitelist name mesh01
[AC-wlan-mesh-whitelist-mesh01] peer ap mac 0046-4b59-1d20
[AC-wlan-mesh-whitelist-mesh01] peer ap mac 0046-4b59-1d40
[AC-wlan-mesh-whitelist-mesh01] peer ap mac 0046-4b59-1ee0
[AC-wlan-mesh-whitelist-mesh01] quit
```

Create a security profile **sp01**, set the security and authentication policy to WPA2-PSK, set the authentication key to 12345678, and set the encryption mode to CCMP.

NOTE

On a WMN, the APs that connect to each other wirelessly support only security policy WPA2+PSK+CCMP.

```
[AC-wlan-view] security-profile name sp01
[AC-wlan-sec-prof-sp01] security-policy wpa2
```

```
[AC-wlan-sec-prof-sp01] wpa2 authentication-method psk pass-phrase simple 12345678
encryption-method ccmp
[AC-wlan-sec-prof-sp01] quit
```

Create a mesh profile named **mesh01**.

```
[AC-wlan-view] mesh-profile name mesh01
[AC-wlan-mesh-prof-mesh01] mesh-id ChinaNet01
[AC-wlan-mesh-prof-mesh01] mesh-link-rssi threshold -70
[AC-wlan-mesh-prof-mesh01] mesh-max-link 3
[AC-wlan-mesh-prof-mesh01] link report-interval 30
[AC-wlan-mesh-prof-mesh01] security-profile name sp01
[AC-wlan-mesh-prof-mesh01] quit
```

6. Configure a WLAN radio profile and WLAN-ESS interfaces.

Create a radio profile **rp01**, retain the default settings in the profile, and bind it to the WMM profile **wp01**.

```
[AC-wlan-view] radio-profile name rp01 id 0
[AC-wlan-radio-prof-rp01] wmm-profile name wp01
[AC-wlan-radio-prof-rp01] quit
[AC-wlan-view] quit
```

Create WLAN-ESS interfaces.

```
[AC] interface wlan-ess 1
[AC-Wlan-Ess1] port hybrid pvid vlan 101
[AC-Wlan-Ess1] port hybrid untagged vlan 101
[AC-Wlan-Ess1] quit
[AC] interface wlan-ess 2
[AC-Wlan-Ess2] port hybrid pvid vlan 102
[AC-Wlan-Ess2] port hybrid untagged vlan 102
[AC-Wlan-Ess2] quit
[AC] interface wlan-ess 3
[AC-Wlan-Ess3] port hybrid pvid vlan 103
[AC-Wlan-Ess3] port hybrid untagged vlan 103
[AC-Wlan-Ess3] quit
```

7. Configure a mesh profile and service sets.

Create a traffic profile **tp01** and retain the default settings in the profile.

```
[AC] wlan
[AC-wlan-view] traffic-profile name tp01
[AC-wlan-traffic-prof-tp01] quit
```

Create and configure a service set with the name **ss01** and SSID **ChinaSer01**.

```
[AC-wlan-view] service-set name ss01
[AC-wlan-service-set-ss01] traffic-profile name tp01
[AC-wlan-service-set-ss01] security-profile name sp01
[AC-wlan-service-set-ss01] ssid ChinaSer01
[AC-wlan-service-set-ss01] service-vlan 101
[AC-wlan-service-set-ss01] wlan-ess 1
[AC-wlan-service-set-ss01] forward-mode direct-forward
[AC-wlan-service-set-ss01] quit
```

Create and configure a service set with the name **ss02** and SSID **ChinaSer02**.

```
[AC-wlan-view] service-set name ss02
[AC-wlan-service-set-ss02] traffic-profile name tp01
[AC-wlan-service-set-ss02] security-profile name sp01
[AC-wlan-service-set-ss02] ssid ChinaSer02
[AC-wlan-service-set-ss02] service-vlan 102
[AC-wlan-service-set-ss02] wlan-ess 2
[AC-wlan-service-set-ss02] forward-mode direct-forward
[AC-wlan-service-set-ss02] quit
```

Create and configure a service set with the name **ss03** and SSID **ChinaSer03**.

```
[AC-wlan-view] service-set name ss03
[AC-wlan-service-set-ss03] traffic-profile name tp01
[AC-wlan-service-set-ss03] security-profile name sp01
[AC-wlan-service-set-ss03] ssid ChinaSer03
[AC-wlan-service-set-ss03] service-vlan 103
[AC-wlan-service-set-ss03] wlan-ess 3
[AC-wlan-service-set-ss03] forward-mode direct-forward
[AC-wlan-service-set-ss03] quit
```

Create a mesh VAP on radio 1 of AP1 and set the role of radio 1 to mesh-portal (MPP), and bind the mesh whitelist **mesh01** and mesh profile **mesh01** to the radio. Create a service VAP on radio 0 of AP1 and bind radio profile **rp01** and service set **ss01** to radio 0.

```
[AC-wlan-view] ap 1 radio 0
[AC-wlan-radio-1/0] radio-profile name rp01
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-1/0] service-set name ss01
[AC-wlan-radio-1/0] quit
[AC-wlan-view] ap 1 radio 1
[AC-wlan-radio-1/1] radio-profile name rp02
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] mesh-role mesh-portal
[AC-wlan-radio-1/1] mesh-whitelist name mesh01
[AC-wlan-radio-2/1] mesh-profile name mesh01
[AC-wlan-radio-1/1] channel 40mhz-plus 157
[AC-wlan-radio-1/1] quit
```

Create a mesh VAP on radio 1 of AP2 and set the role of radio 1 to mesh-node (MP), and bind the mesh whitelist **mesh01** and mesh profile **mesh01** to the radio. Create a service VAP on radio 0 of AP2 and bind radio profile **rp01** and service set **ss02** to radio 0.

```
[AC-wlan-view] ap 2 radio 0
[AC-wlan-radio-2/0] radio-profile name rp01
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-2/0] service-set name ss02
[AC-wlan-radio-2/0] quit
[AC-wlan-view] ap 2 radio 1
[AC-wlan-radio-2/1] radio-profile name rp02
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] mesh-role mesh-node
[AC-wlan-radio-2/1] mesh-whitelist name mesh01
```

```
[AC-wlan-radio-2/1] mesh-profile name mesh01
[AC-wlan-radio-2/1] channel 40mhz-plus 157
[AC-wlan-radio-2/1] quit
```

Create a mesh VAP on radio 1 of AP3 and set the role of radio 1 to mesh-node (MP), and bind the mesh whitelist **mesh01** and mesh profile **mesh01** to the radio. Create a service VAP on radio 0 of AP3 and bind radio profile **rp01** and service set **ss03** to radio 0.

```
[AC-wlan-view] ap 3 radio 0
[AC-wlan-radio-3/0] radio-profile name rp01
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-3/0] service-set name ss03
[AC-wlan-radio-3/0] quit
[AC-wlan-view] ap 3 radio 1
[AC-wlan-radio-3/1] radio-profile name rp02
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] mesh-role mesh-node
[AC-wlan-radio-3/1] mesh-whitelist name mesh01
[AC-wlan-radio-1/1] mesh-profile name mesh01
[AC-wlan-radio-3/1] channel 40mhz-plus 157
[AC-wlan-radio-3/1] quit
```

8. Deliver parameters to APs.

The AP parameters configured on the AC take effect only after they are delivered to APs.

```
[AC-wlan-view] commit ap 1
Warning: Committing configuration may cause service interruption,continue?[Y/N]
] y
[AC-wlan-view] commit ap 2
Warning: Committing configuration may cause service interruption,continue?[Y/N]
] y
[AC-wlan-view] commit ap 3
Warning: Committing configuration may cause service interruption,continue?[Y/N]
] y
```

Run the **display ap all** command on the AC to check whether the status of APs is normal and run the **display mesh-link all** command on the AC to check whether mesh links have been established. If the command output shows that APs are in normal state and displays mesh link information, APs have established mesh links.

```
[AC-wlan-view] display ap all
All AP information (Normal-3,UnNormal-0):
-----
AP      AP              AP              Profile  AP      AP
ID      Type            MAC              ID/Region  State   Sysname
-----
1       AP6010DN-AGN    0046-4b59-1ee0  0/101    normal  ap-1
2       AP6010DN-AGN    0046-4b59-1d20  0/102    normal  ap-2
3       AP6010DN-AGN    0046-4b59-1d40  0/103    normal  ap-3
-----
Total number: 3
```

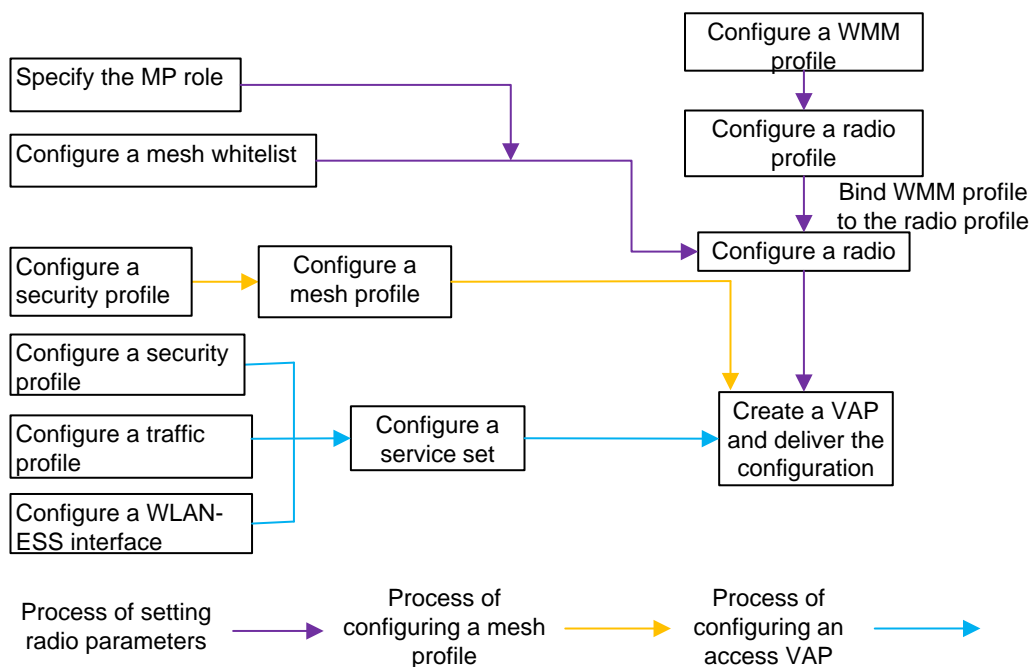
```
[AC-wlan-view] display mesh-link all
```

AP ID	Radio ID	Mesh-link ID	WLAN ID	Peer MAC
1	1	0	16	0046-4b59-1d2f
1	1	1	16	0046-4b59-1d4f
2	1	0	16	0046-4b59-1d4f
2	1	1	16	0046-4b59-1eef
3	1	0	16	0046-4b59-1d2f
3	1	1	16	0046-4b59-1eef

Total: 6

----End

Figure 3-2 WLAN mesh service configuration flowchart



----End

3.4 Configuration Files

- Configuration file of SwitchA

```
#
sysname SwitchA
#
vlan batch 100 to 103
#
interface GigabitEthernet0/0/1
port link-type trunk
```

```
port trunk pvid vlan 100
port trunk allow-pass vlan 100 to 103
port-isolate enable group 1
#
interface GigabitEthernet0/0/2
port link-type trunk
port trunk allow-pass vlan 100 to 103
#
return
```

- Configuration file of SwitchB

```
#
sysname SwitchB
#
vlan batch 100 to 103
#
dhcp enable
#
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 GigabitEthernet0/0/1
port link-type trunk
port trunk allow-pass vlan 100 to 103
port-isolate enable group 1
#
interface GigabitEthernet0/0/2
port link-type trunk
port trunk allow-pass vlan 100
#
return
```

- Configuration file of the AC

```
#
sysname AC
#
vlan batch 100
#
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 GigabitEthernet0/0/1
```



```
port link-type trunk
port trunk allow-pass vlan 100 to 103
#
interface Wlan-Ess1
port hybrid pvid vlan 101
port hybrid untagged vlan 101
#
interface Wlan-Ess2
port hybrid pvid vlan 102
port hybrid untagged vlan 102
#
interface Wlan-Ess3
port hybrid pvid vlan 103
port hybrid untagged vlan 103
#
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 0046-4b59-1ee0 sn AB37026279
region-id 101
lineate-port vlan untagged 101 to 103
ap id 2 type-id 19 mac 0046-4b59-1d20 sn AB37034085
region-id 102
ap id 3 type-id 19 mac 0046-4b59-1d40 sn AB37010864
region-id 103
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 simple 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
mesh-profile name mesh01 id 0
security-profile id 0
mesh-max-link 3
mesh-link-rssi threshold -70
```

```
radio-profile name rp01 id 0
wmm-profile id 0
radio-profile name rp02 id 1
radio-type 80211an
channel-mode fixed
wmm-profile id 1
80211n guard-interval-mode short
mesh-whitelist name mesh01 id 0
peer ap mac 0046-4b59-1ee0
peer ap mac 0046-4b59-1d20
peer ap mac 0046-4b59-1d40
ap 1 radio 0
radio-profile id 0
service-set id 0 wlan 1
ap 1 radio 1
radio-profile id 1
mesh-role mesh-portal
channel 40MHz-plus 157
mesh-whitelist id 0
mesh-profile id 0
ap 2 radio 0
radio-profile id 0
service-set id 0 wlan 1
ap 2 radio 1
radio-profile id 1
channel 40MHz-plus 157
mesh-whitelist id 0
mesh-profile id 0
ap 3 radio 0
radio-profile id 0
service-set id 0 wlan 1
ap 3 radio 1
radio-profile id 1
channel 40MHz-plus 157
mesh-whitelist id 0
mesh-profile id 0
#
return
```

A Abbreviations

Abbreviation	Full Spelling
WLAN	Wireless Local Area Networks
AC	Access controller
AP	Access point
MPP	Mesh portal point
MP	Mesh point
STA	Station
MPM	Mesh peering management
DS	Distribution system