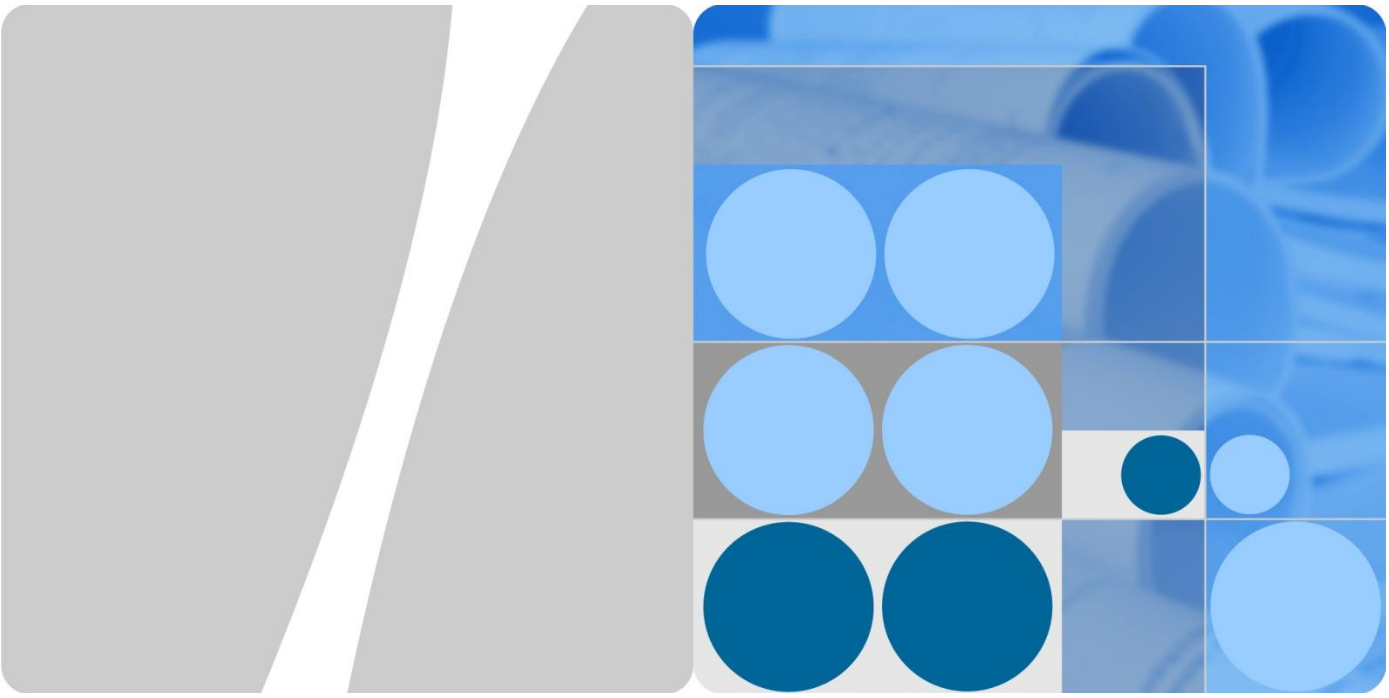


WLAN Application Identification Technology White Paper

Issue 1.0

Date 2015-06-04

HUAWEI TECHNOLOGIES CO., LTD.

Trademarks and Permissions

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: http://www.huawei.com

Email: support@huawei.com

WLAN Application Identification Technology White Paper

Keywords: WLAN, application identification, policy control

Abstract: Huawei WLAN network device uses a smart application identification and classification engine to detect and identify the contents of Layer 4 to Layer 7 and dynamic protocols such as HTTP, FTP, and RTP in the packets. After that, the devices can identify the service and application traffic on a network and implement refined QoS policy control based on classification and analysis results.

Acronyms and abbreviations

Abbreviation	Full Spelling
WLAN	Wireless LAN
Regex	Regular expression
SAC	Smart Application Control
VAP	Virtual Access Point

Contents

Figures

1 Application Identification Overview

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 service applications on intelligent 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 the 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.

1.2 Application Identification Technologies

Application visualization 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

1.3 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 administrator needs to control the specified application traffic, including discarding the traffic, setting the priority, or limiting the rate.

2 Key Technology Implementation

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 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 Basic Principles

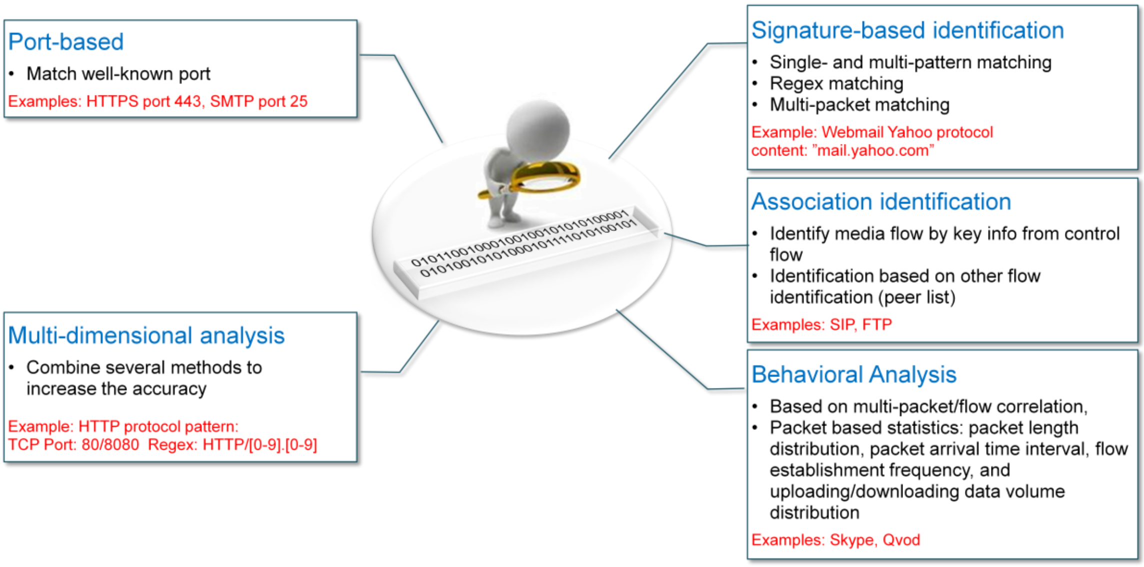
An application identification technology first identifies the application and service traffic on a network. The system then implements the following application and policy control based on identification results so that the administrator can manage and control the network more easily, flexibly, and effectively.

1. The built-in application identification function on an 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 Application Identification Technologies

Huawei uses a smart application and service identification technology to achieve application visualization, 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

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

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

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

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.

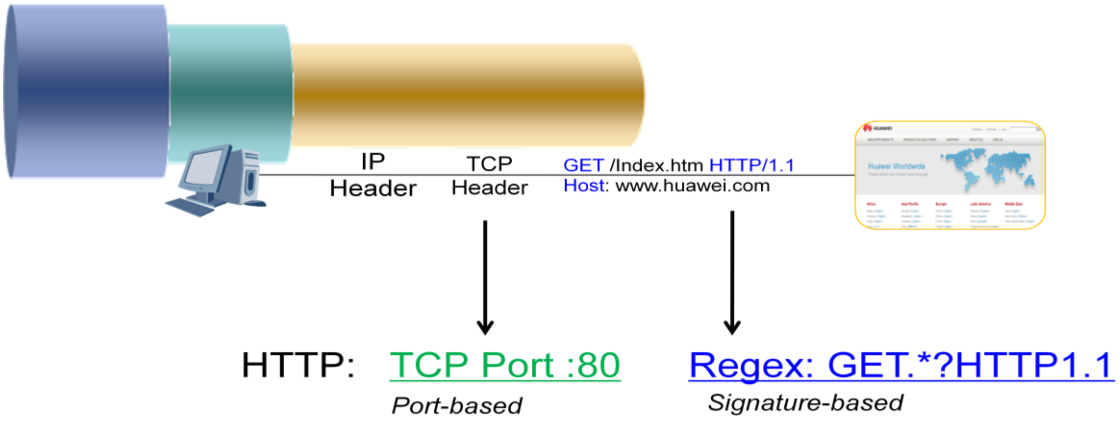
2.2.2 Signature-based Identification

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



Multiple identification methods are often used to increase the identification accuracy. For example, HTTP identification based only on port 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 signature.

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:

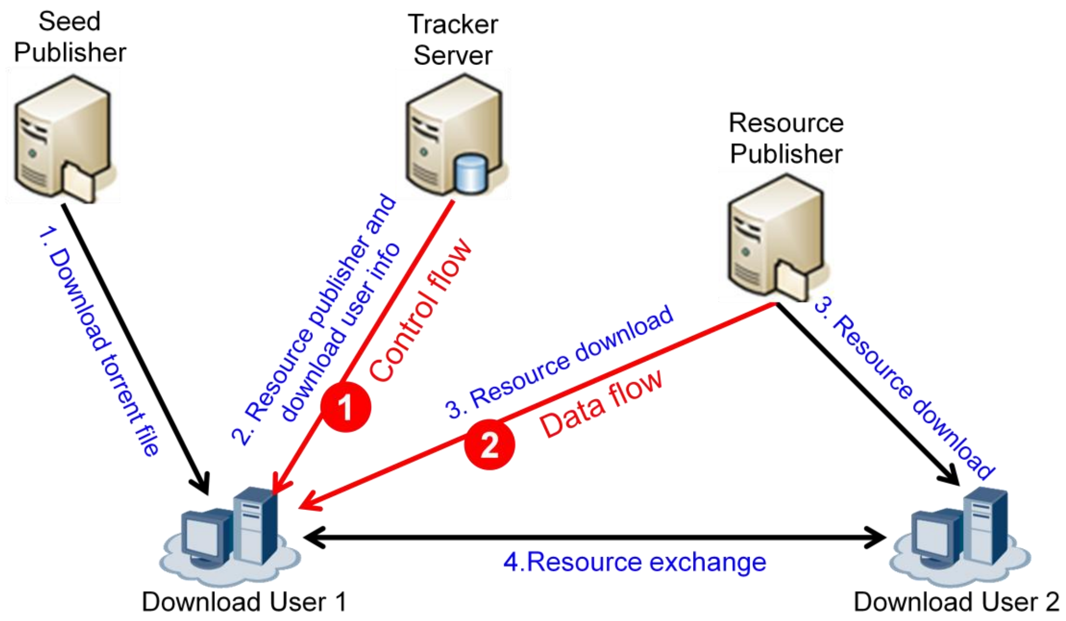
- Identify media flows based on control flow information.
- Identify applications based on other flows (such as P2P data flow).

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



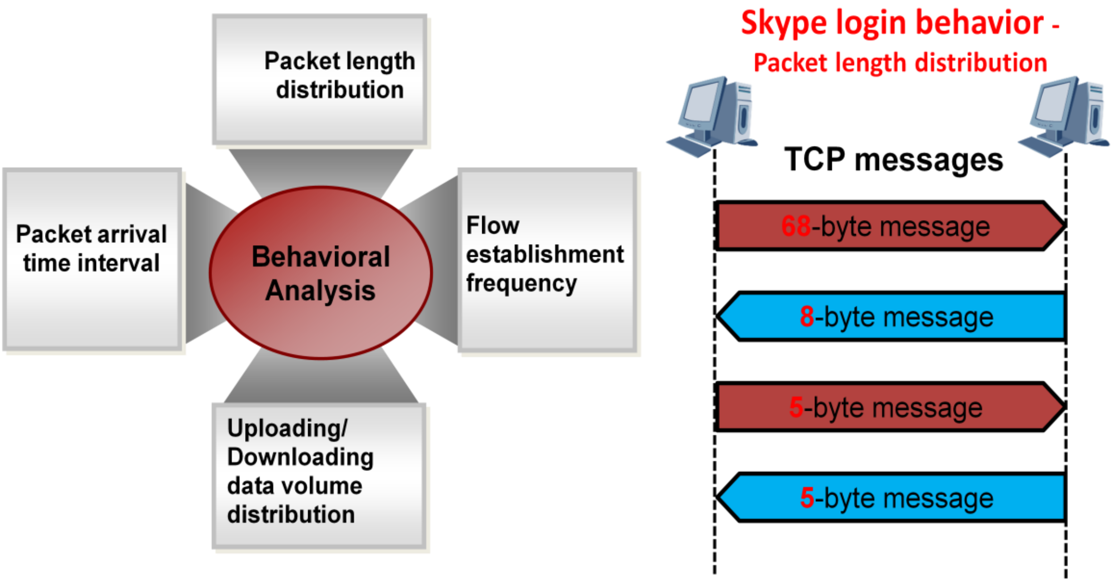
2.2.4 Behavior Analysis-based Identification

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.

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

2.3 Application Traffic Statistics Collection

Application visualization 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 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 visualization 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

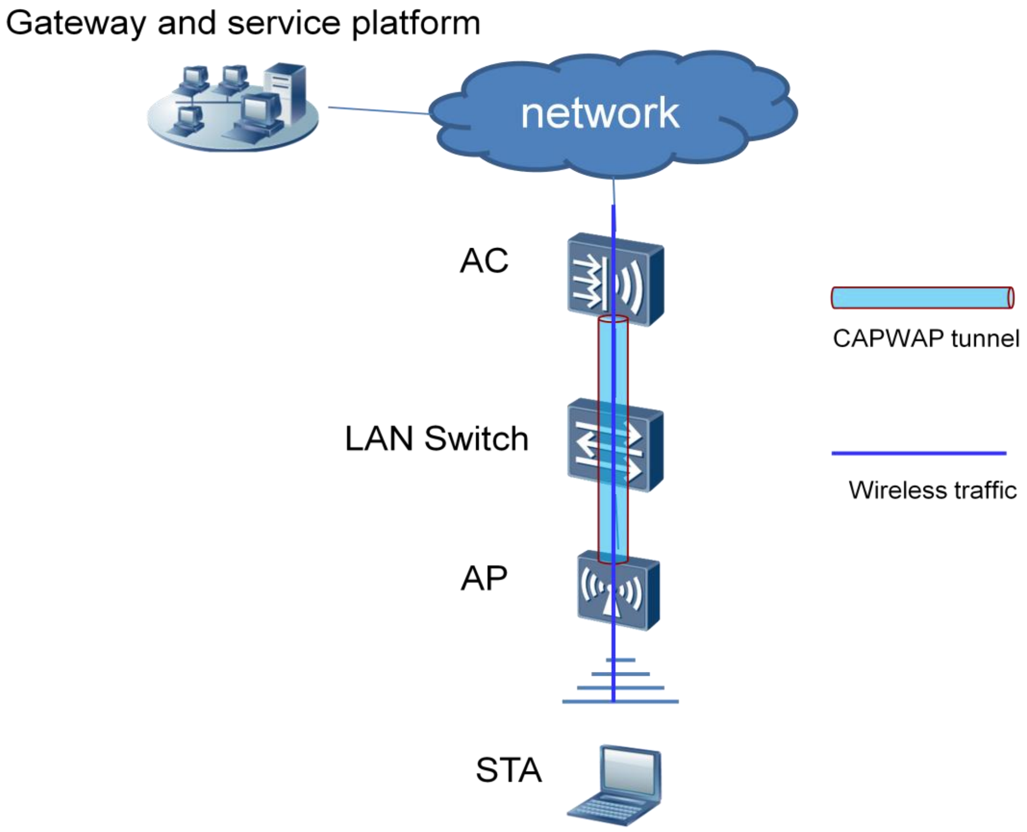
Bandwidth throttling policy is applied to specify an upper limit of the bandwidth allocated to an application. The administrator can set bandwidth upper limits for different applications to specify proportions of various application traffic on a network.

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 Network Deployment and Application

3.1 Networking for WLAN Application Identification

Figure 3-1 Networking diagram for WLAN application identification



Huawei application identification function is supported only on 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 AC. The AC can be connected in bypass mode or inline mode.

It should be noted that on a Huawei independent AC, the application identification function can only be enabled on a wireless port (VAP port) but 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 an AC is connected in inline mode, the traffic passing through a wired port cannot be identified.

On current Huawei WLAN network, an 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 visualization is configured on an AC in a centralized forwarding WLAN networking. After going online on an AP, a user starts various applications on the STA to access the network. The AC analyzes packet flows sent from users to obtain network resource usage of the users' applications. Then the 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.

3.2 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 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.
6. Run a command to check the application traffic statistics.

3.3 Reporting Application Visualization 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 visualization 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 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.

3.4 Implementation of the Application-based Policy Control

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

3.4.1 Setting the Priority for an Application

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 packets of the application the priority of which is to be modified.
4. Configure the AC to analyze and identify the traffic of the user.
5. Set the priority for the identified application traffic.

3.4.2 Limiting the Access of an Application

1. Enable application visualization in the service set profile view.
2. Enable a user associated with the corresponding VAP to access a network.

   Configure the application packets that are to be discarded.
3. Configure the AC to analyze the user's traffic and discard the packets of the specified application.
4. Enable the user to use the application to access the network. The traffic cannot be forwarded.

3.4.3 Setting Bandwidth for an Application Flow

1. Enable application visualization 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 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.