sales@candelatech.com
support@candelatech.com
+1 (360) 380-1618 [PST, GMT -8]

Using own_ie_override for Custom RSN Information Elements of Beacon Frames

Goal: Manually override certain RSN-related information elements of Beacon frames sent by a LANforge system in AP Mode for testing WPA2 authentication.

In this test scenario a LANforge system acts as a WiFi access point configured to use WPA2 authentication. Beacon frames sent by this AP contain information elements about RSN encryption. The `own_ie_override` field in `hostapd.conf` provides a built-in way to override certain parts of these IEs for testing purposes, and may be configured through LANforge **Custom WiFi** parameters. Listed below are several example test cases provided in the hostap repository.

---

1. **Initial Setup for WPA2-Authentication Testing.**
   A. Set up a virtual AP for testing.
   In this test, it is named `vap0000` on parent device `wiphy0`.
   For more information see Create vAP in Bridge Mode

   B. On a separate radio, create a station to authenticate with `vap0000`:
   In the **Port Manager** tab, select `wiphy1` and click **Create**; select **WiFi STA**, then click **Apply**.
   In this test, the station is named `wlan1` on parent device `wiphy1`.
   For more information see Generating Traffic for WLAN Testing

   C. Configure `vap0000` and `wlan1` to use WPA2-PSK encrypted authentication.
   For more information see WPA2 Authentication Test Scenario

   D. Configure `vap0000` and `wlan1` with **SSID** `test-wpa2-psk` and **Keyphrase** `qwertyuiop`.

   E. Create a Monitor Port on its own radio to sniff wireless packets.
   In this test, the monitor port is named `moni3a`.
   For more information see Using Wireshark to Sniff WiFi Monitors

2. **Control (No Change):**
   A. Configure **Custom WiFi** in `vap0000`:
   Select `vap0000` and click **Modify**.
   Navigate to the **Custom WiFi** tab.
   Ensure that no `own_ie_override` parameter is set in **User-Specified supplicant/hostapd configuration text**.
   Click **Apply** then **OK**.

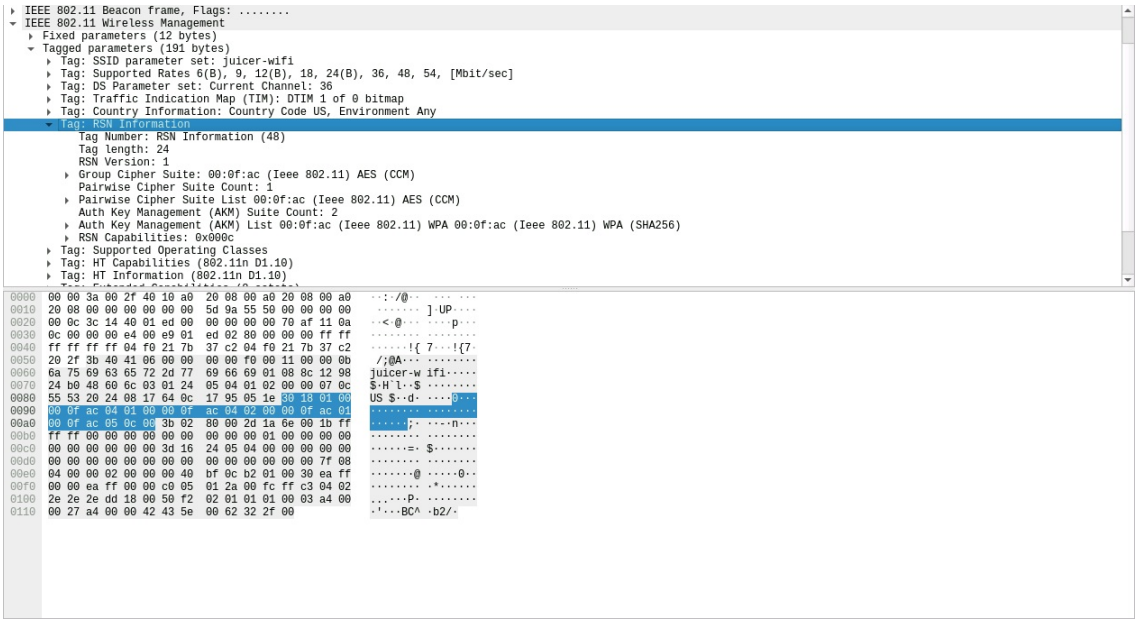
   B. Set the vAP down and back up to allow changes to take effect:
   In the **Port Manager** tab, select `vap0000`.
   Admin all selected interfaces **DOWN** (CTRL-PLUS).
   Admin all selected interfaces **UP** (CTRL-MINUS).

   C. Sniff packets to observe the authentication behavior:
   On the observation system in the **Port Manager** tab, select only `moni3a`:
   Click **Sniff Packets**.

   D. Reset the station to force re-authentication:
   In the Port Manager tab, select only `wlan1`.
   Click **Reset Port**.

   E. Observe the results, which should be similar to the following:
   - Packets are not malformed.
   - The station `wlan1` succeeds in authenticating with `vap0000`.
   - No RSN Information Element is found in Beacon frames sent by `vap0000`.

F. Example results:



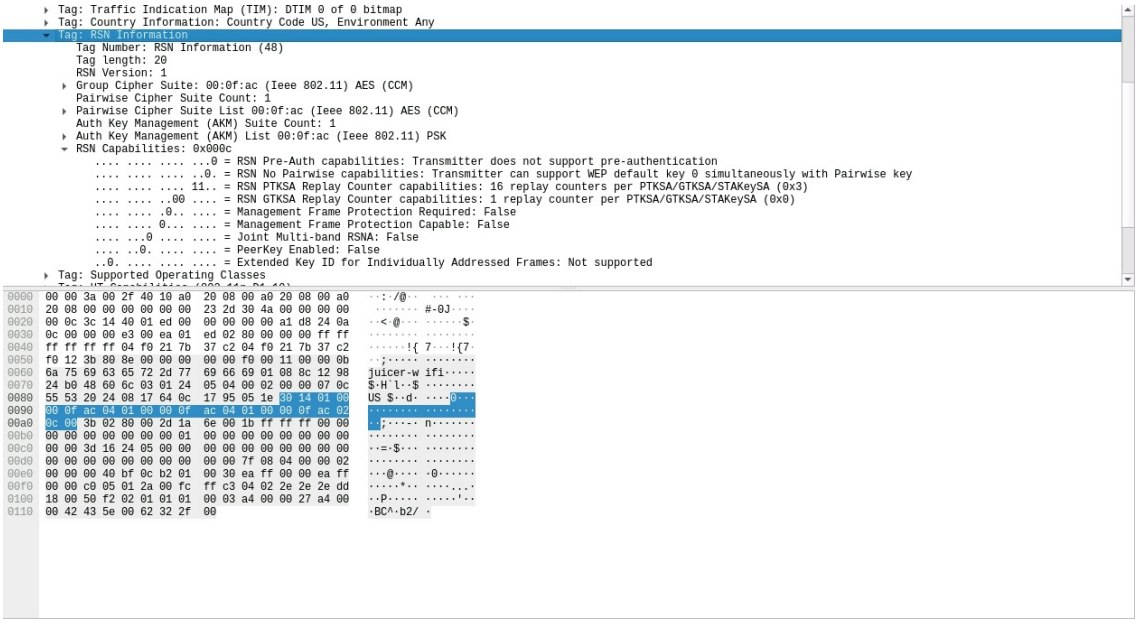
3. **The RSN element used normally by hostapd:**

A. Configure **Custom WiFi** in `vap0000`:
Select `vap0000` and click **Modify**.
Navigate to the **Custom WiFi** tab.
In the **User-Specified supplicant/hostapd configuration text** field, write:
`own_ie_override=30140100000fac040100000fac040100000fac020c0`.
Click **Apply** then **OK**.

B. Reset ports and sniff packets:
Repeat steps B through D of Step 2.

C. Observe the results, which should be similar to the following:
- The station `wlan1` fails to authenticate with `vap0000`.
- RSN Information Element is present in Beacon frames sent by `vap0000`.

D. Example results:



4. **No RSN Capabilities field:**

A. Configure **Custom WiFi** in `vap0000`:
Select `vap0000` and click **Modify**.
Navigate to the **Custom WiFi** tab.
In the **User-Specified supplicant/hostapd configuration text** field, write:
`own_ie_override=30120100000fac040100000fac040100000fac02`.
Click **Apply** then **OK**.

B. Reset ports and sniff packets:
Repeat steps B through D of Step 2.

C. Observe the results, which should be similar to the following:
- The station `wlan1` fails to authenticate with `vap0000`.
- Beacon frames sent by `vap0000` are recognizably malformed.

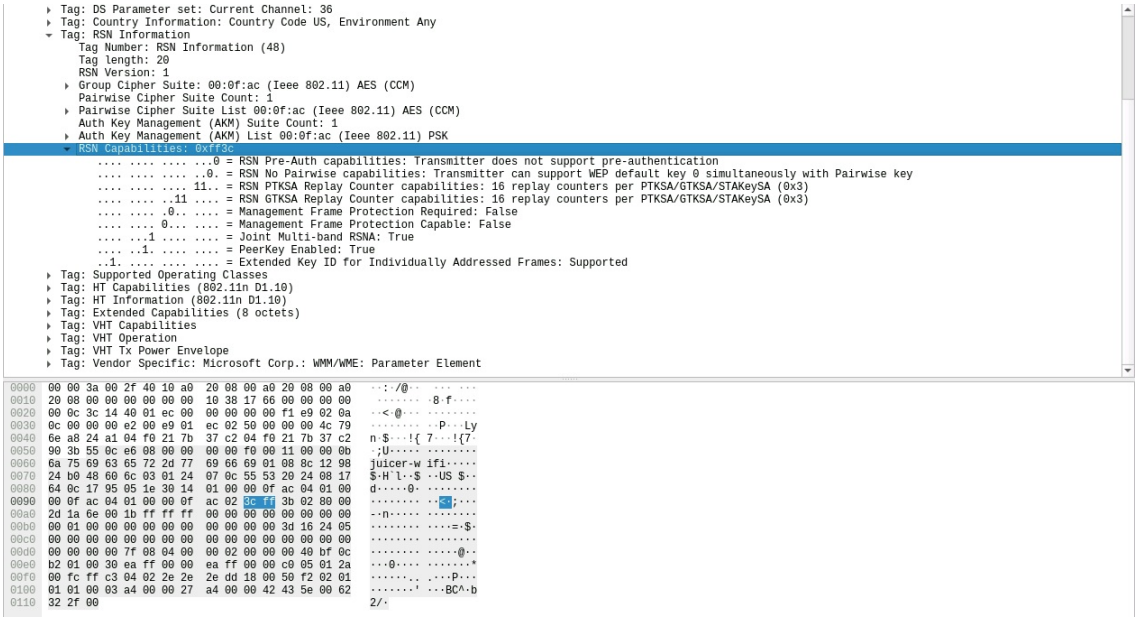
5. **Reserved RSN Capabilities bits set:**

A. Configure **Custom WiFi** in `vap0000`:
Select `vap0000` and click **Modify**.
Navigate to the **Custom WiFi** tab.
In the **User-Specified supplicant/hostapd configuration text** field, write:
`own_ie_override=30140100000fac040100000fac040100000fac023cff`.
Click **Apply** then **OK**.

B. Reset ports and sniff packets:
Repeat steps B through D of Step 2.

C. Observe the results, which should be similar to the following:
- The station `wlan1` fails to authenticate with `vap0000` with `CTRL-MSG: NETWORK NOT FOUND`.
- RSN Information Element is present in Beacon frames sent by `vap0000`.
- Beacon frames sent by `vap0000` are not malformed.

D. Example results:



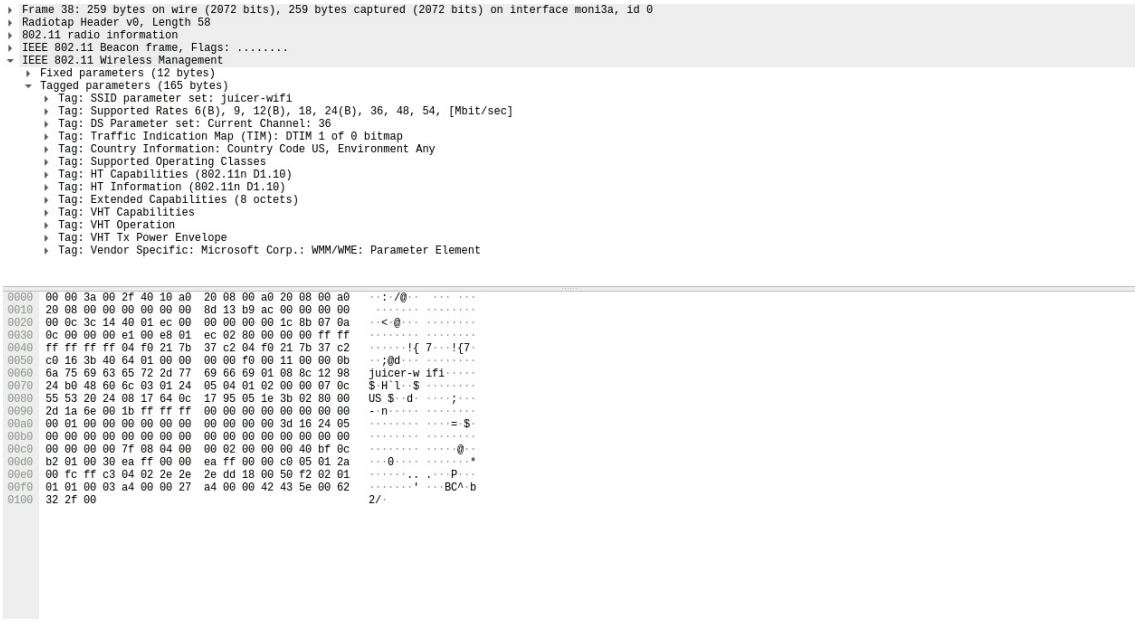
6. **Truncated RSN Capabilities field:**

A. Configure **Custom WiFi** in `vap0000`:
Select `vap0000` and click **Modify**.
Navigate to the **Custom WiFi** tab.
In the **User-Specified supplicant/hostapd configuration text** field, write:
`own_ie_override=30130100000fac040100000fac040100000fac023c`.
Click **Apply** then **OK**.

B. Reset ports and sniff packets:
Repeat steps B through D of Step 2.

C. Observe the results, which should be similar to the following:
- The station `wlan1` fails to authenticate with `vap0000` with `CTRL-MSG: NETWORK NOT FOUND`.
- RSN Information Element is not present in Beacon frames sent by `vap0000`.
- Beacon frames sent by `vap0000` are not malformed.

D. Example results:



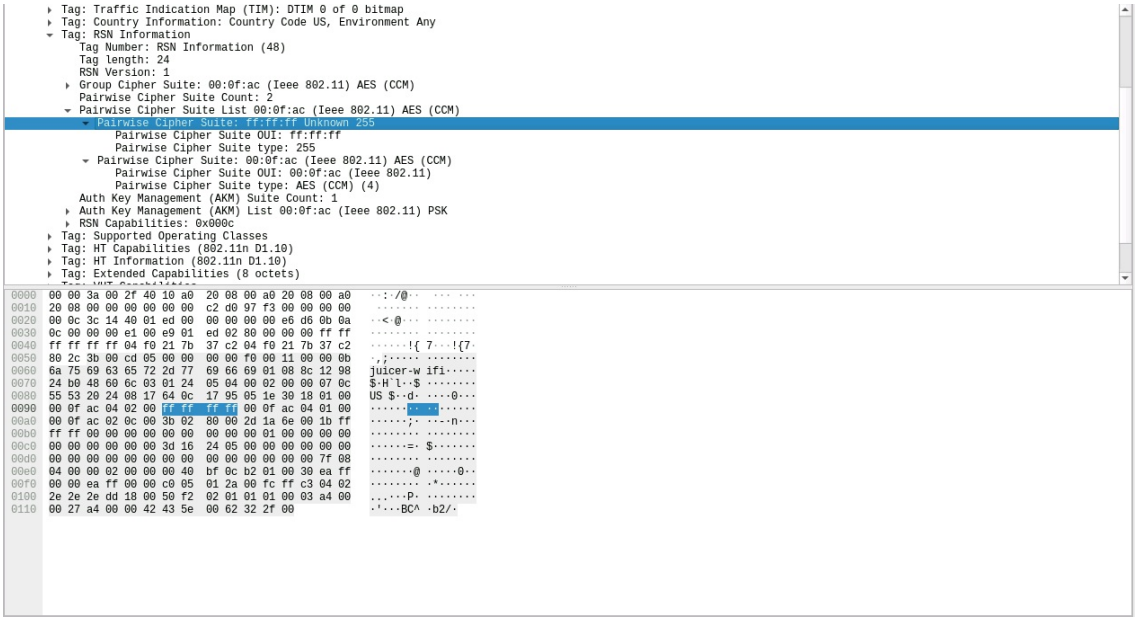
7. **Extra pairwise cipher suite (unsupported):**

A. Configure **Custom WiFi** in `vap0000`:
Select `vap0000` and click **Modify**.
Navigate to the **Custom WiFi** tab.
In the **User-Specified supplicant/hostapd configuration text** field, write:
`own_ie_override=30180100000fac040200ffffffff000fac040100000fac020c00`.
Click **Apply** then **OK**.

B. Reset ports and sniff packets:
Repeat steps B through D of Step 2.

C. Observe the results, which should be similar to the following:
- The station `wlan1` fails to authenticate with `vap0000` with `CTRL-MSG: NETWORK NOT FOUND`.
- RSN Information Element is present in Beacon frames sent by `vap0000`.
- Beacon frames sent by `vap0000` are not malformed.

D. Example results:

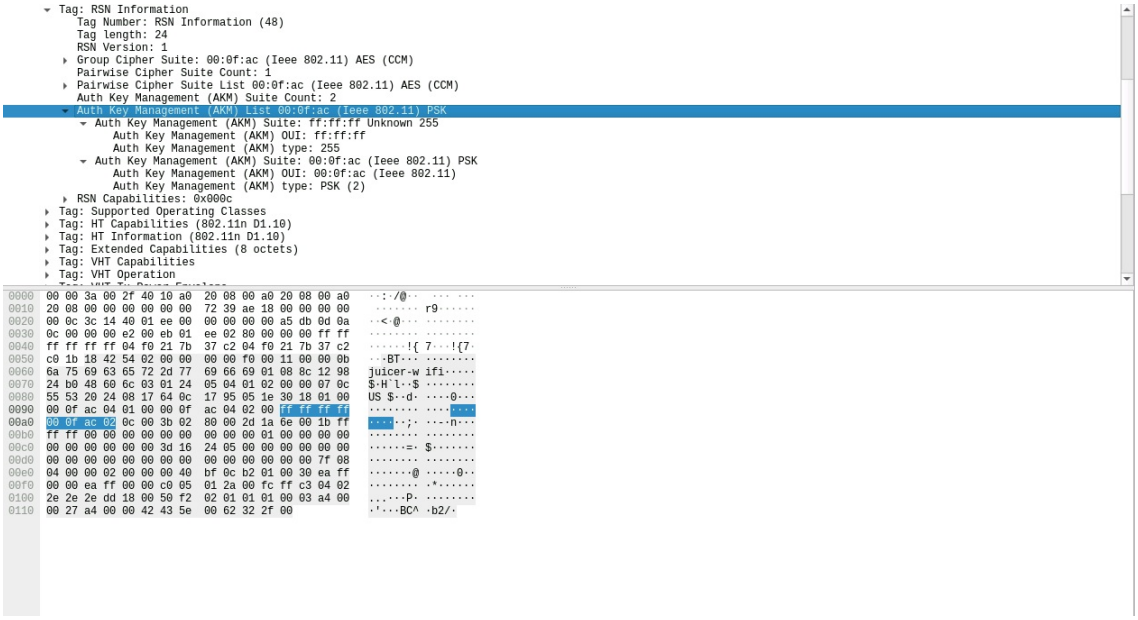


8. **Extra AKM suite (unsupported):**
   A. Configure **Custom WiFi** in `vap0000`:
   Select `vap0000` and click **Modify**.
   Navigate to the **Custom WiFi** tab.
   In the **User-Specified supplicant/hostapd configuration text** field, write:
   `own_ie_override=30180100000fac040100000fac040200ffffffff000fac020c00`.
   Click **Apply** then **OK**.

   B. Reset ports and sniff packets:
   Repeat steps B through D of Step 2.

   C. Observe the results, which should be similar to the following:
   - The station `wlan1` fails to authenticate with `vap0000` with `CTRL-MSG: NETWORK NOT FOUND`.
   - RSN Information Element is present in Beacon frames sent by `vap0000`.
   - The RSN IE in a Beacon frame sent by `vap0000` contains two Pairwise Cipher Suite fields rather than one.
   - Beacon frames sent by `vap0000` are not malformed.

   D. Example results:

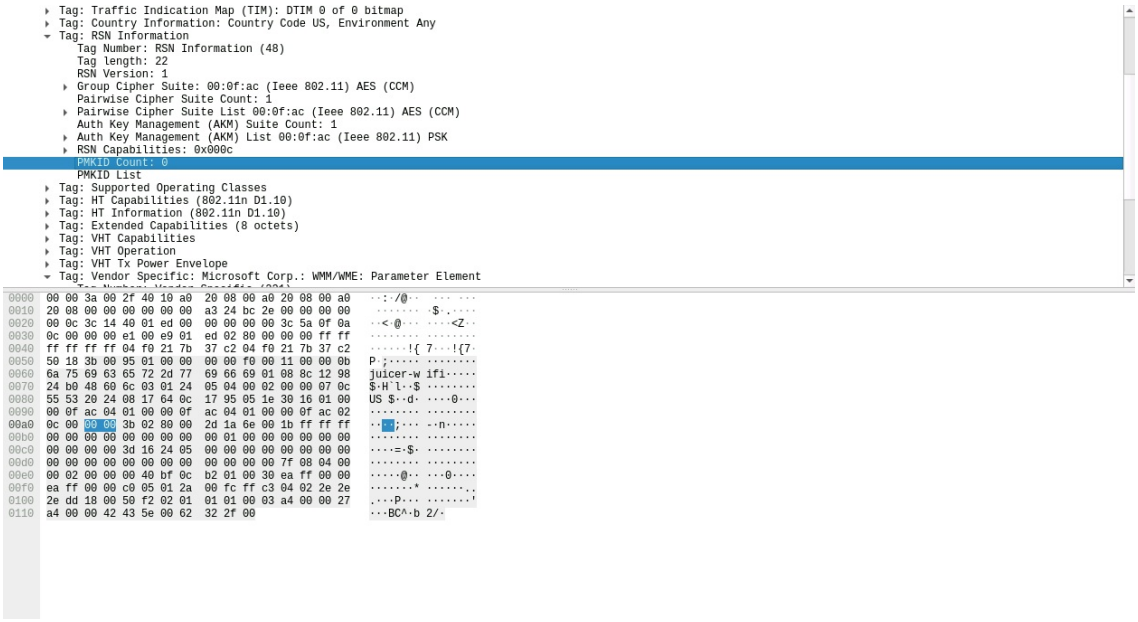


9. **PMKIDCount field included:**
   A. Configure **Custom WiFi** in `vap0000`:
   Select `vap0000` and click **Modify**.
   Navigate to the **Custom WiFi** tab.
   In the **User-Specified supplicant/hostapd configuration text** field, write:
   `own_ie_override=30160100000fac040100000fac040100000fac020c000000`.
   Click **Apply** then **OK**.

   B. Reset ports and sniff packets:
   Repeat steps B through D of Step 2.

   C. Observe the results, which should be similar to the following:
   - The station `wlan1` fails to authenticate with `vap0000` with `CTRL-MSG: NETWORK NOT FOUND`.
   - RSN Information Element is present in Beacon frames sent by `vap0000`.
   - The RSN IE in a Beacon frame sent by `vap0000` contains a PMKIDCount field.
   - Beacon frames sent by `vap0000` are not malformed.

D. Example results:



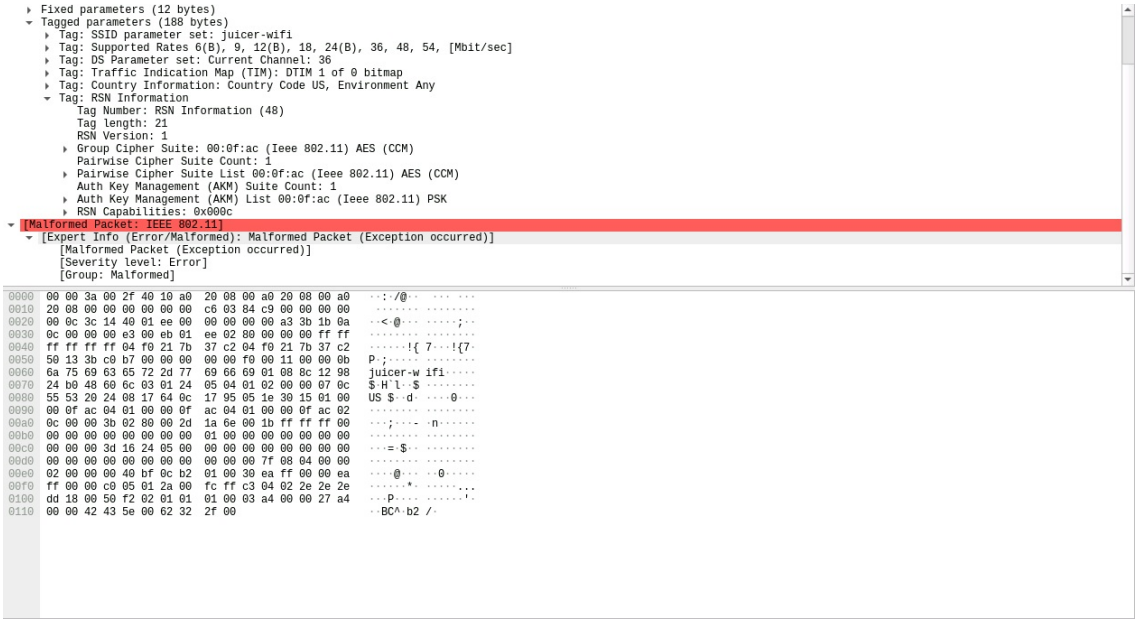
10. **Truncated PMKIDCount field:**

A. Configure **Custom WiFi** in `vap0000`:
Select `vap0000` and click **Modify**.
Navigate to the **Custom WiFi** tab.
In the **User-Specified supplicant/hostapd configuration text** field, write:
`own_ie_override=30150100000fac040100000fac040100000fac020c0000`.
Click **Apply** then **OK**.

B. Reset ports and sniff packets:
Repeat steps B through D of Step 2.

C. Observe the results, which should be similar to the following:
- The station `wlan1` fails to authenticate with `vap0000` with `CTRL-MSG: NETWORK NOT FOUND`.
- The RSN IE in a Beacon frame sent by `vap0000` is present, but incomplete.
- Beacon frames sent by `vap0000` are recognizably malformed.

D. Example results:



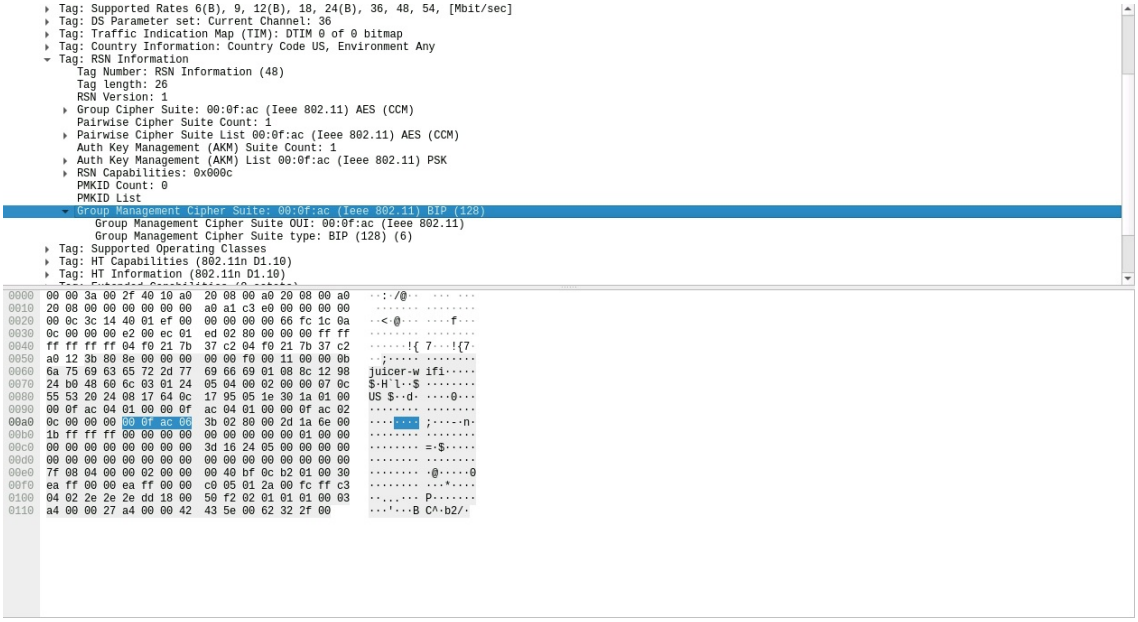
11. **Unexpected Group Management Cipher Suite with PMF disabled:**

A. Configure **Custom WiFi** in `vap0000`:
Select `vap0000` and click **Modify**.
Navigate to the **Custom WiFi** tab.
In the **User-Specified supplicant/hostapd configuration text** field, write:
`own_ie_override=301a0100000fac040100000fac040100000fac020c000000000fac06`.
Click **Apply** then **OK**.

B. Reset ports and sniff packets:
Repeat steps B through D of Step 2.

C. Observe the results, which should be similar to the following:
- The station `wlan1` fails to authenticate with `vap0000` with `CTRL-MSG: NETWORK NOT FOUND`.
- The RSN IE in a Beacon frame sent by `vap0000` contains a Group Management Cipher field.
- Beacon frames sent by `vap0000` are not malformed.

D. Example results:



12. **Extra octet after defined fields (future extensibility):**

A. Configure **Custom WiFi** in `vap0000`:
Select `vap0000` and click **Modify**.
Navigate to the **Custom WiFi** tab.
In the **User-Specified supplicant/hostapd configuration text** field, write:
`own_ie_override=301b0100000fac040100000fac040100000fac020c000000000fac0600`.
Click **Apply** then **OK**.

B. Reset ports and sniff packets:
Repeat steps B through D of Step 2.

C. Observe the results, which should be similar to the following:
- The station `wlan1` fails to authenticate with `vap0000` with `CTRL-MSG: NETWORK NOT FOUND`.
- The RSN IE in a Beacon frame sent by `vap0000` contains a Group Management Cipher field.
- Beacon frames sent by `vap0000` are not malformed.

D. Example results: