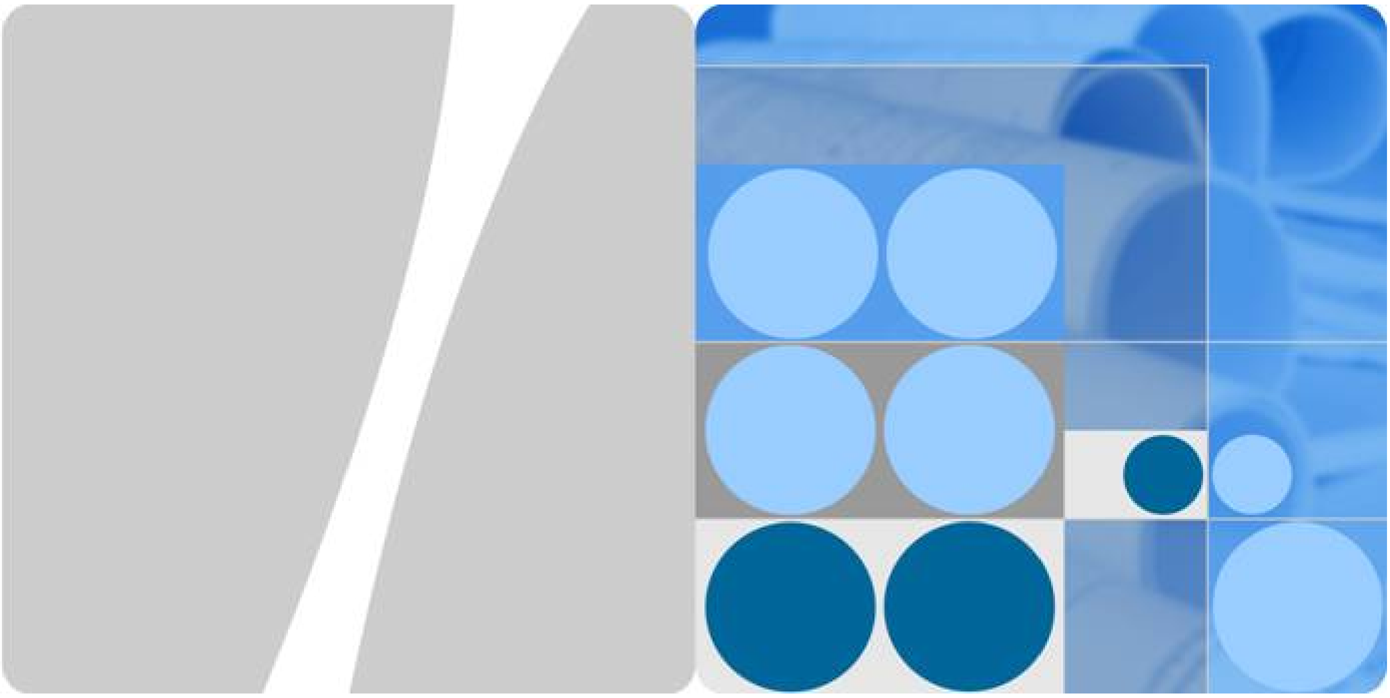


Huawei AC6605 Series Access Controllers

V200R003C00

Issue	**01**
Date	**2013-04-30**

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Huawei Technologies Co., Ltd.

Address: Huawei Industrial Base
Bantian, Longgang
Shenzhen 518129
People's Republic of China

Website: http://enterprise.huawei.com

About This Document

Intended Audience

This document describes the orientation, characteristics, architecture, service features, application scenarios, operation and maintenance functions, and technical specifications of the AC6605.

This document helps you understand the characteristics and features of the AC6605.

This document is intended for:

- Network planning engineers
- Hardware installation engineers
- Commissioning engineers
- Data configuration engineers
- Onsite maintenance engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

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

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

Symbol	Description
📖 NOTE	Provides additional information to emphasize or supplement important points in the main text.

Change History

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

Issue 01 (2013-04-30)

Initial commercial release.

Contents

1 Product Orientation and Characteristics

About This Chapter

The wireless local area network (WLAN) technology defined in IEEE 802.11 is widely used on MANs and enterprise networks. WLAN access can be used as the first-mile access solution. Compared with other wireless access technologies, WLAN provides higher bandwidth with lower costs, fully meeting user requirements for the high-speed wireless broadband service.

1.1 Product Orientation

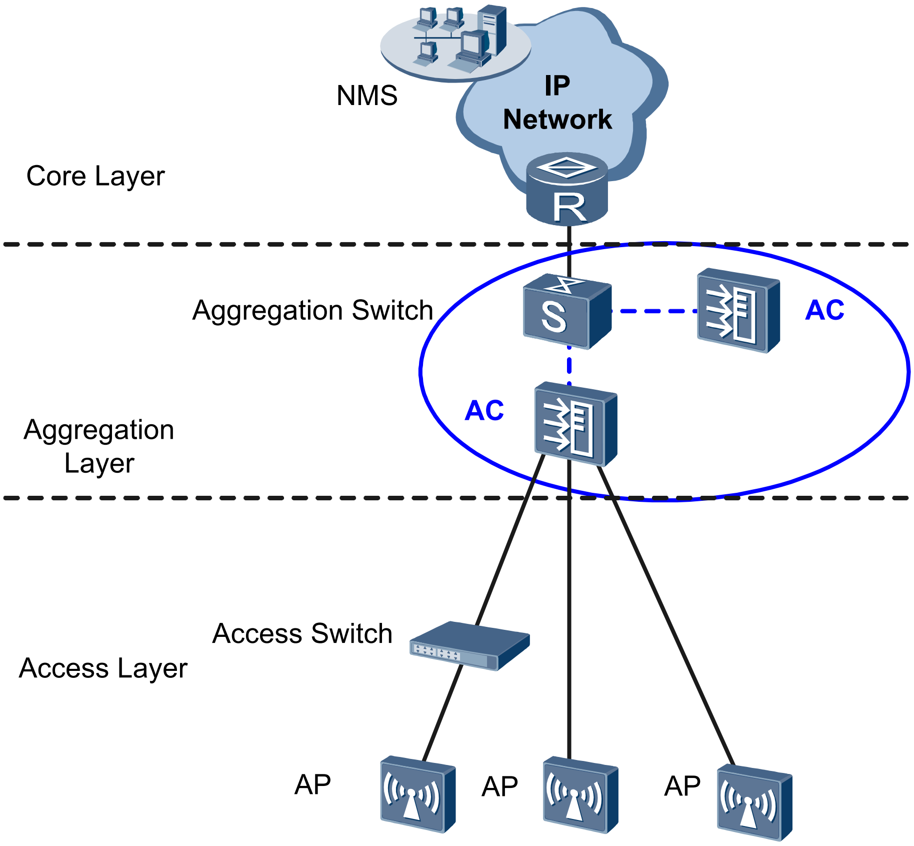
CAUTION

AC6605 is class A product. The AC6605 that is operating may cause radio interference. Customers need to take prevention measures.

Huawei AC6605-26-PWR (AC6605 for short) is access controller (AC) applicable to MANs and enterprise networks for wireless access. AC6605 has a large capacity and high performance. It is highly reliable, easy to install and maintain, and features such advantages as flexible networking and energy conservation.

The AC resides at the aggregation layer to provide the high-speed, secure, and reliable WLAN service. **Figure 1-1** shows the position of the AC in the overall network solution.

Figure 1-1 Position of the AC in the overall network solution



The AC is connected to a BRAS in inline or bypass mode. For details, see **2 Application Scenarios**.

The AC6605 has the following features:

- Has the access and aggregation functions.
- Provides PoE power (15.4 W) or PoE+ power (30 W) for 24 interfaces so that APs can directly connect to these interfaces.
- Has various user policy management and authority control capabilities.
- Supports redundancy backup and hot swapping of AC or DC power supplies, ensuring long-term operation.
- Can be maintained using the eSight, web system, or command line interface.

1.2 Product Characteristics

1.2.1 Abundant Port Types

The AC6605 provides various ports to meet the requirements of all scenarios. **Table 1-1** lists the ports that the AC6605 provides.

Table 1-1 AC6605 port description

Port Type	Quantity	Description
Uplink port	Two 10GE optical ports	The 10GE ports use Small Form-Factor Pluggable (SFP+) optical transceivers.
Service port	24 GE ports	Among the 24 electrical ports, the last four are used with four optical ports as combo interfaces.
Maintenance port	One RJ45 maintenance serial port	It is an RS-232 port.
	One RJ45 maintenance Ethernet port	It is a 100BASE-TX port.
	One mini USB maintenance serial port	It is mutually exclusive with an RJ45 maintenance serial port.

1.2.2 Large Capacity, High Performance, Integrated Design

The AC provide a large capacity and high performance, and adopts an integrated design to allow for flexible deployment.

- Integrated design: An AC device integrates the AC and LSW units to provide wireless access and wired access/aggregation services.
- Large switching capacity: An AC device has 24 GE interfaces and 2 10GE interfaces, and provides 10 Gbit/s forwarding capacity.
- PoE: The AC supports the PoE function and can provide the maximum power on 24 ports. This PoE capability can provide power to APs and other powered devices (PDs) connected to the AC unit.

1.2.3 Carrier-Class Reliability

The AC provides the following reliability designs, ensuring long-term operation.

- The AC supports port backup based on the Link Aggregation Control Protocol (LACP) or Multiple Spanning Tree Protocol (MSTP).
- The AC supports redundant AC/DC power supplies.
- The AC supports hot swappable power supplies.
- The AC supports 1+1 hot backup.

1.2.4 Easy-to-Install and Easy-to-Maintain

The AC is easy to install and maintain, simplifying network deployment.

- The AC6605 dimensions (width x depth x height) are 442 mm × 420 mm × 44.4 mm and the AC6605 can be installed in a standard IEC cabinet (19 inch).
- Power supplies of AC are hot swappable, facilitating maintenance.
- The built-in web system of AC allows local GUI-based management.
- The AC can be managed by the eSight that provides various northbound interfaces.
- The AC support the intra-board temperature probe, which monitors the operating environment of the AC in real time.

1.2.5 Energy Conservation

The AC adopts the following measures to save energy:

- Low noise fans that can adjust the speed automatically are used, thus reducing noises in the system and power consumption of fans.
- The chip switches to the power saving mode when no connected device is detected on a service interface, that is, the interface is idle.
- It uses highly-integrated and energy-saving chips produced through advanced processing techniques. With the help of the intelligent device management system, the chips not only improve system performance but also greatly reduce power consumption of the entire system.

2 Application Scenarios

About This Chapter

The AC is connected to an aggregation switch in chain or branched mode.

NOTE

The following section describes how to connect an AC to an aggregation switch in chain or branched mode.

The AC processes both control flows and data flows. Management flows must be transmitted over Control And Provisioning of Wireless Access Points (CAPWAP) tunnels. Data flows can be transmitted over CAPWAP tunnels or not, as required.

The CAPWAP protocol defines how APs communicate with ACs and provides a general encapsulation and transmission mechanism for communication between APs and ACs. CAPWAP defines data tunnels and control tunnels.

- Data tunnels encapsulate 802.3 data packets to be sent to the AC.
- Control tunnels transmit control flows for remote AP configuration and WLAN management.

Two forwarding modes are available according to whether data flows are transmitted on CAPWAP tunnels:

- Direct forwarding: is also called local or distributed forwarding.
- Tunnel forwarding: is also called centralized forwarding. It is usually used to control wireless user traffic in a centralized manner.

You can select the chain or branched mode according to networking requirements. On the AC, you can configure direct forwarding for some APs and tunnel forwarding for other APs. In tunnel forwarding mode, all wireless user traffic is aggregated to an AC, which may create a switching bottleneck. Therefore, tunnel forwarding is seldom used on enterprise networks.

2.1 Bypass Networking

In bypass networking mode, the AC is connected to a network device (usually an aggregation switch) to manage APs.

The AC manages APs. Management flows are transmitted in CAPWAP tunnels, and data flows are forwarded to the upper layer network by the aggregation switch and do not pass through the AC.

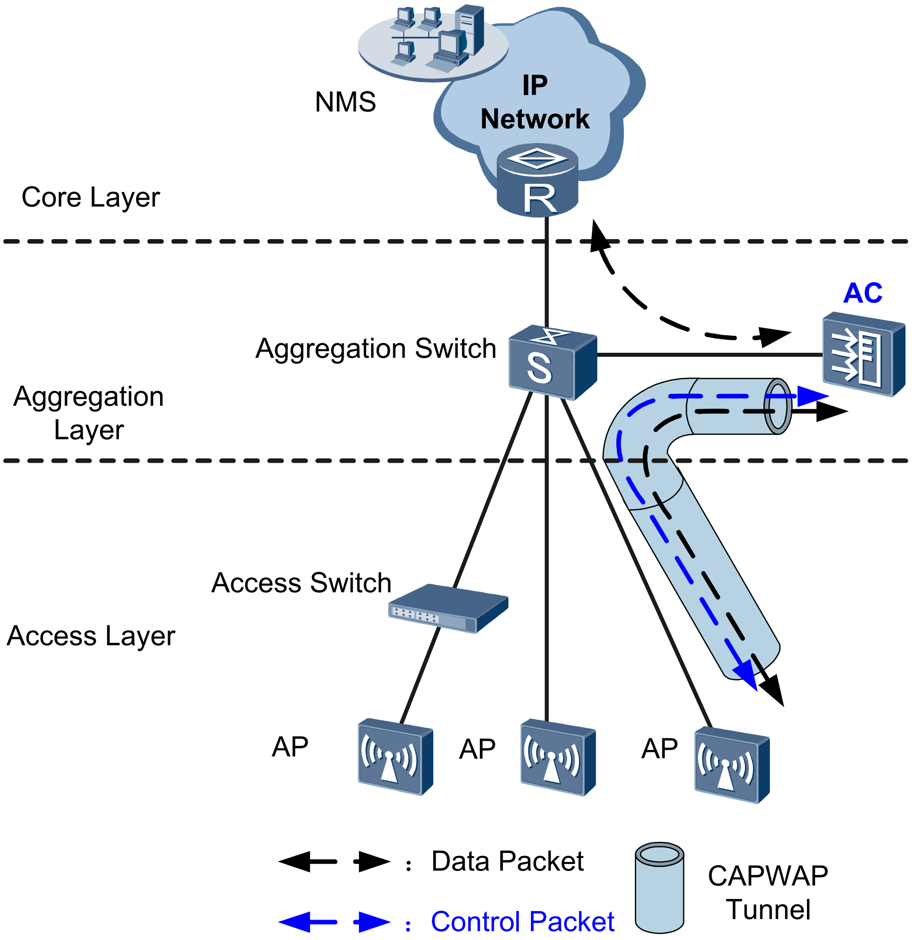
Tunnel Forwarding

In tunnel forwarding mode, wireless user service data is transmitted between APs and ACs over CAPWAP tunnels.

In **Figure 2-1**, both management flows and data flows of APs are transmitted to the AC over CAPWAP tunnels, and then the AC transparently transmits these flows to the upstream device.

Tunnel forwarding is usually used to control wireless user traffic in a centralized manner. This forwarding mode facilitates device deployment and controls all wireless user data flows by aggregating traffic of all wireless users connected to APs to an AC through CAPWAP data tunnels.

Figure 2-1 Bypass networking in tunnel forwarding mode

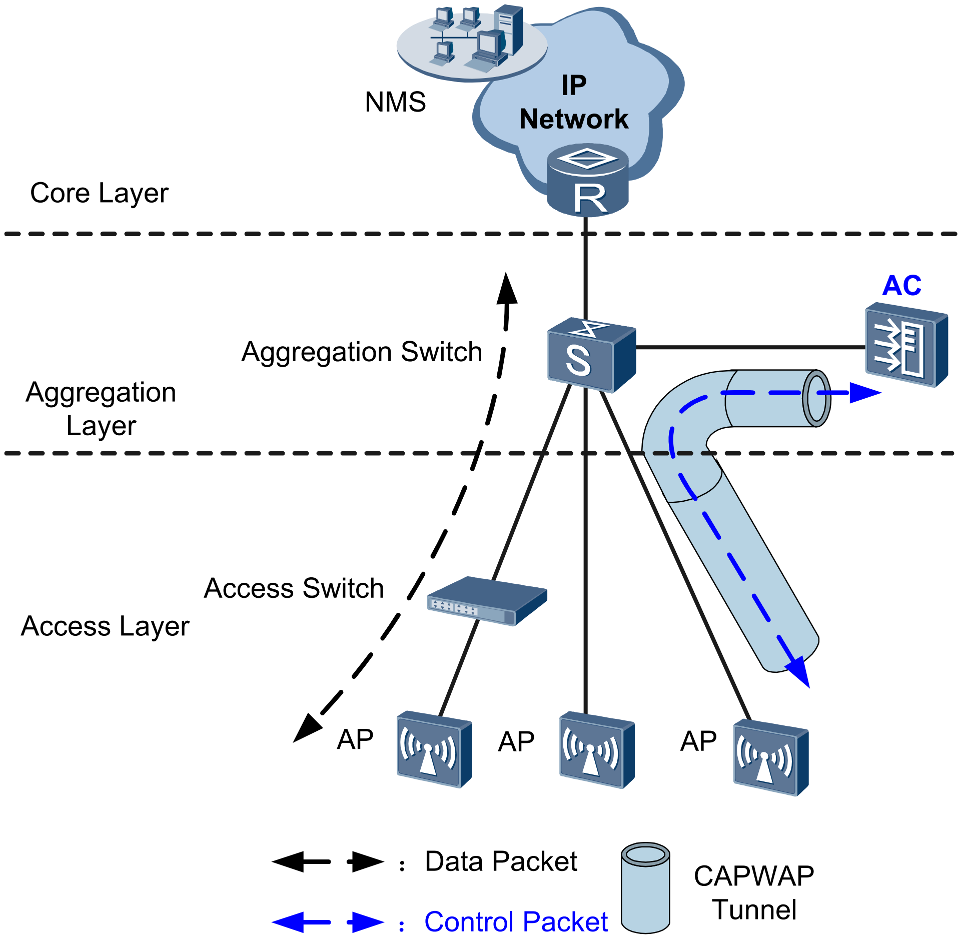


Direct Forwarding

In direct forwarding mode, wireless user service data is translated from 802.3 packets into 802.11 packets, which are then forwarded by an uplink aggregation switch.

The bypass networking mode is often used on enterprise networks. Wireless user service data does not need to be processed by an AC, eliminating the bandwidth bottleneck and facilitating the usage of existing security policies. Therefore, this networking mode is recommended for integrated network deployment.

Figure 2-2 Bypass networking in direct forwarding mode



- The AC only manages APs. All AP control flows must reach the AC.

  Interfaces connected to the AC are reserved on the aggregation switch. The aggregation switch functions as the DHCP server to allocate IP addresses to APs. APs obtain the IP address of the AC using the DNS function, DHCP Option 43 or DHCP Option 15 in DHCP packets.

- Data flows from APs are forwarded by the Layer 2 switch and aggregation switch, and do not pass through the AC.

  Different service VLANs are assigned to STAs with different service set identifiers (SSIDs). The access switch and aggregation switch identify packets from these VLANs and forward these packets to the upstream device. The aggregation switch controls user access, and allocates IP addresses to users. After a user is authenticated by the aggregation switch, traffic from the user is forwarded to the Internet across the IP network.

Application

In bypass networking mode, the AC manages all the APs connected to the aggregation switch. This network topology applies to scenarios where APs are scattered across hot spots.

The bypass networking mode requires only a small modification to the existing network, facilitating device deployment. Tunnel forwarding is recommended for most enterprise networks and commonly used for overlay network deployment.

2.2 Inline Networking

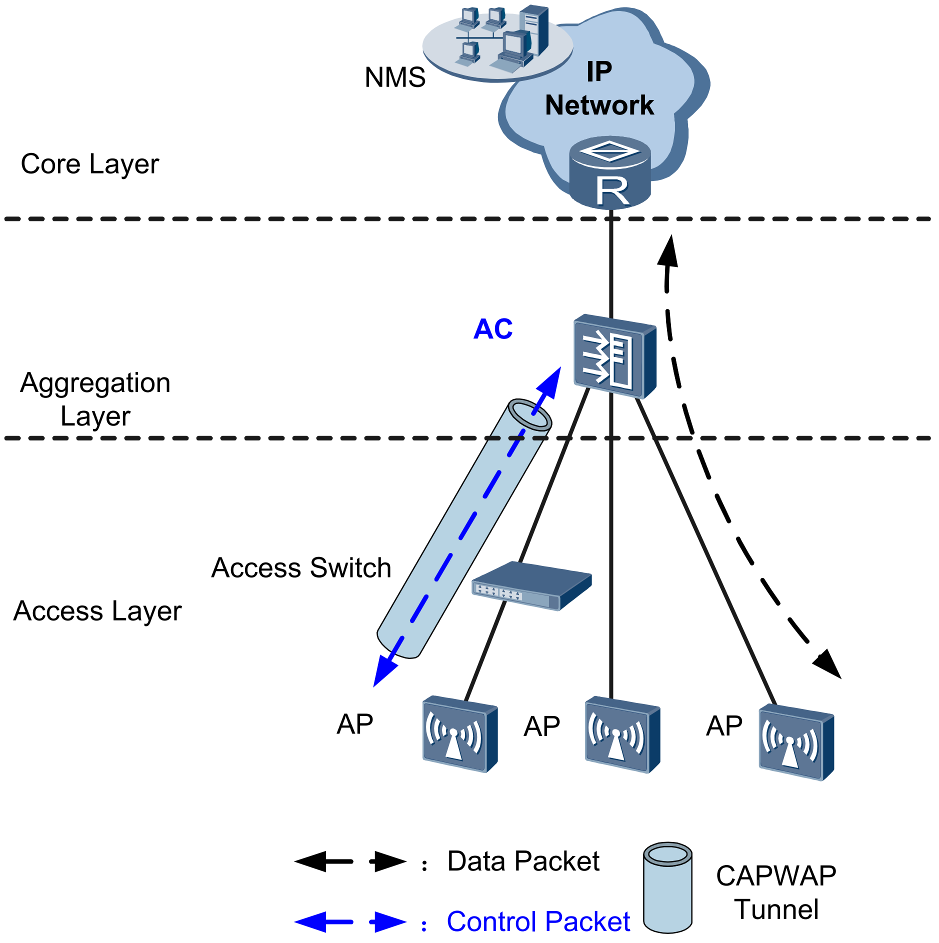
In inline networking mode, APs or access switches are directly connected to the AC. The AC functions as both an AC and an aggregation switch to forward and process APs' data and management services.

In inline networking mode, the AC sets up CAPWAP tunnels with APs to configure and manage these APs over CAPWAP tunnels. Service data of wireless users can be forwarded between APs and the AC over CAPWAP data tunnels or be directly forwarded by APs.

In inline networking mode, direct forwarding is often used so that user service data can be forwarded on APs.

The AC functions as the DHCP server to allocate IP addresses to APs. APs obtain the IP address of the AC using the DNS function, DHCP Option 43 or DHCP Option 15 in DHCP packets, or Layer 2 discovery protocols, and set up data tunnels with the AC.

Figure 2-3 Data flows not transmitted in CAPWAP tunnels



In direct forwarding mode, only control flows are transmitted in CAPWAP tunnels, and data flows sent from APs are transparently transmitted to the upstream device by the AC, as shown in **Figure 2-3**. Data flows are identified by VLAN IDs.

When data flows are not transmitted in CAPWAP tunnels, configure management VLANs and data VLANs as follows:

- On the AC and its upstream devices, configure an AC management VLAN to transmit control flows between the AC and the NMS.
- On the switches between APs and the AC, configure AP management VLANs to transmit control flows between APs and the AC.
- On all switches between APs and the AC, configure data VLANs to differentiate WLAN service flows.

Application

The AC provides powerful access, aggregation, and switching capabilities. In addition, the AC provides PoE or PoE+ power. Therefore, APs can directly connect to the AC. Direct forwarding is often used in inline networking mode. This networking mode simplifies the network architecture and applies to medium- and small-scale and centralized WLANs.

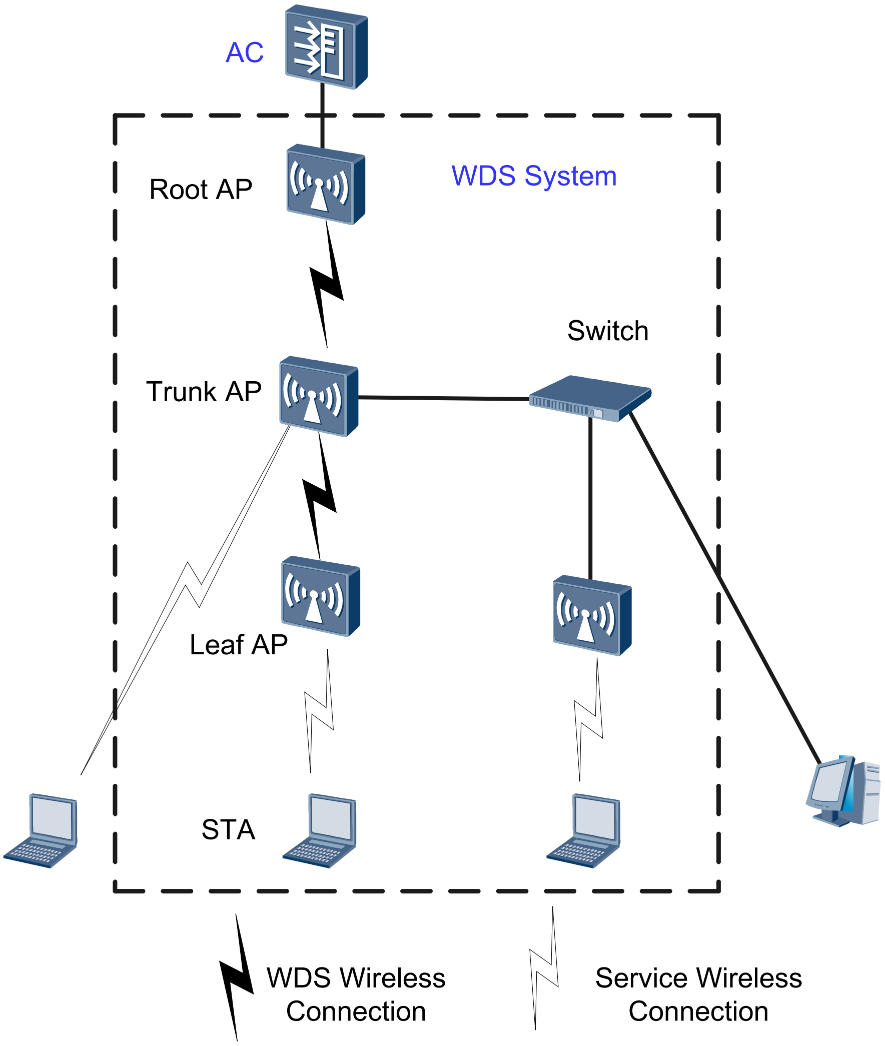
2.3 Wireless Backhaul Networking

The 802.11 wireless technology has been widely used in home networks and enterprise networks. Users can easily access the Internet over WLANs. In this network application, APs must be connected to the existing wired network to provide network access services for wireless users. To expand the wireless coverage area, APs need to be connected using cables, switches, and power supplies. This increases network costs and prolongs network construction period. Wired deployment requirements may not be met in special circumstances. The Wireless Distribution System (WDS) or Wireless Mesh Network allows APs to be connected wirelessly, facilitating WLAN construction in a complex environment.

WDS

The WDS is a distribution system comprised of APs. The WDS connects to an AC on the network side, which is then connected to a network device such as a gateway or an aggregation switch. The WDS connects to a station (STA) or PC on the user side.

Figure 2-4 WDS



On a WDS network, an AC manages the following devices:

- Root AP: connects to an AC on the wired side, and functions as a WDS master to connect to trunk APs or leaf APs.
- Trunk AP: functions as a WDS slave to connect to a root AP, connects to wired devices on the wired side, or functions as a WDS master to connect to leaf APs.
- Leaf AP: functions as a WDS slave to connect to a root AP or trunk AP or connects to STAs on the wireless side.

NOTE

Both root AP and trunk AP can function as leaf APs.

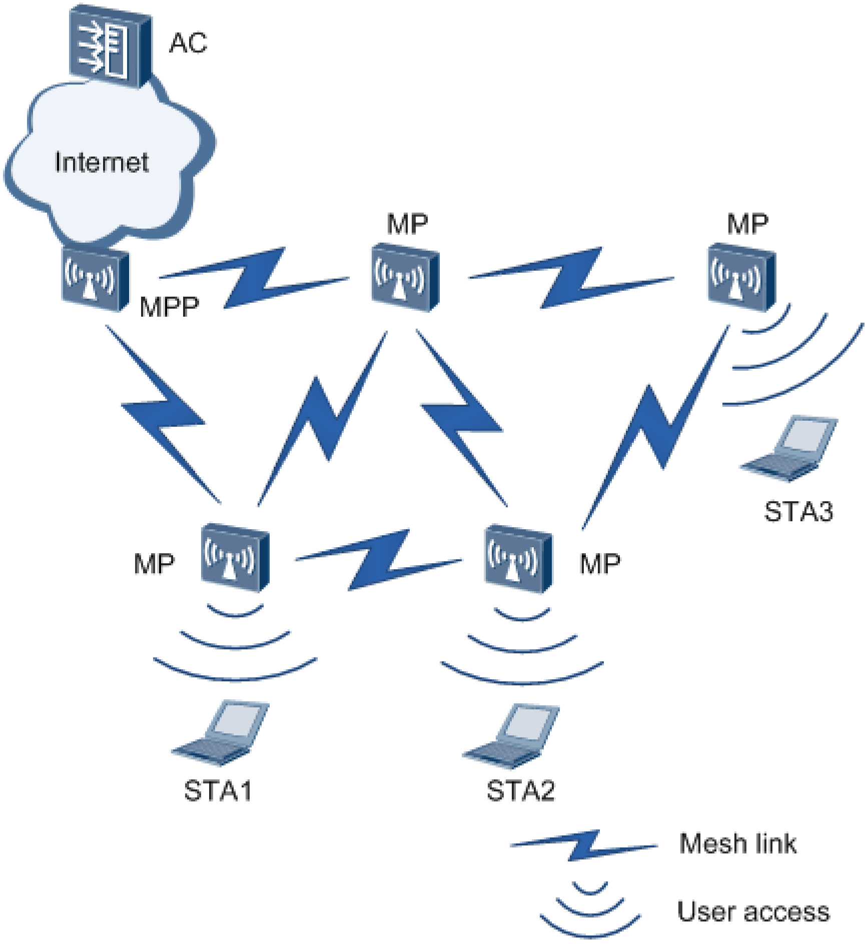
The WDS networking can expand WLANs and applies to indoor wireless deployment scenarios.

Wireless Mesh Network

Compared with a traditional WLAN, a wireless mesh network (WMN) has the following advantages:

- Fast deployment: Mesh nodes can be easily installed to construct a WMN in a short time, much shorter than the construction period of a traditional WLAN.
- Dynamic coverage area expansion: As more mesh nodes are deployed on a WMN, the WMN coverage area can be rapidly expanded.
- Robustness: A WMN is a peer-to-peer network that will not be affected by the failure of a single node. If a node fails, packets are forwarded to the destination node along other paths.
- Flexible networking: An AP can join or leave a WMN easily, allowing for flexible networking.
- Various application scenarios: Besides traditional WLAN scenarios such as enterprise networks, office networks, and campus networks, a WMN also applies to scenarios such as large-scale warehouses, docks, MANs, metro lines, and emergency communications.
- Cost-effectiveness: Only MPPs need to connect to a wired network, which minimizes the dependency of a WMN on wired devices and saves costs in wired device purchasing and cable deployment.

Figure 2-5 Wireless mesh network



Nodes on a WMN can be classified into the following types based on their functions:

- Mesh point (MP)

  A mesh-capable node that uses IEEE 802.11 MAC and physical layer protocols for wireless communication. This node supports automatic topology discovery, automatic route discovery, and data packet forwarding.

- Mesh 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, MPs are fully meshed to establish an auto-configured, and self-healing backbone WMN, and MPPs with the gateway function provide connections to the Internet. An MP provides access services and connects a terminal to a WMN. A WMN uses special mesh routing protocols, which ensures high transmission quality. The WMN is applicable to scenarios that require high-bandwidth and highly-stable Internet connections.

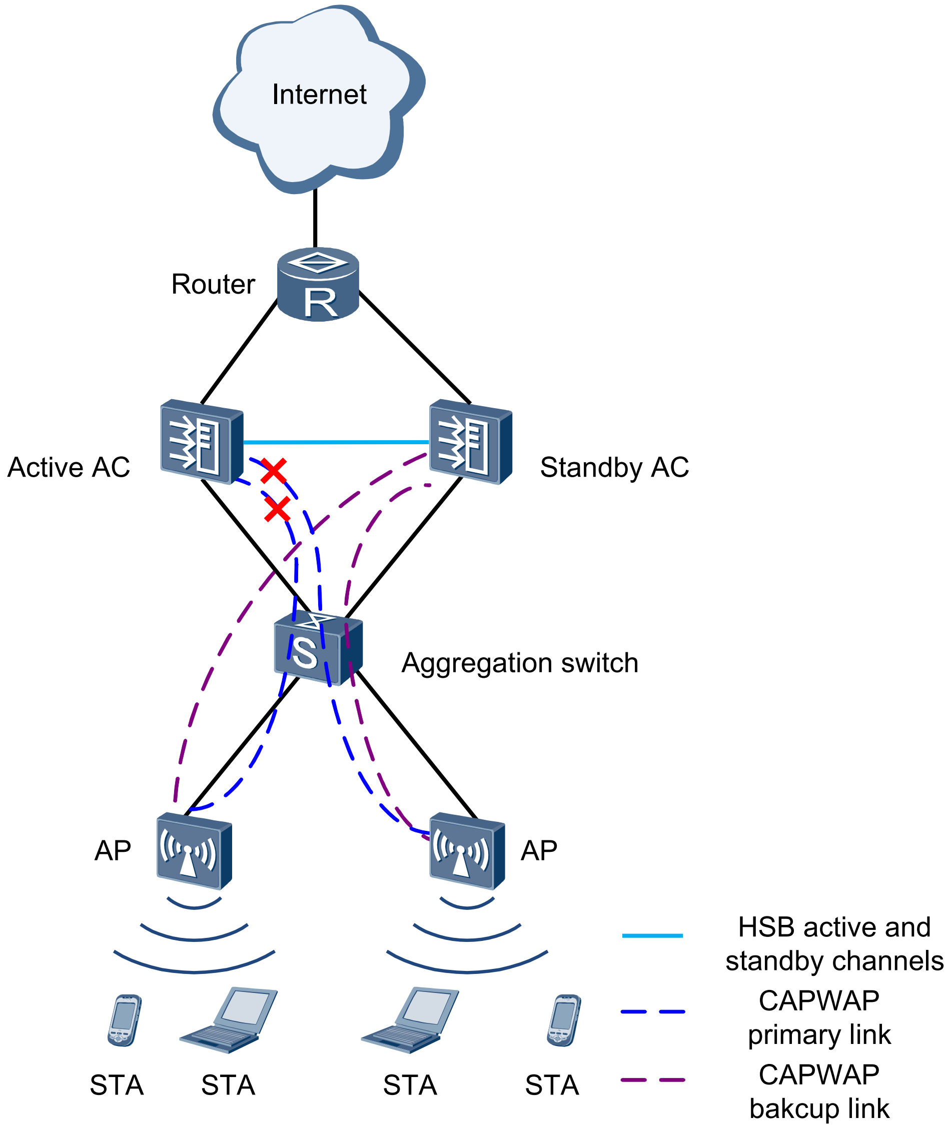
2.4 Dual-AC Networking

To ensure uninterrupted service forwarding, enterprises that require high reliability use active and standby ACs for networking.

Dual-AC backup can be implemented in two modes:

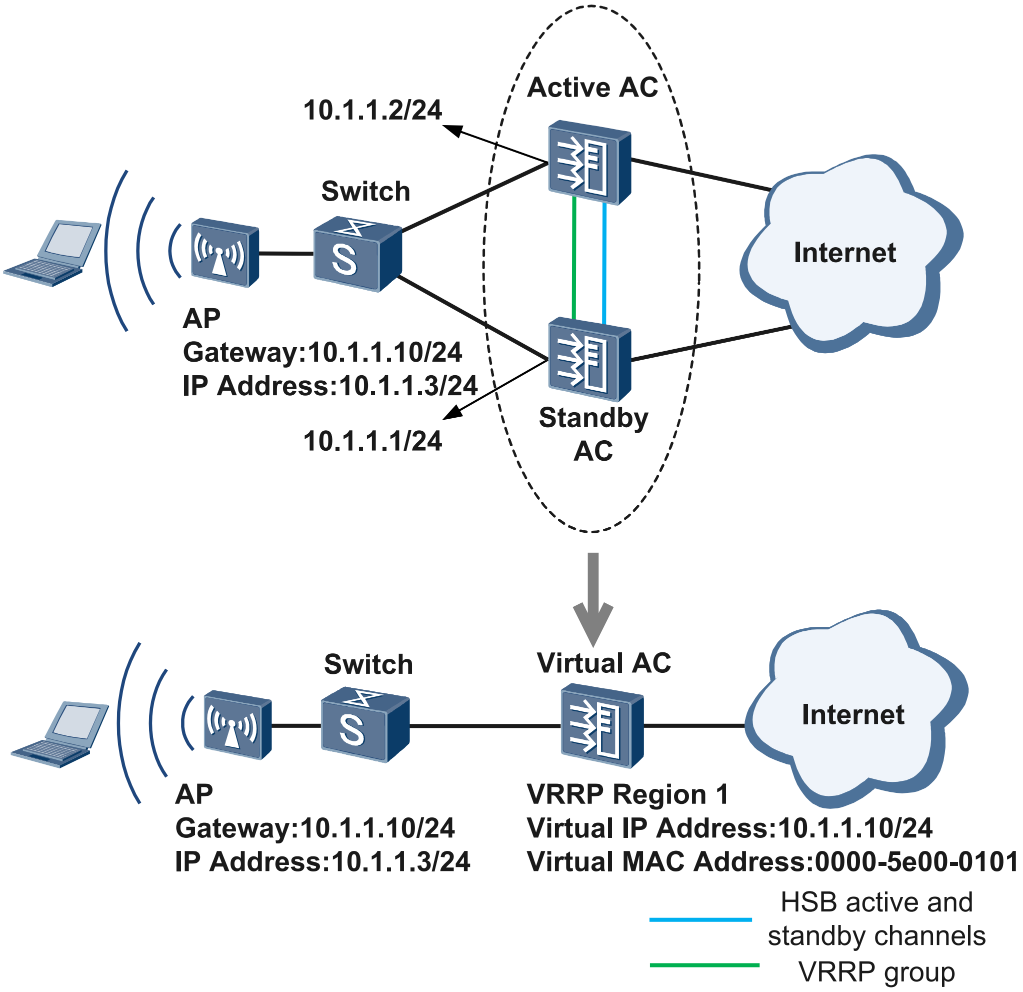
- HSB + dual-link backup: as shown in **Figure 2-6**, an AP establishes CAPWAP tunnels with both the active and standby ACs. The two ACs synchronize service information (such as NAC and WLAN service information) through the hot standby (HSB) function. When an AP is disconnected from the active AC, the AP notifies the standby AC of a switchover.

Figure 2-6 HSB + dual-link backup networking



- HSB + VRRP: as shown in **Figure 2-7**, an AP obtains only the virtual IP address of both the active and standby ACs. The active AC backs up information including AP entries, CAPWAP link information, and user information on the standby AC. In this mode, the AP only detects the presence of one AC. The active/standby switchover is determined by the Virtual Router Redundancy Protocol (VRRP). Currently, this mode cannot be used in a VRRP multi-instance scenario.

Figure 2-7 HSB + VRRP networking



3 Product Structure

About This Chapter

3.1 Device Structure

This section describes the appearance and structure of the AC6605.

Currently, AC6605 only has one model AC6605-26-PWR (AC6605 for short).

Figure 3-1 and **Figure 3-2** show the appearance of the AC6605.

Figure 3-1 Appearance of the AC6605 (front view)

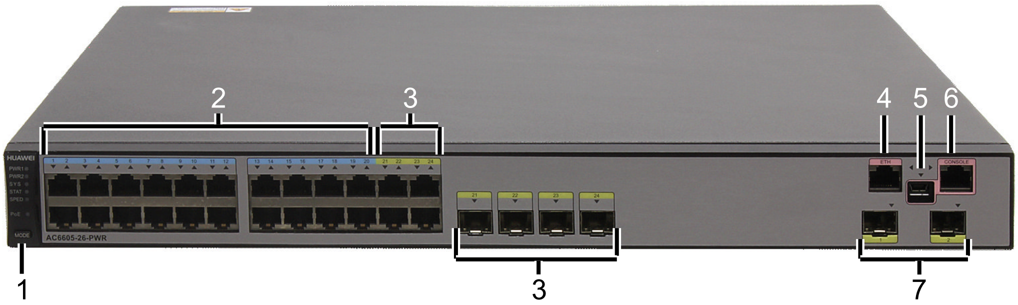
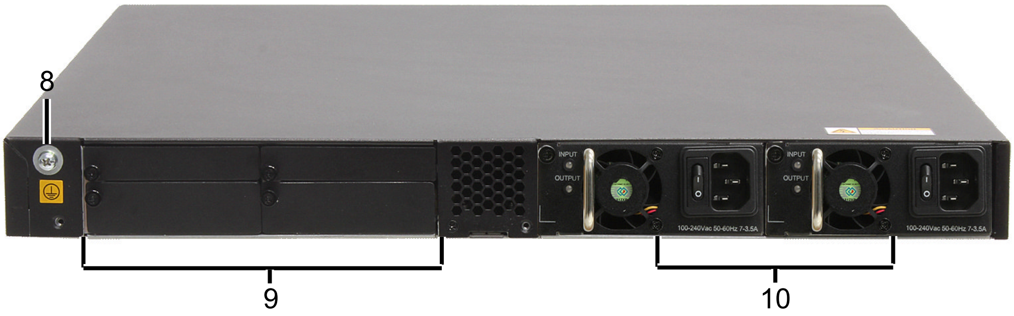


Figure 3-2 Appearance of the AC6605 (rear view)



1. MODE button, switches working mode of indicators.	2. 20 10/100/1000BASE-T Ethernet electrical ports ● Support 10M/100M/1000M auto-sensing. ● Support PoE power supply on 20 ports.	3. Four combo ports
4. One ETH management port	5. One Mini USB port	6. One Console port
7. Two 10GE SFP+ uplink optical ports	8. Ground point	9. Filler panel

10. Two slots for the power supplies The AC6605 supports three types of power supplies: ● 150 W DC Power Supply ● 150 W AC Power Supply ● 500 W AC PoE Power Supply		

3.2 Indicator Description

This section describes the indicators on the AC6605 front panel.

Figure 3-3 shows the indicators on the AC6605 front panel.

Figure 3-3 Indicators on the AC6605 front panel

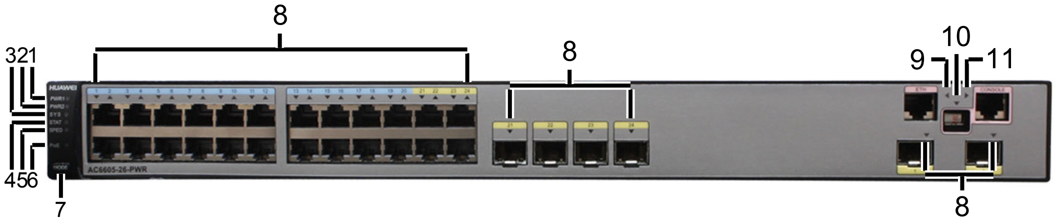


Table 3-1 describes the meanings of indicators on AC6605 front panel.

Table 3-1 Description of indicators on AC6605 front panel

Number	Indicator	Silkscreen	Description
1	On the rear panel: power supply indicator on the right	PWR1	Steady green: The power supply is running properly.
			Steady orange: When the device has two power supplies installed, the power supply in this slot is switched off, is not connected to a power source, or is faulty.
			Off: This slot has no power supply installed or the power supply in the slot is not working properly when only one power supply is installed.
2	On the rear panel: power supply indicator on the left	PWR2	Steady green: The power supply is running properly.

Number	Indicator	Silkscreen	Description
			Steady orange: When the device has two power supplies installed, the power supply in this slot is switched off, is not connected to a power source, or is faulty.
			Off: This slot has no power supply installed or the power supply in the slot is not working properly when only one power supply is installed.
3	System status indicator	SYS	Blinks green once every 2s (0.5 Hz): The system is running properly.
			Blinks green once every 0.25s (4 Hz): The system is being started.
			Steady orange: The temperature or functions of the device become abnormal.
			Blinks orange once every 2s (0.5 Hz): The device has entered the dormancy mode.
			Steady red: After the device is registered, the system does not operate properly, or a power alarm, fan alarm, or temperature alarm is generated.
			Off: The system is not working.
4	State status indicator	STAT	Steady green: The service interface indicator is in the default mode. In this mode, the indicator indicates the state of each interface.
			Off: The indicator is not in the State mode.
5	Speed status indicator	SPED	Steady green: The service interface indicator indicates the speed of each interface. After 45 seconds, the service interface indicator automatically restores to the default mode (STAT).
			Off: The indicator is not in the Speed mode.
6	PoE status indicator	PoE	Steady green: The service interface indicator indicates the PoE status of each interface. After 45 seconds, the service interface indicator automatically restores to the default mode (STAT).
			Steady orange: At least one interface does not support PoE power or has a PoE error when mode switching is not performed.
			Off: The indicator is not in the PoE mode.

Number	Indicator	Silkscreen	Description
7	Mode switch button	MODE	● When you press the button once, the SPED indicator turns green and the service interface indicators show the speed of the interfaces. ● When you press the button for a second time, the PoE indicator turns green and the service interface indicators show the PoE status of the interfaces. ● When you press the button for a third time, the STAT indicator turns green. If you do not press the button within 45 seconds, the indicators restore to the default status. That is, the STAT indicator turns green, and the SPED and PoE indicators are off.
8	Service interface indicator	● 24 GE electrical interfaces: numbered in the up-bottom and left-right orders and begins with 1. ● GE optical interfaces: Each optical interface has a corresponding indicator above it.	Meanings of service interface indicators vary according to the indicator status. For details, see **Table 3-2**.
9	ETH interface indicator	The ETH interface has an arrow above it	Steady green: A link has been established to the interface. Blinks green: The interface is sending or receiving data. Off: No link has been established to the interface.

Number	Indicator	Silkscreen	Description
10	Mini USB interface indicator		Steady green: The Mini USB interface is in use. Off: The Mini USB interface is not in use.
11	Console interface indicator		Steady green: The Mini USB interface is not in use. Off: The Mini USB interface is in use.

Table 3-2 Description of service interface indicators in different modes

Mode	Description
STAT mode	Steady green: A link has been established to the interface.
	Blinks green: The interface is sending or receiving data.
	Off: No link has been established to the interface or the interface has been shut down.
SPED mode	Steady green: ● 10M/100M/1000M interface: The interface is operating at 10/100 Mbit/s. ● 1000M/10G interface: The interface is operating at 1000 Mbit/s.
	Blinks green: ● 10M/100M/1000M interface: The interface is operating at 1000 Mbit/s. ● 1000M/10G interface: The interface is operating at 10 Gbit/s.
	Off: No link has been established to the interface or the interface has been shut down.
PoE mode	Steady green: The interface is providing PoE power.
	The interface cannot provide PoE power due to any of the following reasons: The power of the PD exceeds the power supply capability of the interface or exceeds the threshold. The overall output power has reached the maximum output capability of the device. The PoE power function is not enabled on the interface in manual power-management mode.
	Blinks orange: The interface stops providing PoE power to a PD because a fault occurs (for example, an incompatible PD is connected to the interface).
	Steady orange: The PoE function is disabled on the interface.
	Off: The interface is not providing PoE power to any PD.

4 Features

About This Chapter

4.1 Feature List

Table 4-1 Switching and forwarding features

Feature		Description
Ethernet features	Ethernet	● Operating modes of full duplex, half duplex, and auto-negotiation ● Rates of an Ethernet interface: 10 Mbit/s, 100 Mbit/s, 1000 Mbit/s, and auto-negotiation ● Flow control on interfaces ● Jumbo frames ● Link aggregation ● Load balancing among links of a trunk ● Interface isolation and forwarding restriction ● Broadcast storm suppression
	VLAN	● Access modes of access, trunk, and hybrid ● Default VLAN
	MAC	● Automatic learning and aging of MAC addresses ● Static, dynamic, and blackhole MAC address entries ● Packet filtering based on source MAC addresses ● Interface-based MAC learning limiting
	ARP	● Static and dynamic ARP entries ● ARP in a VLAN ● Aging of ARP entries
	LLDP	● LLDP

Feature		Description
Ethernet loop protection	MSTP	● STP ● RSTP ● MSTP ● BPDU protection, root protection, and loop protection ● Partitioned STP
IPv4 forwarding	IPv4 features	● ARP and RARP ● ARP proxy ● Auto-detection
	Unicast routing features	● Static route ● RIP-1 and RIP-2 ● OSPF ● BGP ● IS-IS ● Routing policies and policy-based routing ● URPF check ● DHCP client, server and relay ● DHCP snooping
	Multicast routing features	● IGMPv1, IGMPv2, and IGMPv3 ● PIM-SM ● Multicast routing policies ● RPF
Device reliability	BFD	● BFD
Layer 2 multicast features	Layer 2 multicast	● IGMP snooping ● Prompt leave ● Multicast traffic control ● Inter-VLAN multicast replication
Ethernet OAM	EFM OAM	● Neighbor discovery ● Link monitoring ● Fault notification ● Remote loopback

Feature		Description
QoS features	Traffic classification	● Traffic classification based on the combination of the L2 protocol header, IP 5-tuple, and 802.1p priority
	Action	● Access control after traffic classification ● Traffic policing based on traffic classification ● Re-marking packets based on traffic classifiers ● Class-based packet queuing ● Associating traffic classifiers with traffic behaviors
	Queue scheduling	● PQ scheduling ● DRR scheduling ● PQ+DRR scheduling ● WRR scheduling ● PQ+WRR scheduling
	Congestion avoidance	● SRED ● WRED
Configuration and maintenance	Terminal service	● Configurations using command lines ● Error message and help information in English ● Login through console and Telnet terminals ● Send function and data communications between terminal users
	File system	● File systems ● Directory and file management ● File uploading and downloading using FTP and TFTP

Feature		Description
	Debugging and maintenance	● Unified management over logs, alarms, and debugging information ● Electronic labels ● User operation logs ● Detailed debugging information for network fault diagnosis ● Network test tools such as traceroute and ping commands ● Interface mirroring and flow mirroring
	Version upgrade	● Device software loading and online software loading ● BootROM online upgrade ● In-service patching
Security and management	System security	● Different user levels for commands, preventing unauthorized users from accessing device ● SSHv2.0 ● RADIUS and HWTACACS authentication for login users ● ACL filtering ● DHCP packet filtering (with the Option 82 field) ● Defense against control packet attacks ● Defenses against attacks such as source address spoofing, Land, SYN flood (TCP SYN), Smurf, ping flood (ICMP echo), Teardrop, and Ping of Death attacks

Feature		Description
	Network management	● ICMP-based ping and traceroute ● SNMPv1, SNMPv2c, and SNMPv3 ● Standard MIB ● RMON

Table 4-2 Wireless networking capabilities

Feature	Description
Networking between APs and ACs	● APs and ACs can be connected through a Layer 2 or Layer 3 network. ● APs can be directly connected to an AC. ● APs are deployed on a private network, while ACs are deployed on the public network to implement NAT traversal. ● ACs can be used for Layer 2 bridge forwarding or Layer 3 routing.
Forwarding mode	● Direct forwarding (distributed forwarding or local forwarding) ● Tunnel forwarding (centralized forwarding) ● Centralized authentication and distributed forwarding Before users are authenticated, tunnel forwarding is used. After users are authenticated, local forwarding is used.
Wireless networking mode	WDS bridging: ● Point-to-point (P2P) wireless bridging ● Point-to-multipoint (P2MP) wireless bridging ● Automatic topology detection and loop prevention (STP) Wireless mesh network ● Access authentication for mesh devices ● Mesh routing algorithm ● Go-online without configuration

Feature	Description
AC discovery	● An AP can obtain the device's IP address in any of the following ways: – Static configuration – DHCP Option 43 – DHCP Option 15 – DNS ● The AC uses DHCP to allocate IP addresses to APs. ● DHCP relay is supported. ● On a Layer 2 network, APs can discover the AC by sending broadcast CAPWAP packets.
CAPWAP tunnel	● Centralized CAPWAP ● CAPWAP control tunnel and data tunnel (optional) ● CAPWAP tunnel forwarding and direct forwarding in an extended service set (ESS) ● Datagram Transport Layer Security (DTLS) encryption, which is enabled by default for the CAPWAP control tunnel ● Heartbeat detection and tunnel reconnection
Active and standby ACs	● Enables and disables the switchback function. ● Supports load balancing. ● Supports 1+1 hot backup.

Table 4-3 AP management

Feature	Description
AP access control	● Displays MAC addresses or SNs of APs in the whitelist. ● Adds a single AP or multiple APs (by specifying a range of MAC addresses or SNs) to the whitelist. ● Automatically discovering and manually confirming APs. ● Automatically discovering APs without manually confirming them.

Feature	Description
AP region management	● Supports three AP region deployment modes: – Distributed deployment: APs are deployed independently. An AP is equivalent to a region and does not interfere with other APs. APs work at the maximum power and do not perform radio calibration. – Common deployment: APs are loosely deployed. The transmit power of each radio is less than 50% of the maximum transmit power. – Centralized deployment: APs are densely deployed. The transmit power of each radio is less than 25% of the maximum transmit power. ● Specifies the default region to which automatically discovered APs are added.
AP profile management	● Specifies the default AP profile that is applied to automatically discovered APs.
AP type management	● Manages AP attributes including the number of interfaces, AP types, number of radios, radio types, maximum number of virtual access points (VAPs), maximum number of associated users, and radio gain (for APs deployed indoors). ● Provides default AP types. ● Supports user-defined AP types.
Network topology management	Supports LLDP topology detection.

Table 4-4 Radio management

Feature	Description
Radio profile management	● The following parameters can be configured in a radio profile: – Radio working mode and rate – Automatic or manual channel and power adjustment mode – Radio calibration interval ● The radio type can be set to 802.11n, 802.11b/g/n, or 802.11a/n. ● You can bind a radio to a specified radio profile.
Unified static configuration of parameters	Radio parameters such as the channel and power of each radio are configured on the AC and then delivered to APs.
Dynamic management	● APs can automatically select working channels and power when they go online. ● In an AP region, APs automatically adjust working channels and power in the event of signal interference: – Partial calibration: The optimal working channel and power of a specified AP can be adjusted. – Global calibration: The optimal working channels and power of all the APs in a specified region can be adjusted. ● When an AP is removed or goes offline, the AC increases the power of neighboring APs to compensate for the coverage hole. ● Automatic selection and calibration of radio parameters in AP regions are supported.
Enhanced service capabilities	● The AC supports 802.1a/b/g/n. These modes can be used independently or jointly (a\n, b\g, b\g\n, and g\n). That is, a total of eight modes can be used. ● The AC preferentially uses the 5 GHz frequency band for STAs.

Table 4-5 WLAN service management

Feature	Description
ESS management	● Allows you to enable SSID broadcast, set the maximum number of access users, and set the association aging time in an ESS. ● Isolates APs at Layer 2 in an ESS. ● Maps an ESS to a service VLAN. ● Associates an ESS with a security profile or a QoS profile. ● Enables IGMP for APs in an ESS.
VAP-based service management	● Adds multiple VAPs at a time by binding radios to ESSs. ● Displays information about a single VAP, VAPs with a specified ESS, or all VAPs. ● Supports configuration of offline APs. ● Creates VAPs according to batch delivered service provisioning rules in automatic AP discovery mode.
Service provisioning management	● Supports service provisioning rules configured for a specified radio of a specified AP type. ● Adds automatically discovered APs to the default AP region. The default AP region is configurable. ● Applies a service provisioning rule to a region to enable APs in the region to go online.
Multicast service management	● Supports IGMP snooping. ● Supports IGMP proxy.
Load balancing	● Performs load balancing among radios in a load balancing group. ● Supports two load balancing modes: – Based on the number of STAs connected to each radio – Based on the traffic volume on each radio

Feature	Description
BYOD (Bring Your Own Device)	● Identification of device types according to the OUI in the MAC address ● Identification of device types according to the user agent (UA) field in an HTTP packet ● Identification of device types according to DHCP Option information ● Carrying of device type information in RADIUS authentication and accounting packets
Positioning services	● Locating AeroScout and Ekahau tags ● Locating Wi-Fi terminals
Spectrum analysis	● Identification of the following interference sources: bluetooth, microwave ovens, cordless phones, ZigBee, game controller, 2.4 GHz/5 GHz wireless audio and video devices, and baby monitors. ● Working with the eSight to locate the interference sources and display spectrum.

Table 4-6 WLAN user management

Feature	Description
Address allocation of wireless users	Functions as a DHCP server to assign IP addresses to wireless users.

Feature	Description
WLAN user management	● Supports user blacklist and whitelist. ● Controls the number of access users: – Based on APs – Based on SSIDs ● Logs out users in any of the following ways: – Using RADIUS DM messages – Using commands ● Supports various methods to view information: – Allows you to view the user status by specifying the user MAC address, AP ID, radio ID, or WLAN ID. – Displays the number of online users in an ESS, AP, or radio. – Collects packet statistics on air interface based on user.
WLAN user roaming	● Supports intra-AC Layer 2 roaming. **NOTE** Users can roam between APs connected to different physical ports on an AC. ● Supports inter-VLAN Layer 3 roaming on an AC. ● Supports fast key negotiation in 802.1x authentication. ● Authenticates users who request to reassociate with the AC and rejects the requests of unauthorized users. ● Delays clearing user information after a user goes offline so that the user can rapidly go online again.
User group management	● Supports ACLs. ● Supports user isolation: – Inter-group isolation – Intra-group isolation

Table 4-7 WLAN security

Feature	Description
WLAN security profile management	● Manages authentication and encryption modes using WLAN security profiles. ● Binds security profiles to ESS profiles.
Authentication modes	● Open system authentication with no encryption ● WEP authentication/encryption ● WPA/WPA2 authentication and encryption: – WPA/WPA2-PSK+TKIP – WPA/WPA2-PSK+CCMP – WPA/WPA2-802.1x+TKIP – WPA/WPA2-802.1x+CCMP ● WAPI authentication and encryption: – Supports centralized WAPI authentication. – Supports three-certificate WAPI authentication, which is compatible with traditional two-certificate authentication. – Issues a certificate file together with a private key. ● Allows users to use MAC addresses as accounts for authentication by the RADIUS server. ● Portal authentication: – Allows an AC to function as a portal gateway. – Prohibits an AC from functioning as a portal gateway. – Supports only Layer 2 portal.
Combined authentication	● Combined MAC authentication: – PSK+MAC authentication ● MAC+portal authentication: – MAC authentication is used first. When MAC authentication fails, portal authentication is used. – This type of authentication applies only to centralized forwarding.

Feature	Description
AAA	● Local authentication/local accounts (MAC addresses and accounts) ● RADIUS authentication ● Multiple authentication servers: – Supports backup authentication servers. – Specifies authentication servers based on account. – Configures authentication servers based on account. – Binds user accounts to SSIDs.
Security isolation	● Port-based isolation ● User group-based isolation
WIDS	Rouge device scan, identification, defense, and countermeasures, which includes dynamic blacklist configuration and detection of rogue APs, STAs, and network attacks.
Authority control	ACL limit based on the following: ● Port ● User group ● User
Other security features	● SSID hiding ● IP source guard: – Configures IP and MAC binding entries statically. – Generates IP and MAC binding entries dynamically.

Table 4-8 WLAN QoS

Feature	Description
WMM profile management	● Enables or disables Wi-Fi Multimedia (WMM). ● Allows a WMM profile to be applied to radios of multiple APs.

Feature	Description
Traffic profile management	● Manages traffic from APs and maps packet priorities according to traffic profiles. ● Applies a QoS policy to each ESS by binding a traffic profile to each ESS.
AC traffic control	● Manages QoS profiles. ● Uses ACLs to perform traffic classification. ● Limits incoming and outgoing traffic rates for each user based on inbound and outbound CAR parameters. ● Limits the traffic rate based on ESSs or VAPs.
AP traffic control	● Controls traffic of multiple users and allows users to share bandwidth. ● Limits the rate of a specified VAP.
Packet priority configuration	● Sets the QoS priority (IP precedence or DSCP priority) for CAPWAP control channels. ● Sets the QoS priority for CAPWAP data channels: – Allows you to specify the CAPWAP header priority. – Maps 802.1p priorities of user packets to ToS priorities of tunnel packets.

4.2 Key Features

WLAN is widely used in public areas such as on campuses, business centers, and airports. The WLAN uses cables at the backbone layer, and users access the WLAN through one or more wireless access points (WAPs) using radio waves. The transmission distance of a WAP is tens of meters.

IEEE 802.11 is widely used by WLANs and provides the following features:

- WLAN services
  - BSS
  - ESS
  - WDS
  - MESH
  - BYOD
  - Positioning services

  - Spectrum analysis
- WLAN user management
  - Dot1X access authentication
  - MAC address authentication
  - Pre-share-key (PSK) authentication
  - EAPOL-Key negotiation
  - User access control
  - AAA for WLAN users
- Radio frequency (RF) management
  - Country code
  - RF type
  - Setting radio transmission rate
  - Setting radio transmission power
  - Setting radio working channels
  - Monitoring and eliminating radio interference
  - Configurable wireless MAC layer parameters
  - Configuring and querying radio attributes
  - Collecting and querying performance statistics of radio frequency interfaces
- WLAN security
  - WEP Open-System link authentication and encryption
  - WEP Share-Key link authentication and encryption
  - WPA PSK authentication and encryption
  - WPA Dot1X authentication and encryption
  - WPA2 PSK authentication and encryption
  - WPA2 Dot1X authentication and encryption
  - WAPI authentication and encryption
  - TKIP/CCMP encryption
  - HMAC-MD5 algorithm
  - User blacklist and whitelist
  - WIDS/WIPS
- WLAN QoS
  - WMM (802.11e)
  - Mapping wireless-side priority to the wired-side priority
  - Bandwidth limit based on users
  - Bandwidth limit based on SSIDs
- Network reliability
  - 1+1 redundancy backup

5 Operation and Maintenance

About This Chapter

5.1 Maintenance and Management

The AC provides the following management modes.

- CLI-based management: You can use the console interface for local configurations or log in to the AC using telnet or SSH.
- GUI-based web system management: The web system supports local GUI-based configurations.
- SNMP-based NMS management: The NMS allows you to configure the AC based on the Simple Network Management Protocol (SNMP).

5.1.1 Robust Hardware Management, Rapid Fault Location and Rectification

The AC provides the following hardware monitoring functions:

- Provides the re-detection function to prevent incorrect detection because of instant interference.
- Checks version matching automatically when the system is running.

5.1.2 Advanced Software Management, Facilitating Smooth Upgrade and Capacity Expansion

The AC can detect the integrity and validity of the system software before the upgrade and provides various methods of upgrading the software:

- In-service upgrade

  The AC supports in-service software upgrade and patching. You can upgrade the features that need to be modified.
- System upgrade

  The entire upgrade process can be completed using only one command, saving upgrade time. The upgrade progress is displayed during an upgrade, and the upgrade result will be displayed after the upgrade process is complete.
- Rollback function

  If the new system software cannot start the system during a system upgrade, the old system software can be used instead.
- In-Service Patching

  The AC supports in-service patching to protect services from being affected when a patch is installed. The software can be restored to the earlier version, and the device data before and after in-service patching is recorded.

5.1.3 Rich Tracing and Monitoring Functions, Helping Customers Learn Real-time Network Status

Ping and TraceRoute

On traditional IP networks, the AC provides the following tools to check network connectivity:

- Ping
- TraceRoute

These tools are used to test network connectivity and record transmission paths of packets to assist fault location.

Black Box

The AC provides the black box function to record information on the feature modules, tasks, and events. In addition, the black box records the process status and function calling track to facilitate fault location.

Mirroring

The AC supports interface-based or flow-based mirroring.

- Port mirroring

  The incoming traffic, outgoing traffic, or both incoming and outgoing traffic at an observed interface is completely copied to an observing interface.
- Flow mirroring

  The traffic at an observed interface is completely copied to an observing interface.

By connecting a monitoring host to an observing interface on the AC, a network administrator can easily observe the packets that pass through the AC in real time. The mirroring result serves as a basis for traffic detection, fault location, and data analysis.

5.2 Network Management System (NMS)

The AC supports the eSight as the unified NMS on enterprise networks.

The eSight provides basic network management, NE management, service management, and system management.

6 Technical Specifications

About This Chapter

6.1 Physical Specifications

This section describes the physical specifications of the AC6605.

Table 6-1 Physical specifications

Item		Description
Dimensions (width x depth x height)		442 mm x 420 mm x 44.4 mm
Maximum power consumption		85 W
Weight		Net weight: 5.48 kg Fully configured with 150 W power supplies: 7.16 kg Fully configured with 500 W power supplies: 7.48 kg
Operating temperature		-5ºC to +50ºC
Relative humidity		5% RH to 95% RH, noncondensing
Operating altitude		150 W DC power supply: 0 m to 2000 m Others: 0 m to 3000 m
AC input voltage	Rated voltage	100 V AC to 240 V AC, 50/60 Hz
	Voltage range	90 V AC to 264 V AC, 47/63 Hz
DC input voltage	Rated voltage	-48 V DC to -60 V DC
	Voltage range	-36 V DC to -72 V DC

6.2 System Configuration

Table 6-2 describes system configurations of the AC6605.

Table 6-2 System configuration of AC6605

Item	Specifications
Processor	Dominant frequency: 1 GHz
Switching capacity	128 Gbit/s
Packet forwarding capacity	10 Gbit/s
DDR memory	4 GB
Flash memory	256 MB

6.3 Performance Specifications

Table 6-3 shows the performance specifications of the AC6605.

Table 6-3 Perform specifications of AC6605

Parameter	Specifications
Number of managed APs	512
Number of access users	● Entire device: 10K ● Single AP: a maximum of 256 (depending on the AP model)
Number of MAC address entries	16K
Number of VLANs	4K
Number of routing entries	10K
Number of ARP entries	8K
Number of multicast forwarding entries	4K
Number of DHCP IP address pools	128 IP address pools, each of which contains a maximum of 16K IP addresses
Number of local users	1000
Number of ACLs	8K
Number of ESSIDs	4K
User group management	● 128 user groups ● Each user group can reference a maximum of eight ACLs. ● Each user group can associate with a maximum of 128 ACL rules.