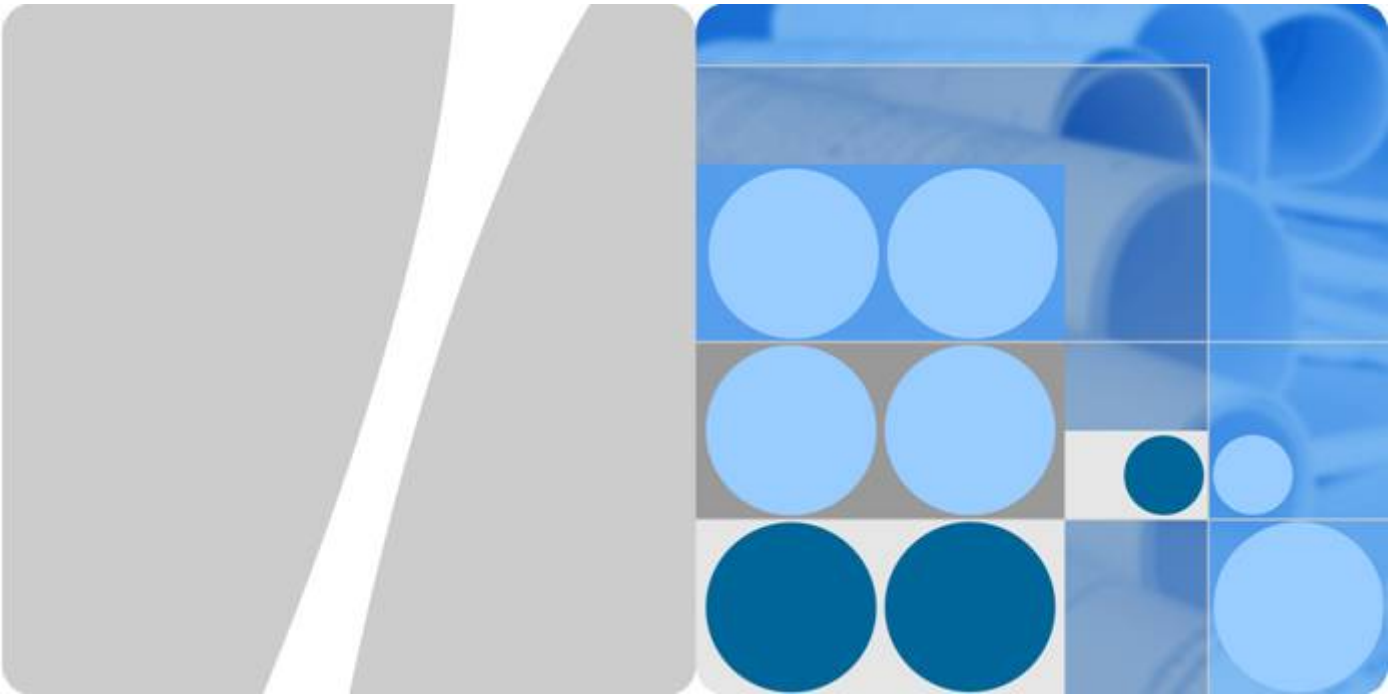


Agile Campus Network Solution

Design Guide and Best Practices

Issue 02

Date 2018-07-25

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://e.huawei.com

Contents

1 About This Document

This document can be used as a reference in the high level design (HLD) and low level design (LLD). It introduces the architecture, design methods, and best practices of Huawei Agile Campus Network Solution. Best practices are based on experiences from delivered projects. By following the best practices in this document, network engineers can improve the project delivery efficiency, simplify network operations and maintenance (O&M), and optimize application performance, allowing networks to run at optimal state. Due to diversity of networks, comprehensive verification is recommended before modifying the network configuration under guidelines of this document.

The document includes the following contents:

- The overview of agile campus network describes the scope, design principles, and design process.
- Network architecture design and best practices: This chapter introduces the network architecture design model and principles, and provides the detailed design instructions and best practices layer by layer.
- Service feature design and best practices: These chapters describe the design guidelines and best practices of various services on agile campus networks from the aspects including reliability, security, and agility.
- Recommended versions and product models: These chapters describe the versions and product models recommended in Huawei Agile Campus Network Solution.
- Product overview: This chapter describes products used in Huawei Agile Campus Network Solution.

This document applies but is not limited to pre-sales engineers, network design engineers, technical support engineers, and users who want to understand the design and deployment of agile campus networks. Before reading this document, you must have basic knowledge of Huawei datacom products. This document is not suitable for beginners.

NOTE

The configurations in this document apply to the following sample versions:

- AC: V200R007C20
- S series switch: V200R010C00
- Firewall: V500R001C30
- Agile Controller-Campus: V100R002C10
- eSight: V300R007C00

2 Overview of Agile Campus Network

A campus network generally refers to the internal network of an enterprise or organization, which is connected to the wide area network (WAN) and data center network. The campus network provides a stable and reliable network environment for continuous operations of enterprise services.

Typically, there are three types of campus networks, namely large, medium-sized, and small, based on the network scale. Sometimes, small campus network and medium-sized campus network are also called small- and medium-sized campus networks. Some enterprises have branches, which are located in different places outside the campus network. From this perspective, a campus network is usually an internal network in a specific geographic area. A campus network is connected to the public network, so it can be considered as a private network of an enterprise or organization.

Mobility, cloud computing, Big Data, the Internet of Things (IoT), and other emerging services are driving enterprises of all sizes to go digital. This trend poses new challenges for enterprise campus networks. Due to complexity and diversity of access scenarios and user roles, it is difficult to guarantee convenient access anytime and anywhere. Separation of service networks intensifies the complexity of O&M and management. Rapid emergence of new services requires campus networks to be more open and flexible. Huawei launches the Agile Campus Network Solution to help enterprise customers to build wireless, intelligent, automated digital campus networks.

Agile Campus Network Solution uses industry-leading S-series campus switches, rich WLAN products, Agile Controller-Campus, security gateway USG series firewalls, and unified network management system eSight. With a series of innovative features, wired and wireless integration and free mobility for policy automation, this solution helps enterprises to build integrated, simple, open, and secure campus networks, allowing networks to be more agile for services.

As a network infrastructure, campus networks provide users with network communication services and resource access rights. Complicated access relationships and diversified service types pose the needs for good design ideas and guidelines. The following design guidelines are available for campus network design:

- **Reliable**: Campus networks must run stably and reliably without service interruption, ensuring service experience. This requires a redundant or backup architecture for key components that can be used to quickly restore faults.

- **Trustworthy**: Campus networks must be secure and trustworthy to guarantee network and service security. This requires comprehensive security protection measures to prevent malicious damages, protecting data and network security.
- **Scalable**: Campus networks must be able to smoothly upgraded and expanded to meet service needs in the next 3 to 5 years, fully create network values, reduce investment, and avoid waste of resources. This requires for on-demand deployment of new services and smooth network expansion.
- **Manageable**: Campus networks must be easy to manage, maintain, and perform network diagnosis and fault locating, reducing the O&M difficulty and improving customer experience. This requires intelligent, active, and integrated management of multiple services over the entire network, real-time network health analysis, active prevention, and quick fault locating to reduce losses.
- **Operational**: Campus networks must support flexible deployment of new services, such as Voice over Internet Protocol (VoIP), Unified Communications (UC), Telepresence, and desktop cloud.
- **Economic**: The return on investment should be maximized and the investment costs should be reduced.

Campus networks are complex and diverse. A small campus network may contain a switch or several APs, while a large campus network may be a distributed network with thousands of devices. Network requirements, such as reliability, security, and ease-of-use, vary with scenarios. Network design is comprised of three stages: 1. Investigation of the customer network environment and service requirements; 2. Requirement analysis based on the investigation results, including the terminal access mode, service traffic model, and network bandwidth; 3. Solution design based on the analysis results, including network architecture design and service feature design

Table 2-1 lists requirement survey and analysis for the campus network design.

Table 2-1 Requirement description

Classification	Objective	Key Points of Requirement Survey	Key Points of Requirement Analysis
Network environment	Finalize the network architecture and design solution.	Network reconstruction or creation	If you are creating a new network, the design constraints are relatively small. If you are upgrading a network, the network design complexity increases, and you need to consider more factors, such as device compatibility and reuse, smooth network transition, and whether service interruption is allowed.
		Network type: wired network, wireless network, or wired and wireless integrated network	Determine whether there is a need to build a wireless network or upgrade the network into a wired and wireless integrated network. If unified authentication is required, the wired and wireless convergence solution is recommended.

Classification	Objective	Key Points of Requirement Survey	Key Points of Requirement Analysis
		Geographical distribution: centralized or dispersed	Finalize the basic network architecture. If the campus network is geographically centralized, consider using the single-core architecture. If the campus network is geographically dispersed, for example, multiple buildings with large network scale have heavy internal traffic between them, consider using multiple core or aggregation points.
		Customer organizational structure	Obtain campus network usage information based on the customer organizational structure, including network usage by organizations, network deployment, whether there is a need to separate networks by department, area, and service, whether there is a need to deploy multiple core or aggregation points, and whether there are branch access requirements (access lines used, if any).
		Distribution of extra-low voltage (ELV) rooms or equipment rooms	If there are many ELV rooms or equipment rooms, deploy an aggregation point in each ELV room or equipment room. If the multi-core interconnection architecture is used, deploy multiple cores in different equipment rooms respectively. In addition, you also need to consider the device layout and distance between the devices.
Network pain points	Determine the features that need to be supported.	(For upgrade or reconstruction) network speed: whether network congestion occurs	Determine network bandwidth and number of devices.
		(For upgrade or reconstruction) network quality: whether services are frequently interrupted or whether the network is stable	Use a network management system or analysis software to identify specific causes of network quality deterioration and take measures accordingly. For example, use products with hardware operation, administration and maintenance (OAM) functions. In addition, analyze the network quality required by services based on the customer's industry characteristics to ensure that the network quality meets service needs.

Classification	Objective	Key Points of Requirement Survey	Key Points of Requirement Analysis
		Network scale: number of accessible users	Understand the number of existing users on the customer network and user growth in the next 3 to 5 years. It is usually possible to increase the number of access switches or to replace existing switches with high-density switches, while taking network capacity into consideration.
		Network capability: whether remote access is required	Determine the remote access mode based on the service application scenarios. The remote access can be SSL VPN for personal access or IPSec VPN for fixed branch access, or both.
Network services	Determine the network bandwidth and service features.	Common services: office, email, and Internet access	Normal office services do not have high network bandwidth requirements.
		Key services: data, VoIP, video, and desktop cloud	Usually, a campus network is a LAN, so you do not need to consider the network delay. If VoIP, video, and desktop cloud services involve branch, metropolitan area network (MAN), or WAN connections, you need to take network delay into consideration. For the VoIP service, consider the following factors: whether a shared or independent network is deployed for PCs; whether PoE power supply is needed; the number and specification of switches. For the desktop cloud service, you need to consider the network reliability or availability. For the video service, you need to take full account of bandwidth requirements.
		VIP services	Design QoS policies to guarantee services of VIP customers, ensuring the customer experience.
		Multicast service	Design the corresponding multicast solution, if needed.
		New services within the next 3 to 5 years	Design a smooth upgrade and capacity expansion solution to meet service development requirements within 3 to 5 years, avoiding waste of resources.

Classification	Objective	Key Points of Requirement Survey	Key Points of Requirement Analysis
		(Optional) Live network services	Obtain the running network protocols, network topology, and device type, and number of devices as well as the live network quality and supported services. The information can be used as a reference during the design.
Service security	Determine service isolation and network security protection solutions.	Service security: service isolation and interoperability	Does the network services need to be isolated? How are services isolated, physically or logically? To isolate network services physically, design independent networks for these services. To isolate network services logically, use technologies such as virtual local area network (VLAN) or Virtual Private Network (VPN) to virtualize one network into multiple campus networks. There is also a need to consider whether interoperability is required between different services. If so, it is necessary to develop interoperability policies and solutions in advance.
		Network security: external security protection	Determine whether there is a need to deploy security devices, such as firewall, intrusion prevention system (IPS), intrusion detection system (IDS), network log audit, and antivirus wall to protect the network edge security. If high network security is required, for example, a specific security level, independent security devices are recommended. Otherwise, integrated security devices such as Unified Threat Management (UTM) or security value-added service cards can be used.
		Network security: internal security protection	The online behavior management software or dedicated device is recommended to prevent security incidents caused by internal users.
		Network security: terminal security protection	Determine whether the Network Admission Control (NAC) solution including terminal security check is required to ensure terminal access security.

Classification	Objective	Key Points of Requirement Survey	Key Points of Requirement Analysis
Network scale	Finalize the network architecture and design solution.	Number of access users or access points	Determine the number of switch ports and the port density and the approximate network bandwidth requirements based on service survey.
		Network scale in 3 to 5 years, or the highest growth rate in recent years	Take capacity expansion and smooth upgrade into consideration when designing the network interfaces, capacity and bandwidth, to meet the service development needs in the next 3 to 5 years. Consider the user scale including both the number of users or number of terminals, as well as the service scale, including the service type, bandwidth, quantity, and scope.
		(Optional) Number of wireless users	Determine the AC specifications and number of APs, and whether there is a need for high-density access in some key areas, such as conference rooms.
		(Optional) Live network information and specifications	Estimate the network reconstruction workload and determine the network upgrade solution, covering device reuse, compatibility, and smooth upgrade.
		(Optional) Branch offices	Consider the mode for interconnection between the headquarters and branches. Does the headquarters need to use leased lines and Internet lines? Does a link need backup?
Terminal type	Determine the network access solution.	Wired terminals: network access capability (interface rate of the NIC)	Determine the approximate specifications of access switches.

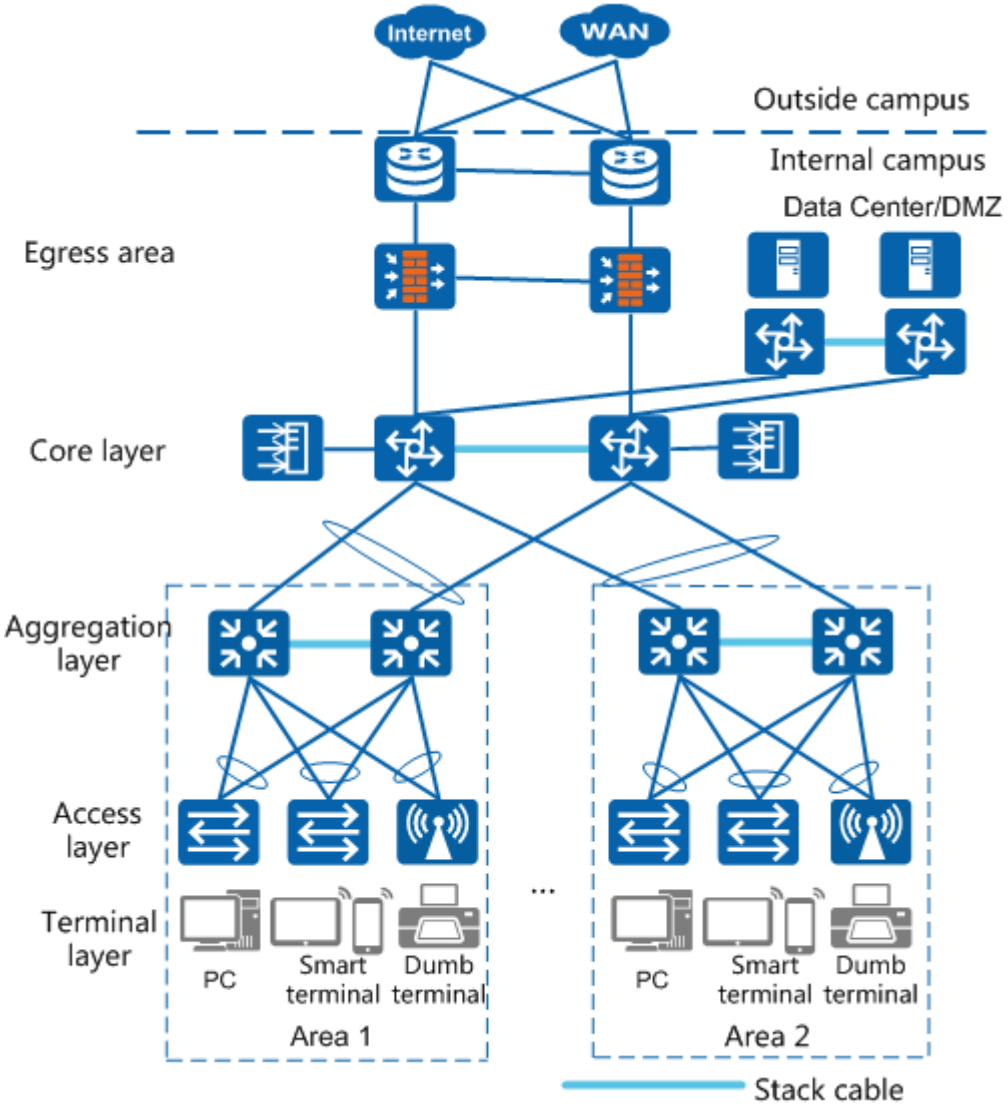
Classification	Objective	Key Points of Requirement Survey	Key Points of Requirement Analysis
		Wireless terminals: ● Terminal type: laptops, smartphones, and mobile smart devices such as tablets ● Wireless access capability: support for 802.11a/b/g/n/ac/ac Wave2 ● AP power supply mode: direct power supply or PoE power supply by switches	Consider the supported access frequency bands and modes. Consider access authentication modes. Consider whether to use unified wired and wireless authentication. Determine whether to allow guest access and access areas if allowed.
		Dumb terminals: IP phones, network printers, and IP cameras	Determine the access and authentication solutions for these dumb terminals.
		Other terminals: industrial control computers and test controllers	Consider model selection of access switches. For example, industrial switches may be required for industrial campuses or production networks. The power supply mode of devices may be affected in outdoor scenarios.
		Special network devices: dedicated network encryption devices and industrial switches	Consider compatibility and performance of these devices to prevent specification mismatch.

3 Network Architecture Design and Best Practices

3.1 Overall Network Architecture Design

Typically, layered and area-based design is performed for campus networks to facilitate network management. An internal network of a campus is composed of the terminal layer, access layer, aggregation layer, core layer, and egress area. Users in another campus or branch and traveling employees access the campus intranet through the Internet or leased lines.

Figure 3-1 Campus network architecture



The functions of each layered module on a network are as follows:

- Terminal layer: This layer contains terminals, such as computers, laptops, printers, fax machines, POS phones, SIP phones, mobile phones, and cameras.
- Access layer: As the edge of a campus network, this layer connects end users to the campus network. The access layer is usually composed of Ethernet switches. For some terminals, a specific access device, such as a wireless access point (AP) is required to connect them to the campus network.
- Aggregation layer: This layer connects a large number of access devices and users to the core layer after aggregation. It extends the number of access users and completes data aggregation or switching. On some campus networks, the Layer 3 gateway is deployed at the aggregation layer to function as a Layer 2 or Layer 3 edge device. The Layer 3 gateway at this layer is responsible for user management, security management, QoS scheduling, and other related services.
- Core layer: This layer is the backbone area of a campus network, which is the data switching core. It connects the various parts of the campus network, such as the data

center, aggregation layer, and egress area. High bandwidth usage and fast convergence of network faults need to be implemented at this layer.

- Egress area: This area is the edge between the campus internal network and the external network. Internal users access the public network through this egress area and external users (including customers, partners, branches, and remote users) access the internal network through this egress area too.
- Data center area: This area has servers and application systems deployed to provide data and application services for internal and external users of the enterprise.
- Demilitarized zone (DMZ): This area has public servers deployed to provide access services to external guests (non-employees). The access permission to this area is strictly controlled.

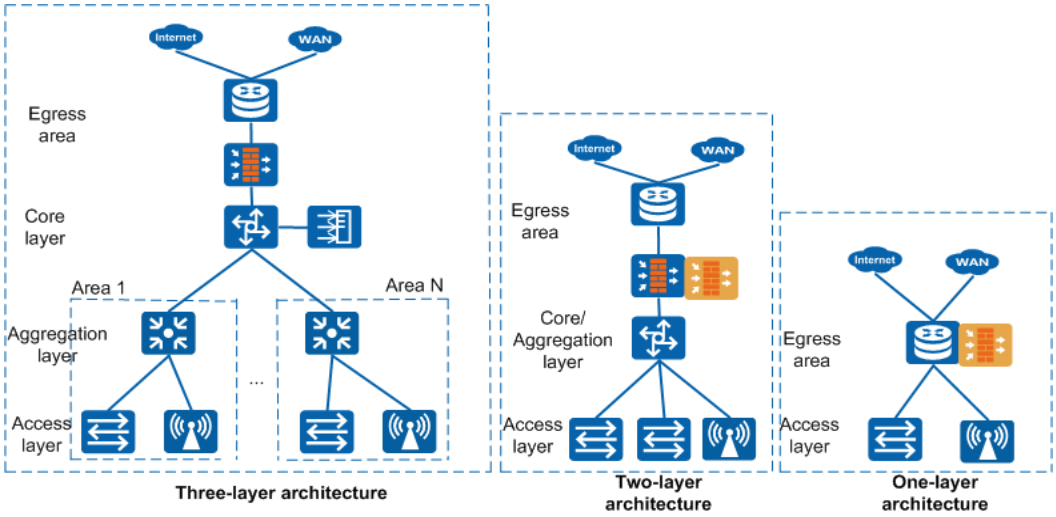
3.2 Design Guidelines

The design of a campus network needs to comply with the following guidelines:

- Layered design: Each layer can be considered as a well-structured module with specific role and function. This layered structure is easy to expand and maintain, reducing the design complexity and difficulty. Theoretically, a layered architecture can have multiple layers, but in most cases, three layers (such as the access layer, aggregation layer, and core layer) are sufficient. This better controls the network size and quality, and facilitates network management and maintenance.
- Modular design: Each module corresponds to a department, function, or service area. Modules can be expanded flexibly based on the network scale, and adjustment in a department or area covers a small scope, which facilitates fault locating.
- Redundancy design: Dual-node redundancy design can ensure device-level reliability. Appropriate redundancy improves reliability, but excessive redundancy makes O&M difficult. If dual-node redundancy cannot be implemented, you may consider card-level redundancy, such as dual main control boards or switch fabric units (SFUs), for modular core switches or egress routers. In addition, Eth-Trunk can be deployed to ensure link-level reliability of important links.
- Symmetry design: The symmetric network structure makes the topology more clear and facilitates service deployment, and protocol design and analysis.

In practical applications, the network architecture can be flexibly divided or adjusted according to the network scale or service needs. Usually, three-layer architecture, two-layer architecture, and one-layer architecture are used. For example, only the access layer and aggregation layer are required for a network for a single building; the access layer, aggregation layer and core layer are required for a network for multiple buildings.

Figure 3-2 Campus network architecture models



There are two criteria for selecting an architecture model:

- Network scale (bottom-up method): the number of access points or users
- Service requirements (top-bottom method): whether service isolation is needed or how services are isolated

In practical applications, these two criteria are generally used at the same time, supplementing each other. If the judgment results of the two criteria are different, the method requiring more layers is used. For example, if the two-layer architecture is proper based on the network scale and the three-layer architecture is proper based on service needs, the three-layer architecture is selected.

The following describes architecture selection from three aspects: number of users, network scale, and service requirements.

Based on the Number of Users

Three-layer and two-layer architectures are most frequently used on networks of large- and medium-sized campuses. The one-layer architecture applies only to mini-sized campuses or branches.

Table 3-1 Architecture model selection based on the number of users

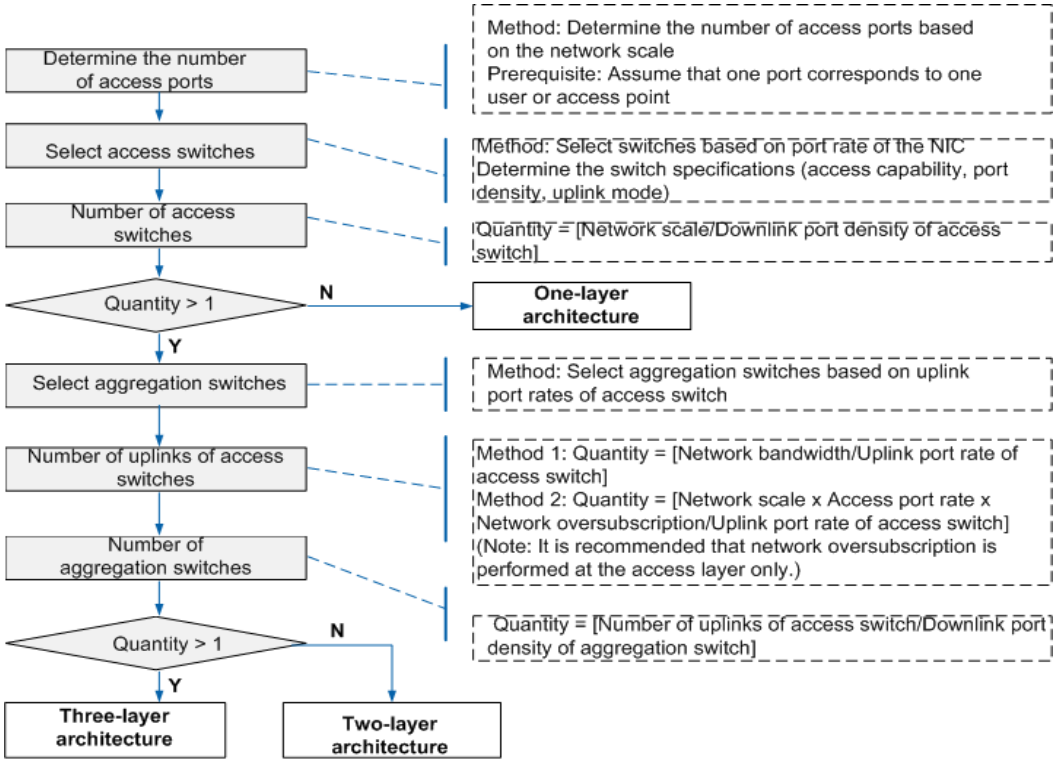
Campus Type	Architecture Type	Description	Application Scenario
Large-sized campus	Three-layer architecture	The number of users, departments, or network areas is large.	Large science and technology campuses or industrial campuses

Campus Type	Architecture Type	Description	Application Scenario
Medium-sized campus	Three-layer or two-layer architecture	The three-layer architecture is used when the user scale is not so large, there are many service departments, and the service control relationship is complex. In other cases, the two-layer architecture is used.	Small- and medium-sized campuses and branches
Small-sized campus	Two-layer or one-layer architecture	The user scale is small.	Mini campuses, SOHO enterprises, and small branches

Based on the Network Scale

Determining layers of the architecture based on the network scale is a bottom-up method.

Figure 3-3 Architecture model selection based on the network scale

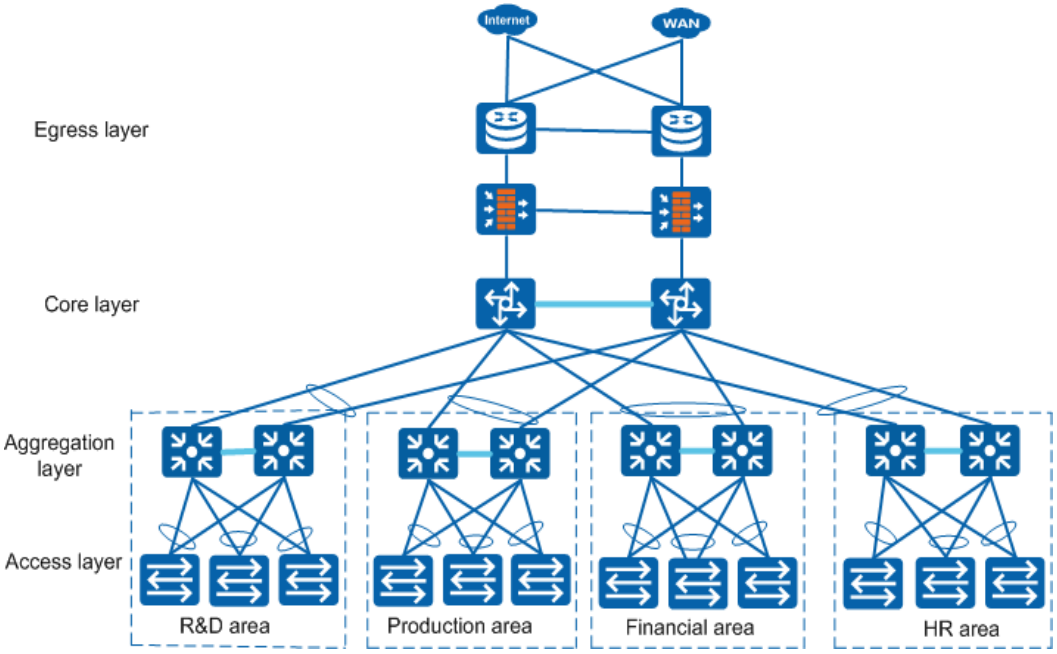


Based on Service Requirements

If a campus network requires service isolation, use the three-layer architecture to realize physical isolation.

For example, a company has R&D, production, financial, HR, and other departments, services of which need to be isolated. Data of each department cannot be directly accessed at Layer 2. It is recommended that an independent aggregation area be deployed for each department to isolate services. Users in the same department can communicate at Layer 2, but users in different departments cannot directly communicate with each other. If there is a need for mutual service access between departments, strict control is required. Access Control Lists (ACLs) can be configured on core switches to implement access control.

Figure 3-4 Architecture model selection based on service requirements



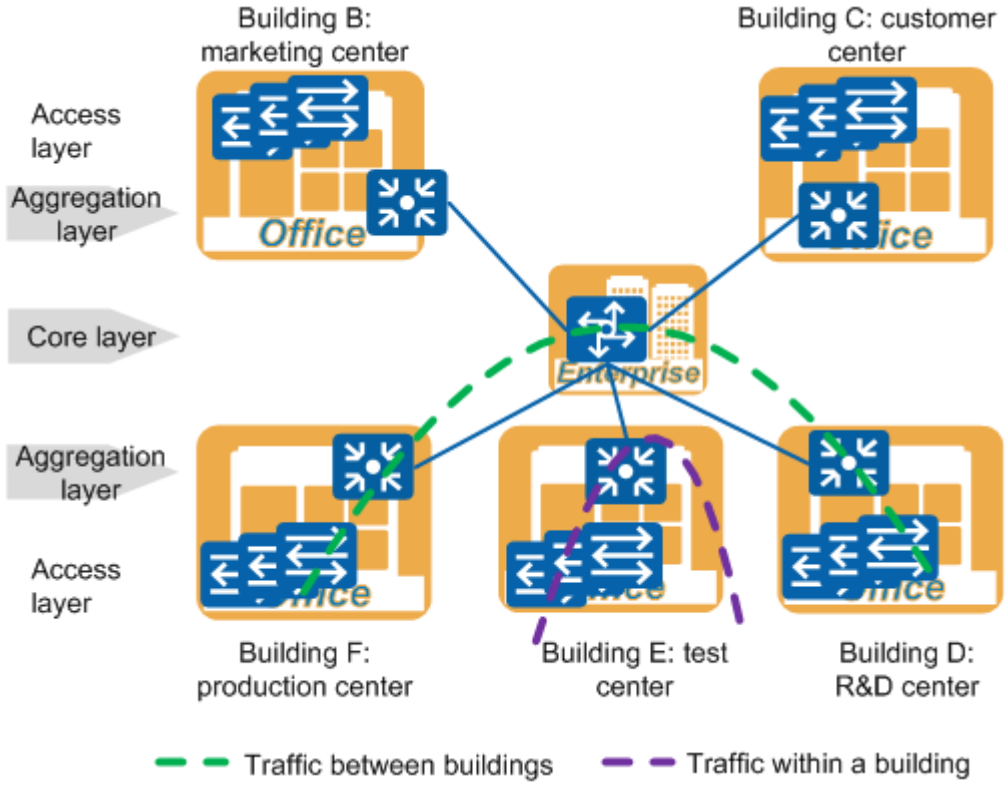
3.3 Best Practices

Network Architecture of a Large-sized Campus

In large campuses, networks are usually deployed by building. The whole campus is deployed with one core layer. Each building is treated as an independent aggregation point and is deployed with networks in a two-layer tree structure.

By using this architecture, data traffic within a building is forwarded locally and data traffic between different buildings is forwarded by the core layer.

Figure 3-5 Tree structure of a large-sized campus network



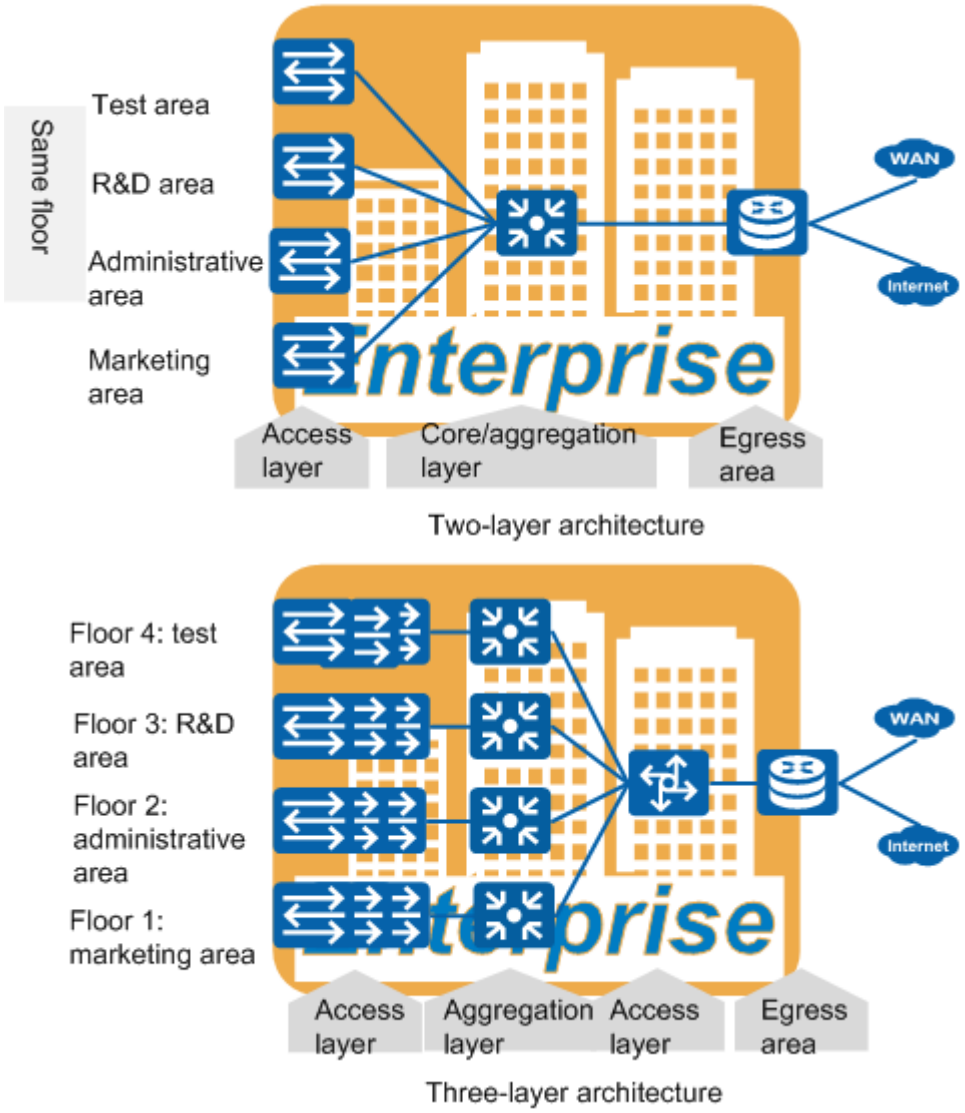
Network Architecture of a Medium-sized Campus

A medium-sized campus usually uses a two-layer structure. A three-layer architecture can also be used, depending on the network scale and service needs.

When there are too many access points requiring multiple aggregation points, three-layer structure is employed. Each floor in a building has an ELV room, which acts as an aggregation point. The whole building uses a three-layer structure and has one core layer.

When different services or departments need to be isolated, an aggregation point needs to be deployed for each service or department. In this case, a three-layer structure is used.

Figure 3-6 Tree structure of a medium-sized campus network

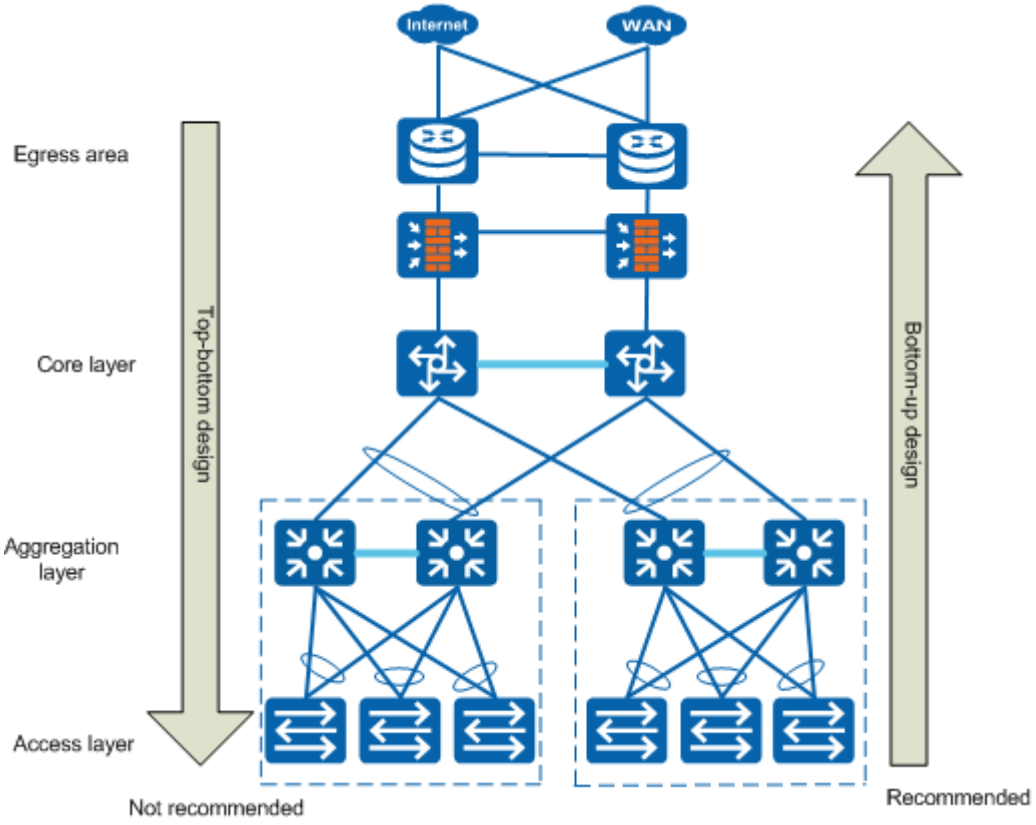


3.4 Layered Design and Best Practices

This chapter describes the detailed design method of each layer, including networking design, link design, device model design, and best practices.

Layered design means to use modular and layer technologies to design each layer, and to plan interconnections between different layers based on the traffic load and user or network behavior analysis.

Layered design includes top-bottom and bottom-up methods. In consideration of engineering implementation, the bottom-up method can better satisfy customer needs, is more applicable, and brings fewer risks. Therefore, it is often recommended. In the bottom-up method, the access layer is designed first, then the aggregation layer, and finally the core layer and egress area.



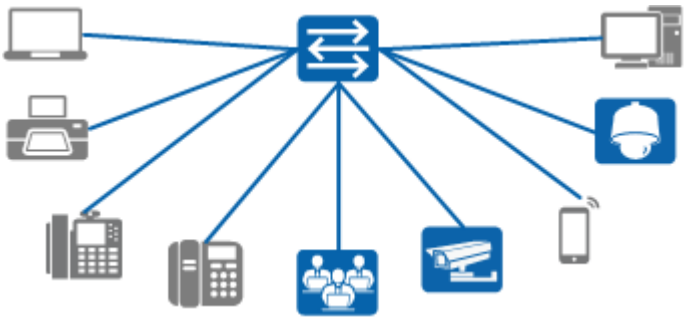
Layered design does not mean that each layer is designed in total isolation. Its aim is to improve the reliability and applicability of the entire network. So when choosing technologies for each layer, you must consider the impacts and restrictions caused by the technologies used at the current layer over other layers and also those caused by the technologies used at other layers over the current layer. Network design is a process that requires constant review and improvement. Mutual influences between layers must be taken into consideration in the final solution.

Campus network design involves multiple factors. Besides commercial and technical factors, other factors such as equipment rooms, environment conditions, compatibility, and reuse must also be considered. Campus network designing is a systematic and global work.

On an agile campus network, wired and wireless networks coexist, but their design focuses differ greatly. For details about the differences between the wired and wireless network design, see **3.4.5 Wireless Network**.

3.4.1 Access Layer

The access layer is the edge of a campus network, which provides various access methods to PCs, network cameras, printers, IP phones, and wireless terminals. It is the first layer of the campus network, and needs to meet all kinds of access demands.



The access layer also needs to protect the entire network by preventing unauthorized users and applications from connecting to the network, so it must provide enough security without compromising network availability. For details about security design, see **5 Security Design and Best Practices**.

The access layer design guidelines:

- Meet different access demands, which may include access from terminals of different types, access with different interface rates, access with different requirements on the network quality, and access with other requirements such as PoE power supply.
- Take scalability into consideration.
- Provide security.
- Simplify network deployment and management.

Key design points of the access layer:

- Networking architecture design: If there are a large number of switches, whether they work in collaboration or in conflict needs to be taken into consideration; how to connect the access layer to the aggregation layer, including the link type and networking mode, also needs to be considered.
- Uplink and downlink design: The design needs to meet the access requirements of the campus network. That is, the downlink interface rates of access switches match the NIC rates of terminals, the network oversubscription ratio is reasonable, and the uplink bandwidth meets the service quality requirements. The number of access switches and the switches' port desity need to be determined based on the number of terminals or users and the network scalability requirement. In terms of scalability, the access layer only needs to satisfy the current access demand.
- Device model design: Device model selection guidelines and methods are involved.

3.4.1.1 Networking Architecture

The working mode and uplink networking mode of switches need to be considered in the networking architecture design. The uplink networking mode includes wired network and wireless network. On a wired network, switches are deployed at the access layer; on a wireless network, APs are deployed at the access layer.

Working Mode

Typically, there are multiple switches at the access layer. If there are many access switches, you need to consider whether the switches need to work in collaboration. Access switches can work in two modes: independent mode and stacking mode.

Table 3-2 Working modes of switches at the access layer

Working Mode	Description	Advantage	Disadvantage
Independent mode	 Each switch works independently without depending on or in collaboration with other switches.	● Each device works independently, so faults of one node will not affect other nodes and the network is easy to expand. ● The network compatibility is high. Different types of configurations can coexist. ● The requirements on devices are low. Devices supporting standard protocols can be used.	● The network has a low reliability and is prone to single point failures. ● The management complexity increases with the number of managed devices. Therefore, this mode is not applicable to large-scale deployment.
Stacking mode	 Switches work together to form one logical switch.	● This mode reduces the management complexity, and is applicable to large-scale deployment. ● Dual-homed uplinks can prevent single-point link failures. ● Uplink resources are saved.	● More links are required to connect devices. ● High device consistency is required, and the compatibility is poor. ● It is difficult to add devices, which increases the difficulty in troubleshooting.

Wired Uplink Networking Mode

There are multiple uplink networking modes for the access layer on a wired network, depending on the working mode of access switches, number of devices at the aggregation layer, and other requirements such as reliability.

Figure 3-7 Wired uplink networking modes

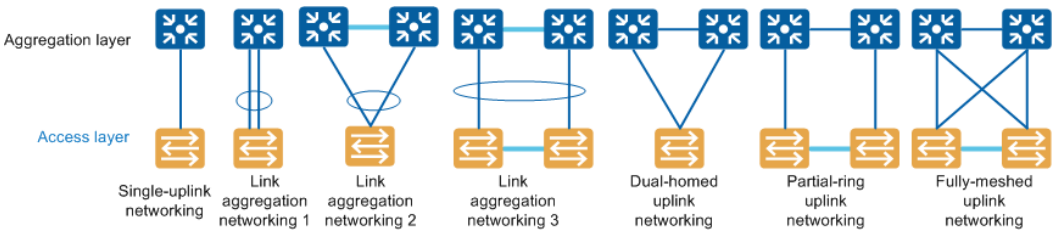


Table 3-3 describes the application scenarios of various networking modes.

Table 3-3 Description of the networking modes for a wired network

Networking Mode	Reliability	Construction Cost	Network Structure	Application Scenario
Single-homed uplink networking	Low	Low	Simple	Only one device needs to be deployed at the aggregation layer, such as on a small-sized campus network.
Link aggregation networking 1	High	Low	Simple	Multiple links need to be aggregated for interconnection on a small-sized campus network with high reliability requirements.
Link aggregation networking 2	High	Medium	Simple	Aggregation switches need to be stacked on a network with extremely high reliability requirements.
Link aggregation networking 3	High	Medium	Simple	Both access switches and aggregation switches need to be stacked on a network with extremely high reliability requirements on the access switches (such as in the scenario where dual-homed access is required).
Dual-homed uplink networking	High	Medium	Medium	Multiple devices need to be deployed at the aggregation layer on a network with high reliability requirements.

Networking Mode	Reliability	Construction Cost	Network Structure	Application Scenario
Partial-ring uplink networking	Medium	Medium	Medium	Access devices need to be stacked on a network with high reliability requirements.
Fully-meshed uplink networking	High	High	Complex	Access devices need to be stacked on a network with extremely high reliability requirements.

Wireless Uplink Networking Mode

There are multiple uplink networking modes for the access layer on a wireless network, depending on the working mode of APs, number of devices at the aggregation layer, and other requirements such as reliability.

Figure 3-8 Wireless uplink networking modes

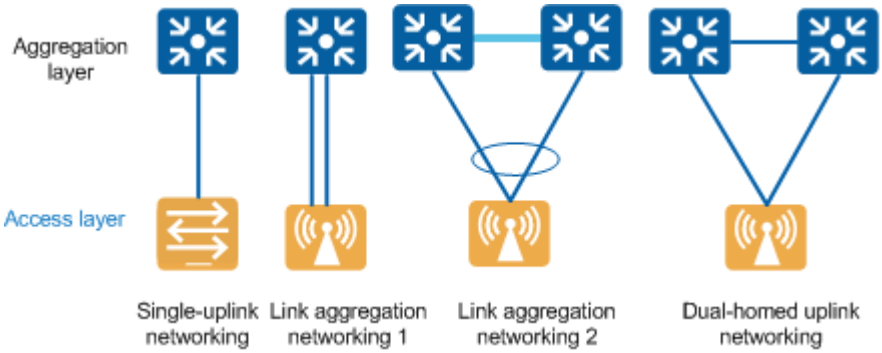
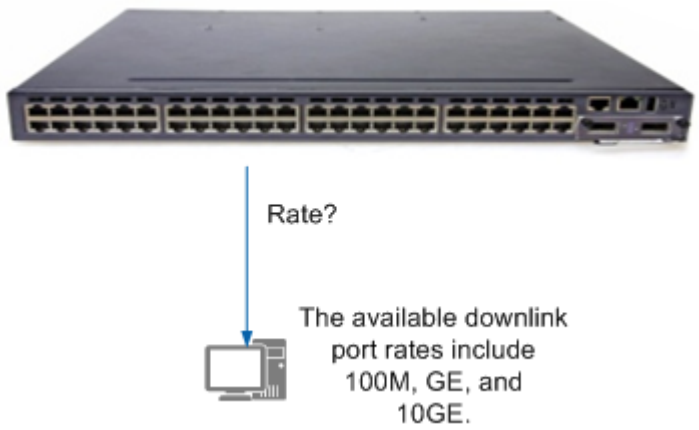


Table 3-4 Description of networking modes for a wireless network

Networking Mode	Reliability	Construction Cost	Network Structure	Application Scenario
Single-homed uplink networking	Low	Low	Simple	There are low reliability requirements on APs, and the bandwidth needs to be sufficient.
Link aggregation networking 1	High	Low	Simple	Dual links need to be aggregated for interconnection. In addition, the aggregation layer needs to have only one device, and requires high reliability or high bandwidth.
Link aggregation networking 2	High	Medium	Simple	Aggregation devices need to be stacked. In addition, APs are required to have high reliability or provide high bandwidth.
Dual-homed uplink networking	High	Medium	Complex	Multiple devices need to be deployed at the aggregation layer without being stacked, and APs are required to have high reliability.

3.4.1.2 Downlink

In downlink designing for the access layer, the downlink type between access switches and terminals, port rate, and power supply mode of terminals need to be considered. Typically, after the terminal access mode is determined, parameters related to access switches, including the port rate and downlink type, can be determined accordingly. Generally, the downlink performance needs to match the NIC rates of terminals.



The following ways are used to determine the link type:

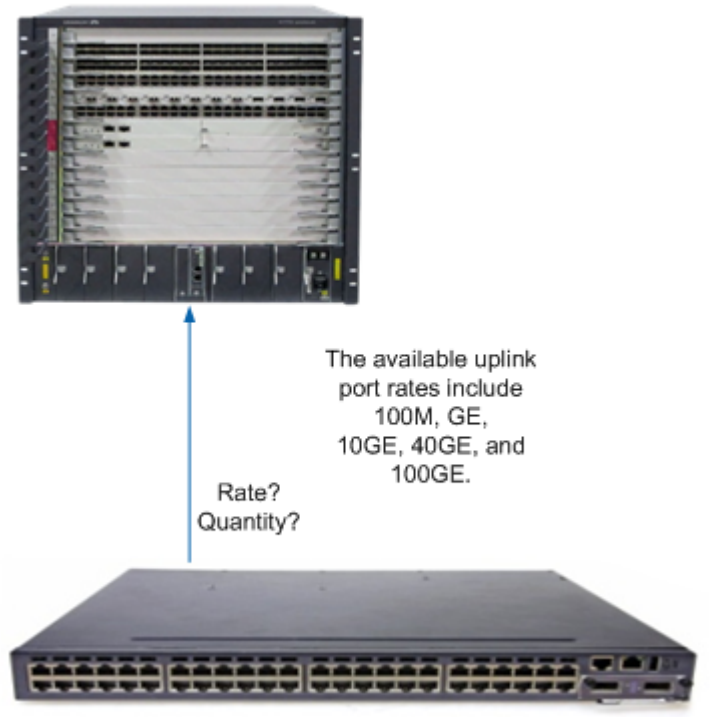
- Determine the downlink port rate of access switches based on the NIC rates of terminals. For example, if all terminals use 100M NICs, access switches that support 100M access or auto-sensing access are recommended, such as S2700 or S3700.
- Determine the downlink port rate of access switches based on the service bandwidth. In this case, you need to analyze the service types and bandwidth requirements of end users. For example, if end users in the media industry need to transmit HD videos through multiple links at the same time, the access switches may require GE ports.

Typically, the first way is recommended. The second way is applicable to new network building (including adding new terminals). The problem with the second way is the difficulty in identifying services and estimating their requirements on the bandwidth.

Besides the link type, the link length must also be considered. When terminals are within 100 meters of access switches, electrical cables are recommended. When they are over 100 meters away from the access switches, optical fibers are recommended.

3.4.1.3 Uplink

Uplinks connect the access layer to the aggregation layer. Uplink designing involves determining the link type (interface rate/bandwidth/link type), number of links, and uplink networking mode. The basic rule is to use the least number of links while still meeting the requirements on the network rate, bandwidth, and reliability.

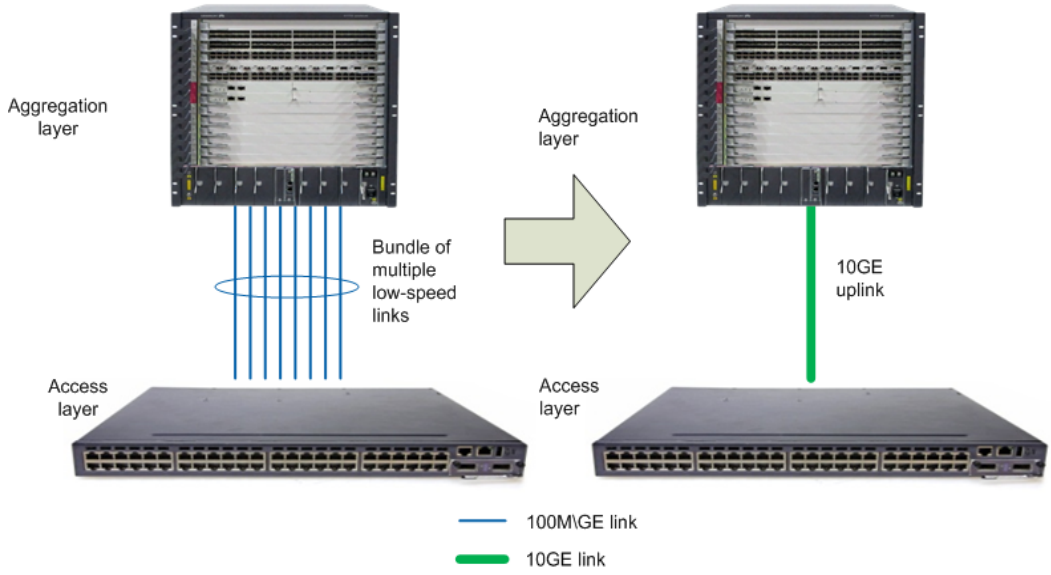


Uplink Interface Rate

Once the model of access switches is determined based on the downlink port rate and density, the uplink port rate is determined accordingly. If there are multiple types of uplink ports of different rates, the one of the highest rate is selected preferentially.

As multimedia services expand, the requirement on the bandwidth of the access layer in a campus network increases rapidly. 10GE uplinks are recommended for the access layer to connect to the aggregation layer so that high-performance and non-blocking network services can be implemented. The advantages of 10GE uplinks are as follows:

- Increase throughput: The bandwidth throughput of physical ports increases by 10 times, effectively avoiding exposure to the risks of insufficient uplink bandwidth.
- Provide high performance: All data traffic is transmitted over a high-speed link rather than over multiple low-speed links, improving transmission efficiency.
- Reduce the total cost of ownership (TCO): The cost of each switch port and the cost of link connection are reduced.
- Facilitate maintenance: Only one high-speed link needs to be managed and maintained.



Uplink Type

The uplink types include electrical cables and optical fibers, depending on a combination of factors such as link media, transmission rate, line standard, and transmission distance.

Table 3-5 describes the mapping between mainstream transmission rates and link types supported by S series switches.

Table 3-5 Mapping between transmission rates and link types

Transmission Rate	Link Type	Interface Type	Maximum Distance
FE (100M)	Electrical cable	RJ45	100 m
	Optical fiber	SFP	80 km
GE (1000M)	Electrical cable	RJ45	100 m
	Optical fiber	SFP	100 km
10GE (10000M)	Electrical cable	RJ45	100 m
	Optical fiber	SFP+/XFP	80 km
40GE	Optical fiber	QSFP+/QSFP28	40 km
100GE	Optical fiber	QSFP28	30 km

If optical fibers need to be used for transmission, pay attention to its transmission modes. Multi-mode optical fibers apply to short-distance transmission (hundreds of meters). Single-mode optical fibers apply to long-distance and high-speed transmission. If optical fibers are in short supply, you can use single-fiber bidirectional optical modules to transmit bidirectional signals.

Uplink Bandwidth and Quantity

After the switch model is determined, the uplink bandwidth and quantity on each switch need to be determined. Generally, each switch requires at least one uplink. If a single uplink does not suffice, multiple uplinks need to be used. In some cases requiring high link reliability, a switch also needs to use multiple uplinks.

There are multiple methods to calculate the uplink bandwidth and quantity, and these methods can be used together. The following two methods are recommended:

- **Service analysis**: Determine the uplink bandwidth and quantity by calculating the maximum bandwidth required by all campus network services. This is a top-bottom analysis method that requires thorough understanding of all campus network services. If this method is used, it is assumed that no service is blocked. (Otherwise, the network oversubscription needs to be considered using the second method.) That is, the assumed network oversubscription ratio is 1:1. This method calculates the uplink bandwidth of the access layer and the number of uplinks on each switch based on the analysis of the maximum network bandwidth required by each end user. The following provides the calculation formulas:
  - Uplink bandwidth of the access layer = Maximum bandwidth of a single user x Number of access users
  - Number of switches = Number of access users/Number of downlink ports on a single switch
  - Number of uplinks on a single switch = Uplink bandwidth/Number of switches/ Uplink port rate of the switch
- **Network oversubscription**: Determine the uplink bandwidth and quantity by calculating the network oversubscription ratio between the access layer and aggregation layer, which is a bottom-up method. The network oversubscription ratio can be determined by customers or be inferred from industry experience value (4 to 20 in general).
  - Uplink bandwidth of a single switch = Number of downlink ports on the switch x Port rate/Network oversubscription ratio
  - Number of uplinks on a single switch = Uplink bandwidth of the switch/Uplink port rate of the switch

NOTE

The calculation results of the above formulas need to be rounded up.

3.4.1.4 Device Model

The access layer does not have high requirements on device performance. Fixed switches will suffice.

Device model selection is affected by technical factors such as interface rate, port density, and PoE, as well as non-technical factors such as price, reuse, and compatibility. **Table 3-6** describes how to select device models based on technical factors.

Table 3-6 Device model selection guidelines

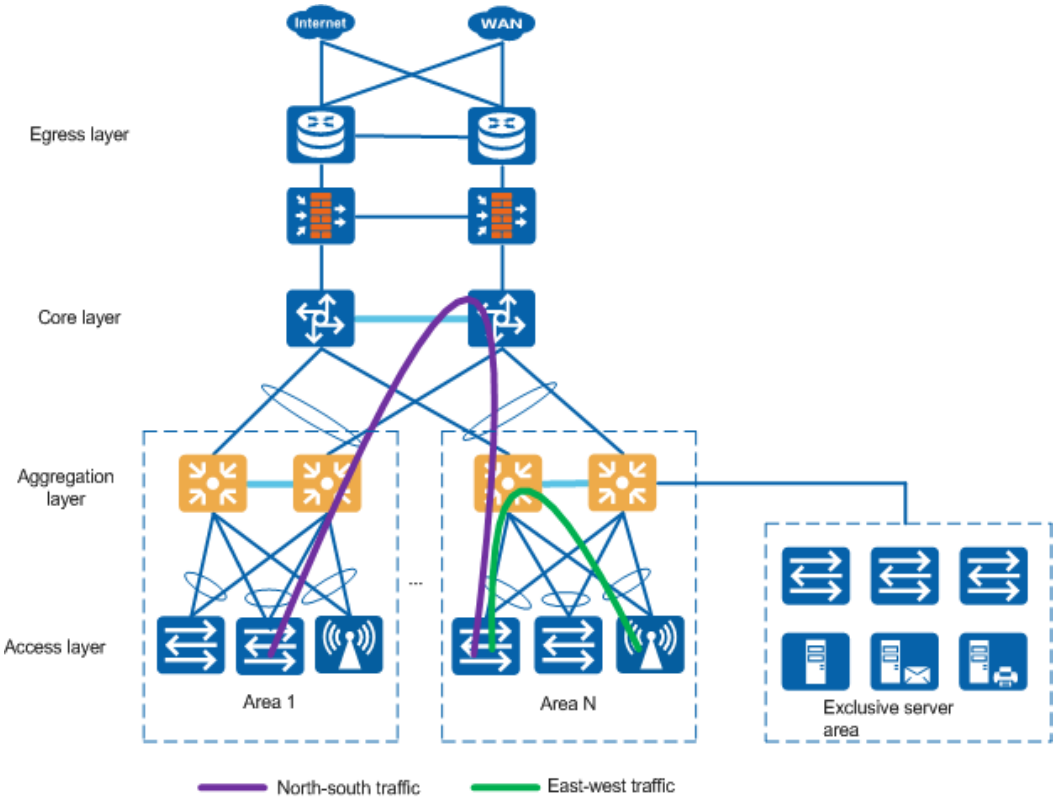
Factor	Model Selection Guideline	Model Selection Method
Downlink interface rate	The selected device model needs to satisfy the access rate or bandwidth requirements of all services in the campus.	Method 1: Select a device model based on service requirements. That is, select the device model with an interface rate higher than and closet to that required by the services with the highest bandwidth requirement. Method 2: Select a device model based on the NIC rates of terminals. For example, select 100M access switches for 100M NICs, and GE access switches for GE NICs.
Port quantity/ density	The selected device model needs to minimize the number of devices to be used to facilitate networking and management.	The total number of switch ports is determined by the number of end users or the number of interfaces they require. If a large number of switch ports are required, select switches with high-density ports. The access layer expansion is simple. Therefore, the network scalability can be ignored at the access layer, but must be considered in the designing of the aggregation layer or the core layer.
PoE	The selected device model needs to meet the specific PoE requirements of terminals.	If there are terminals requiring PoE power supply such as IP phones and APs, select PoE-capable devices.

The S6700/S5700/S3700/S2700 series can be used as access switches. S5720-LI and S5720-SI are recommended. For details about recommended AP models, see **12 Appendix-Recommended Product Models**.

3.4.2 Aggregation Layer

The aggregation layer connects the access layer and the core backbone network of a campus.

The aggregation layer is key in forwarding east-west traffic between departments and north-south traffic to the core layer. The aggregation layer hides the core layer from the access layer. It functions like a cable distribution frame on the campus network and connects a large number of end users to core devices. It can also function as the switching core connecting a department or a campus network to the exclusive server area.



The design guidelines of the aggregation layer are as follows:

- High performance: The design of the aggregation layer needs to fully meet the network bandwidth and performance requirements of campus network services and ensure that the network will not be blocked and services run smoothly.
- Reliability: The network needs to work stably and reliably without interruption.
- Scalability: In the designing of the aggregation layer, the network scalability must be fully considered. The design needs to meet the development requirements of the campus network in the future three to five years so that network upgrade can be implemented smoothly and services can be migrated seamlessly.
- Area-specific configuration: The design of the aggregation layer needs to enable aggregation devices to be configured by area based on network and service isolation requirements. In this way, the network construction can meet the actual requirements better. Different areas can be deployed with network devices of different specifications or be deployed with standard devices to facilitate service expansion and migration. The following describes the design details of the mode in which standard devices are deployed in different areas.

Key design points of the aggregation layer:

- Network architecture design: working mode, uplink networking mode, and architecture model of aggregation devices
- Uplink design: uplink type and bandwidth
- Device model design: Device model selection guidelines and methods are involved.

3.4.2.1 Networking Architecture

The working mode and uplink networking mode of switches need to be considered in the networking architecture design.

Working Mode

Depending on the working relationships between devices at the aggregation layer, there are three working modes of the aggregation switches: independent mode, backup mode, and CSS/stack mode, as shown in the following figure.

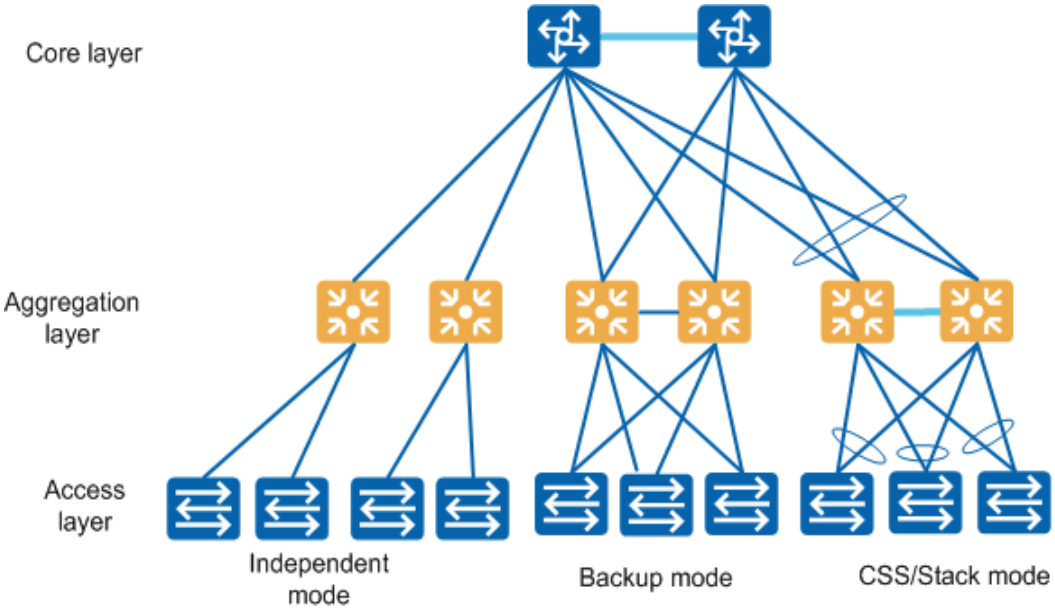


Table 3-7 describes the application scenarios of the three working modes.

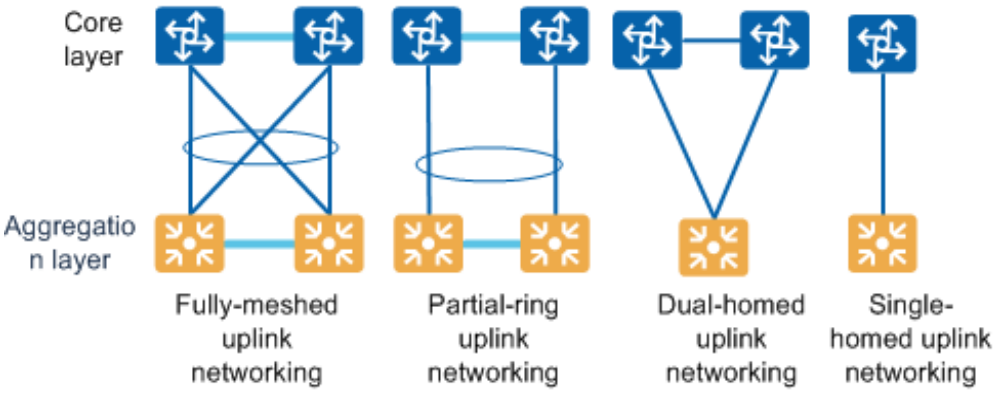
Table 3-7 Working modes of switches at the aggregation layer

Working Mode	Description	Application Scenario
Independent mode	Each device works independently and has independent uplinks and downlinks. They do not collaborate with or back up each other. The status of one device does not affect the running of another device.	Small- or medium-sized campus
Backup mode	Multiple aggregation devices collaborate with and back up one another through link backup.	Medium-sized campus
CSS/Stack mode (recommended)	Multiple aggregation devices work in CSS/stacking mode. Link backup or aggregation is applied.	Medium- or large-sized campus or new campus

Uplink Networking

The aggregation layer can be dual-homed or single-homed to the core layer, as shown in Figure 3-9. The dual-homed mode is recommended for the aggregation layer.

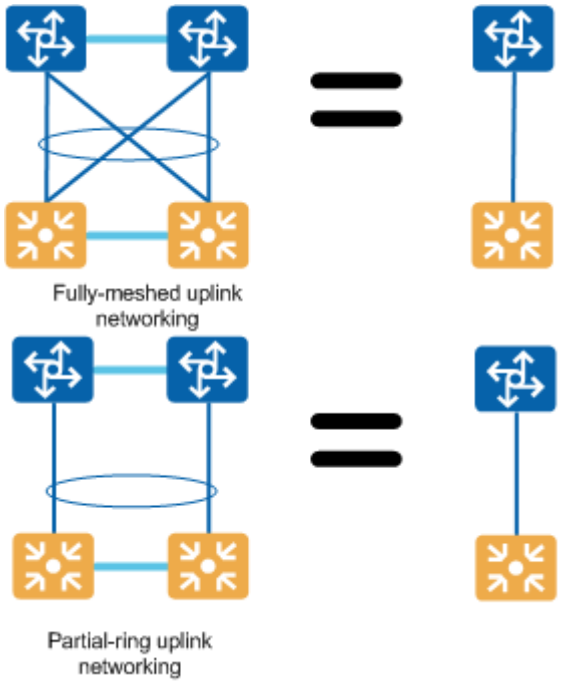
Figure 3-9 Uplink networking modes at the aggregation layer



If the core layer has multiple devices or has high requirements on link reliability, the dual-homed uplink networking is recommended to improve network and link reliability.

If both the core layer and aggregation layer need to be deployed in CSS/stacking mode, the fully-meshed uplink networking or the partial-ring uplink networking is recommended for the aggregation layer to form a loop-free network.

- Fully-meshed uplink networking: All aggregation devices are dual-homed to the core layer, which is applicable to scenarios requiring high reliability.
- Partial-ring uplink networking: Each aggregation device is single-homed to the core layer, which is applicable to long-distance interconnection or cost-saving scenarios.



Depending on the working mode and uplink networking mode of aggregation devices, there are multiple deployment modes for the aggregation layer, as shown in **Figure 3-10**.

Figure 3-10 Networking modeld at the aggregation layer

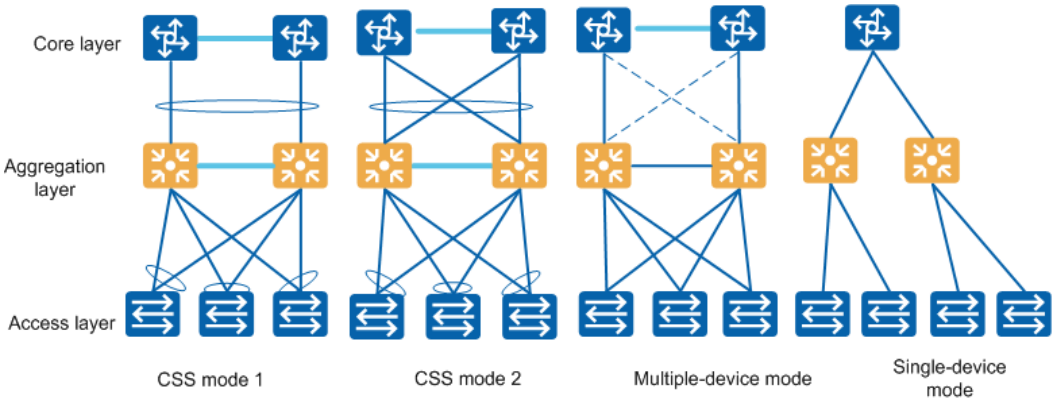


Table 3-8 Description of networking modes at the aggregation layer

Networking Model	Description	Advantage/ Disadvantage	Application Scenario
CSS mode 1	CSS is implemented for aggregation switches. Each switch is single-homed to the core layer. (This mode is applicable to long-distance interconnection scenarios.)	High reliability; medium link cost and reliability	Medium- or large-sized campus or new campus
CSS mode 2	CSS is implemented for aggregation switches. Each switch is dual-homed to the core layer.	Highest reliability; high link cost	Medium- or large-sized campus or new campus
Multiple-device mode	Each aggregation point contains two or more switches to back up one another or for load balancing.	High reliability; complex management	Small- or medium-sized campus
Single-device mode	Each aggregation point contains only one switch working independently.	Low reliability; simple network structure and easy network management	Small- or medium-sized campus

3.4.2.2 Uplink

Typically, the aggregation layer is dual-homed to the core layer. Its uplink design involves the link type (uplink interface rate/bandwidth) and link quantity. The design guidelines are as follows:

- Use high-speed interfaces preferentially.
- Use the minimum number of uplink interfaces. If multiple uplinks are needed, use link aggregation to improve reliability and simplify management.

In consideration of the performance and cost, GE, 10GE, 40GE, and 100GE uplinks are generally used at the aggregation layer. 10GE, 40GE, and 100GE uplinks are recommended for 10GE campuses.

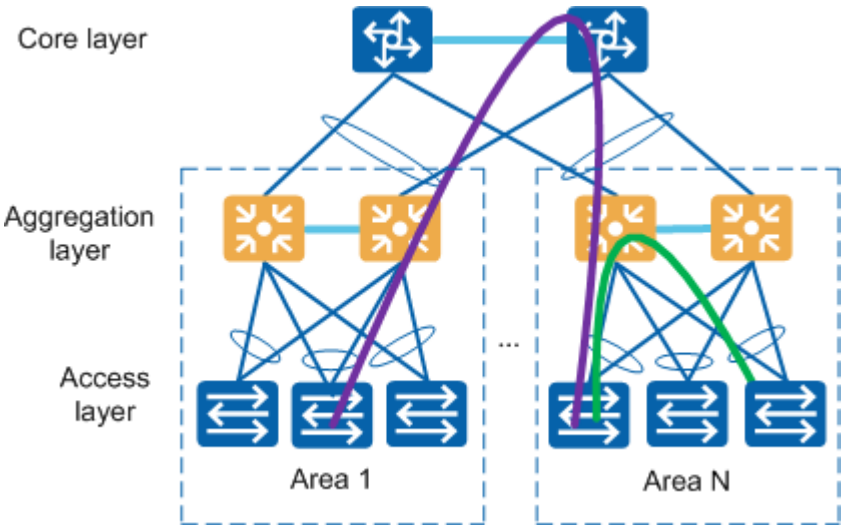
After the switch model and uplink rate of the aggregation layer are determined, the number of uplinks can be calculated according to the following formula:

Number of uplinks = [Uplink bandwidth/Uplink interface rate]

Uplink Bandwidth

You can calculate the uplink bandwidth of each area separately or calculate the uplink bandwidth of all areas using the same standard. You are advised to calculate the uplink bandwidth of all areas using the same standard.

- To ensure smooth service migration, you need to use the maximum area scale and maximum service bandwidth as factors in calculating the uplink bandwidth of all areas.
- To obtain the most secure calculation result and simplify the calculation, you need to treat all traffic passing through the aggregation layer as north-south traffic for calculation.



The uplink bandwidth can be calculated using either of the following methods and the larger calculation result is recommended:

- Service analysis: Calculate uplink bandwidth based on the service bandwidth and the number of access users. The formula is as follows, assuming that no service blocking occurs:

Uplink bandwidth 1 = Service bandwidth x Number of access users x (1 + Network expansion rate within 3 to 5 years)

- Network oversubscription ratio: Calculate the uplink bandwidth based on the network oversubscription ratio and uplink bandwidth of the access layer. The formula is as follows:

Uplink bandwidth 2 = [Uplink bandwidth of all switches at the access layer/Network oversubscription ratio] x (1+ Network expansion rate within 3 to 5 years)

The final uplink bandwidth of the aggregation layer will be:

Uplink bandwidth = MAX (uplink bandwidth 1, uplink bandwidth 2)

NOTE

In the formulas, [] indicates that the value needs to be rounded up.

Link Type

Like that of the access layer, the uplink type of the aggregation layer, electrical cable or optical fiber, also depends on the connection distance and transmission rate between devices.

3.4.2.3 Device Model

Fixed switches or modular switches can be used at the aggregation layer, depending on the network scale. Fixed switches are recommended for small-sized campuses and modular switches are recommended for medium- and large-sized campuses. **Table 3-9** lists the factors that need to be considered during model selection.

For aggregation devices, the performance and scalability need to be the main considerations, and the interconnectivity with the access layer and core layer also needs to be a consideration.

Table 3-9 Device model selection guidelines

Factor	Model Selection Guideline	Model Selection Method
Downlink interface rate	The performance of the selected model needs to match the uplink rate of the access layer.	See chapters on the access layer design. 10GE interfaces are recommended.
Uplink interface rate	High-speed interfaces are preferred to reduce the number of uplinks.	Select uplink interfaces of the highest speed, which must be compatible with the core layer devices.
Switching capacity	The selected model needs to meet campus service requirements.	Select products based on service types, the number of users, and scalability.
Forwarding capability		

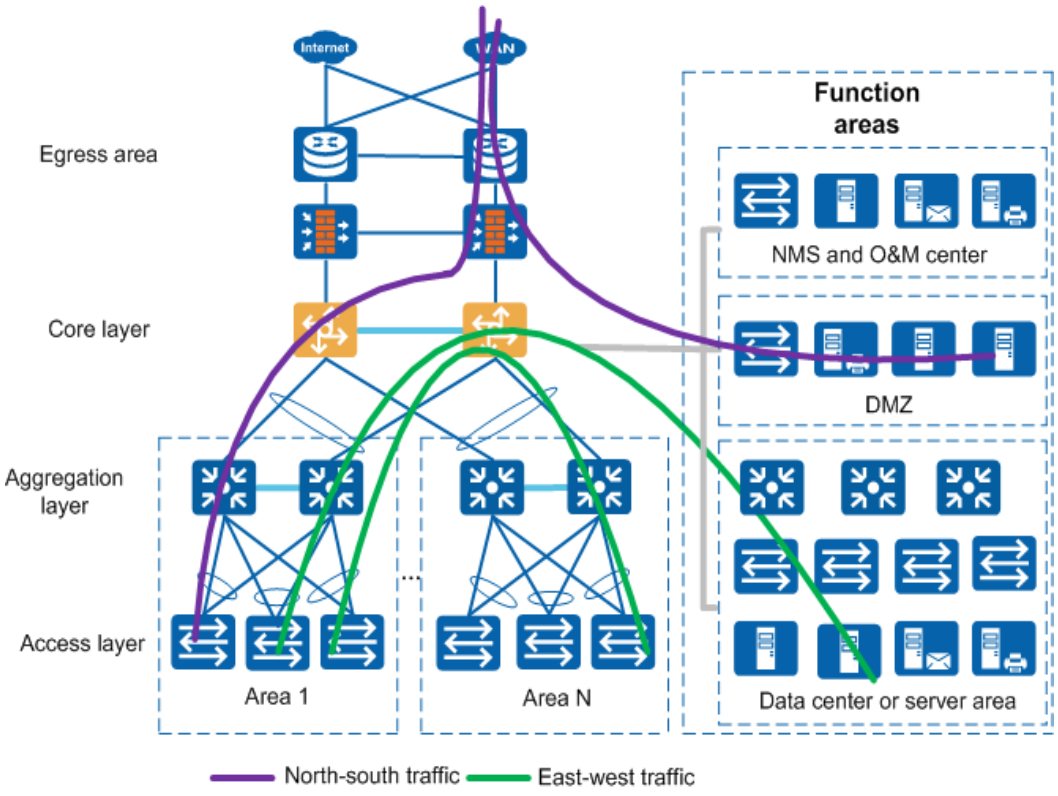
Factor	Model Selection Guideline	Model Selection Method
Port quantity/ density	The selected model needs to minimize the number of devices to facilitate networking and management.	The total number of switch ports is determined by the number of end users or the number of interfaces they require. If a large number of switch ports are required, select switches with high-density ports. The access layer expansion is simple. Therefore, the network scalability can be ignored at the access layer, but must be considered in the designing of the aggregation layer or the core layer.
Port type	The selected model needs to meet the requirements of the transmission rate and distance.	Select optical interfaces or electrical interfaces based on the transmission rate and distance. Electrical interfaces are recommended. Use optical interfaces when high transmission rate and long transmission distance are required.

The S9700/S7700/S6700/S5700 series can be used as aggregation switches. S6720-LI and S6720-SI are recommended for the S6700 series.

3.4.3 Core Layer

The core layer is key in forwarding east-west traffic between users and north-south traffic to external networks and the egress area.

The core layer may also function as a junction node for other network areas such as the data center area, NMS area, and DMZ.



Since requirements on network performance may change, scalability must be considered in network architecture design. The core layer must be able to expand in the future to support adding of devices and applications, network upgrade and evolution, and service migration.

The following factors must be considered in core layer designing:

- Performance
- Capacity
- Scalability
- Reliability
- Service capability

Key design points of the core layer:

- Network architecture design: working mode and uplink networking mode of core devices
- Uplink networking mode: uplink type and bandwidth
- Device model design: device model selection guidelines and methods

3.4.3.1 Networking Architecture

Working Mode

There are three working modes of core switches: single-device mode, multi-device mode, and CSS mode. The working mode can be selected based on the requirements of the performance, capacity, reliability, and scalability.

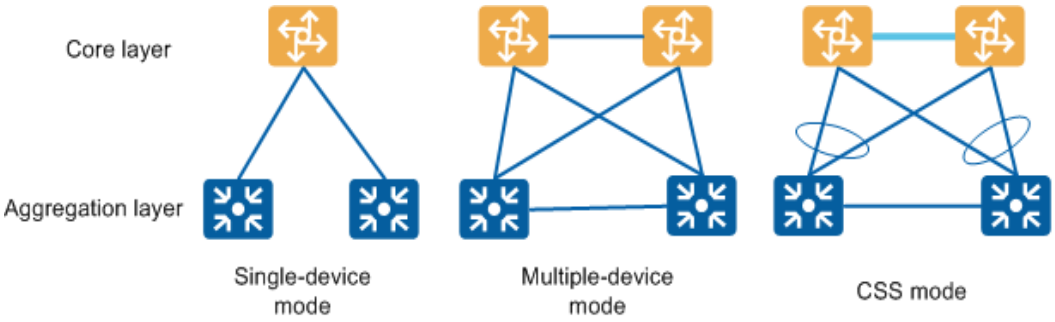


Table 3-10 describes the application scenarios of the three working modes.

Table 3-10 Working modes of switches at the core layer

Working Mode	Description	Application Scenario
Single-device mode	The core layer has only one device.	This mode is applicable to small- and medium-sized campuses that have small networks with low requirements on the network capacity, performance, and reliability. This mode can save the network construction cost.
Multiple-device mode	The core layer contains dual or more devices working independently, forming two or more independent cores.	This mode is applicable to medium- and large-sized campuses that have large networks with medium requirements on the network capacity, performance, and reliability. This mode is usually used in network reconstruction scenarios.
CSS mode	The core layer uses CSS to virtualize two or more core switches into a logical device.	This mode is applicable to medium- and large-sized campuses that have large networks with high requirements on the network capacity, performance, and reliability and require simplified network structure and easy management. This mode is recommended in new network construction scenarios.

Uplink Networking

The core layer can be single-homed or dual-homed to the egress area based on the configurations of the egress devices, as shown in Figure 3-11.

Figure 3-11 Uplink networking modes of the core layer

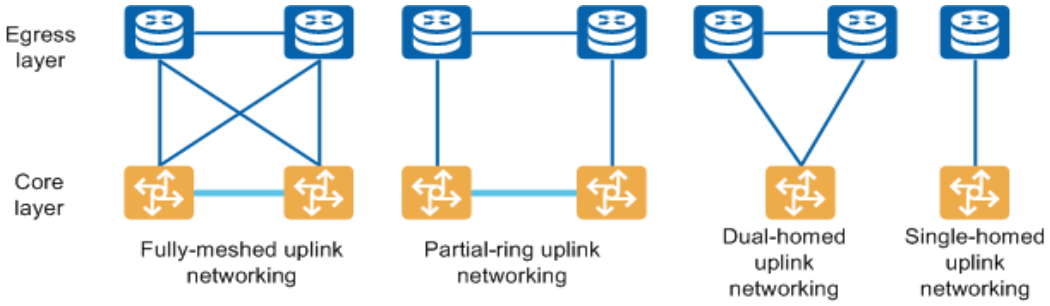


Table 3-11 describes the application scenarios of the networking modes.

Table 3-11 Description of networking modes

Networking Mode	Reliability	Construction Cost	Network Structure	Application Scenario
Fully-meshed uplink networking	High	High	Complex	This mode is applicable to scenarios requiring extremely high reliability and stacking at the core layer.
Partial-ring uplink networking	Medium	Medium	Medium	This mode is applicable to scenarios requiring high reliability and stacking at the core layer.
Dual-homed uplink networking	Medium	Medium	Medium	This mode is applicable to scenarios requiring medium reliability and multiple devices in the egress area.
Single-homed uplink networking	Low	Low	Simple	This mode is applicable to scenarios where there is only one device in the egress area, such as in a small-sized campus.

3.4.3.2 Uplink

Most of the traffic at the core layer is internal traffic, with a small volume of uplink traffic. The number of uplinks of the core layer is determined by the number of egress routers. If there are multiple egress routers, the dual-homed networking is recommended.

In the uplink designing of the core layer, the link type (uplink interface rate/bandwidth) is the main consideration. The guidelines are as follows:

- Select high-speed interfaces to meet service bandwidth demands.
- Use the minimum number of uplink interfaces. If multiple uplinks are needed, use link aggregation to improve reliability and simplify management.

GE, 10GE, 40GE, 100GE uplinks can be used for the core layer. For 10GE campuses, 10GE, 40GE, and 100GE uplinks are recommended.

The uplink bandwidth at the core layer refers to the bandwidth from the core layer to the campus egress, which is usually the campus egress bandwidth. The uplink bandwidth of the core layer is calculated based on the egress service type and the number of users. The formula is as follows:

Uplink bandwidth = Maximum bandwidth of egress services x Number of users x (1 + Network expansion rate within 3 to 5 years)

The core layer is important in the campus network, and the configuration change of the core layer is not recommended in most cases. Therefore, the network scalability must be considered in the designing of the core layer. The network expansion within 3 to 5 years needs to be included in the calculation of the uplink bandwidth of the core layer to reduce the change of the core layer. After the uplink bandwidth is calculated, the uplink rate of core devices can be determined. Generally, the uplink bandwidth can be used as the reference of the lowest rate. In addition, the cooperation with the network devices in the egress area needs to be considered.

3.4.3.3 Device Model

Core switches forward and exchange north-south traffic between a campus network and an external network, as well as east-west traffic within the campus network. Its functions and performance directly determine the campus network service experience of end users.

Generally, core switches need to meet the following requirements:

- High performance: large capacity, high forwarding capability, and non-blocking/line-rate forwarding
- High reliability: high reliability of devices and Layer 2/Layer 3 reliability
- Scalability: service expansion by inserting cards, capacity redundancy, and slot redundancy
- Multi-functionality: integration with wireless AC, firewall, and IPS functions

In addition to technical factors, non-technical factors such as the investment cost, upgrade and reconstruction, reuse, and compatibility must be considered during core device selection.

You can primarily determine the switch series or models based on the device performance requirements (forwarding capability, interface rate, and port type) raised by campus services. Then, determine the specific switch model based on network feature requirements.

Typically, modular switches are selected for the core layer, which provide various types of interface boards and therefore can be used in various scenarios. The key performance indicators of core switches are as follows:

- Forwarding capability: It refers to the capability of forwarding north-south traffic of the campus network, namely, the egress service bandwidth of the campus network. You need to perform calculation based on the campus service analysis result, network scale, and network expansion rate.
- Switching capacity: It refers to data exchange traffic of internal services on the campus network. Generally, it is required that no blocking occurs on the campus network. You

also need to perform calculation based on the campus service analysis result, network scale, and network expansion rate.

Alternatively, core switches can be selected from bottom to top, namely, based on aggregation layer configurations. The method is as follows:

1. Determine the interface configurations (rate, port density, and quantity) of core switches based on the uplinks of the aggregation layer.
2. The switching capacity of the core layer is equal to the total traffic of all uplinks at the aggregation layer (assuming that the aggregation layer does not forward east-west traffic).
3. The forwarding capability of the core layer is equal to the total forwarding capability of all devices at the aggregation layer.

If the core layer is connected to other function areas such as the data center and network management center, the data traffic between them also needs to be considered in the designing. The method is similar to that of the aggregation layer.

The S12700/S9700/S7700/S6700 series can be used as core switches. S6720-HI is recommended for the S6700 series.

3.4.3.4 Multi-core Interconnection Networking Architecture

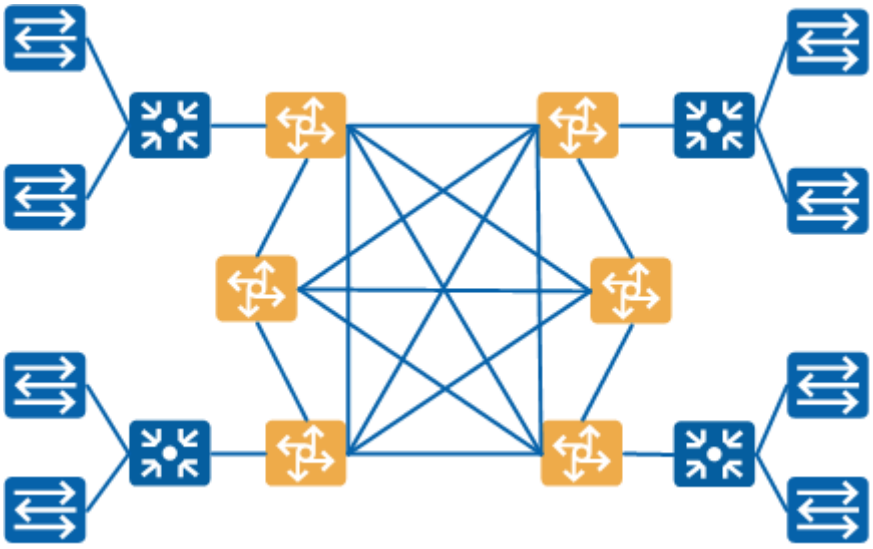
The preceding architecture models are applied to single-core campus networks, namely networks involving onle one core layer. On a large-scale or super-large campus network, there are multiple core layers in the logical structure. Various interconnection solutions are available for the multiple core layers.

Architecture Model

The following describes the four architecture models of multi-core interconnection networks:

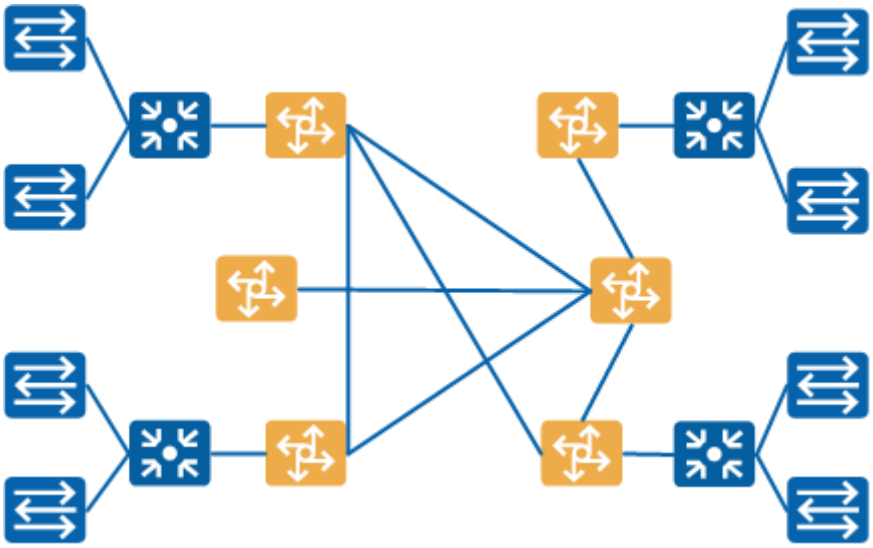
- Full-interconnection architecture (full mesh): All core switches are interconnected with each other, as shown in **Figure 3-12**.

Figure 3-12 Full-interconnection architecture model



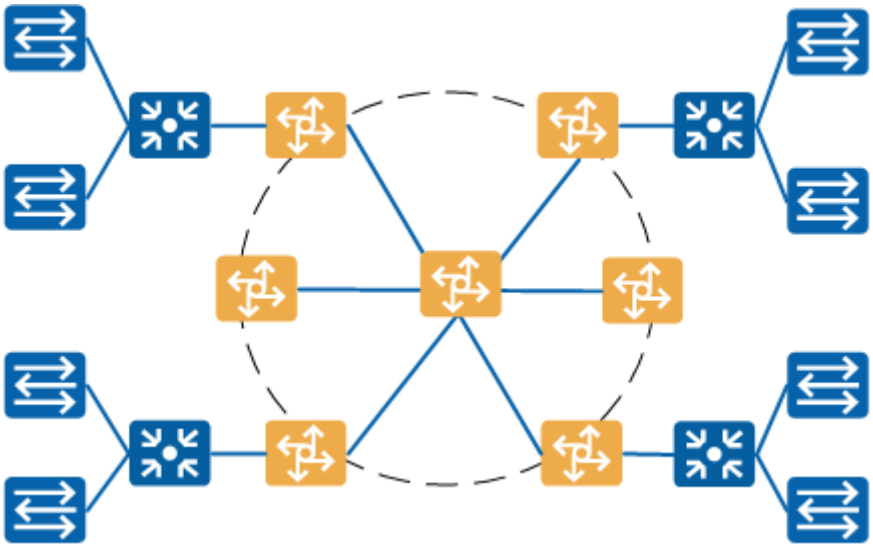
- Partial-interconnection architecture (partial mesh): All core switches are connected to the same one or more (not all) cores switches (with all core switches at the same level), as shown in **Figure 3-13**.

Figure 3-13 Partial-interconnection architecture model



- Improved star architecture: A new core switching node is added to form a two-layer core architecture, as shown in **Figure 3-14**.

Figure 3-14 Star architecture model



- Ring architecture: Adjacent nodes are interconnected to form a ring, as shown in **Figure 3-15**.

Figure 3-15 Ring architecture model

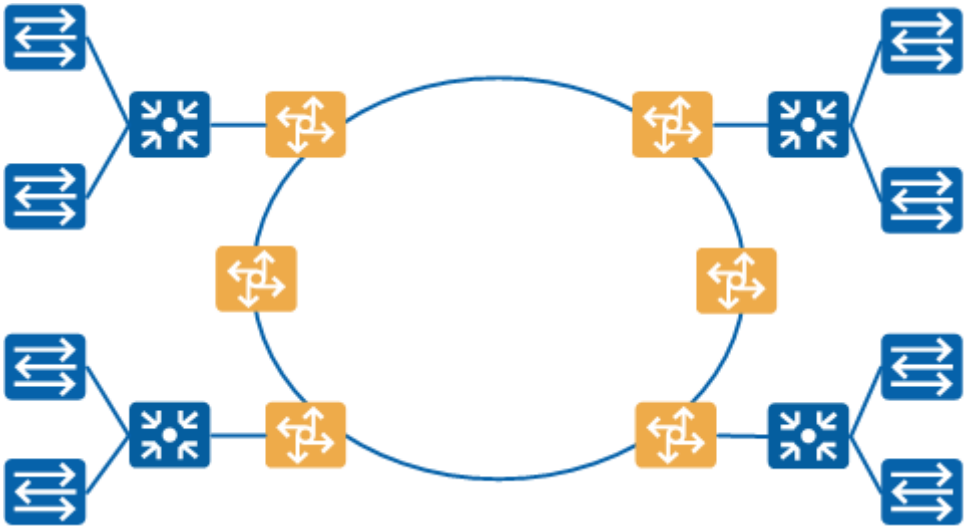


Table 3-12 describes advantages and disadvantages of the different architecture models and their application scenarios.

Table 3-12 Architecture models

Architecture Model	Advantage	Disadvantage	Application Scenario
Full-interconnection architecture	Full interconnection between all core switches, high switching efficiency and reliability	Complex networking, using too many lines and interfaces, poor scalability, difficult to manage	Campus networks that require high forwarding performance, high-end customers such as large Internet service provider (ISP) and Internet data center (IDC)
Partial-interconnect architecture	Saving line resources as only some of the core switches connect to one another, high scalability	Prone to performance bottleneck, decreased forwarding efficiency and reliability, high demands on core switch performance	Common campuses that require low construction costs and have low traffic between core switches
Improved star architecture (recommended 1)	Simple core switch interconnection and network topology, easy to manage and maintain, high scalability	Needing another core device of high performance, low reliability	High-end customers that require high management and forwarding efficiencies in spite of high costs

Architecture Model	Advantage	Disadvantage	Application Scenario
Ring architecture (recommended 2)	Saving line and interface resources, simple network topology, high reliability	Data forwarded multiple times between core switches, resulting in a slightly lower forwarding efficiency and poor scalability	Even data switching between core switches, low investment

Best Practices

- **Example of improved star network architecture**

  When the campus network needs multi-core interconnection, the improved star network architecture is recommended.

  Figure 3-16 Example of improved star network architecture

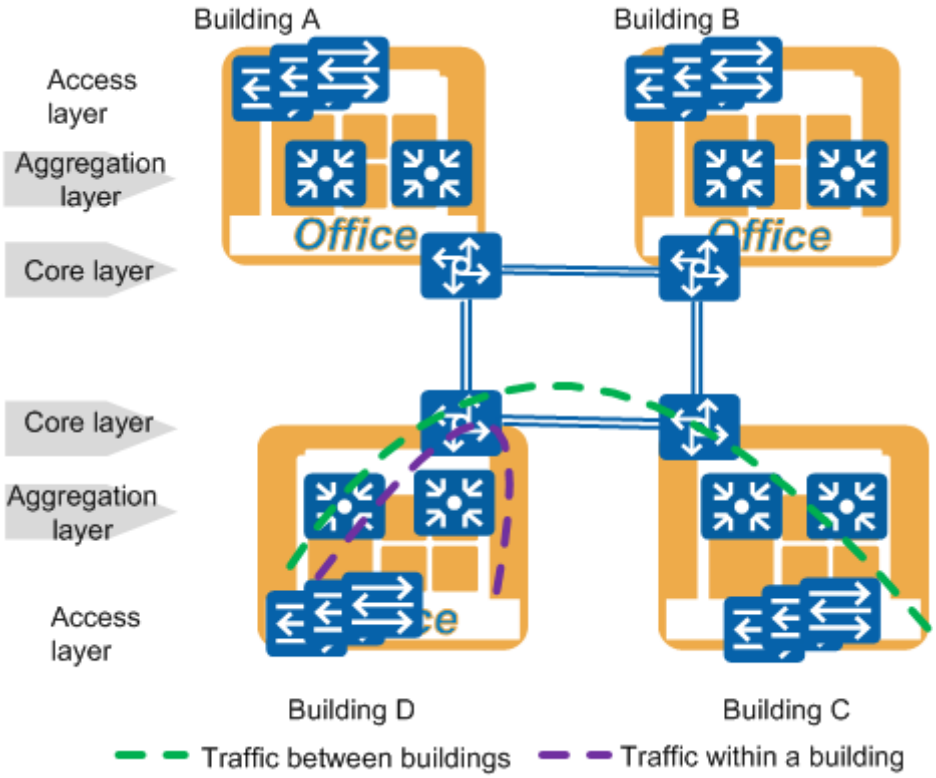
- **Example of ring network architecture**

  If you are subject to limited investment costs and restricted environmental conditions (such as few line resources), the ring network architecture is recommended. When a campus network uses the ring architecture, nodes are designed in tree structure. Communication traffic between nodes is forwarded by the core layer. Both two-layer and three-layer interconnection modes can be used. Three-layer interconnection is recommended.

  The ring architecture has lower scalability and is more difficult to manage than the star architecture, so it is used only in special scenarios meeting all the following requirements:

  - Heavy data switching exists between buildings and all buildings are equally important.
  - The star architecture may cause performance bottleneck.
  - Full interconnection cannot be used between the buildings.

Figure 3-17 Example of ring network architecture

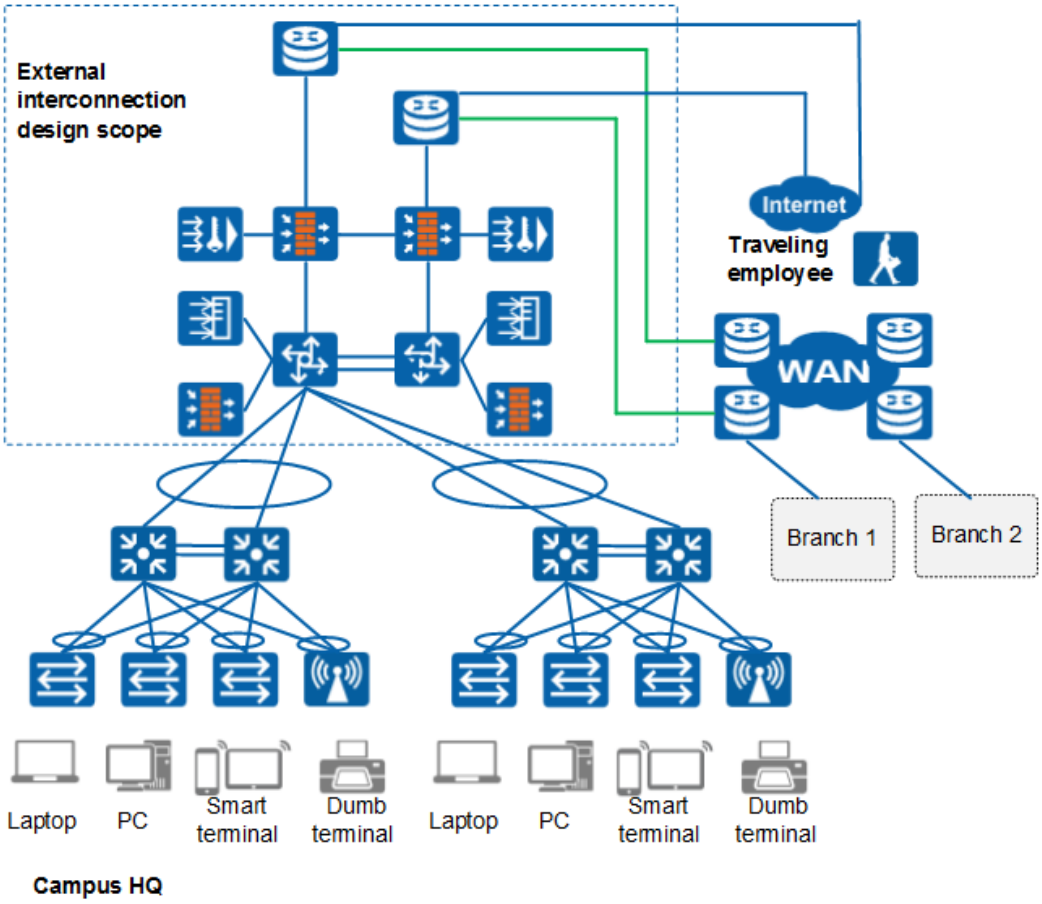


3.4.4 Egress Zone

External interconnection design for a campus network includes Internet egress design and branch/traveling user access design.

The Internet egress design mainly meets campus users' requirements on Internet access and requirements on security protection and load balancing.

The branch/traveling user access design mainly meets the requirements of branch/traveling users on campus service access.



Pay attention to the following points in the egress zone design:

- Internet egress design: Consider whether multiple Internet egress links exist. If yes, consider the requirements on path backup and load balancing. Consider the type of each physical link, because the type of the Internet physical link determines the selection of egress devices.
- Branch access: Consider the geographical location of a branch, which is closely related to the coverage and price of an ISP link. Consider the interworking services between an enterprise and its branches as well as the network scale of branches, because the importance of services and the scale of branch networks affect the selection of branch access links and protocols.
- Traveling user access: Select different access technologies based on the types of terminals carried by traveling users. Consider the access permission policies of traveling users (for example, whether to access the Internet and enterprise intranet at the same time; whether traveling users only have the permission to browse web pages or have the same permission as campus users), because permission policies affect the deployment of access technologies.

3.4.4.1 Internet Egress

The following sections describe key points of designing the Internet egress from the aspects of physical link, egress device reliability, load balancing, and egress security.

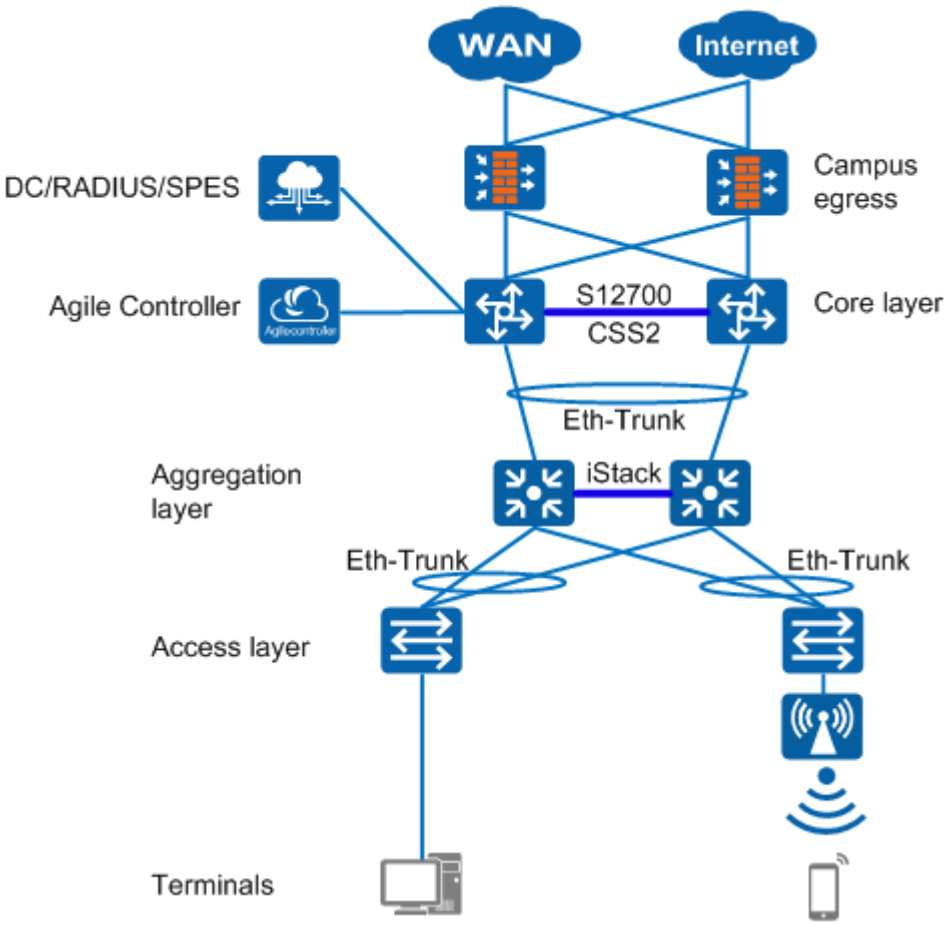
Physical Link

The common physical links and link selection suggestions for the Internet egress are as follows:

- Ethernet links: It is recommended that GE links be selected, which facilitates O&M and reduces card costs. If higher egress bandwidth is required, logical capacity expansion can be performed without replacing the hardware. If there are multiple Internet egress links, you are advised to select links of different carriers.
- xDSL/E1/POS links: It is recommended that xDSL/E1/POS links be used only when local carriers do not support the selection of Ethernet physical links.
- 3G/4G links: 3G/4G links can be used as the backup of Ethernet links, and take effect when Ethernet links are faulty.

Egress Device Reliability

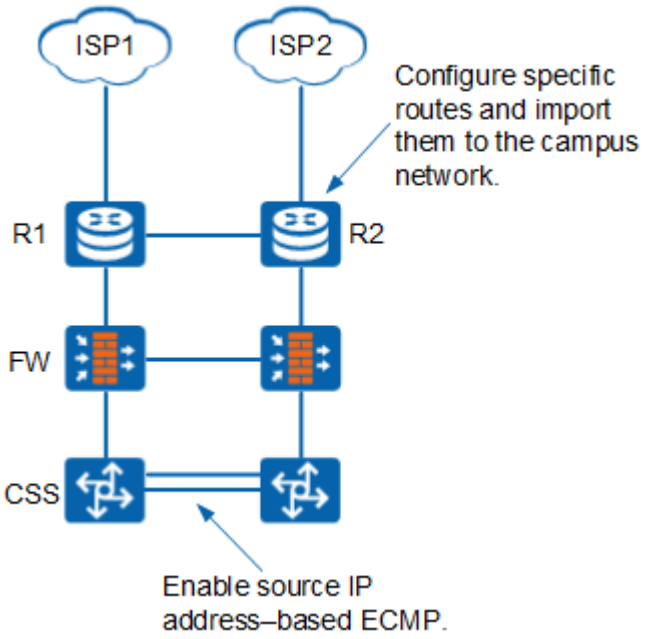
At the network egress, it is recommended that active/standby NGFWs (or high-end routers such as NE devices) be deployed based on Huawei Redundancy Protocol (HRP) and Virtual Router Redundancy Protocol (VRRP) technologies. Active/standby backup (load balancing) is implemented based on dual homing, improving egress device reliability.



Load Balancing

The bandwidth utilization of Internet links at the egress and the actual user experience need to be considered. Assume that the access traffic is destined for ISP1. If the traffic is forcibly

load-balanced on the link of ISP2, the link bandwidth utilization is seemingly even; however, user experience is poor because the data packets need to be routed back from the Internet to ISP1.



The design roadmap for load balancing is as follows:

- After routing protocols are deployed at the egress, two equal-cost default routes are generated on the CSS. You can enable the source IP address–based equal-cost multi-path routing (ECMP) function on the CSS for evenly sending data flows to the two links. After this function is enabled, the CSS sends packets with the same source IP address to the same firewall, ensuring consistent incoming and outgoing paths.
- User experience needs to be considered. Besides default routes on the egress router, you can also configure specific routes and import them into the internal routing domain of the campus network. For example, if services on the network segment 1.1.0.0/16 are in the ISP IDC, you can configure a specific route of 1.1.0.0/16 on R1 and import the specific route to the internal routing domain. After multiple known specific routes are imported, users can access most of the mainstream services through the optimal path, which greatly improves user experience.

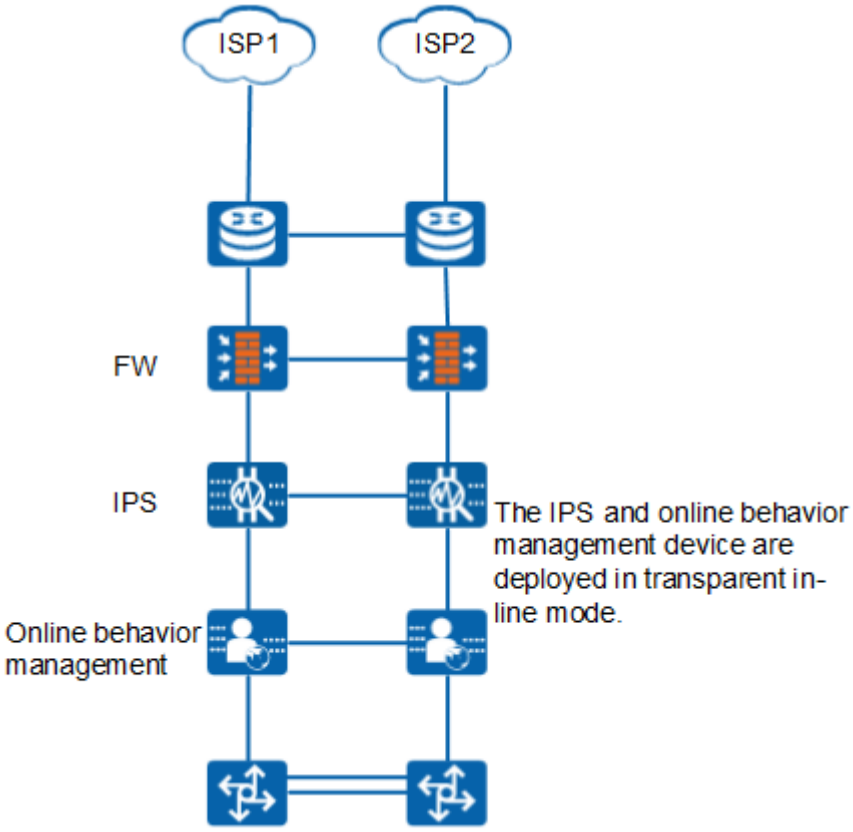
Egress Security

Internet egress security design ensures secure access of campus users to the Internet and allows traveling users to securely access the campus network.

The following is the design roadmap for egress security:

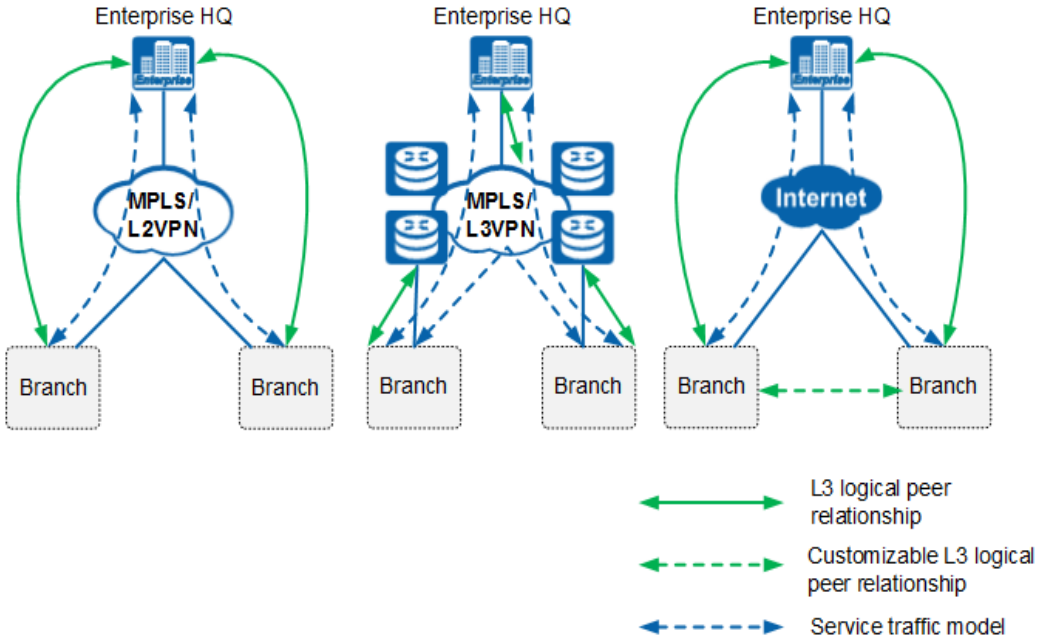
- If a single device is enabled with multiple functions, the device performance may deteriorate. For this reason, it is recommended that security functions be deployed on dedicated devices.
- The IPS is deployed to prevent attacks from external networks, and an online behavior management device is deployed to manage users' online behaviors and control network traffic.

- It is recommended that the IPS and online behavior management device connect to the network in transparent in-line mode to simplify the logical topology of the egress. In addition, an IPS policy must be applied to the direction in which the access is initiated.
- The bypass or HSB function can be enabled to ensure normal traffic forwarding when the IPS and online behavior management device are faulty. The HSB function is recommended, so that the IPS and online behavior management device on the other link can take over corresponding security functions. The bypass function and HSB cannot be enabled together.



3.4.4.2 Branch Access

The logical topology and traffic model of branches vary according to the bearer links between branches, as shown in the following figure.

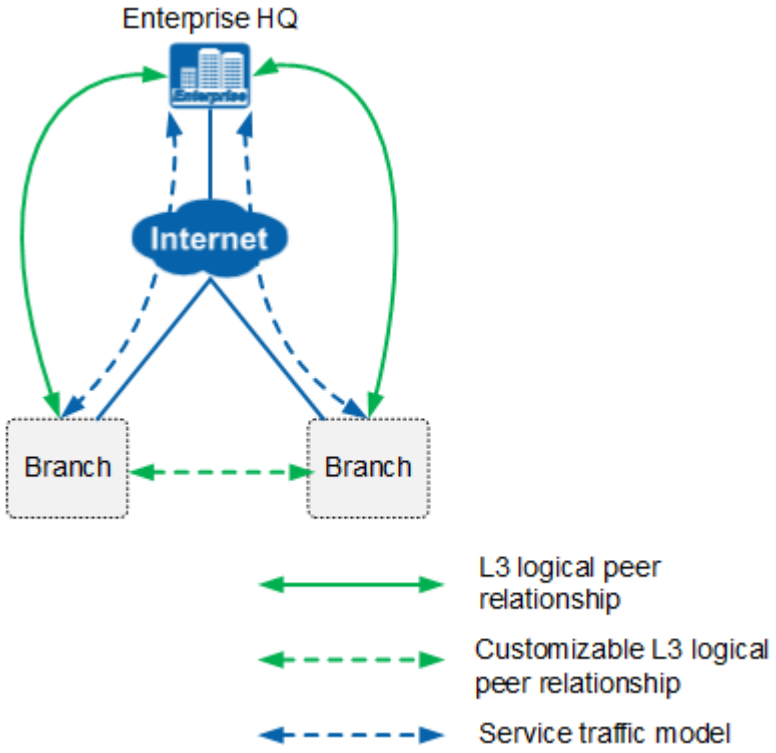


- L2VPN/MPLS: Layer 2 links are used as bearer links and are unaware of the service routes of the campus network. Generally, a tree structure with the Hub deployed at the headquarters is used. The Hub needs to maintain multiple logical links. Communication traffic between branches traverses the headquarters. When L2VPN/MPLS bearer links are used, an IP layer peer relationship is set up between campus and branch egress devices. This deployment mode provides the highest autonomy and ensures good link quality. Additionally, it does not leak routing entries to the ISP, ensuring high security.
- MPLS L3VPN: The ISP needs to obtain the routing entries of an enterprise and transfers these routes for the enterprise. The enterprise headquarters and branches are leaf nodes in a star topology. The headquarters needs to maintain only one logical link. Communication traffic between branches does not need to traverse the headquarters. An IP layer peer relationship is set up between enterprise network border devices and ISP border devices. This deployment mode ensures good link quality and enables convenient maintenance. During the communication between branches, the ISP helps select the optimal link.
- Internet: Instead of transmitting enterprise routing entries, the Internet encapsulates the public IP address before transmitting packets. An enterprise uses the Internet as a Layer 3 overlay link. Each branch needs to define their own logical relationships. Generally, IPSec VPN tunnels are established between the headquarters and branches. To optimize direct communication between branches, deploy DSVPN at the headquarters to dynamically establish IPSec VPN tunnels between branches. An IP layer peer relationship is established between campus and branch egress devices. This deployment mode features low cost and wide coverage. However, the maintenance workload on the enterprise side is heavy and the link quality is poor.

It is recommended that Layer 2 or Layer 3 leased lines be used as the primary bearer links and Internet links be used as backup bearer links.

If two links of different types are required to transmit data simultaneously, you are advised to deploy the same routing protocol on the two links to facilitate traffic adjustment. In this case, you are advised to establish a logical Layer 3 peer relationship between devices at both ends of the enterprise network through a protocol such as GRE and use static routing or BGP as the routing protocol.

Additionally, when the Internet is used as the bearer link for branch interconnection, DSVPN can be deployed to simplify configuration, dynamically establish tunnels between branches, and optimize the traffic model for branch communication.



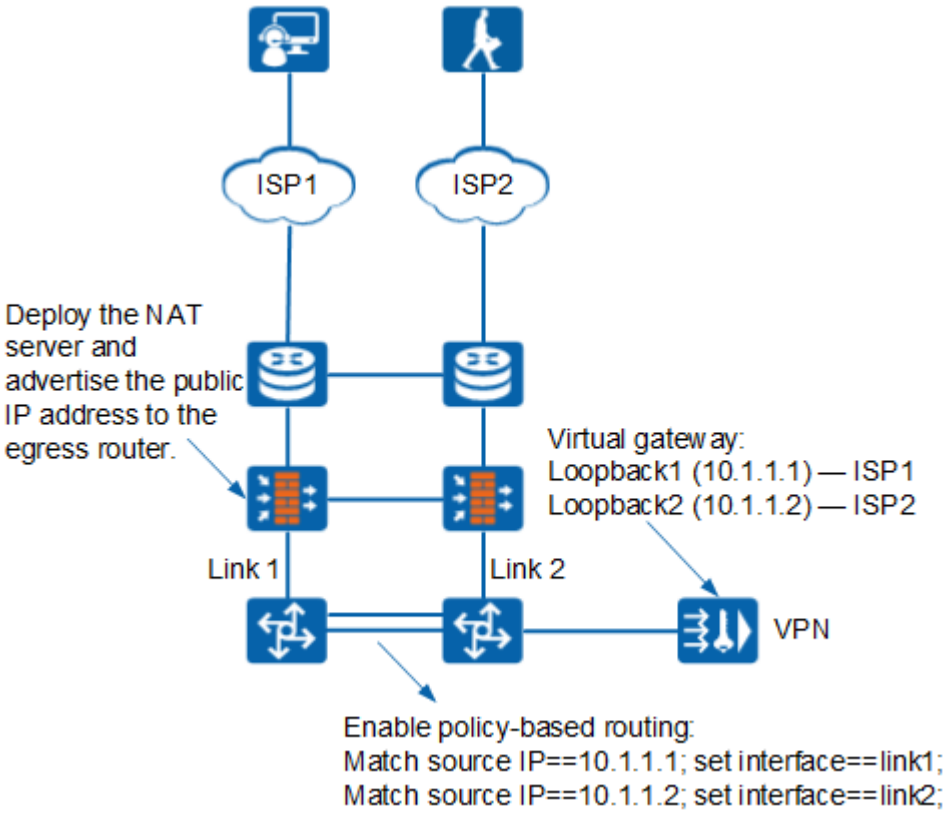
DSVPN deployment suggestions:

- GRE tunnels are deployed at branches and are automatically registered with the headquarters.
- If the number of branches is small, non-shortcut mode can be used. A branch learns all routing entries from the headquarters and other branches. In this way, the branch can directly send an NHRP Resolution Request packet to the headquarters to obtain the public IP address corresponding to the tunnel of the peer branch.
- If there are a large number of branches and the branch router has limited performance, shortcut mode can be used. A branch learns only the summarized routes from the headquarters. Upon branch communication, the first packet is sent to the headquarters to trigger NHRP redirection, and then the branch sends an NHRP Resolution Request packet to obtain the public IP address corresponding to the tunnel of the peer branch.
- Generally, an enterprise adds OSPF routes to the GRE tunnel. In this case, set the DR priority of the branch tunnel interface to 0 so that the interface does not participate in DR election.
- If the traffic traverses the Internet, IPSec over DSVPN needs to be configured. To implement this, deploy an IPSec policy on the GRE tunnel interface so that an IPSec tunnel is established when a GRE tunnel is set up.

3.4.4.3 Traveling User Access

Generally, VPN devices can be deployed on the enterprise intranet to allow traveling users to access intranet resources through the Internet. The SSL VPN is recommended. If terminals of

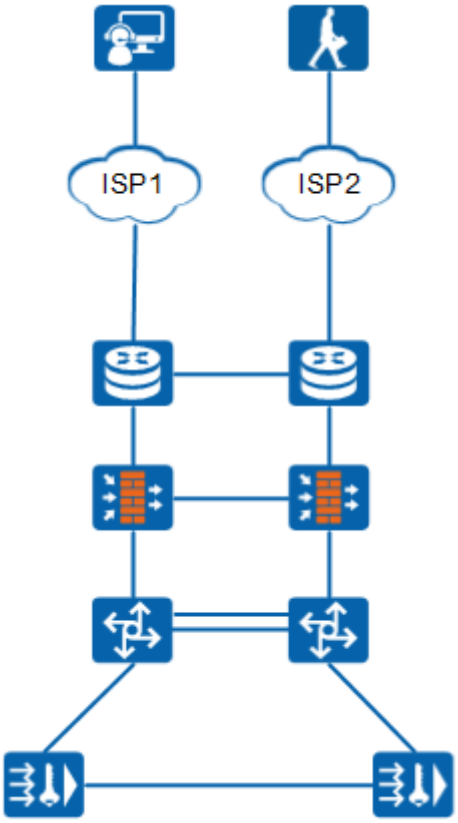
traveling users do not support the SSL VPN client, L2TP over IPSec can be deployed on VPN devices to provide access capabilities.



The followings are some deployment suggestions:

- A VPN device is connected to the core switch in bypass mode. A traveling user accessing the intranet through the VPN device has the same access permissions as intranet users.
- If a single VPN device is deployed, the loopback address can be used as the virtual gateway IP address for the VPN device. If Internet links of multiple ISPs exist, you are advised to configure a loopback address for each ISP link. The link backup function of the virtual gateway is enabled to optimize the access bandwidth for traveling users.
- The SSL VPN is deployed to enable network expansion. The VPN device advertises network segments in the user address pool for traveling users, so that the traffic from the core switch to the user network segment of the VPN device can be forwarded normally.
- The NAT server is deployed on the firewall to implement NAT mapping for multiple IP addresses of the virtual gateway. In addition, the public IP address segment of the NAT server must be advertised to the egress router for proper routing.
- Policy-based routing (PBR) is enabled on the core switch cluster for Internet-to-SVN traffic. Traffic is diverted to the egresses of the two ISPs based on the virtual gateway IP addresses to ensure simple NAT server mapping on the firewall.

For higher reliability, VPN HSB can be deployed.



The followings are some suggestions on deploying VPN HSB:

- The VRRP address is specified as the virtual gateway IP address on the VPN devices. The HSB function and HRP automatic backup mechanism are enabled on the VPN devices.
- If OSPF is deployed between VPN devices and core switches, the two VPN devices advertise the network segment for traveling users, and the standby SVN device automatically increases the cost of the network segment and advertises it.
- If static routing is deployed between VPN devices and core switches, the core switches need to specify a static route destined for the network segment of traveling users and with the VRRP address of the VPN devices as the next-hop address.

3.4.5 Wireless Network

A wireless local area network (WLAN) is a network that uses wireless channels such as radio waves, laser, and infrared rays to replace the transmission media used on a wired LAN. The WLAN technology described in this document is implemented based on 802.11 standards. That is, a WLAN is a network that uses high-frequency signals (for example, 2.4 GHz or 5 GHz signals) as transmission media.

WLANs can provide wireless access services for users anytime and anywhere, and have the following advantages:

- High network mobility: WLANs are easily connected, and are not limited by cable and port positions. This makes WLANs great for scenarios where users are often moving, such as in office buildings, airport halls, resorts, hotels, stadiums, and cafes.
- Flexible network deployment: WLANs provide wireless network coverage in places where cables are difficult to deploy, such as subways and highways. WLANs reduce the

number of required cables, offer low-cost, simplify deployment, and have high scalability.

Different from wired network planning and design, wireless network planning and design require site survey and network planning to ensure the expected signal coverage. The following describes the major concerns during wireless network planning and design. For details about the survey and network planning in different scenarios, see the following documents:

- **Engineering survey and network planning video**
- **WLAN Site Survey Guide**
- **WLAN Scenario-based Pre-sales Network Planning Checklist**
- **WLAN Network Planning & Installation Notice**
- **WLAN Outdoor Network Planning Guide**
- **WLAN Indoor Settled Network Planning Guide**
- **WLAN Indoor Distributed Network Planning Guide**

3.4.5.1 Requirement Survey

Table 3-13 describes the key points during wireless network design.

Table 3-13 Wireless network requirements

Requirement	Key Point of Requirement Survey	Key Point of Requirement Analysis
Network scale	● Number of wireless users and number of terminals per user ● Number of access terminals of different types, such as laptops and mobile phones	Determine the network scale and device model.

Requirement	Key Point of Requirement Survey	Key Point of Requirement Analysis
Branch network	● Whether branch networks exist ● Number of wireless users and number of terminals per user on each branch network ● Whether unified authentication and control are required for branch users	Determine the models of ACs of branch networks and deployment of the ACs.
Traffic security	● Network construction or reconstruction ● Whether wired traffic and wireless traffic need to be managed separately	Determine the forwarding model.
SSID	● Service to be isolated ● Whether a guest network needs to be designed separately	Determine the SSIDs and VLANs.

Requirement	Key Point of Requirement Survey	Key Point of Requirement Analysis
Guest management	● Whether the campus network has the wireless guest access requirement ● Whether guest login accounts need to be managed in centralized mode	Determine the guest access solution.
Authentication mode	● Whether employees are allowed to connect to the network using their own smart phones and tablets ● Whether employees' terminals for office work need to be authenticated for security	Determine the authentication solution.
User roaming	● Whether to support user service roaming ● Service roaming zone ● Whether the traffic of roaming users is forwarded locally	Determine whether the roaming is at Layer 2 or Layer 3, and whether the roaming is intra-AC or inter-AC; determine whether to enable the home agent function when some roaming traffic is forwarded locally.

Requirement	Key Point of Requirement Survey	Key Point of Requirement Analysis
Bandwidth requirement	● Bandwidth required by each terminal ● Number of concurrent online users within the campus ● Whether there are VIP users with preferential access and preferential forwarding	Design the bandwidth throughput. Design wireless QoS.
Coverage mode	● Whether the indoor environment is open or deployed with many obstacles ● How large the outdoor coverage area is, whether it is convenient for cabling, and whether multi-hop AP backhaul is required	Select the AP model. Determine whether wireless backhaul is required outdoors.
Coverage requirement	● Major coverage areas and secondary coverage areas ● Whether high-density coverage is required, such as in libraries and stadiums	Design coverage.

Requirement	Key Point of Requirement Survey	Key Point of Requirement Analysis
Power supply mode	PoE switch or PoE adapter	Design the layout.
Decoration requirement	Determine the installation mode of APs, such as ceiling-mounted, wall-mounted, or pole-mounted, hidden or exposed, and whether extra paint is required.	Design the installation mode.

3.4.5.2 Networking Architecture

WLAN networks can be deployed in different modes according to customer requirements. The following two WLAN network architecture models are available:

- Autonomous architecture (Fat AP)
- Centralized architecture (Fit AP)

The following table shows the comparison between the autonomous architecture and the centralized architecture.

Table 3-14 Comparison between the autonomous architecture and centralized architecture

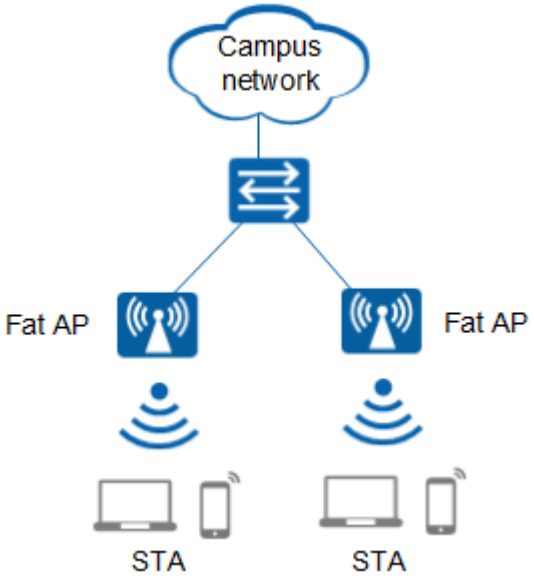
Item	Autonomous Architecture	Centralized Architecture
Application scenario	Mini enterprises and individuals	Large, medium-sized, and small enterprises
Network management	Independent configuration on each AP, with configuration files loaded	Uniform configuration on an AC and zero configuration on APs, simple maintenance
User management	User rights controlled based on wired interfaces of APs, similar to user management on a wired network	User group based management: user rights controlled based on user names, more flexible

Item	Autonomous Architecture	Centralized Architecture
WLAN scale	Layer 2 roaming, applicable to small-scale networks	Layer 2 and Layer 3 roaming, topology independent, applicable to large-scale networks
Value-added services	Simple data access	Abundant services

Autonomous Architecture

As shown in **Figure 3-18**, fat APs are used to implement all wireless access functions, and no AC is required.

Figure 3-18 Autonomous networking architecture

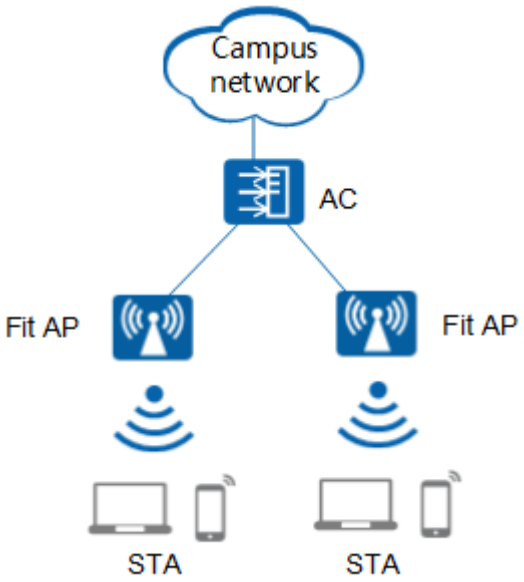


The autonomous architecture was widely applied on WLANs in early days. With an increasing number of APs being deployed, AP configuration and software upgrade bring high costs for operation and management. Therefore, this architecture is used in fewer applications now.

Centralized Architecture

This architecture uses ACs to manage APs, as shown in **Figure 3-19**.

Figure 3-19 Centralized networking architecture



In centralized architecture, APs work with an AC to implement wireless access.

- The AC implements functions including mobility management, identity verification, VLAN assignment, radio resource management, and wireless Intrusion Detection System (IDS) and data packet forwarding.
- APs control air interfaces, including radio signal transmission and detection response, data encryption and decryption, data transmission acknowledgement, and data priority management.

The AC and APs communicate through the Control and Provisioning of Wireless Access Points (CAPWAP) tunnel. They can be directly connected or connected across a Layer 2 or Layer 3 network.

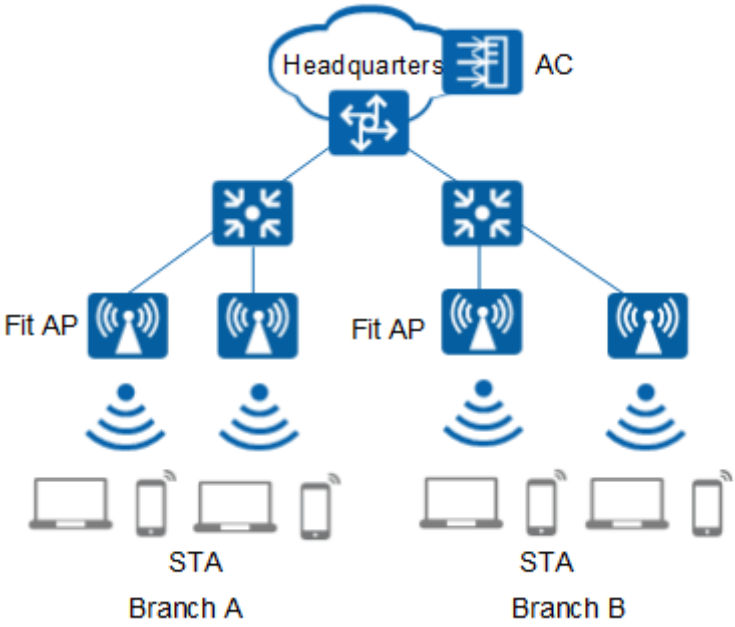
The centralized architecture is the mainstream architecture of enterprise networks and carriers because it allows centralized management, authentication, and security management. The centralized architecture solution is the main enterprise solution.

The centralized network architecture can be divided into the following types:

- The AC can be deployed in centralized or distributed mode.

  In the centralized AC deployment mode, independent ACs are deployed to manage APs on the entire network. An AC can be deployed in chain mode (between an AP and an aggregation or a core switch) or in branched mode (the AC is connected to only the aggregation or core switch), as shown in **Figure 3-20**.

Figure 3-20 Centralized AC deployment



In distributed AC deployment mode, multiple ACs are deployed in different areas to manage APs. This mode integrates AC functions on an aggregation switch to manage all the APs connected to the aggregation switch, without using an independent AC, as shown in **Figure 3-21**.

Figure 3-21 Distributed AC deployment

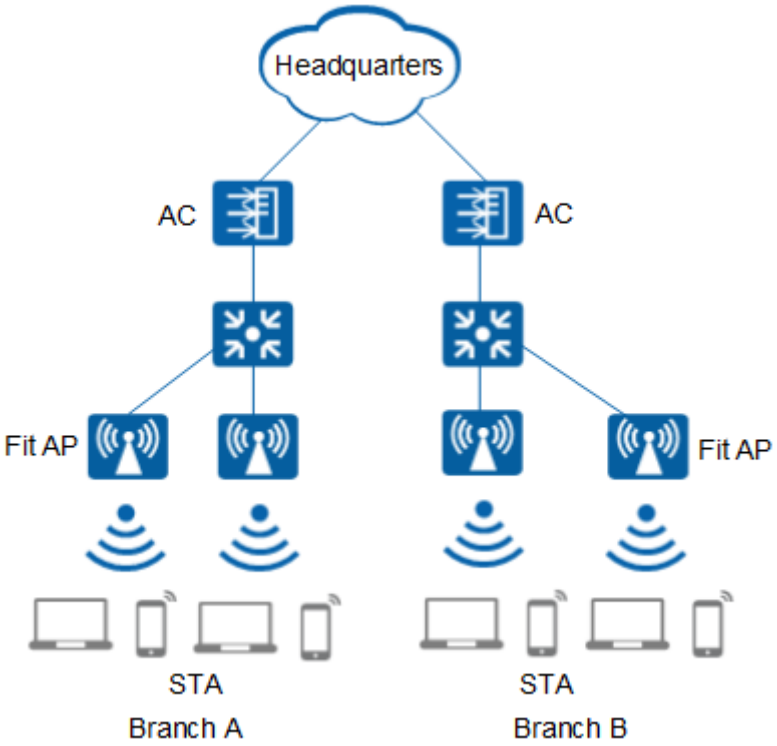


Table 3-15 provides a comparison between centralized AC and distributed AC deployment modes.

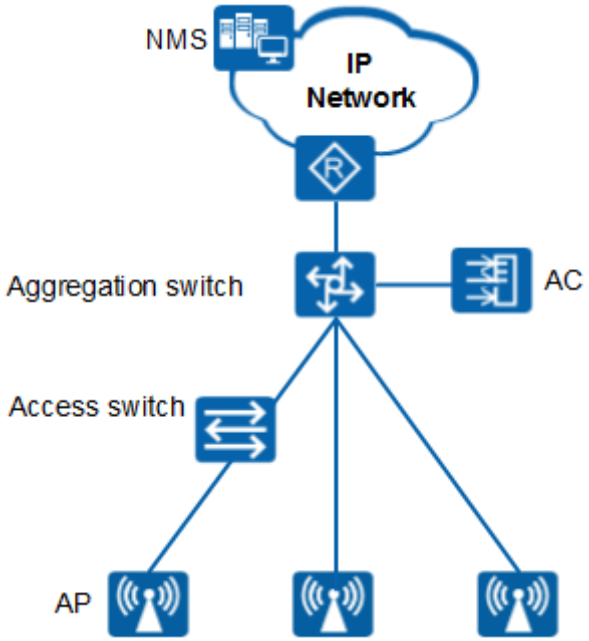
Table 3-15 Centralized AC and distributed AC comparison

AC Deployment Mode	Advantage	Disadvantage
Centralized mode	● Reduces investment costs. ● Simplifies capacity management. ● Facilitates management because fewer wireless service termination points are required. ● Simplifies deployment for roaming between APs. ● Simplifies O&M and management, and allows for centralized management and flexible configuration.	Network deployment between the AC and AP is complex.
Distributed mode	Network deployment between the AC and AP is simple.	● High CAPEX ● Requires roaming between ACs unless roaming is not required. ● High O&M cost

- The AC can be deployed in branched or chain mode based on the AC deployment location.

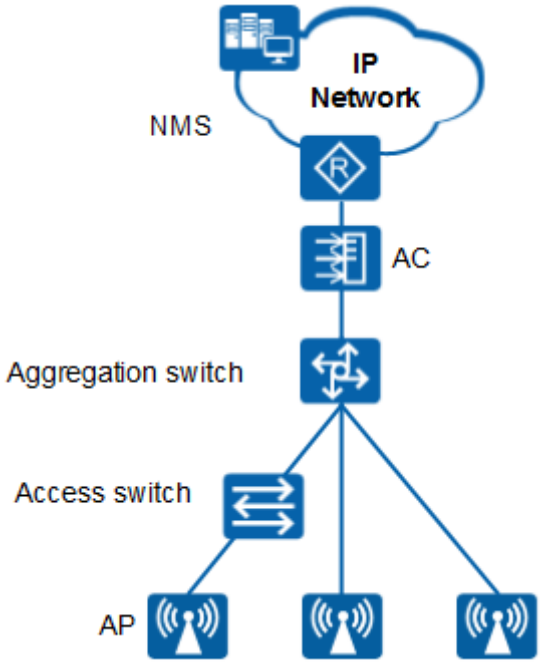
  In branched mode, an AC is deployed at the side of a user gateway (aggregation or core switch) to manage all the APs connected to the user gateway, as shown in Figure 3-22. This mode applies to networks using non-Huawei aggregation/core devices. This mode is mainly applicable for network reconstruction or construction of medium- and large-sized campus networks.

Figure 3-22 AC branched networking



In chain mode, an AC is deployed between an AP and a user gateway (aggregation or core switch) to manage all the APs, as shown in **Figure 3-23**. This mode applies to new small- and medium-sized campus networks or existing networks using Huawei aggregation or core devices.

Figure 3-23 AC chain networking



- Based on the AC hardware type, two types of ACs are available: independent AC, integrated AC (subcard AC), and native AC.

  The independent AC solution uses a hardware AC connected to a gateway in chain or branched mode to manage all the APs. For example, AC6605.

The integrated AC solution uses an integrated AC card or module on a switch but not an independent AC to manage all the APs connected to the switch. For example, ACU2 (installed in the S7700, S9700, and S12700 switches) and AR series routers (with native AC deployed).

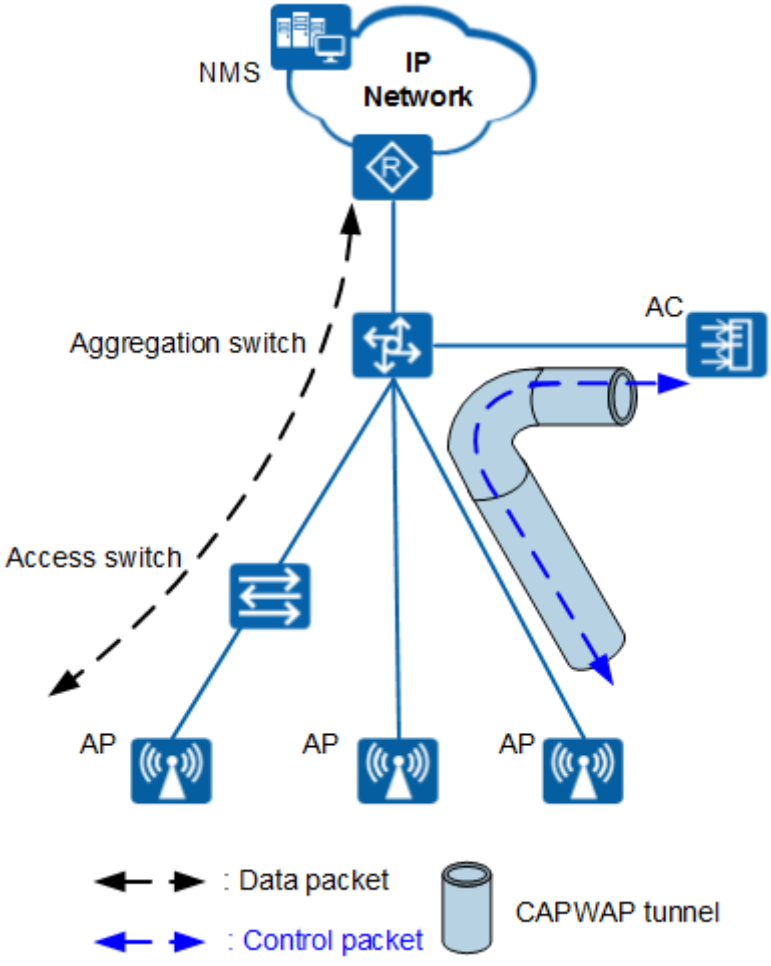
The native AC solution uses a built-in T-bit native AC on an agile switch to implement wired and wireless service integration. For details, see **Wired and Wireless Integration Design**.

- Services can be forwarded in local or centralized mode.

  The forwarding mode determines the way in which APs process service data.

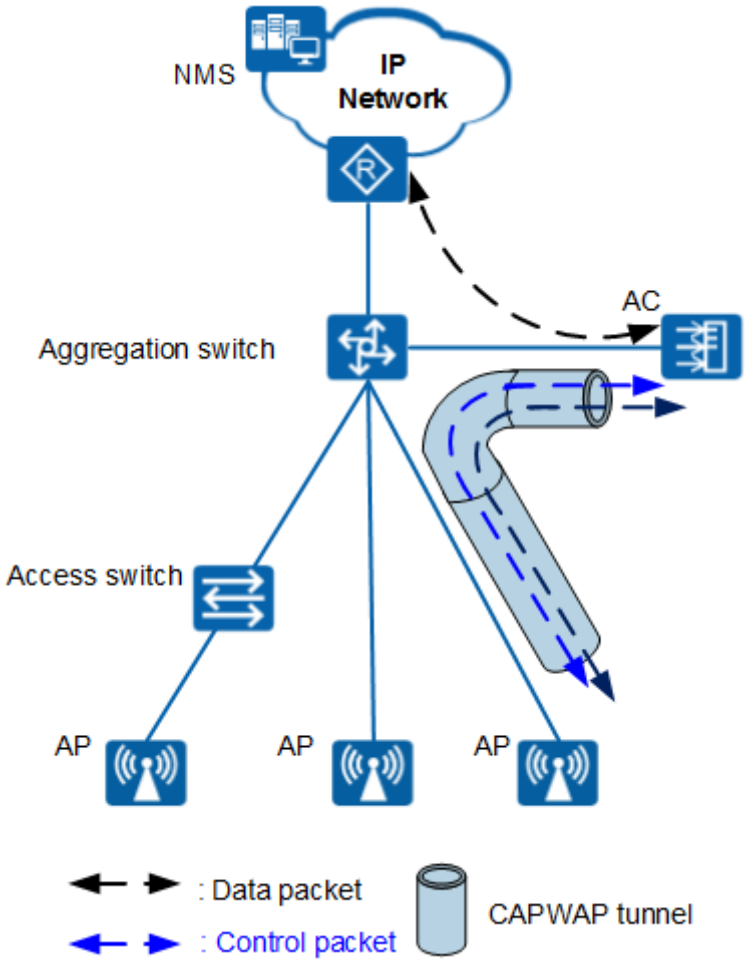
  Local forwarding is also called direct forwarding. APs directly forward data streams to the upper layer, but do not forward it to the AC. AC is only responsible for AP management. Management streams are encapsulated in a CAPWAP tunnel and sent to the AC, as shown in **Figure 3-24**.

Figure 3-24 Local forwarding networking



Centralized forwarding of data packets is also called tunnel forwarding. In this mode, data packets are encapsulated on an AP and sent to the AC. The AC performs AP management and forwards all traffic sent from APs. Management streams and data streams are encapsulated in a CAPWAP tunnel and sent to the AC, as shown in **Figure 3-25**.

Figure 3-25 Centralized forwarding networking



The recommended forwarding modes are as follows:

- The local forwarding mode is recommended for new networks. This forwarding mode improves network performance because data traffic does not pass through the ACs.
- The centralized forwarding mode is recommended for networks where capacity expansion is required. This forwarding mode implements fast deployment because the live network topology and configurations are not changed.
- The hybrid forwarding mode is recommended for scenarios where the headquarters connect to branches across WANs.

Table 3-16 shows a comparison among the preceding forwarding modes.

Table 3-16 Comparison among forwarding modes

Forwarding Mode	Application Scenario	Advantage	Disadvantage
Centralized forwarding	● Applies to scenarios where the AC is responsible for user policy management, and is required to act as the user gateway, authentication and accounting gateway, and DHCP server. ● The AC processes user data and authenticates users in a centralized manner. ● Both APs and ACs support Layer 2 and Layer 3 networking.	An AC forwards all data packets, ensuring security and facilitating centralized management and control.	Service data must be forwarded by an AC, reducing packet forwarding efficiency and burdening the AC.
Local forwarding	● Applies to scenarios where user data can be directly forwarded by the local network, for example, branch networks, saving the link bandwidth between the AC and the AP. ● The user gateway and DHCP server are on the local network. ● Users can be authenticated by an AC in a centralized manner. ● Both APs and ACs support Layer 2 and Layer 3 networking.	Service data does not need to be forwarded by an AC, improving packet forwarding efficiency and reducing the burden on the AC.	Service data is difficult to manage and control in a centralized manner.
Hybrid forwarding	● Applies to both local and centralized forwarding modes, in which data can be forwarded by AP or SSID. For example, the headquarters uses centralized forwarding, and the branch networks use local forwarding. ● User authentication in both modes is centrally performed by the AC. ● Both APs and ACs support Layer 2 and Layer 3 networking.	● Service data does not need to be forwarded by an AC, improving packet forwarding efficiency and reducing the burden on the AC. ● The network bandwidth between the branch network and the headquarters is reduced.	Branch service data is difficult to manage and control in a centralized manner.

3.4.5.3 AP Coverage

Coverage Design Principles

Table 3-17 lists the field strength requirements for coverage areas to ensure good roaming experience.

Table 3-17 Field strength requirements

Coverage Area	Field Strength	Typical Area in Common Projects
Major coverage area	-40 to -65 dbm	Dorm room, library, classroom, hotel room, lobby, meeting room, office, and hall
Common coverage area	> -75 dbm	Corridor, kitchen, storeroom, and dressing room
Special coverage area	NA	Area that is specified or does not allow coverage or installation because of service security or property management

If customers do not have specific field strength requirements and do not consider interference or obstacles, it is recommended that the coverage radius of an AP be 20 m. If there are obstacles, the radius should be reduced.

Table 3-18 describes the relationship between the signal attenuation and transmission distance:

Table 3-18 Relationship between transmission distance and signal attenuation in different frequency bands

Distance	1m	2m	5m	10m	20m	40m	80m	100m
2.4GHz	46dB	53.5dB	63.5dB	71dB	78.5dB	86dB	93.6dB	96dB
5.8GHz	53dB	62dB	74dB	83dB	92dB	101dB	110.1dB	113dB

Table 3-19 lists the signal attenuation caused by obstacles.

Table 3-19 Signal attenuation caused by obstacles

Obstacle	Width (mm)	Signal attenuation at 2.4 GHz (dB)	Signal attenuation at 5 GHz (dB)
Asbestos	8	3	4
Wooden door	40	3	4
Glass window	50	4	7
Colored glass	80	8	10
Brick wall	120	10	20
Brick wall	240	15	25
Bulletproof glass	120	25	35
Concrete	240	25	30
Metal	80	30	35

NOTE

The values of signal attenuation caused by obstacles listed in the preceding table are empirical and for reference only. The actual tested signal attenuation values prevail.

The formula for calculating the signal strength is as follows (regardless of factors such as interference and line loss):

Received signal field strength = AP's transmit power + Antenna gain – Transmission attenuation – Penetration loss

Theoretically, when the signal transmission distance is 20 m, the signal strength (5.8 GHz) can be obtained from the following formula:

AP transmit power (20 dBm) + Antenna gain (3 dBi) – Transmission attenuation (92 dB) – Signal attenuation caused by obstacles (0 dB) = -69 dBm

In addition, AP coverage distance is also determined by Effective Isotropic Radiated Power (EIRP). EIRP values vary with countries, frequency bands, and channels. The outdoor coverage capability is heavily restricted by EIRP. In France, the EIRP value is 20 dBm for 2.4 GHz channels (1-13). In the 5 GHz frequency band, available indoor channels are 36, 40, 44...64, 100, 104, 108...140, and available outdoor channels are 100, 104, 108...140. The EIRP value for all 5 GHz channels is 23 dBm.

The relationship between EIRP, transmit power, and antenna gain is shown as the following:

AP transmit power + antenna gain + MIMO gain ≤ EIRP

The formula for calculating the MIMO gain is as follows:

When a single-stream STA connects to a multi-stream AP, the MIMO gain is obtained. The dual-stream gain is 3 dB, and the triple-stream gain is 5 dB. However, when a multi-stream STA connects to the corresponding number of multi-stream APs, there is no MIMO gain.

When EIRP is calculated, the MIMO gain is calculated using its maximum value, regardless of the actual gain of STAs. Therefore, when the MIMO gain is the same as the antenna gain,

the AP transmit power is affected by EIRP and the coverage distance of the AP is affected too.

3.4.5.4 Terminal Bandwidth

Table 3-20 lists the bandwidth requirements of typical applications on the live network. Typically, the video bandwidth requirement is 500 kbit/s, and the bandwidth requirement for other applications is 250 kbit/s.

Table 3-20 Bandwidth requirements of typical applications

Application	Rate Requirement
Web page browsing	160 to 400 kbit/s
Video stream	280 to 560 kbit/s
Instant messaging	32 to 64 kbit/s
Email	400 kbit/s
Social services	200 kbit/s
VoIP	256 kbit/s
Gaming	200 kbit/s

For example, a stadium plans to build a WLAN for users to browse web pages, access social networks and upload pictures, and browse videos.

Assume that 40% of users browse web pages, 40% of users use SNSs, and 20% of users browse videos. Based on the bandwidth requirements as shown in Table 3-20, the average bandwidth is calculated using the formula: Bandwidth = 400 kbit/s x 40% + 200 kbit/s x 40% + 500 kbit/s x 20% = 340 kbit/s.

The number of allowed concurrent users is reduced when the user access bandwidth is increased. Table 3-21 lists the recommended number of concurrent terminals for a single terminal (one spatial stream) when different access bandwidths are required.

Table 3-21 Recommended numbers of concurrent terminals under different access bandwidths

User Bandwidth (Mbit/s)	Recommended Number of Concurrent Terminals in Single-Band Mode (One/Two Spatial Streams)	Recommended Number of Concurrent Terminals in Dual-Band Mode (One/Two Spatial Streams)
8	5/10	9/18
6	6/11	11/20

User Bandwidth (Mbit/s)	Recommended Number of Concurrent Terminals in Single-Band Mode (One/Two Spatial Streams)	Recommended Number of Concurrent Terminals in Dual-Band Mode (One/Two Spatial Streams)
4	8/12	15/22
2	12/22	22/40
1	20/30	35/55

Table 3-22 lists the number of concurrent terminals (in single-band mode) and bandwidth attenuation for a single terminal (one spatial stream).

Table 3-22 Number of concurrent terminals (in single-band mode) and bandwidth attenuation for a single terminal (one spatial stream)

Number of Users	Uplink Bandwidth (Mbit/s)	Downlink Bandwidth (Mbit/s)
1	45	45
5	7	8
10	3.5	4
15	1.5	2
20	0.5	1
25	0.25	0.5

NOTE

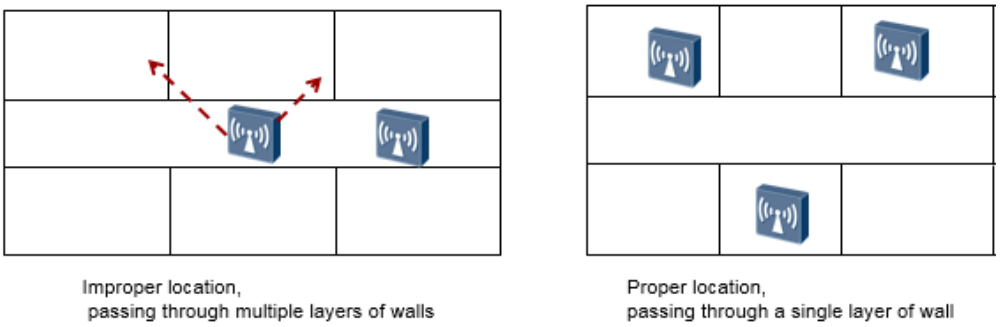
The above values are applicable to scenarios where customers do not have specific bandwidth requirements.

As shown in the preceding table, the bandwidth does not decrease with the increase of the number of users. For example, when one user accesses the network, the bandwidth is 45 Mbit/s. If five users access the network at the same time, the bandwidth of each user is 8 Mbit/s, and the total bandwidth of the five people is 40 Mbit/s.

3.4.5.5 Deployment

AP Deployment Guidelines

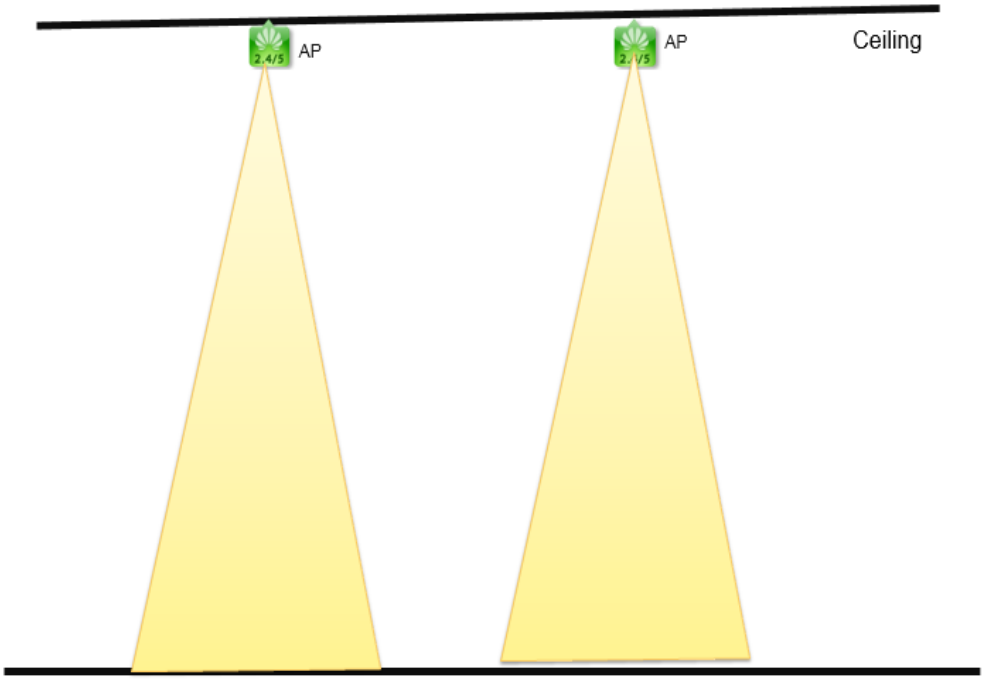
- When installing an AP, try to reduce the number of obstacles that signals traverse.



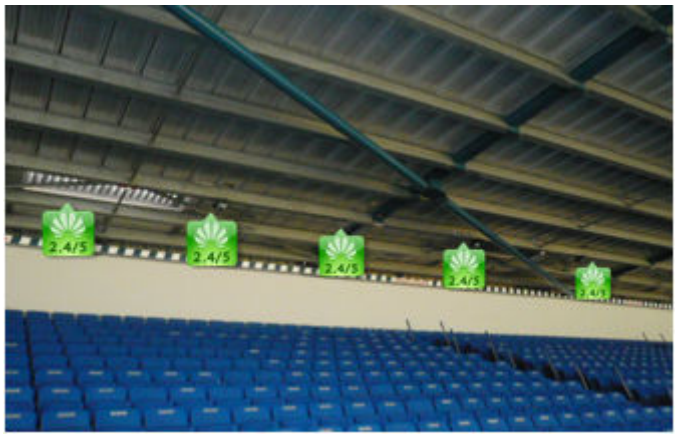
- Ensure that APs and antennas face the target coverage area.
- Deploy APs far away from interference sources, including non-Wi-Fi co-channel interference devices such as carriers' base stations, microwave ovens, wireless cameras, and other Wi-Fi interference devices.

Best Practices for AP Deployment

- For large-scale exhibition venues, conference rooms, or stadiums, ceiling-mounted installation is recommended.

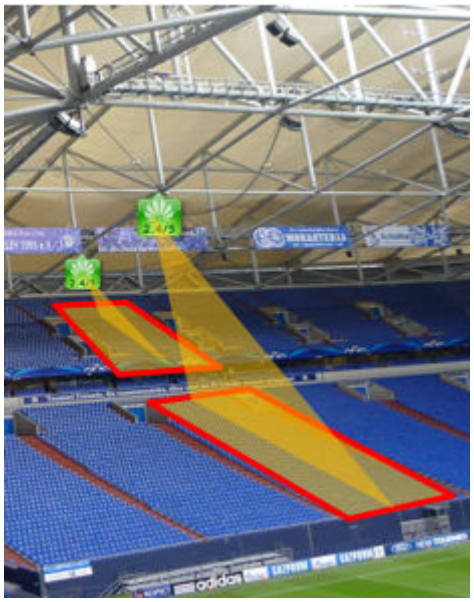


In ceiling-mounted installation mode, an AP is usually installed at a height of about 4 to 6 meters above the last row of seats. The installation is unified and the cabling is convenient, as shown in the following figure.



This mode is recommended because it ensures line of sight transmission between STAs and APs and achieves controllable transmission attenuation. APs are deployed in a line, and co-channel APs are far away from each other, ensuring good anti-interference effect. In addition, the installation and maintenance costs are low. In most cases, the last row is close to the ceiling. When the installation position of APs is low, the audience may touch the APs. Proper camouflage is preferred, for example, hiding the APs behind billboards. If the stand is deep, APs can be installed in the pathway or on the above steel beam.

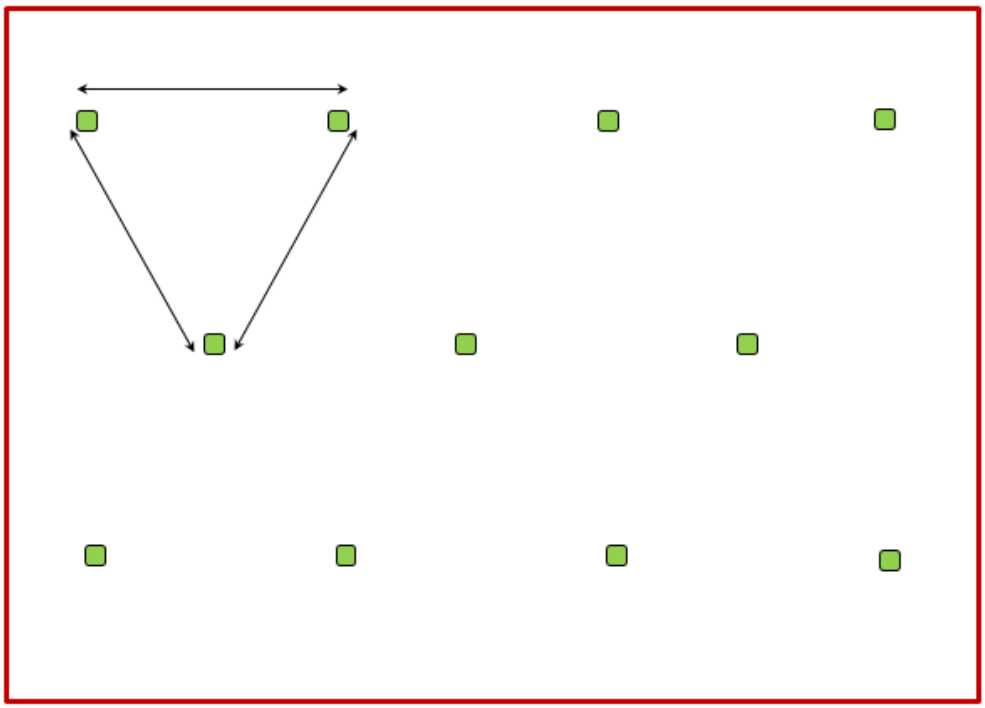
If there is no proper installation position above the last row or the customer does not agree to the installation mode, you can use the following deployment mode. APs are installed on the upper pathway (or steel beam) and face downward towards the seat area. Signals will not be blocked by human bodies, and the coverage effect is good. When an AP is installed at a height of 6 to 15 m, the 2.4 GHz and 5 GHz 30*30° antennas can be used. When the AP is installed at a height of 15 m or higher, the 2.4 GHz 18*18° and 5 GHz 15*15° antennas are recommended. In the channel planning, both the interference from left and right APs and the interference from front and back APs need to be considered. The anti-interference effect is not as good as that in ceiling-mounted installation mode.



- For common office scenarios, ceiling-mounted installation is recommended.

  It is recommended that settled APs be deployed in triangle mode. Based on common capacity requirements, it is recommended that the distance between APs be 15 to 18 m. If the capacity requirement is high, the recommended distance between APs is 12 to 15

m. If the capacity requirement is ultra-high, the recommended distance between APs is 10 to 12 m.



Indoor APs are evenly installed far away from the door. APs in the corridor must be placed at a distance of 3 m away from the office if solid masonry walls are used and 6 m if non-solid-masonry walls (made of gypsum boards or glass) are used.

Access Switch Deployment Guidelines

- An access switch is within 80 m apart from an AP connected to it. The distance is not a straight-line distance; instead, it is calculated according to the cable routing rules. In addition, reliable AC power supply is required.
- The access switches must be installed away from strong electromagnetic interference and be protected with moisture-proof and dust-proof measures (protection boxes can be purchased locally according to the environment).
- You need to determine the total number of APs that can be connected to a switch based on the number of ports on the switch, PoE power supply capability of the power module, and AP power consumption. (Pay special attention to the situation that outdoor APs consume large power.)

3.4.5.6 AP Channels

Available channels in each country or region are different. Some countries or regions may reserve some channels. Confirm the local available channels before performing network planning. For channels in different countries, see **Country Codes and Channels Compliance**.

Channel design guidelines:

- Plan working channels for APs properly to prevent interference from existing radio signals and thereby ensure WLAN access performance. In countries that support channels 1-13, channels 1, 6, and 11 are recommended when a few APs are deployed. If

there are many APs in the same area, channels 1, 5, 9, and 13 are recommended to increase the 2.4 GHz concurrency rate or reduce co-channel interference.

- Deploy APs as far as possible from other APs working at the same or adjacent channels to increase channel usage. In the case of multiple floors, avoid overlapping with channels of APs at the same or adjacent floors. If channel overlapping cannot be avoided, reduce AP power to minimize the overlapping areas.
- If 5G signals only need to cover small indoor areas, high-frequency channels at 5 GHz are recommended. To support access of more concurrent users, combination of high-frequency and low-frequency 5 GHz channels is recommended to ensure that at least one high-frequency 5G signal and one low-frequency 5G signal can be received in each area.

The following figures show the 2.4 GHz and 5 GHz channel design examples.

Figure 3-26 Channel design example – stand of a large-scale stadium

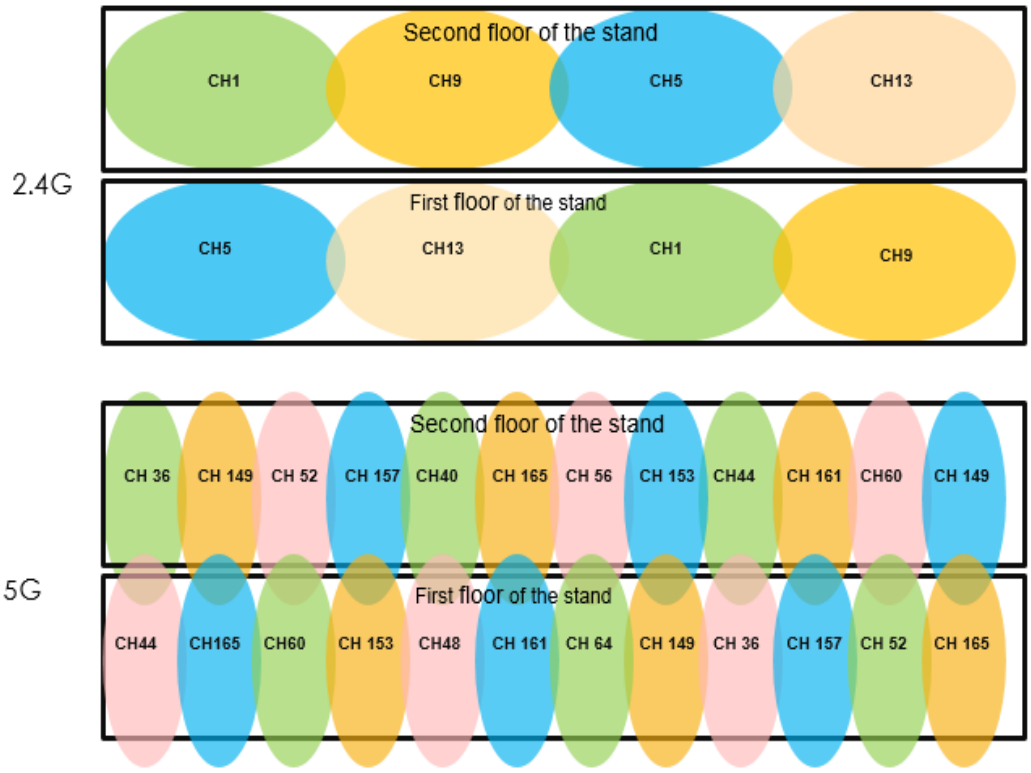


Figure 3-27 Channel design example – indoor AP

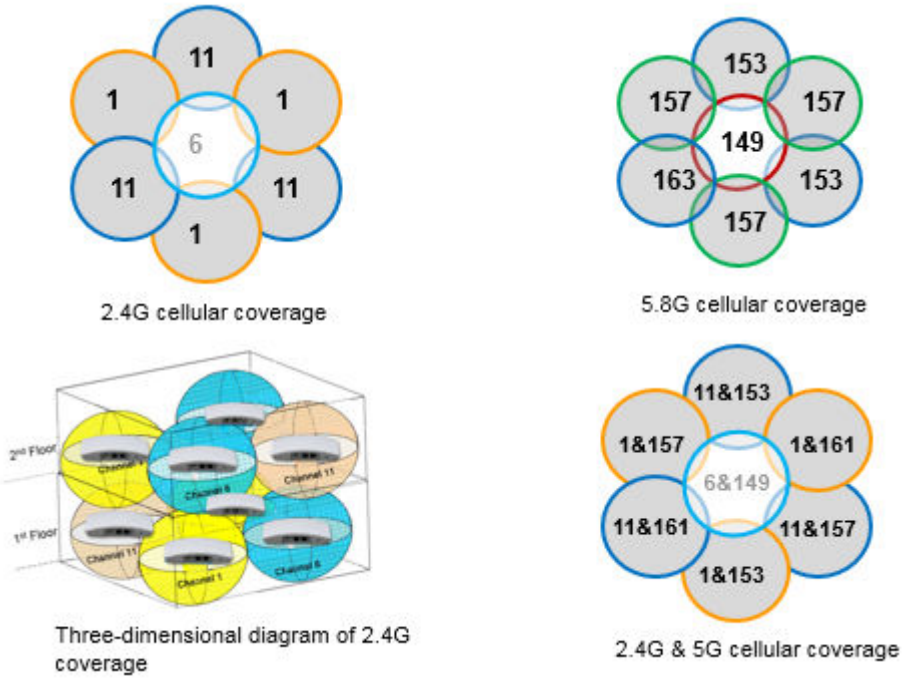


Figure 3-28 Channel design example – building

Floor	Three APs on One Floor		
7	1	6	11
6	11	1	6
5	6	11	1
4	1	6	11
3	11	1	6
2	6	11	1
1	1	6	11

3.4.5.7 AP Power Supply and Cabling

Power supply design guidelines:

- Power supply by a PoE device (recommended)

  When many APs are deployed, PoE devices power the APs and forward data packets sent from the APs to facilitate AP management and maintenance. Generally, PoE devices

include PoE switches, industrial switches, ARs, and ONUs. Industrial devices are installed outdoors and non-industrial devices must be installed in compliance with the installation requirements of power supply devices.

- Power supply by a PoE adapter

  If uplink switches do not support PoE power supply, and outdoor APs use optical fibers for data transmission or no AC power environment is available nearby, PoE adapters can be used to power the APs. In outdoor scenarios, PoE adapters must be installed in an equipment container or cabinet to meet the operating temperature, waterproof, and surge protection requirements. For APs with high power consumption (more than 12.95 W), PoE+ (30 W) power supply is required.

- Local AC power supply

  If uplink switches do not support PoE power supply, outdoor APs use optical fibers for data transmission, and AC power environment is available nearby, local AC power supply can be used to power the APs.

Cabling design guidelines:

- Ensure that the length of the network cable between an AP and a switch is no longer than 80 m, and 5 m is reserved for cable adjustment.
- Keep network cables as far as possible from strong electromagnetic field to prevent interference.
- Communicate with the customer about feasible cabling routes to ensure that cabling will not be affected by asset management or decoration requirements.

3.4.5.8 Device Model Selection

AC models are selected based on the application scenario, number of STAs, and number of site-surveyed APs. For details about device models, see **Table 1 Device model selection reference**.

Table 3-23 Device model selection reference

Device Model	Networking	Application Scenario
AC series	AC devices are connected to the core layer or aggregation layer in bypass mode.	Applies to small- and medium-sized campus networks or branch networks that support hybrid forwarding.
ACU2		Applies to large-sized campus networks or branch networks.
Native AC	Native AC is enabled on core switches.	Applies to wired and wireless unified authentication and unified management of small-, medium-, and large-sized campus networks or branch networks.

Device Model	Networking	Application Scenario
AR series	AR series devices are deployed at the location of egress routers.	Applies to small-sized campus networks or branch networks, and the number of network terminals is less than 100.

For details about recommended AP models and antenna models, see **WLAN Planning Quick Start**.

4 Reliability Design and Best Practices

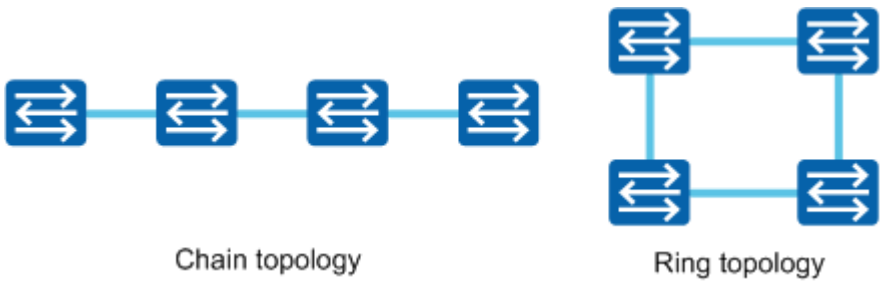
4.1 Access Layer Reliability

Reliability design of the access layer includes:

- Device reliability: Stacking of multiple devices must be supported. A single device must deliver carrier-grade reliability of 99.999% and provide dual power supplies and dual fan modules.
- Link reliability: It is reflected in the link design and networking mode. For example, multi-uplink technologies such as Eth-Trunk/LAG and dual-homing are used to increase link reliability.

Stack Design

Fixed switches can set up an iStack system using either of the following modes:



- Chain topology: The networking and management are simple. However, if one link fails, the stack system splits.
- Ring topology: High reliability is ensured. If one link fails, the stack system can still work. This topology requires an additional stack cable.

To achieve the best practice, you are advised to use ring connections. Typically, two devices are used for stacking. It is recommended that no more than five devices be stacked. In addition, stack members must be switches of the same series.

There are two stacking modes according to stack interfaces used.

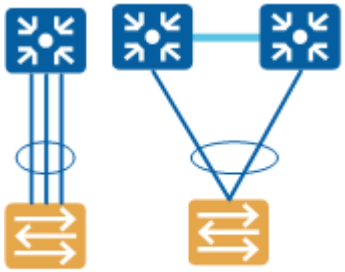
- Using stack cards: Stack switches use stack cards and stack cables to realize interconnection. This mode does not occupy service interfaces, and ensures high speed, stability, and reliability.
- Using service interfaces: Stack switches use standard service interfaces and cables to realize interconnection. This mode does not require additional components, and supports long-distance stacking and Eth-Trunk.

If you remove some member switches from a running stack without powering off the switches or if multiple stack cables fail, the stack splits into multiple stacks. All member switches in a stack use the same IP address and MAC address (that is, the MAC address of the stack). After a stack splits, more than one stack may use the same IP address and MAC address. To prevent this situation, a mechanism is required to check for IP address and MAC address collision after a split. Multi-active detection (MAD) is a protocol used for detecting and handling stack splits. When a stack splits due to a link failure, MAD provides split detection, multi-active handling, and fault recovery mechanisms to minimize impact of the split on services. You are advised to configure MAD after switches set up a stack.

Link Design

Link reliability design for the access layer involves the following key technologies:

- Eth-Trunk: Eth-Trunk is a link aggregation technology that bundles multiple physical Ethernet links into one logical link to improve link bandwidth and reliability and implement load balancing. To ensure Eth-Trunk reliability, it is recommended that member interfaces reside on different cards or chassis.

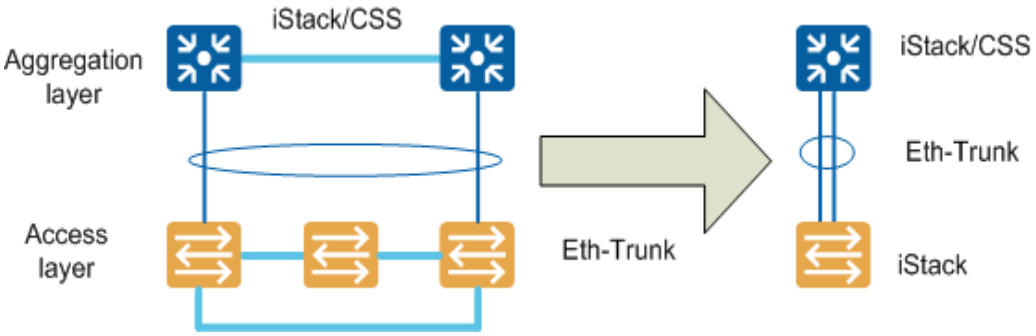


Eth-Trunk

- Dual-homing: Dual-homing means that a lower-layer device connects to two upper-layer devices. If one link fails, the other can still work to ensure uninterrupted data transmission. When the access layer and aggregation layer are connected through a Layer 2 network, a Layer 2 loop prevention protocol, such as STP, MSTP, RSTP, RPR, ERPS, RRPP, SEP, and SmartLink, needs to be deployed.

- Technologies for detecting link faults: include DLDP, ECMP/UCMP, BFD, FRR, and NSF/GR.

When stacking technology is used at the access layer, it is recommended that the aggregation layer devices set up an iStack or a CSS. That is, establish a loop-free topology using the following mode.



According to the best practices, it is recommended that fixed switches at the access layer be stacked and connect to upper-layer switches through inter-chassis Eth-Trunks. Many devices are deployed at the access layer. To reduce investment, the standalone mode can also be used. In this mode, uplink interfaces must be dual-link Eth-Trunk interfaces.

4.2 Aggregation Layer Reliability

As the regional core switching area, the aggregation layer has a high requirement on reliability. Both device reliability and link reliability must be considered.

The device reliability must reach 99.999% and aggregation layer devices must support the following features:

- 1:1 backup of main control boards
- 1+1 backup and 1:1 backup of SFUs
- 1+1 backup of DC power supplies and 1+1/2+2 backup of AC power supplies
- Modular design of fans in which a single-fan failure does not affect system running
- High reliability of the passive backplane
- Independent monitoring unit, which is decoupled from the main control boards
- Hot swap of all modules

The redundancy design of components ensures high reliability of a single device. Device backup can be used to cope with single-node faults. After network protocols detect that a node fails, traffic can be quickly and automatically switched to the backup node, which improves reliability.

Dual-homing can be used to increase link reliability of the aggregation layer. Refer to the chapter of access layer reliability for details. To ensure bandwidth and device performance, you can select either of the following designs:

- If a downlink XGE interface is required, you are advised to select S6720-EI series switches to set up a stack and select an XGE or a 40GE dual-link Eth-Trunk interface as the corresponding uplink interface.
- If a downlink GE interface is required, you are advised to select S5720-EI series switches to set up a stack and select an XGE dual-link Eth-Trunk interface as the corresponding uplink interface.

4.3 Core Layer Reliability

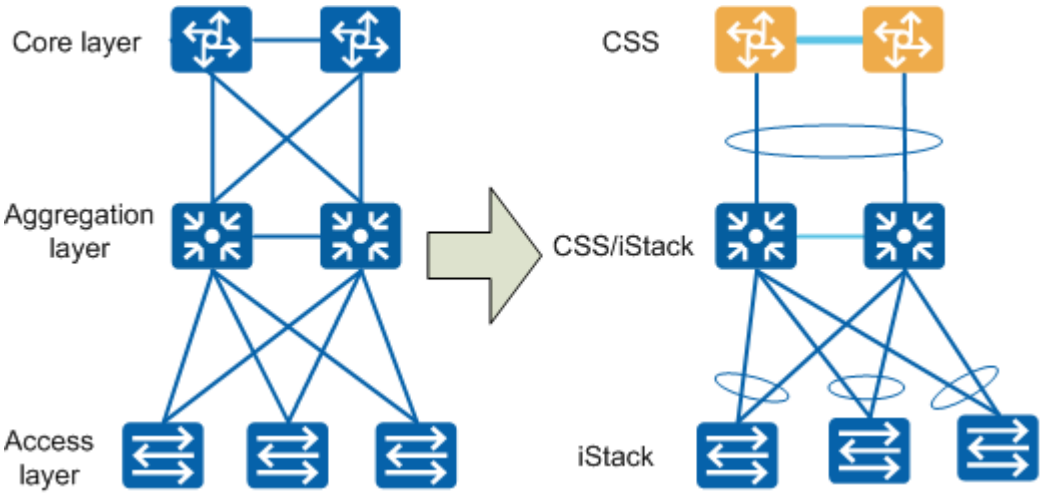
As the core switching area on an entire network, the core layer has an extremely high requirement on reliability. Device reliability, link reliability (Layer 2), and network reliability (Layer 3) must be considered.

It is recommended that modular switches be used at the core layer to provide carrier-grade reliability and the switches must support the following features:

- 1:1 backup of main control boards
- 1+1 backup and 1:1 backup of SFUs
- 1+1 backup of DC power supplies and 1+1/2+2 backup of AC power supplies
- Modular design of fans in which a single-fan failure does not affect system running
- High reliability of the passive backplane
- Independent monitoring unit, which is decoupled from the main control boards
- Hot swap of all modules
- Comprehensive alarm functions
- 1:1 backup of device management modules

For details about the reliability of Layer 2 and Layer 3 links at the core layer, refer to the chapter of access layer reliability.

CSS+iStack loop-free Ethernet technology is recommended. The access layer adopts iStack. The aggregation layer and core layer adopt CSS. Links between layers adopt Eth-Trunk technology. CSS and iStack technologies ensure device reliability. Once a device fails, the other one automatically takes over all services. Eth-Trunk technology ensures link reliability. If one or more links in a trunk fail, traffic is automatically switched to links that are working properly. This technical solution simplifies the network architecture and does not require reliability protocols such as VRRP, simplifying configuration and maintenance, and reducing configuration errors.



Best practices for establishing a CSS using CSS cards:

- You are advised to install at least two SFUs and two CSS cards in each chassis.
- The SFUs in one chassis must be of the same model. The SFUs in two chassis can be of different models; however, the same model is recommended.
- You are advised to configure MAD that can detect and handle the multi-active collision after a CSS splits.

Best practices for establishing a CSS using service interfaces:

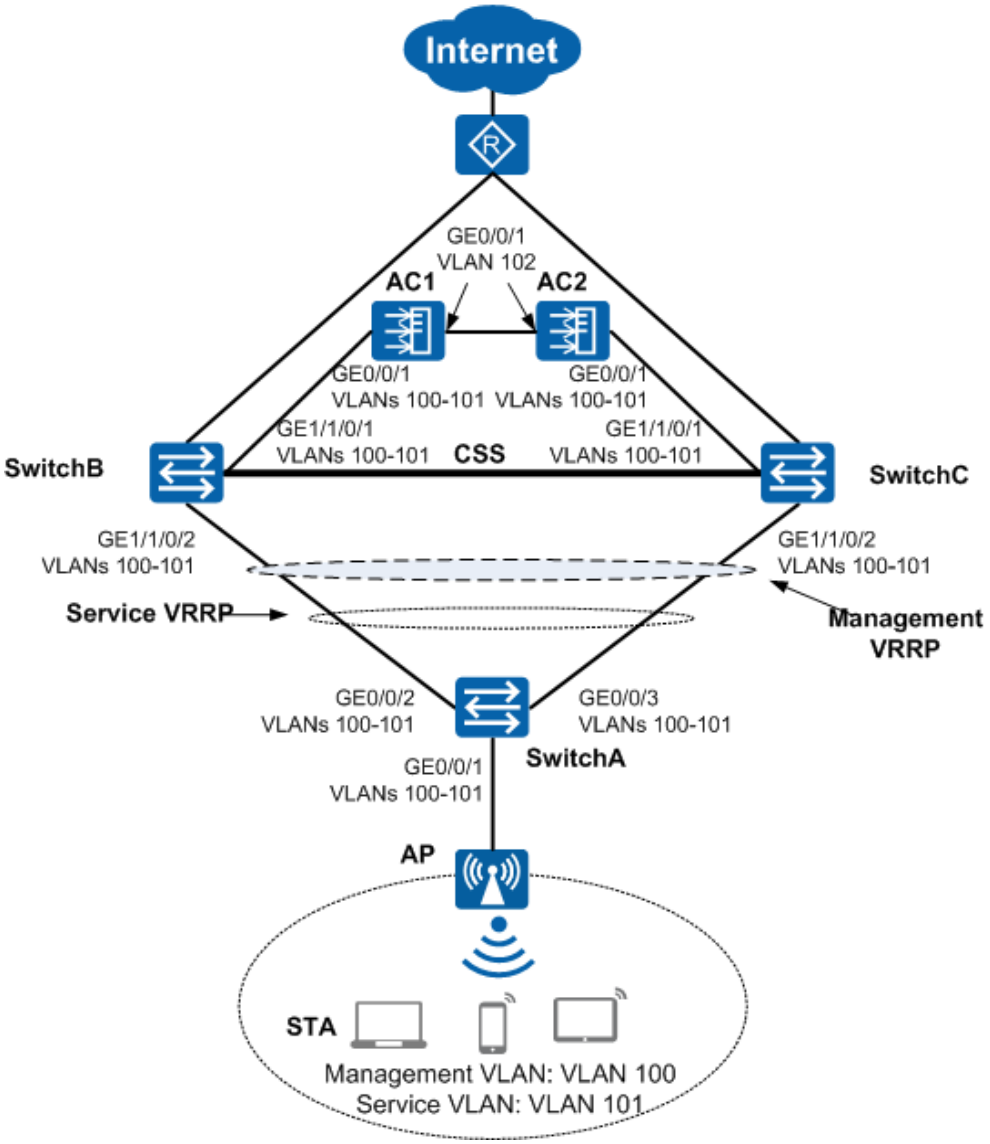
- It is recommended that CSS interfaces be deployed on different cards to prevent CSS splits caused by card faults.
- You are advised to configure MAD that can detect and handle the multi-active collision after a CSS splits.
- The horizontal traffic of a CSS system depends on the bandwidth of CSS links. Physical interfaces can be selected as required.

4.4 Wireless AC Reliability

Reliability design solutions vary according to the networking mode, and include hot standby (HSB), dual-link cold standby, and N+1 cold standby. All of the three backup modes are applicable to non-agile solutions. For agile solutions, stacking or clustering is recommended to implement HSB. If the HSB conditions cannot be met, dual-link cold standby can be used.

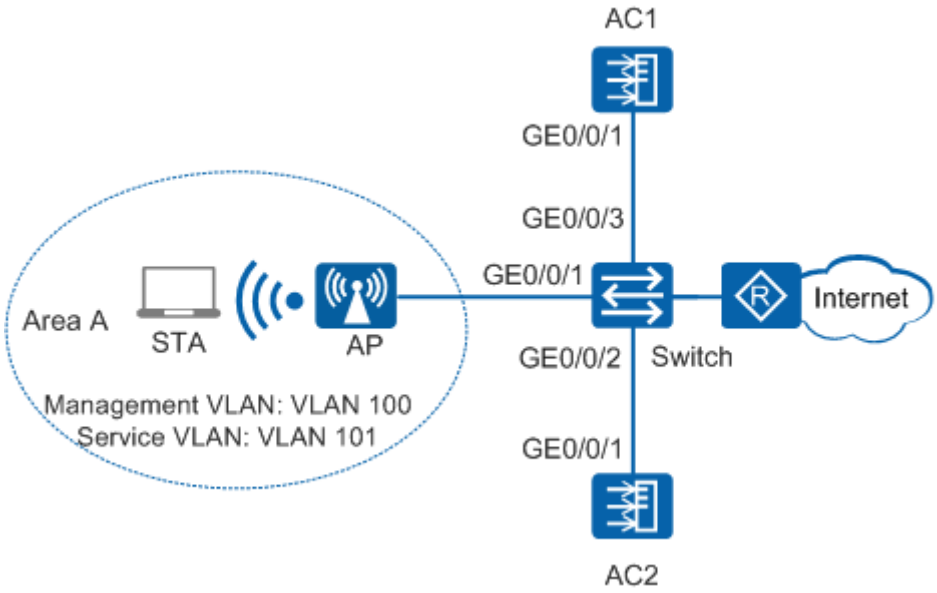
- HSB

  In HSB mode, there are two devices, one acting as a master device and the other a backup one. The master device forwards services and the backup device monitors the forwarding. The master device sends the backup device the status information and information that needs to be backed up in real time. When the master device becomes faulty, the backup device takes over services on the master device. According to different traffic switching modes, HSB is classified into VRRP HSB and dual-link HSB.



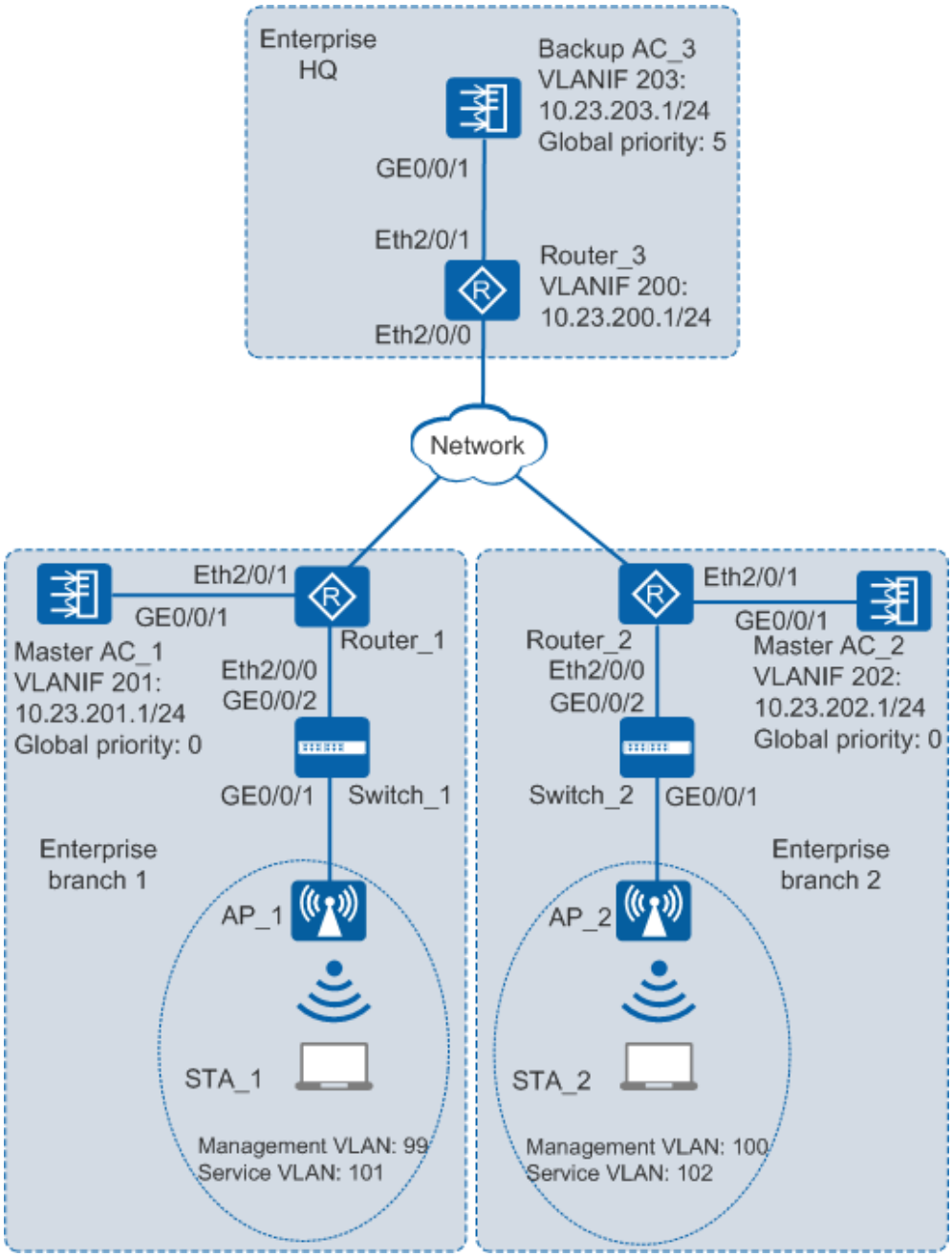
- Dual-link cold standby

  Dual-link cold standby allows two ACs on an AC + Fit AP network to manage APs simultaneously. The APs set up CAPWAP links with both ACs, between which one AC functions as the master AC to provide services for the APs while the other works as the backup AC and does not provide services. When the master AC fails or the CAPWAP link between the master AC and AP becomes faulty, the backup AC replaces the master AC to manage the AP and provide services. To ensure that both ACs provide the same services, it is recommended that the same service configurations be performed on the master and backup ACs.



- N+1 cold standby

  N+1 cold standby uses one backup AC to provide backup services for multiple master ACs on an AC + Fit AP network. When the network runs properly, an AP sets up a CAPWAP link only with the master AC to which it belongs. When the master AC fails or the CAPWAP link becomes faulty, the backup AC replaces the master AC to manage the AP, and establishes a CAPWAP link with the AP to provide services.



For details about AC backup solutions, see **Table 4-1**.

Table 4-1 AC backup solutions

Backup Mode	Application Scenario	Characteristics	Device Model and Version
HSB ● Dual-link HSB ● VRRP HSB	This mode is applicable to scenarios that have high reliability requirements.	User services are not interrupted and high reliability is provided. ● Dual-link HSB: Only STA information is backed up. An AP sets up links with both master and backup ACs, and exchanges management packets with both ACs. ● VRRP HSB: AP, STA, and CAPWAP link information is backed up. After an AP sets up a CAPWAP link with an AC, the CAPWAP link information is directly backed up on the other AC. The AP exchanges packets with only one AC. A backup AC can provide backup services for only one master AC.	The models and software versions of the master and backup ACs must be the same.
Dual-link cold standby	This mode is applicable to scenarios that have low reliability requirements.	Dual-link cold standby provides basic backup functions and lower reliability than HSB. Dual-link cold standby does not back up STA information. An AP establishes links with master and backup ACs. During master/backup switchover or switchback, STAs must go online again and services are temporarily interrupted. A backup AC can provide backup services for only one master AC.	The master and backup ACs can be of different models but must use the same software version.

Backup Mode	Application Scenario	Characteristics	Device Model and Version
N+1 cold standby	This mode is applicable to scenarios that have low reliability requirements and require low cost.	A backup AC can provide backup services for multiple master ACs, which reduces device purchase costs. However, this mode provides lower reliability than HSB. N+1 cold standby does not back up AP or STA information. An AP establishes a link with only one AC. During master/backup switchover or switchback, the AP and STAs must go online again and services are temporarily interrupted. The service interruption time in N+1 backup mode is longer than that in dual-link cold standby mode. A backup AC can provide backup services for multiple master ACs.	The master and backup ACs can be of different models but must use the same software version.

Reliability modes are recommended for networks with more than 400 STAs. The following lists the reliability modes for non-agile solutions in a descending order of reliability: VRRP HSB > dual-link HSB > dual-link cold standby > N+1 cold standby. For agile solutions, clustering or stacking is recommended to implement HSB.

On a small-scale wireless network without AC backup, service holding upon CAPWAP link disconnection can be enabled to ensure nonstop user data forwarding and improve service reliability.

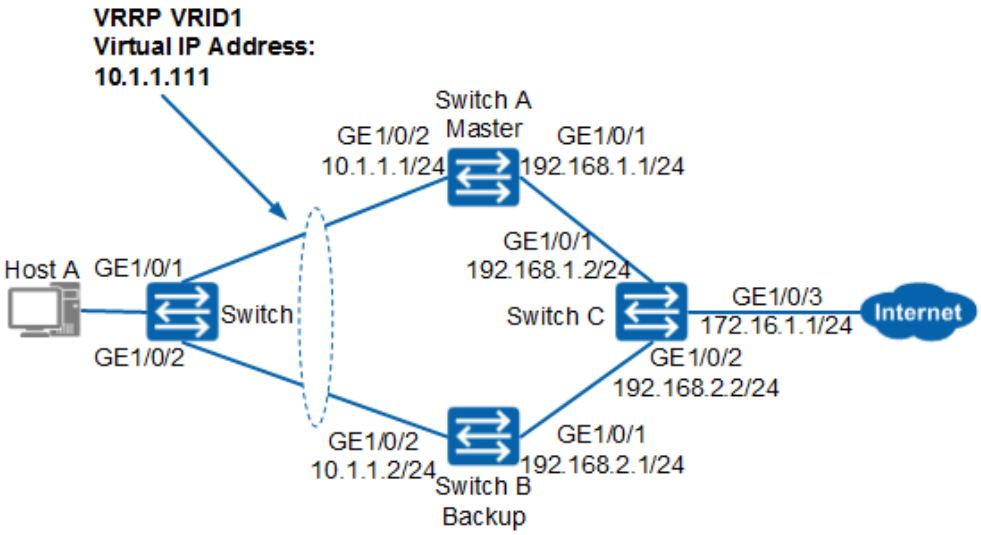
4.5 Service Reliability

4.5.1 VRRP

For switches and AR routers, only the VRRP function is required. For firewalls, the VRRP function needs to be used together with HRP.

- Switch and AR router

  For switches or AR routers, service reliability can be ensured if routes are backed up on two devices. If one of the two devices fails, the other device takes over the services from the faulty device, ensuring service continuity. The following uses switches as an example to illustrate the configuration of the VRRP function (one typical application scenario):



Configure VRRP group 1 on SwitchA, and set the priority of SwitchA to 120 and the preemption delay to 20s.

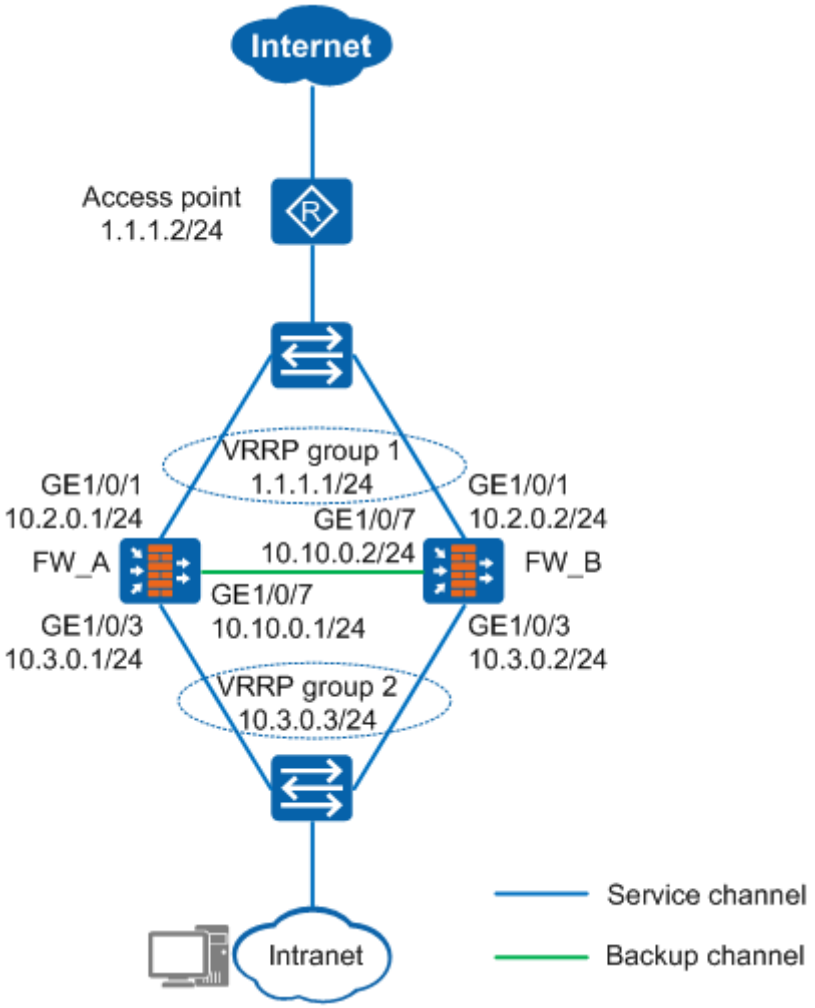
```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchA-Vlanif100] vrrp vrid 1 priority 120
[SwitchA-Vlanif100] vrrp vrid 1 preempt-mode timer delay 20
[SwitchA-Vlanif100] quit
```

Configure VRRP group 1 on SwitchB. Retain the default priority (100) for SwitchB.

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.111
[SwitchB-Vlanif100] quit
```

- Firewall

  Firewall is a status detection device which performs comprehensive check on the first packet in a flow and sets up sessions to record packet status information (including the source IP address, source port number, destination IP address, destination port number, and protocol in the packet). Subsequent packets of the traffic flow are then forwarded according to the session table. Only those matching this table will be forwarded. Packets that do not match this table will be discarded by the firewall. Therefore, when firewalls are deployed in dual-node mode, consider backup of status information such as sessions on the two firewalls. HRP and VRRP configurations for one typical application scenario are as follows:



On FW_A, create VRRP group 1 on the uplink service interface GE1/0/1 and set the group state to active. If the IP addresses of the interface and VRRP group are on different network segments, specify a mask when configuring the IP address of the VRRP group.

```
[FW_A] interface GigabitEthernet 1/0/1
[FW_A-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 1.1.1.1 24 active
[FW_A-GigabitEthernet1/0/1] quit
```

On FW_A, create VRRP group 2 on the downlink service interface GE1/0/3 and set the group state to active.

```
[FW_A] interface GigabitEthernet 1/0/3
[FW_A-GigabitEthernet1/0/3] vrrp vrid 2 virtual-ip 10.3.0.3 active
[FW_A-GigabitEthernet1/0/3] quit
```

Specify the heartbeat interface and enable hot standby on FW_A.

```
[FW_A] hrp interface GigabitEthernet 1/0/7 remote 10.10.0.2
[FW_A] hrp enable
```

On FW_B, create VRRP group 1 on the uplink service interface GE1/0/1 and set the group state to standby.

```
[FW_ B] interface GigabitEthernet 1/0/1
[FW_B-GigabitEthernet1/0/1] vrrp vrid 1 virtual-ip 1.1.1.1 24 standby
[FW_B-GigabitEthernet1/0/1] quit
```

On FW_B, create VRRP group 2 on the downlink service interface GE1/0/3 and set the group state to standby.

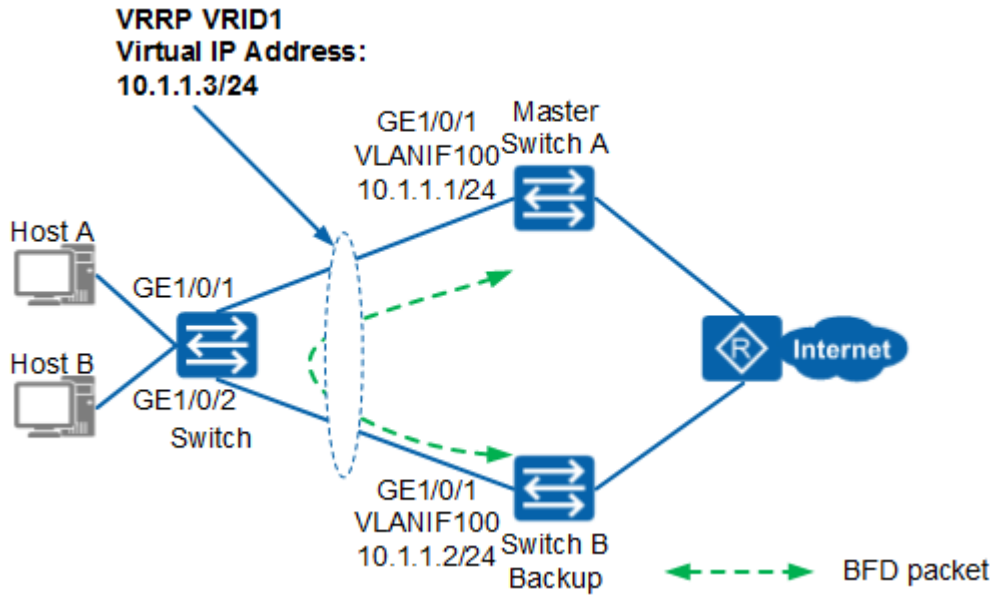
```
[FW_B] interface GigabitEthernet 1/0/3
[FW_B -GigabitEthernet1/0/3] vrrp vrid 2 virtual-ip 10.3.0.3 standby
[FW_B -GigabitEthernet1/0/3] quit
```

Specify the heartbeat interface and enable hot standby on FW_B.

```
[FW_B] hrp interface GigabitEthernet 1/0/7 remote 10.10.0.1
[FW_B] hrp enable
```

4.5.2 BFD

Bidirectional Forwarding Detection (BFD) is a fast fault detection mechanism that rapidly detects link faults and monitor IP connectivity on the entire network independent of media and routing protocols.



The example for configuring BFD between two devices is as follows:

Create a BFD session on SwitchA.

```
[SwitchA] bfd
[SwitchA-bfd] quit
[SwitchA] bfd atob bind peer-ip 10.1.1.2 interface vlanif 100
[SwitchA-bfd-session-atob] discriminator local 1
[SwitchA-bfd-session-atob] discriminator remote 2
[SwitchA-bfd-session-atob] min-rx-interval 100
[SwitchA-bfd-session-atob] min-tx-interval 100
[SwitchA-bfd-session-atob] commit
[SwitchA-bfd-session-atob] quit
```

Create a BFD session on SwitchB.

```
[SwitchB] bfd
[SwitchB-bfd] quit
[SwitchB] bfd btoa bind peer-ip 10.1.1.1 interface vlanif 100
[SwitchB-bfd-session-btoa] discriminator local 2
[SwitchB-bfd-session-btoa] discriminator remote 1
[SwitchB-bfd-session-btoa] min-rx-interval 100
[SwitchB-bfd-session-btoa] min-tx-interval 100
[SwitchB-bfd-session-btoa] commit
[SwitchB-bfd-session-btoa] quit
```

Associate BFD with VRRP as follows to implement fast VRRP switchover:

Configure VRRP group 1 on SwitchA, and set the priority of SwitchA to 120 and the preemption delay to 20s.

```
[SwitchA] interface vlanif 100
[SwitchA-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.3
[SwitchA-Vlanif100] vrrp vrid 1 priority 120
[SwitchA-Vlanif100] vrrp vrid 1 preempt-mode timer delay 20
[SwitchA-Vlanif100] quit
```

Configure VRRP group 1 on SwitchB. Retain the default priority (100) for SwitchB.

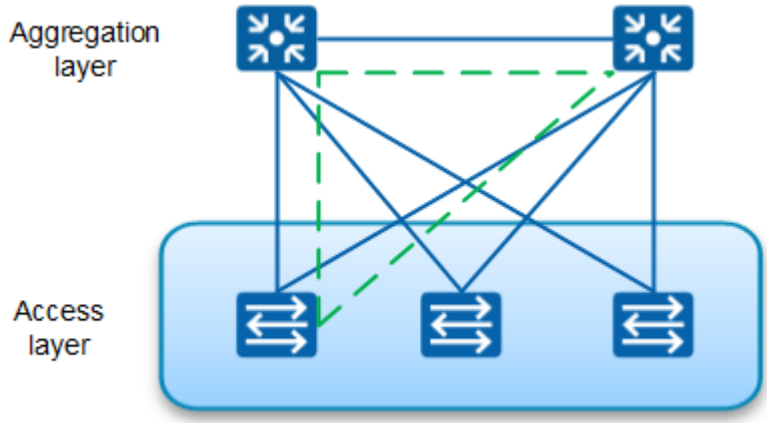
```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 1 virtual-ip 10.1.1.3
[SwitchB-Vlanif100] quit
```

Associate the VRRP group with a BFD session on SwitchB. When the BFD session goes Down, the VRRP priority of SwitchB increases by 40.

```
[SwitchB] interface vlanif 100
[SwitchB-Vlanif100] vrrp vrid 1 track bfd-session 2 increased 40
[SwitchB-Vlanif100] quit
```

4.5.3 Loop Prevention Protocol

Redundant links are used on an Ethernet switching network to provide link backup and enhance network reliability. The use of redundant links, however, may produce loops, causing broadcast storms and making the MAC address table unstable. As a result, network communication may encounter quality deterioration or even be interrupted.



If Layer 2 access is used between the access layer and aggregation layer or if Layer 2 access is used between the access layer, aggregation layer, and core layer, Layer 2 loop prevention protocols must be deployed. The STP, MSTP, and RSTP protocols are recommended on campus networks. **Table 4-2** describes the functions and application scenarios of the protocols.

Table 4-2 Comparison between STP, MSTP, and RSTP

Protocol	Fast Convergence	Multi-instance	Characteristics		Application Scenario
STP	No	No	A loop-free tree is generated. Thus, broadcast storms are prevented and redundancy is implemented.	User or service traffic does not need to be differentiated, and all VLANs share a spanning tree.	Applies to Layer 2 networks that have low requirements on the convergence rate.
RSTP	Yes	No	A loop-free tree is generated. Thus, broadcast storms are prevented and redundancy is implemented. The network is converged at a high speed.		Applies to single rings, intersecting rings, and tangent rings that require fast convergence.
MSTP	Yes	Yes	A loop-free tree is generated. Thus, broadcast storms are prevented and redundancy is implemented. The network is converged at a high speed. Multiple spanning trees perform load balancing and transmit traffic in different VLANs along different paths.	User or service traffic needs to be differentiated and load balanced. Traffic from different VLANs is forwarded through different spanning trees that are independent of each other.	Applies to Layer 2 networks that require fast convergence.

Consider the following factors when selecting an appropriate protocol from among the three protocols:

- Some old switches do not support RSTP or MSTP. STP should be enabled on the network where these switches are working. If budget permits, replace devices that do not support RSTP or MSTP on the network because RSTP and MSTP can improve network performance.

- When all devices on a network support RSTP and the network has only one VLAN, use RSTP to speed up network convergence. If multiple VLANs with the same topology exist on the network and the VLAN configurations on the trunk are the same, use RSTP.
- Use MSTP if multiple VLANs exist on the network but VLAN configurations on the trunk are different.
- If devices support STP and RSTP, RSTP is recommended.
- If devices support STP, RSTP, and MSTP, MSTP is recommended. MSTP can prevent broadcast storms caused by loops and realize load balancing as well. RSTP, an enhancement to STP, allows for fast network topology convergence. STP and RSTP both have a defect: All VLANs on a LAN use one spanning tree, and thus inter-VLAN load balancing cannot be performed. Once a link is blocked, the link will no longer transmit traffic, wasting bandwidth and causing a failure in forwarding certain VLAN packets. Advantages of the MSTP protocol:
  - Supports various complex networking modes and applies to any type of Layer 2 network.
  - Has a good protocol compatibility. MSTP is a standard protocol and supports networking with multiple private protocols such as SEP.
  - Implements load balancing among VLANs, ensuring high utilization of redundant links and improving scalability.
  - Provides BPDU, root, and loop protection and TC-BPDU attack defense capabilities.

5 Security Design and Best Practices

On a traditional campus network, the intranet is considered secure and threats come from the extranet. Firewalls and IDS/IPS are used to ensure security on the campus edge. As security challenges increase, the traditional security measures and independent working mode cannot meet requirements on border defense. The security model should be converted from passive into proactive to solve security problems from the root (terminals), improving information security level of the entire enterprise.

Service models and key points vary at different layers. Therefore, service security can be designed based on service requirements of each layer. Each layer of an agile campus network carries two types of service traffic: wired and wireless service traffic.

This chapter describes service requirement analysis, service security design, and best practices for different layers as well as wired and wireless users.

5.1 Wired Service Security

5.1.1 Access Layer

5.1.1.1 Broadcast Storm Suppression

When a Layer 2 Ethernet interface on a switch receives broadcast, multicast, or unknown unicast packets, the switch forwards the packets to other Layer 2 Ethernet interfaces in the same VLAN because the switch cannot determine the outbound interface based on the destination MAC addresses of these packets. In this case, a broadcast storm may occur and the forwarding performance of the switch deteriorates.

On downlink interfaces of the access layer, configure suppression of broadcast, multicast, unknown unicast packets to reduce broadcast storms.

- You can configure the packet rate limit in percentage.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] broadcast-suppression 5
```

```
[HUAWEI-GigabitEthernet1/0/1] multicast-suppression 5
[HUAWEI-GigabitEthernet1/0/1] unicast-suppression 5
```

- If suppression on broadcast storms needs to be more precise, you can configure the packet rate limit in pps or bps (small granularity control).

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] broadcast-suppression cir 100
[HUAWEI-GigabitEthernet1/0/1] multicast-suppression cir 100
[HUAWEI-GigabitEthernet1/0/1] unicast-suppression cir 100
```

NOTE

Configure rate limits for broadcast, multicast, and unknown unicast packets based on your site scenarios. If a network does not involve or only involve a few broadcast services, you can set the limits to smaller values.

5.1.1.2 Attack Defense

You are advised to configure DHCP snooping on access switches and configure the uplink port as a trusted port.

DHCP snooping defends against bogus DHCP server attacks, DHCP server DoS attacks, bogus DHCP packet attacks, and other DHCP attacks. DHCP snooping allows administrators to configure trusted interfaces and untrusted interfaces, so DHCP clients can obtain IP addresses from authorized DHCP servers. A trusted interface forwards DHCP messages it receives whereas an untrusted interface discards DHCP ACK messages and DHCP Offer messages received from a DHCP server.

An interface directly or indirectly connected to the DHCP server trusted by the administrator needs to be configured as the trusted interface, and other interfaces are configured as untrusted interfaces. This ensures that DHCP clients only obtain IP addresses from authorized DHCP servers and prevents bogus DHCP servers from assigning IP addresses to DHCP clients.

You can configure DHCP snooping based on interfaces or VLANs.

Configure DHCP snooping on an interface of an access switch and configure the uplink interface as a trusted interface.

```
<HUAWEI> system-view
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] dhcp snooping trusted    //Configure the uplink
interface as a trusted interface so that the access switch processes only the
response packets received by the interface from the DHCP server.
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] interface gigabitethernet 0/0/2
[HUAWEI-GigabitEthernet0/0/2] dhcp snooping enable     //Enable DHCP snooping on
the user-side interface.
[HUAWEI-GigabitEthernet0/0/2] quit
```

Configure DHCP snooping in a VLAN.

```
[HUAWEI] dhcp enable
[HUAWEI] dhcp snooping enable
[HUAWEI] vlan 10
[HUAWEI-vlan10] dhcp snooping enable
[HUAWEI-vlan10] dhcp snooping trusted interface gigabitethernet 0/0/1
```

On a network with only wired users, DHCP snooping can be configured on interfaces or in VLANs. If there are both wired and wireless users on a network, you are not advised to enable

DHCP snooping on switch interfaces connecting to APs. This may cause the number of user binding entries on switches to exceed the maximum. You are advised to configure DHCP snooping for wired users in VLANs and configure DHCP snooping for wireless users in the wireless-side VAP profile. For details about how to configure DHCP snooping in a wireless-side VAP profile, see **5.2.1 Traffic Limit**.

You are advised to configure IP packet check and dynamic ARP inspection (DAI) on an interface or in a VLAN.

Unauthorized users often send bogus packets with the source IP address and MAC address of authorized users to access or attack the network. Then authorized users cannot access stable and secure networks. To address this problem, you can configure IP source guard (IPSG). IPSG is used to prevent network access from malicious hosts using the authorized hosts' IP addresses. In addition, IPSG prevents unauthorized hosts from accessing or attacking networks with forged IP addresses.

You can configure DAI to defend against Man in The Middle (MITM) attacks, preventing theft of authorized user information. When a device receives an ARP packet, it compares the source IP address, source MAC address, VLAN ID, and interface number of the ARP packet with binding entries. If the ARP packet matches a binding entry, the device considers the ARP packet valid and allows it to pass through. If the ARP packet does not match any binding entry, the device considers the ARP packet invalid and discards it.

You can enable DAI in the interface or VLAN view. When DAI is enabled in an interface view, the device checks all ARP packets received on the interface against the binding entries. When DAI is enabled in the VLAN view, the device checks the ARP packets received on interfaces that belong to the VLAN against the binding entries.

Enable IP packet check and DAI on GE1/0/1.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] ip source check user-bind enable
[HUAWEI-GigabitEthernet1/0/1] arp anti-attack check user-bind enable
[HUAWEI-GigabitEthernet1/0/1] arp anti-attack check user-bind alarm enable
```

Enable DAI in VLAN 100.

```
<HUAWEI> system-view
[HUAWEI] vlan 100
[HUAWEI-vlan100] arp anti-attack check user-bind enable
```

The two functions are based on the binding table, which can be generated dynamically through DHCP snooping or configured statically.

You are advised to configure ARP/DHCP rate limiting.

If there are many terminals with unknown behaviors on a network, a large number of ARP/DHCP packets may be flooded into the core layer in a short period of time. To reduce the load on the core layer, you can configure rate limits for outgoing ARP and DHCP packets on uplink interfaces of access devices.

Create separate access control lists (ACLs) for DHCP packets and ARP packets.

```
[HUAWEI] acl 3001
[HUAWEI-acl-adv-3001] rule 5 permit udp destination-port eq bootps
[HUAWEI] acl 4001
[HUAWEI-acl-L2-4001] rule 5 permit l2-protocol arp destination-mac ffff-ffff-
ffff
[HUAWEI-acl-L2-4001] rule 10 permit l2-protocol arp
```

Configure rate limits on uplink interfaces.

```
[HUAWEI] interface Eth-Trunk1
[HUAWEI-Eth-Trunk1] traffic-limit outbound acl 3001 cir 192 pir 192 cbs 24000 pbs
24000
[HUAWEI-Eth-Trunk1] traffic-limit outbound acl 4001 cir 32 pir 32 cbs 4000 pbs
4000
```

It is recommended that the uplink interface connecting the access switch to the gateway be added to the whitelist for attack source tracing.

If certain users do not need to be traced regardless of whether they might initiate attacks, add the users to the whitelist for attack source tracing. Typically, packets from the gateway are not discarded. You are advised to add the uplink interface connecting the access switch to the gateway to the whitelist.

In the attack defense policy **test**, add interface GE1/0/1 to the whitelist for attack source tracing and port attack defense.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend whitelist 2 interface gigabitethernet
1/0/1
[HUAWEI-cpu-defend-policy-test] auto-port-defend enable
[HUAWEI-cpu-defend-policy-test] auto-port-defend whitelist 2 interface
gigabitethernet 1/0/1
```

5.1.1.3 Loop Detection

You can configure loop detection on downlink interfaces.

```
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] loopback-detect enable
```

5.1.1.4 Network Access Control

Generally, the number of users allowed on an access interface is fixed. In office scenarios, there are two types of wired terminals: IP phone and PC. In dormitory scenarios, a hub allows access of four to eight users. You can configure a user limit to prevent burst attacks and unauthorized access.

```
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] mac-limit maximum 2
```

5.1.1.5 Port Isolation

You are advised to configure port isolation on the port connecting the access switch to the terminal. This configuration secures user communication and prevents invalid broadcast packets from affecting user services.

Configure port isolation on GE1/0/1 of the access switch.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] port-isolate enable
```

5.1.2 Aggregation Layer

Aggregation devices are responsible for Layer 2 forwarding of service traffic, for example, transparent transmission of VLAN packets or authentication packets. Generally, terminal

devices are not directly connected to the aggregation layer, so only port isolation needs to be configured.

If terminal devices are connected to the aggregation layer, see **5.1.1 Access Layer** for the security design.

If the aggregation device functions as the user gateway or authentication point, see **5.1.3 Core Layer** for the security design.

5.1.3 Core Layer

In most cases, gateways, authentication points, and policies are deployed on core devices. The following lists the basic service requirements for the core layer:

- If a core device serves as a client gateway, routes and ARP entries must be configured.
- On an agile campus network, access users are authenticated by network access control (NAC), which is deployed on core devices. Therefore, a core device needs to manage a large number of user entries.
- If free mobility is involved, core devices need to execute a large number of policies automatically delivered by the Agile Controller-Campus.

NAC authentication for preventing user-side attacks is included in the basic requirements. The following are other service security requirements:

- The CPU is able to process protocol packets when a large number of users access the network.
- ARP security functions need to be deployed on core devices.
- ARP proxy needs to be configured in centralized forwarding mode.

5.1.3.1 Local Attack Defense

Local attack defense is an important function set of a switch. It protects the CPU by preventing service interruption caused by the CPU busy processing a large number of packets or malicious attack packets. This ensures that services can run properly when a switch is attacked. Local attack defense includes the following functions: CPU attack defense, attack source tracing, and port attack defense.

CPU Attack Defense

CPU attack defense can limit the rate of packets sent to the CPU so that only a limited number of packets are sent to the CPU within a certain period of time. This ensures that the CPU can properly process services. The core of CPU attack defense is the Control Plane Committed Access Rate (CPCAR), blacklist, and whitelist.

CPCAR limits the rate of protocol packets sent to the control plane to ensure security of the control plane. Different CPCAR values are set for different protocol packets to limit the rate of sending protocol packets to the CPU, protecting the CPU from a large number of attacks. CPCAR values can be adjusted to enhance protocol packet processing capabilities of switches. However, too large CPCAR values cannot protect the CPU effectively.

As the number of access users and protocol packets for authentication are growing, the default CPCAR value is no longer applicable. If CPCAR values are not properly set, protocol packets may be discarded, and users will not be able to go online or will be disconnected unexpectedly.

The following is an example for changing the CPCAR value for ARP Request packets.

Create an attack defense policy.

```
[Switch] cpu-defend policy policy1
```

Set the CPCAR value of ARP Request packets to 120 kbit/s.

```
[Switch-cpu-defend-policy-policy1] car packet-type arp-request cir 120
Warning: Improper parameter settings may affect stable operating of the system.
Use this command under assistance of Huawei engineers. Continue? [Y/N]: y
```

Apply the attack defense policy to the main control board.

```
[Switch] cpu-defend-policy policy1
```

Apply the attack defense policy to the LPU.

```
[Switch] cpu-defend-policy policy1 global
```

Considering user behaviors on the live network in previous projects, set the CPCAR value based on common user behaviors on the live network in real time.

Create a blacklist and add users with specific characteristics to it. The switch then discards the packets from the blacklisted users. Create a whitelist and add users with specific characteristics to it. The switch then processes the packets matching these characteristics first.

Define ACL rules.

```
[Switch] acl number 2001
[Switch-acl-basic-2001] rule permit source 10.1.1.0 0.0.0.255
[Switch-acl-basic-2001] quit
[Switch] acl number 2002
[Switch-acl-basic-2002] rule permit source 10.2.2.0 0.0.0.255
[Switch-acl-basic-2002] quit
```

Create an attack defense policy.

```
[Switch] cpu-defend policy policy1
```

Configure the blacklist for CPU attack defense.

```
[Switch-cpu-defend-policy-policy1] blacklist 1 acl 2001
```

Configure the whitelist for CPU attack defense.

```
[Switch-cpu-defend-policy-policy1] whitelist 1 acl 2002
```

Apply the attack defense policy to the main control board.

```
[Switch] cpu-defend-policy policy1
```

Apply the attack defense policy to the LPU.

```
[Switch] cpu-defend-policy policy1 global
```

You can use the **display cpu-defend statistics** command to check forwarding and discarding statistics on packets sent to the CPU in real time. These statistics can facilitate fault location.

```
[HUAWEI] display cpu-defend statistics all
```

Attack Source Tracing

After attack source tracing is configured on a switch, the switch analyzes packets sent to the CPU and sends logs or alarms to notify the administrator of the potential attack packets so

that the administrator can take protective measures. The attack source tracing function is enabled by default.

Create an attack defense policy, enable attack source tracing, and enable the function for reporting attack source tracing events.

```
<HUAWEI> system-view
[HUAWEI] cpu-defend policy test
[HUAWEI-cpu-defend-policy-test] auto-defend enable
[HUAWEI-cpu-defend-policy-test] auto-defend alarm enable
[HUAWEI-cpu-defend-policy-test] quit
[HUAWEI] cpu-defend-policy test
```

View attack source information.

```
[HUAWEI] display auto-defend attack-source
```

Corresponding actions (such as discarding) can be configured for switches when attack source tracing is triggered. Actions are not recommended because burst traffic may be transient and packet discarding may affect services. Simply enable the monitoring function of attack source tracing. The preceding commands can be used to monitor a network and determine whether it is undergoing continuous attacks or burst traffic.

Port Attack Defense

After port attack defense is configured, a switch can trace the source and limit the rate of packets sent to the CPU based on ports, protecting the CPU against DoS attacks. This function is enabled on a switch by default.

Create an attack defense policy using the **cpu-defend policy** command and enable port attack defense. An attack defense policy can be applied to the main control board, all interface boards, or a specified interface board. You can use either of the above modes based on the site requirement.

```
[HUAWEI] cpu-defend policy defend
[HUAWEI-cpu-defend-policy-defend] auto-port-defend enable
[HUAWEI-cpu-defend-policy-defend] quit
[HUAWEI] cpu-defend-policy defend             //Apply the attack defense policy
to the main control board.
[HUAWEI] cpu-defend-policy defend global      //Apply the attack defense policy
to all LPUs.
[HUAWEI] slot 3
[HUAWEI-slot-3] cpu-defend-policy test        //Apply the attack defense policy
to the specified LPU.
```

Display port attack defense records.

```
[HUAWEI] display auto-port-defend attack-source
```

The preceding command displays the port attack defense triggering record. Port attack defense is not necessarily triggered by a large number of attack packets. It may be a CPU self-protection process that is triggered by transient ARP packet burst. Port attack defense protects the CPU against transient ARP packet burst and continuous packet attacks.

In some scenarios, network-side interfaces need to receive a lot of valid protocol packets. You should add these interfaces or network nodes connecting to these interfaces to the whitelist. The switch does not trace the source or limit the rate of protocol packets received by the interfaces in the whitelist, so that the CPU can promptly process the packets from the network-side interfaces.

Add the network-side interface GE1/0/0 to the whitelist so that the CPU can promptly process the packets from this interface.

```
[Switch-cpu-defend-policy-policy1] auto-port-defend whitelist 1 interface
gigabitethernet 1/0/0
```

5.1.3.2 TC Attack Defense

After a device receives a topology change (TC) BPDU, it instructs the ARP module to age or delete ARP entries. The device needs to perform ARP learning to obtain the latest ARP entries. However, if the network topology changes frequently or network devices contain many ARP entries, ARP re-learning will lead to excessive ARP packets on the network.

A device will delete MAC address entries and ARP entries when it receives TC BPDUs. Frequent entry deletion may cause high CPU usage. You are advised to enable TC protection on all the STP-enabled devices.

```
<HUAWEI> system-view
[HUAWEI] stp tc-protection
```

Disable the device from responding to TC BPDUs and configure the MAC address-triggered ARP entry update function. The device then does not age out or delete ARP entries when receiving TC BPDUs.

```
<HUAWEI> system-view
[HUAWEI] mac-address update arp
[HUAWEI] arp topology-change disable
```

5.1.3.3 ARP Security

Currently, the following ARP security functions can be enabled on core switches: optimized ARP reply and ARP gateway anti-collision.

1. Optimized ARP reply

   When a switch functions as an access gateway, it receives a large number of ARP packets requesting the interface MAC address of the switch. If all these ARP Request packets are sent to the main control board for processing, the CPU usage of the main control board will increase and other services cannot be processed promptly.

   The optimized ARP reply function addresses this issue. After this function is enabled, the LPU directly returns ARP Reply packets if the ARP Request packets are destined for the local interface. This function helps the switch defend against ARP flood attacks. The optimized ARP reply function is applicable especially when the switch is configured with multiple LPUs. By default, the optimized ARP reply function is enabled on a switch.

   ```
   [HUAWEI] undo arp optimized-reply disable
   ```

2. ARP gateway anti-collision

   If an attacker forges the gateway address to send ARP packets with the source IP address being the gateway IP address on the LAN where the gateway is located, ARP entries on hosts in the LAN record the incorrect gateway address. As a result, all traffic from user hosts to the gateway is sent to the attacker and the attacker can intercept user data, causing network access failures of these hosts.

   To defend against attacks from bogus gateways, enable ARP gateway anti-collision on gateways if user hosts directly connect to the gateways. A gateway considers that a gateway collision occurred if a received ARP packet meets either of the following conditions:

   - The source IP address in the ARP packet is the same as the IP address of the VLANIF interface matching the inbound interface.

- The source IP address of the ARP packet is the virtual IP address of the inbound interface, but the source MAC address is not the VRRP virtual MAC address.

The gateway generates an ARP anti-collision entry and discards the received packets with the same source MAC address and VLAN ID as that ARP packet within a specified period of time. This function prevents ARP packets with the bogus gateway address from being broadcast in a VLAN.

```
[HUAWEI] arp anti-attack gateway-duplicate enable
```

5.1.3.4 ARP Proxy

In centralized forwarding mode, port isolation is configured for all downlink Layer 2 devices. Therefore, corresponding ARP proxy should be configured on core gateways. In most cases, intra-VLAN ARP proxy is used.

```
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] arp-proxy inner-sub-vlan-proxy enable
```

NOTE

In this scenario, port isolation must be configured for access and aggregation devices.

Configure port isolation on GE1/0/1 and GE1/0/2 to implement Layer 2 isolation and Layer 3 connectivity between the two interfaces.

```
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] port-isolate enable group 1
[HUAWEI-GigabitEthernet1/0/1] quit
[HUAWEI] interface gigabitethernet 1/0/2
[HUAWEI-GigabitEthernet1/0/2] port-isolate enable group 1
[HUAWEI-GigabitEthernet1/0/2] quit
```

5.1.3.5 IPv6 Attack Defense

You are advised to configure IPv6 attack defense.

When the network is operating properly, switches can receive ICMPv6 packets correctly. In the event of heavy traffic on the network, if hosts or ports are frequently unreachable, the devices receive a large number of ICMPv6 packets. This causes heavier traffic burdens over the network and degrades the performance of the devices. In addition, attackers may use ICMPv6 error packets to probe into the internal network topology.

To improve network performance and security, disable the system from receiving ICMPv6 Echo Reply packets, Host Unreachable packets, and Port Unreachable packets.

Disable the system from receiving ICMPv6 Echo Reply packets, Host Unreachable packets, and Port Unreachable packets.

```
<HUAWEI> system-view
[HUAWEI] undo ipv6 icmp echo-reply receive
[HUAWEI] undo ipv6 icmp port-unreachable receive
[HUAWEI] undo ipv6 icmp host-unreachable receive
```

5.1.4 Egress Firewall

With the development of networks, more and more people need to access the networks, services are complex, and traffic is diversified, which may incur DDoS attacks. A successful attack may result in huge service losses. Active network viruses threaten network and terminal security. To meet service requirements, the internal network provides network

services, such as the company website and email service. These risks threaten the security of the campus network.

As the network egress, the firewall is responsible for the security of the entire network. To meet the preceding security requirements, you can deploy the following security services on the egress firewall:

1. Assign employees, servers, and the Internet to different security zones to inspect and protect interzone traffic.
2. Enable content security protection functions according to the services to be provided for Internet users. For example, enable file blocking and data filtering on the file server, mail filtering on the mail server, and antivirus and intrusion prevention on all servers.
3. If employees need to access the Internet, enable URL filtering, file blocking, data filtering, antivirus, and application behavior control to defend against Internet threats and prevent information leaks to ensure network security.
4. Enable anti-DDoS to defend against heavy-traffic attacks launched by Internet hosts to ensure normal service operations.
5. Apply traffic policies to traffic between the intranet and Internet to control the bandwidth and number of connections to prevent network congestion and defend against DDoS attacks.
6. Deploy Huawei NMS (to be purchased independently) to manage network operation logs. The logs help the administrator adjust configurations, identify risks, and audit traffic.

5.1.4.1 Security Zones

The system has four default security zones. If the default security zones do not meet your service requirements, you can create security zones and define their security levels. After creating a security zone, add interfaces to it. After that, all packets sent and received on the interfaces are considered in the security zone. By default, an interface does not belong to any security zone and is unable to communicate with interfaces in security zones.

Assign interfaces to security zones.

```
[FW] firewall zone untrust
[FW-zone-untrust] add interface GigabitEthernet 1/0/1
[FW-zone-untrust] quit
[FW] firewall zone trust
[FW-zone-trust] add interface GigabitEthernet 1/0/3
[FW-zone-trust] quit
```

Configure a security policy (by default, all traffic is denied).

Configure a security policy to allow intranet PCs to access the Internet.

```
[FW] security-policy
[FW-security-policy] rule name policy_sec_1
[FW-security-policy-sec_policy_1] source-address 10.3.0.0 mask 255.255.255.0
[FW-security-policy-sec_policy_1] source-zone trust
[FW-security-policy-sec_policy_1] destination-zone untrust
[FW-security-policy-sec_policy_1] action permit
[FW-security-policy-sec_policy_1] quit
[FW-security-policy] quit
```

5.1.4.2 Filtering

- URL filtering

  # Configure the URL filtering profile.

```
[FW] profile type url-filter name profile_url_research
[FW-profile-url-filter-profile_url_research] category user-defined action
block
[FW-profile-url-filter-profile_url_research] category pre-defined action block
[FW-profile-url-filter-profile_url_research] category pre-defined category-id
15 action allow
[FW-profile-url-filter-profile_url_research] category pre-defined category-id
17 action allow
[FW-profile-url-filter-profile_url_research] quit
```

Configure a security policy.

```
[FW-policy-security] rule name policy_sec_research
[FW-policy-security-rule-policy_sec_research] source-zone trust
[FW-policy-security-rule-policy_sec_research] destination-zone untrust
[FW-policy-security-rule-policy_sec_research] user user-group /default/
research
[FW-policy-security-rule-policy_sec_research] action permit
[FW-policy-security-rule-policy_sec_research] profile url-filter
profile_url_research
[FW-policy-security-rule-policy_sec_research] quit
```

Commit the content security profile.

```
[FW] engine configuration commit
Info: The operation may last for several minutes, please wait.
Info: URL submitted configurations successfully.
Info: Finish committing engine compiling.
```

- File blocking

  # Create file blocking profile **profile_file_internet**. Do not upload any executable file.

  ```
  [FW] profile type file-block name profile_file_internet
  [FW-profile-file-block-profile_file_internet] rule name rule1
  [FW-profile-file-block-profile_file_internet-rule-rule1] application all
  [FW-profile-file-block-profile_file_internet-rule-rule1] file-type pre-
  defined name EXE MSI RPM OCX A ELF DLL PE SYS
  [FW-profile-file-block-profile_file_internet-rule-rule1] direction upload
  [FW-profile-file-block-profile_file_internet-rule-rule1] action block
  [FW-profile-file-block-profile_file_internet-rule-rule1] quit
  [FW-profile-file-block-profile_file_internet] quit
  ```

  # Configure security policy **policy_sec_internet** for traffic from the untrust zone to the DMZ and reference profile **profile_file_internet**.

  ```
  [FW-policy-security] rule name policy_sec_internet
  [FW-policy-security-rule-policy_sec_internet] source-zone untrust
  [FW-policy-security-rule-policy_sec_internet] destination-zone dmz
  [FW-policy-security-rule-policy_sec_internet] destination-address 10.2.0.5 24
  [FW-policy-security-rule-policy_sec_internet] profile file-block
  profile_file_internet
  [FW-policy-security-rule-policy_sec_internet] action permit
  [FW-policy-security-rule-policy_sec_internet] quit
  ```

  # Commit the content security profile.

  ```
  [FW] engine configuration commit
  Info: The operation may last for several minutes, please wait.
  Info: DLP submitted configurations successfully.
  Info: Finish committing engine compiling.
  ```

- Data filtering

  # Configure keyword group **keyword1**.

  ```
  [FW] keyword-group name keyword1
  [FW-keyword-group-keyword1] pre-defined-keyword name confidentiality weight 1
  [FW-keyword-group-keyword1] user-defined-keyword name abc
  [FW-keyword-group-keyword1-keyword-abc] expression match-mode Text "abcd"
  [FW-keyword-group-keyword1-keyword-abc] weight 1
  [FW-keyword-group-keyword1-keyword-abc] quit
  ```

  # Create data filtering profile **profile_data_research**.

  ```
  [FW] profile type data-filter name profile_data_research
  [FW-profile-data-filter-profile_data_research] rule name rule1
  ```

```
[FW-profile-data-filter-profile_data_research-rule-rule1] keyword-group name
keyword1
[FW-profile-data-filter-profile_data_research-rule-rule1] application all
[FW-profile-data-filter-profile_data_research-rule-rule1] file-type all
[FW-profile-data-filter-profile_data_research-rule-rule1] direction upload
[FW-profile-data-filter-profile_data_research-rule-rule1] action block
[FW-profile-data-filter-profile_data_research-rule-rule1] quit
```

Configure security policy **policy_sec_research** and reference profile **profile_data_research**.

```
[FW] security-policy
[FW-policy-security] rule name policy_sec_research
[wzh_x3-policy-security-rule-policy_sec_research] source-zone trust
[wzh_x3-policy-security-rule-policy_sec_research] destination-zone untrust
[wzh_x3-policy-security-rule-policy_sec_research] user user-group /default/
research
[wzh_x3-policy-security-rule-policy_sec_research] profile data-filter
profile_data_research
[wzh_x3-policy-security-rule-policy_sec_research] action permit
[wzh_x3-policy-security-rule-policy_sec_research] quit
```

Commit the content security profile.

```
[FW] engine configuration commit
Info: The operation may last for several minutes, please wait.
Info: DLP submitted configurations successfully.
Info: Finish committing engine compiling.
```

5.1.4.3 Antivirus and Intrusion Prevention

- Antivirus

  When an intranet user attempts to download virus-infected files using HTTP, the download connection is interrupted. When an intranet user attempts to download a virus-infected mail using POP3, the attachments in the mail are deleted.

  # Configure an antivirus profile for HTTP and POP3.

  ```
  [FW] profile type av name av_http_pop3
  [FW-profile-av-av_http_pop3] http-detect direction download action block
  [FW-profile-av-av_http_pop3] pop3-detect action delete-attachment
  [FW-profile-av-av_http_pop3] exception application name Netease_Webmail
  [FW-profile-av-av_http_pop3] exception av-signature-id 1000
  [FW-profile-av-av_http_pop3] quit
  ```

  # Configure a security policy for traffic from the intranet to the Internet (from the trust zone to the untrust zone).

  ```
  [FW] security-policy
  [FW-policy-security] rule name policy_av_1
  [FW-policy-security-rule-policy_av_1] source-zone trust
  [FW-policy-security-rule-policy_av_1] destination-zone untrust
  [FW-policy-security-rule-policy_av_1] action permit
  [FW-policy-security-rule-policy_av_1] profile av av_http_pop3
  [FW-policy-security-rule-policy_av_1] quit
  ```

- Intrusion prevention

  # Configure intrusion prevention profile **profile_ips_pc** to protect intranet users.

  ```
  [FW] profile type ips name profile_ips_pc
  [FW-profile-ips-profile_ips_pc] description profile for intranet users
  [FW-profile-ips-profile_ips_pc] capture-packet enable
  [FW-profile-ips-profile_ips_pc] signature-set name filter1
  [FW-profile-ips-profile_ips_pc-sigset-filter1] target client
  [FW-profile-ips-profile_ips_pc-sigset-filter1] severity high
  [FW-profile-ips-profile_ips_pc-sigset-filter1] protocol HTTP
  [FW-profile-ips-profile_ips_pc-sigset-filter1] quit
  [FW-profile-ips-profile_ips_pc] quit
  ```

  # Commit the configuration.

  ```
  [FW] engine configuration commit
  ```

Configure a security policy for traffic from the trust zone to the untrust zone and reference intrusion prevention profile **profile_ips_pc**.

```
[FW] security-policy
[FW-policy-security] rule name policy_sec_1
[FW-policy-security-rule-policy_sec_1] source-zone trust
[FW-policy-security-rule-policy_sec_1] destination-zone untrust
[FW-policy-security-rule-policy_sec_1] source-address 10.3.0.0 24
[FW-policy-security-rule-policy_sec_1] profile ips profile_ips_pc
[FW-policy-security-rule-policy_sec_1] action permit
[FW-policy-security-rule-policy_sec_1] quit
```

5.1.4.4 Anti-DDoS

For example, the firewall is deployed on the egress of an enterprise network; a web server is deployed on the enterprise network. The web server is often received SYN flood, UDP flood, and HTTP flood attacks. To ensure the normal running of the web server, enable the anti-DDoS function on the firewall to defend against the preceding three types of DDoS attacks.

Set anti-DDoS parameters.

```
[FW] interface GigabitEthernet1/0/1
[FW-GigabitEthernet1/0/1] anti-ddos flow-statistic enable
[FW-GigabitEthernet1/0/1] quit
[FW] ddos-mode detect-clean
```

Configure the threshold learning function.

```
[FW] anti-ddos baseline-learn start
[FW] anti-ddos baseline-learn tolerance-value 100
[FW] anti-ddos baseline-learn apply
```

Enable the anti-DDoS function.

```
[FW] anti-ddos syn-flood source-detect
[FW] anti-ddos udp-flood dynamic-fingerprint-learn
[FW] anti-ddos udp-frag-flood dynamic-fingerprint-learn
[FW] anti-ddos http-flood defend alert-rate 2000
[FW] anti-ddos http-flood source-detect mode basic
```

5.1.4.5 Traffic Policies

You can configure traffic policies to equally and dynamically assign bandwidth resources to each user based on the number of online users.

Configure a traffic profile.

```
[FW] traffic-policy
[FW-policy-traffic] profile profile_dep_a
[FW-policy-traffic-profile-profile_dep_a] bandwidth maximum-bandwidth whole
downstream 60000
[FW-policy-traffic-profile-profile_dep_a] bandwidth average per-user manual
multiplier 2 minimum 1000
[FW-policy-traffic-profile-profile_dep_a] quit
```

Configure a traffic policy.

```
[FW-policy-traffic] rule name policy_dep_a
[FW-policy-traffic-rule-policy_dep_a] source-zone trust
[FW-policy-traffic-rule-policy_dep_a] destination-zone untrust
[FW-policy-traffic-rule-policy_dep_a] user user-group /default/dep_a
[FW-policy-traffic-rule-policy_dep_a] action qos profile profile_dep_a
[FW-policy-traffic-rule-policy_dep_a] quit
```

5.1.4.6 Online Behavior Audit and Management

The firewall serves as the gateway at the border of the enterprise network. You can configure the audit function on the firewall, so that the firewall can record the Internet access behavior of employees.

Configure an audit profile.

```
[FW] profile type audit name profile_audit_1
[FW-profile-audit-profile_audit_1] http-audit url all
[FW-profile-audit-profile_audit_1] http-audit url recorded-title
[FW-profile-audit-profile_audit_1] http-audit file direction download
[FW-profile-audit-profile_audit_1] ftp-audit file direction download
[FW-profile-audit-profile_audit_1] http-audit bbs-content
[FW-profile-audit-profile_audit_1] http-audit micro-blog
[FW-profile-audit-profile_audit_1] quit
```

Configure an audit policy and reference the audit profile.

```
[FW] audit-policy
[FW-policy-audit] rule name policy_audit_1
[FW-policy-audit-rule-policy_audit_1] description Policy of auditing for research.
[FW-policy-audit-rule-policy_audit_1] source-zone trust
[FW-policy-audit-rule-policy_audit_1] destination-zone untrust
[FW-policy-audit-rule-policy_audit_1] user user-group /default/research
[FW-policy-audit-rule-policy_audit_1] time-range time_range
[FW-policy-audit-rule-policy_audit_1] action audit profile profile_audit_1
[FW-policy-audit-rule-policy_audit_1] quit
```

Follow-up procedure

By viewing various reports, audit logs, and user activity logs, you can obtain the online behavior of employees in R&D and marketing departments to implement more accurate security policy control.

5.2 Wireless Service Security

5.2.1 Traffic Limit

To protect the CPU of network devices against malicious attacks and ensure that authorized users can use network resources, you need to set rate limits for control and data traffic based on users. It is recommended that you set rate limits on APs located on the network edge.

- Control traffic limit: The broadcast flood attack is enabled on the AP by default, with the default rate threshold of 10 pps. In high-density scenarios that involve a large traffic volume, for example, in a university campus, you can increase the threshold. However, it is recommended that the adjustment range be no greater than 100%.

  # Set the rate threshold for broadcast flood detection to 15 pps.

  ```
  <AC> system-view
  [AC] wlan
  [AC-wlan-view] vap-profile name profile1
  [AC-wlan-vap-prof-profile1] anti-attack broadcast-flood sta-rate-threshold 15
  ```

- Data traffic limit: In Wi-Fi communication, only one device is allowed to send packets at a time on a channel. To ensure a fair network experience for each user when network bandwidth resources are limited, you need to limit the rates of uplink and downlink packets of all STAs or each individual STA on a VAP. You are advised to limit the rate of each STA on a VAP. In most cases, the uplink and downlink bandwidths of 4 Mbit/s can support common Internet access. In indoor high-density scenarios, it is recommended that the downlink bandwidth be 2 Mbit/s and the uplink bandwidth be 1 Mbit/s.

Set the rate limit for downlink packets to 2048 kbit/s for each STA associated with a VAP in the traffic profile **p1** bound to the VAP.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] traffic-profile name p1
[AC-wlan-traffic-prof-p1] rate-limit client down 2048
```

Set the rate limit for uplink packets to 1024 kbit/s for each STA associated with a VAP in the traffic profile p1 bound to the VAP.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] traffic-profile name p1
[AC-wlan-traffic-prof-p1] rate-limit client up 1024
```

5.2.2 Attack Defense

- The user-level rate limiting function is recommended for X series cards and is enabled by default. User-level rate limiting applies to the following types of packet: ARP Request, ARP Reply, ND, DHCP Request, DHCPv6 Request, and 802.1X. By default, the user-level rate limit is 10 pps. You can adjust the rate limit for specified users.

  # Set the rate limit for MAC address 000a-000b-000c to 20 pps.

  ```
  <AC> system-view
  [AC] cpu-defend host-car mac-address 000a-000b-000c pps 20
  ```

- The penalty function of attack source tracing is recommended for non-X series cards and is enabled by default. After the penalty function of attack source tracing is enabled, the device discards the attack packets sent by the attack source it detected to prevent further attacks from the attack source. If the number of protocol packets for normal services exceeds the threshold for attack source tracing detection and penalty actions are configured, the services may be affected. To restore the services, you can disable the attack source tracing function for all protocols or involved protocols. In indoor high-density scenarios, for example, in universities, it is recommended that you set the timer to between 5 to 20 seconds and punish the attack source by dropping packets within the period of time specified in the timer. If the timer expires, the device cancels the penalty action on the attack source.

  # Configure the device to drop packets sent from attack sources, and set the timer to 10 seconds.

  ```
  <AC> system-view
  [AC] cpu-defend policy mypolicy
  [AC-cpu-defend-policy-mypolicy] auto-defend enable
  [AC-cpu-defend-policy-mypolicy] auto-defend action deny timer 10
  ```

  # Delete IGMP and TTL-expired packets from the list of traced packets.

  ```
  <AC> system-view
  [AC] cpu-defend policy mypolicy
  [AC-cpu-defend-policy-mypolicy ] auto-defend enable
  [AC-cpu-defend-policy-mypolicy ] undo auto-defend protocol igmp ttl-expired
  ```

5.2.3 Multicast or Broadcast Packet Suppression

No ACK mechanism is provided for multicast packet transmission on air interfaces. In addition, wireless links are unstable. To ensure stable transmission of multicast packets, they are usually sent at low rates. If a large number of such multicast packets are sent from the network side, the air interfaces may be congested. You are advised to configure multicast packet suppression to reduce impact of a large number of low-rate multicast packets on the wireless network. Exercise caution when configuring the rate limit; otherwise, the multicast services may be affected.

- In tunnel forwarding mode:
  - You are advised to configure multicast packet suppression in the AC traffic profile to prevent the increasing multicast packets from affecting services.

    # Set the maximum rate of broadcast packets to 128 pps in traffic profile **p1.**

    ```
    <AC> system-view
    [AC] wlan
    [AC-wlan-view] traffic-profile name p1
    [AC-wlan-traffic-prof-p1] traffic-optimize broadcast-suppression packets
    128
    ```

    # Set the maximum rate of multicast packets to 128 pps in traffic profile **p1.**

    ```
    <AC> system-view
    [AC] wlan
    [AC-wlan-view] traffic-profile name p1
    [AC-wlan-traffic-prof-p1] traffic-optimize multicast-suppression packets
    128
    ```
  - If a large number of multicast or broadcast packets are sent from the network side to STAs, the air interface usage of an AP becomes high. If the STAs can be identified, you can configure a traffic policy on the AC to suppress the broadcast or multicast packets sent from the AC to the APs associated with the STAs. Before configuring a traffic policy, check whether the corresponding multicast or broadcast services are available on the live network. The following example describes the procedure for configuring a traffic policy for multicast packet suppression.

    # Create a traffic classifier named **test** and define a matching rule.

    ```
    <AC> system-view
    [AC] traffic classifier test
    [AC-classifier-test] if-match destination-mac 0100-5e00-0000 mac-address-
    mask ffff-ff00-0000   //Match the destination MAC address of the
    multicast packets of a user.
    [AC-classifier-test] quit
    ```

    # Create a traffic behavior named **test**, enable traffic statistics collection, and set the traffic rate limit.

    ```
    [AC] traffic behavior test
    [AC-behavior-test] statistic enable
    [AC-behavior-test] car cir 100   //Set the rate limit to 100 kbit/s. If
    multicast services are available, you are advised to limit the rate
    based on service traffic.
    [AC-behavior-test] quit
    ```

    # Create a traffic policy named **test**, and bind the traffic classifier and traffic behavior to the traffic policy.

    ```
    [AC] traffic policy test
    [AC-trafficpolicy-test] classifier test behavior test
    [AC-trafficpolicy-test] quit
    ```

    # Apply the traffic policy to the outbound direction in an SSID profile. (when native AC is deployed).

    ```
    [AC] wlan
    [AC-wlan] ssid-profile name Guest
    [AC-wlan-ssid-prof-Guest] traffic-policy test outbound
    ```

    # Apply the traffic policy to the inbound direction of the AC interface connected to the network (when an independent AC is deployed).

    ```
    [AC] interface gigabitethernet 0/0/1
    [AC-GigabitEthernet0/0/1] traffic-policy test inbound
    ```
- In direct forwarding mode, you are advised to configure multicast packet suppression on the switch interface directly connected to the AP.

  # Create a traffic classifier named **test** and define a matching rule.

  ```
  <HUAWEI> system-view
  [HUAWEI] sysname SwitchA
  ```

```
[SwitchA] traffic classifier test
[SwitchA-classifier-test] if-match destination-mac 0100-5e00-0000 mac-address-
mask ffff-ff00-0000   //Match the destination MAC address of multicast
packets.
[SwitchA-classifier-test] quit
```

Create a traffic behavior named **test**, enable traffic statistics collection, and set the traffic rate limit.

```
[SwitchA] traffic behavior test
[SwitchA-behavior-test] statistic enable
[SwitchA-behavior-test] car cir 100   //Set the rate limit to 100 kbit/s. If
multicast services are involved, you are advised to limit the rate based on
service traffic.
[SwitchA-behavior-test] quit
```

Create a traffic policy named **test**, and bind the traffic classifier and traffic behavior to the traffic policy.

```
[SwitchA] traffic policy test
[SwitchA-trafficpolicy-test] classifier test behavior test
[SwitchA-trafficpolicy-test] quit
```

Apply the traffic policy to the inbound and outbound directions of the interface.

```
[SwitchA] interface gigabitethernet 0/0/1
[SwitchA-GigabitEthernet0/0/1] traffic-policy test inbound
[SwitchA-GigabitEthernet0/0/1] traffic-policy test outbound
[SwitchA-GigabitEthernet0/0/1] quit
```

5.2.4 User Authentication

WPA2+802.1X Access

In indoor high-density scenarios of a university, for example, in a lecture hall, the WPA2-AES encryption mode is recommended, together with the 802.1X authentication mode.

Configure WPA2 802.1X+AES authentication and encryption mode.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] security-profile name p1
[AC-wlan-sec-prof-p1] security wpa2 dot1x aes
```

If multiple types of STAs connect to the network and they support different authentication and encryption modes, you can configure hybrid encryption and authentication modes.

Configure WPA-WPA2 hybrid encryption and 802.1X authentication.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] security-profile name p1
[AC-wlan-sec-prof-p1] security wpa-wpa2 dot1x aes-tkip
```

MAC Address-Prioritized Portal Access

In high-density scenarios of a university, it is recommended that MAC address-prioritized Portal access be configured in public areas, such as auditoriums and canteens. If authenticated users move out of the wireless signal coverage area and move in again within a certain period (60 minutes for example), they can connect to the wireless network directly without entering their user names and passwords again.

In the Portal authentication scenario, users may use spoofed IP addresses for authentication, which brings security risks. It is recommended that you configure attack defense functions such as IPSG and DHCP snooping to avoid security risks.

RADIUS Timeout Configuration

Configure the minimum RADIUS retransmission timeout interval for a large or busy network. A large timeout interval wastes system resources, and a smaller timeout interval can improve the processing capability of the AC.

The default retransmission timeout interval for wireless users is 2s. If more than eight authentication server IP addresses are configured in the RADIUS server profile or 802.1X authentication is used, you are advised to set the timeout interval to 1s for higher network processing efficiency.

Set the retransmission timeout interval to 1s.

```
<AC> system-view
[AC] radius-server template test1
[AC-radius-test1] radius-server timeout 1
```

RADIUS Accounting Configuration

If the accounting server is configured to charge users by duration, the accounting server may be unable to receive Accounting Stop packets after users go offline unexpectedly. The accounting server may continue to charge the users instead. To solve this problem, you can configure real-time accounting on the AC.

A shorter time interval for real-time accounting requires higher performance of the AC and accounting server. If there are more than 1000 users, a long interval for real-time accounting is recommended. It is recommended that the accounting interval be set to 15 minutes for high-density scenarios in universities.

In the accounting scheme named **scheme1**, enable the real-time accounting function and set the interval for real-time accounting to 15 minutes.

```
<AC> system-view
[AC] aaa
[AC-aaa] accounting-scheme scheme1
[AC-aaa-accounting-scheme1] accounting-mode radius
[AC-aaa-accounting-scheme1] accounting realtime 15
[AC-aaa-accounting-scheme1] quit
```

Set a real-time accounting interval based on the user quantity. The following table lists the recommended real-time accounting intervals for different user quantities.

User Quantity	Real-Time Accounting Interval
1-99	3 minutes
100-499	6 minutes
500-999	12 minutes
≥ 1000	≥ 15 minutes

5.2.5 Border Security

5.2.5.1 Technology Introduction

Wireless networks are vulnerable to threats from unauthorized AP users, ad-hoc networks, and denial of service (DoS) attacks.

A wireless intrusion detection system (WIDS) can detect unauthorized users and APs. A wireless intrusion prevention system (WIPS) can protect enterprise networks and users against access from unauthorized devices.

- WIDS against rogue devices

  Monitor APs can be configured on a network to prevent intrusion to the network. When configured with the WIDS function, monitor APs periodically listen on wireless signals. The AC can then obtain information about wireless devices from the monitor APs and take measures to prevent access from unauthorized devices.

  Before configuring WIDS on an AP, configure the working mode of the AP.

  An AP can work in two modes:

  - normal: The radio works in normal mode.
    - If air interface scanning is disabled, the radio transmits basic WLAN service data.
    - If air interface scanning is enabled, the radio provides monitoring functions in addition to transmitting basic WLAN service data. The monitoring functions may affect common WLAN services.
  - monitor: The AP working in monitor mode does not provide basic WLAN services. It only provides WLAN services with monitoring functions, such as WIDS, spectrum analysis, and STA location.

  WIDS consists of two phases: wireless device identification and rogue device identification.

- Containment against rogue devices

  An AC contains three types of unauthorized devices:

  - Rogue AP

    After an AC identifies a rogue AP, it sends information about the rogue AP to a monitor AP. The monitor AP uses the identity information about the rogue AP to broadcast a Deauthentication frame. After STAs that associate with the rogue AP receive the Deauthentication frame, they disassociate from the rogue AP. This containment mechanism prevents STAs from associating with rogue APs.

    NOTE

    Deauthentication frames are used to terminate established wireless links. Either an AP or a STA can send a Deauthentication frame to terminate an established link. Currently, an AC supports only containment on rogue APs and unauthorized APs with open authentication. Rogue APs are unauthorized APs that have the same SSIDs as or similar SSIDs to authorized APs.

  - Rogue STA

    After an AC identifies a rogue STA, it sends information about the rogue STA to a monitor AP. The monitor AP uses the identity information about the rogue STA to unicast a Deauthentication frame. After the AP with which the unauthorized STA associates receives the Deauthentication frame, the AP disassociates from the rogue STA. This containment mechanism prevents APs from associating with rogue STAs.

  - Ad-hoc device

After an AC identifies an ad-hoc device, it sends information about the ad-hoc device to a monitor AP. The monitor AP uses the identity information about the ad-hoc device (BSSID and MAC address of the device) to unicast a Deauthentication frame. After the STAs that associate with the ad-hoc device receive the Deauthentication frame, the STAs disassociate from the ad-hoc device. This containment mechanism prevents STAs from associating with ad-hoc devices.

Configure AP radio 0 to work in monitor mode.

```
[AC-wlan-ap-group-ap-group2] radio 0
[AC-wlan-group-radio-ap-group2/0] work-mode monitor
Warning: Modify the work mode may cause business interruption, continue?
(y/n): y
```

Configure WIDS and WIPS functions to enable wireless device detection and containment.

```
[AC-wlan-group-radio-ap-group2/0] wids device detect enable
[AC-wlan-group-radio-ap-group2/0] wids contain enable
[AC-wlan-group-radio-ap-group2/0] quit
[AC-wlan-ap-group-ap-group2] quit
```

Create a WIDS profile named **wlan-wids** and configure the AC to contain rogue APs.

```
[AC-wlan-view] wids-profile name wlan-wids
[AC-wlan-wids-prof-wlan-wids] contain-mode spoof-ssid-ap
[AC-wlan-wids-prof-wlan-wids] quit
```

Bind the WIDS profile **wlan-wids** to the AP group **ap-group2**.

```
[AC-wlan-view] ap-group name ap-group2
[AC-wlan-ap-group-ap-group2] wids-profile wlan-wids
[AC-wlan-ap-group-ap-group2] quit
```

Commit the configuration.

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

- Attack detection

  On small- and medium-sized WLANs, attack detection can be enabled to allow an AP to add attackers to a dynamic blacklist and send alarms to the AC to alert administrators. When enabled, attack detection can detect the following types of attack: flood attack, weak IV attack, and spoofing attack.

  The following is a configuration example:

  # Enable detection of brute force key cracking attacks and flood attacks in WPA2-PSK authentication mode.

```
[AC-wlan-view] ap-group name ap-group1
[AC-wlan-ap-group-ap-group1] radio 0
[AC-wlan-group-radio-ap-group1/0] wids attack detect enable wpa2-psk
[AC-wlan-group-radio-ap-group1/0] wids attack detect enable flood
[AC-wlan-group-radio-ap-group1/0] quit
[AC-wlan-ap-group-ap-group1] quit
```

  # Set the interval, quantity threshold, and quiet time for flood attack detection to 70s, 350, and 700s, respectively.

```
[AC-wlan-wids-prof-wlan-wids] flood-detect interval 70
[AC-wlan-wids-prof-wlan-wids] flood-detect threshold 350
[AC-wlan-wids-prof-wlan-wids] flood-detect quiet-time 700
```

  # Enable the dynamic blacklist function.

```
[AC-wlan-wids-prof-wlan-wids] dynamic-blacklist enable
[AC-wlan-wids-prof-wlan-wids] quit
```

  # Create an AP system profile named **wlan-system** and set the aging time of the dynamic blacklist to 200s.

```
[AC-wlan-view] ap-system-profile name wlan-system
[AC-wlan-ap-system-prof-wlan-system] dynamic-blacklist aging-time 200
[AC-wlan-ap-system-prof-wlan-system] quit
```

- Defense against brute force PSK cracking

  During a brute force attack, the attacker searches for a password by trying to use all possible password combinations. This method is also called the exhaustive attack method. For example, a password that contains only 4 digits may have a maximum of 10,000 combinations. Therefore, the password can be decrypted after a maximum of 10,000 attempts. In theory, the brute force method can decrypt any password. Attackers, however, are always looking for ways to shorten the time required to decrypt passwords. When a WLAN uses WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key as the security policy, attackers can use the brute force method to decrypt the password.

  Defense against brute force PSK cracking can prolong the time needed to decrypt passwords. An AP checks whether the number of key negotiation attempts during WPA/WPA2-PSK, WAPI-PSK, or WEP-Shared-Key authentication exceeds the configured threshold. If the threshold is exceeded, the AP considers that the user is using the brute force method to decrypt the password and reports an alarm to the AC. If the dynamic blacklist function is enabled, the AP adds the user to the dynamic blacklist and discards all the packets of the user until the dynamic blacklist entry is aged.

  # Create a WIDS profile named **wlan-wids**.

  ```
  [AC-wlan-view] wids-profile name wlan-wids
  ```

  # Set the interval, maximum number of key negotiation failures allowed within the time interval, and quiet time for brute force PSK cracking detection to 70s, 25, and 700s, respectively.

  ```
  [AC-wlan-wids-prof-wlan-wids] brute-force-detect interval 70
  [AC-wlan-wids-prof-wlan-wids] brute-force-detect threshold 25
  [AC-wlan-wids-prof-wlan-wids] brute-force-detect quiet-time 700
  ```

5.2.5.2 Best Practices

WIDS Is Not Recommended

WIDS enables monitor APs to periodically detect wireless signals. In this manner, the AC can obtain information about devices on the wireless network and take measures to prevent access from rogue devices. However, frequent monitoring and reporting results in deterioration of AC performance. Therefore, you are advised not to enable the WIDS function unless necessary.

Channel Scanning for Rogue Devices

If the WIDS function is enabled, the AP scans all channels supported by the corresponding country code by default. Frequent scanning degrades AC performance. Therefore, it is recommended that only calibration channels be scanned.

Configure an air scan channel set that contains all calibration channels.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] air-scan-profile name huawei
[AC-wlan-air-scan-prof-huawei] scan-channel-set dca-channel
```

Properly Configure the Interval for Reporting Unauthorized Devices

By default, an AP reports incremental wireless device information to an AC at an interval of 300 seconds. A shorter reporting interval helps detect suspicious devices in a timely manner. However, when the reporting interval is too short, devices may be mistakenly reported as unauthorized if they go offline shortly after they go online. The result may therefore be inaccurate, and more AP and AC resources may be occupied. Therefore, you are advised not to change the default reporting interval.

In high-density scenarios, you are advised to set the interval for reporting wireless device information to 300-600 seconds if you do not have requirements on real-time wireless device reporting.

Set the interval at which an AP reports incremental wireless device information to 400 seconds.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] air-scan-profile name huawei
[AC-wlan-view] ap-group name default
[AC-wlan-ap-group-default] radio 0
[AC-wlan-group-radio-default/0] wids device detect enable
[AC-wlan-group-radio-default/0] quit
[AC-wlan-ap-group-default] quit
[AC-wlan-view] wids-profile name default
[AC-wlan-wids-prof-default] device report-interval 400
```

5.2.6 Service Security

A wireless network also faces common security threats on the IP network. For example, devices may be spoofed and signals may be intercepted and tampered with. To ensure security on the backhaul network, Huawei WLAN devices support the following security features:

DTLS

CAPWAP tunnels use Datagram Transport Layer Security (DTLS) encryption, sensitive information encryption, integrity check, and heartbeat detection technologies to ensure security.

- DTLS encryption: When an AP establishes CAPWAP tunnels with an AC, the AP determines whether to perform DTLS negotiation with the AC. The DTLS protocol can be used to encrypt packets exchanged between the AP and AC to ensure integrity and privacy of the management packets. Currently, the devices can only encrypt management packets using the pre-shared key (PSK). DTLS encryption affects AC performance. You are advised to disable DTLS encryption unless your site has special security requirements.
- Sensitive information encryption: This security mechanism can be configured if sensitive information (such as FTP user name and password, AP login user name and password, and PSK for service configuration) is transmitted between an AP and AC.
- Integrity check: When CAPWAP packets are transmitted between ACs and APs, the packets may be intercepted or tampered with. An attacker may construct and send malformed packets to attack APs and ACs. The integrity check mechanism protects CAPWAP packets between ACs and APs.
- Heartbeat detection: An AP and an AC periodically exchange Echo packets to determine whether the control tunnel is working properly and periodically exchange Keepalive packets to determine whether the data tunnel is working properly. If the AP or AC does

not receive any response from each other after Echo or Keepalive packets are sent for a specified number of times, the AP or AC considers that the control or data tunnel is terminated and re-establishes the tunnel.

Configuration Item		Procedure	Description
Configure DTLS encryption.	Allow the AP to establish a DTLS session with the AC using the default PSK.	**capwap dtls psk-mandatory-match enable** By default, an AP is disabled from using the default PSK to establish a DTLS session with an AC.	An AP can use a default or configured PSK to establish a DTLS session with an AC. If an AP is allowed to use the default PSK to establish a DTLS session with an AC, and a PSK is configured for DTLS encryption, the PSKs are used in the following ways: ● The AP uses the default PSK during login and uses the configured PSK for re-login after being restarted. ● When the AP and AC have different PSKs (because the AC changes the password multiple times while the AP is offline), the AP uses the default PSK to initiate a DTLS session after three consecutive DTLS session failures. It is recommended that you change the default PSK in a timely manner to ensure device security.
	Configure the PSK used for DTLS encryption.	**capwap dtls psk** *psk-value* By default, the PSK used for DTLS encryption is **huawei_seccwp**.	
	Enable DTLS encryption for control tunnels.	**capwap dtls control-link encrypt** By default, the function of encrypting the CAPWAP control tunnel using DTLS is disabled.	
Configure sensitive information encryption.	Configure a PSK for encrypting sensitive information.	**capwap sensitive-info psk** By default, the default PSK is used for encrypting sensitive information.	

User Isolation

To secure user communication, configure user isolation in the traffic profile so that packets cannot be forwarded between users on the same VAP (that is, users cannot communicate with each other). User traffic is instead centrally forwarded by the gateway, facilitating management operations such as accounting.

- In tunnel forwarding mode, enable user isolation in the traffic profile to isolate all users on a VAP at Layer 2 or Layer 3.
- In direct forwarding mode, enable user isolation in the traffic profile. You are advised to configure port isolation on the interface of the access switch connected to the AP.

Set the user isolation mode to Layer 2 isolation and Layer 3 interworking in traffic profile **p1**.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] traffic-profile name p1
[AC-wlan-traffic-prof-p1] user-isolate l2
Warning: This action may cause service interruption. Continue?[Y/N] y
```

Port Isolation

In wireless application scenarios, APs do not need to communicate with each other at Layer 2 or forward broadcast packets to each other. Therefore, port isolation must be configured on the interface of the access switch connected to APs to secure user communication and prevent invalid broadcast packets from being transmitted to APs. Preventing broadcast packets ensures that APs can forward user services properly.

Configure port isolation on GE1/0/1 of the access switch.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] port-isolate enable
```

ACL

You can configure ACL-based packet filtering in a traffic profile for providing differentiated services for wireless users. For example, some wireless users are denied or allowed to access certain LAN devices and wireless users are not allowed to access some illegal IP addresses.

The device first matches packets and performs actions based on the matching policy:

- If the action in the ACL rule is deny, the device discards packets matching the rule.
- If the action in the ACL rule is permit, the device allows packets matching the rule to pass through.
- Packets that match no rule are allowed to pass through.

If multiple ACL-based packet filtering commands in the same direction are configured in a traffic profile, a packet is matched according to the command configuration order. If one command is matched, the corresponding policy is executed and the matching is stopped. Otherwise, the next command is matched. If all commands are not matched, the packet is allowed to pass through.

You can only configure a maximum of eight ACL rules in the same direction. The sequence in which ACL rules take effect follows the sequence in which the rules are configured. To change the current packet filtering rules, delete all the related configurations and reconfigure the ACL-based packet filtering.

The configuration can reference a numbered ACL (ACL number only) that is not configured. You can configure the referenced ACL after running this command.

Create the traffic profile p1 and configure packet filtering in the inbound direction based on the ACL that permits packets with the source IPv4 address 192.168.0.2/32.

```
<AC6605> system-view
[AC6605] acl 3000
[AC6605-acl-adv-3000] rule 5 permit ip source 192.168.0.2 0
[AC6605-acl-adv-3000] quit
[AC6605] wlan
[AC6605-wlan-view] traffic-profile name p1
[AC6605-wlan-wlan-traffic-prof-p1] traffic-filter inbound ipv4 acl 3000
```

VAP Security

You are advised to enable IPSG for an AP in the VAP profile to prevent IP packets of unauthorized users from entering the external network through the AP.

It is recommended that you enable dynamic ARP detection in the VAP profile. The AP then checks the ARP Request and Reply packets transmitted on all VAPs of the AP, discards invalid and attack ARP packets, and reports an alarm to the AC. This function prevents ARP packets from unauthorized users from entering the external network through the AP, protecting authorized users against interference or spoofing and protecting the AP against CPU attacks.

You are advised to enable strict STA IP address learning through DHCP in the VAP profile, so that STAs associate with the AP. When the STAs obtain IP addresses through DHCP, the AP automatically reports the IP addresses to the AC, so that the mapping between STA IP addresses and MAC addresses can be maintained.

```
[AC6605] wlan
[AC6605-wlan-view] vap-profile name vap1
[AC6605-wlan-vap-prof-vap1] ip source check user-bind enable
[AC6605-wlan-vap-prof-vap1] arp anti-attack check user-bind enable
[AC6605-wlan-vap-prof-vap1] learn-client-address dhcp-strict
```

5.2.7 User Access Security

Link authentication, access authentication, and data encryption are used to ensure validity and security of user access on wireless networks.

Four WLAN security policies are available: Wired Equivalent Privacy (WEP), Wi-Fi Protected Access (WPA), WPA2, WLAN Authentication and Privacy Infrastructure (WAPI). Each security policy has a series of security mechanisms, including the link authentication mechanism used to establish a wireless link, user access authentication mechanism used when users attempt to connect to a wireless network, data encryption mechanism used during data transmission, and STA access control based on a blacklist or whitelist.

- WEP

  WEP, defined in IEEE 802.11, is used to protect data of authorized users from being intercepted during transmission on a WLAN. WEP uses the RC4 algorithm to encrypt data using a 64-bit, 128-bit, or 152-bit encryption key. An encryption key contains a 24-bit initialization vector (IV) generated by the system, so the length of the key configured on the WLAN server and client is 40 bits, 104 bits, or 128 bits. WEP uses a static encryption key. That is, all STAs associating with the same SSID use the same key to connect to the wireless network.

  A WEP security policy defines a link authentication mechanism and a data encryption mechanism.

Link authentication mechanisms include open system authentication and shared key authentication.

- If open system authentication is used, data is not encrypted during link authentication. After a user goes online, service data can be encrypted by WEP or not, depending on the configuration.
- If shared key authentication is used, the WLAN client and server complete key negotiation during link authentication. After a user goes online, service data is encrypted using the negotiated key.

- WPA/WPA2

  WEP shared key authentication uses the RC4 symmetric stream cipher to encrypt data. This authentication method requires the same static key pre-configured on the server and client. Both the encryption mechanism and encryption algorithm are vulnerable to security threats. The Wi-Fi Alliance developed WPA to overcome defects in WEP before more secure policies are provided in 802.11i. WPA still uses the RC4 algorithm, but it defines the Temporal Key Integrity Protocol (TKIP) encryption algorithm based on WEP, uses the 802.1X identity authentication framework, and supports Extensible Authentication Protocol-Protected Extensible Authentication Protocol (EAP-PEAP) and EAP-Transport Layer Security (EAP-TLS) authentication. Later, 802.11i defined WPA2. WPA2 uses a more secure encryption algorithm: Counter Mode with CBC-MAC Protocol (CCMP).

  Both WPA and WPA2 can use 802.1X access authentication and the TKIP or CCMP encryption algorithm, giving better compatibility. WPA and WPA2 provide almost the same security level, with the only difference being the protocol packet format used.

  The WPA/WPA2 security policy involves four phases: link authentication, access authentication, key negotiation, and data encryption.

- WAPI

  WAPI is a Chinese national standard for WLANs, which was developed based on IEEE 802.11. WAPI provides higher security than WEP and WPA, and consists of the following parts:

  WLAN Authentication Infrastructure (WAI): authenticates user identities and manages keys on WLANs.

  WLAN Privacy Infrastructure (WPI): protects data transmitted on WLANs and provides the data encryption, data verification, and anti-replay functions.

  WAPI uses the elliptic curve cryptography (ECC) algorithm based on the public key cryptography and the block key algorithm based on the symmetric-key cryptography. The ECC algorithm is used for digital certificate authentication and key negotiation between wireless devices. The block key algorithm is used to encrypt and decrypt data transmitted between wireless devices. The two algorithms implement identity authentication, link authentication, access control, and user information encryption.

  WAPI has the following advantages:

  - Bidirectional identity authentication

    Bidirectional identity authentication prevents access from unauthorized STAs and protects a WLAN against attacks from unauthorized WLAN devices.

  - Digital certificates as identity credentials

    A WAPI system has an independent certificate server. STAs and WLAN devices use digital certificates to prove their identities, improving network security. When a STA requests to join or leave a network, the administrator only needs to issue a certificate to the STA or revoke the certificate of the STA.

- Well-developed authentication protocol

  WAPI uses digital certificates to identify STAs. During identity authentication, the elliptic curve digital signature algorithm is used to verify a digital certificate. In addition, the secure message hash algorithm is used to ensure message integrity, which prevents attackers from tampering with or forging information transmitted during identity authentication.

  The following table gives recommendations on configuring a WLAN security policy. In public places with high user mobility (such as airports, stations, business centers, conference halls, and sports stadiums), a WLAN security policy should be configured together with Portal authentication, which supports authentication, accounting, authorization, and information pushing.

Table 5-1 Recommendations on configuring a WLAN security policy

Security Policy	Recommended Configuration Scenario	Description	User Access Authentication Mode
Open system authentication	Public places with high user mobility, such as airports, stations, business centers, exhibition halls, and sports stadiums. Open system authentication should be configured together with Portal authentication, which supports user authentication, accounting, authorization, and information pushing.	It is not secure to use open system authentication independently because any wireless terminals can access the network without authentication. You are advised to configure open system authentication together with Portal authentication or MAC address authentication.	External Portal authentication Built-in Portal authentication MAC address authentication
WEP	None	This security policy is not recommended due to its low security.	None
WPA/WPA2-PSK authentication	Individual or home networks	This security policy has higher security than WEP. Additionally, no third-party server is required and the cost is low.	None

Security Policy	Recommended Configuration Scenario	Description	User Access Authentication Mode
WPA/ WPA2-802.1X authentication	Scenarios with fixed users and requiring high security and centralized user management and authorization, such as mobile offices, campus networks, and mobile governments	This security policy provides high security and requires a third-party server.	802.1X authentication
WAPI-PSK authentication	None	This security policy has higher security than WEP and requires no third-party server. Only some terminals support the protocol.	None
WAPI-certificate authentication	None	This security policy has high security and requires a third-party server. Only some terminals support the protocol.	None

- STA blacklist and whitelist

  On a WLAN, a STA blacklist or whitelist can be configured to filter access from STAs based on specified rules. The blacklist or whitelist allows authorized STAs to connect to the WLAN and rejects access from unauthorized STAs. The STA blacklist and whitelist increase the burden on the AC and degrade AC performance. Therefore, the STA blacklist and whitelist are not recommended, unless otherwise required.

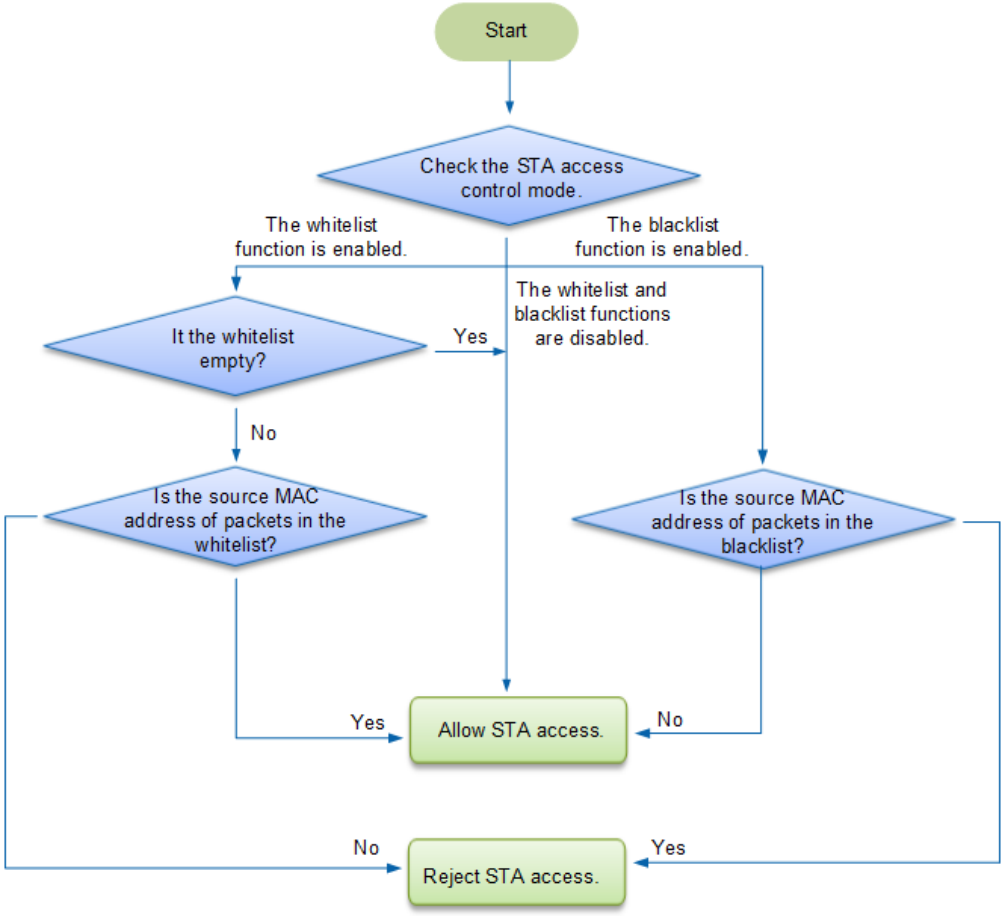
  - STA whitelist

    A STA whitelist contains MAC addresses of STAs that are allowed to connect to a WLAN. After the whitelist function is enabled, only the STAs in the whitelist can connect to the WLAN, and access from other STAs is rejected.

  - STA blacklist

    A STA blacklist contains MAC addresses of STAs that are not allowed to connect to a WLAN. After the blacklist function is enabled, STAs in the blacklist cannot connect to the WLAN, and other STAs can connect to the WLAN.

Figure 5-1 STA blacklist and whitelist working process



The following is an example for configuring a VAP-based STA whitelist.

Create the STA whitelist profile **sta-whitelist** and add MAC addresses of STA1 and STA2 to the whitelist.

```
[AC-wlan-view] sta-whitelist-profile name sta-whitelist
[AC-wlan-whitelist-prof-sta-whitelist] sta-mac 0011-2233-4455
[AC-wlan-whitelist-prof-sta-whitelist] sta-mac 0011-2233-4466
[AC-wlan-whitelist-prof-sta-whitelist] quit
```

Create the VAP profile **wlan-vap** and bind the STA whitelist profile to the VAP profile.

```
[AC-wlan-view] vap-profile name wlan-vap
[AC-wlan-vap-prof-wlan-vap] sta-access-mode whitelist sta-whitelist
[AC-wlan-vap-prof-wlan-vap] quit
```

The following is an example for configuring a global STA blacklist.

Create the STA blacklist profile **sta-blacklist** and add MAC addresses of STA3 and STA4 to the blacklist.

```
[AC-wlan-view] sta-blacklist-profile name sta-blacklist
[AC-wlan-blacklist-prof-sta-blacklist] sta-mac 0011-2233-4477
[AC-wlan-blacklist-prof-sta-blacklist] sta-mac 0011-2233-4488
[AC-wlan-blacklist-prof-sta-blacklist] quit
```

Create the AP system profile **wlan-system** and bind the STA blacklist profile to the AP system profile.

```
[AC-wlan-view] ap-system-profile name wlan-system
[AC-wlan-ap-system-prof-wlan-system] sta-access-mode blacklist sta-blacklist
[AC-wlan-ap-system-prof-wlan-system] quit
```

6 Agile Feature Design and Best Practices

Agile features include free mobility and wired and wireless convergence. The two features can be deployed independently or together. Consider the following when deploying free mobility and wired and wireless convergence.

- Consider access authentication points and policy enforcement points during free mobility deployment. Plan security groups and security policies on the entire network. That is, divide users, resources, and devices into different security groups and configure inter-group access control policies based on security requirements. In addition, specify the deployment positions for authentication devices and policy enforcement devices.
- In wired and wireless convergence planning, specify the device types, deployment positions, access mode of APs, and active/standby work mode. In addition, determine the data forwarding mode for wireless access users and the authentication mode of wired and wireless users.

6.1 Free Mobility

With the construction and promotion of enterprise wireless networks, users have urgent demands for network access at any time and place using any terminals while ensuring a consistent experience.

For the sake of information assets security, enterprises categorize users and grant them different permissions to access information assets, by defining the IP address ranges of the data center servers that users are permitted to access. On a traditional campus network, users' network access permissions are controlled using VLANs and ACLs. In this mode, users' access permissions are bound to IP addresses. Access permissions can be difficult to control if a user moves to another place or a user's IP address changes. In addition, the deployment workload is heavy and users cannot gain a consistent experience. Theoretically, ACLs can be used on traditional campus networks to control network access of any users. However, the IP addresses of the same type of users cannot be aggregated into a network segment. Therefore, a large number of ACLs need to be configured to cover all required IP addresses, which is difficult to implement. Due to limitations in technology, traditional campus networks require users to have fixed locations and different users to be located in different physical areas to facilitate network policy configuration.

Free mobility addresses the requirement of "physical isolation". This solution leverages innovative technology that uses topology-independent security groups to control users'

network access permissions. Focusing on services, users, and experience, the free mobility solution uses service languages and global user groups in replacement of VLAN/ACL/IP to implement policy control, so that policies and network resources can migrate with users.

The enterprise administrator can select an appropriate authentication and authorization solution based on the site scenarios. If the network services do not need to be differentiated among users and are provided to all intranet users, free mobility is not required, and NAC can be used instead for simple authorization management. Free mobility is recommended if network services need to be differentiated among users so different users access different servers, and if there are different types of users on the same network segment or users need to be isolated. Free mobility ensures same network access polices for users regardless of their locations and IP addresses.

The Agile Controller-Campus functions as the authentication center to provide user authentication and centralized management of online information. The Agile Controller-Campus can divide users and resources on the entire network into different security groups from multiple dimensions and centrally manage network-wide policies. It collects user IP addresses in real time, generates dynamic mappings between IP addresses and security groups, and synchronizes the mappings to network devices. A network device finds source and destination security groups that match the source and destination IP addresses of packets based on the dynamic mappings between IP addresses and security groups, and then finds the matching inter-group policy based on the source and destination security groups. Therefore, when configuring a policy, the administrator does not need to consider the IP address range of each type of users. Instead, the administrator only needs to know what servers each type of users access. In this way, service policies and IP addresses are completely decoupled.

Design roadmap for free mobility:

1. **Classify users and servers**
2. **Plan security groups**
3. **Select user authentication points and policy enforcement points**
4. **Select authentication technology**
5. **Plan policies for security groups**

6.1.1 Classifying Users and Servers

User Classification

Free mobility supports refined user rights management and users can be classified in the following dimensions:

- User information
  - Department, such as HR department, Marketing department, and R&D department
  - Role, such as R&D personnel, service personnel, sales personnel, and finance personnel
  - Account: user name used to access the network
- Location information
  - Access device group: physical locations of devices from which users access the network, for example, the offices or buildings where the access devices are located

    Terminal IP address range: range of IP addresses used to connect to the network

    SSID: SSID used to access a WLAN

- Other information
  - Terminal device group: terminal used to connect to the network, for example, a PC running Windows or a smart terminal running Android
  - Time range: range of time during which users are online
  - Customized condition: RADIUS attributes carried in authentication packets, used to determine the current login environment

Categories must be entirely exclusive of one another. This is to ensure that a terminal belongs to only one user category at a time. For example, "R&D department" and "R&D department using wireless access" cannot coexist as two categories, but "R&D department using wired access" and "R&D department using wireless access" should coexist.

There is one situation in which one category can encompass another. For example, a certain type of users use fixed IP addresses, and among these users there are a few privileged ones who have special rights in addition to the basic rights of this type of users. In addition, the administrator knows the IP addresses used by the privileged users. To simplify subsequent user policy configuration, define these privileged users as a sub-category of the users who use fixed IP addresses. In this situation, the two categories are not entirely exclusive of each other, but one category encompasses the other.

Server Classification

Servers are classified based on an enterprise's classification of data center application systems and planning of network permissions. There are two dimensions in which servers can be classified:

- Type: Servers of the same type and function can be classified into a category.
- Permission: Servers that can be accessed by the same type of users can be grouped into one category.

Servers are generally classified by type to facilitate policy adjustment in case of service changes. For example, an enterprise can have an official website, mail system, file sharing system, OA system, and ERP system. Assume that the enterprise has only two types of users: employees and visitors. All servers are accessible to employees, whereas visitors can access only the official website. Based on user permissions, the four other types of servers of the enterprise can be grouped into one category without affecting the solution deployment and access control effect, but this category is not easy to expand. For example, if a new user type is added and these users are not allowed to access the ERP system, the category that contains the four types of server IP addresses needs to be split up. Therefore, it is recommended that you classify servers of the same type or security level into one category in the design phase, so the classification can still apply when the user types and permissions change in the future.

Due to the IP address planning of servers, a network segment of servers may contain special server IP addresses or combinations of IP address and ports. To simplify policy configuration, a category for server IP addresses can encompass another. For example, you can define categories named "public zone servers" and "public zone servers accessible to visitors". The two categories can coexist although the first category encompasses the second one.

In addition to the IP address range of basic service servers, collect the IP address range for the network devices that use static IP addresses for communication, including:

- IP addresses of pre-authentication domain servers (servers accessible before users are authenticated)
- IP addresses of the DMZ servers (intranet servers accessible to public IP addresses)

- Interface IP addresses of network devices (Layer 3 switches, routers, and firewalls)
- IP addresses of authentication-free user terminals (such as some privileged users and dumb terminals that do not need to be authenticated)
- Public network address range provided by ISP carriers (Some enterprises have multiple ISP egresses. Different control policies need to be implement for traffic transmitted through different egresses, so you need to determine the public network addresses managed by each ISP.)

6.1.2 Planning Security Groups

Unlike the traditional IP-based ACL control solution, the free mobility solution classifies different types of network objects with different permissions into different security groups and defines policies using user languages.

Security group planning determines the number of security groups to be created.

Security groups are classified into dynamic user security groups and static resource security groups, depending on network objects.

- Dynamic user security group: It is comprised of users or terminals that can access the network only after authentication.
- Static resource security group: It is comprised of terminals using fixed IP addresses, including data center servers, interface addresses of network devices, and users who access the network using fixed IP addresses without authentication.

Planning for Dynamic User Security Groups

Before designing dynamic user security groups, classify the users based on user rights and network service levels. Group users with the same network resource access rights and network service levels into one category. Each user category corresponds to one security group.

Security groups in the free mobility solution use a flattened architecture and are entirely exclusive of each other. A user terminal can belong to only one security group at a time. After users are grouped into different categories, ensure that categories do not overlap each other and do not contain the same users.

After user are classified, configure authorization rules to describe users of different categories.

An authorization rule is composed of two parts:

- Authorization condition: Users are described based on their login conditions. For details about user classification, see **6.1.1 Classifying Users and Servers**.
- Authorization result: Users matching the authorization conditions are associated with the security group specified in the authorization result at login. That is, the users are assigned certain identities and permissions.

Planning for Static Resource Security Groups

The planning for static resource security groups of an enterprise is determined by the enterprise's classification of data center application systems and network plan. Similar to the planning for dynamic user security groups, static resources accessible to the same type of users can be added to the same security group.

When you design security groups for static resources, determine whether a security group named "Internet" needs to be planned to include Internet users or servers.

Most enterprise networks have two types of Internet-related traffic:

- Traffic generated when intranet users access the Internet
- Traffic generated when hosts on the Internet access intranet servers if the enterprise provides network services for external networks.

Internet hosts are not authenticated on the intranet. If the administrator does not add the Internet addresses to a static resource security group, the previous two types of traffic will match the "intranet user accesses unknown group" and "unknown group accesses server" policies. A switch that functions as an authentication point can only identify locally authenticated users. When locally authenticated users access users that go online on other authentication points, the local switch processes packets based on the "intranet user accesses unknown group" policy. If an enterprise takes different actions for the two types of traffic, for example, the enterprise allows mutual access between users authenticated by different switches but prohibits intranet users from accessing the Internet, the actions of the "intranet user accesses unknown group" policy conflict.

To resolve this problem, define Internet as a static resource security group and configure a policy for intranet users that access the Internet.

Based on experience in deploying traditional campus networks, an enterprise typically needs to plan the following static resource security groups:

- Pre-authentication domain server group (includes servers accessible before users are authenticated)

  To complete user authentication, hosts must access certain servers before or during the authentication, such as the domain server, Portal server, DHCP server, DNS server, and patch server. These servers must be separately defined to provide access to unauthenticated users.
- Public server group

  Includes servers with low security levels that can be accessed by different types of users, for example, internal websites and email servers. Public servers can be classified into multiple security groups, depending on the user permission granularity and application system type.
- Internet group

  If the intranet and the Internet are mutually reachable, you can define an Internet group to include the Internet users or public servers.
- DMZ server group

  Includes servers that provide access to Internet users, such as the enterprise Portal website and SSL VPN gateway on the intranet. These servers are deployed at the Internet egress of a campus network or DMZ in a data center.

  If NAT Server is configured to translate intranet server addresses to public IP addresses so the servers can provide services for Internet users using the public IP addresses accessible to all Internet users, add the servers to the Internet group but not the DMZ server group.

  To allow only certain Internet users to access a public IP address, for example, when an enterprise provides a dedicated server for its partners, you can define an independent security group for the server. In this situation, you need to remove the public IP address of the server from the Internet security group.

- Network device group

  The IP addresses of network devices on an enterprise network include those of both physical and logical interfaces. Because network devices need to communicate with each other, you need to allow communication between network device groups.

  If an enterprise has in-band management enabled (use the enterprise service network for network device management without establishing a dedicated network device management network), you are advised to permit only administrator or bastion host IP addresses to log in to network devices through Telnet or SSH for configuration management.

  To simplify configuration of security groups, IP network segments used by the network devices should be separated from those used by user hosts or servers.

- Group of dedicated application systems for employees

  Includes high-security application systems dedicated for a specific type of users, for example, code server and test server.

  Dedicated application systems can be divided into multiple security groups, depending on the user permission granularity and application system type.

6.1.3 Selecting User Authentication Points and Policy Enforcement Points

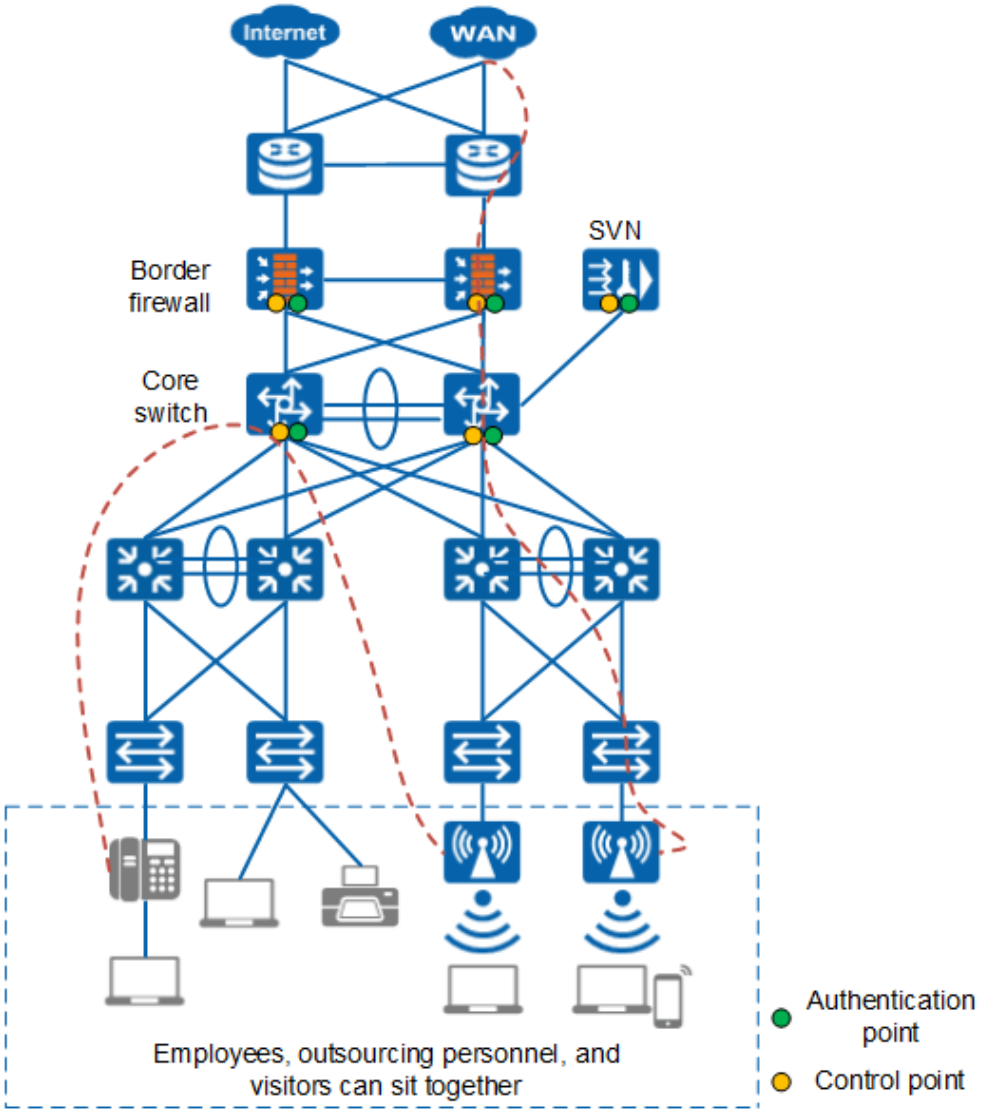
The design of the free mobility solution addresses two issues: where are the users authenticated and where is the traffic controlled.

Generally, the authentication point is located at the core or aggregation layer.

- Authentication at the core layer (recommended)

  As shown in the following figure, the core switch (with native AC installed) functions as the authentication point, gateway, and permission policy enforcement point for wired and wireless users. The border firewall functions as the QoS policy enforcement point for intranet users. If user isolation is required, configure Layer 2 isolation (port isolation or MUX VLAN) on the access or aggregation switch. The isolation policy for users connected to the same core switch is implemented by the core switch itself, whereas the isolation policy for users on different campus networks is implemented by the border firewall.

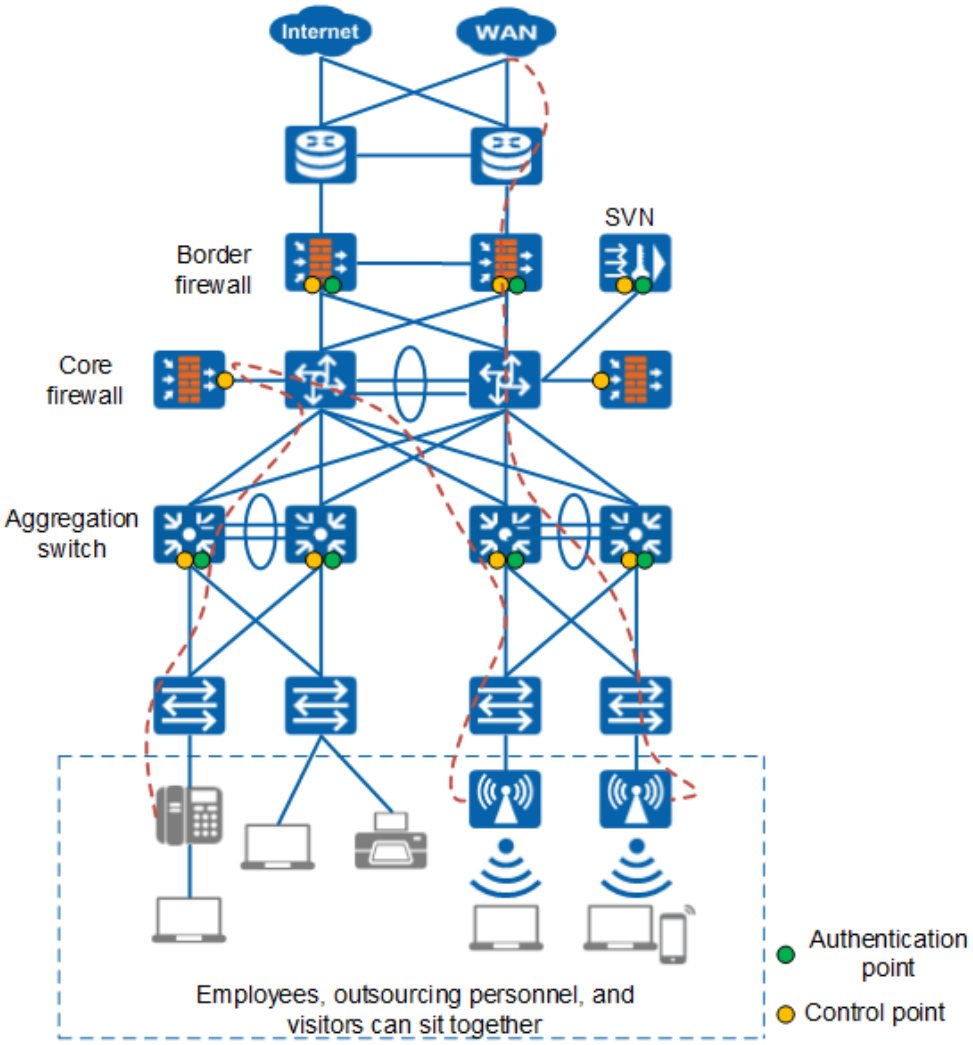
  The border firewall or an SVN device on the intranet functions as the authentication point, gateway, and permission policy control point for VPN users. The border firewall functions as the QoS policy enforcement point for VPN users. When user isolation is required, the policy for isolating intranet users from VPN users and the policy for isolating VPN users are implemented by the authentication firewall or SVN device for VPN users.



- Authentication at the aggregation layer

  As shown in the following figure, the aggregation switch (with native AC installed) functions as the authentication point, gateway, and permission policy enforcement point for wired and wireless users. The border firewall functions as the QoS policy enforcement point for intranet users. If user isolation is required, configure Layer 2 isolation (port isolation or MUX VLAN) on the access switch. The isolation policy for users connected to the same aggregation switch is implemented by the aggregation switch itself. The isolation policy for users connected to different aggregation switches is implemented by the core firewall. The policy for diverting traffic between intranet users must be configured on the core switch. The isolation policy for users on different campus networks is implemented by the border firewall.

  The border firewall or an SVN device on the intranet functions as the authentication point, gateway, and permission policy control point for VPN users. The border firewall functions as the QoS policy enforcement point for VPN users. When user isolation is required, the policy for isolating intranet users from VPN users and the policy for isolating VPN users are implemented by the authentication firewall or SVN device for VPN users.



The key principle for traffic control is that the device functioning as the policy enforcement point must be able to identify the source security group and destination security group that need traffic control.

An agile device identifies security groups as follows when functioning as the policy enforcement point:

- An agile switch only identifies the security group for traffic of locally authenticated users.
- An agile firewall or SVN device can identify the security group for traffic of users authenticated by the Agile Controller-Campus, regardless of whether the users are connected to the agile firewall or SVN device.
- For static users and servers that can be expressed as IP addresses or network segments, the agile switch, firewall, and SVN device can identify the corresponding security groups so long as the administrator defines the mappings between IP addresses or network segments and security groups in the Agile Controller-Campus.

Based on the preceding security group identification principles, the following design is recommended for free mobility:

- Analyze the types of traffic to be controlled on the live network and possible forwarding paths.

- To prevent terminals from communicating with each other at Layer 2, deploy Layer 2 isolation on the Layer 2 network to block Layer 2 communication. Traffic then must pass through a Layer 3 gateway.
- To control traffic for terminals that can communicate with each other through a Layer 3 gateway, configure the Layer 3 gateway as the authentication point and policy enforcement point for these terminals.
- To control traffic for terminals that communicate with each other through different Layer 3 gateways, deploy an agile firewall as the policy enforcement point in the traffic path. If traffic does not pass through the agile firewall in normal situations, configure a traffic diversion policy (PBR or GRE tunnel) on the appropriate device to divert traffic to the agile firewall, for example, the core firewall in the aggregation layer authentication solution.

6.1.4 Selecting Authentication Technology

Different authentication technologies have the corresponding application scopes (for example, **Table 6-1**), which need to be selected based on the customer's requirements. If the application scopes conflict with the customer's requirements, consider the customer's requirements first.

Table 6-1 Application scope of authentication technologies

Authentication Technology	Application Scope
802.1X	802.1X authentication has the highest security. Operating systems of PC terminals have a built-in client. However, professional Huawei clients are recommended. 802.1X authentication directly controls network access and ensures high network security when it is deployed at the access layer. It is applicable to network construction scenarios where users are centralized and there are high security requirements.
PPPoE	PPPoE authentication has a high security. The operating system has a built-in authentication client. PPP encapsulation reduces communication efficiency.
Portal	Portal authentication has a low security. Common Portal authentication requires a secure client while forcibly pushed web-based authentication does not. The authentication mode is flexible, and the authentication page can be customized, which is suitable for commercial service scenarios.
MAC	MAC address authentication has a low security and no security client is required. MAC addresses are used as the user name and password for authentication. You do not need to enter the user name and password on the terminal. The management is complex and MAC addresses need to be registered. MAC address authentication is applicable to scenarios where dumb terminals such as SIP terminals, printers, and fax machines require authentication.

Authentication Technology	Application Scope
SSL VPN	SSL VPN authentication has a high security. The network extension plug-in needs to be installed and the authorization management is flexible. Only the Windows operating system is supported.
L2TP over IPSec	L2TP over IPSec authentication has a high security. The operating system has a built-in authentication client. Huawei clients can also be used. The configuration is complex.

Customers tend to consider the following factors:

- Authentication mode used on the live network
- Whether users need to install and use the authentication client
- Enterprise employees' expectation on the simple authentication process
- Security of the authentication protocol

For details about the recommended authentication and authorization schemes based on customer requirements, see **Table 6-2**.

Table 6-2 Authentication and authorization schemes

User Type	Authentication Mode
Enterprise employee	● First choice: 802.1X ● Second choice: Portal and PPPoE ● Third choice: Authentication-free
Visitor	Portal
Dumb terminal	● First choice: MAC address ● Second choice: Authentication-free
Traveling employee	● First choice: SSL VPN (especially for Windows) ● Second choice L2TP over IPSec
Partner	● If all users of a partner share an account, use inter-gateway permanent L2TP over IPSec tunnel. ● If each user of a partner has an account, use L2TP over IPSec VPN in NAS-Initiated mode.

There are three mainstream technologies used to authenticate wired and wireless terminals connected to the campus network: 802.1x authentication, Portal authentication, and MAC address authentication.

Based on the preceding analysis, the solution recommends the following authentication technologies for different users:

- 802.1x authentication for enterprise employees and users connected to the campus network using the enterprise's distributed terminals, such as outsourcing personnel with enterprise terminals. Dedicated 802.1x client can be installed on enterprise terminals before they are distributed.
- Portal authentication for external visitors and users connected to the campus network using individual terminals, for example, outsourcing personnel carrying individual terminals.
- MAC address authentication for dumb terminals, such as IP phones, printers, and fax machines.

6.1.5 Planning Security Group Policies

Before planning security group policies, you need to understand two built-in security groups.

The system has two built-in security groups: Unknown group (group ID: 0) and Any group (group ID: 65535).

- **Unknown group**

  The Unknown group represents the security group for packets with unknown source or destination IP addresses. It has no members and is only used by network devices to match traffic against service policies. After receiving a packet, if a network device fails to identify the security group of the source or destination IP address of the packet, the network device uses service policies of the Unknown security group to match the packet.

  A network device may fail to identify the security group of an IP address due to multiple reasons, including:

  - An authentication point switch can only identify security groups to which local online users belong. When local users access users that go online on other authentication points, the authentication point switch can only identify the source group of packets but not the destination group. In this case, the authentication point switch processes packets based on policies used by source groups to access the Unknown group.
  - A non-authentication-point device needs to obtain the source and destination groups of packets from the Agile Controller-Campus. If a fault occurs on the Agile Controller-Campus or between the non-authentication-point device and the Agile Controller-Campus, the non-authentication-point device fails to obtain the source and destination groups from the Agile Controller-Campus. The non-authentication-point device then processes packets based on policies used by the Unknown group to access the Unknown group.
  - For the traffic from users to the Internet, because public addresses are not used on the intranet and the administrator does not define any static resource security group to represent the public addresses, the network device will process packets based on policies used by source groups to access the unknown group.

- **Any group**

  The Any group represents the security group for packets with any IP address in a network. The Any group is only used by network devices to match traffic against service policies. In most situations, users have the same rights to access different resource groups. You can configure policies for users' access to the Any group to simplify policy configuration.

  For example, 100 security groups are assigned on servers in an enterprise. Employees in department A are allowed to access most servers. To implement this, configure servers that cannot be accessed by employees in department A in one or more security groups,

configure the deny right for employees in department A to deny their access to one or more security groups, and configure the permit right for employees in department A to permit their access to the Any group. The Any group has the lowest policy priority, so employees in department A can access most servers and are not allowed to access few servers. You do not need to configure the permit policy for employees in department A to access other static resource security groups.

When group A accesses group B, the policies are matched in the following sequence:

- Searches for the exactly matching policy for access from group A to group B. If no action is configured in the policy matrix, proceed to the next step.
- Searches for the policy for access from group A to the Any group. If no action is configured in the policy matrix, proceed to the next step.
- Searches for the policy for access from Any group to Any group. If the policy matrix does not contain the configuration of this policy, the network device performs the predefined policy action. The predefined action on a switch is permit. That is, the switch forwards the traffic that matches no policy by default. The predefined action on a firewall is denied. That is, the firewall drops the traffic that matches no policy by default. The action can be changed to permit.

In the Free Mobility solution, security group policies are configured based on logical groups. The policies are completely decoupled from IP addresses, so an administrator only needs to consider the relationship between two logical groups when planning security group policies. On the Agile Controller-Campus, the administrator can configure security group policies in a policy matrix. In the policy matrix, each row represents a source group and each column represents a destination group.

Notice the policy direction when planning security group policies. Generally, inbound and outbound packets are transmitted between two terminals.

- Traffic from A to B and traffic from B to A are not related to each other. Switches match policies for traffic from A to B and from B to A separately to determine whether to forward the traffic. Therefore, only the source and destination security groups of packets are checked during policy enforcement. If access from A to B is permitted and from B to A is denied, all packets sent from A to B will be permitted, and all packets sent from B to A will be discarded regardless of whether A or B initiates the access. In addition, the default policy of switches is permit.
- For firewalls, there are sessions. A firewall records the IP addresses and port numbers of two communication parties using a session, so the firewall can associate incoming and outgoing traffic during one interaction. The firewall uses the same policy for the incoming and outgoing traffic. Therefore, policies are directional. If access from A to B is permitted and from B to A is denied, A can initiate access to B, and the firewall permits the return packets from B to A. However, B cannot initiate access to A. In addition, the administrator can customize the default policy for access from the Any group to Any group for the firewall. For security purposes, the default policy is disabled.

Network access usually requires bidirectional communication. Therefore, to simplify management, you only need to consider the rights for user security groups to access other users and servers when planning security group policies.

- To prevent a user from accessing a security group, you only need to configure the deny rule in a single direction.
- To permit a user to access a security group, if enforcement points are deployed on switches only, you only need to configure the permit rule in a single direction. If enforcement points are deployed on firewalls, configure policies in both directions.

If only switch enforcement points exist, A and C are users, and B and D are servers, A can communicate with other groups except B, and members in C can only communicate with other members in C and members in D, design policies shown in **Table 6-3**. The communication between B and D does not pass through the campus network and does not need to be planned which is displayed as NA in the following table. In cells filled with Empty, no policy is configured, or the permit/deny policy is configured, which does not affect the control effect.

Table 6-3 Policy planning

Policy	A	B	C	D
A	Permit	Deny	Permit	Permit
B	Empty	NA	Empty	NA
C	Deny	Deny	Permit	Permit
D	Empty	NA	Empty	NA

The Agile Controller-Campus enables administrators to configure a rule from a group to the Any group (that is, default rights of the group), reducing the quantity of policies to be defined and simplifying policy configuration. For example, as described in **Table 6-3**, an administrator simply needs to configure a policy for denying access from group A to group B so that access from group A to the Any group is permitted.

If the policy enforcement point is deployed on a firewall on the network, configure policies in both directions as follows:

- As described in **Table 6-4**, configure policies for permitting access from A to B and from B to A. Configure policies for permitting or denying access from A and B to the Any group. If the permit policy is configured, you do not need to configure the policies for access from A to B and from B to A. In this case, both switches and firewalls forward the packets of A and B in both directions.

  Table 6-4 Policy plan (permitting access from A to B and from B to A)

Policy	A	B	Any
A	NA	Permit	User-defined
B	Permit	NA	User-defined

- As described in **Table 6-5**, configure policies for permitting access from A to B but not from B to A. If the policies for access from B to A and B to Any group are not configured, the default actions of network devices (assume that the action is deny by default) are performed. When B proactively accesses A, the packets sent from B to A match the default action on the firewall and are discarded. B cannot access A. When A proactively accesses B, a packet is sent from A to B through the switch and firewall. The packet matches the permit action in the direction from A to B and is forwarded. A session is established for the packet on the firewall. When the packet is sent from B to A through the firewall, the packet matches the established session and is forwarded. On the switch, the packet matches the default action of the switch and is forwarded.

Table 6-5 Policy plan permitting access from A to B but not from B to A)

Policy	A	B	Any
A	NA	Permit	User-defined
B	Empty	NA	Empty

6.1.6 Best Practices

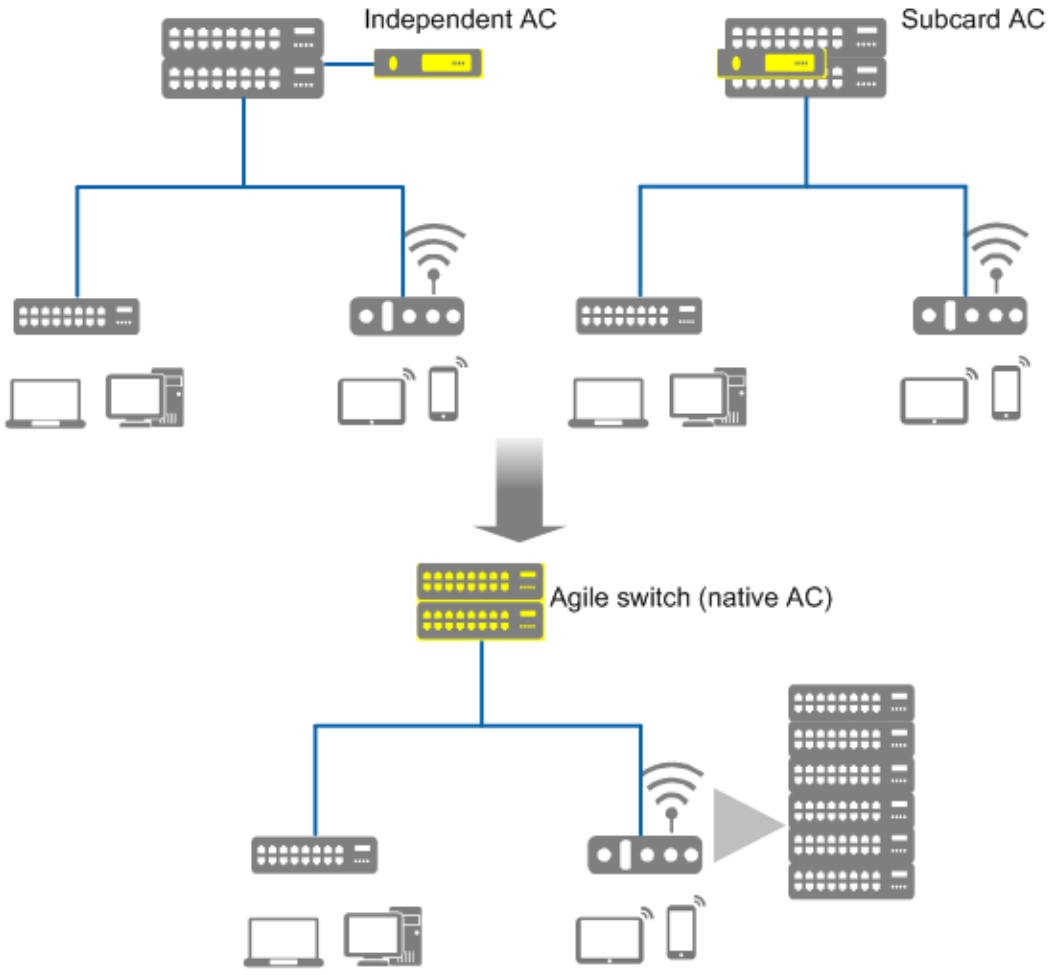
- In the free mobility scenario, the X series cards are recommended.
- Only firewalls support the free mobility QoS policy. To implement free mobility, only firewalls support the application-based access permission control, bandwidth rate limit, and priority-based scheduling. Typically, it is recommended that the free mobility policies (such as resource access permission control) be deployed on switches. The bottlenecks on user bandwidth usually do not exist on internal campus networks. Therefore, it is recommended that the user bandwidth limit and priority scheduling be deployed on the egress firewall, which implements the consistent experience policy (bandwidth limit and priority-based scheduling). To implement application-based access control, policy enforcement points can be deployed only on firewalls. If bandwidth limit or priority-based scheduling is required for accessing data centers or servers, policy enforcement points can be deployed on firewalls in data centers or server zones.
- If only the permission of users to access network resources needs to be controlled, switches can be deployed as authentication points, and both switches and firewalls can be deployed as policy enforcement points.
- If customers want to control the access permission between users and between users and network resources, two scenarios are involved:
  - The authentication points are centralized on core switches. It is recommended that the policy enforcement points be deployed on core switches.
  - User authentication points are distributed on aggregation switches or core switches on different branches. Policy enforcement points must be deployed on switches or firewalls that function as authentication points.
- If there is a requirement for user-to-user access control, Layer 2 isolation must be deployed on access switches to divert all traffic to authentication point switches. User isolation for wireless services needs to be configured in the VAP profile.
- If 802.1X authentication needs to be deployed on switches and firewalls function as policy enforcement points for free mobility, it is required to configure realtime accounting on switches. The switches send accounting packets to report IP addresses to the Agile Controller-Campus for firewalls to query.
- When 802.1X authentication is used for wired users, the authentication points can be core switches or aggregation switches. If the authentication points are core switches, EAP packet transparent transmission must be configured on access switches and aggregation switches. Similarly, if the authentication points are aggregation switches, EAP packet transparent transmission must be configured on access switches.
- When a firewall functions as a policy enforcement point, the user network segment needs to be specified on the internal network segment of the Agile Controller-Campus. This enables the firewall to query the security group to which an IP address belongs. When user access traffic reaches the firewall, the firewall sends the user's IP address to the Agile Controller-Campus to query its security group. Only an IP address in the internal

network segment triggers the query of the security group to which this IP address belongs.

- When a firewall functions as a policy enforcement point, to prevent the security group queries sent from the firewall to the Agile Controller-Campus from being discarded, it is recommended that the Agile Controller-Campus deliver global configurations to the firewall and forward RADIUS packets to the Agile Controller-Campus.
- When a firewall works in agile mode, the security policies cannot be manually configured by default and can only be delivered by the Agile Controller-Campus. To configure more flexible security policies, you can set the firewall to work in manual mode.

6.2 Wired and Wireless Integration Design

As wireless networks are widely used in campuses, wireless networks deployed using traditional independent ACs and built-in AC cards are evolving towards using the wired and wireless integration solution.



The traditional campus solution with independent ACs and built-in AC cards faces the following challenges:

- Wired traffic and wireless traffic are forwarded separately. With the arrival of the 802.11ac gigabit era, the AP management capability of traditional ACs gradually reaches a bottleneck.

- Wired and wireless networks are managed in different systems, making maintenance and troubleshooting difficult.
- Wired and wireless users are authenticated and controlled in a distributed manner, which is difficult to control. Wired user authentication and policy control points are deployed on access switches or independent authentication gateways. Wireless user authentication points are deployed on ACs.

The wired and wireless integration solution (native AC solution) is recommended for agile campus networks. The S series switches, agile switches integrating the AC functions, implement unified forwarding of wired and wireless traffic and unified management of wired and wireless devices. User policies are centralized on agile switches. The wired and wireless integration solution has no performance bottleneck and simplifies device management and service management.

Consider the following points when designing the wired and wireless integration solution:

- Determine whether there is a need to build a wireless network or upgrade the network into a wired and wireless integrated network. If wired and wireless users need to be authenticated in a unified manner and on the unified management GUI, the wired and wireless integration solution is recommended. To save investment, use the wired and wireless integration solution which does not require deployment of WLAN ACs.
- To ensure the reliability of WLAN ACs, configure extra channels for data synchronization. The native ACs can share the cluster channels of switches, improving reliability.
- Check the wireless traffic volume and analyze whether ACs have a forwarding bottleneck to determine whether to use the native ACs with high forwarding capability.
- Be clear of requirements on APs and wired switch management. To simplify management and service configuration and implement on-demand expansion, use the wired and wireless integration solution.

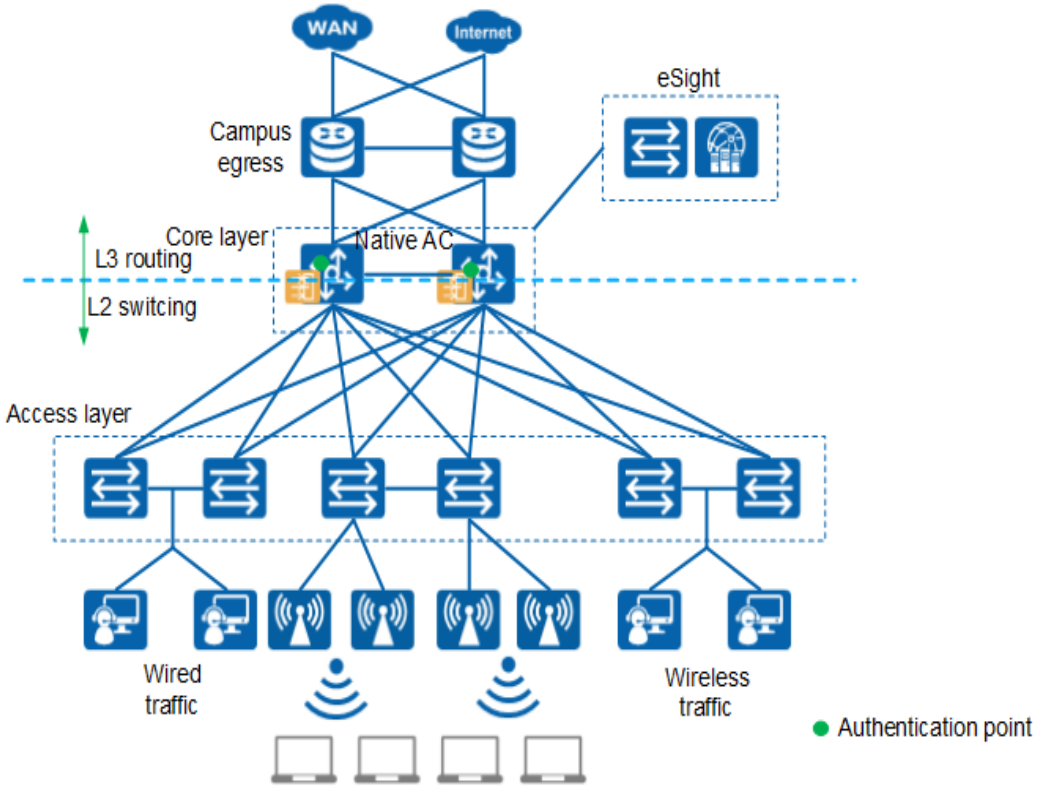
6.2.1 Networking Design

The S7700, 9700, and S12700 agile switches can be used at the core layer and function as the unified authentication points for wired and wireless users. Campus networks can be Layer 2 or Layer 3 networks. Layer 2 networking applies to small- and medium-sized campus networks, and Layer 3 networking applies to large campus networks. The authentication points can be core switches or aggregation switches. **Figure 6-1** shows a Layer 2 network where core switches function as authentication points.

Different authentication modes can be selected based on customers' requirements for security control.

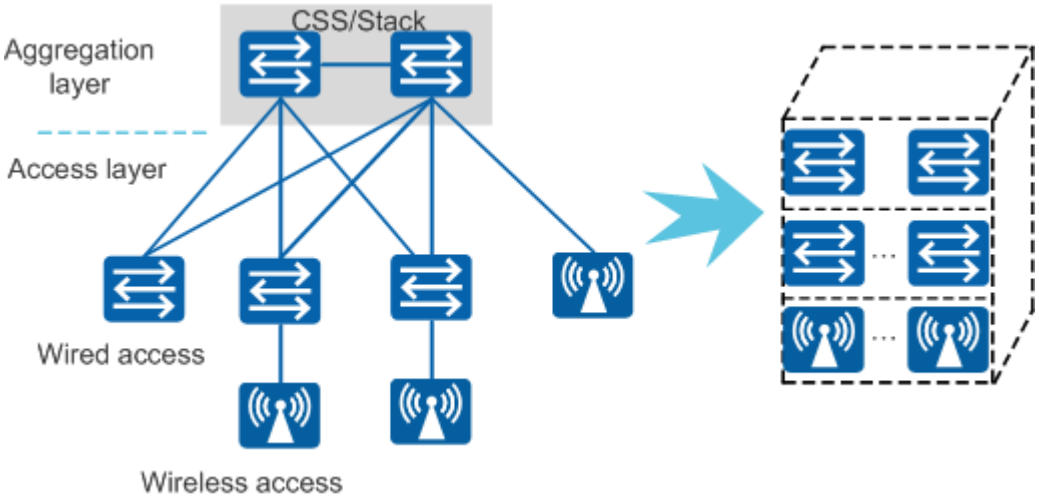
- Portal + MAC authentication is recommended for scenarios with moderate security control requirements. Portal authentication is performed for wired and wireless users and MAC authentication is performed for IP phones, printers, and other dumb terminals.
- 802.1X + MAC authentication is recommended for scenarios with high security control requirements. 802.1X authentication is performed for wired and wireless users and MAC authentication is performed for IP phones, printers, and other dumb terminals. Typically, the authentication points for wired users are deployed on core switches or aggregation switches.

Figure 6-1 Layer 2 networking where core switches function as authentication points



6.2.2 SVF Design

On a traditional campus network, a large number of devices are deployed at the access layer in a distributed mode and are managed using the traditional methods, making the management and configuration complex. Super Virtual Fabric (SVF) technology effectively simplifies management and configuration of access devices. SVF technology virtualizes aggregation and access devices into one logical device and allows aggregation devices to manage and configure access devices.

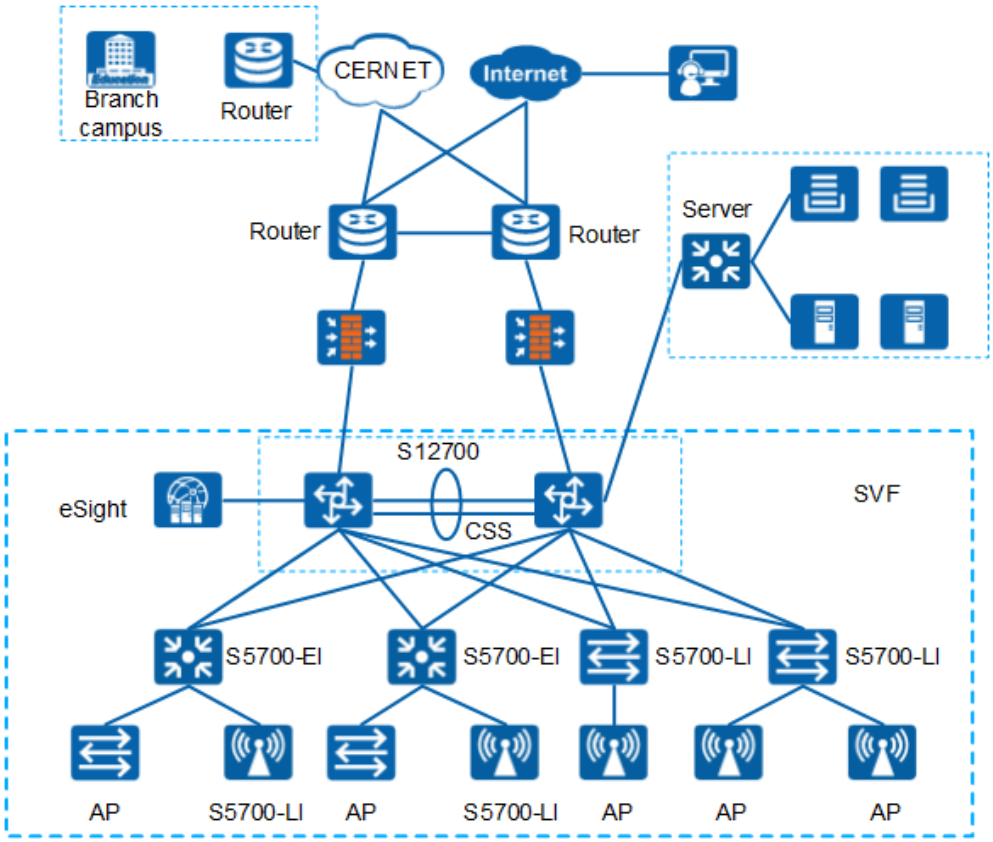


SVF has the following advantages:

- Unified device management. SVF technology virtualizes aggregation and access devices into one logical device and allows aggregation devices to manage and configure access devices.
- Unified configuration. SVF implements batch configuration of access devices based on profiles, removing the need to configure access devices one by one.
- Unified user management. SVF manages wired and wireless access users in a unified manner.

The following describes typical SVF applications:

- Large-scale wired and wireless campus network - college campus network

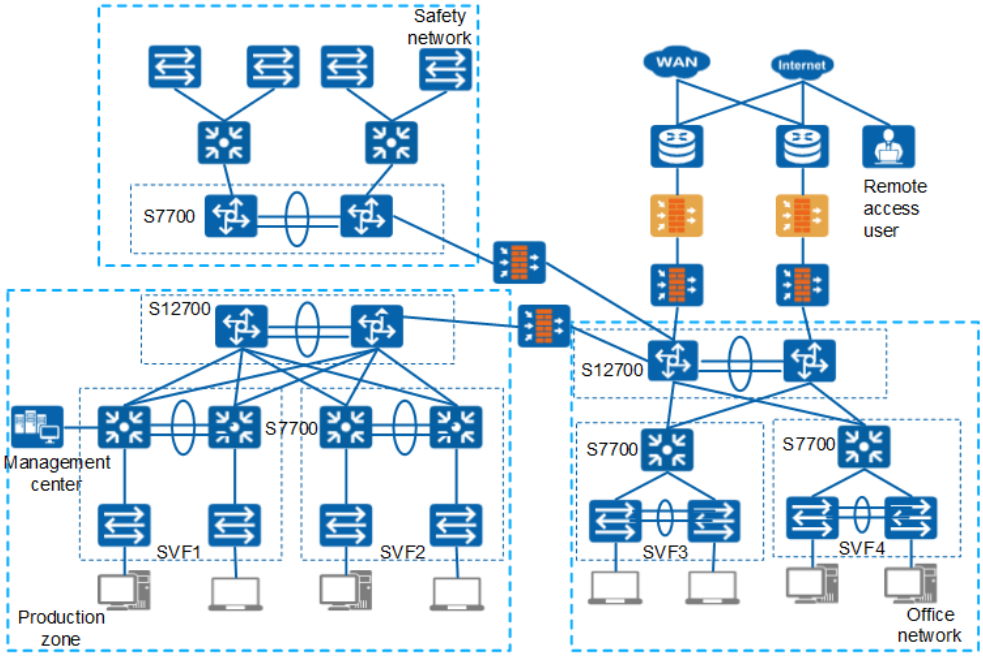


As shown in the preceding figure, the S12700 switches function as the SVF-Parent to manage all access switches and wireless APs. The wired and wireless integration solution is used. It is recommended that the S12700 switches in the core layer be deployed in a cluster for backup.

The authentication point is deployed on the SVF-Parent. If wireless users do not have high security requirements, Portal authentication is recommended. 802.1X authentication is recommended for a higher security requirement. Local authorization can be configured on the SVF-Parent to implement more user-specific access control.

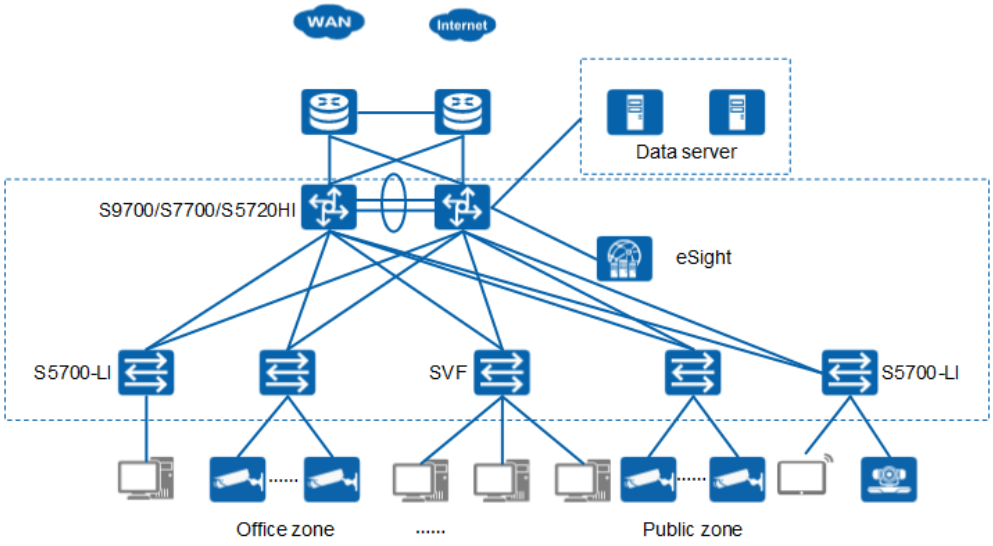
Wireless user traffic is forwarded through tunnels in a centralized manner, which is convenient for the centralized control of wireless traffic. If centralized traffic control is required for traffic of wired users, use the centralized forwarding mode. If the customer does not require high security, use the distributed forwarding mode because it is easy to deploy and can fully use bandwidth of access devices.

- Cross-area large campus network - large-scale enterprises



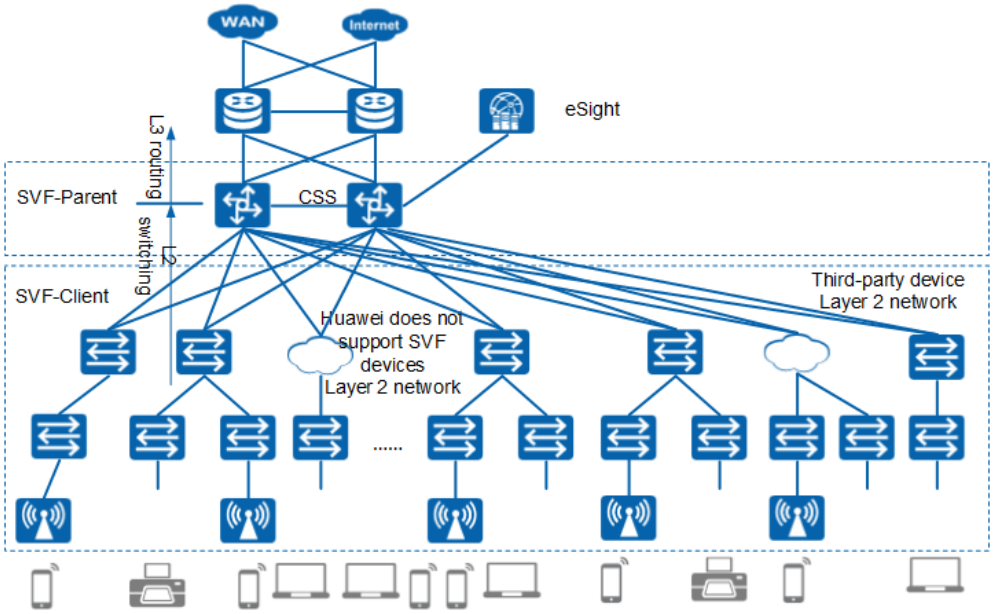
The S12700 switches deployed in different areas in a cluster function as core switches, and the aggregation and lower layers are virtualized into several SVF management systems. The S7700 cluster in each SVF system functions as the SVF-Parent to manage all access switches and functions as the authentication point. The S5700 functions as the SVF-Client. The native ACs are configured on the SVF-Parent to support wireless access at any time.

- Small or medium wired campus network - small enterprise branches



The S9700, S7700, or 5720HI functions as the SVF-Parent to manage all access switches. It is applicable to the scenario where there are few access switches.

- SVF deployed on the existing network - compatible with third-party devices



The existing network is a non-SVF traditional network. To improve network management efficiency, deploy SVF, upgrade devices that support SVF on the original network using software, and implement Layer 2 transparent transmission for network devices that do not support SVF.

6.2.3 Best Practices

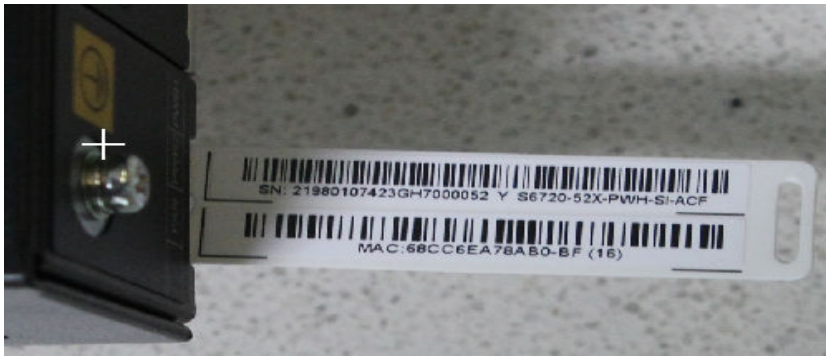
Native AC

- When authentication is deployed on a physical interface, the authentication module of an agile switch cannot distinguish an AP from a wired terminal. Therefore, the AP management channel must be isolated from wired user authentication. You are advised to configure non-authentication for APs using a context profile. You are advised to configure MAC address-based or Portal authentication on VLANIF interfaces for wired users and configure 802.1X authentication for APs and wired terminals on different interfaces.
- When wired and wireless users access the network through the same physical interface, only the tunnel forwarding mode can be used for wireless services.
- The native AC function does not support CAPWAP-based packet fragmentation and reassembly. Therefore, when APs and the native AC are connected through a Layer 3 network, packet fragmentation must be prevented on intermediate links.
- In a centralized AC scenario, when an AP is connected to the AC through an Eth-Trunk, the Eth-Trunk cannot contain interfaces of X interface cards and non-X interface cards. An X or a non-X interface card can join only one WLAN work group. When creating an Eth-Trunk that contains interfaces of different non-X interface cards, ensure that all the member interfaces belong to the same WLAN work group. If an AP is moved from one non-X interface card to another in the same WLAN work group, services on the AP and associated STAs are not interrupted. In other situations, the AP and STAs are forced offline.

SVF

- The SVF networking mode is fixed, and the tree architecture is used. The ring topology is not supported.

- VLAN 1 and VLAN 4093 are reserved VLANs in an SVF system and cannot be configured as common service VLANs.
- If a third-party device exists under the parent device in an SVF system, the third-party device can only perform Layer 2 forwarding (that is, the parent is connected to ASs across a Layer 2 network). In this scenario, only level-1 ASs are supported.
- When an AS goes online, it must be unconfigured (without any startup configuration file) and there is no input on the console port. Before an AS connects to an SVF system, it is recommended that you remove the network cable from the console port. If SecureCRT is used as a HyperTerminal, set SecureCRT not to automatically send characters.
- Each AS can be a stack of up to five member devices that are the same model and provide the same number or different numbers of ports. An AS can be a stack of devices of the same series but different models. If an AS is a stack, you can run the **slot** command to modify the preconfigured device type. Configure multi-active detection (MAD) in a stack to minimize the impact of a stack split on services.
- Each AS has a unique management MAC address. You can view the MAC address of a device on the MAC address label.



- In a stack system, before connecting an AS with the name and MAC address pre-configured on the parent to an SVF system, it is recommended that you set up a stack for the AS and then configure the pre-configured MAC address as the management MAC address. You can configure the MAC address as the MAC address of the master switch in the stack. In this situation, the AS management MAC address is the same as the pre-configured one by default, and no management MAC address needs to be configured. If the AS name and MAC address are configured after the AS connects to an SVF system, the management MAC address does not need to be configured.
- Some Huawei switches can connect to an SVF system through downlink interfaces. Before restarting an AS, check whether the interface that connects this AS to the parent is a downlink interface. (You can run the **display port connection-type access all** command on this AS to view all downlink interfaces on it.) If this interface is a downlink

interface, run the **uni-mng up-direction fabric-port** command on this AS to configure this interface as an uplink interface before restarting this AS. Otherwise, this AS cannot go online.

- Stack member switches connected using downlink service interfaces cannot join an SVF system as ASs.
- All member devices in an AS stack system must have the same model.
- If downlink service interfaces of an AS are configured as member interfaces of an uplink fabric interface, all the downlink interfaces of the AS cannot be configured as stack member interfaces.
- Pay attention to the following notes when replacing a faulty AS:
  - An AS can only be replaced by a device of the same model. If the new device is a different model, the SVF system considers it as a new AS, which then cannot inherit services on the previous AS.
  - Only a standalone AS can be replaced, and a stacked AS cannot be replaced.
  - AS automatic replacement is not supported when an AS connects to the parent through a network.
  - To ensure that a replacement AS can be successfully authenticated, run the **auth-mode none** command to set the AS authentication mode to none, or run the **whitelist mac-address** command to add the management MAC address of the replacement AS to the whitelist. If the replacement AS has no management MAC address configured, the system MAC address is used as the management MAC address.

7 QoS Design and Best Practices

In addition to traditional data services such as web, email, and FTP services, campus networks transmit the services such as video surveillance, video conference, voice call, and production scheduling, which are sensitive to bandwidth, delay, and jitter. For example, video surveillance and video conference require high bandwidth, short delay, and low jitter. The voice service does not require high bandwidth, but requires short delay. When congestion occurs, the voice service must be processed first.

Quality of service (QoS) is a common concept in various scenarios where service supply and demand relationships exist. It evaluates the capability of a service provider to provide support for customers' service requirements. The purpose is to provide end-to-end service quality assurance for users' services. It evaluates services using the following indicators:

- Throughput: also called bandwidth, indicates the average rate of service flows in a period of time. Bandwidth is scheduled by committed access rate (CAR) and generic traffic shaping (GTS).
- Delay: indicates the average time for a service flow to pass through a network. On a device, flows of different priorities require different delay levels and are processed by queue scheduling.
- Jitter: refers to the variation in duration when service flows pass through a network. Jitter can be prevented by congestion avoidance.
- Packet loss ratio: indicates the highest ratio that packets are discarded when being transmitted on a network. In most cases, packets are discarded due to network congestion.

Based on the required bandwidth, delay, jitter, and packet loss ratio, QoS can use technologies such as priority mapping, traffic policing, traffic shaping, queue scheduling, and congestion avoidance, to improve network quality and bring good user experience.

Table 7-1 describes the requirements for QoS design.

Table 7-1 QoS design requirements

Requirement Type	Key Point of Requirement Survey	Key Point of Requirement Analysis
Current network situations	● Bandwidth bottlenecks on networks: Generally, the nodes on WANs, data center networks, and Internet egress, and intranets with fast bandwidth convergence. ● Egress bandwidth of each egress device.	Determine the deployment position of the QoS policy in the future and the values of bandwidth-related parameters.
Traffic requirement	● Key services that need to be focused on in the current network. ● Characteristics of various types of traffic that can be identified by network devices. For example, whether voice traffic uses the proprietary protocols SIP and H.323; whether switches identify voice packets based on voice VLANs; whether the traffic is destined for or from a specific port on a specific server; and whether the traffic is from or destined for a specific host network segment. Check whether the application signature database can be used to identify applications, for example, BT and YouTube, if there are protocols through dynamic port negotiation and application-layer protocols that cannot be distinguished by port number. ● Bandwidth requirements of key services. For example, multimedia services of different vendors and bit rates require different bandwidths to ensure smooth video or audio services. ● Enterprises' processing polices for different multimedia applications. For example, in respect to the online video, some enterprises believe that the online video provided by the internal network needs to be guaranteed, but the online video provided by the Internet is irrelevant to work and does not need to be ensured.	Specify traffic classification and management requirements of each type of traffic.

7.1 Design Principles

The basic principle of QoS design is to mark or re-mark packets at the boundaries of different DiffServ domains and perform bandwidth control. Devices in the same DiffServ domain only perform queuing and scheduling for packets according to marks of border devices. QoS deployment on a campus network consists of service identification at the access layer, DiffServ scheduling at the aggregation and core layers, and bandwidth control on egress routers.

- Service identification at the access layer

  Access switches function as edge switches. They identify, classify, and mark data flows on the user-to-network interfaces (UNIs), and perform congestion management, congestion avoidance, and traffic shaping on the network-to-network interfaces (NNIs).

  In practice, access switches connect to different terminals through different ports. Different priorities are assigned to services on access switches to implement priority scheduling.

- DiffServ deployment at the aggregation and core layers

  Ports on aggregation and core switches are configured to trust DSCP or 802.1p priorities. Aggregation and core switches perform QoS policies using queue scheduling, traffic shaping, and congestion avoidance based on QoS parameters at the access layer, to ensure that high-priority services are scheduled first.

- Bandwidth control on egress routers

  Egress routers are also in the DiffServ domain and are configured to trust DSCP or 802.1p priorities and implement QoS policies. Due to limited egress bandwidth, different bandwidths should be configured on WAN ports. In addition, QoS policies configured on egress devices vary according to the enterprise WAN construction mode.

  - The WAN QoS policies can be managed by an enterprise itself in the following scenarios: the enterprise-built WAN, direct connection using leased fibers, and customized enterprise QoS policies configured by the WAN carrier. In this case, the campus egress devices or PE devices do not need to re-mark traffic on edge nodes.
  - The WAN QoS policies are not controlled by an enterprise. For example, the enterprise leases an MPLS VPN network from a carrier, the carrier does not trust the packets marked by the enterprise, or the two parties have different definitions on the same packet mark. In this case, the campus egress devices or PE devices may need to re-mark traffic on edge nodes.

In traditional QoS policies, only the service type of traffic is considered. For example, only voice traffic is guaranteed. Free mobility provides a new assurance capability for the QoS design on an agile campus network: user-based assurance.

- Bandwidth control on authentication points

  You can configure the Agile Controller-Campus in the free mobility solution to limit the total intranet bandwidth of a single user after the user accesses the network. The authentication point interacts with the Agile Controller-Campus to perform user authentication. After a user passes the authentication, the Agile Controller-Campus delivers the uplink and downlink bandwidth thresholds to the authentication point and performs rate limiting based on the thresholds.

  In network planning, you can configure different bandwidth thresholds for different security groups. For example, for a common PC, the bandwidth is limited to 2 Mbit/s.

For an IP phone, the bandwidth is limited to 4 Mbit/s. For an HD video terminal, the bandwidth is limited to 8 Mbit/s. For a VIP user, the bandwidth is limited to 10 Mbit/s. By properly allocating bandwidth, you can prevent common users from affecting the intranet experience of VIP users in the same area by running high bandwidth applications or transmitting large-sized files.

- Egress firewall queue scheduling service

  In the free mobility solution, some user groups can be specified as VIP user groups on the Agile Controller-Campus and a forwarding priority can be assigned to these user groups. The egress firewall can identify the traffic of VIP users by interacting with the Agile Controller-Campus. According to the unified configuration on the controller, traffic of VIP users is sent to the corresponding queue according to the specified priority so that the traffic can be preferentially forwarded at the egress. This ensures the egress experience of VIP users.

7.2 Traffic Classification

Different types of services have different requirements for service quality. For details about traffic classification and hierarchical design, see **Table 7-2**.

Table 7-2 Traffic classification and hierarchical design recommendations

Category		Typical Application or Protocol	Packet Loss Tolerance	Delay Tolerance	Jitter Tolerance
Network management	Network protocol	Inter-device network communication protocols, such as loop prevention protocols at link layers, routing protocols, and multicast group management protocols.	Low	Low	Allowed
	Management protocol	Protocols used by network administrators to monitor network devices, deliver configurations, and diagnose faults. For example, ICMP, SNMP, Telnet, and XMPP.	Low	Low	Allowed
User service	VoIP data flow	Real-time voice calls through the IP network. The network must provide low delay and low jitter. Otherwise, both involved parties can perceive the poor quality.	Very low	Very low	Very low

Category		Typical Application or Protocol	Packet Loss Tolerance	Delay Tolerance	Jitter Tolerance
	Voice signaling	Signaling protocols for controlling VoIP calls and establishing communication channels, such as SIP, SIP-T, H.323, H.248, and Media Gateway Control Protocol (MGCP). Generally, signaling protocols take less precedence over the VoIP data flow because most people think that interrupted voice communication is worse than the failure of getting through using a phone.	Low	Low	Allowed
	Multimedia meeting	Multi-party sharing through the live camera or computer desktop on the IP network. In addition, the protocols or application programs provide the bit rate adaptation function. When the network quality is poor, the system automatically decreases the bit rate and image quality to ensure video smoothness.	Medium and low	Very low	Low
	Real-time online interaction	Online interactive programs for the network to ensure low packet loss, delay, and jitter. The operator expects quick and accurate responses. For example, a network game in which operation instructions are transmitted through RTP/UDP and a multimedia conference system that cannot perform bit rate adaptation. These systems impose higher requirements on a network.	Low	Very low	Low
	Streaming media	Playback of online audio and video programs on a network. Because these audio and video programs are made in advance, user terminals can cache and play back these programs, thereby reducing the requirement for network delay, packet loss, and jitter.	Medium and low	Medium	Allowed
	Online live broadcasting	Different from streaming media, online live broadcasting is implemented in real time. Although user terminals can cache online live broadcasting programs, the network is required to provide low packet loss rate and jitter to ensure good real-time viewing effect.	Very low	Medium	Low

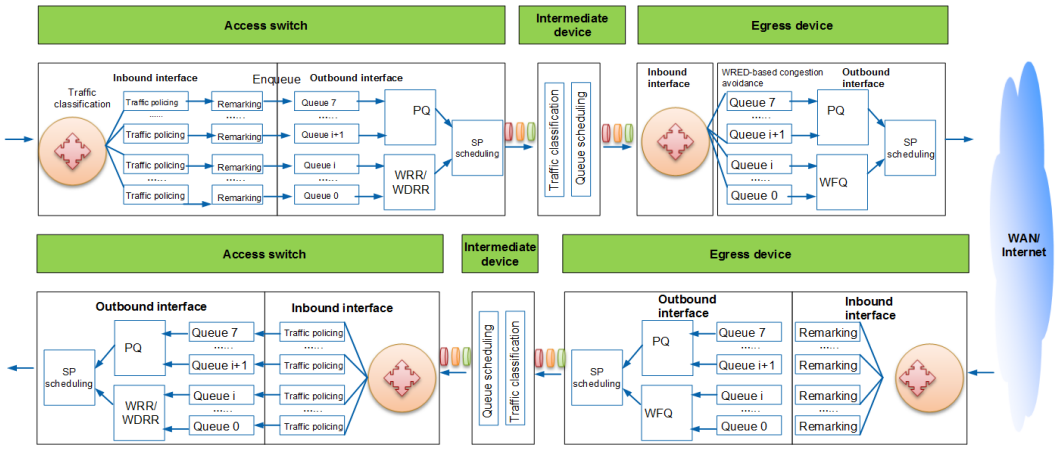
Category		Typical Application or Protocol	Packet Loss Tolerance	Delay Tolerance	Jitter Tolerance
	Low-delay data service	Data service of which users wait for the outcome. For example, in a network order placement system or an ERP system, a long delay hinders the benefits of enterprises or decreases the work efficiency.	Low	Medium and low	Allowed
	Large amount of data service	Network services in which a large amount of data is transmitted for a long time, such as FTP, database network backup, and file dump.	Low	Medium and high	Allowed
	Common service	Basic services on the enterprise network, which have no special requirements on the network nor high priorities. These services include mails and website browsing.	No special requirements		
	Low-priority service	Services that enterprises do not want to care about and guarantee. For example, network applications irrelevant to work, such as Facebook and YouTube.	High	High	Allowed

NOTE

Lower tolerance indicates the requirement for lower packet loss rate, delay, and jitter.

7.3 Queue Scheduling

After services are classified in QoS deployment, the service flows are introduced to queues. Queue scheduling is used to perform the QoS policies. The following figure shows the recommended design of queues and scheduling in the inbound and outbound directions of the network.



7.4 Bandwidth Allocation

- Bandwidth allocation principles
  - PQ scheduling

    Designed for core services, priority queue (PQ) scheduling is applied to queues in descending order of priority. Low-priority queues are processed only after all high-priority queues are empty. Packets of key services are added to high-priority queues and packets of common services are added to low-priority queues. This ensures that the key service packets are sent first, and common service packets are sent after the key services are processed. PQ scheduling is useful for low-delay services. Assume that data flow X is mapped to the queue of the highest priority on each node. When packets of data flow X reach a node, the packets are processed first. However, the PQ scheduling mechanism may result in package starvation in low-priority queues. For example, if data flows mapped to a queue of high priority arrive at a 100% link rate in a given period, the scheduler does not process flows in queues of lower priorities. To prevent package starvation, upstream devices need to accurately define service characteristics of data flows to prevent service flows mapped to a queue of high priority from exceeding a certain percentage of link capacity. This prevents the queue of high priority from becoming full and allows the scheduler to process packets from low-priority queues.

    Therefore, to prevent no bandwidth for low-priority services due to bandwidth occupation by high-priority services of the PQs, set the bandwidth to a large value. However, it is recommended that the bandwidth be no more than one third of the total available bandwidth.

  - WFQ scheduling

    Weighted fair queuing (WFQ) ensures that network resources are allocated evenly so that all queues can be scheduled. Therefore, the WFQ queues do not have obvious differences in their priorities. However, sufficient bandwidth must be provided for multimedia applications. It is recommended that the bandwidth be between 30% and 50% of the total available bandwidth.
- Traffic policing principles
  - Interface-based rate limiting is usually configured for egress devices on the network. The available bandwidth provided by the carrier is usually less than the link bandwidth. To prevent packets from being discarded without a reason on the carrier side, you can configure interface-based rate limiting on the enterprise side.

In this case, traffic policing and queue scheduling based on traffic classification can be used to discard packets based on their priorities.

- Typically, traffic policing needs to be configured only on the network boundaries.

- Parameter design of traffic policing
  - Committed information rate (CIR) controls the rate of incoming traffic on a network. Committed burst size (CBS) controls the number of burst packets that are transmitted instantaneously.
  - The CBS should not be smaller than the maximum length of a packet. For example, the CIR is 100 Mbit/s, and the CBS is 200 bytes. If a device receives 1500-byte packets, the packet length always exceeds the CBS, causing the packets to be marked red or yellow even if the traffic rate is lower than 100 Mbit/s. This leads to an inaccurate committed access rate (CAR) implementation.
  - The depth of a token bucket is set based on actual rate limit requirements. In principle, the bucket depth is calculated based on the following conditions:
    i. Bucket depth must be greater than or equal to the MTU.
    ii. Bucket depth must be greater than or equal to the allowed burst traffic volume.
  - Condition 1 is easy to meet. Condition 2 is difficult to operate, and the following formula is introduced:

    Bucket depth (bytes) = Bandwidth (kbit/s) x RTT (ms)/8. Note that RTT refers to round trip time of the TCP and is set to 200 ms.
  - The following formulas are used:
    - When the bandwidth is lower than or equal to 100 Mbit/s: Bucket depth (bytes) = Bandwidth (kbit/s) x 1500 (ms)/8.
    - When the bandwidth is higher than 100 Mbit/s: Bucket depth (bytes) = 100,000 (kbit/s) x 1500 (ms)/8.

8 Operations and Maintenance Management Design and Best Practices

Huawei eSight is a next-generation operation and maintenance (O&M) solution designed for enterprise networks. It uniformly manages enterprise resources, services, and users, and associates these resources intelligently. eSight uses a componentized architecture and provides various components based on a unified management platform. Users can flexibly choose components to suit specific needs.

8.1 Basic Network Management

Table 8-1 describes the key points of basic network management design.

Table 8-1 Key points of basic network management

Requirement Type	Key Point of Requirement Survey	Key Point of Requirement Analysis
Network scale	Number of various types of devices, such as wired devices, wireless devices, and multimedia devices	The network management system (NMS) hardware configuration depends on the calculation result of the quantity and type of managed network devices.

Requirement Type	Key Point of Requirement Survey	Key Point of Requirement Analysis
Network structure	Network structure and hierarchy	● Whether the campus is centralized or distributed geographically. ● Whether different campuses use separate NMSs for management. ● Whether the NMS at the headquarters needs to manage NMSs and devices at all branches.
Network services	Various deployed services, features, and traffic models	● NMS components are used according to services that users are concerned about and expect to manage (such as WLAN, VPN, and VLAN services). ● The NMS software and hardware configuration depends on the scale of managed devices that transmit services.
Network quality	● Whether the network is congested or not ● Whether services are frequently interrupted or not	● Whether network problems need to be located using SLA and iPCA. ● Whether to monitor network device traffic using NetStream. ● Whether to view or audit device behavior using the LogCenter.

The design roadmap for basic network management is as follows:

1. NMS configuration
2. NMS deployment
3. Basic NMS functions (provided by default and no requirement for design)
4. NMS component functions

NMS Configuration

The NMS configuration depends on the number of existing devices on the campus network and the number of devices to be expanded in the future. **Table 8-2** lists the recommended NMS configuration.

Table 8-2 Recommended NMS configuration

Network Scale	Management Scale	NMS Version	Description
Small network: management and maintenance of devices only, with low expected costs	0 to 40 nodes	Compact version	● Supports management only by a user. ● Supports management of alarms, performance, topology, configuration files, NEs, links, VLANs, logs, physical resources, electronic labels, IP topology, smart configuration tool, self-defined devices, security, terminal resources, MIBs, device software, system monitoring tool, database backup/ restoration tool, and fault collection tool.
Medium- and large-sized networks: management of mainstream network devices, network services, and applications	0 to 5K nodes	Standard version (mainstream application version)	● Supports management by multiple users. ● Supports all functions of the compact version, and Agile Reporter, SNMP northbound interfaces, SLA Manager, WLAN Manager, NTA, MPLS VPN Manager, MPLS Tunnel Manager, Secure Center, IPSec VPN Manager, and Mobile Manager.

Network Scale	Management Scale	NMS Version	Description
Ultra-large network: multi-region, multi-layer, and hierarchical network management	0 to 20K nodes	Professional version	• Supports management of lower-layer NMSs. • Supports all functions of the standard version and dual-node hot standby.

NMS Deployment

If high reliability is required, the reliability deployment is recommended. One set of eSight is installed on active and standby servers, respectively. The data is synchronized between active and standby servers through leased lines.

If the active and standby servers are deployed in the same campus, you are advised to set a floating IP address for them. By doing so, after the active/standby switchover, devices do not need to connect to the NMS again.

If the active and standby servers are deployed in different campuses, the two eSight servers use different IP addresses. It is recommended that you set IP addresses of active and standby servers on a managed device. After the active/standby switchover, information such as the device alarm is automatically sent to the standby server to ensure normal device monitoring and management.

Basic NMS Functions

eSight provides basic network management, NE management, service management, and system management, including:

- User management
- Log management
- Resource management
- Topology management
- Alarm management
- Performance management
- Report management

NMS Component Functions

You can install different functional components based on the actual network requirements, as shown in **Table 8-3**.

Table 8-3 Functions of main components of the NMS

Component Name	Function Description
WLAN Manager	WLAN Manager offers an integrated solution that manages wired and wireless networks. WLAN Manager delivers wireless service configurations to APs in batches; centrally manages ACs, APs, wireless users, and areas; diagnoses user access network faults and health level after users access the network; uses WIDS to uniformly monitor network intrusion devices and non-Wi-Fi interference sources, and provide spectrum analysis; displays AP physical locations in a visualized manner and AP heatmap coverage.
MPLS VPN Manager	BGP/MPLS VPN Manager offers end-to-end solutions for VPN service deployment, monitoring, and fault diagnosis. BGP/MPLS VPN Manager deploys service data including VRF, interfaces, and routes for PEs and CEs in batches; automatically discovers VPN services that have been deployed on the network without specifying device roles; displays the logical structure of PE-PE and PE-CE services and displays service alarms in real time; monitors the service running status from multiple aspects, such as alarm, performance, and service link SLA; offers one-click VPN service fault diagnosis by network segment or layer.
MPLS Tunnel Manager	MPLS Tunnel Manager monitors MPLS TE and LDP tunnels, including the tunnel running status, backup status, tunnel topology, alarms, and tunnel-related VPN services.
NTA	eSight Network Traffic Analyzer (NTA) can quickly and efficiently analyze IP network traffic and generate traffic reports. It enables users to detect abnormal traffic in a timely manner based on the real-time application traffic distribution on the entire network and plan networks based on the long-term network traffic distribution. Therefore, NTA can implement transparent network management.
SLA Manager	SLA Manager provides the network performance measurement and diagnosis functions. Users can create SLA tasks to periodically monitor the delay, packet loss, and jitter on the network. SLA services help users to calculate the network compliance. By default, SLA Manager offers 24 services. You can also customize services to meet your specific demands. SLA Manager offers the Dashboard to globally monitor SLA tasks and allows you to quickly learn the quality of all or specific services on the live network. On the SLA view page, you can establish a view that consists of multiple tasks, which helps you compare task data. Quick diagnosis helps you quickly diagnose the links and carried services between source and destination devices, facilitating network fault location.
QoS Manager	eSight provides QoS Manager to monitor traffic. When traffic policies are configured for interfaces, the tool measures network performance counters such as rate of packets matching a traffic classifier, packet drop rate, rate of packets exceeding the CIR, and bandwidth usage for the interfaces.

Component Name	Function Description
IPSec VPN Manager	The IPSec VPN Manager enables you to monitor and diagnose IPSec VPN services, covering the service activation status and alarm status, service topology, performance, and historical tunnel information.
Secure Center	Secure Center can manage security policies of devices on a network where a large number of Huawei firewalls, switches, and routers are deployed. Its main functions include: device management, policy management, object management, monitoring and O&M, and global settings.

8.2 Network Quality Management

The objectives of network quality management design are as follows:

- Service quality evaluation: Preset SLA types based on services, implement proactive O&M, and monitor and score network quality to detect problems in advance.
- Proactive service monitoring and early warning: Create periodic SLA tasks based on the service status and send alarms timely upon detecting services and indicators that exceed the thresholds.
- Quick diagnosis and fault demarcation: Implement fast diagnosis based on services, and find out fault causes and devices according to diagnosis results.
- Policy implementation and result verification: Use the intelligent configuration tool of eSight to configure QoS policies. Create tasks based on service types and monitor QoS queues. Compare QoS queue monitoring results to quickly locate network quality problems.
- Historical data analysis: Compare the SLA task data of each queue to preliminarily locate the fault. You can know the start time and end time of a fault by viewing historical data.

The following measurement solutions are available for network quality management:

- IP SLA measurement solution: This solution supported by the Network Quality Analysis (NQA) feature of network devices proactively sends diagnosis packets between devices to measure key performance indicators such as packet loss rate, delay, and jitter on links. In this way, the quality of related services on the network can be evaluated.
- RTP measurement solution: This solution uses RTP packets to measure the quality of voice and video services in the sending and receiving directions using RTCP packets. For each RTP packet, you can measure the service quality by obtaining the packet sequence number, NTP time flag, RTP time flag, number of sent packets, number of sent bytes, and arrival interval for each RTCP packet.
- iPCA measurement solution: This quality measurement solution is based on Packet Conservation Algorithm for Internet (iPCA) technology developed by Huawei. iPCA implements packet loss monitoring and fault location on a connectionless IP network by coloring real service packets and partitioning the network. It allows a network to perceive service quality and quickly locate faults. In addition, iPCA breaks the limitation of traditional measurement technologies.

Table 8-4 describes the advantages, disadvantages, and application scenarios of the above three solutions.

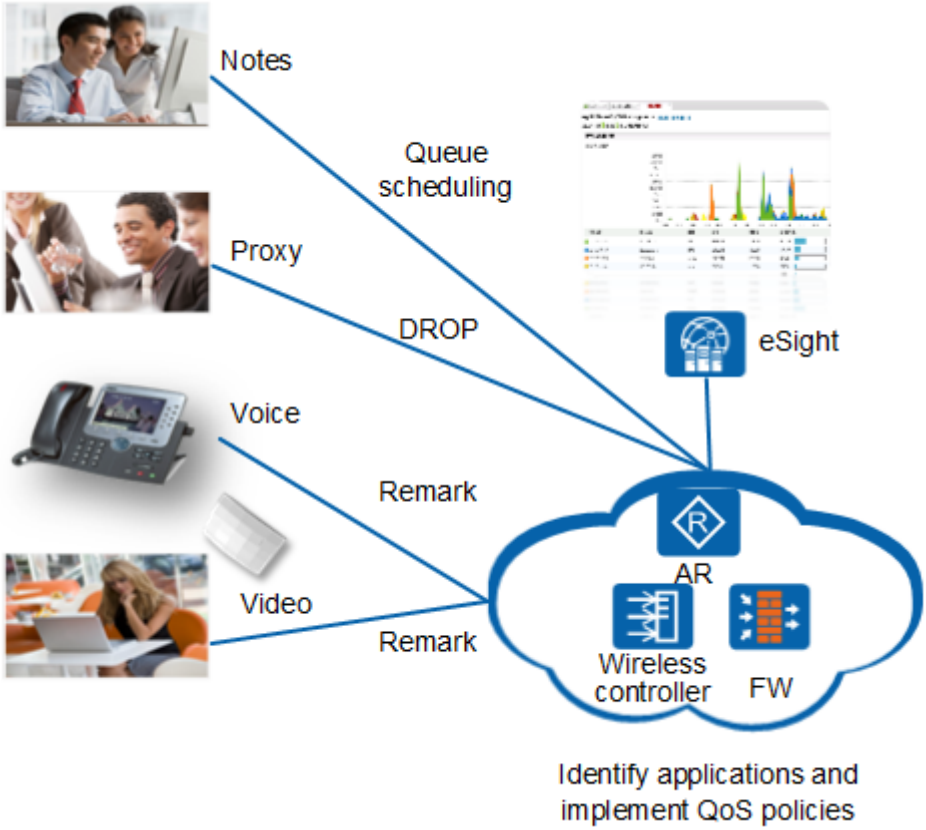
Table 8-4 Measurement solution comparison

Solution Name	Advantage	Disadvantage	Application Scenario
IP SLA	● Specifies the services to be measured, duration, number of times, and interval based on user requirements to perform planned monitoring. ● Does not depend on real service flows and can be measured at any time. ● Performs measurement between any two devices along a path. ● Supports measurement on packet loss, delay, and jitter.	● Uses simulated packets sent by devices. ● Supports measurement only on some fixed service packets. ● The transmission of simulated packets may be different from that of real packets. ● The delay test is based on the round-trip path, which is inaccurate.	Supports measurement only on several fixed protocol packets, such as UDP jitter, ICMP jitter and connectivity/ disconnectivity, FTP, HTTP, and SNMP packets.
RTP	● Uses real RTP packets for measurement. ● Performs measurement based on the fields contained in the RTP protocol and does not need to modify the service flow packets. ● Supports measurement on packet loss, delay, and jitter.	● Does not support other non-RTP packets. ● Cannot perform measurement at any time, and does not support pre-event simulated measurement. ● The source and destination devices that generate packets participate in the measurement.	● Applies to RTP-based applications. ● Only implements measurement between two devices.

Solution Name	Advantage	Disadvantage	Application Scenario
iPCA	● Supports measurement on all IP packets. ● Measures real packets in real time. ● Provides accurate packet loss statistics on a device or link. ● Performs measurement between any two devices along a path.	● Only supports packet loss measurement. ● Cannot perform measurement at any time, and does not support pre-event simulated measurement. ● Needs to identify and use the ToS field in the IP packet header. The packet encapsulation or modification causes the measurement to fail.	● Applies to IP packets. ● Applies to scenarios where faults on devices along a service flow transmission path need to be located.

8.3 Smart Application Control

Smart Application Control (SAC) detects and identifies L4-L7 content and some dynamic protocols (such as HTTP and RTP) in packets based on the service awareness capability of network devices. The identification results are reported to eSight, which then performs statistical analysis and displays results in a unified manner. In addition, SAC implements refined QoS policy control based on application priorities and user requirements.



The SAC solution has the following characteristics:

- Deeply identifies application types based on the service awareness capability of devices.
- Implements refined QoS control policies for service flows based on applications.
- Centrally presents the application statistics of network-wide SAC-monitored devices on the eSight GUI.

When designing SAC, you need to consider the following points:

- Enable the SAC capability depending on whether traffic needs to be controlled based on applications.
- Check whether the monitored service flows are located on a wired or wireless network, and determine device models according to the existing networking and services.
- Check whether customized applications need to be supported and determine device models according to functions supported by the devices.

Design principles for selecting enforcement point devices, control actions, and components are as follows:

- **Enforcement point**

  SAC is an enhanced feature of network management. You are advised to select enforcement points based on the device capability of the existing network.

  WLAN device (AC6005/AC6605/ACU2): When you need to perform application-based control on wireless traffic, set WLAN devices as the SAC enforcement points.

  Firewall: When you need to perform application-based control on wired traffic in campus egresses or data centers, set ARs or firewalls as the SAC enforcement points.

- **Control action**

  The suggestions for setting different control actions are as follows:

  - Remark: used when customers want to modify the packet priority of a specified application.
  - CAR: used when customers want to limit the rate of packets of an application.
  - DROP: used when customers want to drop the packets of an application.
  - Queue scheduling: used when customers want to perform queue scheduling on packets of an application according to the priority re-marking policy.
  - Shaping: used when the traffic of burst applications needs to be buffered to relieve the impact on the network.

- **Component**

  In the SAC solution, eSight and LogCenter collect application identification results from various devices. eSight configures SAC control policies on devices. You are advised to select product components to be deployed based on device types.

  - Application identification result collection:
    - AR/WLAN device (AC6005/AC6605/ACU2): basic component that reports the result to eSight
    - NGFW/NGFW card: product that reports the result to LogCenter
  - SAC control policy delivery:
    - AR/WLAN device (AC6005/AC6605/ACU2): depends on the eSight smart configuration tool module to deliver configurations. (The eSight WLAN service module can also deliver configurations to WLAN devices.)
    - NGFW/NGFW card: depends on the eSight security policy management module to deliver configurations.

8.4 Zero Touch Provisioning

Zero Touch Provisioning (ZTP) aims to help users simplify the network installation process. Multiple functions can be integrated on the eSight platform including network topology planning, automatic configuration generation, topology collection, intelligent error correction, and scheduled configuration backup. ZTP provides automatic and zero manual intervention deployment services for new networks. In addition, this solution implements seamless integration with network deployment planning and maintenance, greatly improving network management and O&M efficiency and reducing labor and time costs.

During the ZTP design, consider the following points:

- Network construction or reconstruction: Specify the ZTP mode. Typically, the topology-based deployment mode is used for new networks and the device identifier deployment mode is used for a few new devices on an existing network.
- Types and quantity of devices to be deployed: Check whether the devices support the deployed features and whether the quantity meets the specifications.
- Stacking mode of fixed switches: Determine whether fixed switches use stack cards or service ports to set up stacks. The two modes have a great impact on subsequent deployment.

The following solutions can be used to implement ZTP:

- Switch EasyDeploy solution: After new switches are installed and powered on, they start the ZTP process to automatically load configuration files, system software packages, patch files, and other required files. The network administrator does not need to commission the switches onsite.
- ZTP solution with manually entered MAC/ESN: The network administrator enters MAC addresses or ESNs of the undeployed switches on eSight and map the MAC addresses or ESNs to configuration files.
- Topology-based ZTP solution: The network topology is planned on eSight in advance and configuration files are generated in batches. After the switches to be deployed are powered on, they collect the topology automatically, and perform mappings to automatically specify the configuration files to be downloaded.

Table 8-5 describes the advantages, disadvantages, and application scenarios of the above three solutions.

Table 8-5 ZTP solution comparison

ZTP Solution	Component	Configuration UI	Configuration Generation Tool	Configuration File	Application Scenario
Switch EasyDeploy solution	● Switch (including the web configuration page) ● DHCP server ● File server	CLI /Web system configuration page	A third party tool (such as notepad)	1. Manually specify the configuration file for each MAC/ESN. 2. Specify the configuration file for each device after the topology is discovered.	Small campus
ZTP solution with manually entered MAC/ESN	● Switch ● eSight (including the file server) ● DHCP server	eSight	eSight	Manually specify the configuration file for each MAC/ESN.	
Topology-based solution				Specify the configuration file based on the topology after the topology is planned on eSight.	Medium- and large-sized campuses

9 Feature Design and Best Practices of Wired Services

9.1 General Best Practices

You Are Advised to Disable Interfaces Not in Use

To prevent interfaces from being misused, you are advised to disable interfaces that are not in use.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] shutdown
```

You Are Advised to Remove All Service Interfaces from VLAN 1

VLAN 1 is a special VLAN on the network. Generally, network devices transparently transmit packets of VLAN 1 by default. Therefore, the default broadcast domain of VLAN 1

is large. It is recommended that you not use VLAN 1, remove interfaces from VLAN 1, and delete the VLANIF1 interface.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] undo port trunk allow-pass vlan 1
[HUAWEI-GigabitEthernet0/0/1] quit
[HUAWEI] undo interface vlanif 1
```

Disabling Interfaces from Transparently Transmitting Packets of All VLANs

Disable interfaces from transparently transmitting packets of all VLANs and only allow packets of corresponding service VLANs to pass through. This minimizes the broadcast domain and reduces the impact of multicast packets.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 0/0/1
[HUAWEI-GigabitEthernet0/0/1] port link-type trunk
[HUAWEI-GigabitEthernet0/0/1] undo port trunk allow-pass vlan 1
[HUAWEI-GigabitEthernet0/0/1] port trunk allow-pass vlan 100 to 102
```

You Are Advised to Configure ACL Filtering on the FTP Server

To ensure the security of an FTP server, you need to configure an ACL for it to specify FTP clients that can access the current FTP server.

Allow the clients whose ACL number are 2000 to log in to the FTP server.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule permit source 10.10.10.1 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] ftp server enable
[HUAWEI] ftp acl 2000
```

9.2 VLAN

The Layer 2 technologies used on campus networks include VLAN technology and loop prevention technology.

VLAN Assignment Mode

The five VLAN assignment modes in descending order of priority are as follows: policy-based VLAN assignment -> MAC address-based or IP subnet-based VLAN assignment (MAC address-based VLAN assignment is used by default. You can configure which of these two is the preferred assignment mode.) -> protocol-based VLAN assignment -> interface-based VLAN assignment. The most commonly used assignment mode is interface-based VLAN assignment.

Table 9-1 describes the application scenarios of different VLAN assignment modes.

Table 9-1 VLAN assignment mode description

VLAN Assignment Mode	Application Scenario	Advantage	Disadvantage
Interface-based assignment	Applies to networks of any scale and with devices at fixed locations.	It is simple to define VLAN members.	The network administrator needs to reconfigure VLANs when VLAN members change.
MAC address-based assignment	Applies to small-scale networks where user terminals often change physical locations but their network adapters seldom change, for example, mobile computers.	When physical locations of end users change, the network administrator does not need to reconfigure VLANs for the users. This improves security of end users, and implements flexible access.	This mode is applicable only to simple networks where network adapters are not changed frequently. The network administrator must predefine VLANs for all members on a network.
IP subnet-based assignment	Applies to scenarios where there are high requirements for mobility and simplified management and low requirements for security.	● When physical locations of users change, the network administrator does not need to reconfigure VLANs for the users. ● This mode reduces communication traffic and allows a broadcast domain to span multiple switches.	Users are distributed regularly and multiple users are on the same network segment.

VLAN Assignment Mode	Application Scenario	Advantage	Disadvantage
Protocol-based assignment	Applies to networks using multiple protocols.	This mode binds service types to VLANs, facilitating management and maintenance.	● The network administrator must preconfigure mappings between all protocol types and VLAN IDs. ● The switch needs to analyze protocol address formats and convert the formats, which consumes excessive resources. Therefore, this mode slows down switch response time.
Policy-based assignment	Applies to complex networks.	● This mode provides high security. MAC addresses or IP addresses of users that have been bound to VLANs cannot be changed. ● The network administrator can flexibly select which policies to use according to the management mode and requirements.	Each policy needs to be manually configured.

If there is no special requirement for VLAN assignment on a campus network, you are advised to use the interface-based assignment mode.

Management VLAN and Interconnection VLAN Design

A Layer 2 switch cannot create a Layer 3 interface. You need to create a VLANIF interface. In this case, a management VLAN needs to be specified. Commonly, a Layer 2 switch uses

the VLANIF interface address as the management address, and a Layer 3 switch uses the loopback interface address as the management address. If the network scale is small, it is recommended that all Layer 2 switches share the same management VLAN and the management IP addresses be on the same network segment. If the network scale is large, you can allocate a management VLAN to the Layer 2 switches under the same gateway and ensure that the management IP addresses are on the same network segment.

An interconnection VLAN is usually deployed between two Layer 3 switches or between a Layer 3 switch and a router. VLANIF interfaces are created for Layer 3 interconnection. If a switch supports switching between Layer 2 and Layer 3 modes, you are advised to switch to Layer 3 mode to configure the interconnection address. If a switch does not support switching between Layer 2 and Layer 3 modes and the interconnection VLAN must be used, it is recommended that the interconnection VLAN be distinguished from the service VLAN. Each interconnection link is assigned a VLAN, and the physical interconnection interface is set to work in Trunk mode.

Voice VLAN Design

Voice and non-voice packets are usually transmitted on the same network. Voice data must have a higher priority than other service data to minimize delay and packet loss during transmission. Voice VLANs help simplify user configurations and facilitate management of voice traffic transmission.

A voice VLAN works in two modes. **Table 9-2** describes the implementation and application scenarios of the two modes.

Table 9-2 Working mode of the voice VLAN

Working Mode	Implementation Method	Application Scenario
Secure mode	The interface where voice VLAN is enabled checks if the source MAC address of every incoming packet matches the OUI. ● If the matching succeeds, the packet is forwarded in the voice VLAN. ● If the matching fails: – If the interface where voice VLAN is enabled to allow packets from other common VLANs to pass through, packets are forwarded in specified VLANs. – If the interface where voice VLAN is disabled from allowing packets from other common VLANs to pass through, the interface discards the packet that fails to match the OUI.	The secure mode is used when multiple types of data traffic (HSI, VoIP, and IPTV) are transmitted to a Layer 2 network through an interface. This interface allows only voice data flows to be transmitted. The secure mode prevents a voice VLAN from being attacked by malicious data flows, but consumes system resources to check packets.
Normal mode	The interface enabled with the voice VLAN function transmits both voice packets and service data packets. In normal mode, the interface is vulnerable to attacks from malicious data traffic.	The normal mode is used when multiple types of data traffic (HSI, VoIP, and IPTV) are transmitted to a Layer 2 network through an interface. This interface allows both voice data flows and service data flows to be transmitted.

VLAN Planning Principles and Suggestions

The principles for planning VLANs on a Layer 2 network are as follows:

- Differentiate the service VLANs, management VLANs, and interconnection VLANs.
- Assign different VLANs to different service zones.
- Assign a VLAN to each service type (Web, app, or DB) in the same service area.
- Use consecutive VLAN IDs to ensure that VLANs are used properly.
- Reserve some VLAN IDs for future expansion.

Assign VLANs as follows:

- By logical area:

  For example:

  - Core network area: VLANs 100 to 199
  - Server area: VLANs 200 to 999 (VLAN IDs 1000 to 1999 are reserved.)
  - Access network area: VLANs 2000 to 3499
  - Service network area: VLANs 3500 to 3999
- By geographic area:

  For example:
  - Area A: VLANs 2000 to 2199
  - Area B: VLANs 2200 to 2399
- By organization:

  For example:
  - Department A in area A: VLANs 2000 to 2009
  - Department B in area A: VLANs 2010 to 2019
- By service function (When free mobility is used, VLANs do not need to be associated with personnel identities. Therefore, this factor can be ignored.):

  For example:
  - Web server area: VLANs 200 to 299
  - App server area: VLANs 300 to 399
  - DB server area: VLANs 400 to 499

9.3 IP Address

In the Internet, Internet Protocol (IP) is a set of rules that enable all communication devices on a network to communicate with each other. Network devices produced by any manufacturer can access the Internet as long as they comply with the IP protocol. An IP address is a numerical label assigned to each device on a network.

IP address planning needs to consider factors such as network services and number of devices. In addition to keeping a unified live network architecture and clear addresses, you need to ensure that the network architecture and routing domain are stable when new IP addresses are added.

Table 9-3 describes the requirements for IP address design.

Table 9-3 IP address design requirements

Requirement Type	Key Point of Requirement Survey	Key Point of Requirement Analysis
Connection point	● Number of user terminals ● Number of servers ● Number of connection points required by each service ● Whether an independent terminal is required to run a single service	The number and types of connection points determine the IP address segment division and the range of each network segment.

Requirement Type	Key Point of Requirement Survey	Key Point of Requirement Analysis
Address space	● Whether the address spaces used for office work and production strictly isolated from each other. ● Users who need to access the Internet ● Whether the IP addresses of partners or branches are uniformly planned by the campus administrator. Services that partners and branches need to access	Services with different address spaces have different address plans. IP addresses may overlap. If the overlapping IP addresses need to communicate, policies such as NAT and proxy need to be deployed.

IP address planning is important in network design. On a large network, IP addresses must be planned in a unified manner. The IP address planning affects routing protocol efficiency, network performance, network expansion, network management, and applications on the network.

Considering network expansion, IP addresses need to be managed easily.

Except for certain devices that use public IP addresses in the DMZ and the Internet interconnected area, devices on the campus network use private IP addresses.

You are advised to assign static IP addresses for servers, special terminals (such as punch-card machine, printing server, and IP video surveillance devices), and production devices. It is recommended that office devices such as PCs and IP phones obtain dynamic IP address using DHCP.

The principles for planning IP addresses are described as follows:

- Uniqueness: The IP address of each node on a campus network must be unique. Even if MPLS VPN isolation is used, it is recommended that different VRFs do not use the same IP address.
- Continuity: The node addresses of the same service must be consecutive to facilitate route planning and summary.
- Scalability: IP addresses need to be reserved at each layer. When the network is expanded, no address segments and routes need to be added.
- Easy maintenance: Device address segments and service address segments need to be clearly distinguished from each other, facilitating subsequent statistics monitoring and security protection based on address segments. If an IP address is planned properly, you can determine the device to which the IP address belongs. The IP address planning can correspond to the VLAN planning. For example, the third byte of an IP address should be the same as the last three bits of the VLAN ID, which helps administrators to memorize and manage IP addresses.

Campus IP addresses are classified into the following types:

- Management address:

  A Layer 2 devices use the VLANIF address as the management IP address. It is recommended that all Layer 2 switches under a gateway use the same network segment.

  You are advised to set the loopback address as the management IP address for Layer 3 devices and set the mask of the loopback address to 32 bits.

  You can reserve two management IP addresses for a stack or cluster system.

- Interconnection address:

  An interconnection address refers to the IP address of an interface connected to anther device's interface.

  An interconnection address must use a 30-bit mask. Core devices use smaller interconnection IP addresses. Interconnection addresses are usually aggregated before being advertised. Therefore, you should allocate contiguous and aggregatable IP addresses as interconnection IP addresses.

- Service address:

  A service address refers to an IP address used by a server, host, or gateway on an Ethernet. Gateway addresses are assigned the same fourth octet. For example, all IP addresses ending with .254 are gateway addresses.

  You must clearly define the address range of each type of sub-service and the address ranges of servers and clients of each type of sub-service.

  The terminal addresses of each type of service are continuous and can be aggregated.

  Considering the scope of the broadcast domain and easy planning, it is recommended that an address segment with a 24-bit mask be reserved for each service address segment. If the number of service terminals exceeds 200, an address segment with a 24-bit mask is extended.

- Internal IP address on a campus network:

  Usually, internal hosts on a campus network use private IP addresses, and NAT devices are deployed at the campus egress to translate private IP addresses into public IP addresses.

  An aggregation switch may connect to multiple network segments. When allocating IP addresses, ensure that these network segments can be aggregated to reduce number of routes on core devices.

- IP address in free mobility:

  Security group planning in the free mobility solution is very important. IP address planning also has a great impact on the configuration of static resource security groups. If IP addresses of interfaces of the same purpose, hosts, or servers are in the same network segment, the security group configuration can be greatly simplified.

  For example, the interconnection IP addresses of all network forwarding device interfaces are separated into multiple network segments (such as 10.1.1.0/30 and 10.1.1.4/30) through subnet masks. However, if a unified network segment (10.1.0.0/16) is reserved for the device interface IP addresses during IP address planning, it is very convenient to configure a security group for network interfaces.

All IP addresses on a campus network belong to the same address space, facilitating mutual access.

When internal users access the Internet, NAT is performed in the Internet egress area to prevent the coexistence of public and private addresses on the network. NAT is performed only for private IP addresses that have the permission to access the Internet. If public

addresses are insufficient, you are advised to use private IP addresses for interconnection interfaces and deploy the public address pools only on NAT devices.

Local addresses of partners and branches may not be uniformly planned by the campus administrator. The campus network must reserve IP address segments for partners and branches based on the campus address space, and allocate IP address segments to partners and branch users through NAT or VPDN at the access border.

9.4 DHCP

DHCP is recommended for office networks in a campus.

Planning a Server

A client broadcasts DHCP Discovery messages. When multiple DHCP servers (or DHCP relay agents) are deployed on a network segment, the client accepts only the first received DHCP Offer message and therefore may obtain an unexpected IP address. Planning DHCP servers ensures that a client obtains network parameters from an expected DHCP server.

Plan VLANs to ensure that only one DHCP server (or a DHCP relay agent) can receive DHCP Discovery messages in a VLAN.

Configure DHCP snooping on uplink access devices of clients to ensure that the clients can apply to the correct DHCP servers for network parameters.

Planning an IP Address

Typically, allocate DHCP addresses based on the service area and allocate static IP address segments and dynamic IP address segments consecutively, which facilitates unified management and problem locating.

- IP address range that can be automatically allocated

  Plan an IP address range based on the number of concurrent online clients on the network. If the number of IP addresses in this range is too small, some clients cannot obtain IP addresses. If the number of IP addresses in this range is too large, IP addresses are wasted.
- (Optional) IP addresses that cannot be automatically allocated

  Some IP addresses in an address pool are reserved for devices that require static IP addresses. For example, in an IP address pool ranging from 192.168.100.1 to 192.168.100.254, 192.168.100.2 is reserved for a DNS server. Exclude the IP address 192.168.100.2 from the IP address pool so that the DHCP server will not allocate 192.168.100.2 to other clients.
- IP address allocation

  DHCP supports dynamic and static IP address allocation. Network administrators can use either of the two mechanisms to allocate IP addresses to hosts based on network requirements.
  - Dynamic allocation: DHCP allocates an IP address with a limited validity period (known as a lease) to a client. This mechanism applies to scenarios where hosts temporarily access the network and the number of idle IP addresses is less than the total number of hosts. For example, this mechanism can be used to allocate IP addresses to laptops used by employees on business trips or mobile terminals in cafes.

- Static allocation: DHCP allocates fixed IP addresses to specified clients with special IP address requirements. For example, the file server of an enterprise needs to use a fixed IP address to provide services for extranet users. Compared with manual IP address configuration, DHCP static allocation prevents manual configuration errors and helps network administrators perform unified maintenance and management.

Planning a Lease

Plan an IP address lease for a client based on the online duration of the client. By default, the IP address lease is one day.

- In locations where clients often move and stay online for a short period of time, for example, in cafes, Internet bars, and airports, plan a short-term lease to ensure that IP addresses are released quickly after the clients go offline.
- In locations where clients seldom move and stay online for a long period of time, for example, in office areas of an enterprise, plan a long-term lease to prevent system resources from being occupied by frequent lease or address renewals.

For medium- and large-sized campus networks, independent DHCP servers are deployed in campus data centers or server areas. DHCP relay is enabled on the gateway at the aggregation layer and a DHCP server for assigning IP addresses in a uniform manner is specified for the aggregation gateway. Generally, a DHCP server assigns IP addresses based on VLANs. In certain scenarios, the DHCP server can assign IP addresses based on the Option 82 field inserted into DHCP packets by access switches.

9.5 Gateway

The gateway hereinafter refers to the gateway of end users and is the boundary between Layer 2 and Layer 3 of the campus network. The gateway must be designed based on factors such as network services and number of terminals.

Table 9-4 describes the requirements for gateway design.

Table 9-4 Gateway design requirements

Requirement Type	Key Point of Requirement Survey	Key Point of Requirement Analysis
Service requirements	● Whether the mutual access between different modules in a campus is under centralized control. ● Whether VLANs can be deployed across devices in a large scale (such as wireless roaming, VM migration, voice VLAN, and VLAN assignment based on user identities).	Relevant network services and management policies affect the gateway deployment locations.
Network architecture	● Whether devices and links are redundant on the network. ● Whether the two gateways are of the same model. ● Whether the physical network is a two-layered or three-layered structure.	The physical structure affects the gateway location. You can select a reliability solution based on the network architecture.
Network Scale	● Types and number of enterprise user terminals ● Number of network devices at each layer	You are advised to evaluate the network scale and service requirements, because this may affect the functions and specifications of the gateway and uplink devices.
Network maintenance	● Whether you are more experienced in O&M for Layer 2 network or Layer 3 network. ● Precise network fault location	You can adjust the logical network structure by referring to the specific network O&M experience.

The following sections present the design suggestions for the selection of gateway deployment locations and gateway reliability.

Gateway Location

As the boundary between Layer 2 switching and Layer 3 routing, a gateway can be flexibly deployed based on the network scale and service requirements.

Theoretically, a gateway can be deployed at any layer of the network. When a gateway is deployed in different locations, the coverage areas of the switching and routing domains are

different, and the network services that can be deployed on the campus network are different. Therefore, a gateway must be deployed at a proper location. This requires you to consider factors comprehensively such as network services, performance, and management.

- Deployed at the aggregation layer: In a typical three-layer structure, a gateway is usually deployed at the aggregation layer. In this way, the Layer 2 broadcast range is moderate, and the number of access terminals and the requirement for ARP/MAC entry specifications of the gateway are also appropriate.
- Deployed at the core layer: In some scenarios, if access behavior in the campus needs to be managed in a centralized manner, or VLANs are deployed across devices in a large scale (such as wireless roaming, VM migration, voice VLAN, and user identity-based VLAN assignment), the gateway is deployed at the core layer. In this scenario, all terminals use the core device as the gateway, and the requirement for ARP entries, MAC addresses, and number of users on the core device is high. Also, the gateway located at the core layer has a large broadcast domain. You need to take other measures to reduce the broadcast domain. For example, port isolation can be used or a VLAN can be assigned to each port. If the VLAN specification is inconsistent with the number of terminals, you may need to deploy QinQ VLANs.
- Deployed at the access layer: The Ethernet network does not have an independent control plane, and most entries are learned from the forwarding plane. As a result, faults cannot be accurately located on an Ethernet network. Considering this, some users try to minimize the scope of the Layer 2 network and deploy the gateway at the access layer. By doing so, faults on a Layer 3 network can be located precisely. In addition, you can flexibly select an authentication mechanism to implement security policies that can be deployed at the access layer. A three-layered network has a large scope. Therefore, you need to divide the routing domain. In addition, access devices must support Layer 3 functions.

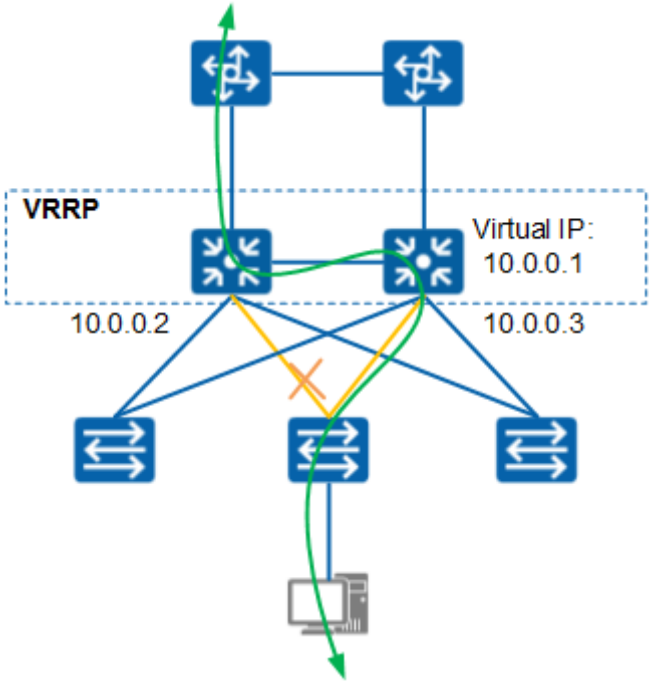
Gateway Reliability

A gateway affects the normal communication between the intranet and extranet of a campus. You can deploy two gateways for terminals to improve reliability. Virtual Router Redundancy Protocol (VRRP) or cluster features can be deployed on the two gateways. The reliability design of the gateway deployed at the aggregation layer is similar to that deployed at the core layer. The following uses the gateway deployed at the aggregation layer as an example.

- **VRRP**

  VRRP is a mature standard protocol and has rich deployment cases. Devices of different models from different vendors can interconnect with each other using VRRP. The specifications of the two gateways are calculated separately and proper overbooking is acceptable.

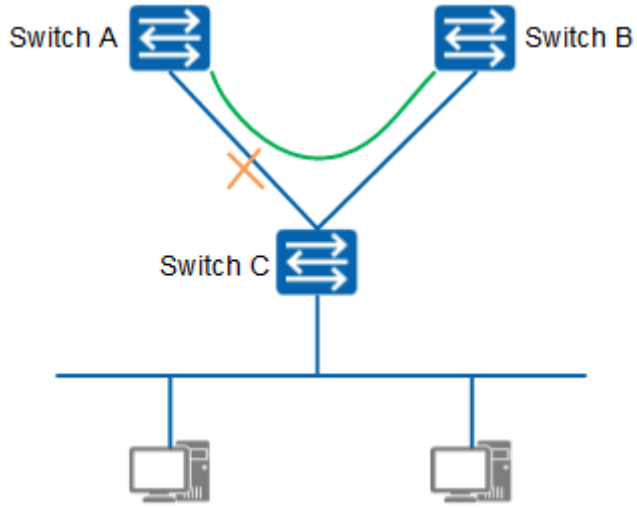
  VRRP is deployed to provide gateway redundancy. When the master device fails, the backup device takes over the gateway function.



VRRP deployment suggestions:

- Run STP at Layer 2. In the same VLAN, deploy the STP root bridge and the VRRP master on the same device so that the Layer 2 and Layer 3 topologies are the same.
- Specify master and backup devices in a VRRP group by setting different priorities.
- Perform the VRRP master/backup switchover not depending on the uplink status of the gateways. Allow the interconnection links between the master and backup devices to participate in route calculation and use the Layer 3 routes to direct traffic forwarding.
- Run STP between the gateway and access device. When the link between them is faulty, STP convergence implements link switchover. The master/backup switchover does not occur between the VRRP gateways.
- When multiple VLANs (corresponding to multiple network segments) are terminated on the gateway, deploy VLAN-based load balancing at Layer 2 and Layer 3.

If the direct physical link between gateways is a Layer 3 link, it cannot transparently transmit packets from service VLANs of downstream switches. If a downlink is faulty (as shown in the following figure), the link cannot be converged by STP, but the fault can be detected by the VRRP protocol. To speed up the master/backup VRRP switchover, you can deploy BFD for VRRP.



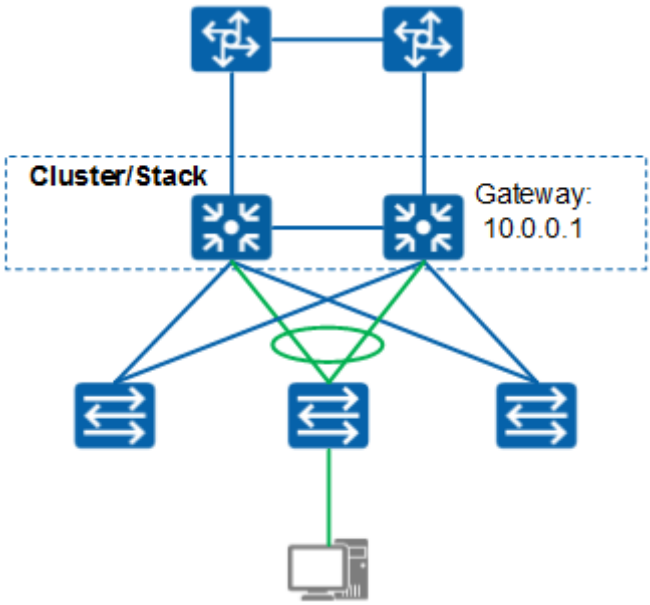
BFD for VRRP deployment suggestions:

- Configure BFD on the backup device, and associate BFD with VRRP so that a master/backup switchover can be triggered when a BFD fault occurs.
- Configure immediate preemption on the backup device and delayed preemption on the master device to prevent traffic loss during switchback.
- BFD has a short delay and consumes a lot of device performance. When VRRP gateways in multiple VLANs exist, you can deploy an independent management VRRP (mVRRP) to associate with BFD. Multiple service VRRP gateways associate with the master/backup status of the mVRRP group. VRRP gateways in each service VLAN does not exchange the master/backup status with each other.
- When VLAN-based VRRP load balancing is deployed, you need to deploy two mVRRP groups and associate the VRRP backup device in the corresponding VLAN with BFD.

- **CSS/Stack**

  Switches in a CSS or stack form a logical device, which has a unified configuration platform. You just need to deploy gateways on the logical device. The switchover upon device or link faults is ensured by the CSS mechanism and does not need to be designed by administrators.

  Deploying a CSS or stack simplifies the logical topology, because only a single gateway needs to be deployed on a logical device. The switchover upon device or link faults is ensured by the CSS mechanism and does not need to be designed by administrators.



Deployment suggestions:

- Deploy the two gateways in a cluster or stack, which forms a logical device and has a unified configuration platform.
- Deploy the service gateway address on the unified configuration platform.
- Bundle multiple links between an access switch and the two gateways into an Eth-Trunk.
- Deploy independent dual-active detection links between the two gateways, or use links between the gateways and access switches to implement dual-active detection.

9.6 Route

The route design aims to simplify the network structure, involve a single protocol, and deploy as few policies as possible.

Table 9-5 describes the requirements for route design.

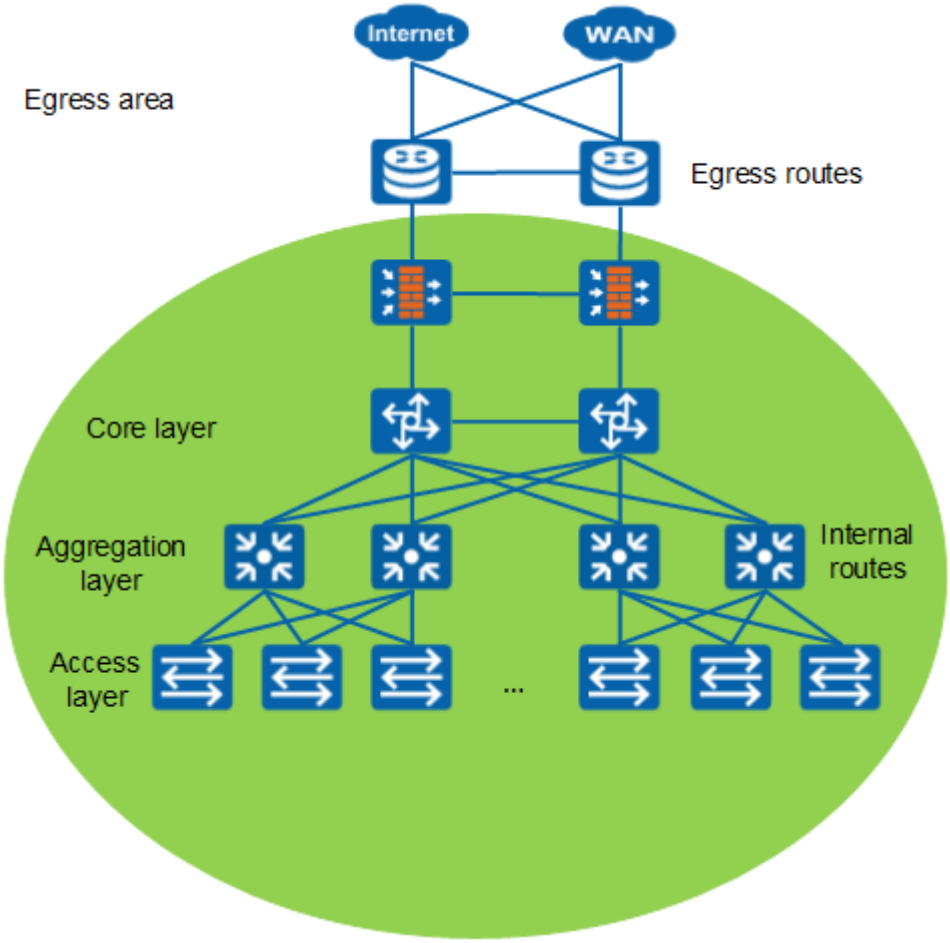
Table 9-5 Route design requirements

Requirement Type	Key Point of Requirement Survey	Key Point of Requirement Analysis
Service requirements	● Whether multiple services need to be transmitted on different paths in the campus network. ● Whether service routes and device routes comply with one protocol.	Service transmission affects routing protocol selection and whether multiple routing protocols need to be deployed on the campus network.

Requirement Type	Key Point of Requirement Survey	Key Point of Requirement Analysis
Network architecture	● Whether there are multiple Internet egresses. ● Whether there are redundant Layer 3 links.	Redundant links affect the selection of static and dynamic routing protocols.
Network scale	● Number of devices in a Layer 3 network ● Routing entries included in a Layer 3 network	The number of nodes and routing entries in a routing domain affect the routing protocol selection and routing domain division.
Network maintenance	● Routing protocols with which the administrator is more familiar ● Whether the carrier needs to update routing information in real time when connecting to the Internet.	You can select the routing protocols to be deployed based on specific network O&M experience.

9.6.1 Design Principles

The route design of a campus network includes the internal route design and the route design between the campus egress and the Internet/WAN devices.



The internal route design of a campus network enables communication between internal devices and terminals. Internal routes can interact with external routes. The internal route design mainly considers the features of selected protocols and fast convergence design.

The egress route design enables intranet users on a campus network to access the Internet and WAN. This chapter describes only the Internet route design for egress routers. WAN routes are designed independently and are not described in the campus route design. The Internet bandwidth is precious. Therefore, the egress route design focuses on the full utilization of the link bandwidth and aims to enhance user experience.

Internal Route Design Principles

It is recommended that aggregation switches be used as the boundary between routing and switching. Such being the case, routes only need to be configured on aggregation switches and core switches. A large number of access switches only perform Layer 2 switching, which simplifies configuration and reduces configuration and maintenance workload.

Static routes or other Interior Gateway Protocol (IGP) routes can be deployed on the campus network. There are many redundant links in the network topology to harden the network. Multiple static routes need to be deployed to ensure reliability. Also, you may need to manually adjust the priorities. Since no proactive detection and withdrawal mechanisms are available for static routes, you need to deploy BFD to trigger withdrawal and replacement of static routes. The configuration is complex.

The IGP can dynamically detect network topology changes and converge in a timely manner. In addition, the performance of the current network devices is sufficient for IGP running. Therefore, the dynamic routing protocols are recommended.

Among multiple IGP protocols, Open Shortest Path First (OSPF) and Intermediate System to Intermediate System (IS-IS) have mature large-scale deployment cases. A single IS-IS area supports more devices and the cost values of all links are the same by default. Generally, no more optimization policies are deployed. IS-IS is applicable to the large-scale ISP backbone network with device specifications pretty much the same.

Multiple OSPF features are suitable for campus networks of various sizes. Most enterprise network administrators are familiar with OSPF. Therefore, OSPF is recommended in the campus network.

Except for network integration scenarios, multiple routing protocols are deployed on a campus network so that cost values can be flexibly set for route selection at the boundary of the routing domain. Currently, the bandwidth and link quality of the campus network are far beyond the requirements. You are advised to deploy only OSPF on the campus network.

Egress Route Design Principles

When egress devices are connected to the Internet or WAN, static routes or Border Gateway Protocol (BGP) are used. Static routes are deployed in most campus networks.

BGP needs to be deployed only when there are multiple links between an enterprise network and an ISP network and these links can provide differentiated routing services. BGP can manage a large number of routes and provides more attributes to control traffic paths.

9.6.2 OSPF Design

Based on the current device performance and existing mature cases, OSPF supports up to 1000 routers, and an OSPF area can accommodate a maximum of 100 devices. These specifications meet the requirements of most campus networks.

Router ID Planning

The stability of the LSDB on each OSPF router is a prerequisite for ensuring the stability of the OSPF network. In an LSDB, LSAs received from different OSPF routers are distinguished by the router ID. If the router ID of a router changes, the router floods its LSA again. As a result, all OSPF routers on the network update their LSDBs and perform SPF calculation again, leading to OSPF network flapping. Therefore, choosing stable router IDs is the first task in OSPF network design.

Router IDs can be configured manually. If no router ID is specified for a router through a command, the system automatically selects an interface IP address as the router's router ID. The router ID selection rules are as follows:

- The system preferentially selects the largest IP address among loopback interface addresses as the router ID.
- If no loopback interface is configured, the system selects the largest IP address among interface addresses as the router ID.
- The system reselects the router ID only when the interface address used as the router ID is deleted or changed.

In actual applications, you are advised to use the IP addresses of loopback interfaces as the router IDs. First, plan a private network segment such as 192.168.1.0/24 for OSPF router ID

selection. Before starting the OSPF process, create a loopback interface on each OSPF router, and use a private IP address with a 32-bit mask as the IP address of the loopback interface. The private IP address is then used as the router's router ID. If there is no special requirement, this loopback interface address does not need to be advertised to the OSPF network.

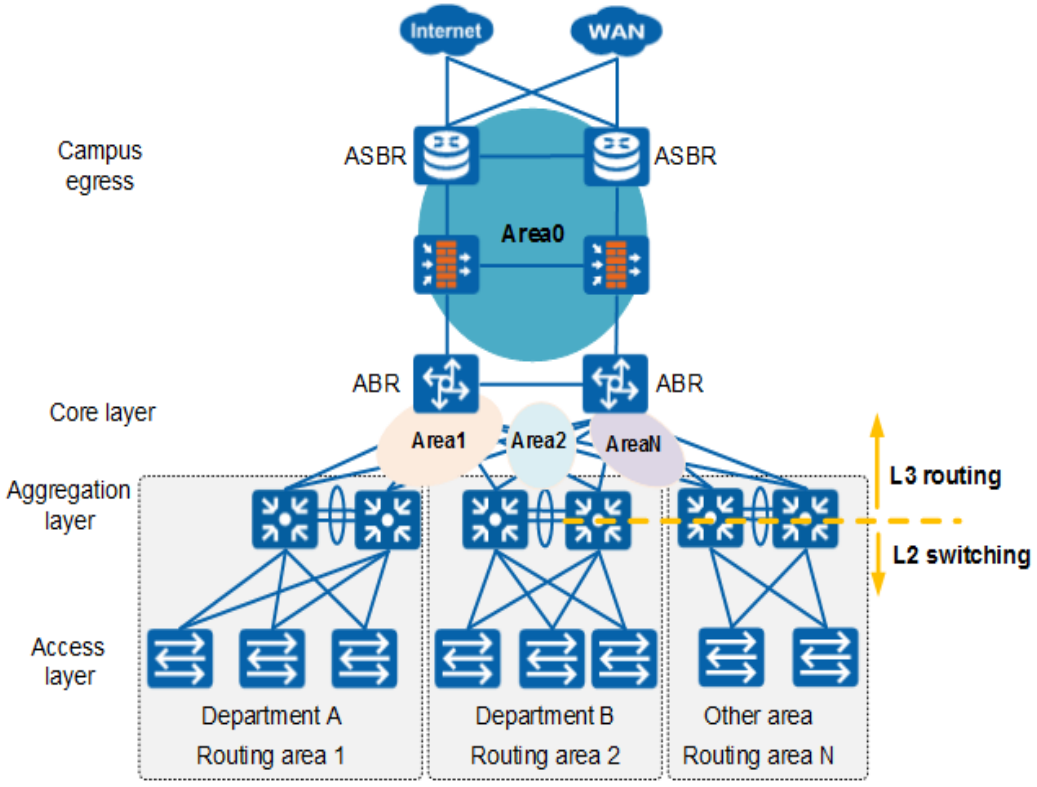
Area Division

OSPF is a network protocol that requires hierarchical design. The concept of area is used in an OSPF network. From a hierarchical perspective, areas on an OSPF network are classified into backbone and non-backbone areas. The number of the backbone area is 0 and that of a non-backbone area ranges from 1 to 4294967295. An OSPF router at the border between the backbone area and a non-backbone area is called an area border router (ABR).

You can only plan the backbone area for small networks such as a network with several routers as the core and aggregation devices. However, hierarchical network design must be considered on large OSPF networks.

For large OSPF networks, the core, aggregation, and access layers must be considered in OSPF area design. In addition, OSPF backbone routers generally are egress routers and core switches. Non-backbone area design depends on the geographical location and device performance. If many low-end Layer 3 switching devices are deployed in a non-backbone area, the number of routes should be minimized to reduce the area size or a special area can be used due to product positioning and performance limitations of the switching devices.

In the scenario where the gateway is deployed at the aggregation layer, Area 0 is deployed to cover the backbone area between the core layer and the egress area. Configure egress routers as autonomous system border routers (ASBRs) or ABRs, and configure core switches as ABRs. Configure an OSPF area on each pair of aggregation switches and core switches. The areas are numbered 1, 2, and N.



Routing Entry Optimization

Using special areas can optimize routing entries on routers in non-backbone areas. Generally, the number of routing entries on routers in a non-backbone area needs to be reduced in the following scenarios:

- The non-backbone area has only one ABR as the egress router and all traffic for accessing external areas passes through this egress router. In this case, non-ABR routers in this non-backbone area do not need to obtain detailed information about external areas, and only an egress is required to send traffic outside this area.
- Some low-end Layer 3 switches are deployed in the non-backbone area and their routing tables cannot contain too many routing entries because of performance limitations. Special areas can be configured to reduce the number of routing entries on the devices.

Switches support four types of special areas defined in OSPF: stub area, totally stub area, NSSA, and totally NSSA.

In most cases, routers in non-backbone areas on a typical OSPF network only need to know the outbound interface of the default route. Therefore, it is recommended that non-backbone areas be planned as totally NSSAs. This configuration significantly reduces the number of routing entries on internal routers of the non-backbone areas and the number of OSPF packets exchanged among these routers. Route computing and topology changes in an area do not affect other areas. A network fault causes route flapping only in the local area.

Because routers in the backbone area are responsible for route exchange among areas, these routers have large routing tables. You can properly plan IP subnets used by non-backbone areas and summarize routes on routers at area borders to optimize routing entries on routers in the backbone area.

It is recommended that an IP network facilitating route summarization be used as a new OSPF network, and IP addresses be planned again for expanded OSPF networks. Route summarization reduces the number of routing entries in routing tables of routers in the backbone area and the number of OSPF packets exchanged among these routers. After routes are summarized, a single-point link failure or network flapping does not affect route update on the entire network. Therefore, route summarization improves network stability.

Route summarization reduces the number of routes and improves network stability in many scenarios. However, routing loops may occur in route summarization. Blackhole routes can solve this problem. A router discards packets that match a blackhole route, and does not send any error information to the packet sender. Therefore, route summarization and blackhole routes are often used together in OSPF network design.

Route Import

There are multiple specific routes and default routes on the egress router regardless of whether static routes or BGP routes are running between the campus egress and the ISP.

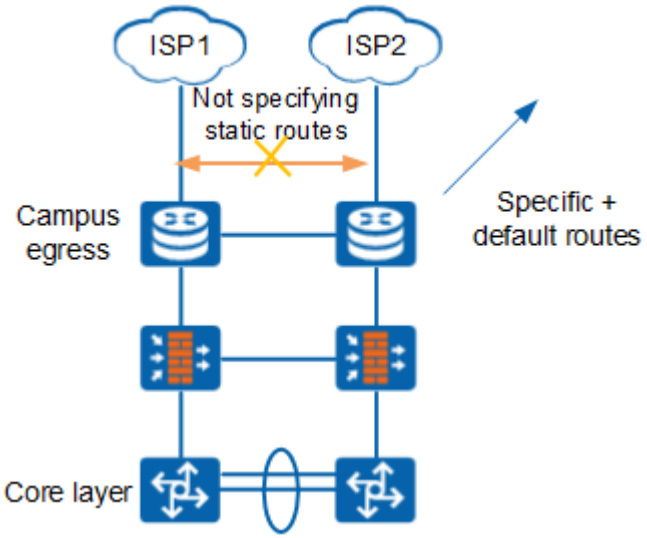
If static routes are running between the egress device and the ISP, you can simply import all the specific routes and default routes to OSPF. It is not recommended to advertise the default routes forcibly to OSPF. If the local default routes do not exist, OSPF deletes the default routes from the intranet.

If BGP is running between the egress device and the ISP, only the default routes need to be imported. **Egress Route Design** describes the design of preferentially selecting specific routes.

When routes of the user network segment are imported to the gateway, you are advised to use the network + silent interface mode to advertise the routes. In this manner, the user routes are calculated as OSPF internal routes.

9.6.3 Egress Route Design

Static Route Design



The design roadmap for static routes is as follows:

- Two egress routers on the campus network are configured with static default routes, which are imported to the campus network.
- The address segments of ISPs are collected and deployed at corresponding egresses using specific static routes, which are imported to the campus network.
- When BFD or NQA is associated with static routes, the invalid static routes can be deleted.

  BFD needs to be deployed bidirectionally. That is, devices on the ISP must be deployed with BFD. Otherwise, BFD does not take effect.

  NQA only needs to be deployed on the campus egress device, which has to negotiate with the ISP device to set a security policy that permits and responds to NQA packets.

  Single-hop detection is recommended for both BFD and NQA. Otherwise, the deployment is complex and response packets may fail to be routed.
- The NAT policy is deployed on the firewall. The source address of the packets sent by the egress router is bound to an ISP. In this case, the two egress routers do not forward packets destined for the Internet. This prevents the packets from being filtered by the uRPF policy of the ISP. Therefore, no static route is deployed between the two egress routers.

BGP Route Design

A campus network uses BGP in the following situations:

- Scenario 1: The number of routes on the network is so large that OSPF is not capable of processing all the routes. In most cases, a campus network does not have too many routes. If a large number of routes exist on the campus egress routers caused by many

enterprise branches and improper IP address planning, you are advised to deploy BGP to properly plan IP addresses and import some routes.

- Scenario 2: Due to service requirements, a large number of routing policies and service traffic distribution are required. The OSPF protocol is not good at processing these issues. BGP can be used to control routing policies and direct service flows.
- Scenario 3: MPLS VPN is used to provide complex isolation policies.

BGP planning suggestions on the campus network are as follows:

- Router ID planning

  BGP and OSPF share the same router ID, which is the IP address of the loopback interface.
- Planning of AS numbers

  BGP uses private AS numbers because an enterprise network is a private network.
- Selection of IBGP or EBGP

  Typically, IBGP is used because the size of an enterprise network is not very large.

  IBGP is deployed between two egress routers and an IBGP peer relationship is established using loopback interface addresses. Ensure normal addressing for the internal device traffic regardless of the egress device to which the traffic is sent, as long as the external network is reachable.
- The enterprise intranet runs only IGP (usually OSPF) and does not run BGP. Because the OSPF routing table is much smaller than the BGP routing table, the two egress routers advertise only default routes to the internal network (through IGP), and do not advertise BGP routes to the intranet devices.
- To prevent an enterprise from being traversed by Internet traffic and become a free ISP, you need to filter routes in the outbound direction and advertise only the public network segments of the enterprise to the ISP. Prefix List is used to filter routes by route prefix so that only the route prefix of the local AS can be advertised. As Path List is used to filter routes in the As-Path dimension so that only locally originated routes can be advertised.
- The private IP addresses, class D/E IP addresses, and loopback IP addresses in the inbound direction as well as the applied public IP addresses need to be filtered.
- To simplify O&M and reduce the BGP table capacity, only prefixes originating from the peer ISP devices are received and the As-Path List is used to filter the prefixes.

9.6.4 Best Practices

You are advised to configure OSPF packet authentication.

To ensure route security and avoid importing invalid routes, you are advised to configure OSPF packet authentication. Two authentication methods are supported: area-based authentication and interface-based authentication. If both authentication methods are configured, interface-based authentication is used preferentially.

If **plain** is selected during the area-based authentication configuration, the password is saved in the configuration file in plain text. This brings security risks. It is recommended that you select **cipher** to save the password in cipher text. HMAC-SHA256 is recommended for ciphertext authentication. The authentication modes and passwords of all the devices must be the same in any given area, but can differ between several areas.

Configure HMAC-SHA256 authentication for OSPF area 0.

```
<HUAWEI> system-view
[HUAWEI] ospf 100
[HUAWEI-ospf-100] area 0
[HUAWEI-ospf-100-area-0.0.0.0] authentication-mode hmac-sha256 ciper huawei@123
```

Interface-based authentication is used to set the authentication mode and password used between neighboring devices. It takes precedence over area-based authentication.

Configure OSPF HMAC-SHA256 authentication on VLANIF100.

```
<HUAWEI> system-view
[HUAWEI] interface vlanif 100
[HUAWEI-Vlanif100] ospf authentication-mode hmac-sha256 ciper huawei@123
```

Configuring the network type of an interface

By default, the network type of an interface is determined by the physical interface. The network type of an Ethernet interface is broadcast. When a network type is configured for an interface, the original network type of the interface is replaced.

The network type of an interface can be configured to suit networking requirements. For example:

- If the network type of an interface is broadcast and a switch does not support multicast addresses, change the network type of the interface to NBMA.
- If the network type of an interface is NBMA and the network is fully meshed (any two switches are directly connected), change the network type of the interface to broadcast. Configuring neighboring router information on the interface is not required.
- If the network type of an interface is NBMA and the network is not fully meshed, change the network type of the interface to P2MP. This allows two indirectly connected switches to communicate through one switch that can directly reach both of the two switches. Configuring neighboring switch information on the interface is not required.
- If only two switches run OSPF on the same network segment, change the network type of the interface to P2P.

You are advised to disable the receiving and sending of OSPF packets on an interface that does not need to establish a neighbor relationship.

To ensure that OSPF routing information is not obtained by the devices of a certain network and the local device does not receive routing update information advertised by other devices, you can run the **silent-interface** command to disable an interface from receiving and sending OSPF packets, thereby preventing routing loops.

In OSPF network design, OSPF packets are often prohibited from being sent to users, preventing end users from obtaining OSPF packet information. If a user can intercept OSPF packets, the user knows how to connect to the OSPF network, making the OSPF network prone to attacks or damages. For example, if a router is connected to an OSPF network and the router's OSPF process is unstable, the OSPF network flaps or even breaks down.

To ensure security and stability of an actual OSPF network, it is recommended that silent interfaces be configured on edge devices of the OSPF network to prevent OSPF packets from being sent to users. These silent interfaces are prohibited from receiving and sending OSPF packets. These interfaces can still advertise direct routes, but cannot establish neighbor relationships because Hello packets are blocked.

Disable interfaces except VLANIF 100 from sending or receiving OSPF packets.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] silent-interface all
[HUAWEI-ospf-1] undo silent-interface vlanif 100
```

You are advised to enable the OSPF sham-hello function.

After this function is enabled, the device maintains neighbor relationships through both the Hello packets and also all OSPF protocol packets. This accurately senses the existence of OSPF neighbors and stabilizes neighboring relations.

Enable the sham-hello function.

```
<HUAWEI> system-view
[HUAWEI] ospf 1
[HUAWEI-ospf-1] sham-hello enable
```

Modifying the cost value properly

An OSPF router determines whether a route is optimal by calculating its cost, and preferentially adds a route with a smaller cost to its routing table. Therefore, you can adjust the costs of OSPF interfaces to make a router select different outbound interfaces for load balancing.

By default, the reference bandwidth for OSPF cost calculation is 100 Mbit/s. By default, OSPF considers that the cost of an interface with bandwidth larger than 100 Mbit/s is 1. The switch provides the function of changing the reference bandwidth. In OSPF network construction, you can run the **bandwidth-reference** command on the switch to configure a proper reference bandwidth.

For route selection optimization on an OSPF network, it is recommended that you select a proper reference bandwidth and then change costs of OSPF interfaces.

The cost values of devices at both ends of a link must be the same so that incoming and outgoing traffic can be transmitted along the same path.

9.7 AAA

You are advised to accurately match the rights of a local user.

You are advised to configure only the required access type according to the actual situation to avoid redundant configurations.

Set the user access type to ftp, ssh, or terminal.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user huawei service-type ftp ssh terminal
```

If the web system is not used, you are advised to disable the HTTP service of the user.

Using HTTP has potential security risks. If the web system is not used, you are advised not to enable the HTTP service.

In V200R010C00 and later versions, the HTTP and Terminal services are enabled for the **admin** user by default. If the web system is not used, you are advised to disable the HTTP service.

Set the access type of the local user **admin** to terminal.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] local-user admin service-type terminal
```

In V200R008C00, only the HTTP service is enabled for the **admin** user by default. If the HTTP service is not used, the user is invalid. Therefore, you are advised to delete the local user named **admin** in AAA mode if the web system is not used.

Delete the local user **admin**.

```
<HUAWEI> system-view
[HUAWEI] aaa
[HUAWEI-aaa] undo local-user admin
```

9.8 Eth-Trunk

- To ensure reliability, it is recommended that member interfaces reside on different cards or chassis.
- It is recommended that the number of member interfaces be no more than 8.
- The Ethernet type of member interfaces of an Eth-Trunk must be the same.
- When you connect two devices, ensure the link aggregation modes on them are the same.

  If both ends support Link Aggregation Control Protocol (LACP), you are advised to deploy link aggregation in LACP mode. When the status of a member interface in a link aggregation group (LAG) changes, you do not need to manually modify the configuration of the member interface. LACP automatically adjusts the link aggregation status to rectify the fault, and the entire process does not affect traffic forwarding.

  NOTE

  If one end does not support LACP, link aggregation can only be deployed manually.

  # Configure Eth-Trunk 1 to work in LACP mode.

  ```
  [HUAWEI] interface eth-trunk 1
  [HUAWEI-Eth-Trunk1] mode lacp
  [HUAWEI-Eth-Trunk1] quit
  ```

- When you configure the number of LAGs and the number of member interfaces, the cards installed on devices must be cards of scalable Eth-Trunk specifications. If the index of an Eth-Trunk interface exceeds 127 and an LPU of lower specification is inserted, the LPU fails to register and an alarm L2IFPPI_1.3.6.1.4.1.2011.5.25.219.2.2.13_hwBoardPowerOff is generated. If a low-specification LPU has been installed on the device, the index of the Eth-Trunk interface cannot exceed 127.
- When BFD is used for inter-card Eth-Trunk detection, it is recommended that the detection time be set to a value greater than 300 ms. Otherwise, the BFD link flaps when the interface goes Down or the card is reset.

9.9 HTTP

You Are Advised to Disable the HTTP Service Not in Use

If you do not require the web system service, it is recommended that the HTTP service not in use be disabled.

By default, the HTTP IPv4 service is enabled and the HTTP IPv6 service is disabled. The HTTPS IPv4 service is enabled, and the HTTPS IPv6 service is disabled.

Disable the HTTP IPv4 and HTTPS IPv4 services.

```
[HUAWEI] undo http server enable
[HUAWEI] undo http secure-server enable
```

You Are Advised to Forbid Users to Log In to a Device Through HTTP If HTTPS Is Used

When a device functions as an HTTPS server, you can configure an ACL on the device to allow only the specified clients to log in to the device through HTTPS. This function improves system security.

Set the ACL number to 2000 for the HTTPS IPv4 server.

```
<HUAWEI> system-view
[HUAWEI] acl 2000
[HUAWEI-acl-basic-2000] rule 1 permit source 10.1.1.1 0
[HUAWEI-acl-basic-2000] quit
[HUAWEI] http acl 2000
```

You Are Advised to Forbid Users to Log In to a Device Through HTTP If HTTPS IPv6 Is Used

When a device functions as an HTTPS server, you can configure an ACL on the device to allow only the specified clients to log in to the device through HTTPS. This function improves system security.

Set the ACL number to 2000 for the HTTPS IPv6 server.

```
<HUAWEI> system-view
[HUAWEI] acl ipv6 2000
[HUAWEI-acl6-basic-2000] rule 1 permit source fc00:1::1 128
[HUAWEI-acl6-basic-2000] quit
[HUAWEI] http ipv6 acl 2000
[HUAWEI] http ipv6 server enable
[HUAWEI] http ipv6 secure-server enable
```

9.10 Loop Detection

If a network fault possibly caused by a loop occurs, you are advised to configure loop detection on the network.

When a loop occurs on a network, broadcast, multicast, and unknown unicast packets are circulated on the network. This wastes network resources and can result in network breakdown. Quickly detecting loops on a Layer 2 network is crucial for users to minimize the

impact of loops on a network. A detection technology is required to help users check network connections and configurations, and control the looped interface.

Loop detection periodically sends detection packets on an interface to check whether the packets return to the local device (through the same interface or another interface), and determines whether a loop occurs on the interface, local network, or downstream network.

- If detection packets are received and sent by the same interface, a loopback occurs on the interface or a loop occurs on the network connected to the interface.
- If detection packets are received by another interface on the same device, a loop occurs on the network connected to the interface or device.

NOTICE

- The loop detection function needs to send a large number of detection packets to detect loops, occupying system resources. Therefore, disable this function if loops do not need to be detected.
- When a loop occurs on the network-side interface where the Block or Shutdown action is configured, all services on the device are interrupted. Therefore, you are not advised to deploy loop detection on a network-side interface.

```
<HUAWEI> system-view
[HUAWEI] loop-detection enable
[HUAWEI] vlan batch 10 to 20
[HUAWEI] loop-detection enable vlan 10 to 20
[HUAWEI] loop-detection interval-time 10
[HUAWEI] interface gigabitethernet 1/0/0
[HUAWEI-GigabitEthernet1/0/0] stp disable
[HUAWEI-GigabitEthernet1/0/0] port link-type hybrid
[HUAWEI-GigabitEthernet1/0/0] port hybrid tagged vlan 10 to 20
[HUAWEI-GigabitEthernet1/0/0] loop-detection mode port-quitvlan
[HUAWEI-GigabitEthernet1/0/0] quit
```

9.11 SNMP

You are advised to set the SNMP version to v3.

Using SNMPv1 and SNMPv2c has potential security risks. SNMPv1 and SNMPv2c use a limited security authentication mechanism based on community names, which are transmitted in plain text. You are not advised to use SNMPv1 or SNMPv2c on untrusted networks.

In the user-based security model, SNMPv3 eradicates security defects in SNMPv1 and SNMPv2c and provides authentication and encryption services.

Create an SNMPv3 user group to authenticate and encrypt SNMP messages, and configure the view that the SNMPv3 user group can read and write to public. Configure an SNMPv3 user with user name **huawei**, group name **huawei**, authentication mode sha, authentication password 8937561bc, encryption mode aes128, and encryption password 68283asd.

```
[HUAWEI] snmp-agent group v3 huawei privacy read-view iso_view write-view
iso_view acl 2999
[HUAWEI] snmp-agent mib-view included iso_view iso
[HUAWEI] snmp-agent usm-user v3 huawei group huawei
[HUAWEI] snmp-agent usm-user v3 huawei authentication-mode sha
Please configure the authentication password (8-64)
```

```
Enter Password:
Confirm Password:
[HUAWEI] snmp-agent usm-user v3 huawei privacy-mode aes128
Please configure the privacy password (8-64)
Enter Password:
Confirm Password:
```

9.12 STP

You are advised to disable STP on uplink interfaces of gateways

Gateways are the boundary between Layer 2 and Layer 3 networks. If STP is enabled in a downlink Layer 2 network of a gateway, you are advised to disable STP on uplink interfaces to prevent STP convergence from affecting uplink Layer 3 links.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] stp disable
```

You are advised to configure user-side interfaces of an access switch as edge interfaces.

After a user-side interface is configured as an edge interface, it does not participate in spanning tree calculation. This configuration speeds up network topology convergence and enhances network stability. It is recommended that interfaces on access switches connecting to PCs and access terminals be configured as edge interfaces.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] stp edged-port enable
```

You are advised to configure BPDU protection.

When an attacker sends a simulated BPDU to an edge interface, it changes to a non-edge interface. After BPDU protection is enabled, an edge interface will be shut down upon receiving a BPDU, and its attribute will not change.

```
<HUAWEI> system-view
[HUAWEI] stp bpdu-protection
```

NOTE

After BPDU protection is enabled, an edge interface will be shut down upon receiving a BPDU, and its attribute will not change. By default, an interface cannot automatically restore to Up state after it is shut down. To restore the interface, run the shutdown and undo shutdown commands on the interface in sequence. Alternatively, run the restart command on the interface to restart the interface. To configure the interface to go Up automatically, run the **error-down auto-recoverycausebpdu-protection interval** *interval-value* command in the system view to set a recovery delay. After the delay, the interface goes Up automatically.

You are advised to manually specify the priority and location of the root bridge.

Generally, a high-performance switch at a high network layer is required to be selected as the root bridge. However, the high-performance switch at a high network layer may not have a high priority. Therefore, the root bridge of a spanning tree can be specified, so as to ensure that the device becomes the root bridge. To ensure that network traffic is not interrupted, configure a secondary root bridge. When the root bridge is faulty or is powered off, the secondary root bridge becomes the root bridge during spanning tree calculation.

Set the switch as the root bridge of spanning tree instance 1 when MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp instance 1 root primary
```

Set the switch as the secondary root bridge of spanning tree instance 2 when MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] stp instance 2 root secondary
```

You are advised to configure root protection on a designated port of the root bridge.

Due to incorrect configurations or malicious attacks on a network, a valid root bridge may receive BPDUs with a higher priority. Consequently, the valid root bridge is no longer able to serve as the root bridge and the network topology is changed, triggering spanning tree recalculation. As a result, traffic may be switched from high-speed links to low-speed links, causing network congestion. To prevent network congestion, enable root protection on the switch to protect the role of the root switch by retaining the role of the designated port.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] stp root-protection
```

NOTE

Root protection takes effect only on designated ports.

You are advised to set a fixed cost value for an Eth-Trunk interface to prevent intermittent service disconnection on the interface that causes frequent STP convergence.

After STP is enabled on an Eth-Trunk, the STP cost value changes when member interfaces of the Eth-Trunk change (for example, the member interfaces go Down). Therefore, you are advised to set a fixed cost value for an Eth-Trunk interface to prevent STP convergence caused by changes of member interfaces.

Set the path cost of Eth-Trunk 1 in spanning tree instance 2 to 200 when MSTP is running.

```
<HUAWEI> system-view
[HUAWEI] interface Eth-trunk 1
[HUAWEI-Eth-trunk1] stp instance 2 cost 200
```

10 Feature Design and Best Practices of Wireless Services

10.1 General Best Practices

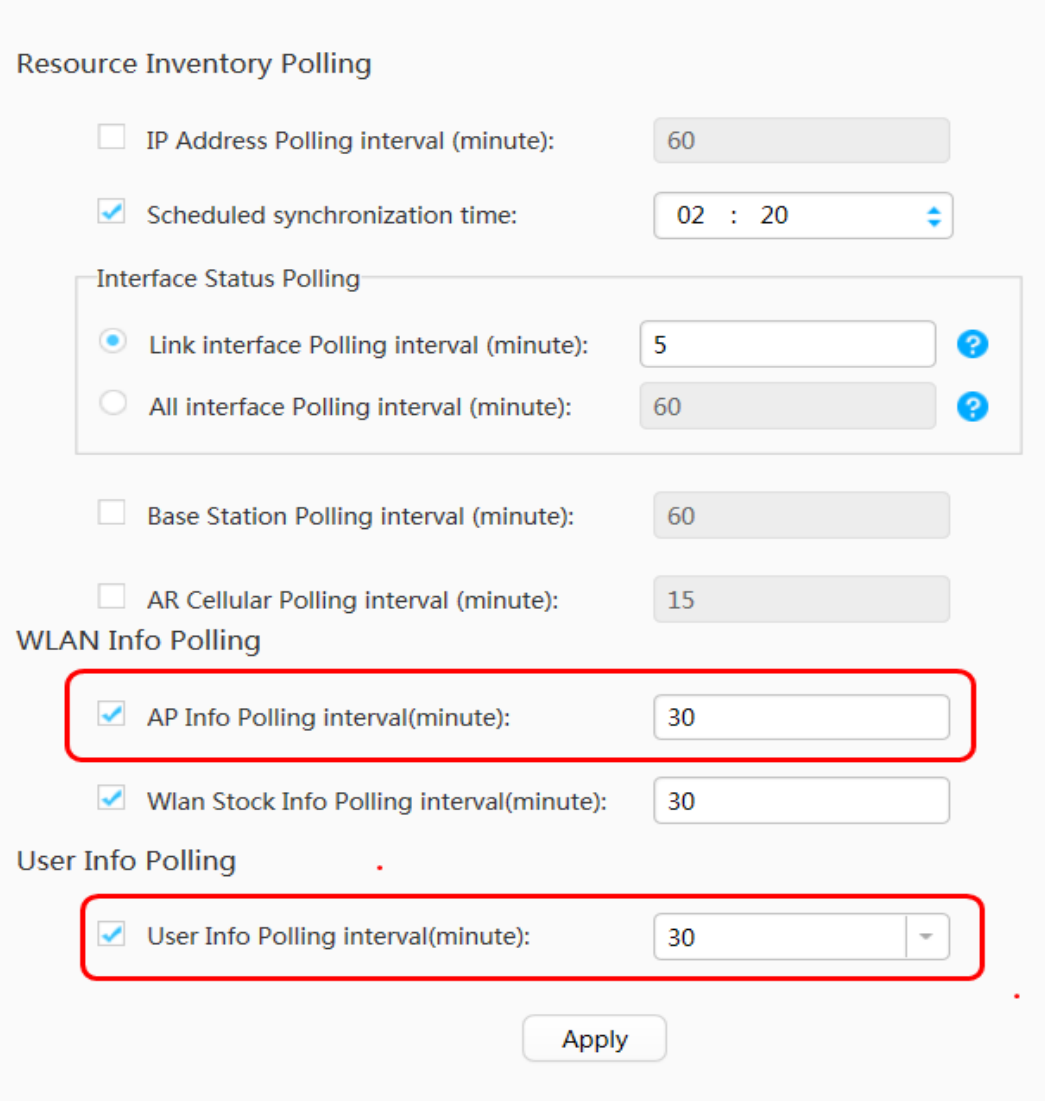
Recommended Interval at Which the Performance Statistics Are Sampled

If eSight is deployed, it periodically collects system data from the AC. In this case, you need to deploy Performance Management (PM) and set the collection interval to 30 minutes or longer.

Set the collection interval to 30 minutes on the AC.

```
<AC> system-view
[AC] pm
[AC-pm] statistics-task task1
[AC-pm-statistics-task1] sample-interval 30
```

On eSight, choose System > Network Management Settings > Polling Settings. Set AP Info Polling interval (minute) and User Info Polling interval (minute) to 30 minutes or longer.



PM technology periodically collects system data and consumes system resources. If eSight is not deployed, it is recommended that PM be disabled.

You Are Advised to Enable Fast ICMP Reply

Ping is a common method for checking network connectivity. However, a large number of ICMP packets affect device performance, reducing the number of wireless users supported by the AC. The ICMP fast reply function is enabled on an AC by default. Keep this function enabled, unless otherwise required.

Enable fast ICMP reply on the wireless controller.

```
<AC> system-view
[AC] icmp-reply fast
```

Shortening the Aging Time of STAs

Due to the high mobility of end users, some APs deployed in cafeterias and lecture halls are associated with a large number of terminals within a short period of time. As a result, new

users cannot access the network after the number of associated terminals reaches the upper limit. In fact, because many terminals are in free mobility and may quickly go beyond the coverage area of APs. Therefore, it is recommended that the aging time of STAs be reduced to one minute.

Set the association aging time of STAs to one minute in the SSID profile **ssid1**.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] ssid-profile name ssid1
[AC-wlan-ssid-prof-ssid1] association-timeout 1
Warning: This action may cause service interruption. Continue?[Y/N] y
```

Saving Configuration

You can run commands to modify the current configuration of the device, but the modified configuration will be lost after the device restarts. To enable the new configuration to take effect after a restart, save the current configuration in the configuration file before restarting the device.

```
<HUAWEI> save
The current configuration (excluding the configurations of unregistered boards or
cards) will be written to flash:/vrpcfg.zip.
Are you sure to continue?[Y/N]y
Now saving the current configuration to the slot 4.
Info: Save the configuration successfully.
```

Run the following command to compare the current configuration with the configuration file for next startup.

```
<HUAWEI> compare configuration
```

10.2 VLAN

In actual applications, it is recommended that management packets and service data packets use different VLANs. You are not advised to use VLAN 1 as the management VLAN or service VLAN.

Since WLANs provide flexible access modes, STAs may connect to the same WLAN at the office entrance or stadium entrance, and then roam to different APs. If each SSID has only one service VLAN to deliver wireless access to STAs, IP address resources may become insufficient in areas where many STAs access the WLAN, and IP addresses in other areas are wasted. Create a VLAN pool, add multiple VLANs to the VLAN pool, and configure the VLAN pool as the service VLAN for a VAP. In this way, an SSID can use multiple service VLANs to provide wireless access services. Newly connected STAs are dynamically assigned to VLANs in the VLAN pool, which reduces the number of STAs in each VLAN and also the size of the broadcast domain. Additionally, IP addresses are evenly allocated, preventing IP address waste.

10.3 IP Address

The IP addresses planned during the wireless network design include IP addresses of ACs, APs, and terminals.

- IP addresses of ACs

  The AC manages APs. Generally, static IP addresses are assigned to ACs manually.

- IP addresses of APs

  Because there are a large number of APs and the configuration workload is heavy, it is recommended that a DHCP server be used to allocate IP addresses. For details, see the following table.

  Table 10-1 IP address assignment mode of APs

Address Assignment Mode	Description	Characteristics	Application Scenario
Assignment based on the Option 60 field	The DHCP server assigns IP address to APs by matching the Option 60 field.	● AP IP addresses are separated from IP address of wireless users. ● The DHCP relay agents must be able to identify the DHCP Option 60 field.	Networks that require separate management of AP IP addresses and user IP addresses

Address Assignment Mode	Description	Characteristics	Application Scenario
Assignment based on VLANs	The AP interfaces connecting to switches are added to VLANs in trunk mode, and interface address pools corresponding to the VLANs are configured to allocate addresses to STAs.	● AP IP addresses are separated from IP address of wireless users. ● The configuration workload is heavy and APs cannot be used immediately when they are connected to switches.	Networks that require separate management of AP IP addresses and user IP addresses
Assignment based on MAC addresses	MAC addresses and IP addresses of APs are configured on the DHCP server.	● AP IP addresses are separated from IP address of wireless users. ● The configuration workload is heavy and IP address management is difficult.	Networks that impose special management requirements on a few APs

Address Assignment Mode	Description	Characteristics	Application Scenario
Uniform assignment	AP IP addresses are assigned uniformly, which is the same as that for wireless users.	● Network configuration is simple. ● AP IP addresses and IP addresses of wireless users cannot be managed separately.	Networks that do not impose any requirements on AP IP address management

- IP addresses of STAs

  Dynamic IP address assignment through DHCP is recommended for mobile users.

  Static IP addresses can be configured for STAs that seldom move, for example, wireless printers.

10.4 ARP

Proxy ARP Is Not Recommended When the AC Serves as the Gateway

The proxy ARP function increases the burden on the gateway, reducing the number of wireless users supported by the AC. It is recommended that the proxy ARP function be disabled when the AC serves as the gateway, unless otherwise required.

When the AC Functions as a Gateway, You Are Advised to Disable a Device from Responding to TC BPDUs and Configure the MAC Address-Triggered ARP Entry Update Function (Native AC Scenario)

When Spanning Tree Protocol (STP) detects network topology changes, the device sends TC BPDUs to instruct the ARP module to age or delete ARP entries. The device then needs to relearn ARP entries. If the network topology changes frequently or there are many ARP entries on the network, ARP entry relearning will cause excess ARP packets to be generated. As a result, a large number of system resources are occupied and services are affected. To address this issue, run the **arp topology-change disable** command to disable the device from responding to TC BPDUs. The device does not age or delete ARP entries even if the network topology changes.

After the device is disabled from responding to TC BPDUs, it does not age or delete ARP entries when the network topology changes. If the MAC address-triggered ARP entry update function is disabled, user services may be interrupted because the device does not update the

saved ARP entries in real time. In this case, you are advised to run the **mac-address update arp** command to enable the MAC address-triggered ARP entry update function.

```
<AC> system-view
[AC] arp topology-change disable
[AC] mac-address update arp
```

You Are Advised to Enable the Optimized ARP Reply Function on an LPU (Native AC Scenario)

When a device functions as an access gateway, it receives a large number of ARP request packets requesting the MAC address of the local interface. In this case, you can enable the optimized ARP reply function. After this function is enabled, the LPU directly returns ARP Reply packets if the ARP Request packets are destined for the local interface. This function helps the device defend against ARP flood attacks. The optimized ARP reply function is applicable especially when the switch is configured with multiple LPUs. By default, the optimized ARP reply function is enabled on a switch.

```
<AC> system-view
[AC] undo arp optimized-reply disable
```

10.5 DHCP

When an AC Functions as a Gateway, It Is Not Recommended to Deploy the AC as the DHCP Server

Wireless users roam, causing DHCP lease renewal (a short lease). This poses high requirements for the performance of the DHCP server. When the AC serves as a DHCP server, AC system performance is consumed, reducing the number of wireless users supported by the AC. Therefore, it is not recommended that the AC serve as both the gateway and DHCP server, unless otherwise required.

Configuring a Proper Lease for User Addresses

In high-density scenarios, you are advised to plan a short-term lease to ensure that IP addresses are released quickly after the clients go offline.

- Based on an interface:
  ```
  [AC-Vlanif10] dhcp server lease day 0 hour 2
  ```
- Based on a global IP address pool:
  ```
  [AC-ip-pool-1] lease day 0 hour 2
  ```

Keeping IP Address Pool Resources Consistent with the Network Capacity Planning

Ensure that the addresses in the IP address pool are sufficient so that all users can access the network after the network is provisioned.

Preventing Address Conflict by Configuring the Management Addresses of APs in Different Network Segments from User Addresses

The management addresses of APs should be configured in different network segments from user addresses to prevent address conflict. Similarly, it is recommended that management VLANs of APs be separated from user service VLANs.

If the AC and AP are in different network segments, you need to configure the Option 43 field on the DHCP server.

If an AP and an AC are located in different network segments, the AP cannot discover the AC through broadcast after it obtains an IP address from the DHCP server. To address this problem, you can configure Option 43 on the DHCP server to advertise the AC's IP address to the AP. You can choose either of the following methods:

1. Run the **option 43 hex 031D3231312E3133372E3139342E35302C3231312E3133372E3139342E3534** command to configure the device to specify AC IP addresses 211.137.194.50 and 211.137.194.54 for APs. **03** is a fixed value, **1D** indicates that the length of the IP address (including the dot (.)) is 29, **3231312E3133372E3139342E3530** indicates the ASCII code of the IP address 211.137.194.50, **2C** indicates the ASCII code of the comma (,), and **3231312E3133372E3139342E3534** indicates the ASCII code of the IP address 211.137.194.54.
2. Run the **option 43 sub-option 1 hex C0A80001C0A80002** command to configure the device to specify AC IP addresses 192.168.0.1 and 192.168.0.2 for APs. In the command, **C0A80001** indicates the hexadecimal format of 192.168.0.1, and **C0A80002** indicates the hexadecimal format of 192.168.0.2.
3. Run the **option 43 sub-option 2 ip-address 192.168.0.1 192.168.0.2** command to configure the device to specify AC IP addresses 192.168.0.1 and 192.168.0.2 for APs.
4. Run the **option 43 sub-option 3 ascii 192.168.0.1,192.168.0.2** command to configure the device to specify AC IP addresses 192.168.0.1 and 192.168.0.2 for APs.

NOTE

If you need to configure multiple IP addresses when the option is specified as an ASCII character string, use commas (,) to separate the IP addresses.

Configure the AC IP address for APs as 10.23.100.1.

```
[AC] dhcp enable
[AC] ip pool huawei
[AC-ip-pool-huawei] network 10.23.10.0 mask 24
[AC-ip-pool-huawei] gateway-list 10.23.10.1
[AC-ip-pool-huawei] option 43 sub-option 3 ascii 10.23.100.1
```

10.6 LLDP

You Are Advised to Enable LLDP

To view the Layer 2 link status between network devices and analyze the network topology, enable Link Layer Discovery Protocol (LLDP). You are advised to enable LLDP on the AC.

Enable LLDP globally.

```
<AC> system-view
[AC] lldp enable
```

To view the Layer 2 link status between APs and access switches on the AC and analyze the network topology, enable WLAN LLDP.

WLAN LLDP can be enabled in the system view and the AP wired port link profile view. The AP sends or receives LLDP packets only when the two switches are enabled. By default, the two switches are enabled.

Enable LLDP in the WLAN view and AP wired port profile **P1**.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] ap lldp enable
[AC-wlan-view] port-link-profile name P1
[AC-wlan-port-link-prof-P1] lldp enable
```

NOTE

This function is not recommended in the native AC solution. If there are a large number of APs, the load on the device is affected, causing a high CPU usage.

You Are Advised to Enable LLDP on the Access Switch's PoE Interface Connected to APs

After LLDP is configured, the device can analyze powered devices (PDs). When LLDP is disabled, the device can detect and classify PDs only by analyzing the current and resistance between the device and PDs. Compared with current and resistance analysis, the LLDP function provides a more comprehensive and accurate analysis.

Enable LLDP globally. After the function is enabled in the system view, all interfaces are enabled with LLDP by default.

```
<HUAWEI> system-view
[HUAWEI] lldp enable
```

10.7 STP

You Are Advised to Configure Interfaces Connecting to APs as STP Edge Interfaces

STP is enabled by default to enhance network stability and prevent network loops caused by incorrect connections. When an STP interface is connected to a device that does not support STP, the STP interface is blocked for 30 seconds. It is recommended that interfaces on access switches supporting STP be configured as STP edge interfaces so that APs can quickly access the network.

```
<HUAWEI> system-view
[HUAWEI] interface gigabitethernet 1/0/1
[HUAWEI-GigabitEthernet1/0/1] stp edged-port enable
```

You Are Advised to Enable STP TC Protection (Native AC Scenario)

When the STP topology changes, Topology Change (TC) BPDUs are sent to instruct other devices to update the forwarding table. If network flapping occurs, a large number of TC packets are received within a short period of time. If MAC address entries and ARP entries are updated frequently, the switch is heavily burdened, causing potential risks to the network.

After TC protection is enabled, if the number of TC BPDUs received by a switch exceeds the specified threshold within a given period, the switch handles only the specified number of TC BPDUs. After the specified number of times is reached, the switch processes excess TC BPDUs at one time only. In this way, the switch does not need to frequently delete MAC entries and ARP entries. By default, the TC protection function is enabled.

Enable the trap function for TC protection.

```
<AC> system-view
[AC] stp tc-protection
```

10.8 VRRP

The Virtual Router Redundancy Protocol (VRRP) groups multiple routing devices into a virtual router and sets the next hop routing address of the host as the IP address of the virtual router. When the next-hop gateway connecting to the host fails, VRRP selects another gateway to transmit service traffic, ensuring reliable communication.

VRRP is a Layer 2 protocol and can be deployed only on Layer 2 networks.

- **Setting the recovery delay of the VRRP group**

When an interface or a BFD session associated with a VRRP group alternates between Up and Down states, the VRRP group status may flap, causing user traffic loss. To solve this problem, set a delay before a VRRP group recovers.

Set the recovery delay of the VRRP group to 60s.

```
<AC> system-view
[AC] vrrp recover-delay 60
```

- **Configuring preemption delay for the wireless controller in a VRRP group**

On an unstable network, even if the master is working properly, the backup may not receive packets from the master because of network congestion. In this case, the VRRP group status flaps, causing traffic loss.

You are advised to set the preemption delay of the backup in a VRRP group to 0, configure the master in preemption mode, and set the preemption delay to be longer than 1800s.

Set the preemption delay of backup group 1 to 1800s.

```
<AC> system-view
[AC] interface vlanif 100
[AC-Vlanif100] vrrp vrid 1 preempt-mode timer delay 1800
```

10.9 Radio Frequency

You Are Advised to Enable Airtime Fair Scheduling

The indoor high-density scenarios in universities are densely populated and the types of terminals are various. On a WLAN, the physical layer rates of users have great differences due to different radio modes supported by the terminals or radio environment where the terminals reside. If the users with lower physical layer rates occupy wireless channels for a long period, user experience of the entire WLAN is affected.

You are advised to enable airtime fair scheduling, which computes wireless channel occupation time of users in the same VAP and preferentially schedules users who occupy the channel for a relatively short time. In this way, each user is assigned equal time to occupy the channel, ensuring fairness in channel usage and guaranteeing user experience.

Enable airtime fair scheduling in the RRM profile **default**.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] rrm-profile name default
[AC-wlan-rrm-prof-default] airtime-fair-schedule enable
```

Enabling Short Interframe Space

In indoor high-density scenarios in universities, it is recommended that the short interframe space (SIFS) be enabled to improve the transmission rate of 802.11n and 802.11ac packets.

Set the GI mode to short.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] radio-2g-profile name default
[AC-wlan-radio-2g-prof-default] guard-interval-mode short
```

Configuring the RTS-CTS Operation Mode in the Radio Profile

The Request To Send/Clear To Send (RTS/CTS) handshake mechanism prevents data transmission failures caused by channel conflicts. If STAs perform RTS/CTS handshakes before sending data, RTS frames consume high channel bandwidth. In high-density indoor scenarios in universities, the RTS-CTS mode is recommended.

Set the RTS-CTS operation mode to rts-cts in the radio profile.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] radio-2g-profile name default
[AC-wlan-radio-2g-prof-default] rts-cts-mode rts-cts
[AC-wlan-radio-2g-prof-default] rts-cts-threshold 1400
[AC-wlan-radio-2g-prof-default] quit
[AC-wlan-view] radio-5g-profile name default
[AC-wlan-radio-5g-prof-default] rts-cts-mode rts-cts
[AC-wlan-radio-5g-prof-default] rts-cts-threshold 1400
[AC-wlan-radio-5g-prof-default] quit
```

You Are Advised to Configure APs to Disconnect Weak-Signal STAs

If the uplink signal strength of a STA received by an AP is weak, it indicates that the STA is far away from the AP. If the STA continues to access the AP with weak signals, retransmission is serious and air interface resources are wasted. To prevent the STA from affecting the throughput of the AP, it is recommended that the AP disconnect the STA so that the STA can reassociate with another AP with strong signal strength.

NOTE

If the threshold is set to a too large value, users may be disconnected easily. You can adjust the threshold as required.

```
[AC-wlan-view] rrm-profile name default
[AC-wlan-rrm-prof-default] smart-roam enable
[AC-wlan-rrm-prof-default] smart-roam roam-threshold check-snr
[AC-wlan-rrm-prof-default] smart-roam quick-kickoff-threshold snr 20
```

Configuring the Interval at Which an AP Sends Beacon Frames

An AP broadcasts Beacon frames at intervals to notify STAs of an existing 802.11 network. A long interval for sending Beacon frames lengthens the dormancy time of STAs, while a short interval for sending Beacon frames increases air interface costs. Therefore, you are advised to set the interval for sending Beacon frames for an AP based on the VAP quantity.

The following intervals for sending Beacon frames are recommended for APs with different VAP quantities on a single radio:

- No more than 4 VAPs: about 100 TUs

- 5 to 8 VAPs: about 200 TUs
- 9 to 12 VAPs: about 300 TUs
- 13 to 16 VAPs: about 400 TUs

Set the interval for sending Beacon frames to 200 TUs in the 2G radio profile **default**.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] radio-2g-profile name default
[AC-wlan-radio-2g-prof-default] beacon-interval 200
```

You Are Advised to Enable Dynamic EDCA Parameter Adjustment

A WLAN has only three non-overlapping channels on the 2.4 GHz frequency band. When APs are deployed densely in high-density indoor scenarios in universities, multiple APs have to work in the same channel, resulting in co-channel interference. This interference degrades network performance.

The dynamic EDCA parameter adjustment function automatically detects the number of users, and allows APs to adjust EDCA parameters flexibly to reduce the possibility of collision, improve the throughput, and enhance user experience.

Enable dynamic EDCA parameter adjustment.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] rrm-profile name huawei
[AC-wlan-rrm-prof-huawei] dynamic-edca enable
```

Properly Deploying Radio Calibration

On a WLAN, operating status of APs is affected by the radio environment. In this case, you can configure radio calibration. The radio calibration function can dynamically adjust channels and power of APs managed by the same AC to ensure that the APs work at the optimal performance. Frequent radio calibration, however, degrades AC performance.

In high-density indoor scenarios in universities, radio signals are concentrated, which may easily cause signal overlapping and interference. This frequently triggers radio calibration. Therefore, it is recommended that automatic radio calibration be disabled and manual or scheduled radio calibration mode be used.

Set the radio calibration mode to manual.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] calibrate enable manual
```

Configure a radio calibration policy and set the time for scheduled radio calibration to 03:00:00.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] calibrate enable schedule time 03:00:00
[AC-wlan-view] calibrate policy rogue-ap
[AC-wlan-view] calibrate policy non-wifi
[AC-wlan-view] regulatory-domain-profile name default
[AC-wlan-regulatory-domain-prof-default] dca-channel 2.4g channel-set 1,6,11
```

Properly Deploying Band Steering

Compared with the 2.4 GHz frequency band, the 5 GHz frequency band has less interference and more available channels, and provides higher access capability. Especially in indoor high-

density scenarios in universities, APs are deployed in a centralized manner, and interference of the 2.4 GHz frequency band is severe. You are advised to enable band steering to associate STAs with the 5 GHz frequency band.

Enable the band steering function, which is enabled by default.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] vap-profile name huawei
[AC-wlan-vap-prof-huawei] undo band-steer disable
```

Properly Deploying the AP Load Balancing Function

Load balancing distributes users to APs in a group based on the number of users and traffic volume. In static load balancing mode, APs providing the same services are manually added to a load balancing group. When a STA needs to access a WLAN, it sends an Association Request packet to an AC through an AP. The AC determines whether to permit access from the STA according to a load balancing algorithm. In dynamic load balancing mode, a STA sends broadcast a Probe Request frames to scan available APs. The APs that receive the Probe Request frames all report the STA information to the AC. The AC adds these APs to a load balancing group, and then uses a load balancing algorithm to determine whether to allow access from the STA.

Load balancing distributes users evenly to APs in the same load balancing group, improving system capacity and user experience. To maximize the benefits of load balancing, you are advised to apply this function to scenarios where the following conditions are met:

(1) High-density scenarios where there is a high degree of overlap between APs' coverage ranges. To meet high-density access requirements, the distance between APs is small. In this scenario, a STA usually receives signals from multiple APs with good signal quality. After load balancing between APs is enabled, the STA can connect to an AP with strong signal strength.

(2) Scenarios where the number of APs in a static load balancing group is not too large. The farther a STA is away from an AP, the weaker signal strength the STA receives from the AP. If there are too many APs in a load balancing group, a STA may access an AP with poor signal strength, which does not help improve user experience.

(3) When setting a static load balancing group, you can perform a site survey to determine which APs should be placed in the same group. This prevents two APs, physically close to each other but actually blocked by obstacles, from being added to the same load balancing group. In this case, the two APs cannot work in load balancing mode.

Configure static load balancing.

a. Create a static load balancing group and add APs area_1 and area_2 to the group.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] sta-load-balance static-group name wlan-static
[AC-wlan-sta-lb-static-wlan-static] member ap-name area_1
[AC-wlan-sta-lb-static-wlan-static] member ap-name area_2
```

b. Configure the static load balancing mode and relevant parameters.

Configure static load balancing based on user quantity.

```
[AC-wlan-sta-lb-static-wlan-static] mode sta-number
```

Set the start threshold for static load balancing based on the number of users to 20 and load difference threshold to 25%.

```
[AC-wlan-sta-lb-static-wlan-static] sta-number start-threshold 20
[AC-wlan-sta-lb-static-wlan-static] sta-number gap-threshold 25
[AC-wlan-sta-lb-static-wlan-static] quit
```

Configure dynamic load balancing.

Create the RRM profile **wlan-net**, enable dynamic load balancing in this profile, and set the start threshold for dynamic load balancing to 20 and load difference threshold to 25%.

```
[AC-wlan-sta-lb-static-wlan-static] sta-number start-threshold 20
[AC-wlan-sta-lb-static-wlan-static] sta-number gap-threshold 25
[AC-wlan-sta-lb-static-wlan-static] quit
```

Pay attention to the following points:

(1) After the STA dynamic load balancing function is enabled, APs in a load balancing group send Probe Request packets to an AC after receiving the packets. The AC determines the AP to which a STA is connected. If this function is enabled, however, the AC performance deteriorates.

(2) Load balancing increases the access delay for STAs and affects user experience. Especially in scenarios where delay-sensitive services exist on the network, you are advised to enable this function with caution.

You Are Not Advised to Enable Spectrum Analysis

The spectrum analysis function has a certain impact on the AC performance. Therefore, you are not advised to enable this function. This function is disabled by default.

10.10 STA

You Are Not Advised to Enable the Logging Function

After the function of recording successful STA associations in the log is enabled, successfully associated STAs are recorded in the log, so that the administrator can view information about successful STA associations. However, logging affects AC performance, especially in indoor high-density scenarios. Therefore, you are not advised to enable this function. This function is disabled by default.

Disable the function of recording successful STA associations in the log.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] undo report-sta-assoc enable
```

You Are Not Advised to Enable the Function of Reporting STA Traffic Statistics and Online Duration on APs

You can enable an AC to report information about STA traffic statistics and online duration on APs to the eSight. After the function is enabled, the AC collects and reports the information to the eSight when STAs go offline or roam within the AC, which facilitates data query on the eSight.

It is not recommended that this function be enabled regardless of whether eSight is deployed on the network. It is because that frequent reporting of information affects AC performance, especially in scenarios with a large number of users. This function is disabled by default.

Disable an AC to report information about STA traffic statistics and online duration on APs.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] undo report-sta-info enable
```

You Are Not Advised to Enable the STA Location Function

The STA location function affects AC performance. Therefore, you are not advised to enable this function at sites that do not require STA location. This function is disabled by default.

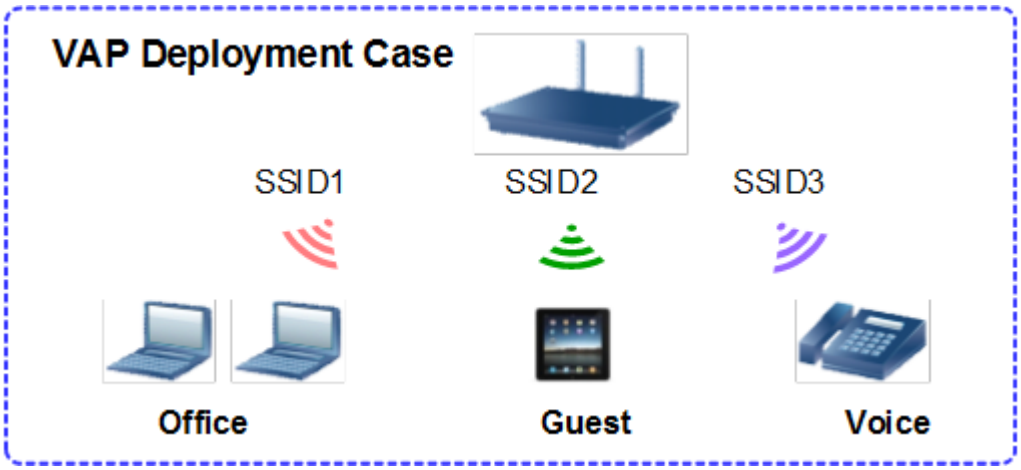
10.11 SSID

Service VLANs identify services and users. On WLANs, SSIDs have the same function as service VLANs. Therefore, you must determine the mapping between VLANs and SSIDs. The number of service VLANs and number of SSIDs should be in the ratio of 1:1, 1:N, N:1, or N:N based on service requirements.

NOTE

The range of a radio broadcast domain is determined by an SSID. Therefore, if the number of SSIDs and number of service VLANs are in the ratio of 1:N or N:N, you are advised to enable broadcast-to-unicast conversion to avoid the generation of a radio broadcast domain.

It is recommended that SSIDs are assigned based on service types. As shown in the following figure, there are three SSIDs for different wireless services: SSID1 for wireless office, SSID2 for guest areas, and SSID3 for voice services.



In actual deployment, it is recommended that the number of SSIDs configured on an AC be limited. Although each AP can be configured with a maximum of 16 SSIDs, excessive SSIDs occupy AC system resources. Therefore, you are advised to create as few SSIDs as possible.

10.12 User Roaming

WLAN roaming allows a STA to move from the coverage area of an AP to that of another AP with nonstop service transmission.

It can address the following problems:

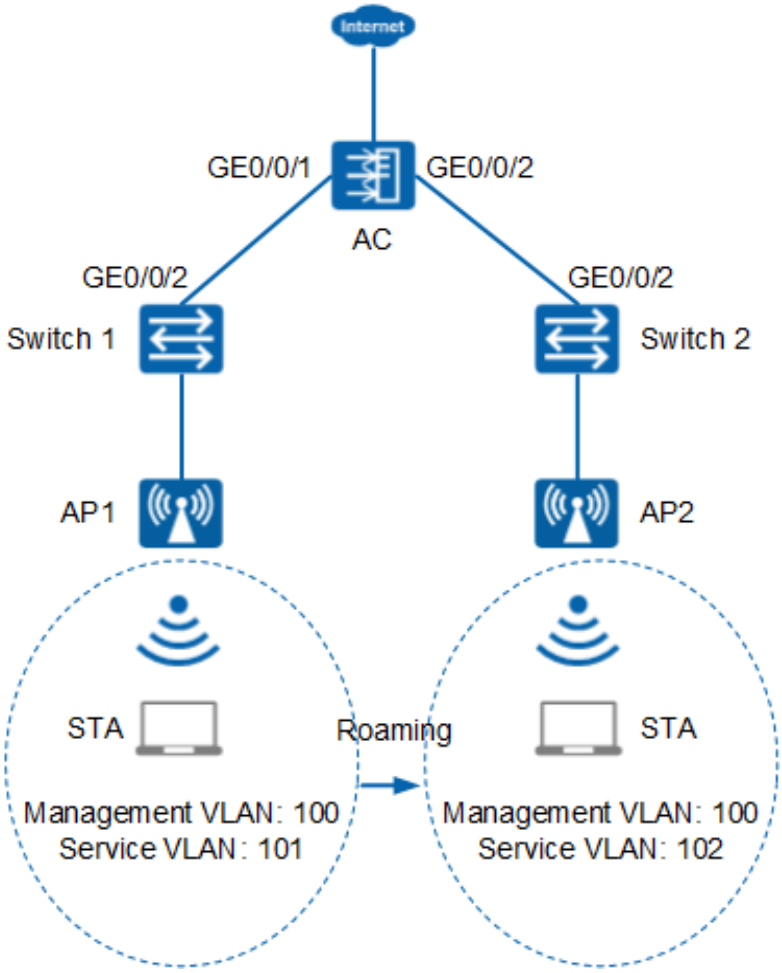
- Retains the STA's IP address. After roaming, the STA can still access the initially associated network and retains its services.

- Prevents packet loss or service interruption caused by long-term authentication.

Wireless user roaming is classified into the following types based on the STA roaming range:

- Intra-AC roaming

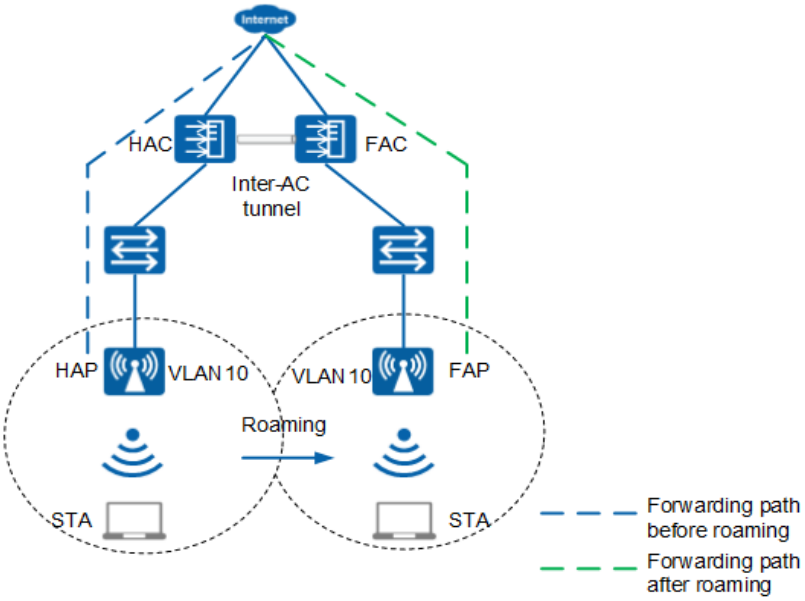
  The STAs before and after roaming belong to the same AC. This mode applies to the scenario where only one AC needs to be deployed on the network.



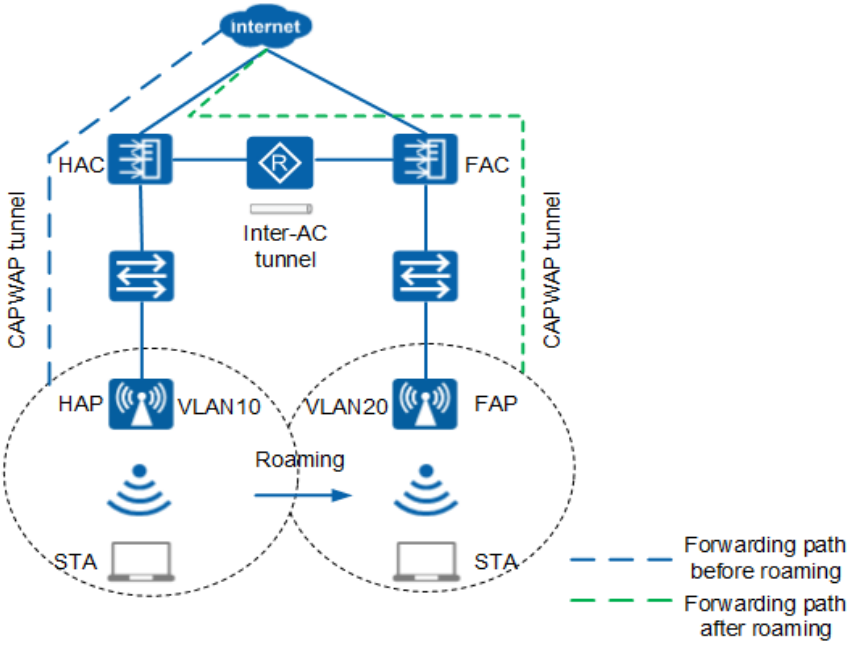
- Inter-AC roaming

  Inter-AC roaming can be classified into Layer 2 roaming and Layer 3 roaming.

  - Layer 2 roaming: STAs before and after roaming belong to different ACs but they have the same service VLAN and roaming domain. During Layer 2 roaming, the STA stays within the same subnet. The FAP/FAC processes packets of a Layer 2 roaming STA in the same way as it processes packets of a newly online STA. The FAP/FAC forwards the packets on the local network but does not send the packets back to the HAP/HAC over the inter-AC tunnel.

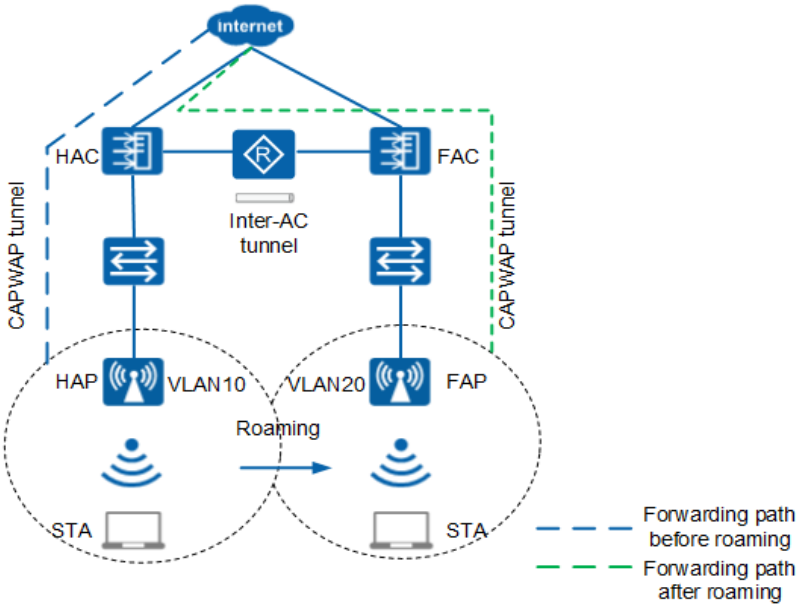


- Layer 3 roaming: Based on data forwarding modes, Layer 3 roaming is classified into centralized forwarding and local forwarding.
  - Centralized forwarding: STAs before and after roaming belong to different ACs and they have different service VLANs and roaming domains. In centralized forwarding mode, service packets exchanged between the HAP and HAC are encapsulated through a CAPWAP tunnel, and the HAP and HAC can be considered in the same subnet. Instead of forwarding the packets back to the HAP, the HAC directly forwards the packets to the upper-layer network.



    - Local forwarding: STAs before and after roaming belong to different ACs and they have different service VLANs and roaming domains. In local forwarding mode, service packets exchanged between the HAP and HAC are not encapsulated through the CAPWAP tunnel; therefore, whether the HAP and HAC reside in the same subnet is unknown. Packets are forwarded back to the HAP by default. If the HAP and HAC are located

in the same subnet, configure the HAC with higher performance as the home agent. This reduces the load on the HAP and improves the forwarding efficiency.



You Are Advised to Enable Smart Roaming

On a WLAN, when a STA is farther from an AP, the access rate of the STA becomes lower but the STA still associates with the AP without reinitiating a connection with the AP or roaming to another AP. This degrades user experience. When detecting that the signal-to-noise ratio (SNR) or access rate of a STA is lower than the specified threshold, the AP sends a Disassociation packet to the STA so that the STA can reconnect or roam to another AP.

Smart roaming is recommended for indoor high-density scenarios in universities, such as large lecture halls and multi-function reporting halls.

Enable smart roaming.

```
<AC> system-view
[AC] wlan
[AC-wlan-view] rrm-profile name huawei
[AC-wlan-rrm-prof-huawei] smart-roam enable
```

Set the trigger mode of smart roaming to check-snr and the threshold to 25.

```
[AC-wlan-view] smart-roam roam-threshold check-snr
[AC-wlan-rrm-prof-huawei] smart-roam roam-threshold snr 25
```

Set the smart roaming trigger mode for quickly disconnecting STAs to check-snr and the threshold to 20.

```
[AC-wlan-rrm-prof-huawei] smart-roam quick-kickoff-threshold snr 20
```

You Are Not Advised to Enable 802.11r

The 802.11r protocol is a standard defined by IEEE for fast roaming. Before a client is associated with the target AP, 802.11r completes the initial authentication handshake, which reduces the number of information exchanges and reduces the service data flow delay during roaming. Users are unaware of service interruption, improving user experience. The 802.11r

fast roaming function has the following limitations. Therefore, you are advised not to enable this function.

(1) The 802.11r fast roaming and Protected Management Frame (PMF) functions are mutually exclusive. If the 802.11r fast roaming function has been configured, the PMF function cannot be configured.

(2) When the 802.11r uses 802.1X authentication, the lab test shows that Wi-Fi terminals in the market have many defects in supporting the 802.11r protocol, which may cause compatibility problems, such as device disconnection and failure to go online.

To obtain the STA compatibility test report, visit the following website: **http://enterprise.huawei.com/topic/wlan-Interworking-cn/index.html**

11 Appendix-Recommended Version Mapping

The following table lists the recommended product versions involved in the Agile Campus Network Solution.

Table 11-1 Recommended versions of the native AC solution

Product Name	Recommended Version
S series switch	V200R011C10SPC600
AP	V200R007C20
Agile Controller-Campus	V100R003C30
USG series firewall	V500R001C60
eSight	V300R008C00

Table 11-2 Recommended versions of the independent AC solution

Product Name	Recommended Version
S series switch	V200R010C00SPC600
AC/AP	V200R007C20
Agile Controller-Campus	V100R002C10
USG series firewall	V500R001C30
eSight	V300R007C00

12 Appendix-Recommended Product Models

Table 12-1 lists the recommended product models involved in the Agile Campus Network Solution.

Table 12-1 Recommended product models

Location on a Network	Device Type	Recommended Device Model	Description
Egress area/DMZ	Router	NE40E series	Medium- and large-sized campuses
		NE20E-S series	Small- and medium-sized campuses
		NE16EX series	Small- and medium-sized campuses
		AR3200/2200/1200 series	● Small- and medium-sized campuses ● Campus that supports voice services
		AR150/160/200 series	Small campus
		AR530 series industrial switching router	Industrial park
	Security device	USG6300/6500/6600/9500 series	Firewall
		AntiDDoS1000/8000 series	AntiDDoS

Location on a Network	Device Type	Recommended Device Model	Description
		NIP6000 series	IPS/IDS
		WAF5000 series	Web application firewall
Core layer	Switch	S12700/S9700/ S7700/S6700 series	Ultra-large campus and medium- and large-sized campuses
		CE12800 series	Ultra-large campus and large campus
	AC	ACU2	Medium- and large-sized campuses
		AC6605	Medium- and large-sized campuses
		AC6005	Small- and medium-sized campuses
Aggregation layer	Switch	S9700/S7700/ S6700/S5700 series	NA
Access layer	Switch	S6700/S5700/ S3700/S2700 series	NA
	AP	AP2010DN/ AP2030DN/ AP2050DN/ AP4030DN/ AP4050DN/ AP4050DN-E/ AP5030DN/ AP6050DN/ AP4030TN/ AP7050DE/ AP7050DN-E/ AP7030DE	Indoor settled AP
		AD9430DN/ AD9431DN+ R230D/R240D/ R250D	Indoor agile distributed AP
		AP8030DN/ AP8050DN/ AP8130DN/ AP8150DN/ AP6510DN-AGN/ AP6610DN-AGN	Outdoor AP

For details about recommended AP and antenna models in different scenarios, see the following documents:

- **WLAN Planning Quick Start**
- **AP Antenna Quick Start**

13 Appendix-Product Overview

13.1 Agile Controller-Campus

The Agile Controller-Campus is Huawei's next-generation controller for campus and branch networks. Leveraging innovative solutions such as automatic network deployment, automatic policy delivery, and SD-WAN, the Agile Controller-Campus reduces operating expense (OPEX) and O&M costs of enterprises, accelerates service cloudification and digital transformation, and makes network management more agile and network O&M more intelligent.

For details about the Agile Controller-Campus, refer to the following link: **http://support.huawei.com/enterprise/zh/sdn-controller/agile-controller-campus-pid-21085964**

13.2 eSight

eSight is a next-generation network management system (NMS) designed for enterprise agile campus networks and enterprise branch networks. It uniformly manages and intelligently associates enterprise resources, services, and users.

eSight supports centralized management of enterprise basic networks, unified management of Huawei network devices, WLAN monitoring and configuration management, as well as network quality monitoring and analysis through Packet Conservation Algorithm for Internet (iPCA), service level agreement (SLA), and network traffic analyzer (NTA). eSight also

provides a flexible and open platform and enables enterprises to establish their own intelligent management system.

For details about eSight, refer to the following link: **http://support.huawei.com/enterprise/zh/network-management/esight-network-pid-6725036/doc**

13.3 S Series Switch

The S series switches are Huawei next-generation smart core, aggregation, and access switches for campus networks, allowing for flexible networking. The following describes several mainstream product series.

The S12700 series switches are agile core switches designed for next-generation campus networks and data center networks. Using a fully programmable architecture, the S12700 series switches allow flexible and fast customization and support smooth evolution to software-defined networking (SDN). The S12700 series switches use Huawei's innovative Ethernet network processor (ENP) chip and provide the native AC function to help build a wired and wireless converged network. It supports Packet Conservation Algorithm for Internet (iPCA) to perform hop-by-hop monitoring of any service flow, helping customers manage services in a more refined way. Based on Huawei's Versatile Routing Platform (VRP), the S12700 provides high-performance Layer 2/Layer 3 switching services and integrates diversified network services such as MPLS VPN, hardware IPv6, desktop cloud, and video conferencing. The S12700 also provides various reliability technologies including in-service software upgrade, non-stop forwarding, CSS2 switch fabric hardware clustering, 1+N MPU backup, hardware Ethernet OAM/BFD, and ring network protection. These technologies improve customers' network efficiency and maximize the network operation time, reducing customers' total cost of ownership (TCO).

The S9700 series switches are high-end intelligent terabit core routing switches designed as core switches for campus networks and aggregation switches for data centers. The S9700 uses Clos multi-level switching architecture that allows for high bandwidth scalability and complies with the 40GE and 100GE Ethernet standards. An S9700 can be upgraded to an agile switch when it is equipped with X series cards, the line cards with Huawei's first ENP. Agile switches allow customers to make innovations on their networks.

The S7700 series switches are high-end intelligent routing switches designed as aggregation switches for large enterprise networks, aggregation switches for data center networks, and core switches for campus networks of small- and medium-sized enterprises. Based on intelligent multistage switching technology, the S7700 switches can function as aggregation or core switches in a campus network or data center network to provide integrated wireless access, voice, video, and data services, helping enterprises build an integrated end-to-end network. The S7700 running V200R005C00 or a later version can be upgraded to an agile switch using an agile card, which is equipped with the ENP of Huawei. Customers can enjoy the innovative experience brought by the agile switch.

The S6700 is a fixed switch with the highest performance in the industry. It provides up to 24 or 48 line-speed 10GE interfaces, a wide variety of services, comprehensive security policies, and rich QoS features. The S6700 can function as an access switch for servers on a data center network or a core switch on a campus network. Various product models are offered, such as S6720-HI series agile 10GE switches, S6720-EI series enhanced 10GE switches, S6720-SI series multi-rate 10GE switches, and S6720-LI series simplified 10GE switches.

The S5700 series Ethernet switches are next-generation energy-saving gigabit high-performance Ethernet switches designed to meet the demand for high-bandwidth access and Ethernet multi-service aggregation. The S5700 provides a large switching capacity, high

reliability, and high-density GE interfaces to accommodate 10 Gbit/s uplink transmissions. It also supports Energy Efficient Ethernet (EEE) and iStack. The S5700 can be used in extensive enterprise network scenarios. For example, it can function as an access or aggregation switch on a campus network, a gigabit access switch in an Internet data center (IDC), or a desktop switch to provide 1000 Mbit/s access for terminals. The S5700 is available in a simplified (LI) series, a standard (SI) series, an enhanced (EI) series, and an advanced (HI) series.

The S3700 series switches are Ethernet switches that provide both access, aggregation, and transmission functions, meeting the enterprise networks' requirements for reliable multi-service access and high-quality transmission. In aggregation and access scenarios on enterprise campus networks, the switches provide simple installation and maintenance methods, flexible VLAN deployment, PoE capability, comprehensive routing functions, and capability to migrate to an IPv6 network.

The S2700 series enterprise switches are next-generation energy-saving intelligent 100M access Ethernet switches. They are easy to install and maintain, and are designed with flexible network deployment capabilities, comprehensive security and QoS control policies, and energy-saving technologies.

The S1700 series enterprise switches are next-generation energy-saving Ethernet access switches. They provide a rich array of features to help customers build secure, reliable high-performance networks. The S1700 is easy to install and maintain and is suitable for use by small- and medium-sized enterprises, Internet cafes, hotels, and schools.

For details about S series switches, refer to the following link: **http://support.huawei.com/onlinetoolsweb/ptmngsys/Web/Switch/Switch_Information_Service_Portal.html**

13.4 CE12800 Series Switch

The CE12800 series switches are next-generation high-performance core switches provided by Huawei for data center networks and high-end campus networks. Using the next-generation Huawei operating platform VRP8, the switches provide stable, reliable, secure, and high-performance Layer 2/Layer 3 switching services, helping to build a scalable, virtualized, and high-quality network. The CE12800 series switches use an industry-leading Clos architecture and a strict front-to-back airflow design to provide industrial-grade reliability. The switches also provide comprehensive virtualization capabilities and abundant data center service features. In addition, the CE12800, as a next-generation core switch, uses multiple innovative energy conservation technologies to greatly reduce power consumption.

For details about CE series switches, refer to the following link: **http://support.huawei.com/onlinetoolsweb/ptmngsys/Web/DC/DC_Information_Service_Portal.html**

13.5 WLAN

Huawei provides a full series of WLAN products that are compatible with 802.11a/b/g/n/ac standards to establish high-speed, secure, and reliable wireless network connections in indoor and outdoor application scenarios.

The Access Controller (AC) provides a large switching capacity and high performance. It is highly reliable, easy to install and maintain, and features such advantages as flexible networking and energy conservation. The mainstream product models include:

- The AC6605 is a wireless access controller that provides wired and wireless access services. It can provide wireless coverage in large or medium-sized enterprises and their branch campus networks or office networks.
- The AC6005 access controllers (ACs) are small wireless ACs designed for small- and medium-sized enterprises (SMEs). The AC6005 is mainly used on enterprise office networks and campus networks of SMEs and branches.
- Huawei Access Controller Unit 2 (ACU2) is a value-added service unit used on a modular switch and provides access control capabilities on WLANs of large enterprises. A WLAN can be built rapidly by adding ACU2s to wired network switches. This enriches switch service functions, integrates multiple services, and reduces the Total Cost of Ownership (TCO).
- Embedded with Huawei's first Ethernet ENP, the native AC cards can function as common LPUs to provide data access and switching services and also as WLAN ACs to provide wireless access control functions. In this way, the cards achieve wired and wireless convergence. The ENP-embedded native AC cards can be installed on the S12700, S9700, and S7700 agile modular switches to allow these switches to provide wireless service functions, lowering network construction costs.

The wireless access points (APs) of rich models can be used in various indoor and outdoor scenarios, comply with the latest 802.11ac Wave 2 standard, and support 4×4 MIMO (four spatial streams). APs include wall plate APs (such as AP2000, AP3000, AP4000, AP5000, AP6000, AP7000, and AP8000) and agile distributed APs (such as AD9431DN, AD9430DN, R250D, and R450D).

For details about WLAN products, refer to the following link: **http://support.huawei.com/onlinetoolsweb/ptmngsys/Web/WLAN/WLAN_Information_Service_Portal.html**

13.6 USG Series Firewall

The firewall is a security gateway product designed for medium- and large-sized campus networks. It integrates multiple security capabilities and logs Internet access in locally, meeting the security compliance requirements. The firewall provides refined application-layer security protection and service acceleration and integrates multiple security features such as NAT, VPN, IPS, virtualization, and service awareness to help enterprises build data center border security protection in the cloud computing era. Mainstream product models include USG6000 and USG9000.

For details about USG series firewalls, refer to the following link: **http://support.huawei.com/onlinetoolsweb/ptmngsys/Web/Security/Security_Information_Service_Portal.html**

13.7 AR Series Router

The AR series enterprise router is an integrated enterprise gateway that integrates the routing, switching, voice, security, and wireless functions. It inherits Huawei's rich experience in data communication, wireless communication, PON access, and switching based on the proprietary Versatile Routing Platform (VRP). It provides wired and wireless Internet access, private line access, private branch exchange (PBX), convergent communication, and security functions. It also provides an open service platform to meet enterprises' requirements for high performance, high reliability, and multi-service convergence.

The AR3200/2200/1200 series routers are widely deployed on medium- and large-sized campus network egresses and headquarters or branches of medium- and large-sized enterprises.

The AR150/160/200 series routers apply to enterprise branches and small enterprises.

The AR530 series industrial switching router is a dedicated industrial gateway for communication in challenging environments such as extreme temperature, high humidity, and electromagnetic interference.

For details about AR series routers, refer to the following link: **http://support.huawei.com/onlinetoolsweb/ptmngsys/Web/AR/AR_Information_Service_Portal.html**

13.8 NE Series Router

NE series routers are high-end core routers that work as backbone network nodes, meeting the requirements of key services for low latency and high reliability.

The NE40E universal service router series is a range of high-end network products developed by Huawei. These routers mainly serve as core nodes on enterprise WANs, access nodes on large enterprise networks, interconnection and aggregation nodes on campus networks, and edge nodes on large IDC networks. The NE40E, NE20E, and NE5000E can work together to provide a complete hierarchical IP network solution.

The NE20E-S series unified service routers are high-end network products developed by Huawei for next-generation enterprise services. They can serve as aggregation nodes on IP backbone networks, core nodes on small- and medium-sized enterprise networks, edge nodes on campus networks, and access nodes on small- and medium-sized campus networks.

The Huawei NE16EX series multi-service routers function as aggregation and access nodes on backbone networks in various industries and egress nodes on large- and medium-sized campus networks. They can also be deployed in the headquarters or branches of large- and medium-sized enterprises. The NE16EX and other NE series routers, including NE5000E, ME60, NE40E, and NE20E, together provide a complete, layered IP network solution.

For details about NE series routers, refer to the following link:

http://support.huawei.com/onlinetoolsweb/ptmngsys/Web/NE/datacom_information_service_portal.html

14 Appendix-Terminology

AC Access Controller

AP Access Point

ASG Application Security Gateway

BFD Bidirectional Forwarding Detection

BGP Border Gateway Protocol

CSS Cluster Switch System

DDoS Distributed Denial of Service

DMZ Demilitarized Zone

IDS Intrusion Detection System

IPS Intrusion Prevention System

iStack Intelligent Stack

LACP Link Aggregation Control Protocol

LAG Link Aggregation Group

MAD Multi-Active Detection

MPLS MultiProtocol Label Switch

MSTP Multiple Spanning Tree Protocol

NAC Network Admission Control

NIP Network Intelligent Prevention

OSPF Open Shortest Path First

PoE Power over Ethernet

QoS Quality of Service

RIP Routing Information Protocol

RSTP Rapid Spanning Tree Protocol

SSL Secure Socket Layer

STP Spanning Tree Protocol

USG Unified Security Gateway

VLAN Virtual Local Area Network

VPN Virtual Private Network

VRRP Virtual Router Redundancy Protocol

WAN Wide Area Network