Huawei CloudCampus WLAN SmartApp (Application Identification and Acceleration)

Technology White Paper

HUAWEI

Executive Summary

With the development and application of wireless communications technologies, more and more users and terminals connect to WLANs. On a WLAN, voice and video services are delay-sensitive services. Once network congestion occurs, voice and video service experiences become poor. This document describes how SmartApp (application identification, voice and video enhancement, and mDNS) on a WLAN ensures user experiences and its major application on the network.

Contents

1 Overview

1.1 Application Identification

1.1.1 Background and Objective

As the network scale increases, network statistics collection and control methods based on only interfaces, IP addresses, or other characteristics of original packets cannot meet network management requirements. A more customer-centered classification control and statistics collection method is required.

To meet the requirements for market competition and provide better solutions, an enterprise requires refined service management, visualized management and control for the services and applications on smart terminals, improved security, and effective bandwidth management and control.

- Application-based traffic statistics collection allows network administrators to easily understand network traffic usage.
- The administrator can enforce policies on the specified applications to limit the bandwidth they can use.
- The administrator can set priorities for the quality-sensitive applications based on the application type so that packets of high-priority applications can preferentially obtain bandwidth resources.

Benefits to the network provider:

- Visualized application statistics collection allows network administrators or operators to better understand network traffic usage.
- Unexpected application traffic can be limited or blocked to increase bandwidth use efficiency.
- Service level of key services can be improved and QoS can be ensured.

Benefits to end users:

- The QoS of key services can be better guaranteed.

1.1.2 Application Identification Technologies

Application visibility on Huawei WLAN network devices identifies traffic of different applications based on the following key technologies:

- Port-based identification
- Signature-based identification
- Association identification
- Behavior analysis-based identification
- Multi-dimensional identification

1.1.3 Policy Control on Identified Applications

A WLAN network transmits traffic of various applications. The network administrator needs to know the traffic usage of applications to plan network capacity and locate problems on the network. WLAN devices need to support the analysis of the forwarded traffic on the device and display the traffic analysis results to users.

After understanding the application traffic usage on a network, the WLAN network administrator needs to control the specified application traffic, including discarding the traffic, setting the priority, or limiting the rate.

1.2 Voice and Video Enhancement

1.2.1 Background

Different from common wireless network data services, Voice over Internet Protocol (VoIP) sessions among voice and video traffic flows are more prone to frame freezing or loss due to the delay, packet loss, and jitter of AP services.

More QoS control variables are available for transmission of voice and video services on WLANs than those on wired networks. If these new variables are not comprehensively or completely handled, WLANs can hardly provide users with satisfactory voice and video service experience.

It is unrealistic to eliminate network congestion by simply increasing bandwidth of WLANs. Improving end-to-end QoS can solve the problem. On one hand, the Wi-Fi Alliance (WFA) provides and defines basic protocols (such as WMM, namely, Wi-Fi Multimedia) to ensure QoS of Wi-Fi networks. On the other hand, simply using WMM cannot deliver good user experiences for high-end customers in diversified application scenarios.

Common WLANs provide equal access bandwidth for all associated Wi-Fi terminals. WMM ensures the same QoS for voice and video services as that for common data services, but provides no optimization for improving voice and video service experience.

1.2.2 QoS Measurement Parameters

Bandwidth/Throughput: Bandwidth typically refers to the frequency range that is occupied by a modulated carrier signal. When used for channel description, bandwidth indicates the maximum frequency range that signals can effectively pass a channel, in Mbit/s.

Delay: indicates the duration for transmitting a packet from one end to another on a network. For example, the delay of voice services is the time for transmitting voice from a talker to a listener. A long delay causes unclear voice or interruption.

Jitter: also called delay variation, indicates the delay variances between different packets in the same service flow. Jitter is caused by differences in the queuing time of contiguous packets in a service flow. Jitter has the most significant impact on QoS. For some types of services, especially real-time services such as voice and video services, jitter cannot be tolerated. If packets reach the destination at different time, voice and video services are interrupted.

Packet loss rate: indicates the percentage of lost and error packets to the total number of transmitted packets within a sample period (1 second typically) during transmission. The packet length is an important factor that affects the packet loss rate. A small number of lost packets do not have much impact on services. If a large number of packets are lost, service transmission efficiency is compromised.

Voice and video services have different requirements on the network bandwidth, delay, jitter, and packet loss rate, as listed in the following table.

Service Type		Delay	Jitter	Packet Loss Rate
Voice	Media	≤ 50 ms	≤ 10 ms	≤ 1%
	Signaling	≤ 100 ms	≤ 10 ms	≤ 0.1%
Interactive personality TV (IPTV)	Multicast	≤ 1s	≤ 200 ms	≤ 0.1%
	Video On Demand (VoD)	≤ 10s	≤ 200 ms	≤ 0.1%

1.2.3 Customer Benefits

After the voice and video enhancement function is provided by WLAN products, it is enabled by default.

After the voice and video enhancement function is enabled, existing voice and video services on the upstream wired network and downstream air interface of a WLAN are assigned higher forwarding priorities than other data services. For example, with the voice and video enhancement function enabled, a Huawei WLAN provides 10% better user experience for the live WeLink video service than competitors' WLANs. Users' video mean opinion score (VMOS) values are increased, and the service transmission delay, jitter, and packet loss rate are reduced.

1.3 mDNS

Multicast DNS (mDNS) is the domain name service based on multicast technology. It is an open standard that implements zero configuration networking.

mDNS-capable devices include server and client devices. TV sets and printers are server devices, whereas smartphones and tablets are client devices. An mDNS server broadcasts service information on the local network, and listens on and responds to service requests from clients. Then smart terminals can discover the mDNS server and use the mDNS service.

Figure 1-1 mDNS application

With mDNS technology, music on a smart terminal (smartphone or tablet) can be placed on a stereo device near the smart terminal, video programs on the smart terminal can be displayed on a TV, and documents on the smart terminal can be printed by the nearest printer. However, mDNS application is restricted within a VLAN. Therefore, mDNS is only applicable for family use and cannot be used in enterprises.

Huawei WLAN products support the mDNS protocol analysis and service control functions, and implement inter-VLAN mDNS application. This makes it possible to apply mDNS technology to enterprises.

2 Application Identification Technologies

As broadband networks become popular, broadband data services develop rapidly. Network administrators need to understand the network traffic usage and implement certain control methods, for example, to ensure that key service flows are processed preferentially and network resources are not abused. For example, many point-to-point (P2P) applications occupy network resources maliciously, causing network congestion. Therefore, the network needs capabilities for the smart application identification and implementation of network policy control based on identification results.

A traditional traffic classification technology can only detect contents of Layer 4 and lower layers in IP packets, including source address, destination address, source port, destination port, and service type but cannot identify applications of the packets. Smart application identification can analyze the packet header and contents of the application layer, which is an application layer-based traffic detection and control technology.

Huawei's smart application control (SAC) is a smart application identification and classification engine. It detects and identifies contents of Layer 4 to Layer 7 and protocols such as HTTP, FTP, and RTP in packets and implements refined QoS policy control based on classification results.

2.1 Implementation

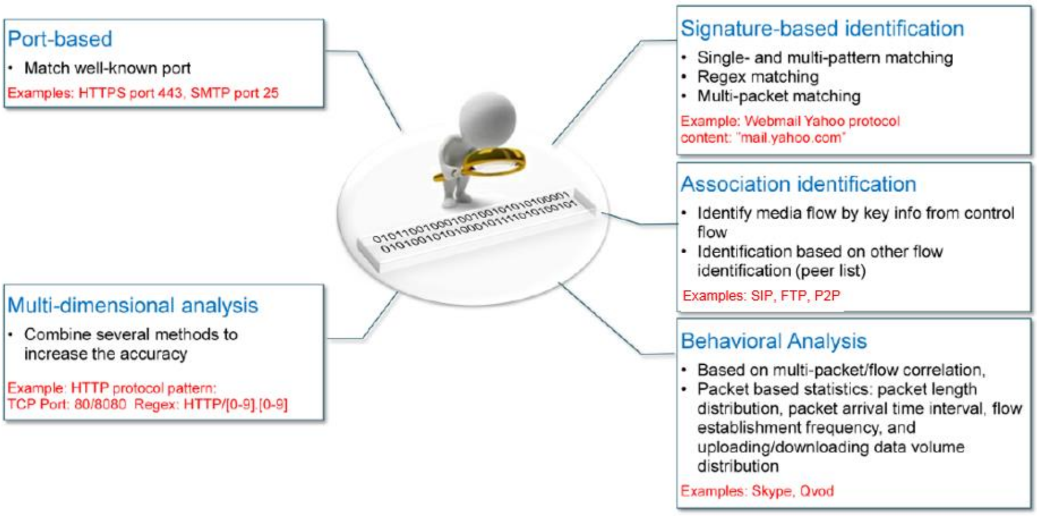
An application identification technology first identifies the application and service traffic on a network. The system then implements the following application and policy control based on identification results so that the administrator can manage and control the network more easily, flexibly, and effectively.

1. The built-in application identification function on a WLAN AC can identify common applications in various working scenarios.
2. The traffic statistics of identified applications can be collected, and can be saved and displayed on eSight.
3. Priority adjustment, scheduling, blocking, or rate limiting can be implemented for user services.

2.2 Key Technologies

Huawei uses a smart application and service identification technology to achieve application visibility, which identifies network traffic and collects traffic statistics. Huawei uses the following methods to identify network traffic.

Figure 2-1 Application identification technologies



Port-based
- Match well-known port

Examples: HTTPS port 443, SMTP port 25

Multi-dimensional analysis
- Combine several methods to increase the accuracy

Example: HTTP protocol pattern:
TCP Port: 80/8080 Regex: HTTP/[0-9].[0-9]

Signature-based identification
- Single- and multi-pattern matching
- Regex matching
- Multi-packet matching

Example: Webmail Yahoo protocol content: "mail.yahoo.com"

Association identification
- Identify media flow by key info from control flow
- Identification based on other flow identification (peer list)

Examples: SIP, FTP, P2P

Behavioral Analysis
- Based on multi-packet/flow correlation,
- Packet based statistics: packet length distribution, packet arrival time interval, flow establishment frequency, and uploading/downloading data volume distribution

Examples: Skype, Qvod

2.2.1 Port-based Identification

This traditional identification technology identifies protocols based on ports. That is, the technology matches protocols with well-known ports. For example, HTTP corresponds to port 80, HTTPS corresponds to port 443, and SMTP corresponds to port 25.

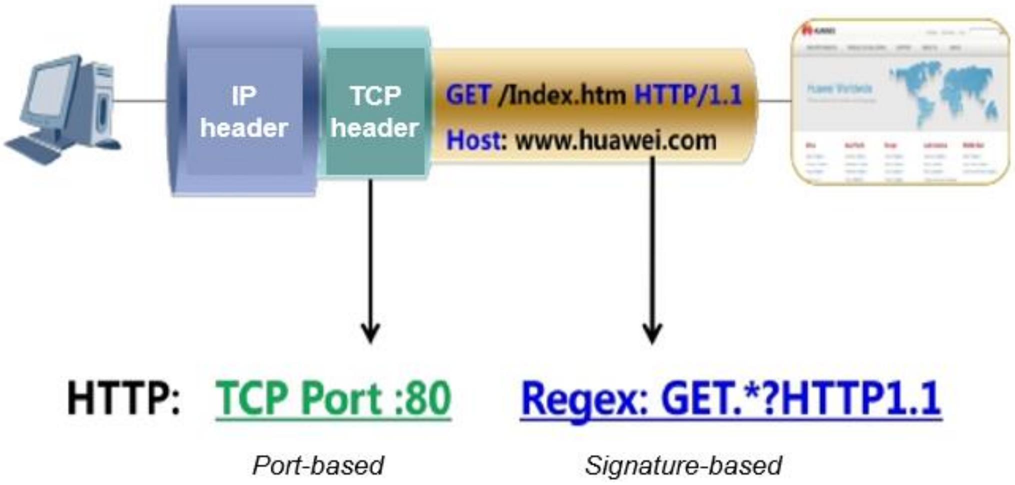
2.2.2 Signature-based Identification

This technology identifies signature codes in packets, including specific keyword strings and combinations of multiple keyword strings. This technology is classified into three types:

- Single- and multi-pattern matching
- Regex matching
- Multi-packet matching

For, example, packets of the Webmail Yahoo protocol contain the keyword string "mail.yahoo.com."

Figure 2-2 HTTP identification



More than one identification methods are often used together to increase the identification accuracy. For example, HTTP identification based only on port numbers is inaccurate because port 80 can also be used by other applications. Therefore, signature-based identification method can be added to increase the identification accuracy.

Generally, HTTP packets contain some fixed keywords, such as "GET", "POST", "HTTP/1.1", and "HOST", which can be used to design HTTP signatures.

2.2.3 Association Identification

The association identification technology identifies protocols based on protocol association. This technology analyzes specific application protocols and parses protocol interaction processes to identify the application traffic. This technology is classified into two types:

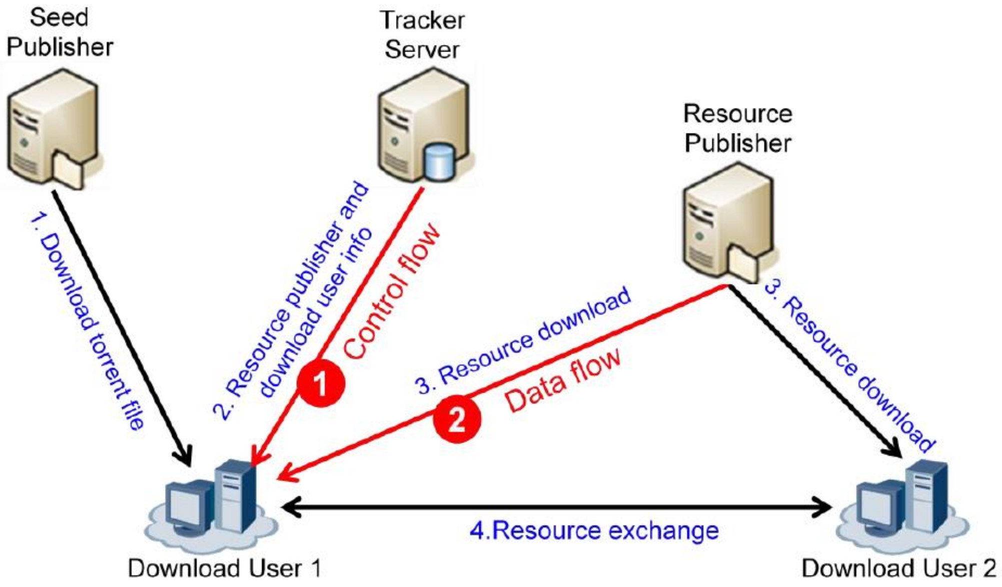
- Identify media flows based on control flow information.
- Identify applications based on other flows (such as P2P data flow).

For example, port numbers used for media flows are dynamically negotiated through the interaction of SIP and FTP protocols. The corresponding media flows can be identified based on the analysis of control protocols.

A similar method is also usually used for identifying P2P applications: Devices identify the control protocol of a P2P application based on the signature (keyword), and then obtain and cache the IP address and port number of the resource publisher from the corresponding control flows.

Devices monitor the encrypted data flow with no any feature. If the destination IP address and port number of the data flow match the cached IP address and port number, the data flow is considered as the P2P application traffic (such as BitTorrent).

Figure 2-3 P2P application identification



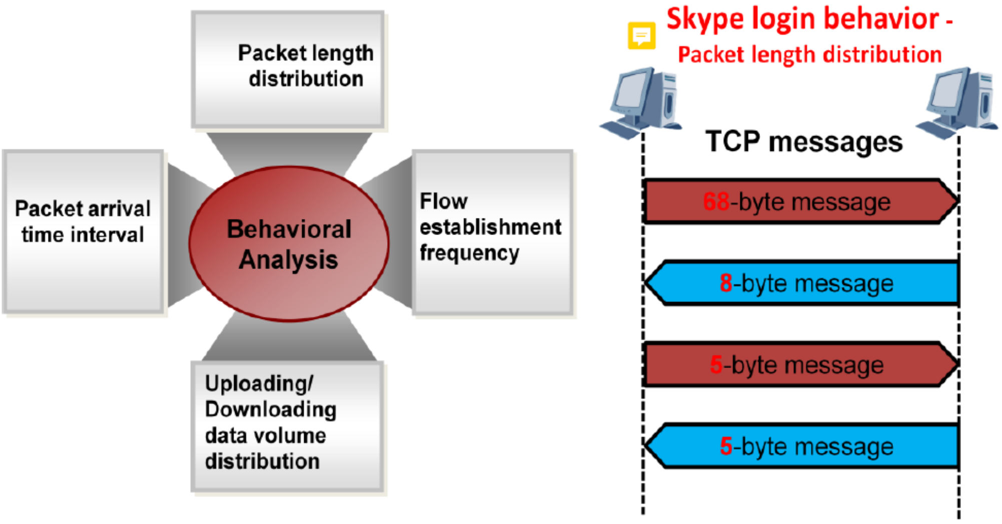
2.2.4 Behavior Analysis-based Identification

This technology is implemented based on the statistics collection of the behavior characteristics in a flow and between flows, such as packet length, transmission interval, and transmission direction.

- Based on multi-packet/flow association
- Packet statistics collection, including packet length distribution, packet arrival time interval, flow establishment frequency, and uploading/downloading data volume distribution

This technology is generally used for identifying Skype and Qvod flows.

Figure 2-4 Skype traffic identification based on behavior analysis


Packet length distribution
Packet arrival time interval
Behavioral Analysis
Flow establishment frequency
Uploading/ Downloading data volume distribution
Skype login behavior -
Packet length distribution
TCP messages
68-byte message
8-byte message
5-byte message
5-byte message

A small part of the Skype flows has signatures. TCP traffic sometimes uses ports 80 and 443, and UDP traffic sometimes uses ports 12340 and 12350, so a combination of port-based, signature-based, and behavior analysis-based identification methods can be used to identify the Skype traffic effectively.

2.2.5 Multi-dimensional Identification

Multi-dimensional identification and multiple identification methods can be used to increase the identification accuracy. For example, the HTTP protocol can be identified based on the TCP protocol and well-known port 80 only; however, there is a risk of misjudgment. This is because other applications can also use the TCP protocol and port 80. To increase the identification accuracy, port-based and signature-based identification methods can be used together to define the HTTP protocol model. For example:

TCP Port :80/8080 Regex: HTTP/[0-9].[0-9]

2.3 Application Traffic Statistics Collection

Application visibility allows the traffic usage of various applications on a network to be displayed to the administrator based on collected application traffic statistics. Huawei offers three application traffic statistics collection schemes:

- Global statistics collection: counts traffic of applications on the entire WLAN AC.
- SSID-based traffic statistics collection: counts traffic of the specified WLAN SSIDs.
- User-based traffic statistics collection: counts traffic of the applications of the specified users.

The application visibility feature collects traffic statistics for each type of application in the preceding dimensions based on application traffic identification.

2.4 Application-based Policies

A specific policy can be implemented for an application after packets of this application are identified. WLAN devices support three policies.

2.4.1 Blocking

After the blocking policy is implemented for an application, all packets of this application will be discarded.

2.4.2 Setting a Priority

If the priority policy is implemented for an application, the priority field (DSCP or 802.1p) in the packets of the application will be set to a preset value. Changing the priority field of the packets may change the packet processing sequence on a network. Packets of a higher priority will be preferentially transmitted, and therefore have a shorter delay and lower drop probability. Packets of a lower priority will be scheduled and processed later. The packets that cannot be transmitted in time will be temporarily saved in the buffer queue on the device. If the buffer overflows, the packets may be discarded. The administrator can set priorities for different applications to ensure the QoS of important applications.

2.4.3 Bandwidth Throttling

Bandwidth throttling policy is applied to specify an upper limit of the bandwidth allocated to an application. The administrator can set bandwidth upper limits for different applications to specify proportions of various application traffic on a network.

Bandwidth throttling prevents a small number of applications from occupying a large number of network resources to ensure the proper running of the other applications. For example, the administrator can set a limit for the bandwidth of P2P download applications to prevent P2P applications from abusing network resources.

3 Voice and Video Enhancement Technology Implementation

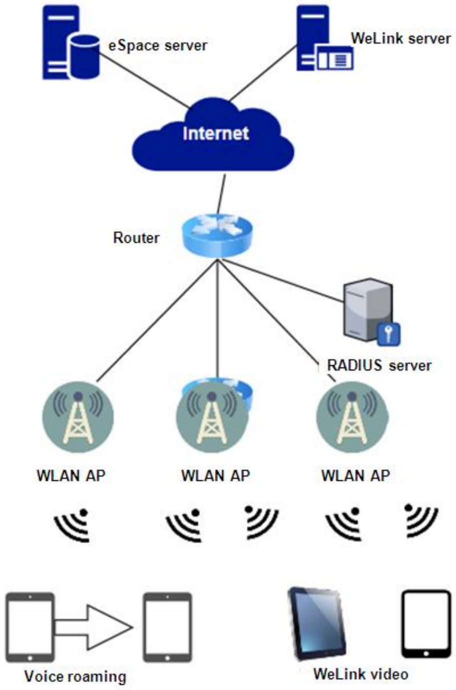
3.1 Overall Structure

In most cases, WLAN voice and video services are used in mobile office scenarios on enterprise campuses.

In AP+AC networking mode, various voice and video services exist, including inter-AP roaming voice call services on the same WLAN AC (not involving inter-AC roaming). It is required that voice and video service packets be identified and packet priorities be increased to achieve QoS scheduling and improve user experiences.

In addition, O&M visibility is required for network IT personnel to learn the status and quality of voice and video services run on networks.

Figure 3-1 Networking for WLAN voice and video services



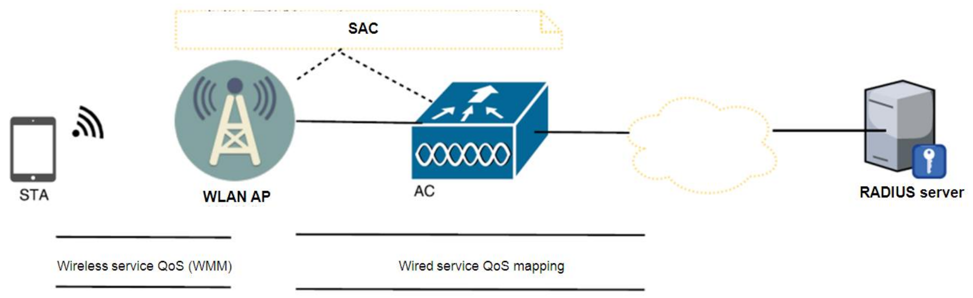
3.2 Technical Framework

When no network congestion occurs on a WLAN, user experience on all services is good.

The MAC address layer of a WLAN is shared by multiple Wi-Fi terminals, and the total bandwidth of frequency bands is limited. Therefore, with the increase in the number of users and per-user service traffic volume, network congestion is inevitable. In this case, end-to-end QoS policies are critical to the WLAN. The voice and video enhancement function of WLAN devices aims to provide proper wireless network resources matching users' service traffic, and reduce the voice service delay and video data traffic loss by setting QoS priorities based on service and user types.

The voice and video enhancement function of WLAN devices is developed based on Smart Application Control (SAC) and the WLAN QoS technical framework. SAC provides service awareness capabilities, while WLAN QoS is classified into wireless service QoS (AP-STA) and wired service QoS (AP-AC). Wireless service QoS, in compliance with the IEEE 802.11e standard (WMM), provides wireless resource management and network congestion control based on user and service types. Wired service QoS, in compliance with the IEEE 802.11p standard, provides QoS mapping of wired bearer services, traffic class expediting, and dynamic multicast filtering.

Figure 3-2 Technical framework of WLAN voice and video enhancement



3.3 Key Technologies

3.3.1 Voice and Video Service Identification

SAC is a smart engine developed by Huawei that can identify and classify application protocols. It is deployed on WLAN APs and ACs in distributed mode. SAC uses service awareness technology to identify dynamic protocols such as the HTTP and RTP by checking Layer 4 to Layer 7 information in data packets. SAC provides a technical basis for fine-grained QoS policy control.

The SAC signature database of WLANs can identify the following types of voice and video services:

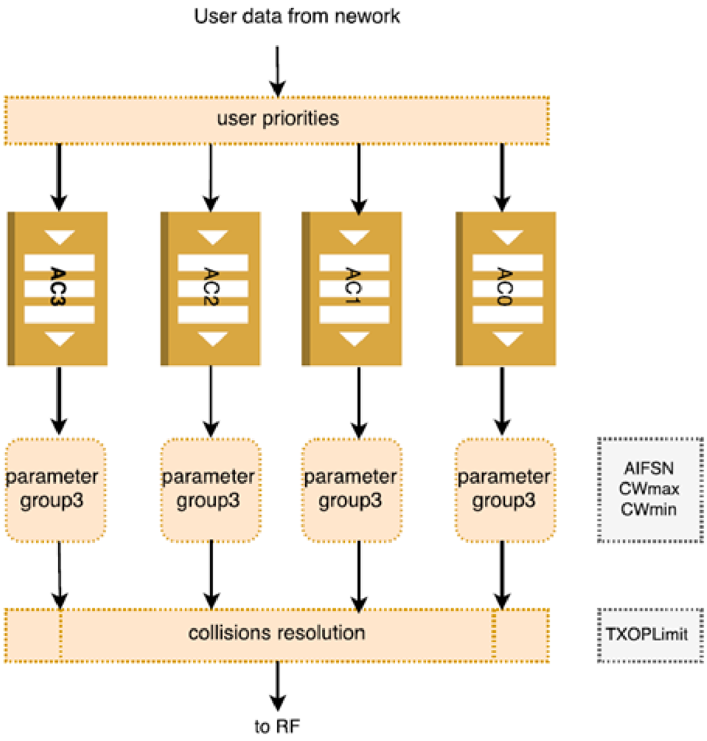
1. Session Initiation Protocol (SIP) voice and video
2. Voice service packets transmitted using RTP
3. Microsoft Skype4B and Lync/Skype for Business
4. Tencent QQ
5. Tencent WeChat
6. WeLink VoD
7. DingTalk

SAC is supported by all Huawei WLAN devices. For details about the technical implementation, see related WLAN product documentation.

3.3.2 Dynamic EDCA Parameter Adjustment

WMM defines enhanced distributed channel access (EDCA) parameters in 802.11e. EDCA classifies data packets into four access categories (ACs) in descending order of priorities: AC-voice (AC-VO), AC-video (AC-VI), AC-best effort (AC-BE), and AC-background (AC-BK). Data packets in a high-priority access category have greater capabilities in channel preemption. A set of EDCA parameters is set for each AC queue. These EDCA parameters determine the capabilities of AC queues in channel preemption. Figure 3-3 shows how AC queues preempt channels.

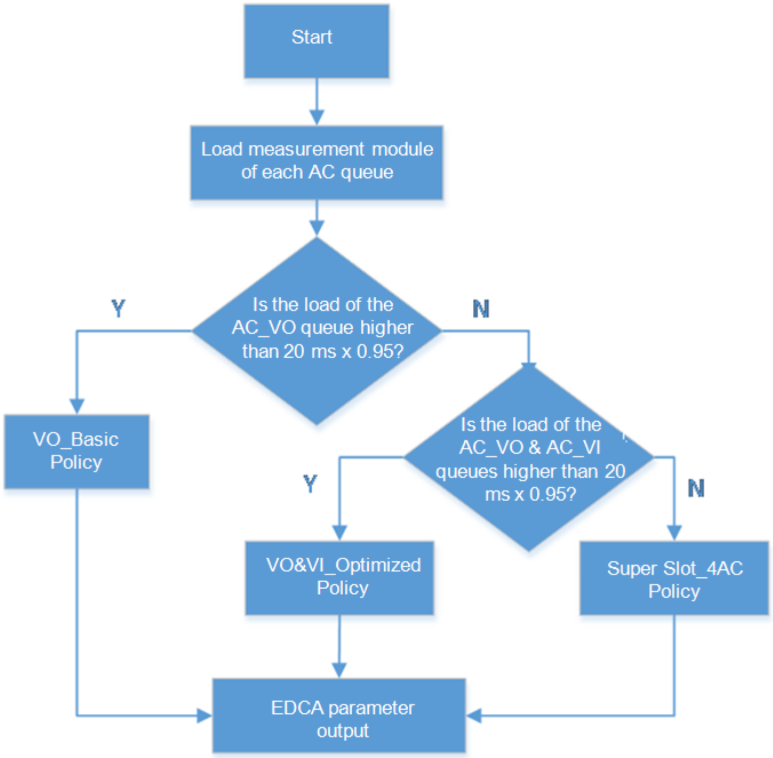
Figure 3-3 Schematic diagram of channel preemption by AC queues



Parameter Name	Description
Arbitration Interframe Spacing Number (AIFSN)	In the distributed coordination function (DCF) mechanism, the DCF interframe space (DIFS) has a fixed value. WMM provides different DIFS values for different ACs. A large AIFSN value indicates that a STA must wait for a long time and has a low priority.
Exponent Form of CWmin (ECWmin) and Exponent Form of CWmax (ECWmax)	ECWmin specifies the minimum backoff time, and ECWmax specifies the maximum backoff time. They together determine the average backoff time. Large ECWmin and ECWmax values indicate that the average backoff time for a STA is long and the STA priority is low.
Transmission Opportunity Limit (TXOPLimit)	After successfully preempting a channel, a STA can occupy the channel within the period of TXOPLimit. A large TXOPLimit value indicates that the STA can occupy the channel for a long time. If the TXOPLimit value is 0, the STA can send only one data packet every time it preempts a channel.

Dynamic EDCA parameter adjustment is enabled for APs to dynamically adjust EDCA parameters of detected voice and video services. The following figure shows the dynamic EDCA parameter adjustment process.

Figure 3-4 Dynamic EDCA parameter adjustment process


Start
Load measurement module of each AC queue
Is the load of the AC_VO queue higher than 20 ms x 0.95?
Y
N
VO_Basic Policy
Is the load of the AC_VO & AC_VI queues higher than 20 ms x 0.95?
Y
N
VO&VI_Optimized Policy
Super Slot_4AC Policy
EDCA parameter output

The dynamic EDCA parameter adjustment process is described as follows:

1. Load measurement module of each AC queue: collects statistics on the forwarding duration of data packets to be sent in the AC queue on air interfaces for calculating the load of the AC queue to be scheduled.
2. Parameter configuration policy selection mechanism: Select a parameter configuration policy based on the weight of AC queue loads in a WLAN system.
3. Parameter configuration policy: The following parameter configuration policies are provided in a WLAN system: VO_Basic Policy, VO&VI_Optimized Policy, and Super Slot_4AC Policy.
4. By default, dynamic EDCA parameter adjustment is enabled on WLAN devices.

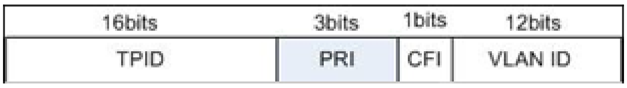
3.3.3 Traffic Mapping

The voice and video enhancement function defines priority mapping of users' voice and video services on networks.

Different from other data service packets, voice and video service packets are transmitted by WLAN APs carrying different QoS priorities. For example, VLAN packets carry 802.1p priorities, and IP packets carry DSCP priorities.

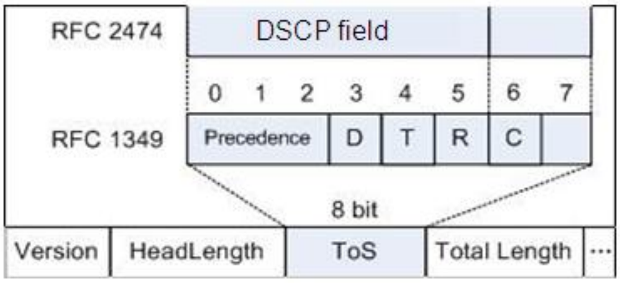
Priorities of VLAN frames are mapped based on the Class of Service (CoS) field in a VLAN frame header. The PRI field (802.1p priority) in a VLAN frame header identifies the QoS requirement. The PRI field defines eight transmission priorities 7, 6, 5, 4, 3, 2, 1 and 0 in descending order of priority. For example, packets with priority 7 enter queue 7, packets with priority 6 enter queue 6, and so on. The following figure shows the PRI field in a VLAN frame.

Figure 3-5 PRI field in a VLAN frame



IP packets are marked by the first 3 bits (IP precedence field) or first 6 bits (DSCP field) in the Type of Service (ToS) field in an IP packet header. If the DSCP field is used to identify IP packets, IP packets can be classified into a maximum of 64 classes. The following figure shows the ToS field in an IP packet header.

Figure 3-6 ToS field in an IP packet header



The preceding describes how priorities of wired-side packets are classified and identified. When service packets from STAs are forwarded between WLAN APs and ACs, priority mapping needs to be configured to achieve QoS processing of the service packets on air interfaces and the wired side.

Table 3-1 Mapping from the DSCP priority to the 802.1p priority (CoS) and 802.11e user priority (WMM)

DSCP Priority	802.1p Priority (CoS)	802.11e User Priority (WMM)
0–7	0	0
8–15	1	1
16–23	2	2
24–31	3	3
32–39	4	4
40–47	5	5

DSCP Priority	802.1p Priority (CoS)	802.11e User Priority (WMM)
48–55	6	6
56–63	7	7

3.3.4 Fast Roaming Optimization

If a STA roams between WLAN APs when using voice and video services, voice and video service packets need to be processed in different ways based on the user access mode.

For example, if the user access mode of a WLAN is WPA/WPA2+PSK or WPA/WPA2+802.1X, STAs must negotiate keys with or be authenticated by a new WLAN AP when attempting to roam to it. This leads to a long roaming switchover time, a low roaming success rate, and even service interruption. Huawei WLAN devices support IEEE 802.11r, allowing for fast roaming of STAs without compromising STA access security. For details, see the *Huawei WLAN Fast Roaming Technology White Paper*.

The voice and video enhancement function of Huawei WLAN devices is also optimized on the basis of fast roaming in the following aspects:

1. When the user access mode of a WLAN is WPA-WPA2, fast roaming is supported if STAs' association request packets carry a pairwise master key (PMK).
2. In opportunistic key caching (OKC) based fast roaming scenarios, after a STA passes access authentication, a WLAN AC delivers a PMK to the associated AP and neighboring APs. Each time the STA roams, the WLAN AC delivers a PMK to neighboring APs. In this way, when determining that a STA is roaming, the AP to which the STA attempts to roam first checks whether the STA's PMK exists in the cache. If the cached PMK exists, a 4-way handshake process is triggered immediately. The AP waits for the WLAN AC to deliver a PMK only when the STA's PMK does not exist in the cache.

Voice and video service are delay-sensitive. The preceding measures shorten the time taken by a STA to roam to another AP.

4 mDNS Technology Implementation

4.1 Overview

mDNS implements multi-screen sharing. For example, music on a smart terminal (smartphone or tablet) can be placed on a stereo device near the smart terminal, video programs on the smart terminal can be displayed on a TV, and documents on the smart terminal can be printed by the nearest printer. However, these new applications can only be used at home for the following reasons:

- mDNS application is restricted within a VLAN and is not applicable in enterprises.
- APs forward multicast packets at low speeds, reducing the capacity of the entire wireless network. This is acceptable in family usage scenarios but not acceptable in enterprises.

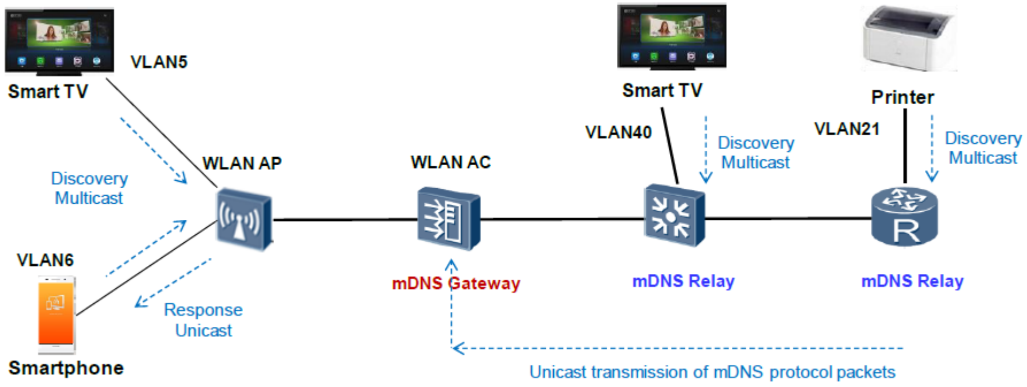
To enable mDNS application in enterprises, Huawei offers the mDNS relay component (deployed on a switch) and mDNS gateway component (deployed on a WLAN AC).

- **mDNS relay:** It is deployed in the same VLAN as mDNS-capable devices. It converts mDNS multicast packets into unicast packets and communicates with the mDNS gateway over Layer 3.
- **mDNS gateway:** It collects and records mDNS service information in each VLAN and subnet, and responds to service requests from mDNS clients.

The mDNS relay discovers all devices that can work as mDNS servers, and then sends mDNS service information to the mDNS gateway in unicast mode. When mDNS clients search for mDNS servers, the mDNS relay forwards the requests from the clients to the mDNS gateway in unicast mode. The mDNS gateway then responds to the requests.

Figure 4-1 shows the inter-VLAN mDNS application.

Figure 4-1 mDNS application across VLAN/Layer 3 network



4.2 Implementation

4.2.1 mDNS Protocol

Zero configuration networking is implemented using the mDNS and DNS-Based Service Discovery (DNS-SD) protocols.

NOTE

The mDNS protocol is defined in RFC 6762 (Multicast DNS), and the DNS-SD protocol is defined in 6763 (DNS-Based Service Discovery).

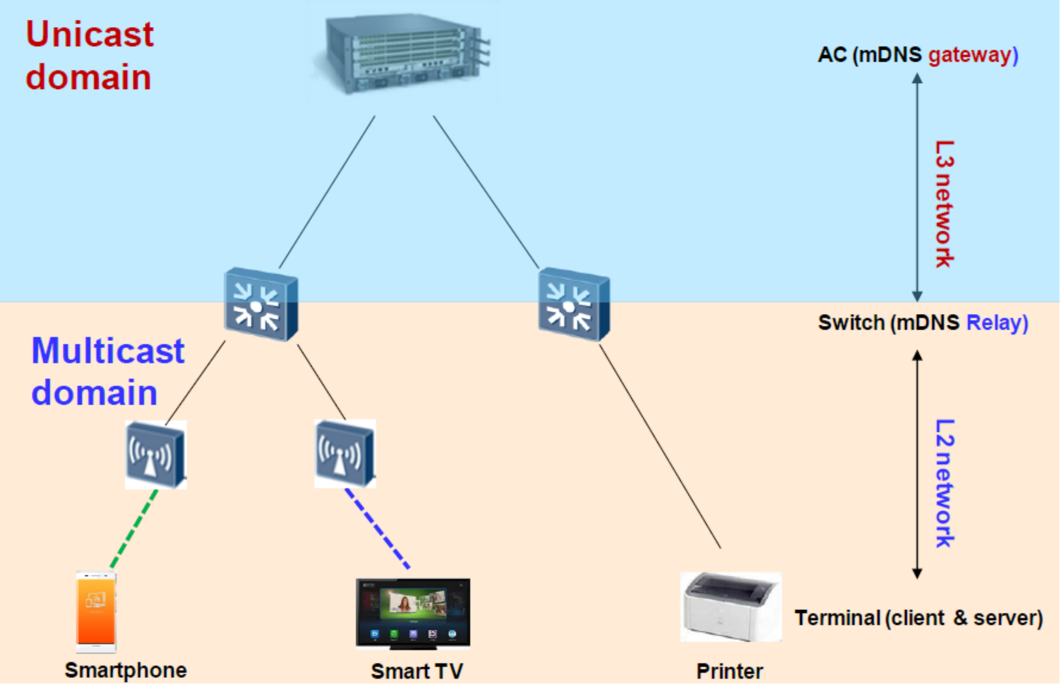
mDNS devices propagate their service information on the local network and listen on service information from other devices. The mDNS protocol enables clients to discover service systems and services without intervention of the administrator.

The mDNS protocol uses a fixed destination IPv4 address 224.0.0.251 (or IPv6 address FF02::FB) and port 5353 for multicast transmission. This protocol works well within a VLAN or a subnet. However, the destination IP address is a link-local address, so mDNS cannot be implemented across a Layer 3 network and different VLANs.

4.2.2 Network Components

In an enterprise network, mDNS servers include printers, smart TVs, and smart set top boxes (STBs). These mDNS servers do not belong to the same VLAN as wireless mDNS clients, such as smartphones and tablets. The mDNS protocol only works at Layer 2 and cannot provide services cross VLANs. Therefore, an mDNS gateway needs to be deployed to forward mDNS packets and maintain service information between VLANs. An enterprise network is usually large, and routers or other devices exist between the client/server and the gateway. Therefore, the switch at the edge of a subnet must provide the mDNS relay function to forward mDNS packets to the gateway.

Figure 4-2 Roles in the mDNS solution



- **mDNS relay**: The devices connecting to TVs or printers run the mDNS relay function (enabled globally, in VLANs, or on interfaces). They listen on service registration packets and forward the packets to the gateway in unicast mode. The mDNS relay devices support periodic detection.
- **mDNS gateway**: enabled globally, in VLANs, or on interfaces. The mDNS gateway sends the unicast packets received from the mDNS relay to the CPU, and maintains a service list and other information, including the service name, domain name, IP address, port number, L4 protocol type, and VLAN ID.

In Huawei mDNS solution, the mDNS gateway centrally maintains a database for service resources on the entire network, such as smart TVs and printers, and sends resource lists to clients in unicast mode. After a client discovers a required service, the client and server can perform point-to-point communication using TCP or UDP.

mDNS protocol identification: Huawei network products support mDNS snooping. They can intercept mDNS packets on air interfaces (WLAN products) and wired interfaces (switch and AR products), and record mDNS packet information, including source MAC address, source IP address, inbound interface, and VLAN ID. The mDNS relay sends the intercepted mDNS packets to the mDNS gateway in unicast mode based on the configuration.

Inter-VLAN mDNS packet forwarding: The mDNS relay converts the intercepted mDNS packets into unicast packets and routes the packets to the specified client or server (for example, a smart TV) through the Layer 3 mDNS gateway). The mDNS-to-unicast conversion solves the problems of inter-VLAN mDNS service and AP performance deterioration caused by multicast packets.

4.3 mDNS Service Process

The process of mDNS service across a Layer 3 network is as follows:

1. An mDNS server advertises its host name in unicast mode.
2. The mDNS relay forwards the multicast packet with the host name to the mDNS gateway, which then records the host name and IP address.
3. The mDNS server advertises its service in unicast mode.
4. The mDNS relay forwards the multicast packet with the service information to the mDNS gateway, which then records the service information.
5. A client sends a unicast service request.
6. The mDNS relay forwards the multicast service request to the mDNS gateway.
7. The mDNS gateway sends the search result to the mDNS relay.
8. The mDNS relay forwards the search result in multicast mode.

4.3.1 mDNS Service Advertisement by a Server

An mDNS server sends multicast mDNS packets in the local network segment to advertise its service information. The mDNS relay uses the specified ACL rules to obtain qualified multicast mDNS packets. The mDNS relay forwards the multicast mDNS packets to the local network segment according to the multicast forwarding rule, and also copies the packets, changes the source and destination IP addresses of the packets, and then sends the packets to the mDNS gateway in unicast mode. The mDNS gateway records and registers the service information.

The mDNS relay processes the multicast mDNS packets as follows:

1. The mDNS relay obtains mDNS packets with the destination address 224.0.0.251, protocol type UDP, and destination port 5353.
2. The mDNS relay changes the destination IP address to the gateway IP address, the source IP address to its own IP address, and assigns a transaction ID to a packet. It records the mapping of the client IP address, client VLAN ID, and transaction, and starts the aging timer. Then it sends the modified packet to the mDNS gateway, so that the gateway can register service information and perform conflict detection.

4.3.2 mDNS Service Discovery by a Client

The service discovery process includes steps 5 to 8 in the mDNS service process. The process of sending a query request packet to the mDNS gateway is the same as the process of advertising the mDNS service.

After the mDNS gateway receives the query request from the client, it searches for the requested service in the online service list and domain name table, and returns the search result to the mDNS relay.

The search result is carried in a unicast UDP packet with the source IP address as the gateway IP address, destination IP address as the mDNS relay's IP address, destination port 5353, and protocol type UDP.

After receiving the response packet from the mDNS gateway, the mDNS relay finds information about the client that sends the query request according to the transaction ID in the response packet. The mDNS relay then modifies the response packet by changing the destination IP address to 224.0.0.251, source IP address to its own IP address, transaction ID to 0 and TTL to 255, and multicasts the packet to the VLAN where the client is located. Finally, the mDNS relay deletes the mapping of client IP address, client VLAN, and transaction ID.

4.3.3 Service Conflict Notification by the Gateway

Clients and servers detect service conflicts and domain name conflicts by sending query request packets. After receiving a service query request from a client, the mDNS gateway matches the packet with the specified ACL and sends the packet to the CPU if the match succeeds. The gateway searches for the requested service in the online service list and domain name table, and sends a response packet to the mDNS relay. After receiving the response, the client/server takes measures to handle the conflict (if any).

4.3.4 mDNS Service Discovery by the Gateway

If a VLAN contains only mDNS servers that have started before network connections are established, the servers do not inform the mDNS gateway what services they provide. In this case, the mDNS gateway needs to periodically update the service list and server states.

When a response packet sent from a server reaches the mDNS relay, the packet is processed on the control plane of the mDNS relay as follows:

The mDNS relay changes the destination IP address to the gateway address and the source IP address to its own IP address. The relay does not assign a transaction ID to the packet and does not record the mapping of the client IP address, client VLAN ID, and transaction ID.

The mDNS relay then sends the modified response packet to the mDNS gateway.

4.4 Logical Network Elements and Functions

Huawei enterprise mDNS solution is implemented in the following way:

1. The mDNS gateway centrally maintains an online service list.
2. The mDNS relay converts multicast mDNS packets into unicast packets in a VLAN so that the packets can be forwarded at Layer 3.
3. Clients and servers then use IP to communicate with each other.

4.4.1 mDNS Gateway

Huawei WLAN ACs have an mDNS gateway module, which provides the following functions:

- Responds to mDNS requests sent from clients in unicast mode.
- Identifies and intercepts mDNS protocol packets, and sets up a resource database to maintain resource information on the entire network. Resource information includes IP addresses and names of service providers.
- Sends mDNS request packets to request for information about service provider devices in a specified network segment, such as printers, audio devices, and TVs.

Key points about mDNS gateway implementation are as follows:

- If a server connects to a network and obtains an IP address before the mDNS gateway is deployed, the server does not report its service to the gateway. Therefore, the gateway needs to periodically detect servers that connect to its Layer 2 network.
- The default service aging time of a smart TV is 2 minutes. According to the mDNS protocol, an mDNS device sends a query request after 80% of the timer value elapses (120s x 80% = 96s). The default query interval defined by Huawei is 90s (configurable). That is, if the default setting is used, Huawei devices will send a query request before the aging timer of a smart terminal times out. This reduces the network resources consumed by service query.
- When a record maintained by the mDNS gateway is about to expire, the gateway sends a query request packet to the mDNS relay. In the packet, the source address is the gateway IP address, the destination address is the relay IP address, and the transaction ID is 0. The mDNS relay finds that the transaction ID of the packet is 0 and therefore it cannot find the VLAN ID of the client or server. Then the relay multicasts the query request to all VLANs connected to it, and obtains service information in all these VLANs.

4.4.2 mDNS Relay

Huawei LAN switches integrate the mDNS relay module, which provides the following functions:

- Supports configuration of the mDNS relay destination address, that is, the destination WLAN AC's IP address.
- Converts multicast mDNS packets into unicast packets with the destination IP address and the WLAN AC's IP address.
- Forwards mDNS unicast packets according to the normal forwarding process.

Key points about mDNS relay implementation are as follows:

- To enable mDNS packets to be transmitted to the mDNS gateway, the mDNS relay needs to change the destination IP addresses of the packets to the gateway IP address.
- To enable the response packets to be sent back to the relay, the relay needs to change the source IP addresses of packets to its own IP address.
- The transaction ID field is used as a keyword to match the request and response packets sent from clients with the request and response packets sent from the gateway.
- To find the VLAN of a client according to a response packet sent from the gateway, the mDNS gateway needs to record the source address, VLAN information, and allocate a transaction ID when it changes the source and destination IP address of a packet sent to the gateway. (Clients send the transaction ID of multicast mDNS packets to 0, so multicast forwarding is not affected.)
- According to the mDNS protocol, a client can communicate with the relay if the client considers that the response packet is sent from the same network segment of is a multicast packet. Therefore, to communicate with clients, the relay needs to modify a response packet by changing the source IP address to the IP address of the local Layer 2 network, the destination to the mDNS multicast address 224.0.0.251, TTL to 255, and transaction ID to 0.

4.4.3 Exception Handling

- Periodic update based on the aging time

  The mDNS gateway maintains a list of services available on the network. Each service has an aging time. When 80% of the aging time elapses, the gateway sends a query request to the relay. The relay multicasts the request in the local network segment. If a valid response is received, the gateway resets the aging timer. If no valid response is received, the queried service has become invalid. If the gateway does not receive any registration message for this service, it deletes the service from the service list.

- Periodic detection

  If period detection is enabled on the mDNS relay, the relay sends multicast service query requests in the local network segment when the detection timer expires.

  If period detection is enabled on the mDNS gateway, the gateway sends multicast service query requests in the directly connected network segments when the detection timer expires.

  The detection interval is configurable, and the default interval is 90s.

- Service conflict handling

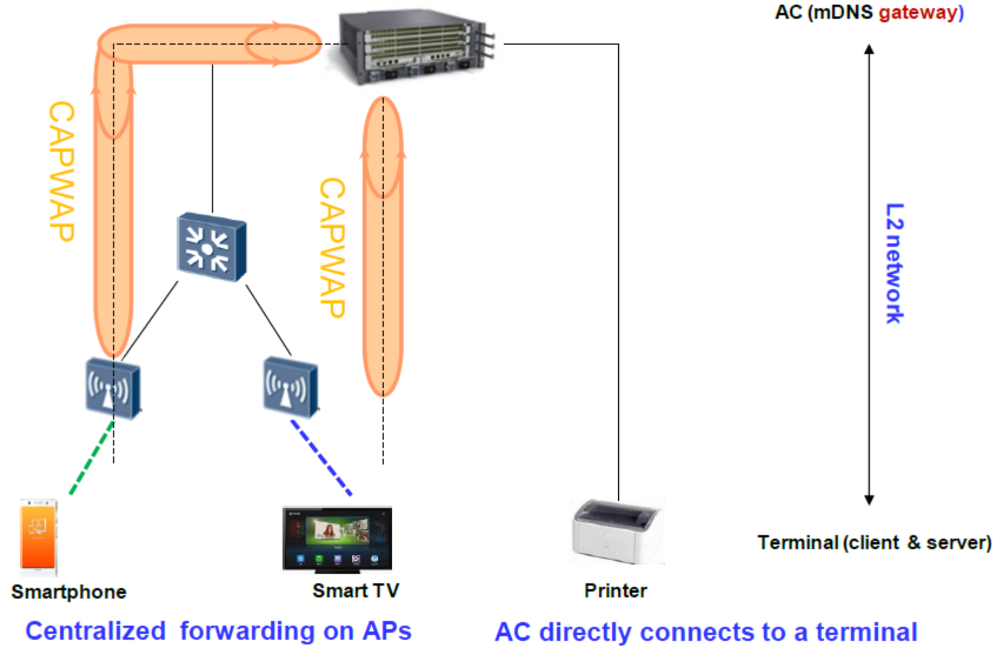
  If the service names or host names of mDNS servers conflict, the gateway sends a defend message to the relay in the network segment where the conflict occurs. The relay then multicasts the defend message in the network segment.

- Service process when the gateway starts later than servers

  An mDNS gateway may start later than servers on the network. If clients send service query requests, they cannot find valid mDNS service because the gateway does not have a complete network service list. To solve this problem, the gateway actively sends service query requests to discover available services after it is powered on.

4.5 Special Networking Scenarios

Figure 4-3 Centralized forwarding on APs and direct connection between a WLAN AC and a terminal


AC (mDNS gateway)
CAPWAP
CAPWAP
L2 network
Smartphone
Smart TV
Printer
Terminal (client & server)
Centralized forwarding on APs
AC directly connects to a terminal

4.5.1 Centralized Forwarding on APs

When APs use the centralized forwarding mode, data packets sent from smart terminals are forwarded to the WLAN AC through Control and Provisioning of Wireless Access Points (CAPWAP) tunnels. The mDNS service process is the same as that in the scenario where terminals are directly connected to the WLAN AC. For details, see section 4.5.2 "Direct Connection Between a WLAN AC and a Terminal."

4.5.2 Direct Connection Between a WLAN AC and a Terminal

If smart terminals are in the same network segment as a WLAN AC, the mDNS relay is not required. The mDNS gateway accepts mDNS packets with a multicast destination address, and records VLAN IDs of mDNS packets when it records entries in the service list and host table. When the gateway sends packets to the directly connected terminals, it sets the destination IP address to the mDNS multicast address and sets the VLAN ID in the packets.

4.6 Characteristics of Huawei WLAN mDNS Technology

4.6.1 Inter-VLAN mDNS Service

Due to limitation of the mDNS protocol, the mDNS service is only applicable to small-scale LANs. Therefore, mDNS is mainly used in family scenarios and seldom used in enterprises.

Huawei products support mDNS relay and mDNS gateway functions, which implement inter-VLAN mDNS service.

4.6.2 mDNS Service Across a Layer 3 Network

The mDNS relay and mDNS gateway components integrated on Huawei products not only provide inter-VLAN mDNS service, but also support the mDNS service across a Layer 3 network.

4.6.3 mDNS Service on Wired and Wireless Networks

Huawei integrates the mDNS relay component on switches and integrates the mDNS gateway component on WLAN ACs. You can deploy both the mDNS relay and mDNS gateway on a network to provide mDNS service across VLANs and Layer 3 networks. Alternatively, you can deploy the mDNS gateway alone to implement inter-VLAN mDNS service.

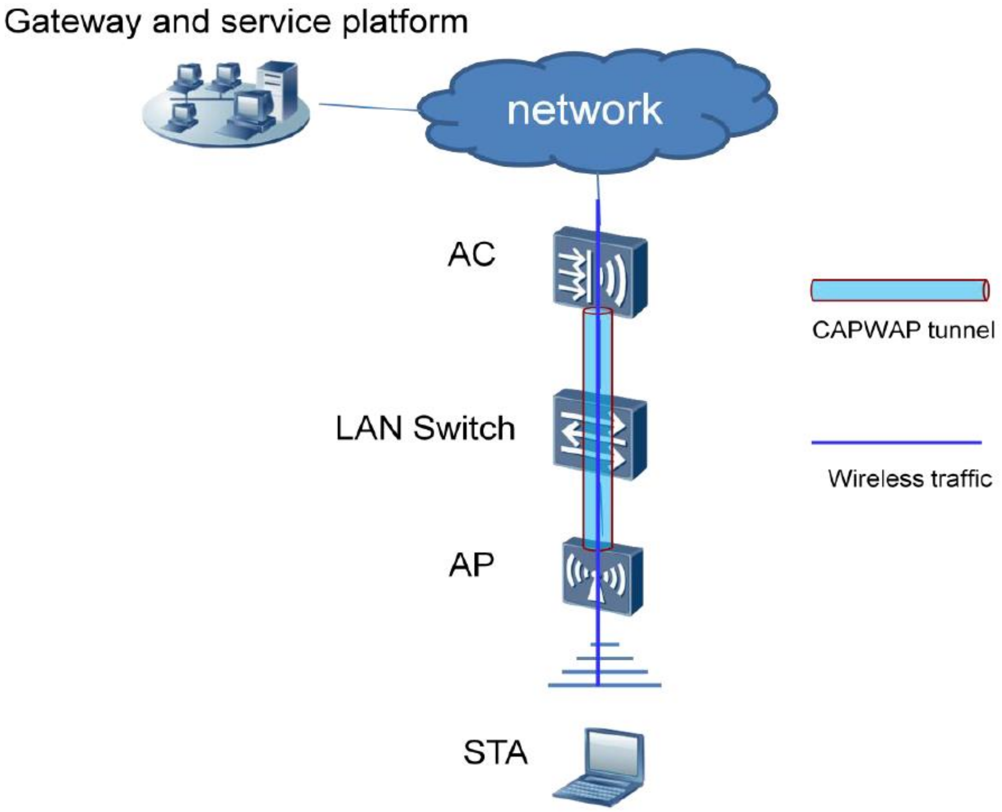
Both wired and wireless terminals can function as mDNS clients or servers, no matter which networking is used.

5 SmartApp Networking Applications

5.1 Application Identification Technology Application

5.1.1 Networking for WLAN Application Identification

Figure 5-1 Networking diagram for WLAN application identification



Huawei application identification function is supported only on WLAN ACs and applies only to the wireless user traffic transmitted in tunnel forwarding mode. To enable the application identification function in a Huawei WLAN system, the administrator needs to set the forwarding mode to tunnel forwarding and enable application identification on the WLAN AC. The WLAN AC can be connected in bypass mode or inline mode.

It should be noted that on a Huawei independent WLAN AC, the application identification function can only be enabled on a wireless port (VAP port), not on a wired port. Therefore, the application identification function takes effect only for the wireless traffic transmitted in tunnel forwarding mode and does not take effect for wired data traffic. Even if a WLAN AC is connected in inline mode, the traffic passing through a wired port cannot be identified.

On current Huawei WLAN network, a WLAN AC can collect traffic statistics, but cannot identify the contents of the traffic. Therefore, the statistics can only be collected on a per port/user basis but not for specific service types (such as Thunder, QQ, or Facebook). As these applications cannot be identified, the policy control cannot be implemented for the applications.

Application visibility is configured on a WLAN AC in a centralized forwarding WLAN networking. After going online on a WLAN AP, a user starts various applications on the STA to access the network. The WLAN AC analyzes packet flows sent from users to obtain network resource usage of the users' applications. Then the WLAN AC reports the collected statistics to the network management system (NMS). So the statistics will be displayed and saved on the NMS for the administrator to view at any time.

If network congestion occurs, the administrator can apply policies based on applications, including traffic blocking, priority setting, and rate limiting.

5.1.2 Application Statistics Collection

The application identification technology helps collect traffic statistics of different applications, enabling the administrator to clearly know the actual situation of data traffic on a network. The collected application statistics can also be used for network application evaluation, policy control, and network optimization/capacity expansion and as an important means or design basis for network monitoring, optimization, and upgrade.

Perform the following operations to configure application statistics collection:

1. Enable application visualization in the service set profile view.
2. Enable a user associated with the corresponding VAP to access a network.
3. Configure the WLAN AC to analyze and identify the traffic of the user.
4. Collect statistics of the identified user traffic based on WLAN + user + application.
5. Collect traffic statistics every 30 seconds, and save the statistics to the memory.
6. Save the statistics (3*30 seconds) on the WLAN AC.
7. Run a command to check the application traffic statistics.

5.1.3 Reporting Application Visibility Information to the NMS

The identified traffic statistics can be reported to Huawei NMS or a third-party NMS through NetStream for more accurate and powerful traffic statistics and analysis and will be displayed in reports.

1. Enable application visibility in the service set profile view.
2. Enable NetStream statistics collection in the corresponding VAP.

3. Enable a user associated with the VAP to access a network.
4. Configure the WLAN AC to analyze and identify the traffic of the user.
5. Collect statistics of the identified user traffic based on WLAN + user + application.
6. Configure NetStream to collect and report the statistics to the NMS.
7. Save the statistics on the NMS.

5.1.4 Implementation of the Application-based Policy Control

After an application is identified, the administrator can perform the priority control, access control, and bandwidth limit.

- Setting the priority for an application
  1. Enable application visibility in the service set profile view.
  2. Enable a user associated with the corresponding VAP to access a network.
  3. Configure the packets of the application the priority of which is to be modified.
  4. Configure the WLAN AC to analyze and identify the traffic of the user.
  5. Set the priority for the identified application traffic.
- Limiting the access of an application
  1. Enable application visibility in the service set profile view.
  2. Enable a user associated with the corresponding VAP to access a network.
  3. Configure the application packets that are to be discarded.
  4. Configure the WLAN AC to analyze the user's traffic and discard the packets of the specified application.
  5. Enable the user to use the application to access the network. The traffic cannot be forwarded.
- Setting the bandwidth for an application flow
  1. Enable application visibility in the service set profile view.
  2. Enable a user associated with the corresponding VAP to access a network.
  3. Set the bandwidth limit for traffic of the specified application.
  4. Configure the WLAN AC to analyze the traffic of the user and discard the packets that exceed the bandwidth limit.
  5. Enable the user to use the application to access the network. The user can access the network normally.
  6. Specify the bandwidth limit for an application to limit the traffic within the allowed bandwidth range.

5.2 Voice and Video Enhancement Application

5.2.1 Technical Highlights

The voice and video enhancement function of Huawei WLAN devices has the following highlights:

1. Supports in-service upgrade of the SAC signature database, which is not supported by Company H.
2. Supports Tencent QQ, Tencent WeChat, WeLink VoD, and DingTalk services, which are not supported by competitors' WLAN devices.
3. Supports radio-based control of the number of voice users.
4. Supports visualized O&M of voice and video services.

5.2.2 Capability Restrictions

Pay attention to the following precautions when configuring the voice and video enhancement function on Huawei WLAN devices:

1. This function can be configured in WLAN AC+Fit AP and WLAN AC+central AP/RU networking modes. Fat, Fat central, cloud, and cloud central APs do not support this function.
2. WLANs only act as wireless communication channels for voice and video services, but do not guarantee end-to-end QoS of voice and video services.
3. Radio-based control of the number of video users is not supported.
4. In direct forwarding mode, the SAC signature database needs to be loaded on both WLAN ACs and APs.
5. Bandwidth cannot be reserved for roaming voice and video users.
6. The Wi-Fi calling service does not support voice and video enhancement. Wi-Fi calling is also called Voice over WiFi (VoWiFi) in the mobile carrier technical field.

Function	Description	Company H	Company C	H3C	Huawei
Voice user status monitoring	Monitoring of media service states, including voice calling, connection, and disconnection	Supports Apple FaceTime, Alcatel-Lucent New Office Environment (NOE), Microsoft Lync/Skype for Business, Cisco Jabber, Cisco Skinny Call Control Protocol (SCCP), SpectraLink Voice Priority (SVP), SIP, H.323, Vocera, and Wi-Fi Calling.	Supports SIP RFC 3261.	Not supported	Supports SIP and Microsoft Lync/Skype for Business.
WPA/WPA2 and OKC-based fast roaming	Improving mobile network access experience	Supported	Supported	N/A	Supported
Voice and video service identification	Improving packet forwarding priorities	Supported (forwarding priority of voice packets: 46;	N/A	N/A	Supported

Function	Description	Company H	Company C	H3C	Huawei
enabled by default		forwarding priority of video packets: 34)			
Dynamic EDCA parameter adjustment based on voice and video enhancement	Improving air interface performance	Not supported	Not supported	Not supported	Supported
Radio bandwidth reservation for voice users	Call Admission Control (CAC)	N/A	Supported	Not supported	Not supported
Voice user access control	CAC	N/A	Supported	Not supported	Supported
Radio-based control of the number of video users	CAC	N/A	Supported	Not supported	Not supported
Visualized O&M: supporting collection of statistics on the delay, jitter, packet loss, and MOS	Improving O&M capabilities	Supported	Not supported	Not supported	Supported

5.3 Typical Networking and Applications of mDNS

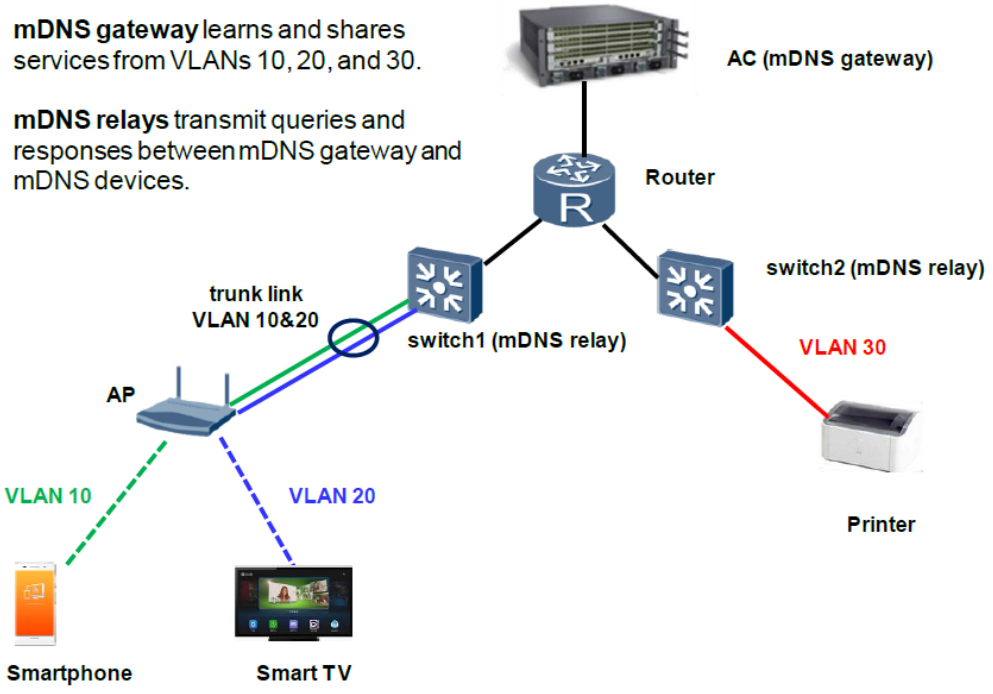
Depending on locations of mDNS devices and the WLAN AC, mDNS can be applied in three typical networking modes.

5.3.1 Networking with mDNS Relay

When mDNS devices connect to a WLAN AC through a Layer 3 network, the mDNS relay component is required to forward mDNS traffic to the WLAN AC.

Figure 5-2 shows the typical networking with mDNS relay devices. In this networking, the smartphone, smart TV, and printer are located in different VLANs or network segments, and a router is deployed between the terminals and the WLAN AC. The mDNS relay devices forward mDNS service advertisements and query requests. The mDNS gateway records services on the network and responds to query requests.

Figure 5-2 Networking with mDNS relay


mDNS gateway learns and shares services from VLANs 10, 20, and 30.
mDNS relays transmit queries and responses between mDNS gateway and mDNS devices.
AC (mDNS gateway)
Router
switch2 (mDNS relay)
trunk link
VLAN 10&20
switch1 (mDNS relay)
VLAN 30
AP
VLAN 10
VLAN 20
Printer
Smartphone
Smart TV

The WLAN AP uses the direct forwarding mode. It converts wireless traffic sent from the smartphone and smart TV into wired network traffic and sends the traffic to switch 1. The WLAN AP and switch 1 use trunk interfaces to send packets of the two VLANs. With the mDNS relay function enabled, the switches change destination IP addresses of mDNS packets in each VLAN into a unicast address, and then send the packets to the WLAN AC. The WLAN AC maintains the service information and responds to query requests. In this way, terminals can discover services in different VLANs and network segments.

In this scenario, you need to perform the following configurations:

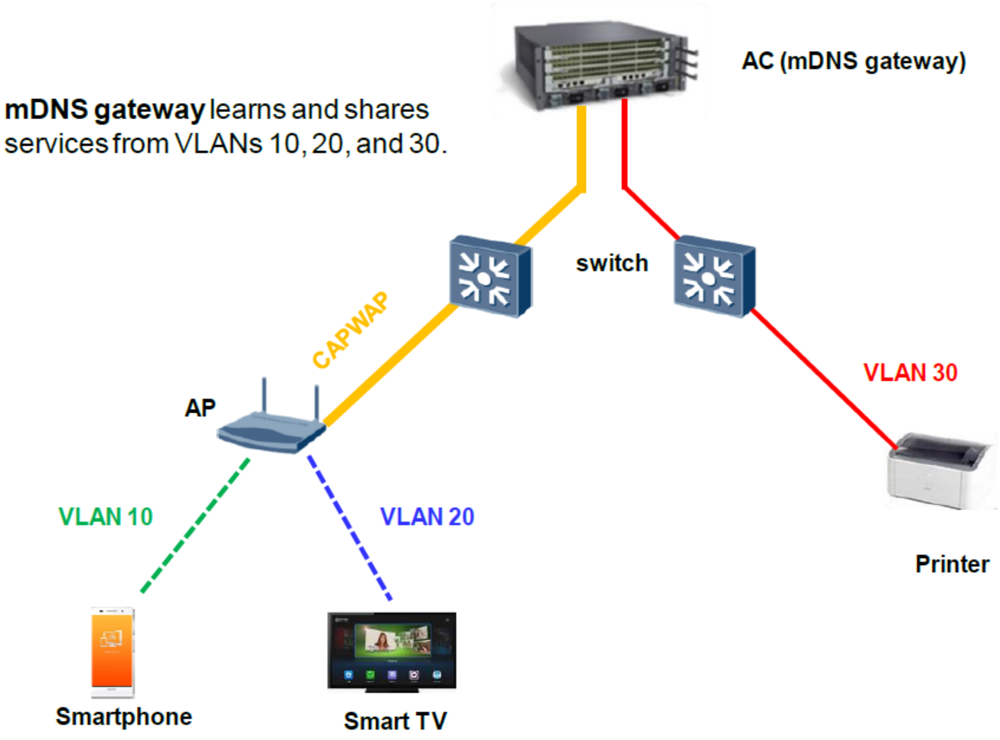
- Enable the mDNS gateway function on the WLAN AC.
- On switch 1, configure the gateway IP address and enable the mDNS relay function in VLAN 10 and VLAN 20.
- On switch 2, configure the gateway IP address and enable the mDNS relay function in VLAN 30.

5.3.2 Networking Without mDNS Relay

When mDNS devices are located in the same VLAN or network segment as the WLAN AC, mDNS relay is not required.

Figure 5-3 shows the networking without mDNS relay. The smartphone, smart TV, and printer are located in different VLANs, but they are in the same VLAN as the WLAN AC (or connected to the WLAN AC through CAPWAP tunnels). The mDNS gateway records services on the network and responds to query requests.

Figure 5-3 Networking without mDNS relay



The WLAN AP uses the centralized forwarding mode, and forwards traffic from the smartphone and smart TV to the WLAN AC through the CAPWAP tunnel. The printer is also in the same VLAN as the WLAN AC. The switch between the printer and WLAN AC forwards traffic following the normal Layer 2 forwarding process. With the mDNS gateway function enabled, the WLAN AC maintains services in VLANs 10, 20, and 30, and responds to query requests, allowing service discovery across VLANs and network segments.

After mDNS devices discover services using the mDNS protocol, traffic of the corresponding applications is not processed by the mDNS protocol, and the mDNS gateway does not participate in service traffic forwarding. Therefore, a routing module is required to forward service traffic across VLANs and network segments. The routing function can be implemented by configuring VLANIF interfaces on the WLAN AC or deploying a router.

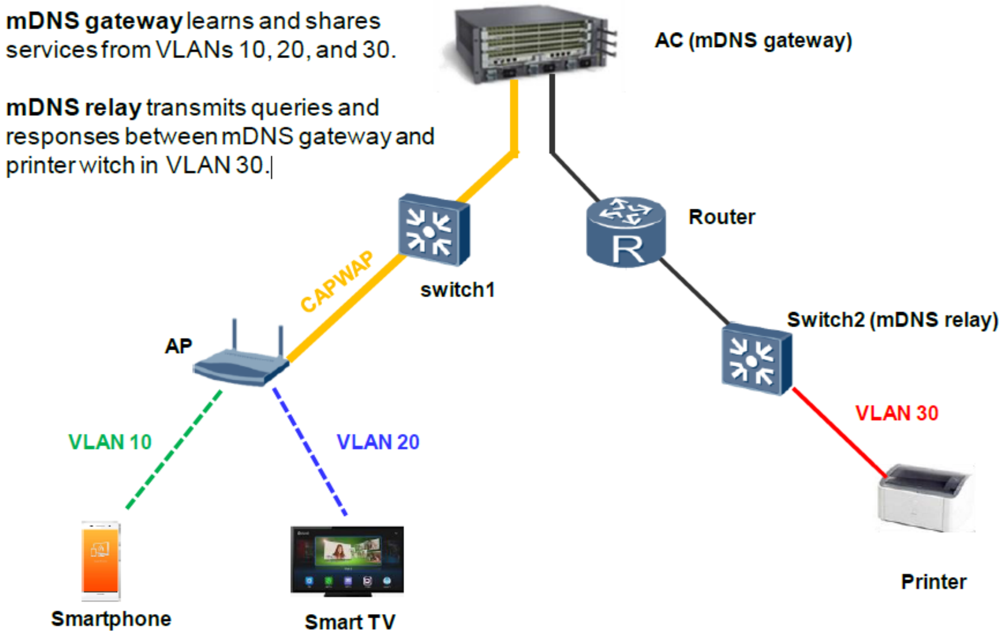
In this scenario, you need to enable the mDNS gateway function on the WLAN AC.

5.3.3 Hybrid Networking

In a hybrid networking, some mDNS devices belong to the same VLAN as the WLAN AC, while mDNS devices do not. In this case, deploy mDNS relay for the terminals that do not belong to the same VLAN as the WLAN AC.

Figure 5-4 shows the hybrid networking.

Figure 5-4 Hybrid networking


mDNS gateway learns and shares services from VLANs 10, 20, and 30.
mDNS relay transmits queries and responses between mDNS gateway and printer witch in VLAN 30.
AC (mDNS gateway)
Router
switch1
CAPWAP
AP
Switch2 (mDNS relay)
VLAN 30
VLAN 10
VLAN 20
Printer
Smartphone
Smart TV

In this scenario, you need to perform the following configuration:

- Enable the mDNS gateway function on the WLAN AC.
- On switch 2, configure the gateway IP address and enable the mDNS relay function in VLAN 30.

A Acronyms and Abbreviations

Numerics	
802.11e	802.11e user priority
802.1p	802.1p priority
A	
AC	Access Controller
AP	Access Point
AIFSN	Arbitration Inter Frame Spacing Number
B	
BSSID	Basic Service Set Identifier
C	
CAPWAP	Control And Provisioning of Wireless Access Points
CSMA/CA	Carrier Sense Multiple Access with Collision Avoidance
D	
DSCP	Differentiated Services Code Point
E	

ECWmin	Exponent form of CWmin
ECWmax	Exponent form of CWmax
EDCA	Enhanced Distributed Channel Access
M	
mDNS	multicast DNS
Q	
QoS	Quality of Service
R	
regex	Regular expressions
RTMP	Real Time Messaging Protocol
S	
SAC	Smart Application Control
SCCP	Skinny Call Control Protocol
SIFS	Short Interframe Space
SIP	Session Initiation Protocol
SSID	Service Set Identifier
V	
VAP	Virtual AP
W	
WLAN	Wireless Local Area Networks
WPA	Wi-Fi Protected Access
WMM	Wi-Fi Multimedia

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