Test Bed Overview

Our testbed includes the following:

- WiFi framework provided by [1]
    - Includes hostap implementation that is the same as the general hostap driver but customized to handle the framework
    - Includes predefined and custom test cases for processing WiFi messages, but is expandable for further customization
    - Our modified hostap source files simply allow for denying pre-authentication messages from the access point to allow for monitoring the station's reaction

Installing the testbed

First, download the WiFi Framework at https://github.com/domienschepers/wifi-framework

a. Download our customized hostap files and Python test
    i. Files included in the submission
    ii. Follow the README included with the customized files to understand where they must be placed
        1. They will be placed in sub directories for the hostap dependency included in the framework

b. Follow the WiFi Framework install instructions on the main Github page (https://github.com/domienschepers/wifi-framework)
    i. Run the following commands to ensure required packages are installed:
        1. apt-get update
        2. apt-get install git make gcc python3-venv net-tools
        3. apt-get install libdbus-1-dev libnl-3-dev libnl-genl-3-dev libnl-route-3-dev libssl-dev

    ii. Change to the dependencies directory and run build.sh with sudo
    iii. Change to the setup directory and run pysetup.sh with sudo
        1. Use git submodule init and git submodule update with sudo to enable libwifi

    iv. WPA2 is used by default, so we must change the configuration options to use WPA3
        1. Change to the setup directory and run the following commands:
            a. sudo mv supplicant.conf old-supplicant.conf
            b. sudo ln -s supplicant-wpa3-personal.conf supplicant.conf
            c. sudo ./load-config.sh wpa3-personal

    v. The usage instructions for the framework are also included on the Github page. You can activate the Python environment using the source command, but we ran everything in the generic environment

c. Create virtual interfaces by running the setup-hwsim.sh file in the setup directory with sudo
    - i. Ex. sudo ./setup/setup-hwsim.sh 3
        1. This creates 3 interfaces (1 to act as an access point, 1 to act as a station, and 1 to act as our monitor interface
    - ii. Turn wlan2 into a monitor interface
        1. sudo ifconfig wlan2 down
        2. sudo iwconfig wlan2 mode monitor
        3. sudo ifconfig wlan2 up

<u>Step-by-step instructions to reproduce the issue</u>

- Start Wireshark with sudo and start monitoring on the wlan2 interface
- Run the desired ap denial test
    - sudo python3 run.py wlan0 [TEST NAME]
    - The test names are outlined in test-dos.py
        - ap-deny-probe-response
        - ap-deny-auth-commit
        - ap-deny-auth-confirm
        - ap-deny-assoc-resp
    - You should now see beacon frames occurring in Wireshark and occasional probe frames from wlan1
- Run the station connection test (this is one that is included in the WiFi Framework)
    - Sudo python3 run.py wlan1 example-demo

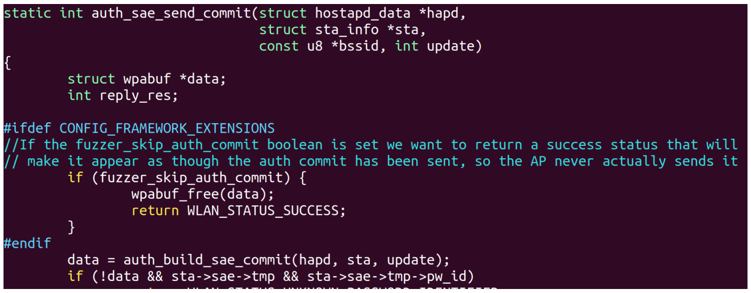
<u>Proof-of-concept or exploit code</u>

Each denial of service test will be further shown and outlined below. You may reference the list in the previous section to further understand how the station interacts in each test. Each test simply integrates a boolean that can be set in the Python Framework user-defined test that will change the functionality of hostap. There is a simple if statement in each section of code that would permit sending of the targeted access point messages.

Note

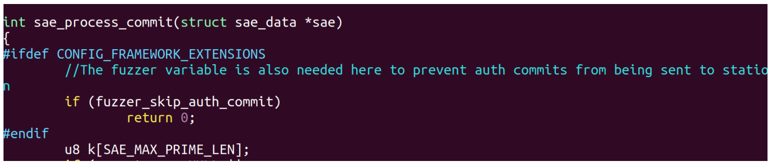
Access Point: 20:00:00:00:00:00
Station: 20:00:00:00:01:00

Denying Authentication Commits from the Access Point



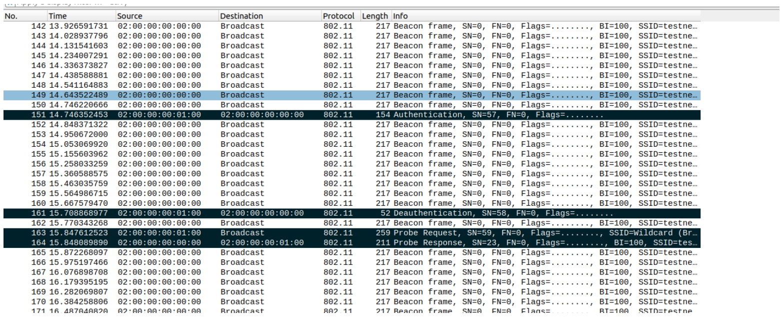
```
static int auth_sae_send_commit(struct hostapd_data *hapd,
                                struct sta_info *sta,
                                const u8 *bssid, int update)
{
        struct wpabuf *data;
        int reply_res;

#ifdef CONFIG_FRAMEWORK_EXTENSIONS
//If the fuzzer_skip_auth_commit boolean is set we want to return a success status that will
// make it appear as though the auth commit has been sent, so the AP never actually sends it
        if (fuzzer_skip_auth_commit) {
                wpabuf_free(data);
                return WLAN_STATUS_SUCCESS;
        }
#endif
        data = auth_build_sae_commit(hapd, sta, update);
        if (!data && sta->sae->tmp && sta->sae->tmp->pw_id)
```

Skip authentication commit in ieee802_11.c in src/ap



```
int sae_process_commit(struct sae_data *sae)
{
#ifdef CONFIG_FRAMEWORK_EXTENSIONS
        //The fuzzer variable is also needed here to prevent auth commits from being sent to statio
n

        if (fuzzer_skip_auth_commit)
                return 0;
#endif
        u8 k[SAE_MAX_PRIME_LEN];
```

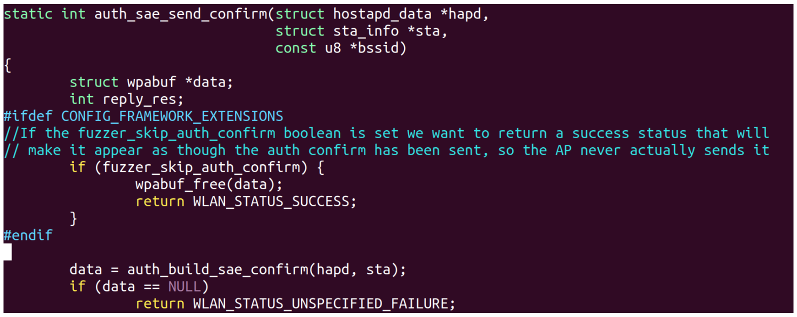
Skip authentication commit in sae.c in src/common



```
No.   Time          Source             Destination        Protocol Length Info
  142 13.926591731  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  143 14.028937796  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  144 14.131541603  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  145 14.234007291  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  146 14.336373827  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  147 14.438588881  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  148 14.541164883  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  149 14.643522489  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  150 14.746220666  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  151 14.746352453  02:00:00:00:01:00  02:00:00:00:00:00  802.11   154 Authentication, SN=57, FN=0, Flags=........
  152 14.848371322  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  153 14.950672000  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  154 15.053069920  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  155 15.155603962  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  156 15.258033259  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  157 15.360588575  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  158 15.463035759  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  159 15.564986715  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  160 15.667579470  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  161 15.708868977  02:00:00:00:01:00  02:00:00:00:00:00  802.11    52 Deauthentication, SN=58, FN=0, Flags=........
  162 15.770343268  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  163 15.847612523  02:00:00:00:01:00  Broadcast          802.11   259 Probe Request, SN=59, FN=0, Flags=........, SSID=Wildcard (Br…
  164 15.848089890  02:00:00:00:00:00  02:00:00:00:01:00  802.11   211 Probe Response, SN=23, FN=0, Flags=........, BI=100, SSID=tes…
  165 15.872268097  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  166 15.975197466  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  167 16.076898708  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  168 16.179395195  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  169 16.282069807  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  170 16.384258806  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
  171 16.487040820  02:00:00:00:00:00  Broadcast          802.11   217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne
```

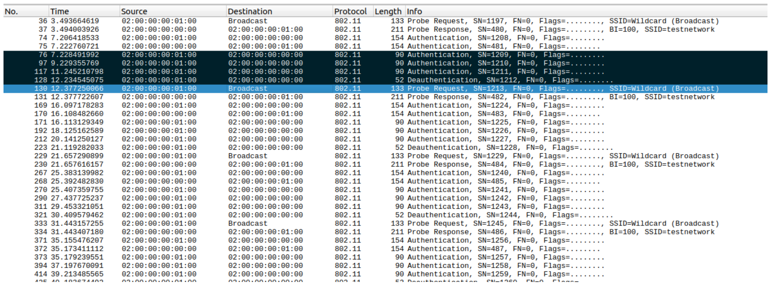
Last authentication commit followed by deauthentication and return to probing for retry

Denying Authentication Confirms from the Access Point



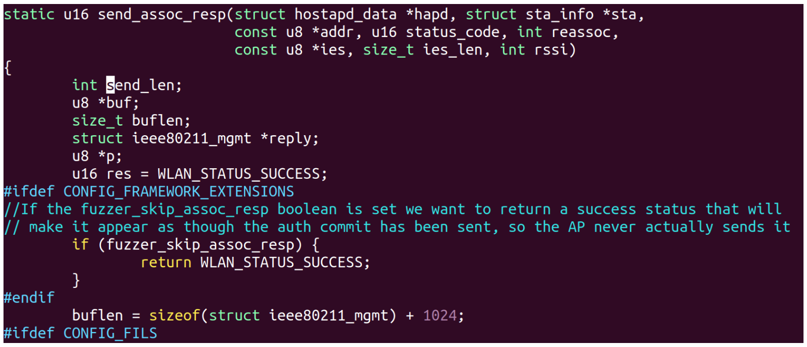
```
static int auth_sae_send_confirm(struct hostapd_data *hapd,
                                 struct sta_info *sta,
                                 const u8 *bssid)
{
        struct wpabuf *data;
        int reply_res;
#ifdef CONFIG_FRAMEWORK_EXTENSIONS
//If the fuzzer_skip_auth_confirm boolean is set we want to return a success status that will
// make it appear as though the auth confirm has been sent, so the AP never actually sends it
        if (fuzzer_skip_auth_confirm) {
                wpabuf_free(data);
                return WLAN_STATUS_SUCCESS;
        }
#endif

        data = auth_build_sae_confirm(hapd, sta);
        if (data == NULL)
                return WLAN_STATUS_UNSPECIFIED_FAILURE;
```

Skip authentication confirm in ieee802_11.c in dependencies/hostap_2_9/src/ap



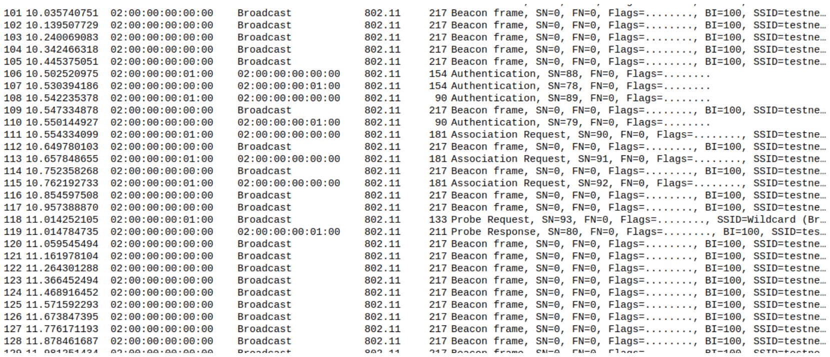
```
No.     Time          Source              Destination         Protocol  Length Info
     36 3.493664619   02:00:00:00:01:00   Broadcast           802.11     133 Probe Request, SN=1197, FN=0, Flags=........, SSID=Wildcard (Broadcast)
     37 3.494003926   02:00:00:00:00:00   02:00:00:00:01:00   802.11     211 Probe Response, SN=480, FN=0, Flags=........, BI=100, SSID=testnetwork
     74 7.206418533   02:00:00:00:01:00   02:00:00:00:00:00   802.11     154 Authentication, SN=1208, FN=0, Flags=........
     75 7.222760721   02:00:00:00:00:00   02:00:00:00:01:00   802.11     154 Authentication, SN=481, FN=0, Flags=........
     76 7.228491992   02:00:00:00:01:00   02:00:00:00:00:00   802.11      90 Authentication, SN=1209, FN=0, Flags=........
     97 9.229355769   02:00:00:00:01:00   02:00:00:00:00:00   802.11      90 Authentication, SN=1210, FN=0, Flags=........
    117 11.245210798  02:00:00:00:01:00   02:00:00:00:00:00   802.11      90 Authentication, SN=1211, FN=0, Flags=........
    128 12.234545075  02:00:00:00:01:00   02:00:00:00:00:00   802.11      52 Deauthentication, SN=1212, FN=0, Flags=........
    130 12.377250066  02:00:00:00:01:00   Broadcast           802.11     133 Probe Request, SN=1213, FN=0, Flags=........, SSID=Wildcard (Broadcast)
    131 12.377722607  02:00:00:00:00:00   02:00:00:00:01:00   802.11     211 Probe Response, SN=482, FN=0, Flags=........, BI=100, SSID=testnetwork
    169 16.097178283  02:00:00:00:01:00   02:00:00:00:00:00   802.11     154 Authentication, SN=1224, FN=0, Flags=........
    170 16.108482660  02:00:00:00:00:00   02:00:00:00:01:00   802.11     154 Authentication, SN=483, FN=0, Flags=........
    171 16.113129349  02:00:00:00:01:00   02:00:00:00:00:00   802.11      90 Authentication, SN=1225, FN=0, Flags=........
    192 18.125162589  02:00:00:00:01:00   02:00:00:00:00:00   802.11      90 Authentication, SN=1226, FN=0, Flags=........
    212 20.141250127  02:00:00:00:01:00   02:00:00:00:00:00   802.11      90 Authentication, SN=1227, FN=0, Flags=........
    223 21.119282033  02:00:00:00:01:00   02:00:00:00:00:00   802.11      52 Deauthentication, SN=1228, FN=0, Flags=........
    229 21.657290899  02:00:00:00:01:00   Broadcast           802.11     133 Probe Request, SN=1229, FN=0, Flags=........, SSID=Wildcard (Broadcast)
    230 21.657616157  02:00:00:00:00:00   02:00:00:00:01:00   802.11     211 Probe Response, SN=484, FN=0, Flags=........, BI=100, SSID=testnetwork
    267 25.383139982  02:00:00:00:01:00   02:00:00:00:00:00   802.11     154 Authentication, SN=1240, FN=0, Flags=........
    268 25.392482830  02:00:00:00:00:00   02:00:00:00:01:00   802.11     154 Authentication, SN=485, FN=0, Flags=........
    270 25.407359755  02:00:00:00:01:00   02:00:00:00:00:00   802.11      90 Authentication, SN=1241, FN=0, Flags=........
    290 27.437725237  02:00:00:00:01:00   02:00:00:00:00:00   802.11      90 Authentication, SN=1242, FN=0, Flags=........
    311 29.453321051  02:00:00:00:01:00   02:00:00:00:00:00   802.11      90 Authentication, SN=1243, FN=0, Flags=........
    321 30.409579462  02:00:00:00:01:00   02:00:00:00:00:00   802.11      52 Deauthentication, SN=1244, FN=0, Flags=........
    333 31.443157255  02:00:00:00:01:00   Broadcast           802.11     133 Probe Request, SN=1245, FN=0, Flags=........, SSID=Wildcard (Broadcast)
    334 31.443407180  02:00:00:00:00:00   02:00:00:00:01:00   802.11     211 Probe Response, SN=486, FN=0, Flags=........, BI=100, SSID=testnetwork
    371 35.155476207  02:00:00:00:01:00   02:00:00:00:00:00   802.11     154 Authentication, SN=1256, FN=0, Flags=........
    372 35.173411112  02:00:00:00:00:00   02:00:00:00:01:00   802.11     154 Authentication, SN=487, FN=0, Flags=........
    373 35.179239551  02:00:00:00:01:00   02:00:00:00:00:00   802.11      90 Authentication, SN=1257, FN=0, Flags=........
    394 37.197670091  02:00:00:00:01:00   02:00:00:00:00:00   802.11      90 Authentication, SN=1258, FN=0, Flags=........
    414 39.213485565  02:00:00:00:01:00   02:00:00:00:00:00   802.11      90 Authentication, SN=1259, FN=0, Flags=........
```

Denying Association Responses from the Access Point



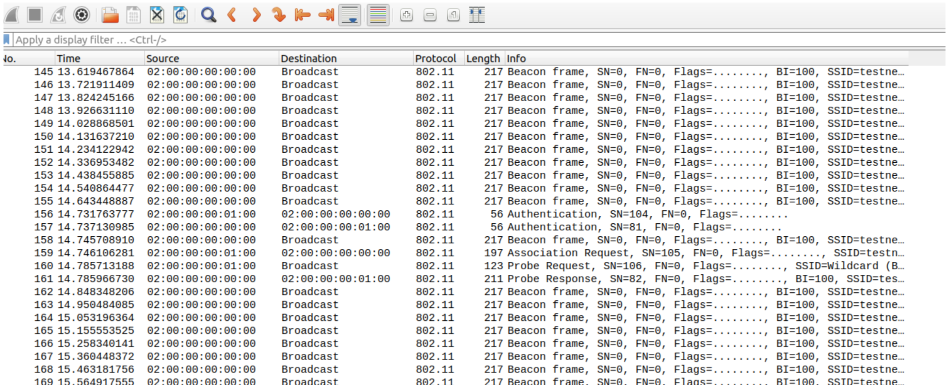
```
static u16 send_assoc_resp(struct hostapd_data *hapd, struct sta_info *sta,
                           const u8 *addr, u16 status_code, int reassoc,
                           const u8 *ies, size_t ies_len, int rssi)
{
        int send_len;
        u8 *buf;
        size_t buflen;
        struct ieee80211_mgmt *reply;
        u8 *p;
        u16 res = WLAN_STATUS_SUCCESS;
#ifdef CONFIG_FRAMEWORK_EXTENSIONS
//If the fuzzer_skip_assoc_resp boolean is set we want to return a success status that will
// make it appear as though the auth commit has been sent, so the AP never actually sends it
        if (fuzzer_skip_assoc_resp) {
                return WLAN_STATUS_SUCCESS;
        }
#endif
        buflen = sizeof(struct ieee80211_mgmt) + 1024;
#ifdef CONFIG_FILS
```

Skip association response in ieee802_11.c in dependencies/hostap_2_9/src/ap



```
101 10.035740751  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
102 10.139507729  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
103 10.240069083  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
104 10.342466318  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
105 10.445375051  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
106 10.502520975  02:00:00:00:01:00    02:00:00:00:00:00    802.11     154 Authentication, SN=88, FN=0, Flags=........
107 10.530394186  02:00:00:00:00:00    02:00:00:00:01:00    802.11     154 Authentication, SN=78, FN=0, Flags=........
108 10.542235378  02:00:00:00:01:00    02:00:00:00:00:00    802.11      90 Authentication, SN=89, FN=0, Flags=........
109 10.547334878  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
110 10.550144927  02:00:00:00:00:00    02:00:00:00:01:00    802.11      90 Authentication, SN=79, FN=0, Flags=........
111 10.554334099  02:00:00:00:01:00    02:00:00:00:00:00    802.11     181 Association Request, SN=90, FN=0, Flags=........, SSID=testne…
112 10.649780103  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
113 10.657848655  02:00:00:00:01:00    02:00:00:00:00:00    802.11     181 Association Request, SN=91, FN=0, Flags=........, SSID=testne…
114 10.752358268  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
115 10.762192733  02:00:00:00:01:00    02:00:00:00:00:00    802.11     181 Association Request, SN=92, FN=0, Flags=........, SSID=testne…
116 10.854597508  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
117 10.957388870  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
118 11.014252105  02:00:00:00:01:00    Broadcast            802.11     133 Probe Request, SN=93, FN=0, Flags=........, SSID=Wildcard (Br…
119 11.014784735  02:00:00:00:00:00    02:00:00:00:01:00    802.11     211 Probe Response, SN=80, FN=0, Flags=........, BI=100, SSID=tes…
120 11.059545494  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
121 11.161978104  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
122 11.264301288  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
123 11.366452494  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
124 11.468916452  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
125 11.571592293  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
126 11.673847395  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
127 11.776171193  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
128 11.878461687  02:00:00:00:00:00    Broadcast            802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
```

Association request being resent but eventually returning to probing



```
No.  Time         Source             Destination        Protocol Length Info
 145 13.619467864 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 146 13.721911409 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 147 13.824245166 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 148 13.926631110 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 149 14.028868501 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 150 14.131637210 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 151 14.234122942 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 152 14.336953482 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 153 14.438455885 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 154 14.540864477 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 155 14.643448887 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 156 14.731763777 02:00:00:00:01:00  02:00:00:00:00:00  802.11      56 Authentication, SN=104, FN=0, Flags=........
 157 14.737130985 02:00:00:00:00:00  02:00:00:00:01:00  802.11      56 Authentication, SN=81, FN=0, Flags=........
 158 14.745708910 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 159 14.746106281 02:00:00:00:01:00  02:00:00:00:00:00  802.11     197 Association Request, SN=105, FN=0, Flags=........, SSID=testn…
 160 14.785713188 02:00:00:00:01:00  Broadcast          802.11     123 Probe Request, SN=106, FN=0, Flags=........, SSID=Wildcard (B…
 161 14.785966730 02:00:00:00:00:00  02:00:00:00:01:00  802.11     211 Probe Response, SN=82, FN=0, Flags=........, BI=100, SSID=tes…
 162 14.848348206 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 163 14.950484085 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 164 15.053196364 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 165 15.155553525 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 166 15.258340141 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 167 15.360448372 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 168 15.463181756 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
 169 15.564917555 02:00:00:00:00:00  Broadcast          802.11     217 Beacon frame, SN=0, FN=0, Flags=........, BI=100, SSID=testne…
```

Authentication success being sent, followed by association request and returning to probing

References

[1] D. Schepers, M. Vanhoef, and A. Ranganathan, “A framework to test and Fuzz Wi-Fi devices,” *In Proceedings of the 14th ACM Conference on Security and Privacy in Wireless and Mobile Networks (WiSec 2021)*. June 2021.