Huawei CloudCampus WLAN Wireless Bridging

Technology White Paper

HUAWEI

Executive Summary

This document describes wireless distribution system (WDS) and mesh technologies used on wireless access devices. WDS and mesh technologies can implement long-distance wireless connections between networks, expand the network coverage area, and reduce network deployment costs.

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

Contents

Executive Summary ii

1 Overview 1

1.1 Wireless Bridging Technologies 1

1.1.1 WDS 1

1.1.2 Mesh 1

1.2 WDS Implementation 2

1.2.1 Introduction to WDS 2

1.2.2 WDS Setup 4

1.3 WDS Networking Mode 6

1.3.1 P2P Networking 6

1.3.2 P2MP Networking 7

1.4 Mesh Implementation 8

1.4.1 Basic Concepts 8

1.4.2 Mesh Link Establishment 10

1.4.3 Login of MPs to an AC 11

1.4.4 Mesh Route Establishment 13

1.4.5 Data Packet Forwarding 14

1.4.6 Eliminating Mesh Network Loops 15

1.5 Mesh Networking Modes 15

1.5.1 Linear Networking 15

1.5.2 Star Networking 16

1.5.3 Mesh Networking 16

1.5.4 Multi-MPP Networking 16

2 Application Scenario 18

2.1 WDS Networking 18

2.1.1 Indoor WDS Networking 19

2.1.2 Outdoor WDS Networking 19

2.2 WDS Network Planning 22

2.2.1 Transmission Distance Planning 22

2.2.2 Network Bandwidth Planning 24

2.3 Mesh Networking Scenarios 28

2.3.1 Wireless Coverage 28

2.3.2 Road Surveillance Backhaul 28
2.3.3 Long-Distance Wide Coverage 29
2.3.4 Dual-Link Reliable Backhaul 30
2.4 Mesh Networking Planning 30
2.4.1 Mesh Backhaul Layer Planning 30
2.4.2 Mesh Transmission Distance Planning 32

3 Typical Configuration Examples 36

3.1 WDS Configuration Example 36
3.1.1 Networking Requirements 36
3.1.2 Configuration Analysis 37
3.2 Mesh Configuration Example 38
3.2.1 Networking Requirements 38
3.2.2 Configuration Analysis 39

A Acronyms and Abbreviations 41

1 Overview

1.1 Wireless Bridging Technologies

1.1.1 WDS

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.

802.11 wireless technology has been widely used on home, SOHO, and enterprise networks. Users can easily access the Internet over wireless LANs (WLANs). On a wireless network, access points (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 with each other using cables, switches, and power supplies. This increases network costs and prolongs the network construction period. In this case, WDS technology can be used to connect APs wirelessly, facilitating WLAN construction in a complex environment.

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. WDS technology facilitates network deployment and device installation.

1.1.2 Mesh

A wireless mesh network (WMN) is a communications network that consists of multiple wirelessly connected 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.

On a traditional 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.

1.2 WDS Implementation

1.2.1 Introduction to WDS

Concepts

On a traditional WLAN, you can create service virtual APs (VAPs) on APs to provide access for 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 WVL: a WVL used to transmit service data on a WDS network.
- Management WVL: a WVL used to transmit management data on a WDS network. After the wireless bridge function is enabled on APs, the APs automatically set up management WVLs. Management WVLs transmit only management and configuration packets.

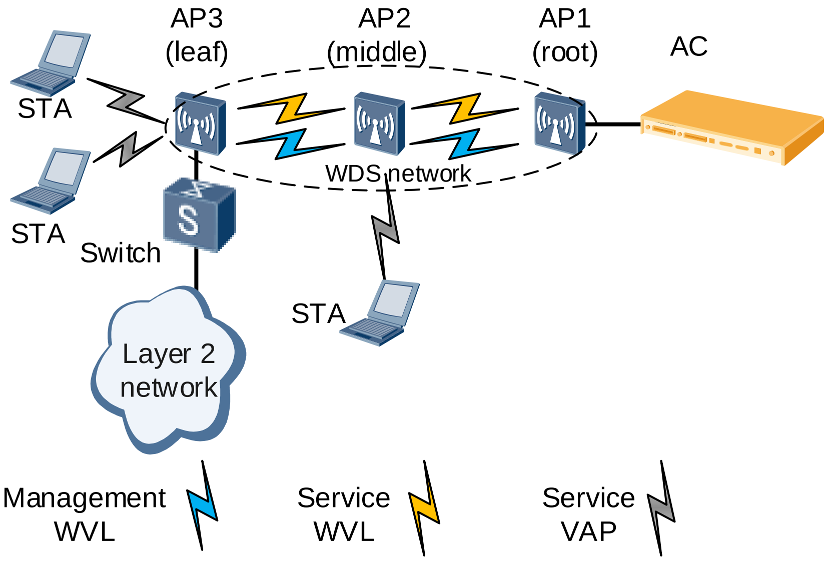
Depending on an AP's location on a WDS network, a wireless bridge works in root, middle, or leaf mode.

- Root: The AP functions as a root node to directly connect to an access controller (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. The wired interface on an AP works in root or endpoint mode depending on the AP's location.

- Root interface: connects to an AC.
- Endpoint interface: connects to a switch or host.

Figure 1-1 WDS network

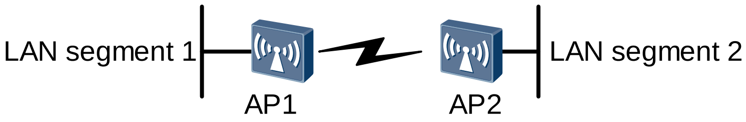


WDS Architecture

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

- P2P mode

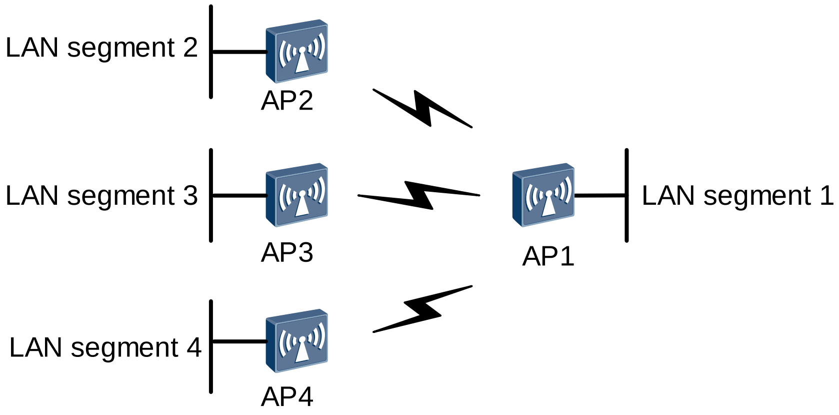
Figure 1-2 P2P networking



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 Media Access Control (MAC) address can be configured on each AP to determine the bridging link to be set up.

- P2MP mode

Figure 1-3 PM2P networking



As shown in Figure 1-3, on a P2MP network, AP1 is used as the central AP, and all the other APs establish wireless bridge links only with AP1. This implements connection of multiple networks. LAN segments 2, 3, and 4 can communicate with LAN segment 1 only 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 a management WVL between APs. The AP connects to an AC through the management WVL and obtains configurations from the AC. A service 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 connection Keepalive packets to each other to maintain the connection. If one end does not respond for a long time, 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.

An 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 in which WDS is 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 in which WDS is 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 neighboring 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) to detect loops.

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

1.3 WDS Networking Mode

1.3.1 P2P Networking

Figure 1-4 P2P networking

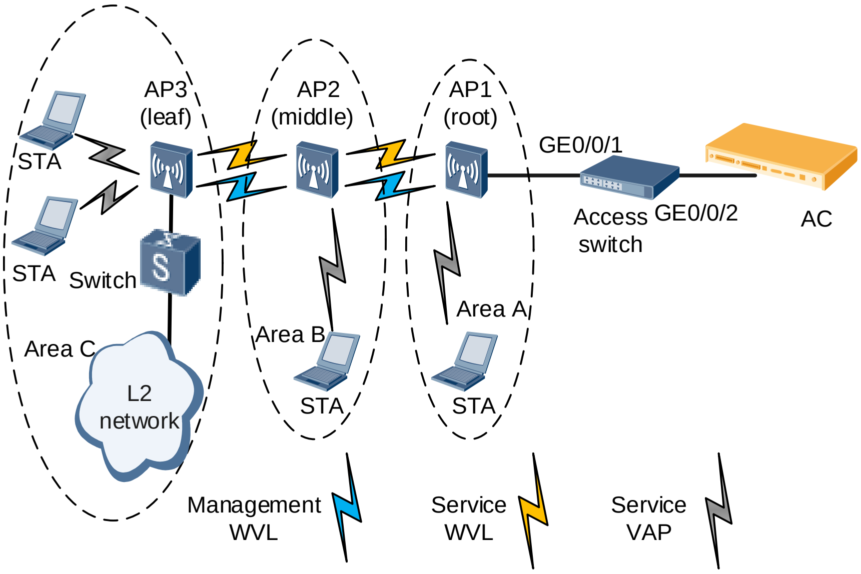


Figure 1-4 shows the P2P WDS topology. The root AP connects only to a middle or leaf AP in bridging mode. Dual-band APs are used on the actual network. The APs use the 5 GHz radio for radio backhaul and the 2.4 GHz radio to provide access for STAs.

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 • Area A: VLAN 101 for wireless services • Area B: VLAN 102 for wireless services • Area C: VLAN 103 for wireless services • Area C: VLANs 104, 105, and 106 on wired interfaces of AP3

- Management WDS links do not support STP; therefore, other measures must be taken to ensure that no loop will occur on the management WDS 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.
- 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 bridge 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 the middle AP and leaf AP.

1.3.2 P2MP Networking

Figure 1-5 P2MP networking

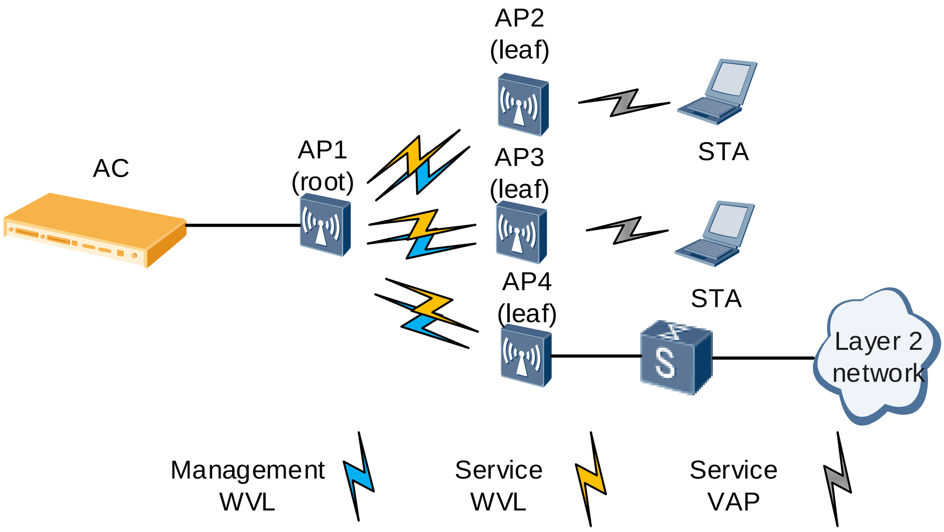


Figure 1-5 shows the P2MP WDS topology. AP1 connects to multiple APs through WDS in bridging mode. Data from AP2, AP3, and AP4 can only be forwarded by AP1.

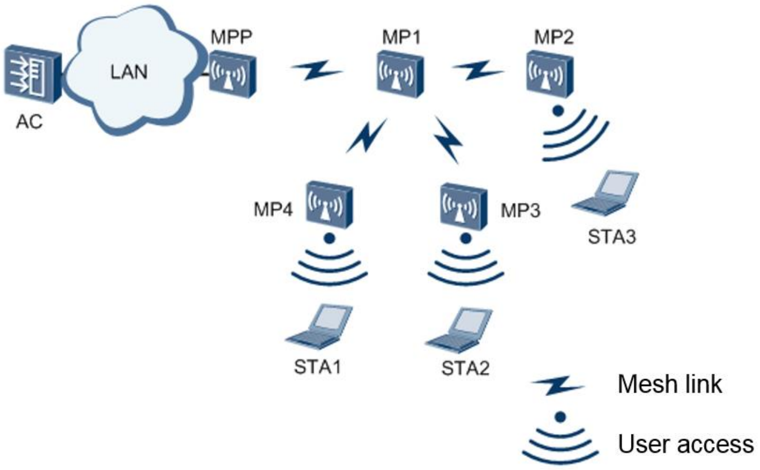
The configuration notes in P2MP networking are as follows:

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 six.

1.4 Mesh Implementation

1.4.1 Basic Concepts

Figure 1-6 Mesh networking



On a traditional WLAN, service 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. An MP can provide both the mesh service and user access service.
- Mesh portal point (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.

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

- Mesh link: a wireless link established between two neighboring MPs through the MPM protocol.

- Mesh path: a wireless path comprising a series of mesh links between the source MP and destination MP.
- Peer MP: a neighboring MP that has established a mesh link with an MP.
- Neighboring MP: an MP that directly communicates with another MP. Not all neighboring MPs are peer MPs.
- Candidate MP: a neighboring MP with which an MP prepares to establish a mesh path.

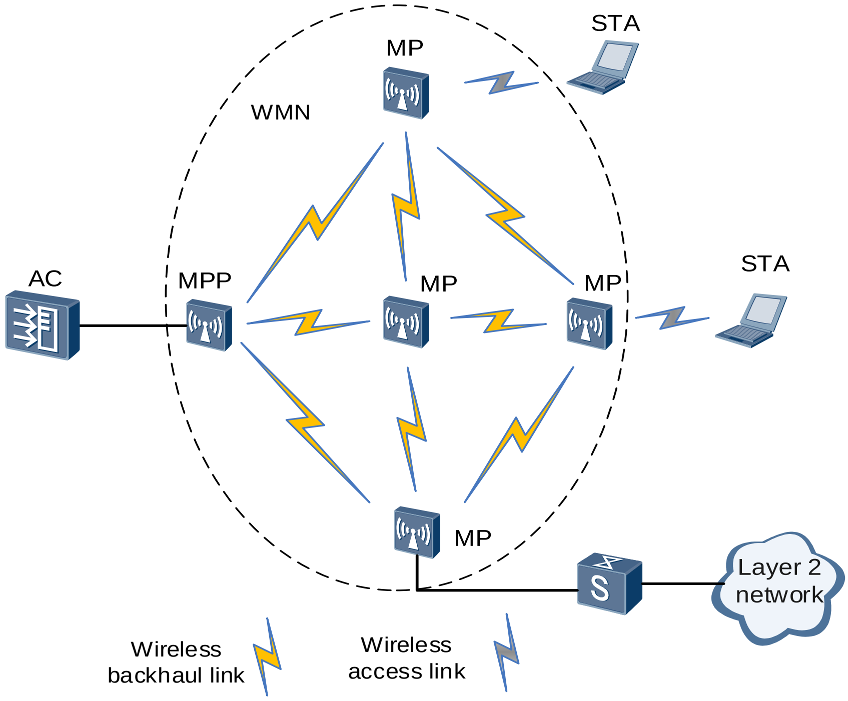
A WMN is a fully meshed WLAN. On a WMN, multiple mesh paths are available between any source and destination, and the transmission quality of these mesh paths varies according to the surrounding environment. Therefore, a WMN must support routing protocols to ensure that data frames are transmitted along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

- Mesh gateway: an MPP that connects a WMN to another type of network.
- Mesh proxy: an MP 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 packets over 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 1-7 WLAN deployed using mesh technology

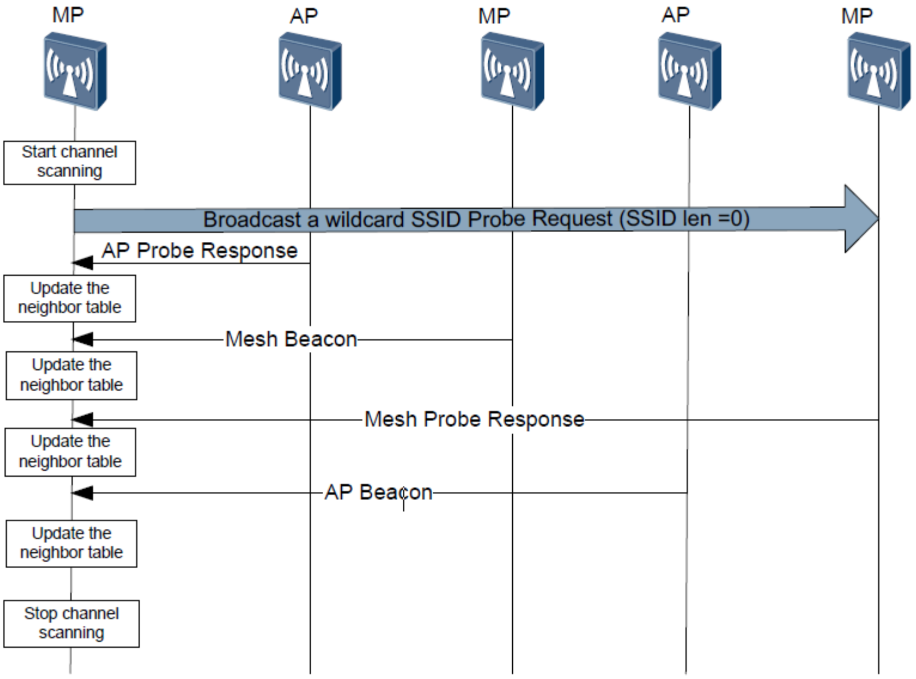


1.4.2 Mesh Link Establishment

Mesh Neighbor Discovery

- Mesh neighbor discovery is the first step to establish a WMN. An MP actively sends a Mesh Probe Request frame (in a non-DFS channel) or passively listens on the Mesh Beacon frames to collect information about neighboring MPs. A Beacon or Probe frame contains information including the mesh ID, mesh configuration, and security capability.
- The MP updates its neighbor relationship table. Each MP has a neighbor relationship table that contains information about four types of neighboring nodes: common APs, nodes of other WMNs, candidate MPs, and peer MPs. In passive scanning mode, the MP checks whether the mesh ID in a Mesh Beacon frame received from a neighboring MP is the same as its own mesh ID. If the two mesh IDs are the same, the MP records the neighboring MP as a candidate MP in the neighbor relationship table. If the two mesh IDs are different, the MP records the neighboring MP as a node of another WMN. If the received Mesh Beacon frame contains no mesh ID, the MP records the neighboring MP as a common AP.

Figure 1-8 Obtaining information about neighboring APs/MPs in a specified channel through active scanning and passive scanning

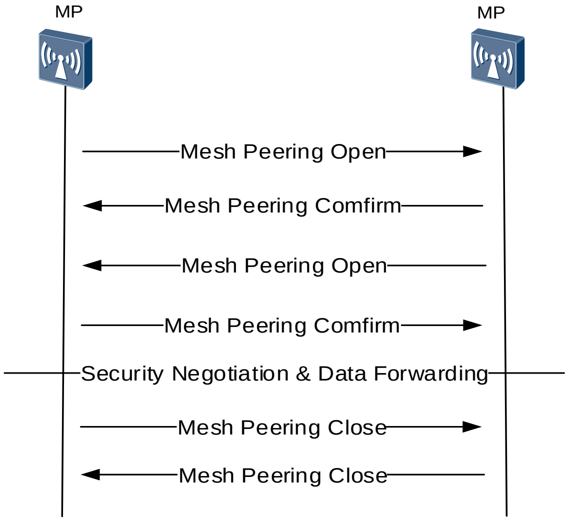

MP
AP
MP
AP
MP
Start channel scanning
Broadcast a wildcard SSID Probe Request (SSID len =0)
AP Probe Response
Update the neighbor table
Mesh Beacon
Update the neighbor table
Mesh Probe Response
Update the neighbor table
AP Beacon
Update the neighbor table
Stop channel scanning

Mesh Link Management

After mesh neighbor discovery is complete, mesh link establishment and teardown need to be performed. Mesh links are established and torn down through exchange of three types of Mesh Action frames: Mesh Peering Open, Mesh Peering Confirm, and Mesh Peering Close frames.

- Mesh link establishment: An MP can initiate a mesh link with a candidate MP. The two MPs are peers and exchange Mesh Peering Open and Mesh Peering Confirm twice to establish a mesh link. After the two MPs establish a mesh link, they start the key negotiation phase. The two MPs can forward mesh data only after the key negotiation succeeds.
- Mesh link teardown: 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 1-9 Mesh link establishment and teardown

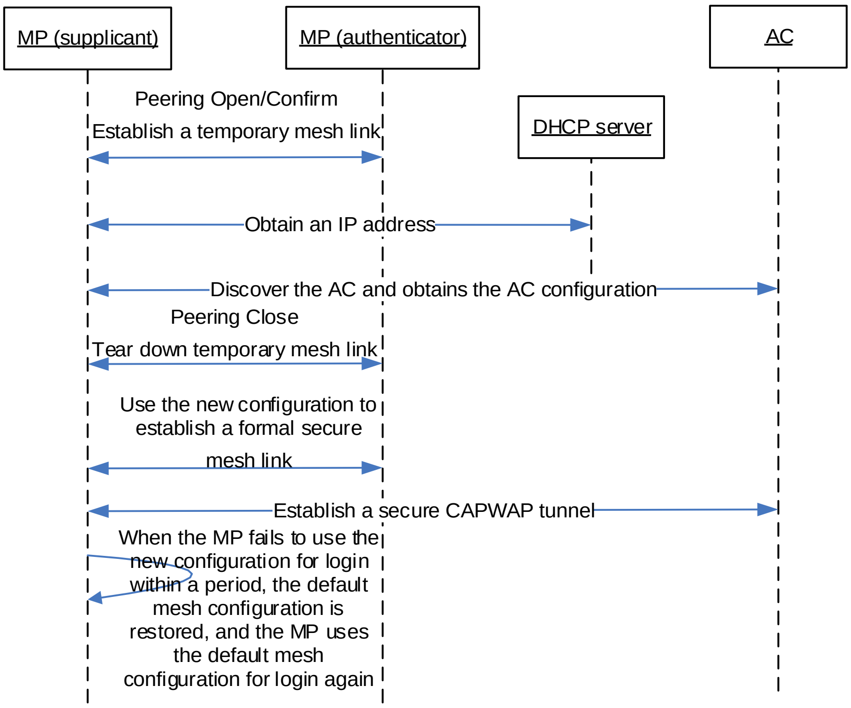


1.4.3 Login of MPs to an AC

The mesh feature supports the Zero Touch Provisioning (ZTP) 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 ZTP process, a mesh node automatically discovers and associates with an AC and obtains the configuration of a WMN from the AC.

Figure 1-10 Login of MPs to an AC through ZTP


MP (supplicant)
MP (authenticator)
AC
DHCP server
Peering Open/Confirm
Establish a temporary mesh link
Obtain an IP address
Discover the AC and obtains the AC configuration
Peering Close
Tear down temporary mesh link
Use the new configuration to establish a formal secure mesh link
Establish a secure CAPWAP tunnel
When the MP fails to use the new configuration for login within a period, the default mesh configuration is restored, and the MP uses the default mesh configuration for login again

The process of MP login to an AC through ZTP is as follows:

1. 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 and establishes a route to the MPP. The Mesh Beacon and Mesh Probe Response frames sent by a neighboring MP carry the flag indicating whether it has associated with the AC. A new MP selects only the neighboring MP that has associated with the AC to establish a mesh link.

2. The new MP obtains an IP address and the AC's IP address from the DHCP server through the mesh link.

3. The new MP discovers and associates with the AC through the mesh link, establishes a temporary insecure CAPWAP tunnel with the AC, and obtains the mesh configuration and other configurations.

4. After the new MP obtains the new configuration, it sends a Mesh Peering Close frame to tear down the temporary insecure mesh link.

5. The new MP exchanges Mesh Peering Open and Mesh Peering Confirm frames with the peer MP using the new mesh configuration 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.

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 temporary mesh link with the AC to obtain the new mesh configuration. During configuration delivery, the following situations may occur:

- If the AC delivers the radio with the mesh function disabled, the MP disables backhaul VAPs, stops automatic discovery, and stops sending link Keepalive packets. Service access parameters can be set, but mesh parameters cannot be set.
- If the AC delivers the radio with the mesh function 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 the access mode to accept the VAP parameters.

1.4.4 Mesh Route 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. Therefore, routing protocols are required on the WMN. The Hybrid Wireless Mesh Protocol (HWMP) defined in 802.11s can address routing issues. The following route management frames are defined in 802.11s:

- Root Announcement (RANN) frame: announces the presence of an MPP.

  When a node is configured as an MPP, it periodically broadcasts an RANN frame. After an MP receives am RANN frame, it reduces the time to live (TTL) of the frame by 1, updates the path metric, and broadcasts the frame without processing it. After another MP reads the RANN frame, it checks whether the gateway specified in the RANN frame exists in its local gateway list. If the gateway does not exist in its local gateway list, the MP adds the gateway information to the gateway list. If the gateway exists in its local gateway list, the MP updates the gateway information in the gateway list according to the information in the RANN frame.
- Route Request (RREQ) frame and Route Reply (RREP) frame

  In on-demand routing mode, the source MP broadcasts an RREQ frame to establish a route to the destination MP. The destination MP responds with an RREP frame after receiving the RREQ frame.

A WMN supports the following routing modes.

- On-demand routing: The source node broadcasts an RREQ frame to establish a route to the destination node. After receiving the RREQ frame, a transit node checks the frame. If the sequence number of the RREQ frame is greater than or equal to the sequence number of the previous RREQ frame but has a smaller metric, the transit node creates or updates the route to the source node. If no route to the destination route is available, the transit node continues forwarding the RREQ frame.
- Proactive routing: The MPP periodically broadcasts an RANN frame. When an MP receives the RANN frame and needs to create or update the route to the MPP, the MP unicasts an RREP frame to the MPP and broadcasts the RANN frame. Then, the MPP

creates a reverse path to the source node, and the MP creates a forwarding path from the MPP to the source node.

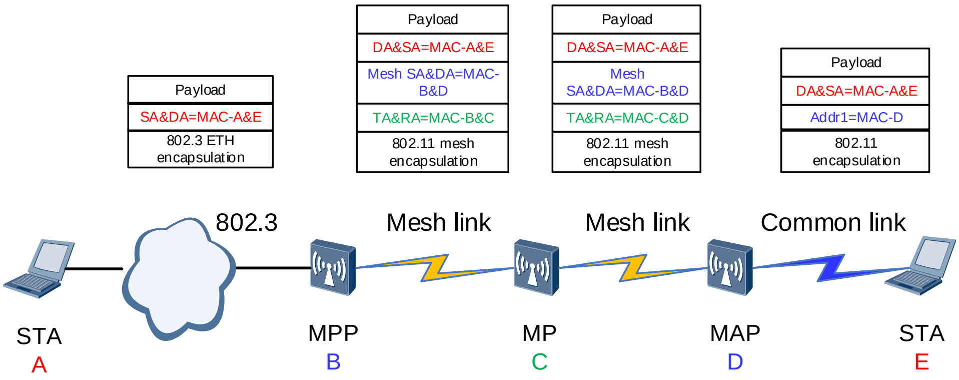
HWMP combines the two routing modes to ensure that data frames are always transmitted over mesh paths with the best transmission quality.

Huawei develops and optimizes a proprietary mesh routing protocol based on 802.11s to implement the route load balancing function. This mesh routing protocol reduces the number of frame forwarding times during the wireless link establishment process and enables construction of the forwarding topology based on the static path with only a few hops from the source node to the destination node.

1.4.5 Data Packet Forwarding

In typical scenarios, an MP can connect an external node to a WMN using the proxy function. In this case, the MP needs to check whether the destination node is associated with another proxy MP according to the destination address of data packets. If the destination node is associated with another proxy MP, the MP converts data packets into mesh frames and finally forwards the mesh frames to the destination node over the WMN.

Figure 1-11 Address encapsulation of a mesh data packet on a WMN during the forwarding process



In the preceding figure:

- **SA** and **DA** indicate the final source and destination addresses of the packet, respectively.
- **Mesh SA** and **Mesh DA** indicate the source and destination addresses of the packet on the WMN (mesh nodes at the edge of the WMN), respectively.
- **TA** and **RA** indicate the addresses of the MPs that transmit and receive the packet respectively when the packet is transmitted hop by hop.

Common 802.11 packets are encapsulated with three addresses, while WMNs encapsulate packets with six addresses. After receiving a standard 802.11 packet originating at a STA, an MP searches its forwarding table and forwards the packet to the WMN. At this moment, the MP needs to convert the standard frame into a mesh frame, encapsulates the standard 802.11 packet with six addresses instead of three addresses, and then transmits the packet over the WMN to the destination MP hop by hop. The packet is then converted into the packet in the corresponding encapsulation format according to the link type of the destination STA.

When a mesh node receives a broadcast or multicast packet from a STA, it broadcasts the packet on the WMN. That is, it copies the packet and sends it over all its mesh paths. Each mesh node on the mesh paths receives and processes the packet as required, and copies the packet and sends it out through their own paths (all mesh and non-mesh paths). Finally, all mesh nodes on the WMN will receive and process the packet.

When a common mesh node receives a unicast packet containing an unknown route to the destination address (that is, the path to which the packet is forwarded is unknown), the mesh node forwards the packet to the MPP over the mesh path. If the MPP fails to look up the forwarding table and still does not know the destination route of the packet, it forwards the packet out from its wired interface.

1.4.6 Eliminating Mesh Network Loops

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

- 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 the mesh frame is a duplicate frame. An MP needs to maintain a table with <mesh SA, 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 andWMNs.

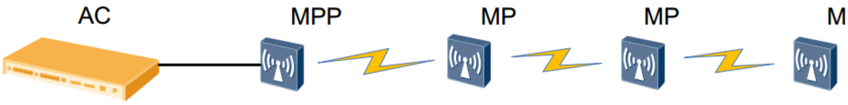
1.5 Mesh Networking Modes

Wireless mesh networking is mainly classified into three modes as follows:

1.5.1 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.

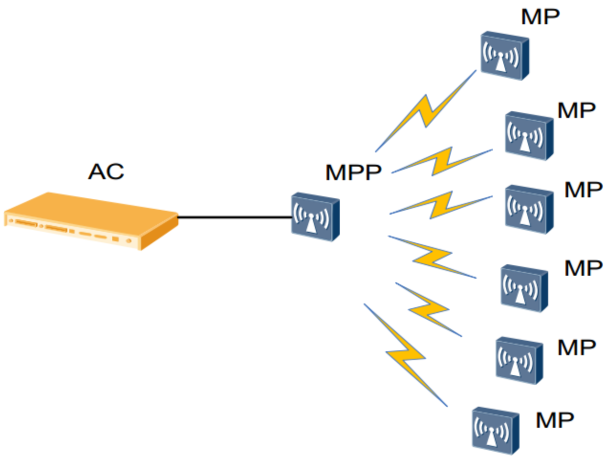
Figure 1-12 Linear networking



1.5.2 Star Networking

In star networking, all MPs depend on an MPP for data forwarding. All LAN data is transmitted through the MPP. This networking mode is typically used for providing hotspot coverage in small squares. Remote MPs connect to an MPP directly through wireless mesh links to provide wider wireless coverage.

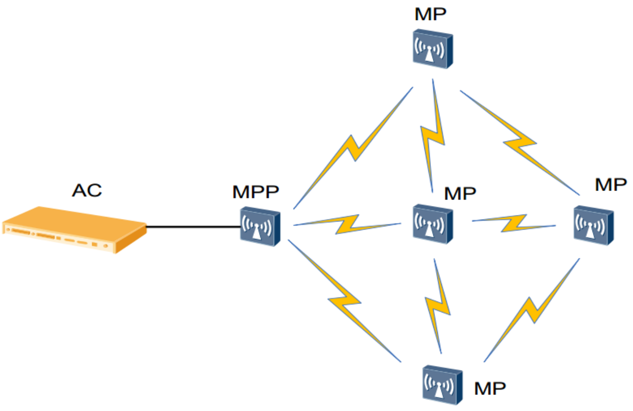
Figure 1-13 Start networking



1.5.3 Mesh Networking

The nodes in mesh networking can discover the nodes on other LANs and connect to them. 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.

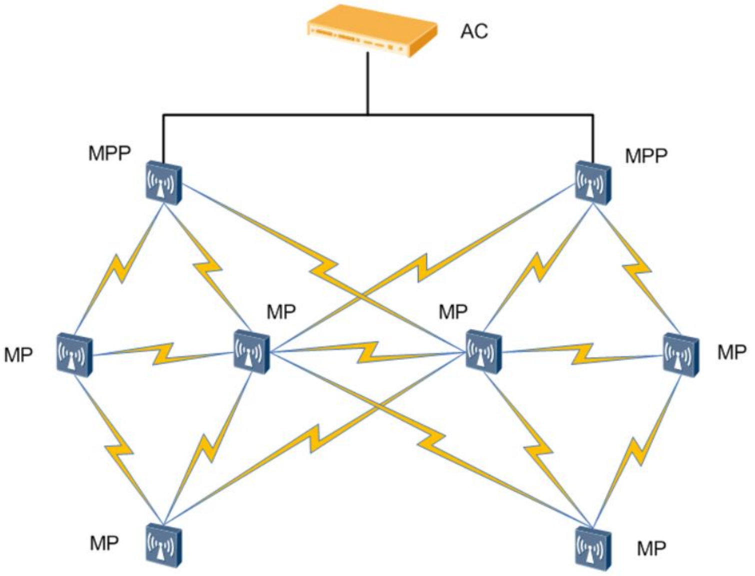
Figure 1-14 Mesh networking



1.5.4 Multi-MPP Networking

In multi-MPP networking, multiple MPPs are deployed on a WMN. Each MPP is connected to a wired network. That is, the WMN has multiple wired egresses, and network devices on the WMN can connect to the fixed wired network through multiple MPPs. This networking mode implements wired link backup through multiple MPPs, improves reliability of the backhaul network, and achieves multi-MPP load balancing.

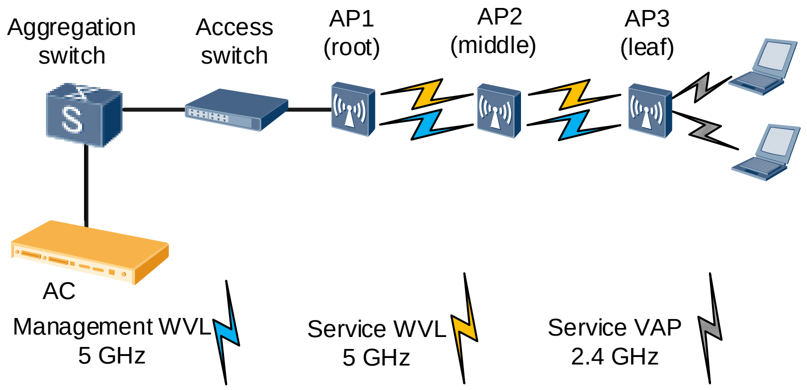
Figure 1-15 Multi-MPP networking



2 Application Scenario

2.1 WDS Networking

Figure 2-1 APs connecting to an AC through WDS

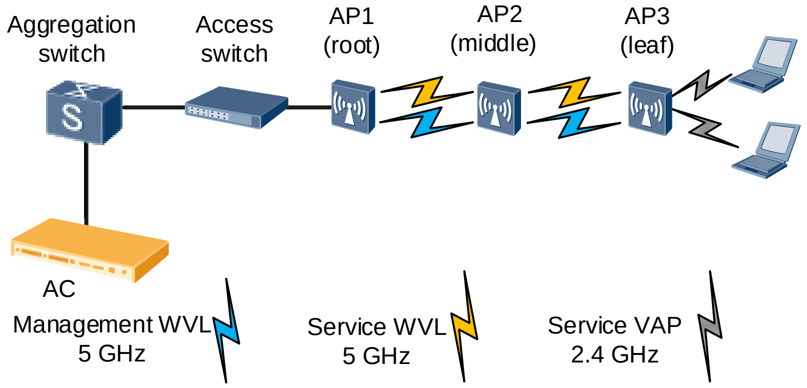


As shown in Figure 2-1, a WDS network connects multiple APs. The APs can set up wireless multi-hop connections and connect to the AC wirelessly. STAs are unaware of the differences between traditional WLANs and WDS networks because the only difference between them is the backbone layer.

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 2-2 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-building 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 radian of the Earth must be considered if the transmission distance is long. Therefore, select and install antennas based on the site condition.

Outdoor Networking Scenario (1)

Figure 2-3, Figure 2-4, and Figure 2-5 show the WDS networks that connect networks 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

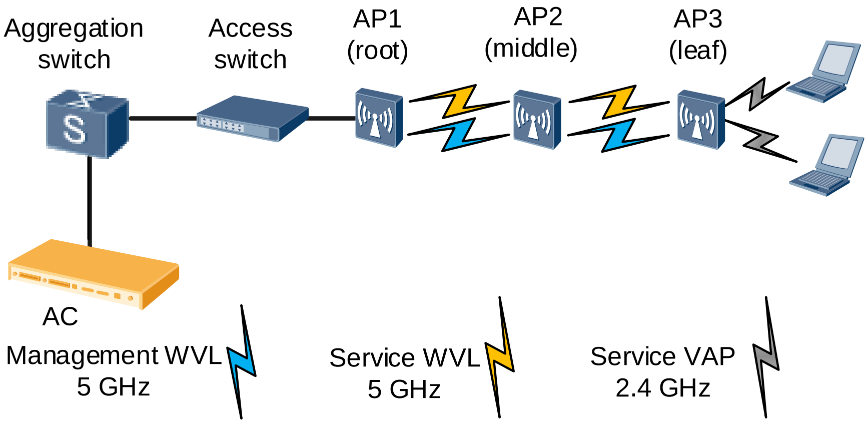


Figure 2-4 Outdoor WDS networking 2

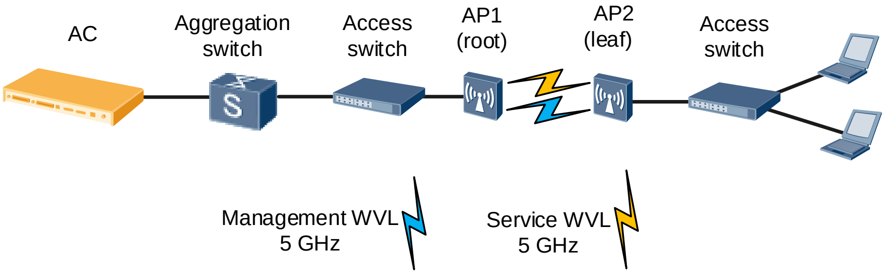
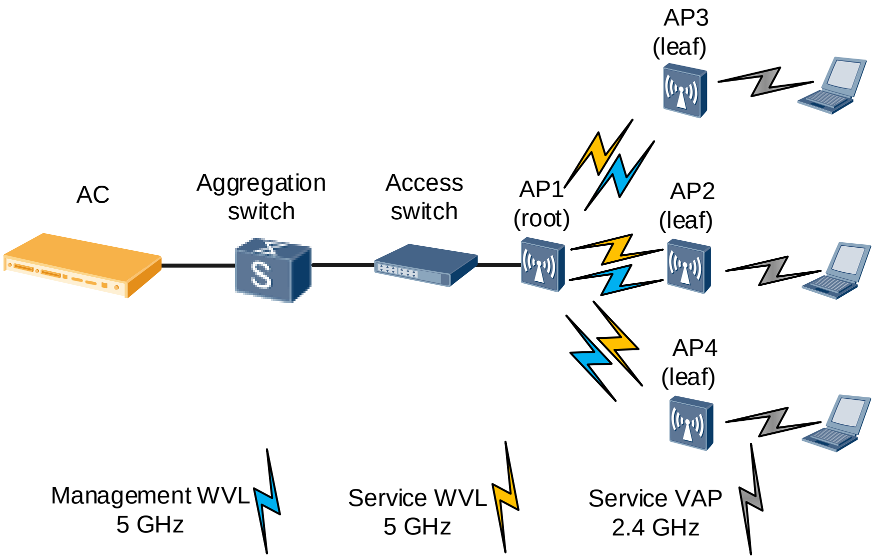


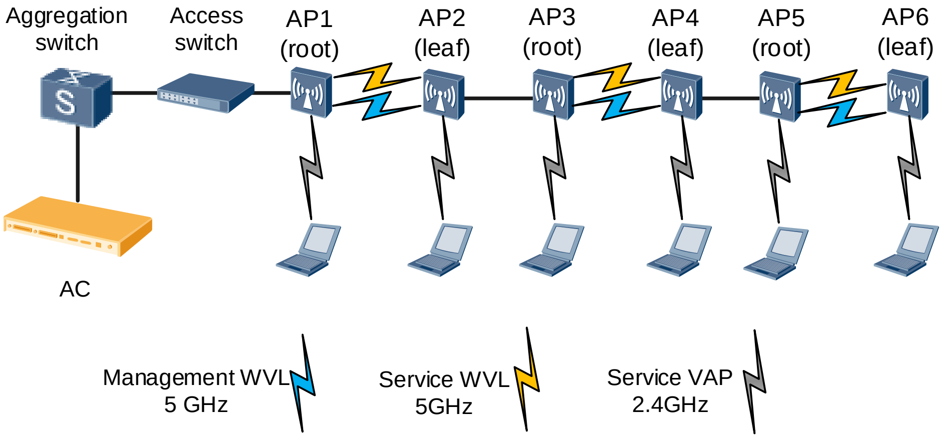
Figure 2-5 Outdoor WDS networking 3



Outdoor Networking Scenario (2)

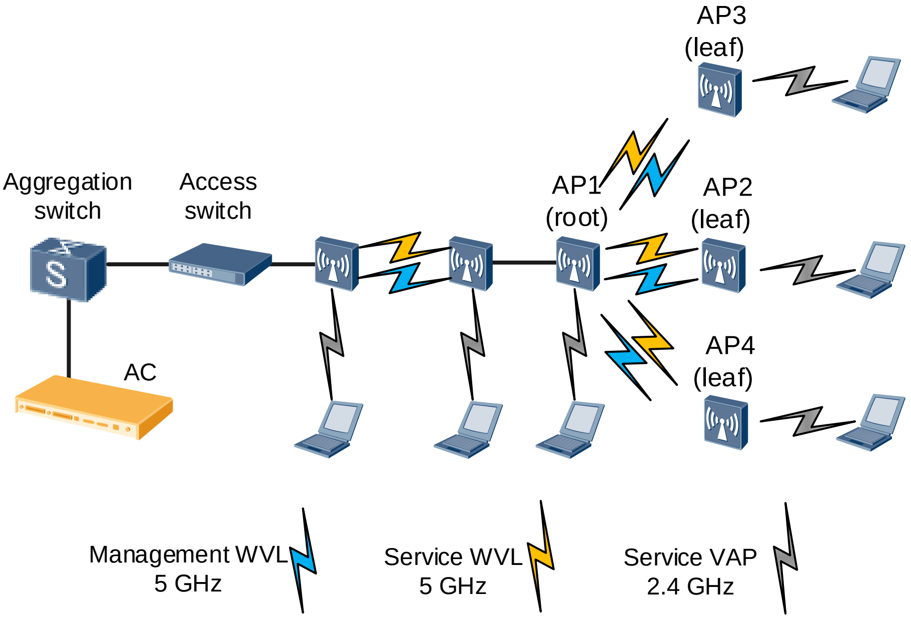
When obstacles exist between networks to be connected or the transmission distance is long, deploy two WDS APs through wired interfaces in back-to-back mode to provide the relay bridging function, as shown in Figure 2-6. This network deployment mode ensures bandwidth of wireless links in long-distance network transmission.

Figure 2-6 Outdoor WDS networking 4



Outdoor Networking 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 in 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:

$PL = 32.45 + 20\ lg(d) + 20\ lg(f)$

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:

$PL = 32.45 + 10n\ lg(d) + 20\ lg(f)$

The environmental factor *n* varies according to the transmission environment and ranges from 2 to 5. Generally, *n* ranges from 4 to 5 in downtown areas 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, in WDS networking, two APs 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:

$PL = 32.45 + 10*2*\ lg(1) + 20\ lg(5000) = 106.4\ dB$

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

Antenna Parameters

Antenna parameters include the gain, lobe width, polarization direction, electrical downtilt, 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 most cases, when the antenna gain increases, the lobe width decreases and radiant energy transmitted by the antenna is more concentrated.

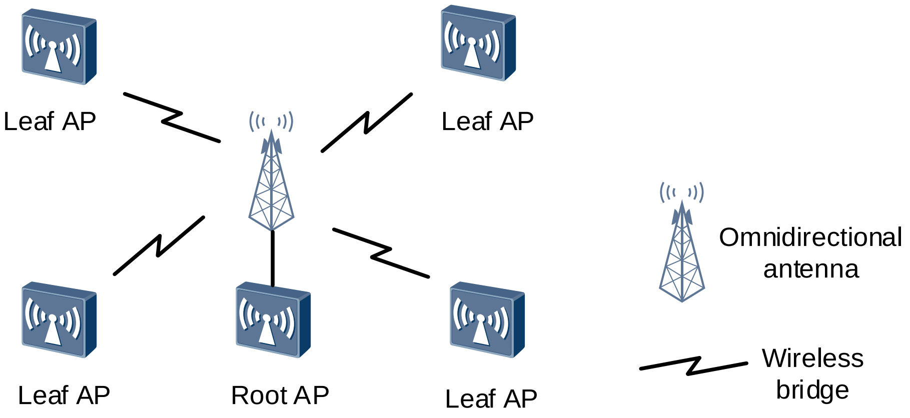
Antenna Type

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.

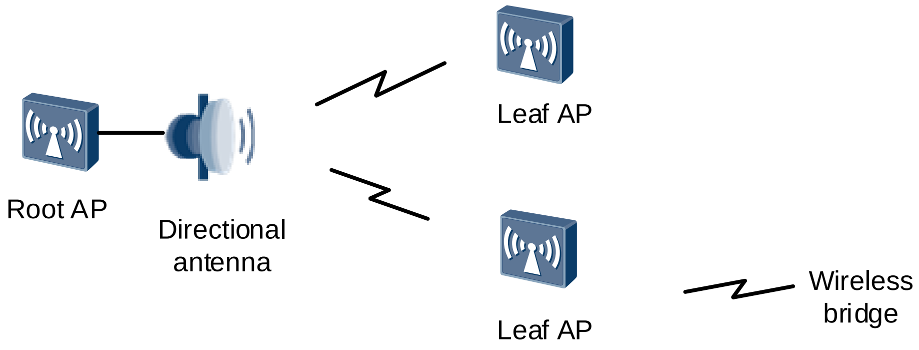
  Figure 2-8 WDS networking with omnidirectional antennas

- 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 devices to be linked exist or the devices to be linked are concentrated in a certain angle.

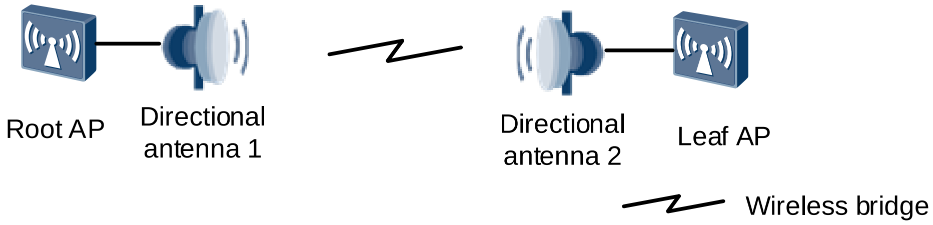
  On a P2MP WDS network, pay attention to the lobe width of antennas when using directional antennas. The angle between an antenna and the device to be linked must be no larger than the lobe width of the antenna. The device to be linked must be within the antenna coverage. As shown in the following figure, 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.

Figure 2-9 P2MP WDS networking with directional antennas



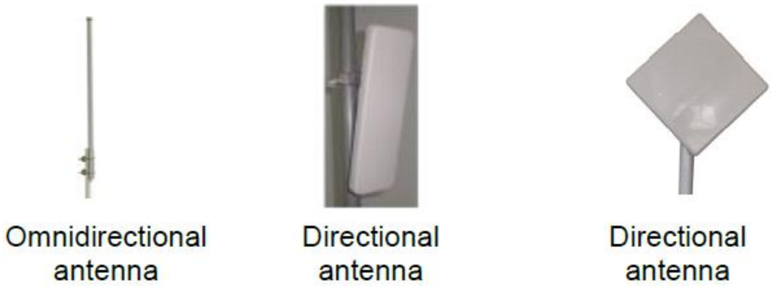
In P2P WDS networking, directional antennas with a small lobe width are recommended because they can improve the transmission distance and signal quality. Directional antennas with a small lobe width have a high antenna gain and can concentrate energy in a narrow range.

Figure 2-10 P2P WDS networking with directional antennas



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

Figure 2-11 Typical 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 in 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 in 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, 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 throughput impact factors in Table 2-3:

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

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

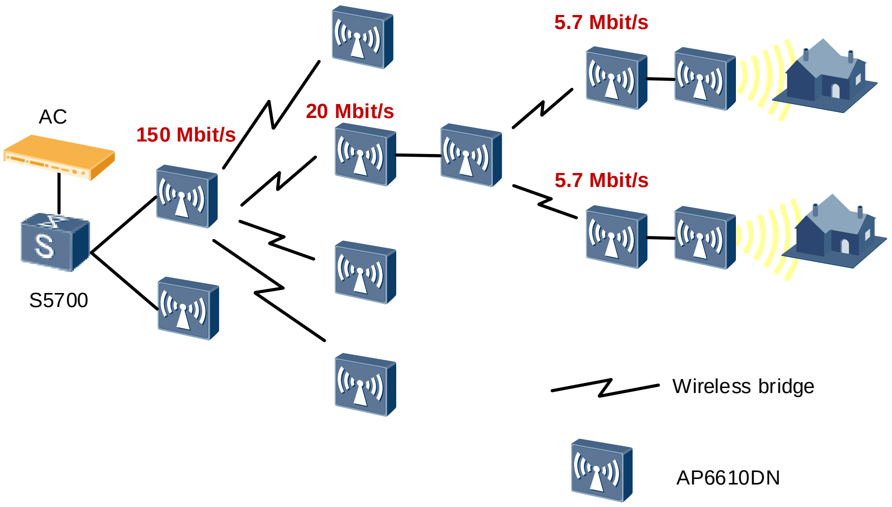
The total link bandwidth of bridges reduces from 80 Mbit/s in P2P networking to 43.2 Mbit/s in P2MP networking (**M** equals 3). The bandwidth on each link is only 14.4 Mbit/s in P2MP networking (**M** equals 3). This example proves that the maximum bandwidth in P2MP networking is much lower than that 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 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 that 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 outdoor dual-band APs (AP6610DN) 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 2-12 Networking diagram

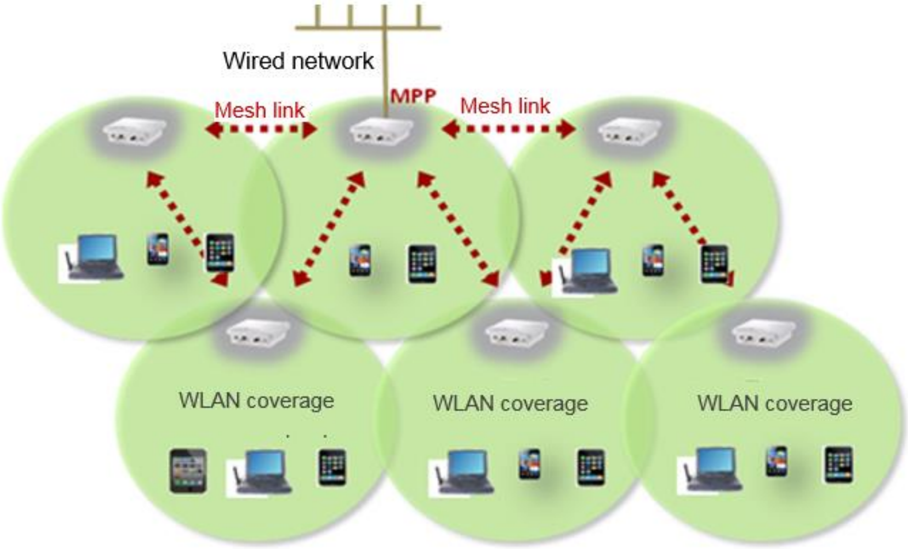


If the first bridge provides 150 Mbit/s bandwidth on the network, the bandwidth is decreased to 20 Mbit/s after the first hop and to 5.7 Mbit/s after the second hop. As 100 users share 10 Mbit/s bandwidth, 5.7 Mbit/s bandwidth is sufficient for 20 users.

2.3 Mesh Networking Scenarios

2.3.1 Wireless Coverage

Figure 2-13 Wireless coverage

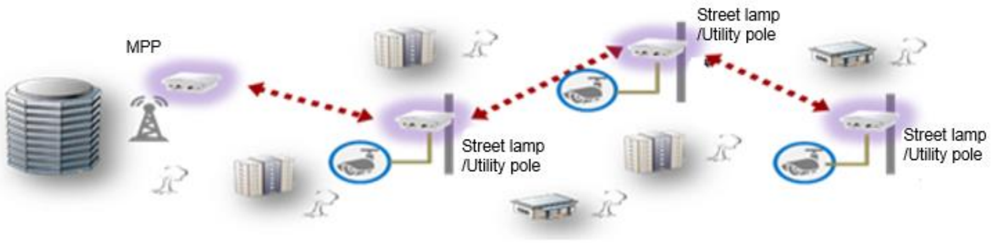


In office buildings, warehouses, subways, and factory buildings, radio signals attenuate when they penetrate walls or other obstacles. Coverage holes exist due to poor signal coverage of APs. Mesh technology can solve this problem, expands the wireless network coverage, and saves cabling costs.

When no optical fiber cable is available in outdoor hotspot areas such as parks and squares, APs cannot be deployed nearby in wired mode. In addition, WLAN hotspot services need to be deployed in wireless backhaul mode. In this case, outdoor mesh networking with high-gain antennas can be used to provide WLAN hotspot services in large areas and provide WLAN access services for employees and citizens.

2.3.2 Road Surveillance Backhaul

Figure 2-14 Road surveillance backhaul



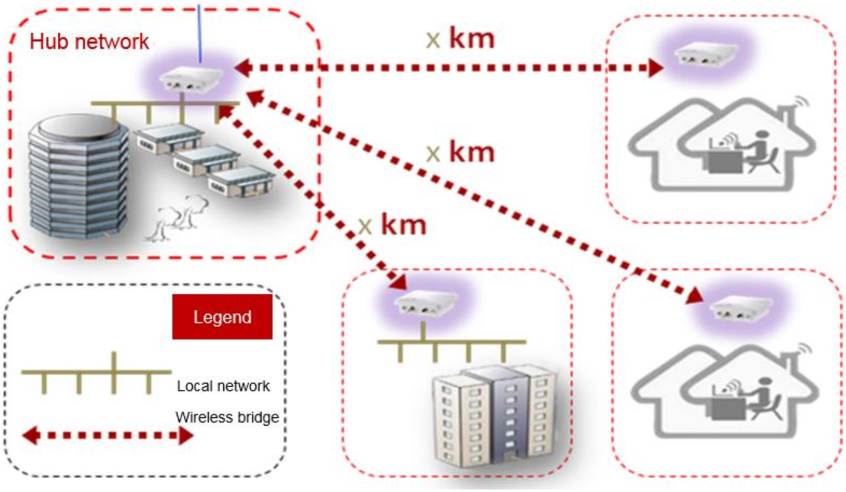
In arterial roads and highways, video surveillance data needs to be collected and reported to the data surveillance center when no wired line is available.

In such scenarios, outdoor APs are deployed on street lamps or utility poles (for convenient power supply). The APs are connected to video surveillance cameras through wired interfaces and send video surveillance data back to the surveillance center over wireless mesh links. APs far away from the MPP need to transmit data through multi-hop mesh links.

On a WMN, multi-hop path loss may be high, greatly compromising bandwidth. In normal cases, multi-hop network deployment is avoided through various methods. For example, directional antennas can be deployed to support a longer transmission distance for the MPP. In this way, more MPs can be connected to the MPP through only one hop to avoid chain networking. However, urban roads may not be straight and high buildings may block radio signals. Therefore, chain networking may still be used to construct a wireless backhaul mesh network.

2.3.3 Long-Distance Wide Coverage

Figure 2-15 Long-distance wide coverage



Compared with indoor scenarios, outdoor scenarios are much wider and more open. Different antennas can be used to greatly improve the WLAN backhaul distance. Two MPs can connect to each other over several or even 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, mesh networking applies to scenarios such as education campuses, plantations, mountainous areas, and high buildings.

In vast rural areas or mountainous areas where no wired lines (such as optical fibers) are deployed, it is fast and convenient to deploy WMNs. WMNs support long-distance data transmission and provide wireless Internet access for users in these areas.

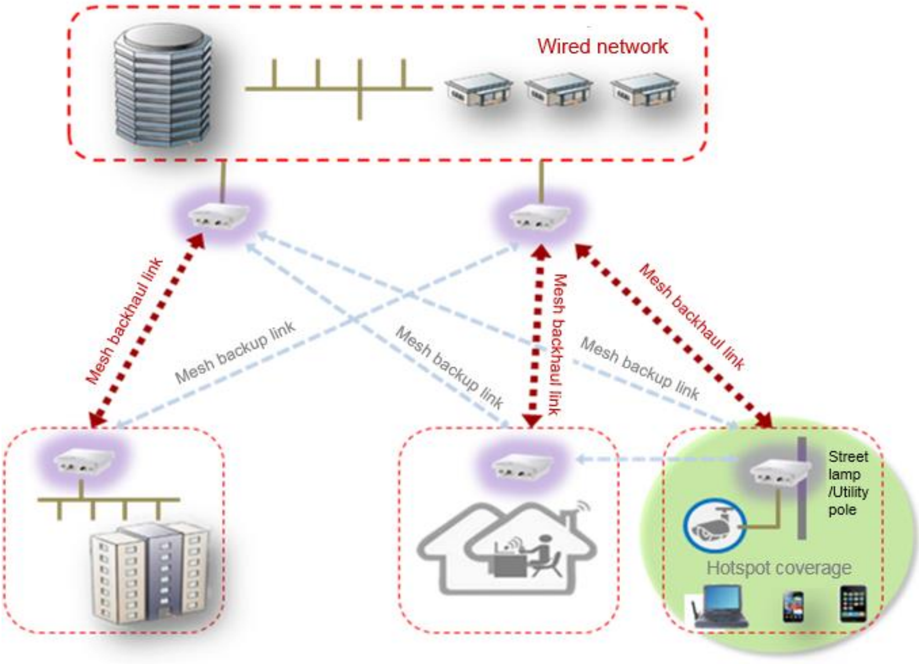
Mesh networking is applicable to scenarios with multiple office buildings far away from each other. Mesh links can be used as active interconnection channels between office buildings or the standby channels for wired links.

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 conditions.

2.3.4 Dual-Link Reliable Backhaul

Figure 2-16 Dual-link reliable backhaul



In mesh networking scenarios requiring high reliability, multiple MPPs can be deployed to ensure reliability of multiple backhaul links. Data traffic can be load-balanced on multiple remote MPs. In addition, the MPPs work in active/standby mode to implement fast service switchover if any root node, root link, or remote backhaul link fails.

2.4 Mesh Networking Planning

2.4.1 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 topology and forwarding capability of a WMN.

Gateway Deployment

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

Backhaul Topology

Typical backhaul topologies are shown in section 1.5 "Mesh Networking Modes." 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

  If each MP uses multiple backhaul radios and transmits uplink traffic and downlink traffic on different channels, each hop has the same throughput without regard to the even allocation of bandwidth to the branches on the backhaul path. 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 the wired network. 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 configure 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 ZTP of an MP, a backhaul VAP on a 5-GHz radio is enabled by default. To use a 2.4-GHz channel as a backhaul channel, you must manually configure a backhaul VAP.

- HT40 and HT20 selection

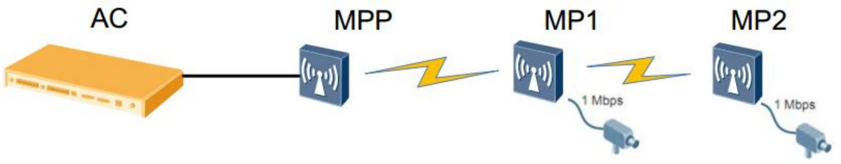
  At the backhaul layer, 5-GHz radios are often used. Therefore, the HT40 mode is recommended at the backhaul layer to provide a higher backhaul rate. At the access layer, many handheld devices do not support the HT40 mode, and the HT40 mode is rarely used on 2.4-GHz radios. Therefore, the HT20 mode is 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

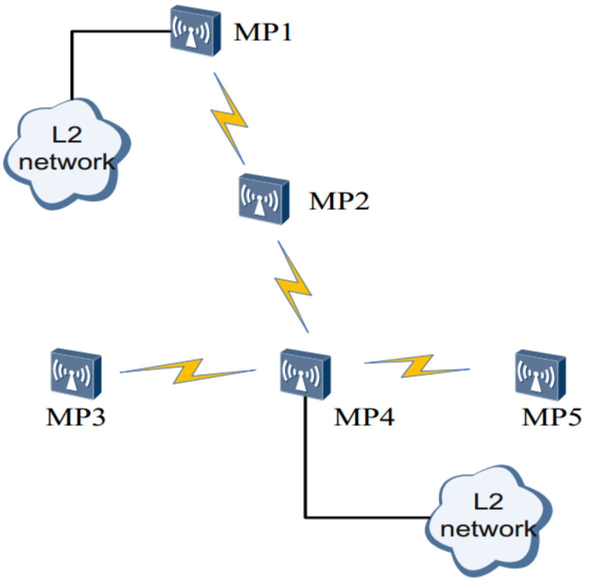
Figure 2-17 Backhaul layer performance deterioration model in the case of a single channel



For example, in the scenario shown in Figure 2-17, all the MPs use the same 5-GHz channel, there is no other channel around the 5-GHz channel, 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 surveillance 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 peak throughput value of each node is **C/N**; the average throughput per MP is **2C/(N*(N+1))** (**N** indicates the total number of hops); the performance deterioration rate 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 2-18 if MP4 is an MPP and MP1 is not.

Figure 2-18 Backhaul layer performance deterioration analysis in the case of a single channel



2.4.2 Mesh Transmission Distance Planning

Signal Attenuation

In WDN networking, at least two MPs need to interconnect over a distance of several hundred meters or dozens of kilometers. Radio waves will attenuate in 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 that the 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 the transmission environment and ranges from 2 to 5. Generally, *n* ranges from 4 to 5 in downtown areas 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, in 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:

$PL = 32.45 + 10*2* \lg(1) + 20 \lg(5000) = 106.4$ 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 in first Fresnel zone. In this way, you can calculate signal attenuation easily.

Antenna Parameters

Antenna parameters include the gain, lobe width, polarization direction, electrical downtilt, 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.

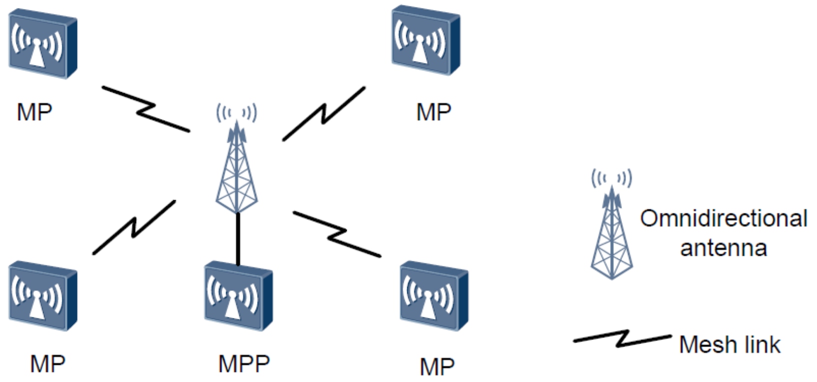
In most cases, when the antenna gain increases, the lobe width decreases and radiant energy transmitted by the antenna is more concentrated.

Antenna Selection

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

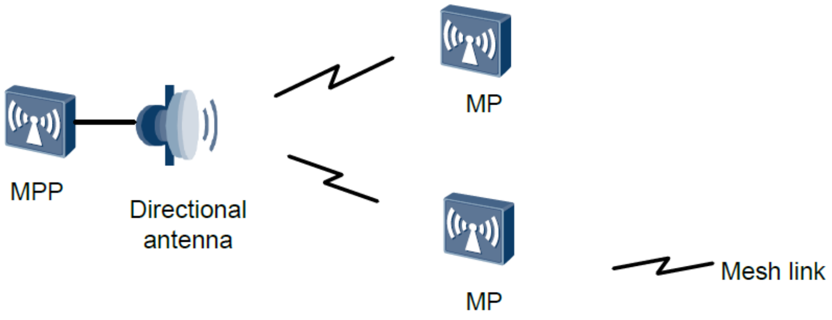
- Omnidirectional antenna: Signals from an omnidirectional antenna are evenly distributed 360 degrees around the central point. The lobe width of an omnidirectional antenna is 360 degrees, but its antenna gain is low.

  Omnidirectional antennas can be used for mesh links when many devices to be linked 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.

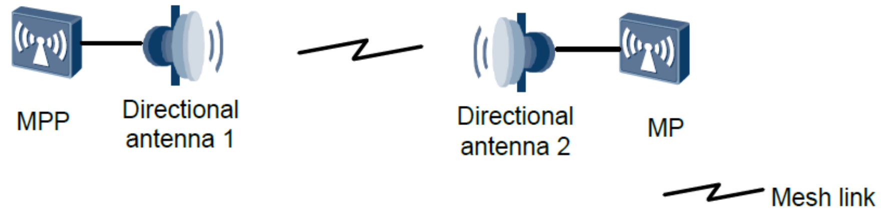


- Directional antenna: Signals from a directional antenna radiate in a certain angle. Directional antennas can concentrate energy and transmit signals to a specified direction. Therefore, directional antenna is a good choice when there are a few to-be-linked devices or the to-be-linked devices are concentrated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

  In a P2MP WMN networking, pay attention to the lobe width when selecting directional antennas. The angle formed by the to-be-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 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 Configuration Examples

3.1 WDS Configuration Example

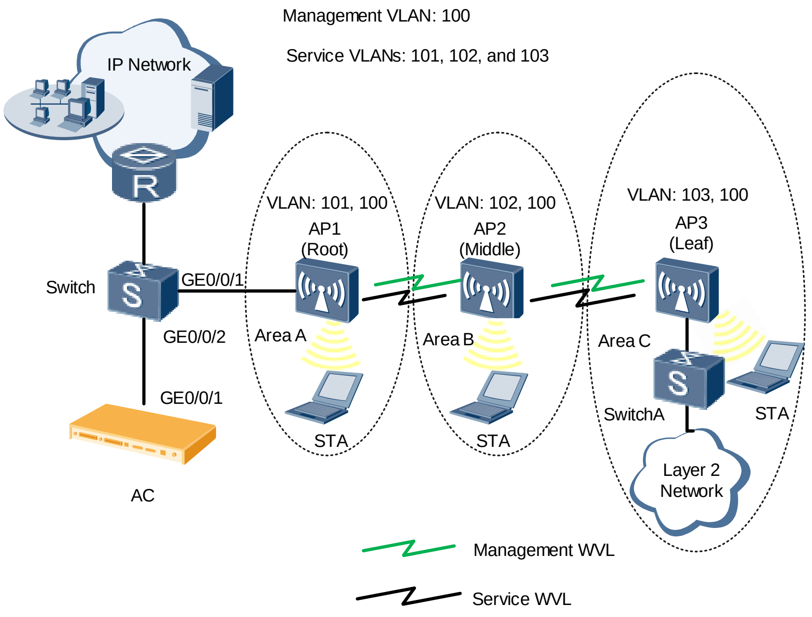
3.1.1 Networking Requirements

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 Diagram of configuring the WLAN WDS service



3.1.2 Configuration Analysis

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

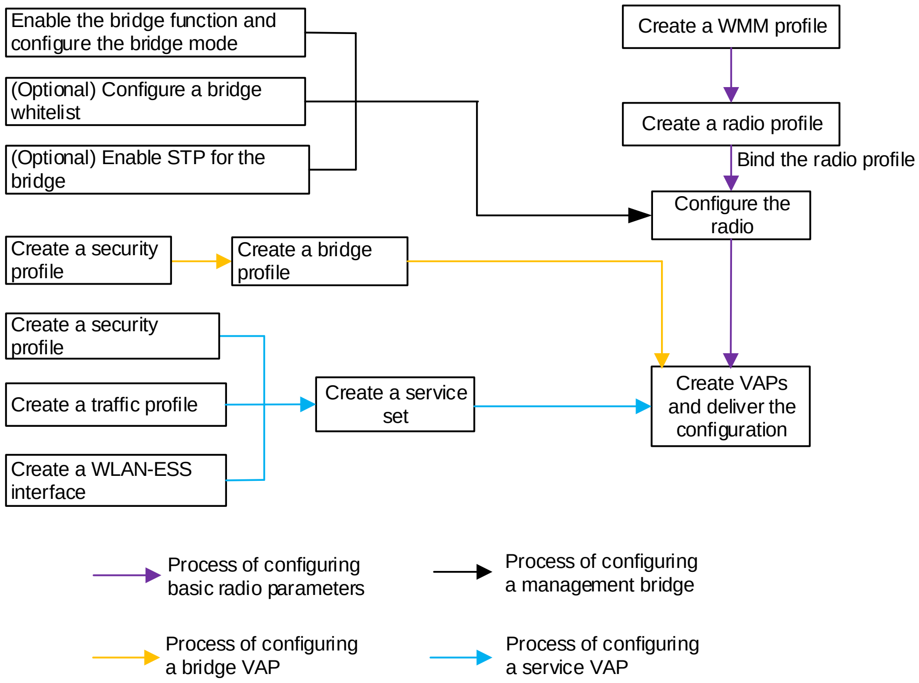
Table 3-1 VLAN configuration plan

Item	Data
VLAN	Management VLAN: 100
	Service VLANs: 101, 102, 103, 104, 105, and 106 • Area A: VLAN 101 for wireless services • Area B: VLAN 102 for wireless services • Area C: VLAN 103 for wireless services • Area C: VLANs 104, 105, and 106 on wired interfaces of AP3

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

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

Figure 3-2 Flowchart for configuring WLAN WDS services


Enable the bridge function and configure the bridge mode
(Optional) Configure a bridge whitelist
(Optional) Enable STP for the bridge
Create a WMM profile
Create a radio profile
Bind the radio profile
Configure the radio
Create a security profile
Create a bridge profile
Create a security profile
Create a traffic profile
Create a WLAN-ESS interface
Create a service set
Create VAPs and deliver the configuration
Process of configuring basic radio parameters
Process of configuring a management bridge
Process of configuring a bridge VAP
Process of configuring a service VAP

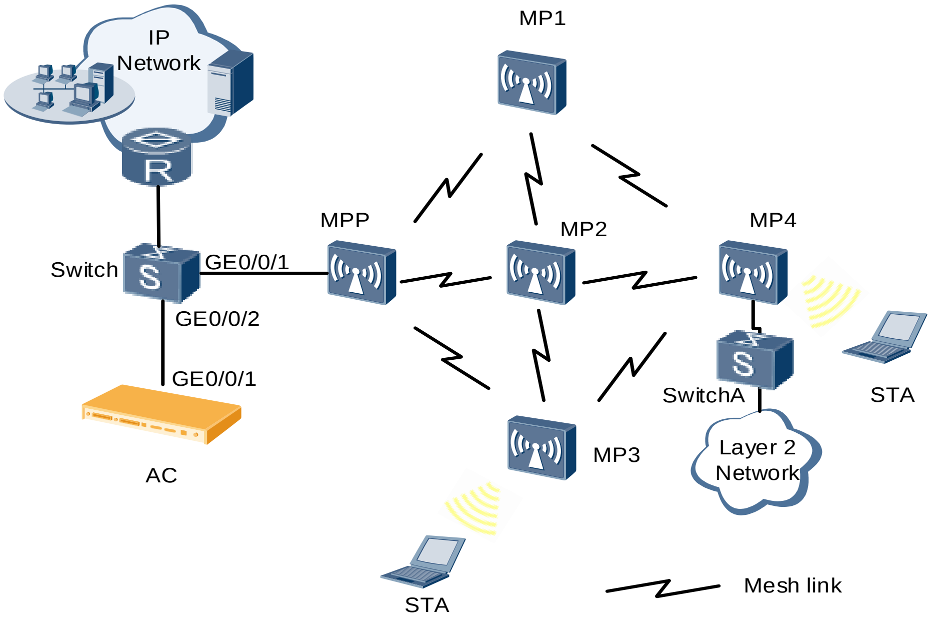
3.2 Mesh Configuration Example

3.2.1 Networking Requirements

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

- The AC6605 provides the AC function.
- The AC functions as a DHCP server to assign 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 connect to the MPP wirelessly and form a WMN. MP3 and MP4 provide the wireless access function, and MP4 accesses a Layer 2 wired network.

Figure 3-3 Diagram of configuring the WLAN mesh service



3.2.2 Configuration Analysis

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. (The actual data needs to be verified.)
- 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 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.

Configuration Procedure

Step 1 Create a radio profile. Configure radio channels because 5 GHz radios need to be used for radio backhaul. Set the radio coverage distance (default value: 3) based on the actual distance between APs to improve the data transmission efficiency between the APs.

Step 2 Create a security profile. To ensure WMN security, configure a security profile and a security policy for the WMN. Currently, a WMN supports only the WPA2+PSK+AES security policy.

Step 3 Configure a mesh whitelist. A mesh whitelist contains the MAC addresses of neighboring MPs that are allowed to connect to the local MP. If a mesh whitelist is bound to a radio of an MP, only the neighboring MPs whose MAC addresses are in the mesh whitelist can connect to the MP.

Step 4 Configure the role of an MP on the WMN, and bind the mesh role to radios of each MP. By default, the role of an MP on a WMN is **mesh-node**. To change the role of an MP to MPP, set the MP's role to **mesh-portal**.

Step 5 Create a mesh profile. A mesh profile is an attribute set that contains mandatory parameters for an MP to establish mesh links with its neighboring MPs. Bind the security profile and mesh whitelist to the mesh profile.

Step 6 Bind the radio profile to the AP specific profile or an AP radio in the AP group.

Step 7 Deliver the configured mesh profile and radio profile to the corresponding AP.

----End

A Acronyms and Abbreviations

A	
AC	Access Controller
AP	Access Point
D	
DS	Distribution Systems
M	
MP	Mesh Point
MPM	Mesh Peering Management
MPP	Mesh Portal Point
P	
P2P	Point-to-Point
P2MP	Point-to-Multipoint
S	
STA	Station
W	
WDS	Wireless Distribution System
WLAN	Wireless Local Area Networks
WVL	Wireless Virtual Link

Huawei Technologies Co., Ltd.
Address: Huawei Industrial Base Bantian,
Longgang Shenzhen 518129 People's Republic of China
Website: e.huawei.com

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.