WLAN Simulation Experiment Based on ENSP

Juan Chen¹, Xueqiang Zheng²*, Lei Zhang³, Laixian Peng⁴ and Xi Liu⁵

¹,²,³,⁴,⁵ Institute of Communications Engineering, Army Engineering University of PLA, Nanjing, Jiangsu, 210007, China

*Corresponding author’s e-mail: zxqq302@163.com

Abstract. WLAN technology is one of the main contents of computer network course. In order to enable students to better understand the principle of WLAN, this paper designs the experimental scheme of WLAN on the simulation platform eNSP, builds the experimental environment, realizes the interconnection of network by configuring AC and AP, and mobile users can roam in the wireless signal coverage area. At the same time, we use Wireshark to capture packets, analyse the principle of wireless access point control and configuration protocol, and verify the process of wireless terminal roaming. Through the experiment, the students’ understanding of WLAN technology principle is enhanced, and their practical ability and data analysis ability are also exercised.

1. Introduction

With the rapid development of wireless communication technology, WLAN is more and more widely used. WLAN has two definitions in broad and narrow sense: WLAN is a network composed of radio channels of various radio waves (such as laser, infrared, etc.) instead of some or all transmission media in wired local area networks; WLAN is defined as a LAN in narrow sense, which is based on the standard of 802.11 series of IEEE, using high frequency radio frequency (such as 2.4 GHz or 5 GHz band radio electromagnetic wave) as transmission medium. WLAN in our daily life refers to the narrow definition of WLAN. 802.11 series standards have become the mainstream technical standards of WLAN because of their relatively simple implementation technology, reliable communication, high flexibility and relatively low implementation cost. Moreover, 802.11 series standards have become synonyms of WLAN technical standards. [1]

2. Principles of WLAN

IEEE 802.11 is a general standard for WLAN. The WLAN standard announced by IEEE (the Institute of Electrical and Electronics Engineers) in 1997 is suitable for the communication between wired stations and wireless users or between wireless users. It defines the MAC (media access control) layer and the physical layer. The wireless terminal is connected to the network after running 802.11 protocol access AP (Wireless Access Point). The access process includes scanning, link authentication, identity authentication and association. AP is the HUB in the traditional wired network, and it is also the most commonly used device in the construction of small wireless local area network. AP is equivalent to a bridge connecting wired network and wireless network. Its main function is to connect various wireless network clients together and then connect wireless network to Ethernet.

WLAN has two basic architectures: [2]

One is FAT AP (FAT Access Point) architecture, which cannot only transmit radio frequency to provide wireless signal for wireless terminal access, but also independently complete security
encryption, user authentication and user management and other management functions. FAT AP is often the most suitable choice for use scenarios such as home WLAN or small business WLAN.

One is the FIT AP (FIT Access Point) architecture, which has no control function except providing radio frequency signals. In order to realize the function of WLAN, besides FIT AP, AC (Access Controller) which has the function of management and control is also needed. The main function of AC is to manage and control all FIT APs in WLAN. AC cannot transmit radio frequency signals, and cooperate with FIT AP to complete WLAN functions. It’s generally applicable to large and medium-sized use scenarios. According to the different regions and throughput controlled by AC, AC can appear in convergence layer or core layer, while FIT AP is generally deployed in access layer and enterprise branch.

Compared with home WLAN application scenarios, enterprises with larger number of users use centralized control to build WLAN networks. AC centralizes the management and control of associated APs in the network. CAPWAP (Control and Provision of Wireless Access Points) protocol runs between AP and AC, which makes AP configure from AC by establishing CAPWAP tunnel. Signal, it cooperates with AP to complete WLAN system function.

3. Introduction of eNSP
ENSP (Enterprise Network Simulation Platform) is a free, scalable and graphical enterprise network simulation software platform provided by Huawei. It mainly simulates enterprise network routers, switches, firewalls, WLAN and other devices. Its interface is friendly, and it can perfectly present the real equipment reality, support large-scale network scale, and give users the opportunity to model without real equipment. At the same time, the real network card can be used to realize the docking with the real network equipment, which can display the protocol interaction process more intuitively and facilitate users to learn network technology. [3]

4. Network simulation

4.1. Experimental purpose
The purpose of this simulation experiment is to make students understand the basic principle of WLAN and the process of CAPWAP session establishment, master the configuration method of AC and switch in simple WLAN, and understand the roaming state of mobile clients.

4.2. Scene and Requirements
The Academy has purchased an AP (AP2050) for each of the educational and personnel departments, and prepared an AC (AC6005) for management. Two APs add to the access layer switch (S3700), AC is connected to the convergence layer switch (S5700). The wireless access point is required to join the same VLAN and realize the roaming access of mobile clients. It is required to establish network topology, configure AC, configure convergence layer switch and access layer switch, and assign AP address by DHCP, so that mobile clients can roam and switch between different APs. The network topology is shown in figure 1, and the equipment address is shown in table 1. [4]
Table 1 Equipment Address

| Equipment | Interface /VLAN | IP address   | Subnet mask |
|-----------|----------------|-------------|-------------|
| S1(S5700)| GE0/0/1, VLAN 2| 192.168.2.1 | 255.255.255.0 |
|           | GE0/0/2, VLAN 10| 192.168.10.1| 255.255.255.0 |
|           | GE0/0/3, VLAN 1 | 192.168.1.1 | 255.255.255.0 |
|           | VLAN100         | 192.168.100.1| 255.255.255.0 |
| AC1(AC6005)| GE0/0/0, VLAN 2| 192.168.2.2 | 255.255.255.0 |
| R1(AR1220)| GE0/0/0, VLAN 1 | 192.168.1.2 | 255.255.255.0 |
|           | Loopback0      | 192.168.0.1 | 255.255.255.0 |

4.3. Experimental Simulation Procedures

4.3.1. Equipment Registration. Before building the network topology, in the menu bar, select the tool-registration device, check the box in front of all devices, and click on registration.

4.3.2. Equipment configuration

The IP address of GE0/0/0 interface is configured in router R1. Meanwhile the IP address of loopback 0 is configured to be used as the local loopback interface. Turn on the DHCP function and add it to VLAN 2. Set the GE 0/0/1 interface type and add it into VLAN 2.

```
[R1-GigabitEthernet0/0/0] ip address 192.168.1.2 24
[R1] interface loopback 0
[R1-LoopBack0] ip address 192.168.0.1 24
[AC] dhcp enable
[AC] vlan batch 2
[AC-GigabitEthernet0/0/1] port link-type access
[AC-GigabitEthernet0/0/1] port default vlan 2
```

Configure the IP address of VLAN 2, which is the gateway address of AP. DHCP server function of interface address pool mode is enabled and static routing is set.

```
[AC-Vlanif2] ip address 192.168.2.2 24
[AC-Vlanif2] dhcp select interface
[AC] ip route-static 0.0.0.0 0.0.0.0 192.168.2.1
```

Specify the source IP address of AC, that is, to build CAPWAP tunnel with AP.

```
[AC-wlan-view] capwap source interface Vlanif 2
```

Create various templates, including domain management module, radio frequency template, traffic
template, security template SSID template, VAP template, etc. The country code of AC can be set in the domain management module. When the RF template is successfully created, the parameters in the template are automatically configured to default values. After the security template is created, the parameters in the template are automatically configured as default values, and the default configuration is unauthenticated and unencrypted.

```
[AC-wlan-view]regulatory-domain-profile name TEST
[AC-wlan-regulate-domain-TEST]country-code cn
[AC-wlan-view]radio-2g-profile name TEST
[AC-wlan-view]radio-5g-profile name TEST
[AC-wlan-view]security-profile name TEST
[AC-wlan-sec-prof-TEST]security wpa psk pass-phrase !@#$%qwERTQWERT aes
```

In terms of security strategy, WPA (Wi-Fi Protected Access) encryption has four authentication modes: WPA, WPA-PSK, WPA2, WPA2-PSK. There are two encryption algorithms: AES (Advanced Encryption Standard) and TKIP (Temporal Key Integrity Protocol). Generally, on the home wireless router settings page, it always uses WPA-PSK or WPA2-PSK authentication type. The corresponding shared password can be set as long as possible, and after a period of time, change the shared password to ensure the security of the home wireless network.

SSID (Service Set Identifier) technology can divide a wireless local area network into several sub-networks which need different authentication. Only the authenticated users can enter the corresponding sub-network to prevent unauthorized users from entering the network. Generally, SSID is the name given to wireless networks. Here we create an SSID template named TEST and configure its name as TEST.

```
[AC-wlan-view]ssid-profile name TEST
[AC-wlan-ssid-prof-TEST]ssid TEST
```

VAP (Virtual Access Point) is a virtual AP on a physical entity AP. Each VAP provides the same functions as the physical entity AP. Users can create different VAPs on an AP to provide wireless access services for different user groups. By default, the service VLAN of VAP is VLAN 1, where the corresponding service VLAN 10 of VAP is specified.

```
[AC-wlan-view]vap-profile name TEST
[AC-wlan-vap-prof-TEST]forward-mode tunnel
[AC-wlan-vap-prof-TEST]traffic-profile TEST
[AC-wlan-vap-prof-TEST]security-profile TEST
[AC-wlan-vap-prof-TEST]ssid-profile TEST
[AC-wlan-vap-prof-TEST]service-vlan vlan-id 10
```

Create the AP group TEST, which is used to add the same configuration APs to the same AP group, referring to the domain management module and the VAP template.

```
[AC-wlan-vap-prof-TEST]ap-group name TEST
[AC-wlan-ap-group-TEST]regulatory-domain-profile TEST
[AC-wlan-ap-group-TEST]vap-profile TEST wlan 1 radio all
```

There are three authentication modes for AP: mac-auth is the MAC authentication mode, which is the default mode. No-auth is not authenticated. Sn-auth is an authentication mode of SN. Add AP corresponding to MAC address in AC and configure parameters, including naming, adding AP group, binding RF template, etc. Also set AP2 and bind it to ap-id 1, named test-2.

```
[AC-wlan-view]ap auth-mode mac-auth
[AC-wlan-view]ap-id 0 type-id 69 ap-mac 00E0-FC77-04E0
[AC-wlan-ap-0]ap-name jwbm
[AC-wlan-ap-0]ap-group TEST
[AC-wlan-ap-0]radio 0
[AC-wlan-radio-0/0]radio-2g-profile TEST
[AC-wlan-ap-0]ap-id 1 ap-mac 00E0-FC83-2E10
[AC-wlan-ap-1]ap-name rsbm
[AC-wlan-ap-1]ap-group TEST
[AC-wlan-ap-1]radio 0
```
In 2.4 GHz bandwidth, it has 83 MHz and is divided into 13 channels. Each channel has 22 MHz bandwidth, which means that these channels must have overlapping parts. In these channels, we can choose (1, 6, 11), (3, 8, 13) or (1, 5, 9, 13) to avoid channel overlapping. The default channel is Channel 1. In order to avoid the interference between the signal overlap areas of AP1 and AP2, the command is used to set the AP2 channel to Channel 6.

The next step is to configure the convergence layer switch S1. The method is shown below.

```bash
[S1]dhcp enable
[S1]vlan batch 2 10 100
[S1-GigabitEthernet0/0/1]port link-type access
[S1-GigabitEthernet0/0/1]port default vlan 2
[S1-GigabitEthernet0/0/2]port link-type trunk
[S1-GigabitEthernet0/0/2]port trunk allow-pass vlan 2 10 100
[S1-GigabitEthernet0/0/2]interface GigabitEthernet 0/0/3
[S1-GigabitEthernet0/0/3]port link-type access
[S1-GigabitEthernet0/0/3]port default vlan 1
[S1]interface Vlanif 1
[S1-Vlanif1]ip address 192.168.1.1 24
[S1]interface Vlanif 2
[S1-Vlanif2]ip address 192.168.2.1 24
[S1-Vlanif2]interface Vlanif 10
[S1-Vlanif10]ip address 192.168.10.1 24
[S1-Vlanif10]dhcp select interface
[S1-Vlanif10]interface Vlanif 100
[S1-Vlanif100]ip address 192.168.100.1 24
[S1-Vlanif100]dhcp select interface
[S1-Vlanif100]dhcp server option 43 sub-option 3 ascii 192.168.2.2
```

When Huawei devices are used as DHCP servers, DHCP server option 43 sub-option 3 needs to be configured. Option 43 refers to supplier-specific information, which enables terminal AP to acquire the IP address of wireless control by setting sub-option of DHCP server, so that AP can be registered on AC. The next step is to configure the access layer switch S2. The method is shown below.

```bash
[S2]vlan batch 2 10 100
[S2]interface GigabitEthernet 0/0/1
[S2-GigabitEthernet0/0/1]port link-type trunk
[S2-GigabitEthernet0/0/1]port trunk allow-pass vlan 10 100
[S2-GigabitEthernet0/0/1]interface Ethernet0/0/1
[S2-Ethernet0/0/1]port link-type trunk
[S2-Ethernet0/0/1]port trunk pvid vlan 100
[S2-Ethernet0/0/1]port trunk allow-pass vlan 2 10 100
[S2-Ethernet0/0/1]interface Ethernet0/0/2
[S2-Ethernet0/0/2]port link-type trunk
[S2-Ethernet0/0/2]port trunk pvid vlan 100
[S2-Ethernet0/0/2]port trunk allow-pass vlan 2 10 100
```

4.3.3. Check all AP's online status. After setting the parameters of each device, the wireless signal coverage is shown in figure 2. Double-click STA1 to connect the wireless network. After inputting the password we configured before, we can see in the Vap list that the channel of AP1 is the default channel 1, and the channel of AP2 is channel 6. Once set up, STA can be connected to AP via wireless signals. In order for STA to roam between two APs, the signal coverage of AP should overlap. As long as the password is properly configured, STA1 can automatically connect to the network during coverage movement. In figure 2, we can see the relevant information of the network, such as channel, radio frequency and rate, on the right side of the radio signal range.
4.4. Grab bag analysis
First, we stop running two APs, then restart AP1. At the same time, we capture packets on the link between S1 and S2. Then we filter the packets in the condition of "bootp or capwap". We can see the messages of DHCP and CAPWAP protocol, and get the results of grabbing as follows.

Messages 68-72 are AP1 to get the IP address and default gateway through DHCP, and to get the IP address of AC. Messages 93-94 are the discovery request sent by AP1 to AC and the discovery response of AC. In the response message, it will tell AP1 the number of AP on line, the maximum number of AP can be managed and the upper limit of the number of mobile terminals accessed. Messages 97-98 are the join request and the join response. Messages 101-102 are changes of status request and response messages. If AC returns the response messages, it completes the process of establishing control tunnel and enters the run state. When AC receives the Keep-Alive live message sent by AP1 and responds, it indicates that the data tunnel is established. AP1 enters the normal state and begins to work.

5. Conclusion
From the above experiments, we can verify the session establishment process of CAPWAP:
  - **AP acquires IP address.** If the static IP address isn’t configured after AP is powered on, it is necessary to obtain the IP address and default gateway address through DHCP.
  - **AP found AC.** AP uses AC discovery mechanism to know which AC is available, and decides to establish CAPWAP tunnel connection with the best AC.
- **Add operation.** During the interaction, AC checks the current version of AP, updates the version of AP if the version of AP does not match the requirements of AC, and checks the consistency of configuration if the version of AP meets the requirements.

- **Configuration consistency check.** Check the matching between the existing configuration of AP and the configuration of AC, and exchange configuration information between them.

- **AP running.** AP and AC have successfully established control and data tunnels. The WLAN configuration of AP receiving AC, such as creating WLAN, setting up channels, adjusting transmission power, and so on, has developed WLAN services.

**References:**

[1] Cao Xuefeng, Meng Wei, Chen Risheng, WLAN experimental design and Implementation Based on eNSP [J], Research and Exploration in Laboratory, Vol. 36 No. 7 Jul. 2017,

[2] Tu Wenjie, HCNA Network Technology Experiment Guide [M], August 2017

[3] Yang Bin, Simulation experiment of spanning tree protocol principle based on ENSP[J]. Software, 2017,38(2): 125-129

[4] Wang Da. Huawei Switchboard Learning Guide [M]. Beijing: People’s Posts and Telecommunications Publishing House, 2016.07.