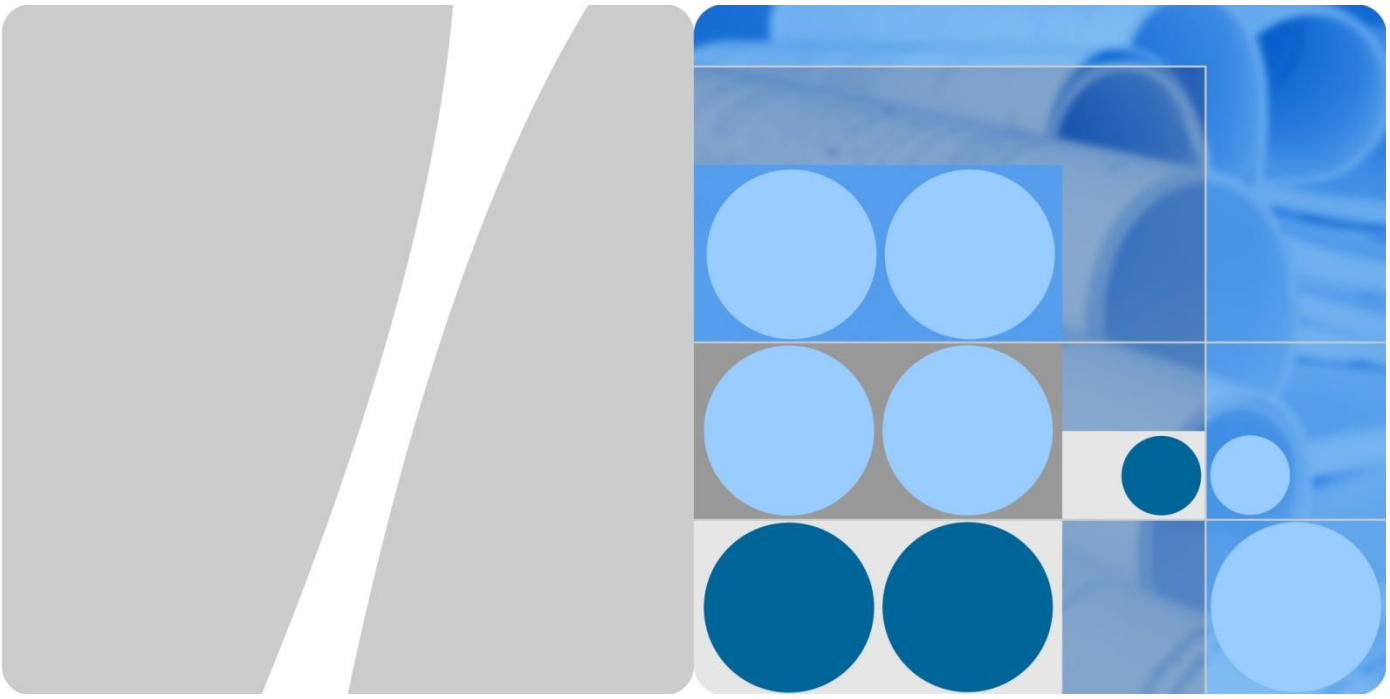


WLAN IPv6 Technology White Paper

Issue 1.0

Date 2014-06-16

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

Email: support@huawei.com

About This Document

Keywords

WLAN, IPv6

Abstract

IPv4 address resources are nearing exhaustion as the Internet continues to expand. IPv4 networks are being gradually upgraded to IPv6 networks to meet new broadband access user requirements and new service deployment requirements. This document describes how to deploy IPv6 on WLAN networks.

Abbreviations

Abbreviation	Full Name
SSID	Service Set Identifier
BSSID	Basic Service Set Identifier
CAPWAP	Control And Provisioning of Wireless Access Points
SAVI	Source Address Validation Improvement
SLAAC	Stateless address autoconfiguration
ND	Neighbor Discovery
MLD	Multicast Listener Discovery
SG	Source Guard
DAI	Dynamic ARP Inspection
SNP	Snooping
ISATAP	Intra-Site Automatic Tunnel Addressing Protocol

Contents

1 Overview

Development of the Internet is driven by services and applications, and the IP protocol requires that each network terminal have a unique addressable IP address. However, currently, there are only 4.3 billion IPv4 addresses, among which about 3 billion IPv4 addresses are available. These IPv4 addresses are not enough to assign one address to everyone on the planet. IPv4 address resources are nearing exhaustion as the Internet continues to expand, which in turn limits service and subscriber development. Transitioning from IPv4 to IPv6 can solve this problem.

Countries in the world designed IPv6 development strategies. Windows and Linux terminals already support IPv6; intelligent terminals (mobile phones and tablets) support IPv6; the majority of routers and switches of network vendors also support IPv4/IPv6 dual-stack. You can build a pure IPv6 network or dual-stack IPv4/IPv6 network.

Since the late 1990s, China has regarded the IPv6 key technology research project as a national major project. China Education and Research Network (CERNET) joined 6Bone in June, 1998, later started the Internet 6 plan, and has built an IPv6 network among China's universities, forming a large-scale IPv6 research and experimental network.

The Internet Assigned Numbers Authority (IANA) had allocated the last five Class A IPv4 addresses in February 2011. IPv4 address allocation is not balanced because of historical reasons. IP address shortage has become a serious problem for operators, limiting the development of new services such as terminal terminals and Internet of Things (IoT). Several years again, operators clearly required that purchased network devices support IPv4/IPv6 dual stack to ensure that networks support IPv6.

Huawei WLAN ACs/APs support IPv4/IPv6 dual stack, and WLAN solutions support IPv4 and IPv6 network deployment. Multiple networking modes such as IPv4 over IPv4, IPv4 over IPv6, IPv6 over IPv4, and IPv6 over IPv6 are available.

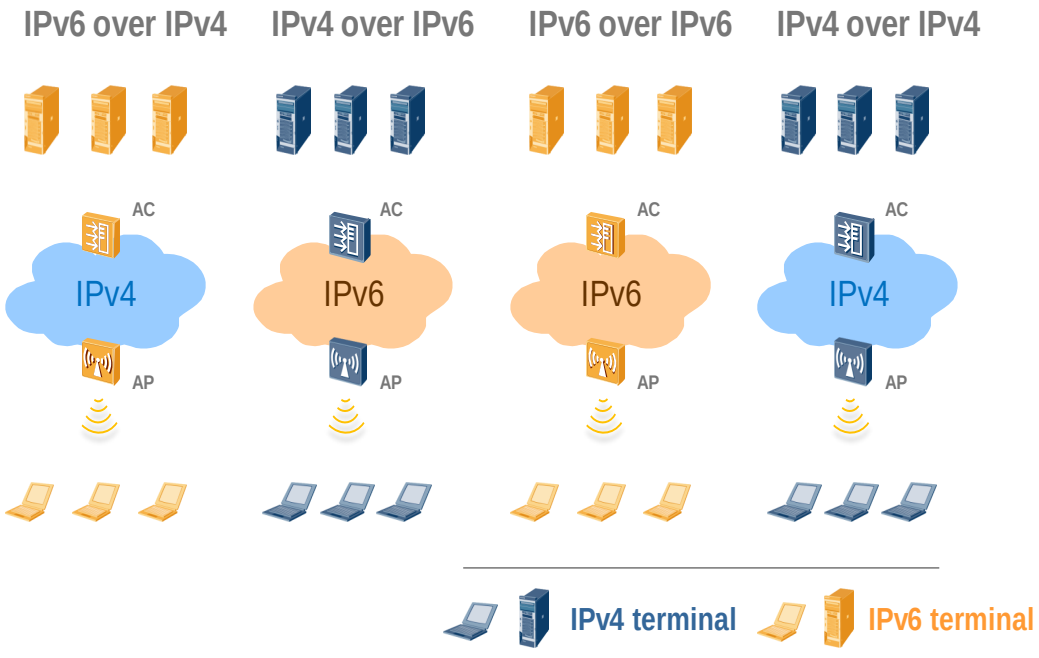
2 WLAN IPv6 Technology Implementation

2.1 WLAN IPv6 Networking Scenarios

2.1.1 WLAN IPv6 Networking Modes

A WLAN network has the following four networking scenarios based on the basic network type and AP communication type.

Figure 2-1 WLAN IPv4/IPv6 networking modes



In Figure 2-1, WLAN IPv6 networking modes include IPv6 over IPv4, IPv4 over IPv6, and IPv6 over IPv6. IPv4 over IPv4 networking is pure IPv4 networking and the current most mainstream networking mode.

- IPv6 over IPv4 networking applies to the scenario where the basic access bearer network is a pure IPv4 network and wireless terminals use IPv6 for communication.

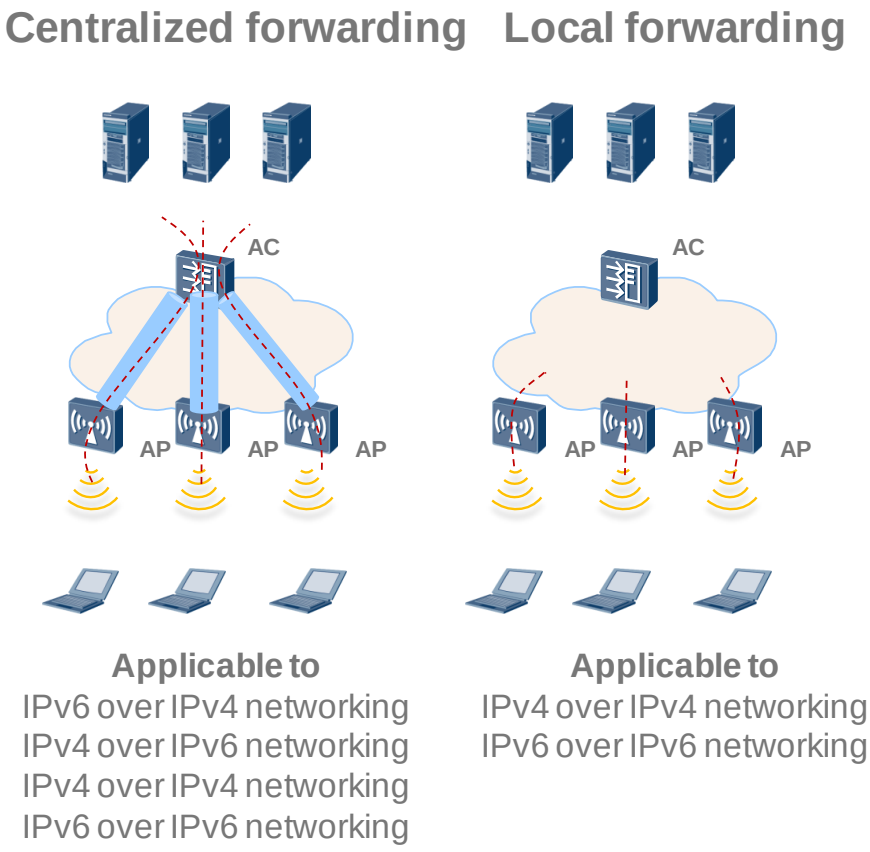
- IPv4 over IPv6 networking applies to the scenario where the basic access bearer network is a pure IPv6 network and wireless terminals use IPv4 for communication.
- IPv6 over IPv6 networking applies to a pure IPv6 network where a wireless IPv6 network is built in an IPv6 network.

Currently, basic access networks of most enterprises and institutions are pure IPv4 networks. Building an IPv6 WLAN on such a basic network forms typical IPv6 over IPv4 networking. This networking mode allows STAs accessing IPv6 networks to communicate with each other across IPv4 access networks. Therefore, IPv6 over IPv4 networking is the most important WLAN IPv6 network scenario among the preceding three networking scenarios.

2.1.2 Local Forwarding and Centralized Forwarding

In the infrastructure WLAN networking of Fit AP+AC, Huawei products support two forwarding modes: local forwarding and centralized forwarding.

Figure 2-2 WLAN centralized forwarding and local forwarding



In centralized forwarding mode, STA data packets are encapsulated in CAPWAP tunnels, pass through the basic access bearer network, and are transmitted to the AC for original packet forwarding. In local forwarding mode, STA data packets are directly transmitted from APs to the basic access bearer network for forwarding without having to be transmitted to the AC for centralized forwarding.

IPv6 over IPv4 and IPv4 over IPv6 networking modes support only the centralized forwarding mode.

2.1.3 Layer 2 Bridge and Layer 3 Gateway

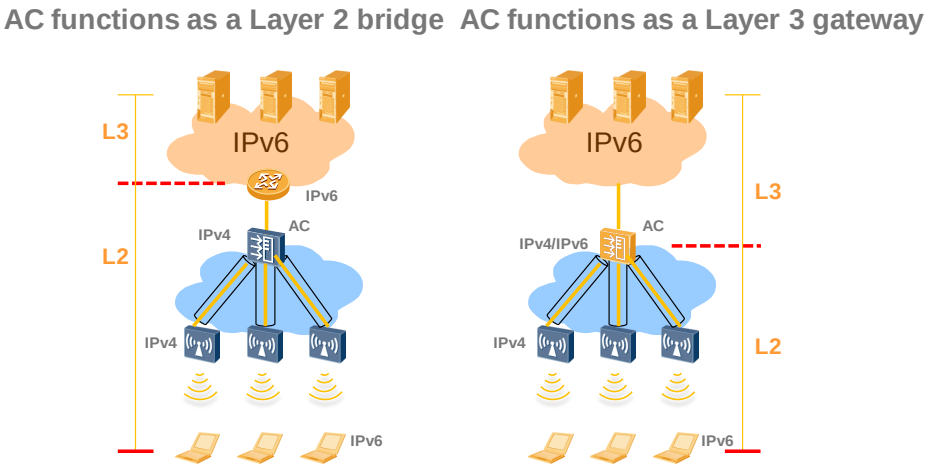
Centralized forwarding is also called tunnel forwarding and is an overlay networking mode in nature. The WLAN system transmits data packets of wireless users over CAPWAP tunnels between an AC and AP to the basic access bearer network for packet forwarding.

A pure IPv6 network scenario (IPv6 over IPv6) is the only WLAN IPv6 networking scenario that can use local forwarding, while other networking scenarios can only use tunnel forwarding. In tunnel forwarding mode, an AC plays different roles and must provide different functions in IPv6 networking.

The following uses IPv6 over IPv4 as an example. In centralized forwarding mode, a CAPWAP tunnel exists between an AP and an AC, and STA data passes through the access bearer network through the CAPWAP tunnel. In this situation, the AP and AC are endpoints of the tunnel and visible to the STA data, but the intermediate access bearer network is invisible to the STA data. In STA communication, an AP always functions as a Layer 2 switch, but an AP functions as a Layer 2 switch or an IPv6 Layer 3 gateway/router in different networking scenarios.

In Figure 2-3, WLAN ACs function as a Layer 3 gateway and a Layer 2 bridge for wireless users.

Figure 2-3 ACs functioning as a Layer 3 gateway and a Layer 2 bridge



NOTE

In the figure, the networking scenario is IPv6 over IPv4, which is similar to IPv4 over IPv6 and IPv6 over IPv6.

- The AC functions as a Layer 2 switch for STAs (as shown in the left part of the figure).

  When an AC functions as a Layer 2 bridge, the AC just forwards packets received from STAs in tunnels at Layer 2, removing the need to support the IPv6 Layer 3 routing function or IPv6 protocols such as IPv6 dynamic routing protocols and DHCPv6. In this situation, the AC only needs to support the Layer 2 switching function of the single IPv4 protocol stack.

NOTE

When the AC needs to support Layer 3 features of STAs such as Portal authentication, DHCP snooping (SNP), and IP source guard (SG), the AC still needs to have IPv4/IPv6 dual stack capabilities even though it functions only as a Layer 2 switch.

- The AC functions as a Layer 3 gateway (router/Layer 3 switch) for STAs (as shown in the right part of the figure).

  When an AC functions as a Layer 3 gateway, the AC becomes the border between an IPv6 network and an IPv4 network. That is, the AC directly accesses an upstream IPv6 network. This is different from the scenario where an AC functions as a Layer 2 bridge. In this scenario, an AC accesses an IPv6 network through a separate upstream IPv6 router. Therefore, the AC needs to support IPv6 protocol functions and must be an IPv4/IPv6 dual-stack device.

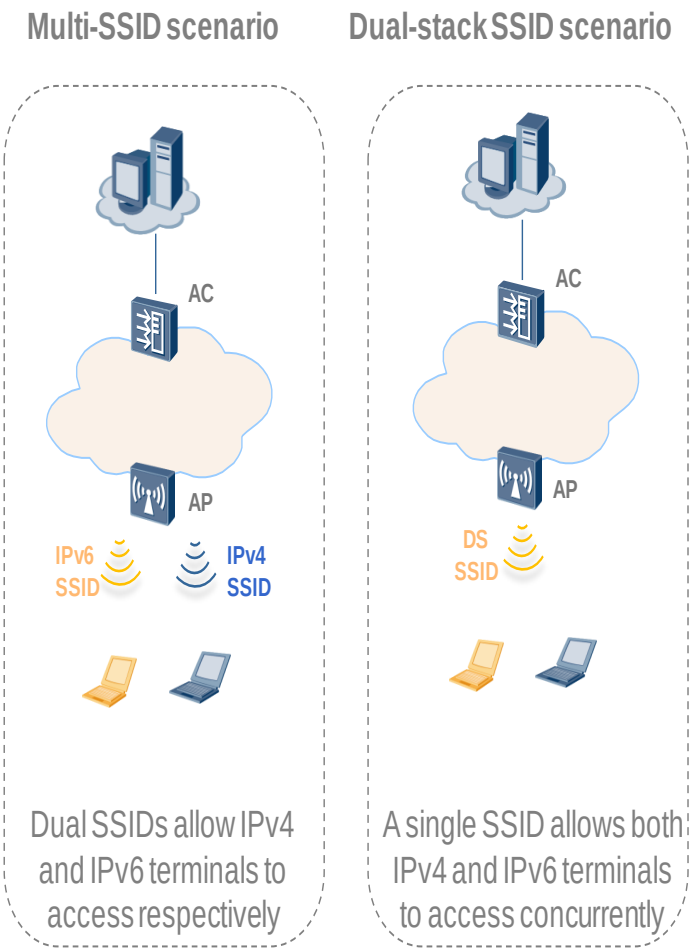
In three centralized forwarding scenarios: IPv6 over IPv4, IPv4 over IPv6, and IPv6 over IPv6, ACs can function as both Layer 2 bridges and Layer 3 gateways and have similar function requirements. In IPv6 over IPv6 local forwarding scenario, an AC is a node on an IPv6 network and must support IPv6 dynamic routing protocols.

Huawei WLAN products support the IPv4/IPv6 dual stack, and WLAN ACs support IPv6 dynamic routing protocols (including OSPFv6, RIPv6, ISISv6, and BGPv6) to meet flexible networking requirements of customers.

2.1.4 IPv4/IPv6 Hybrid Access

When both IPv4 and IPv6 terminals exist, you can use either of the following two access deployment schemes.

Figure 2-4 IPv4/IPv6 wireless hybrid access scenario



1. Deploy two different SSIDs for IPv4 and IPv6 terminals to provide WLAN wireless access services.
2. Deploy one SSID for both IPv4 and IPv6 terminals and allow each terminal to use a single IP address (IPv4 or IPv6 address) for communication.

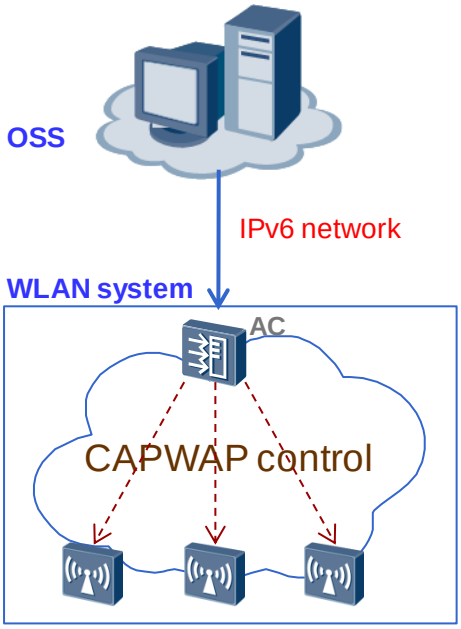
2.2 IPv6 Management and Control

As IPv4/IPv6 dual-stack devices, WLAN APs/ACs support the following network management and control features:

- WLAN AC IPv6 network management
- WLAN AP IPv6 address configuration
- WLAN IPv6 AC discovery mode
- WLAN IPv6 AP-AC tunnel setup
- WLAN AP version load

2.2.1 WLAN Network Management Requirements

Figure 2-5 WLAN IPv6 network management



IPv4/IPv6 dual-stack WLAN products can be directly managed by the OSS, which is the IPv6 network management platform. In the Infrastructure WLAN, an AC provides the network management interface; the OSS performs network management control on the AC; the AC manages and controls all the APs through CAPWAP control channels. That is, only the AC has network management channels, but APs do not have independent network management channels.

Similar to data communication devices (switches/routers), WLAN devices must support the following IPv6 functions:

- IPv6 TCP/UDP communication
- SNMPv6
- Telnet IPv6 and SSH IPv6
- IPv6 web network management

Although IPv4 network management is used on most live networks, Huawei products still support IPv6 network management on the WLAN system and allow IPv6 terminals to log in from WLAN AC service interfaces using IPv6 web network management feature and Telnet IPv6 to implement network management.

2.2.2 AP's IPv6 Address Configuration Mode

- Stateless Address Autoconfiguration (SLAAC) mode: An AP has the SLAAC function. SLAAC is an IPv6-specific address autoconfiguration mode. In this mode, a host (an AP) automatically generates a global IPv6 address using the prefix generated from the network segment address and host address carried in a received Router Advertisement (RA).
- Static mode: An IPv6 address is configured statically. You can log in to an AP through a console interface to configure an IPv6 address for the AP. Alternatively, set up a connection between the AP and AC, and then forcibly configure the AP with a static IPv6 address on the AC and restart the AP to make the configuration take effect.

2.2.3 AC's IPv6 Address Configuration Mode

An AC's IPv6 address is configured statically.

2.2.4 IPv6 AC Discovery Modes

- DHCPv6 option 52: The AC IPv6 list is obtained through Option 52 (RFC 5417).

NOTE

The AC IPv4 list is obtained through Option 138 (Option 43 is commonly used).

When obtaining an IP address through DHCP, an AP also obtains DHCP Option52 to obtain the AC's IPv6 address list.

- DNS AAAA (IPv6) (based on V6 interconnection): In IPv4 networking, an AP obtains an AC's IP address from a DNS server. In IPv6 networking, an AP obtains an AC's IPv6 address from a DNSv6 server. The DHCP Option carries the AC domain name and DNSv6 server. The AP obtains an AC's IPv6 address according to the domain name.
- That is, a DNSv6 server is deployed on the network. After an AP obtains its IP address through DHCP and obtains the AC's domain name through the DHCP Option, the AP queries the AC's IPv6 address through DNSv6.

2.2.5 Tunnel Setup Between an AP and AC

- IPv6 tunnel setup: When there is an IPv6 network between the AP and AC, set up an IPv6 CAPWAP tunnel.
- DS AP preferring IPv4 tunnel: For a dual-stack AP, when IP address allocation and AC discovery can be implemented in IPv4 and IPv6 modes, IPv4 CAPWAP tunnels are set up preferentially. When IPv4 CAPWAP tunnels cannot be set up, IPv6 CAPWAP tunnels are set up.

The process of automatically setting up a tunnel for a Fit AP is as follows:

1. The Fit AP is powered on, operates normally, and obtains an IP address in DHCP, static, or SLAAC mode.
2. When no statically configured AC's IP address is available, the AP dynamically discovers an AC.
3. If both IPv4 and IPv6 connections can be set up, the AP sets up an IPv4 connection with the AC first.
4. If the AP fails to set up an IPv4 connection with the AC, the AP attempts to set up an IPv6 connection with the AC.
5. After the AP sets up an IPv6 connection with the AC, the AP obtains the configuration from the AC to provide wireless services. If no IPv6 connection is set up, the AP initiates a connection setup process using IPv4 first.

NOTE

The preceding process also applies to Layer 2 and Layer 3 networking scenarios between an AP and an AC.

The preceding describes the process of setting up a CAPWAP tunnel between an AP and an AC on an IPv4/IPv6 dual-stack network. The following describes the process of setting up a CAPWAP tunnel between an AP and AC on an IPv6 network.

A Fit AP transitions to the IPv6 mode in one of the following conditions:

- The AP fails to obtain an IPv4 address from a DHCP server.
- No ACs on an IPv4 network respond to the discovery request of the AP.
- The AP cannot set up a connection with any AC on an IPv4 network.

After the AP transitions to the IPv6 mode, it sets up a CAPWAP tunnel with an AC:

1. The AP configuration is performed on the AC; a domain name is configured on the DHCP server and carried in Option 15; an IP address corresponding to the AC's domain name is configured on the DNS server.
2. After the AP starts, it obtains an IP address, DNS server address, and domain name through DHCP.
3. The AP obtains the IP address corresponding to the AC's domain name from the DHCP server and sends a discovery request to this IP address.
4. After receiving the discovery request, the AC checks whether the AP has the access right. If the AP is authorized, the AC replies with a discovery response.
5. The AC and AP set up a CAPWAP tunnel.

NOTE

An AP can obtain an AC's address in many modes. The preceding describes the DHCP+DNS mode. For other modes, see section 2.2.4 "IPv6 AC Discovery Modes."

2.2.6 AP Version Load

Two AP version load modes are available: CAPWAP and FTP.

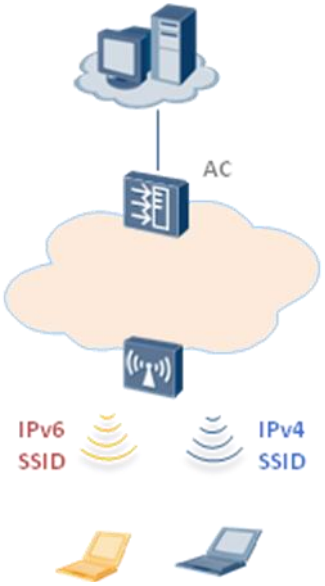
- CAPWAP mode: An AP obtains its version from an AC through the CAPWAP control signaling and control channel. This process is supported in both IPv4 and IPv6 networks.
- FTP mode: An AP supports the FTPv6 client. Administrators can save the AP version on the FTPv6 server, which can be a WLAN AC or an independent FTPv6 server. The AC obtains its version from the FTPv6 server through the built-in FTPv6 client function.

2.2.7 Multi-SSID IPv6 Support

A WLAN AP supports a maximum of 16 VAPs, each of which can use different SSIDs to provide different WLAN access services. You may need to deploy multiple SSIDs to provide wireless access services for IPv4 and IPv6 or deploy one SSID to provide wireless access services for IPv4 terminals, IPv6 terminals, and dual-stack terminals.

IPv6/IPv4 SSID hybrid configuration is supported.

Figure 2-6 IPv6/IPv4 SSID hybrid deployment



NOTE

This deployment uses the scenario where STAs are IPv4 or IPv6 terminals as an example and also applies to the scenario where STAs are IPv4/IPv6 dual-stack terminals.

2.3 QoS and Multicast

2.3.1 QoS Mapping and Scheduling

Figure 2-7 WLAN QoS mapping

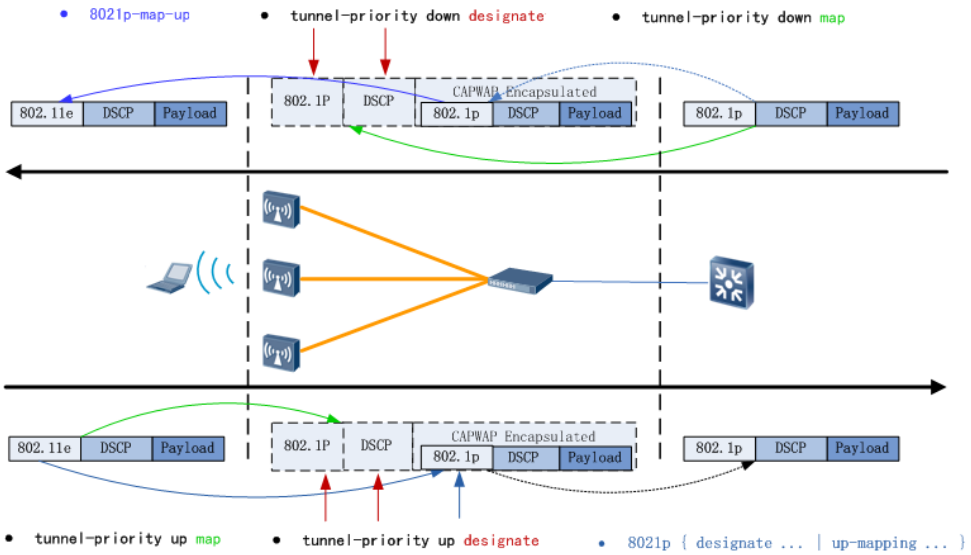


Figure 2-7 includes the following functions:

- Mapping from the user DSCP field to tunnel DSCP field

  The DSCP field of CAPWAP tunnel packets is determined based on the DSCP field of STA packets, corresponding to the mappings in green.
- Specifying tunnel priorities (DSCP or 802.1p)

  High-order bits are set to specify the QoS priority of tunnel packets and low-order bits are set to 0s.
- Traffic classification and specifying the priority and QoS (DSCP or 802.1p)
- WMM QoS

  IPv6 TC field of STA packets is mapping to WMM field of air interface.

When an AP uses centralized forwarding, it adds a CAPWAP header to the packets transmitted from the AP to an AC. Then the packets contain two MAC headers as shown in the dashed lines of the figure.

Upstream direction: After the AP receives air-interface packets of STAs, administrators can use IP headers or 802.11e priorities as packet priorities and map the priorities to user priorities (as indicated by the green arrow in the lower part of the figure). Administrators can also specify user priorities. 802.1p priories of converted Ethernet packets in the tunnel are directly mapped from 802.11e priorities. When the packets arrive at the AC, the AC removes the CAPWAP header from the packets.

Downstream direction: After the AC receives network-side packets, administrators can use IP headers or 802.1p priorities as packet priorities and map the priorities to user priorities (as indicated by the green arrow in the upper part of the figure). Administrators can also specify

user priorities. On the AP, when packets are sent from an air interface, 802.11e priories of the packets in tunnels are directly mapped based on the priorities of original packets in the tunnel.

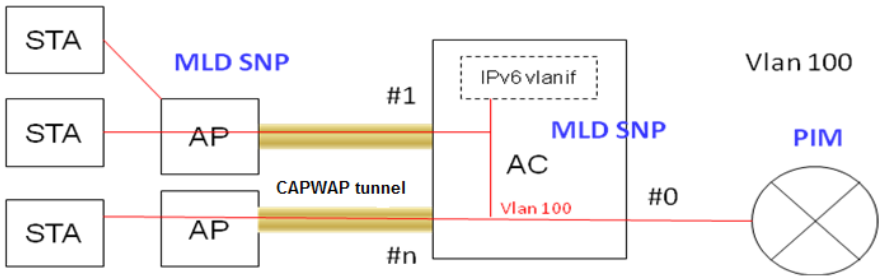
This QoS priority mapping process is the QoS mapping mechanism in IPv4 and does not have special function requirements in IPv6 except that DSCP fields are different in IPv4 and IPv6.

- In IPv4: DSCP value = high-order 3 bits of the ToS field in an IPv4 header
- In IPv6: DSCP value = high-order 3 bits of the traffic class (TC) field in an IPv6 header

NOTE
During priority mapping, the low-order bits that are not overwritten are set to 0s.

2.3.2 Multicast Function Requirements

Figure 2-8 WLAN IPv6 multicast



In the preceding typical multicast scenario, centralized forwarding is performed between APs and the AC; the AC functions as a Layer 2 switch and supports IPv6 MLD snooping; the AC is not an IPv6 router for STAs. In this scenario, the AC does not need to support IPv6 PIM but needs to support MLD snooping and Layer 2 as well as Layer 3 multicast functions. When an AC functions as a Layer 3 gateway, it also supports multicast deployment in IPv6 MLD proxy mode (this mode is not mentioned here).

NOTE
The preceding figure describes a centralized forwarding scenario, which is similar in principles to a local forwarding scenario.

The WLAN system supports the following multicast functions:

- IPv6MLD snooping

  Both APs and ACs support MLD snooping. An AP/AC monitors upstream MLD join requests, records the multicast joins of downstream interfaces, and establishes a multicast forwarding table. When receiving packets of a multicast group from an upstream interface, the AP/AC queries the multicast forwarding table, duplicates the packets, and forwards the packets to other interfaces in the multicast group.

NOTE
IPv6 MLD snooping is supported in both centralized forwarding and local forwarding modes.

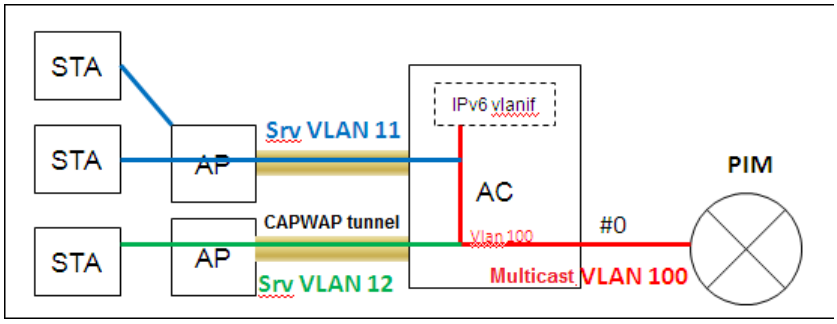
- IPv6 MLD snooping proxy

  The AC does not function as the gateway of STAs, has MLD snooping proxy enabled, sends multicast joins for STAs to the upstream listener (router), and responds to multicast reports to the upstream router.

NOTE
Only the AC supports IPv6 MLD snooping proxy. Therefore, this feature applies to the centralized forwarding mode.

- IPv6 multicast VLAN

Figure 2-9 WLAN IPv6 multicast VLAN



In IPv6 multicast VLAN, different VAPs use different service VLANs (Srv VLANs for short) but correspond to the same upstream multicast VLAN. This feature is the same as IPv4 multicast VLAN. Allocation requirements of this feature are as follows: WLAN DBSS virtual interfaces must support multicast VLAN.

NOTE

This feature only needs to be supported in centralized forwarding mode. That is, only the AC needs to support this feature.

- IPv6 multicast-to-unicast conversion

  An AP unicasts the multicast packets received from the network side to STAs through an air interface. This function has been supported in IPv4 to solve the problem of multicast retransmission failures and low multicast rate. In IPv6, service multicast inherits this feature; however, RA multicast requires special handling. For details, see "RA multicast-to-unicast conversion".

NOTE

This function must be supported in both centralized forwarding and local forwarding modes.

- RA multicast-to-unicast conversion
  - When an AP has multiple VAPs configured and different VAPs correspond to different IPv6 network segments, the RA multicast-to-unicast function must be enabled to support IPv6 inter-VLAN roaming.

    Otherwise, multicasting RAs to a STA will cause the roaming STA to receive RAs of multiple network segments in a roaming area and multiple IPv6 addresses will be generated based on the SLAAC mechanism.
  - In IPv6, RAs are periodically broadcast to all the STAs. Converting these broadcast packets to unicast packets will consume a large amount of air interface resources.

    If multiple VAPs and multiple IPv6 network segments are not required, for example, only a single VAP needs to be deployed, consider disabling the RA multicast-to-unicast function to reduce the consumption of air interface resources when there are a small number of IPv6 access terminals (fewer than five access terminals).

2.4 Security and Authentication

2.4.1 Network Security

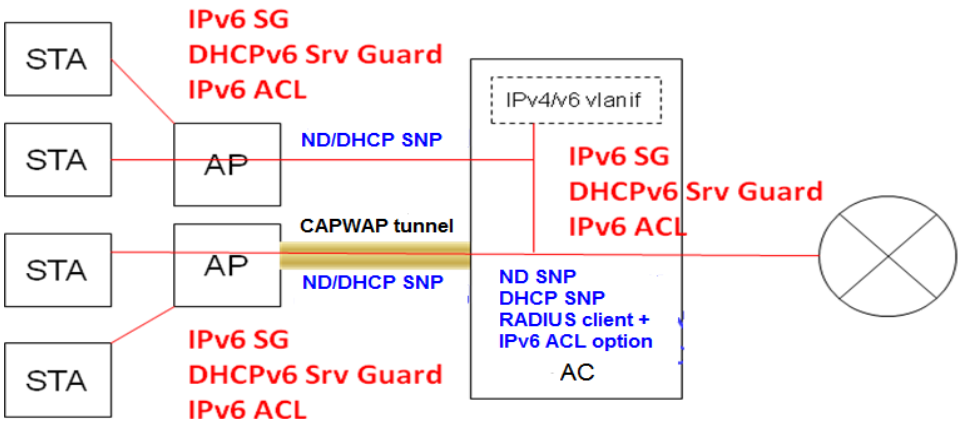
Layer 3 network security isolation is implemented through ACLs. In the WLAN system, ACLs are implemented differently according to forwarding modes:

- In centralized forwarding, authentication-free rules/ACLs are implemented on WLAN ACs.
- In local forwarding, data traffic is directly forwarded on a WLAN AP, and WLAN ACs may be not in the data forwarding path. Therefore, authentication-free rules/ACLs are implemented on a WLAN AP.

Huawei full series WLAN products support IPv4 and IPv6 ACLs.

2.4.2 Terminal Security Defense

Figure 2-10 WLAN IPv6 multicast



NOTE

1. Characters in red indicate device features, and characters in blue indicate device functions that are used to support the implementation of features in red.
2. These features must be supported in both centralized forwarding and local forwarding modes.

Figure 2-10 shows the following features and functions:

- IPv6 SG

  Similar to IPv4 SG, IPv6 SG aims to prevent terminal IP address spoofing. IPv6 SG obtains STA IP configurations based on DHCPv6 snooping or statically binding and set up binding between STA IP addresses and MAC addresses. This feature is implemented based on the ND SNP/Cache and DHCP SNP, similar to IPv4 SG. The mechanism is that an AP checks received packets based on the bindings between IPv6 addresses and MAC addresses of STAs, discards the packets that do not match the bindings, starts the ND SNP function to check ND packets and discard invalid ND packets that do not match the bindings.

- DHCPv6 Srv Guard

  Similar to DHCPv4 Srv Guard, DHCPv6 Srv Guard aims to prevent STAs from deploying a bogus DHCP server by discarding DHCP response packets sent from STAs.

DHCPv6 Srv Guard is supported in both centralized forwarding and local forwarding modes. Therefore, this feature is implemented on an AP.

Wired interfaces on an AC also support this feature.

- Dynamic ND protection

  This feature prevents other terminals to forge the IPv6 address of a STA to make an ND response, similar to IPv4 Dynamic ARP Inspection (DAI).

  This feature is implemented on an AP for WLAN access users or implemented on an AC for non-WLAN access users (such as terminals access from an AC wired interface).

- User/role-based IPv6 ACL (also user ACL specified by RADIUS)

  This feature corresponds to Cisco AAA Override. That is, RADIUS delivers user ACLs or roles (user group), and applies the ACLs or roles to users to be authenticated. This feature has been implemented in IPv4. IPv6 has new system function requirements:

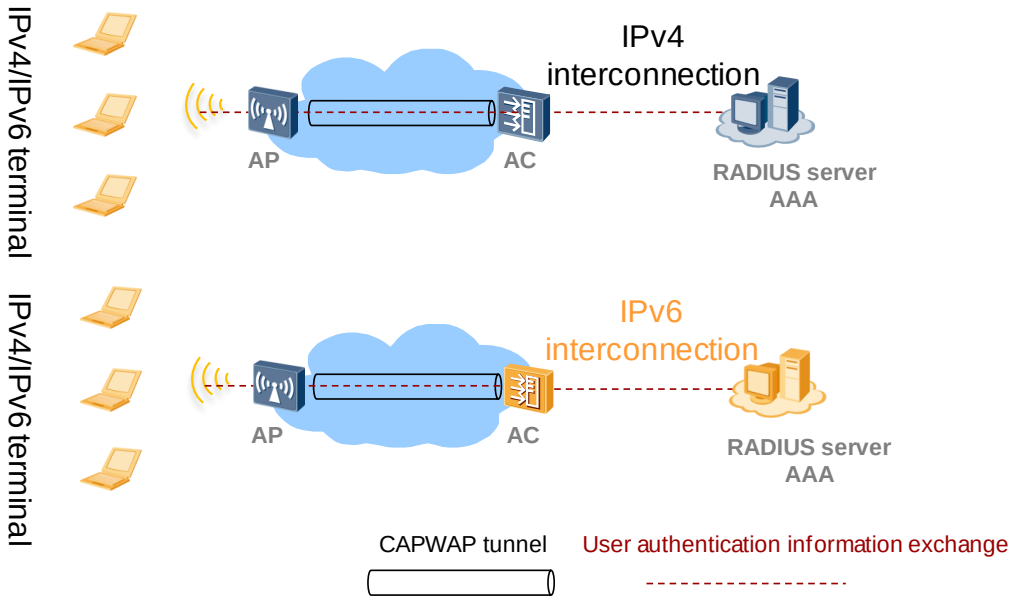
  - Add the RADIUS attribute and carry the IPv6 ACL so that RADIUS notifies the user IPv6 ACL.
  - Modify the user group configuration, specify IPv6 ACLs, and bind IPv4 and IPv6 ACLs.

2.4.3 AAA

Wireless terminal user authentication consists of two modes: 802.1X authentication and Portal authentication.

The basic framework for 802.1X authentication is client—authenticator—authentication server. Pure Layer 2 technologies are used between the client and authenticator, independent of IPv4 or IPv6. RADIUS authentication is often used between the authenticator and authentication server. If IPv6 must be supported, communication with the IPv6 RADIUS server must be supported.

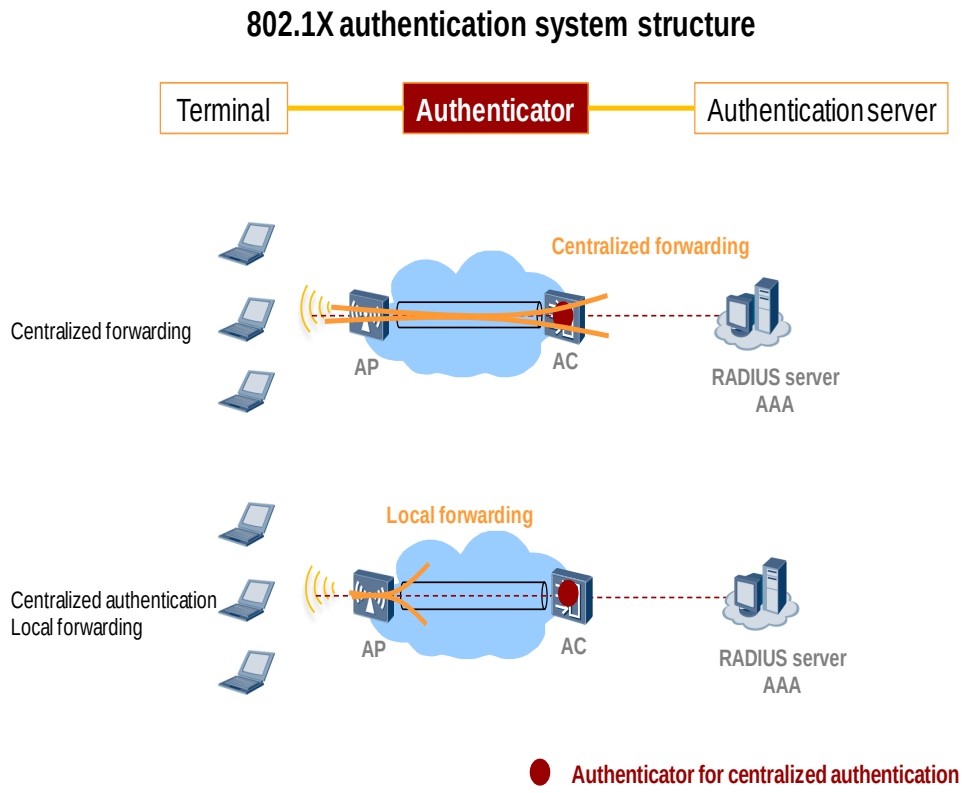
Figure 2-11 WLAN IPv6 AAA networking



A WLAN AC supports the IPv4/IPv6 dual stack and can connect to an IPv4 or IPv6 RADIUS server.

In the basic framework for 802.1X authentication, there are three roles: client, authenticator, and authentication server. The authenticator includes the RADIUS client function. The WLAN system has two network elements: AP and AC. Centralized authentication is used regardless of which forwarding mode (centralized or local forwarding) is deployed in the WLAN system. In this situation, a WLAN AC plays a fixed role: authenticator to implement the RADIUS client function, as shown in Figure 2-12.

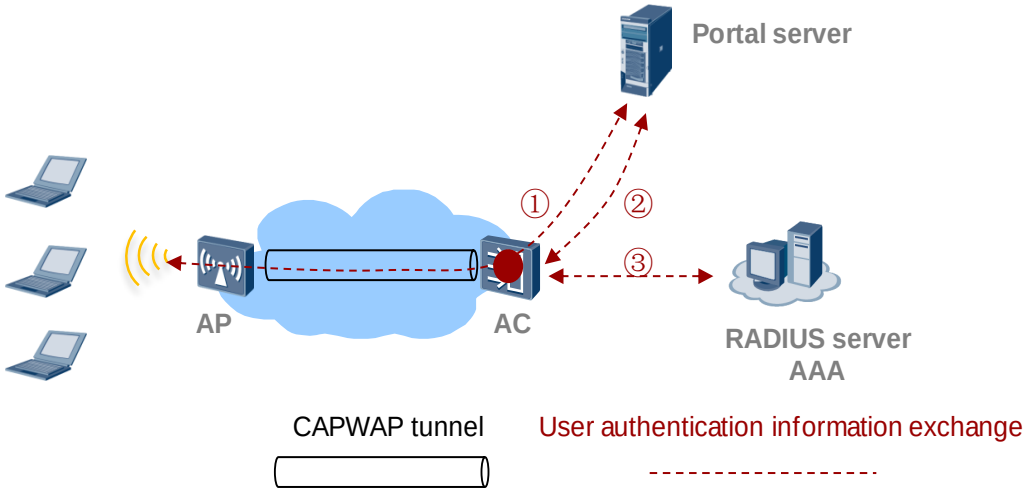
Figure 2-12 WLAN networking scenario for 802.1X authentication



During RADIUS authentication, an AC may obtain IPv6-related extended options from the RADIUS server, such as ACL and STA's IP address, to support the access authentication, authorization, and accounting functions of IPv6 clients.

Figure 2-13 shows the basic framework for Portal authentication.

Figure 2-13 Portal authentication flowchart in the WLAN system



Portal authentication has three steps:

1. A STA accesses the Portal server and inputs an account/password to trigger authentication.
2. The Portal server sets up a connection with the WLAN AC to exchange user account/password information.
3. The WLAN AC sets up a connection with the RADIUS server to complete user authentication.

An IPv6 STA can directly access an IPv6 Portal server, and the Portal server must support IPv4/IPv6 dual-stack capabilities and communicate with the WLAN AC through an IPv4 address to complete subsequent user authentication.

Currently, in the WLAN system, a WLAN AC can only function as the authenticator, and a Portal or RADIUS server cannot be deployed beside a WLAN AP.

During Portal authentication, wireless links are often open (open mode at the link layer). That is, wireless users can set up an air interface connection without link authentication. However, wireless users cannot access network resources at this moment. Huawei provides authentication-free rules to allow users to access resources in the open service zone before the users pass Portal authentication. Resources include the DNS server, security patching server, and Portal server. Authentication-free rules are implemented through ACLs and support both IPv4 and IPv6 ACLs. In centralized forwarding, authentication-free rules/ACLs are implemented on WLAN ACs. In local forwarding, data traffic is directly forwarded on WLAN APs, and WLAN ACs may be not in the data forwarding path; therefore, authentication-free rules/ACLs are implemented on WLAN APs.

2.5 Other Features

2.5.1 WLAN Roaming

Among three IPv6 networking scenarios: IPv4 over IPv6, IPv6 over IPv4, and IPv6 over IPv6, IPv4 over IPv6 networking supports roaming features in IPv4 over IPv4 networking because IPv4 STA roaming does not affect IPv6 networks.

In IPv6 STA roaming capabilities, the system supports intra-VLAN roaming and inter-VLAN roaming. The current version does not support inter-AC roaming of IPv6 terminals.

- Intra-VLAN roaming

  IPv6 intra-VLAN roaming is the same as IPv4 intra-VLAN roaming and has no special function requirements on the WLAN system.

- IPv6 inter-VLAN roaming

  If an IPv6 terminal uses a statically configured IPv6 address or DHCPv6 address, the destination AP encapsulates the packets of the terminal in the pre-roaming VLAN and forwards the packets to the network after the terminal roams to the destination AP. This process ensures that the IP address of the wireless user remains unchanged, implementing smooth roaming and uninterrupted services.

- Inter-AC roaming

  IPv6 inter-AC roaming is similar to IPv4 inter-AC roaming and has no special requirements on the IPv6 static address configuration and DHCP address configuration modes. IPv6 roaming in SLAAC address configuration mode has the same problem as IPv6 inter-VLAN roaming: RA multicast-to-unicast conversion is required to implement roaming.

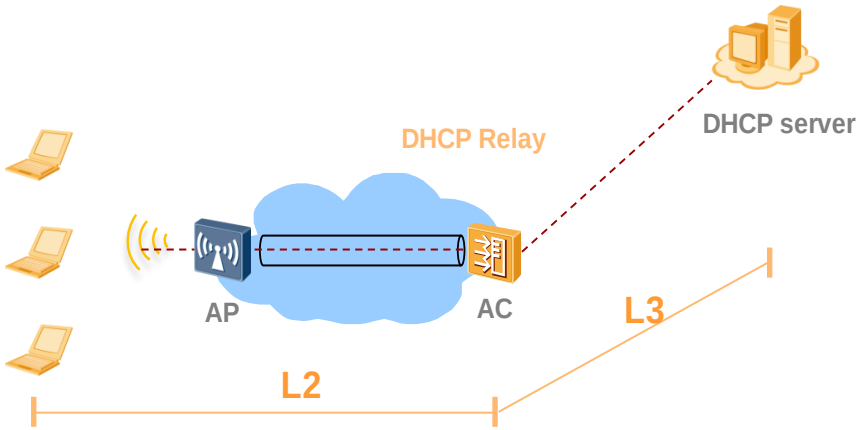
2.5.2 DHCPv6

In IPv6 networking, you can deploy an independent DHCPv6 server or use a WLAN AC with a built-in DHCPv6 server to reduce network construction costs and implement fast network deployment.

When an independent DHCPv6 server is deployed on the network, a WLAN AC can provide the DHCP relay or DHCP SNP function.

- WLAN AC supporting DHCPv6 relay

Figure 2-14 WLAN AC DHCP relay deployment



If a WLAN AC functions only as a Layer 2 switch for STAs, you can deploy the DHCPv6 relay function on the upstream router to allocate IPv6 addresses to STAs, as shown in Figure 2-15.

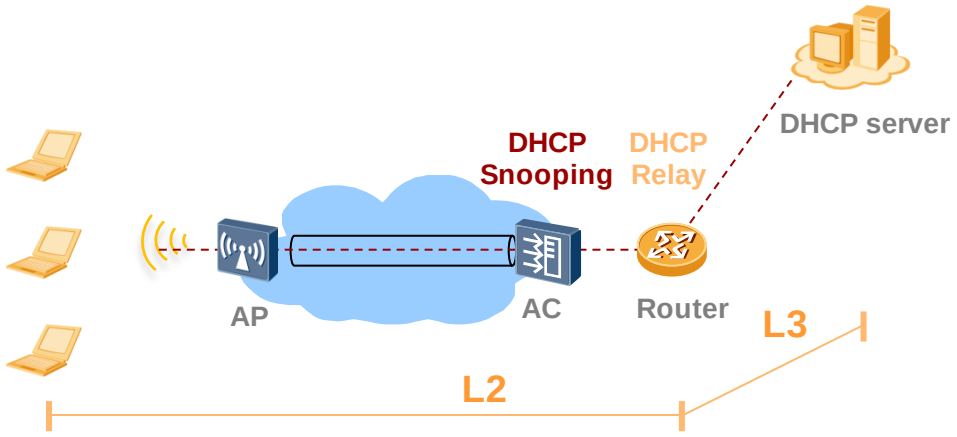
When a WLAN AC functions as a Layer 3 gateway for STAs, you can enable the DHCPv6 relay function on the AC to allocate IPv6 addresses to STAs.

NOTE

Although a CAPWAP tunnel exists between an AP and an AC, the AC can function as a DHCPv6 relay agent for STAs regardless of whether centralized or local forwarding is used.

- AP/AC supporting DHCPv6 SNP

Figure 2-15 WLAN AC DHCP snooping deployment



When a WLAN AC functions as a Layer 2 switch for STAs, you can enable the DHCPv6 SNP function to obtain the IPv6 addresses allocated to STAs and provide support for IPv6 SG.

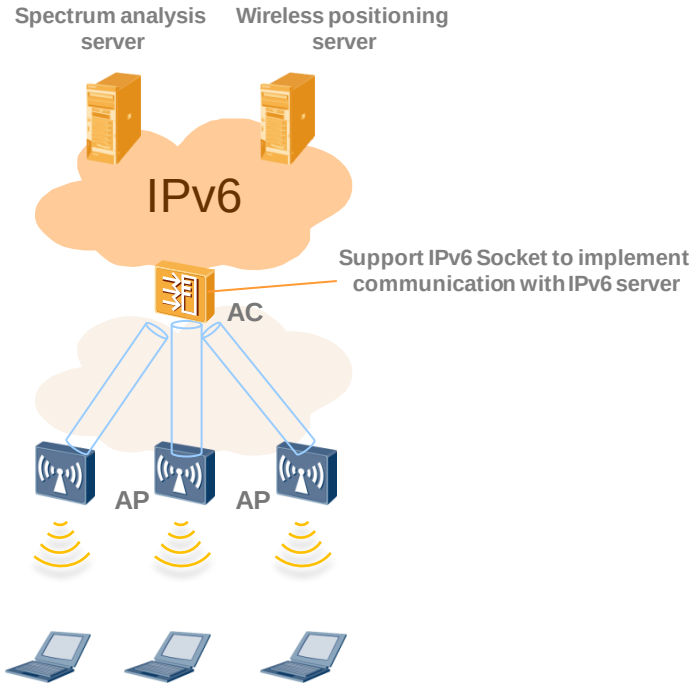
NOTE

Although a CAPWAP tunnel exists between an AP and an AC, the AC can still provide the DHCPv6 SNP function for STAs regardless of whether centralized or local forwarding is used.

If no independent DHCPv6 server is deployed, you can start the DHCPv6 server function on a WLAN AC to allocate IPv6 addresses to STAs and APs. DHCPv6 Option 52 must be supported to specify an AC's IP address for an AP.

2.5.3 Spectrum Analysis and Wireless Positioning

Figure 2-16 IPv6 support for spectrum analysis and wireless positioning



Spectrum analysis and wireless positioning are independent of which version (IPv4 or IPv6) wireless terminals are using. A WLAN AP collects wireless channel information and sends the information to a WLAN AC for centralized pre-processing, which then sends the information to the connected IPv6 server through an IPv6 socket connection for processing. In this situation, the WLAN AC must support the IPv6 protocol stack and set up an IPv6 socket connection with an IPv6 server.

3 Technology Characteristics of Huawei IPv6 Implementation

3.1 Supporting Flexible IPv6 Networking Modes

Currently, basic access networks of most enterprises and institutions are pure IPv4 networks. Building an IPv6 WLAN on such a basic network forms typical IPv6 over IPv4 networking. This networking mode allows STAs accessing IPv6 networks to communicate with each other across IPv4 access networks.

In addition to the typical IPv6 over IPv4 networking mode, Huawei WLAN products also support another two IPv6 WLAN networking modes: IPv4 over IPv6 and IPv6 over IPv6. These networking modes provide flexible WLAN IPv6 networking support to meet customer network requirements.

3.2 Supporting a Variety of IPv6 Dynamic Routing Protocols

In the infrastructure WLAN networking of Fit AP+AC, Huawei products support two forwarding modes: local forwarding and centralized forwarding. Centralized forwarding is also called tunnel forwarding and is an overlay networking mode in nature. The WLAN system transmits data packets of wireless users over CAPWAP tunnels between an AC and AP to the basic access bearer network for packet forwarding. However, products of some vendors can only provide the Layer 2 forwarding function in the WLAN system, and WLAN ACs cannot function as the IP gateway of terminals. In Huawei WLAN IPv6 networking solutions, WLAN ACs can function as IPv6 gateways of STAs and support multiple IPv6 dynamic routing protocols in addition to the IPv6 static routing protocol.

Huawei WLAN ACs can function as IPv6 gateways and support multiple IPv6 dynamic routing protocols regardless of whether local or centralized forwarding is used. These IPv6 capabilities provide flexible and diverse networking modes and remove the need to deploy independent IPv6 routers.

3.3 Providing Powerful IPv6 Network Management, AAA, and DHCP Capabilities

Huawei WLAN AP/AC system can work with the IPv6 network management system to provide comprehensive network management and work with the IPv6 AAA (RADIUS) system to provide authentication, authorization, and accounting for IPv4 and IPv6 terminals.

WLAN ACs support the DHCPv6 relay and DHCPv6 SNP features, can work with an external DHCPv6 server to allocate IPv6 addresses to terminals, or provide a built-in DHCPv6 server function to directly allocate IPv6 addresses to terminals and APs. The built-in DHCPv6 server function facilitates network construction and saves network construction costs.

3.4 Offering Rich IPv6 Security Functions

Huawei WLAN system supports traditional IPv6 ACLs and IPv6 ACLs dynamically delivered during RADIUS authorization.

Huawei WLAN system supports IPv6 SG to prevent IP address spoofing, supports DHCPv6 Srv Guard to prevent bogus DHCPv6 server, and supports dynamic ND protection to prevent other STAs from forging the IPv6 address of an authorized STA to make an ND response (similar to IPv4 DAI).

4 Typical Networking Applications

Currently, IPv4 dominates the Internet. However, universities and education networks have established an IPv6 backbone network (IPv6 CRENET) to achieve IPv6 interconnection between colleges and universities. The following uses universities as an example to describe WLAN IPv6 networking.

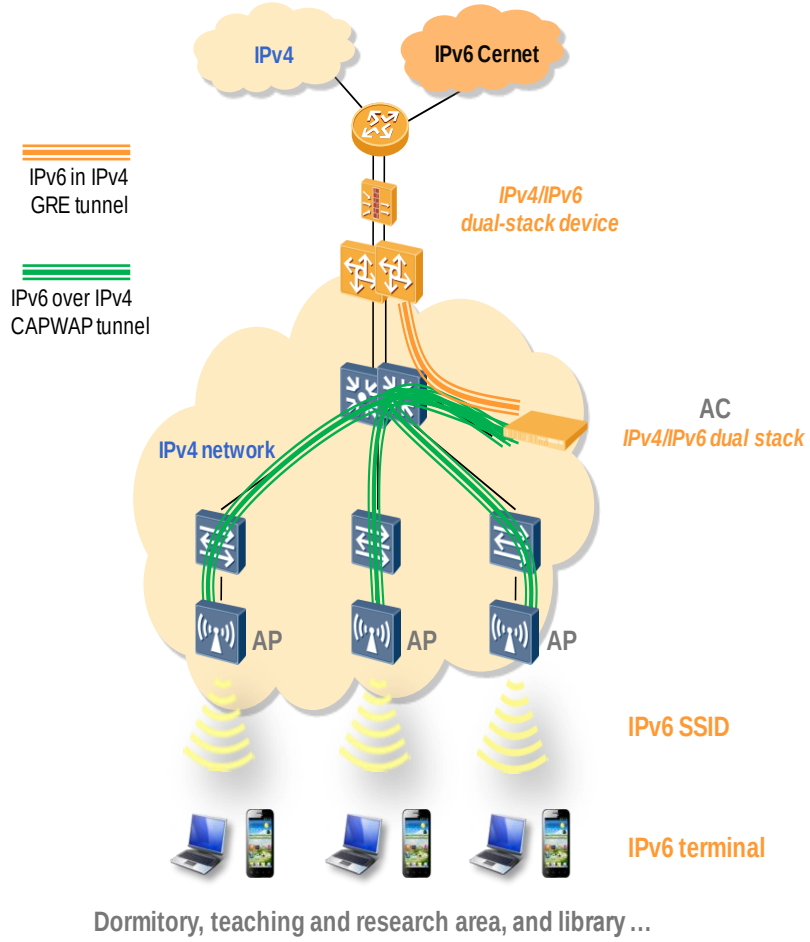
Each university can deploy an IPv6 network independently according to service requirements. Universities require that newly purchased network devices have IPv4/IPv6 dual-stack capabilities. However, there are still many old devices that do not support IPv6 communication on live networks. Furthermore, IPv6 is not the mainstream application. IPv4 is still the basic communication mode in campus networks. In this situation, a common practice to deploy an IPv6 WLAN is to build an IPv6 network over the traditional IPv4 access bearer network.

The following describes two typical WLAN IPv6 networking scenarios.

4.1 IPv4/IPv6 Dual-Stack Network Solution

The basic access bearer network is still an IPv4 network. A WLAN network can be deployed on the IPv4 network to allow IPv6 wireless terminals to access, implementing IPv6 wireless communication.

Figure 4-1 Dual-stack network solution



In a dual-stack network solution, a WLAN server needs to be deployed for traditional IPv4 terminals and the WLAN SSID access service must be independently deployed to provide IPv6 wireless communication service. APs use the centralized forwarding mode to encapsulate IPv6 packets of terminals in IPv4 CAPWAP tunnels and send the packets to the WLAN AC for processing. The AC is an IPv4/IPv6 dual-stack device, sets up an IPv4 GRE tunnel with the upstream IPv6 backbone network boarder router (the core switch supporting IPv4/IPv6), obtains original IPv6 packets from the IPv4 CAPWAP tunnel, and sends the packets to the IPv4/IPv6 dual-stack core network through the IPv4 GRE tunnel (IPv6 in IPv4) for forwarding.

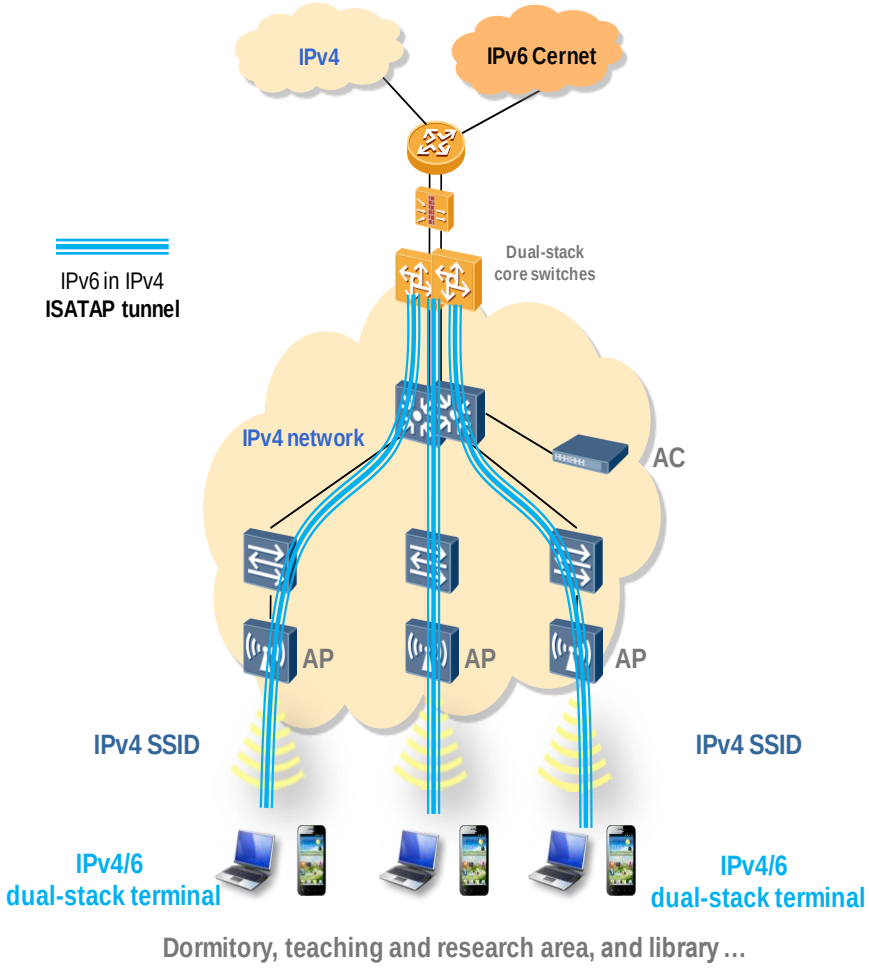
NOTE

In most cases, a dedicated IPv6 SSID can be deployed to provide wireless IPv6 communication service or an SSID with dual-stack capabilities can be deployed to provide wireless communication service for both IPv4 and IPv6 terminals.

4.2 Terminal Tunnel Solution

In an IPv6 network deployment solution, a terminal can function as a tunnel endpoint. IPv4/IPv6 dual-stack terminals set up Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) tunnels with dual-stack core switches, encapsulate IPv6 communication packets in ISATAP tunnels, and send the packets to dual-stack core switches for IPv6 communication.

Figure 4-2 Terminal tunnel solution



The Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) is a technology that assigns IP addresses and automatically sets up tunnels between hosts, and between hosts and routers. It provides IPv6 hosts with unicast IPv6 connectivity across an IPv4 network. ISATAP usually transmits IPv6 packets between dual-stack nodes on an IPv4 network. In Figure 4-2, terminals automatically set up IPv6 in IPv4 ISATAP tunnels with core switches. APs and the AC in the WLAN system regard the encapsulated packets as IPv4 packets but not IPv6 packets. That is, as the access bearer network, the WLAN system only needs to provide IPv4 communication service. In this solution, administrators can use centralized forwarding and local forwarding as required regardless of whether IPv6 communication is started on terminals.