

WLAN Spectrum Analyzer Technology White Paper

Issue 01
Date 2013-05-10

Copyright © Huawei Technologies Co., Ltd. 2013. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

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

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

Huawei Technologies Co., Ltd.

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

Website: <http://enterprise.huawei.com>

About This Document

Purpose

This document describes WLAN Spectrum Analyzer (WSA) technology in V200R003C00 of Huawei wireless access devices. WSA technology identifies interference sources of different types on the WLAN for users to rectify faults, increase the throughput, and improve user experience.

This document provides the WSA working mechanism and technical implementation. In addition, the WSA configuration is described.





Intended Audience


This document is intended for:

- Data configuration engineers
- Commissioning engineers
- Network monitoring engineers
- System maintenance engineers

Symbol Conventions

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

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

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

Change History

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

Issue 01 (2013-05-10)

This is the first official release.

Contents

About This Document.....	ii
1 WSA.....	1
1.1 Overview	1
1.2 Availability.....	1
1.3 Technology Description	2
1.3.1 Introduction.....	2
1.3.2 Architecture.....	4
1.3.3 Implementation	6
2 WSA Configuration	10
2.1 Configuration Roadmap.....	10
2.2 Configuration Procedures	10
2.3 Configuration File.....	11

1 WSA

1.1 Overview

Definition

WLAN Spectrum Analyzer (WSA) technology identifies interference sources of different types on the WLAN for users to rectify faults and improve user experience.

Purpose

802.11 wireless technology has been widely used in home, small office and home office (SOHO), and enterprise networks. Users can easily access the Internet over WLANs. 802.11 technology uses public spectrum resources, which are also used by other wireless devices, such as Bluetooth devices and cordless phones. Wireless signal conflict and interference occur on the WLAN, disconnecting users and making the network unstable. WSA technology detects these interference sources for users to rectify faults and obtain a wireless network without interference.

Benefits

WSA detects interference sources of different types on the WLAN to locate and rectify faults.

1.2 Availability

Products and Versions

Table 1-1 Mapping between the products and versions

Product	Model	Version
AC	AC6605	V200R003C00
	AC6005	V200R003C00

Product	Model	Version
AP	AP6x10 AP7x10	V200R003C00

1.3 Technology Description

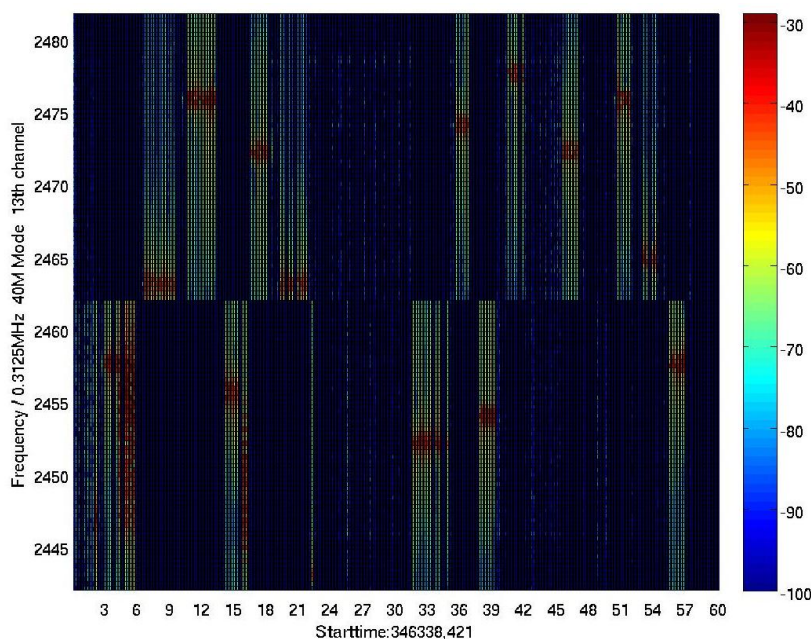
1.3.1 Introduction

WSA technology detects interference sources of different types on the WLAN. Based on the frequency, interference sources can be classified into frequency hopping devices and fixed-frequency devices.

Frequency Hopping Devices

Frequency hopping devices, such as cordless phones, Bluetooth devices, and game controllers, feature changing frequencies. Figure 1-1 shows the spectrum diagram of a Bluetooth device with the abscissa indicating time and the ordinate indicating frequency. Red squares in the diagram indicate the signal strength of the Bluetooth device. In 6s to 9s, the frequency is 2465 MHz; in 9s to 12s, the frequency is 2475 MHz; in 12s to 15s, the frequency is 2465 MHz; in 15s to 18s, the frequency is 2475 MHz; in 18s to 21s, the frequency is 2465 MHz; in 21s to 24s, the frequency is 2475 MHz; in 24s to 27s, the frequency is 2465 MHz; in 27s to 30s, the frequency is 2475 MHz; in 30s to 33s, the frequency is 2465 MHz; in 33s to 36s, the frequency is 2475 MHz; in 36s to 39s, the frequency is 2465 MHz; in 39s to 42s, the frequency is 2475 MHz; in 42s to 45s, the frequency is 2465 MHz; in 45s to 48s, the frequency is 2475 MHz; in 48s to 51s, the frequency is 2465 MHz; in 51s to 54s, the frequency is 2475 MHz; in 54s to 57s, the frequency is 2465 MHz; in 57s to 60s, the frequency is 2475 MHz.

Figure 1-1 Spectrum of a frequency hopping device



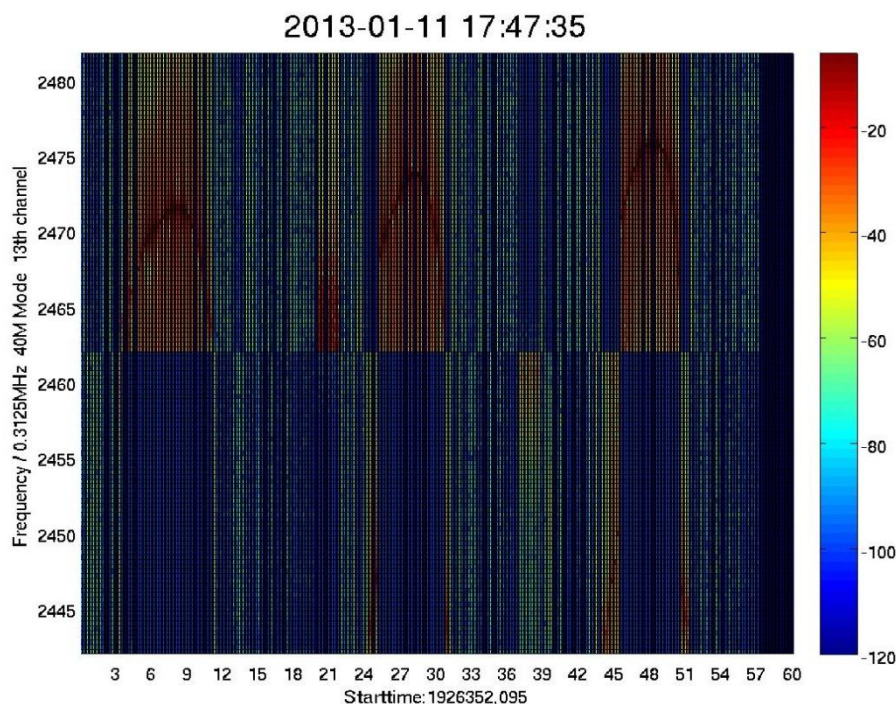
Fixed-Frequency Devices

Fixed-frequency devices, such as microwave ovens, wireless cameras, and wireless audio and video transmitters, feature unchanged frequency. Based on the occupied bandwidth, fixed-frequency devices can be classified into broadband devices and narrowband devices.

- Broadband devices

A broadband device, such as a microwave oven, occupies high bandwidth and low duty cycle and covers multiple channels including channels 11, 12, and 13. Figure 1-2 shows the typical real-time spectrum diagram of a microwave oven with the abscissa indicating time and the ordinate indicating frequency.

Figure 1-2 Spectrum of a broadband device

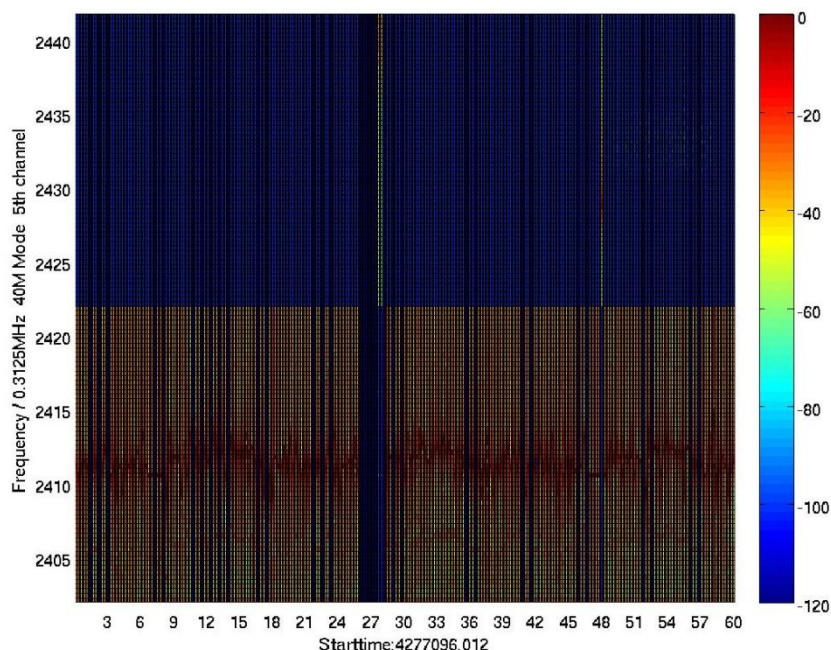


As shown in the preceding figure, the microwave oven has the characteristics of the broadband device and obvious frequency sweep feature, that is, the central frequency point flaps up and down. The frequency sweep feature is essential in device recognition.

- Narrowband devices

A narrowband device, such as a wireless camera, wireless audio and video transmitter, and baby monitor, occupies low bandwidth and high duty cycle. Figure 1-3 shows the typical real-time spectrum diagram of a baby monitor with the abscissa indicating time and the ordinate indicating frequency.

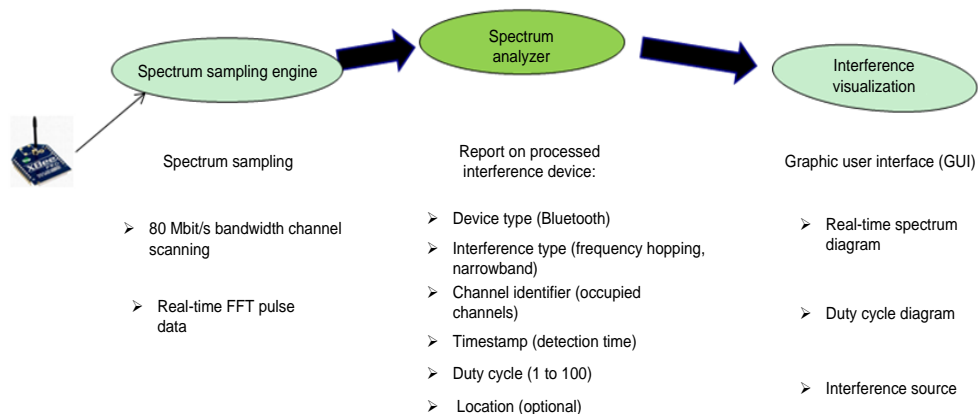
Figure 1-3 Spectrum of a narrowband device



1.3.2 Architecture

Figure 1-4 shows the WSA architecture.

Figure 1-4 WSA architecture



WSA includes the following components:

- Spectrum sampling engine: collects and transmits spectrum information of the WLAN to the spectrum analyzer. The spectrum sampling engine works in three modes:
 Monitor mode: The radio to which the spectrum sampling engine belongs is used specifically to collect real-time spectrum data. Generally, the radio periodically switches channels to scan the whole frequency band, for example, channels 1 to 13 on the 2.4

GHz frequency band. Note that users cannot access the radio in this mode to prevent service interruption.

Hybrid mode: The radio to which the spectrum sampling engine belongs is used to transmit user service traffic at most of the time and collect spectrum data for a short period of time (for example, 100 ms in 30s). Note that the spectrum sampling engine controls the radio to switch to different channels for collecting spectrum data of the whole channel.

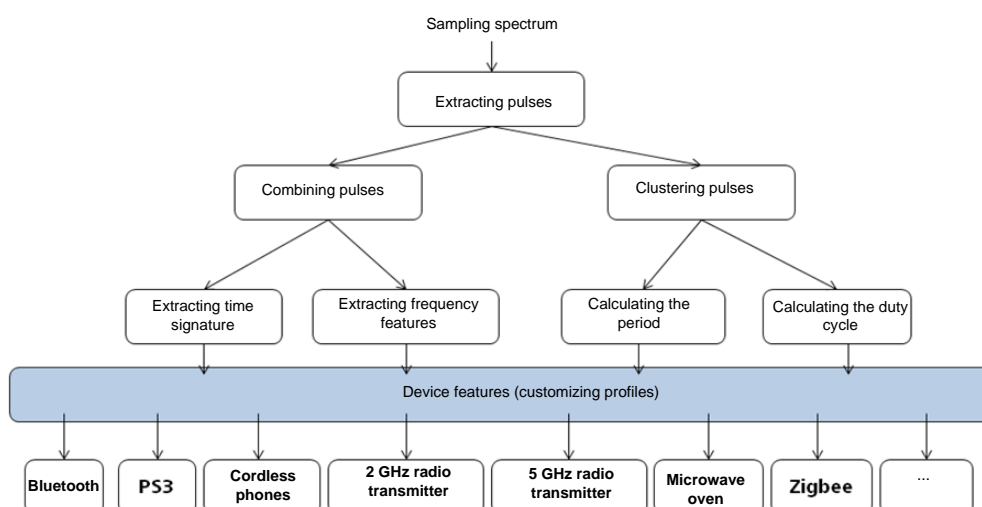
Local mode: The spectrum sampling engine and the radio to which the spectrum sampling engine belongs are on the same channel, that is, the spectrum sampling engine does not control the radio to switch to different channels. In this mode, services are not interrupted.

- **Spectrum analyzer:** analyzes spectrum data, identifies interference source type, and sends the report on the interference device to the interference visualization module. The spectrum analyzer uses the decision tree algorithm. It extracts all effective pulses in the sampling period from spectrum sampling data, and combines or clusters the pulses. After pulse combination, a specific time signature and frequency characteristics are generated, and after pulse clustering, the spectrum period and duty cycle can be calculated. By comparing these characteristics with characteristics of devices, the spectrum analyzer can identify the interference device type.

After identifying the interference device, the spectrum analyzer generates a report on the interference device with the following parameters: device type, interference type, channel identifier, detected timestamp, and duty cycle (optional).

Figure 1-5 shows the working process of the spectrum analyzer.

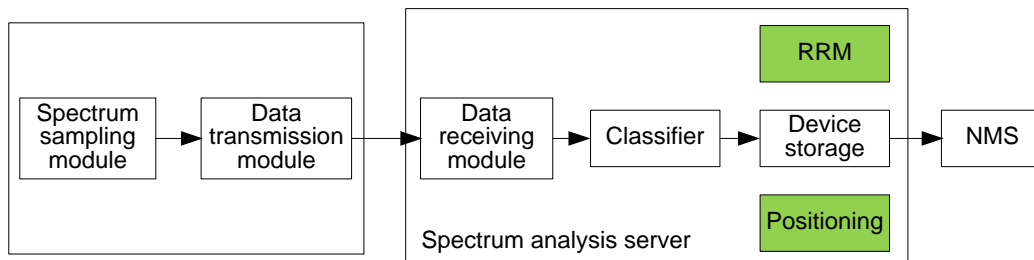
Figure 1-5 Working process of the spectrum analyzer



- **Interference visualization:** displays information about interference sources in graphic mode, including alarms and real-time spectrum diagrams.

1.3.3 Implementation

Figure 1-6 Working process of the spectrum analyzer



Spectrum Sampling Module

The spectrum sampling module scans and samples signals to generate FFT data.

- Spectrum scanning
 - Hybrid mode
 - The hybrid mode includes two working mechanisms. The spectrum sampling module scans and collects spectrum data only on its working channel. Usually, the working channel, especially the 2.4 GHz radio, uses the 20M bandwidth. Therefore, a little frequency data is available and the interference identification accuracy in this mode is lower than that in the monitor mode. It is difficult for the spectrum scanning module to identify a frequency hopping device that works on other channels other than the working channel.
 - The spectrum sampling module can also scan spectrum data by time sequence. For example, one minute after the module works on its working channel, it switches to channel 1 to scan data for 100 ms; it then switches back to the working channel; after working for 1 minute, it switches to channel 2 to scan data for 100 ms, and so on. After the frequency band is scanned, the module analyzes the spectrum data to identify interference sources. When the module uses this working mechanism to scan data, services are slightly affected. Since the data of a whole frequency band is scanned and collected, the interference identification accuracy is high. By default, this working mechanism is preferred when the spectrum sampling module works in hybrid mode.
 - Monitor mode
 - In monitor mode, the spectrum sampling module only scans data in the frequency band but does not transmit services. Use 2.4 GHz as an example. The 80M bandwidth band is divided into two 40M sub-bands (5 or 13) or divided into 13 sub-bands by channel. The module scans one sub-band for 1s every time.
- Spectrum sampling
 - Raw frequency sampling data is obtained through the spectrum scanning process. Each collected data sample includes a group of sub-bands. Each sub-band has a bandwidth of 312.5 kHz (sub-band bandwidth of Atheros chip is used as an example. The sub-band bandwidth may vary according to chips). When a 20 MHz bandwidth band is scanned, the data sample includes 56 sub-bands; when a 40 MHz bandwidth band is scanned, the data sample includes 128 sub-bands. The data sample also includes high-precision time stamp and real-time noise level used to identify interferences.

Data Transmission Module

The data transmission module packs spectrum data collected by the AP and sends the data to the spectrum analysis server.

Assume that the spectrum collection period is 100 ms, each sampling point has 56 FFT bins or 128 FFT bins (bin indicates the signal energy), and an AP collects data of about 300 sampling points in the spectrum collection period, the AP collects a large amount of data and needs to fragment the data into multiple packets before sending the data.

Data Receiving Module

The data receiving module receives data collected by the AP and sends the data to the spectrum analysis module for processing.

The AP sends data in packets and adds the start flag to the first packet and end flag to the last packet. However, in consideration of packet loss, a timer must be enabled when the server starts to receive the packets. If the server does not receive all packets in the period specified by the timer or the number of lost packets exceeds the allowed range, this spectrum analysis is canceled.

Classifier

The classifier identifies interference sources and classifies the collected spectrum sampling data.

As shown in Figure 1-5, the classifier works based on the decision tree algorithm. Its working process includes extracting pulses, combining pulses, clustering pulses, extracting time signature, extracting frequency features, calculating the cluster period, calculating the duty cycle, and identifying device features.

Extracting Pulses

Each data sample includes a group of sub-bands but not all sub-bands are valid. A pulse refers to a collection of valid sub-bands included in the collected spectrum sampling data.

Extracting pulses include searching for a candidate pulse peak, identifying candidate pulses, and filtering pulses.

Step 1: Search for a pulse peak from the spectrum sampling data using either of the following algorithm.

- Ranking algorithm: rank the sub-bands and choose the sub-band with the highest energy as a candidate pulse peak.
- Threshold-based algorithm: set an energy threshold and choose sub-bands with energy higher than the threshold as candidate pulse peaks.

Step 2: Identify pulses based on the pulse peak. Find valleys (lowest energy points) on the left and right side of the pulse peak and calculate the center frequency and bandwidth of the candidate pulses.

Step 3: Filter pulses based on the center frequency and bandwidth and discards candidate pulses whose center frequency and bandwidth do not meet requirements.

Combining Pulses

Combine consecutive pulses that have similar center frequency and bandwidth, and modify the center frequency and bandwidth of the combined pulses.

The pulses are combined as a frame. All frames of a group of spectrum sampling data form a pulse sequence.

Clustering Pulses

Consecutive pulses are combined into a pulse cluster.

Extracting Time Signature

Compute the time width of the combined pulses.

Extract frames with similar time width and form a pulse sequence. This process is called time signature.

Extracting Frequency Features

Extract frames with similar frequency bandwidth and form a pulse sequence.

Calculating the Cluster Period

There are two computing formulas:

Cluster period = Start time of the latter cluster – Start time of the former cluster

Cluster period = End time of the latter cluster – End time of the former cluster

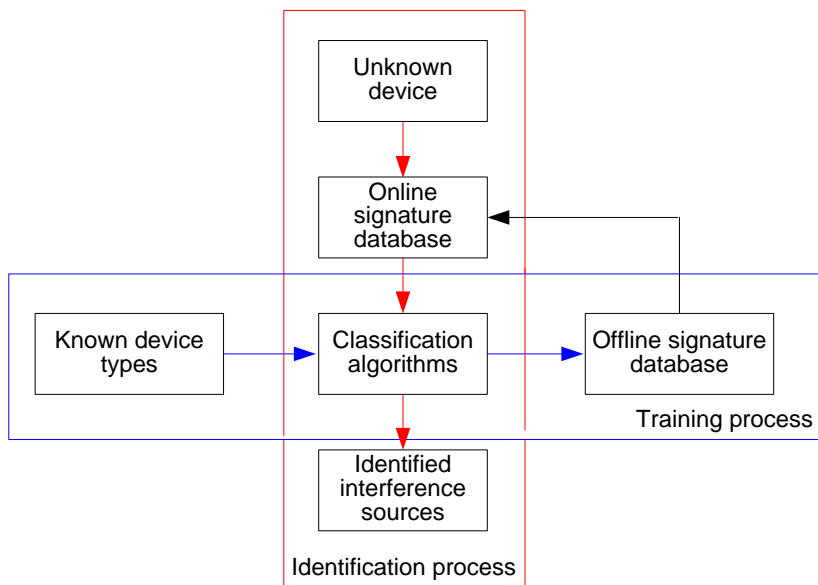
Calculating the Duty Cycle

Duty cycle = Cluster time width / (Cluster time width + Time width between clusters)

Identifying Device Features

After obtaining the preceding features, compare the obtained features with interference source features in the signature database to identify interference device type.

Figure 1-7 shows the working process of the classifier which includes the training process, identification process, and signature database.



Training Process

Usually, the training process is carried out in the lab to detect and analyze radio signals of known interference devices, such as Bluetooth and microwave ovens. The classifier obtains the device features through analysis and adds the mapping relationships <Interference device, Device features> to the signature database.

Identification Process

When detecting radio signals of unknown interference devices, network devices report the signals to the classifier. The classifier analyzes the device features and searches for the corresponding mapping relationship <Interference device, Device features> to obtain the device type.

Signature Database

Offline signature database and online signature database are available. The offline signature database contains device features obtained during the training process. The offline signature database is loaded to the network devices through remote control to generate an online signature database. If the corresponding license has been installed, a signature database that contains features of common interference devices has been loaded on the devices before the devices are delivered.

Storage, Display, and Report

If device identification is performed on the AC, the AC stores and displays information about the detected devices and provides MIB query interface. The AC also reports alarms to the NMS, but alarms must be suppressed.

Alarms reported to the NMS provide the following parameters:

- ID and MAC address of the detecting AP
- Device type
- Interference type
- Radio identifier
- Center frequency
- Bandwidth
- Duty cycle
- Detection interval

2 WSA Configuration

2.1 Configuration Roadmap

You can configure WSA on an AC or a specialized spectrum analysis server. If WSA is enabled on an AC, configure the IP addresses and interfaces for a spectrum analysis and a drawing server. The drawing server is used to draw the spectrum diagram.

2.2 Configuration Procedures

- Step 1** Configure an IP address and a listening port for the spectrum analysis server (currently, only the AC can function as a spectrum analysis server).

```
[AC-wlan-view] spectrum-analysis ap-report-server ac port 6000
```

- Step 2** Enable spectrum analysis and configure the AP radio to work in monitor mode.

```
[AC-wlan-radio-0/0] spectrum-analysis enable
```

Step 1 and step 2 are mandatory. After the two steps are performed, run the **commit** command to deliver the configuration to the AP. Then, spectrum analysis can be enabled.

Configure the spectrogram server (currently, only eSight can function as the spectrogram server).

- Step 3** [AC-wlan-view] spectrum-analysis spectrogram-server ip-address 10.138.20.1 port 6000 Enable the spectrum sever to report spectrum data.

The AC reports real-time spectrum data detected by AP only after this command is executed. The spectrogram server can then display corresponding spectrum graphs.

```
[AC-wlan-radio-0/0] spectrum-analysis spectrogram-server-report enable
```

- Step 4** Set a scanning period for spectrum analysis. The value ranges from 60 to 100, in milliseconds. The default value is 60.

```
[AC-wlan-radio-prof-test] spectrum analysis scan-time 80
```

- Step 5** Set a scanning interval for spectrum analysis. The value ranges from 10 to 180, in seconds. The default value is 10.

```
[AC-wlan-radio-prof-test] spectrum analysis scan-frequency 30
```

Step 6 Set the aging time of the non-Wi-Fi device. The value ranges from 1 to 30, in minutes. The default value is 3.

```
[AC-wlan-view] spectrum-analysis non-wifi-device aging-time 5
```

Step 7 Display the detected non-Wi-Fi devices.

```
<AC> display wlan non-wifi-device all
-----
Detect Non-WiFi-device ApID      : 2
Detect Non-WiFi-device RadioID   : 0
Detect Non-WiFi-Device type     : 4
Detect Non-WiFi-device Ap Channel : 1
Non-wifi-device name            : Bluetooth
Non-wifi-device frequency type   : hop Frequency
Non-wifi-device RSSI            : -71,-71,-70
Non-WiFi-device channel         : 5,4,3
Non-WiFi-device detect time last : 2013-04-11/09:13:47
Non-WiFi-device bandwidth(KHz)  : 7109
Non-WiFi-device duty            : 0
Non-WiFi-device interfere level  : 0
-----
```

Step 8 Display the IP address, monitoring port number, and aging time of the spectrum analysis server.

```
[AC-wlan-view]display wlan spectrum-analysis config
Spectrum analysis config:
-----
Spectrum analysis server IP      :192.168.120.1 (AC)
Spectrum analysis server udp-port :6000
Spectrogram server IP          :10.138.20.1
Spectrogram server udp-port     :6000
Spectrum analysis aging time (min) :5
-----
```

----End

2.3 Configuration File

```
#
vlan batch 88 100 to 104 300 to 301 1000 2000 4091
#
wlan ac-global country-code DE
#
dhcp enable
#
diffserv domain default
#
interface Wlan-Ess0
port hybrid pvid vlan 101
port hybrid untagged vlan 101
#
wlan
wlan ac source interface vlanif100
```



```
ap-auth-mode no-auth
ap id 4 type-id 17 mac cccc-8176-f040 sn 210235447410C9000028
wmm-profile name wp0 id 0
traffic-profile name tp0 id 0
security-profile name sp1 id 1
  security-policy wpa2
  wpa authentication-method psk pass-phrase cipher %$%$Jy1'xQ0CC5j^/ILvVdLy@J1%
service-set name ss3 id 3
  wlan-ess 0
  ssid AC119-3
  traffic-profile id 0
  security-profile id 1
  service-vlan 101
radio-profile name 80211bgn id 0
  radio-type 80211bgn
  wmm-profile id 0
spectrum-analysis scan-time 80
spectrum-analysis scan-frequency 30
ap 0 radio 0
  radio-profile id 0
  service-set id 3 wlan 1
  spectrum-analysis enable
spectrum-analysis spectrogram-server-report enable
spectrum-analysis ap-report-server ac port 6000
spectrum-analysis spectrogram-server ip-address 10.138.20.1 port 6000
spectrum-analysis non-wifi-device aging-time 5

#
```