

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:

```

> IEEE 802.11 Beacon Frame, Flags: .....
> IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  > Tagged parameters (191 bytes)
    > Tag: SSID parameter set: juicer-wifi
    > Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
    > Tag: DS Parameter set: Current Channel: 36
    > Tag: Traffic Indication Map (TIM): DTIM 1 of 0 bitmap
    > Tag: Country Information: Country Code US, Environment Any
  > Tag: RSN Information
    Tag Number: RSN Information (48)
    Tag length: 24
    RSN Version: 1
    > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    > Pairwise Cipher Suite Count: 1
    > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
    > Auth Key Management (AKM) Suite Count: 2
    > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) WPA 00:0f:ac (Ieee 802.11) WPA (SHA256)
    > RSN Capabilities: 0x000c
    > Tag: Supported Operating Classes
    > Tag: HT Capabilities (802.11n D1.10)
    > Tag: HT Information (802.11n D1.10)
  > Tag: HT Information (802.11n D1.10)
0000 00 00 3a 00 2f 40 10 a0 20 08 00 a0 20 08 00 a0  ....:/@...
0010 20 08 00 00 00 00 00 5d 9a 55 50 00 00 00 00  ...:..]UP...
0020 00 0c 3c 14 40 01 ed 00 00 00 00 70 af 11 0a  ...<.@...p...
0030 0c 00 00 00 e4 00 e9 01 ed 02 80 00 00 00 ff ff  ....:..{7...{7...
0040 ff ff ff ff 04 f0 21 7b 37 c2 04 f0 21 7b 37 c2  ...:/@A...
0050 20 2f 3b 40 41 06 09 00 00 09 f9 00 11 00 00 0b  ...:/@A...
0060 6a 75 69 63 65 72 2d 77 69 66 69 01 08 0c 12 98  juicer-wifi...
0070 24 b0 48 60 6c 03 01 24 05 04 01 02 00 00 07 0c  $-H'L-$...
0080 55 53 20 24 08 17 64 0c 17 95 05 1e 30 14 01 00  US$-d-...
0090 00 0f ac 04 01 00 0f ac 04 02 00 00 0f ac 01  ....:..n.....
00a0 00 0f ac 05 0a 01 0b 02 00 00 2d 1a 0e 00 1b ff  ....:..n.....
00b0 ff ff 00 00 00 00 00 00 00 00 00 01 00 00 00 00  ....:..$.....
00c0 00 00 00 00 00 00 3d 16 24 05 04 00 00 00 00 00  ....:..$.....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 7f 08  ....:..@.....
00e0 04 00 00 02 00 00 00 40 bf 0c b2 01 09 39 ea ff  ....:..@.....
00f0 00 00 00 ff 00 00 05 01 2a 00 fc ff c3 04 02  ....:..@.....
0100 2e 2e 2e dd 18 00 50 f2 02 01 01 01 00 03 a4 00  ...:..P.....
0110 00 27 a4 00 00 42 43 5e 00 62 32 2f 00  ....:..BCA-b2/..

```

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:

```

> Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
> Tag: Country Information: Country Code US, Environment Any
> Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 20
  RSN Version: 1
  > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  > Pairwise Cipher Suite Count: 1
  > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
  > Auth Key Management (AKM) Suite Count: 1
  > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
  > RSN Capabilities: 0x000c
    ....0 = RSN Pre-Auth capabilities: Transmitter does not support pre-authentication
    ....0 = RSN No Pairwise capabilities: Transmitter can support WEP default key 0 simultaneously with Pairwise key
    ....11 = RSN PTKSA Replay Counter capabilities: 16 replay counters per PTKSA/GTKSA/STAKEySA (8x3)
    ....00 = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STAKEySA (8x0)
    ....0 = Management Frame Protection Required: False
    ....0 = Management Frame Protection Capable: False
    ....0 = Joint Multi-band RSNA: False
    ....0 = PeerKey Enabled: False
    ....0 = Extended Key ID for Individually Addressed Frames: Not supported
  > Tag: Supported Operating Classes
0000 00 00 2a 00 2f 40 10 a0 20 08 00 a0 20 08 00 a0  ....:/@...
0010 20 08 00 00 00 00 00 23 2d 30 4a 00 00 00 00  ...:..#-0J...
0020 00 0c 3c 14 40 01 ed 00 00 00 00 a1 d8 24 0a  ...<.@...$...
0030 0c 00 00 00 e3 00 ea 01 ed 02 80 00 00 00 ff ff  ....:..$.....
0040 ff ff ff ff 04 f0 21 7b 37 c2 04 f0 21 7b 37 c2  ...:/@A...
0050 f0 12 3b 00 8a 00 00 00 00 f9 00 11 00 00 00 00  ...:/@A...
0060 6a 75 69 63 65 72 2d 77 69 66 69 01 08 0c 12 98  juicer-wifi...
0070 24 b0 48 60 6c 03 01 24 05 04 00 02 00 00 07 0c  $-H'L-$...
0080 55 53 20 24 08 17 64 0c 17 95 05 1e 30 14 01 00  US$-d-...
0090 00 0f ac 04 01 00 0f ac 04 02 00 00 0f ac 01  ....:..n.....
00a0 00 0f ac 05 0a 01 0b 02 00 00 2d 1a 0e 00 1b ff  ....:..n.....
00b0 00 00 00 00 00 00 01 00 00 00 00 00 00 00 00  ....:..$.....
00c0 00 00 3d 16 24 05 00 00 00 00 00 00 00 00 00 00  ....:..$.....
00d0 00 00 00 00 00 00 00 00 00 00 7f 08 04 00 00 02  ....:..@.....
00e0 00 00 00 bf 0c b2 01 09 39 ea ff 00 30 ea ff 00 ea ff  ...:..@.....
00f0 00 00 c9 05 01 2a 00 fc ff c3 04 02 2e 2e 2e dd  ...:..@.....
0100 18 00 50 f2 02 01 01 01 00 03 a4 00 00 27 a4 00  ...:..P.....
0110 00 42 43 5e 00 62 32 2f 00  ....:..BCA-b2/..

```


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=30180100000fac040100000fac040200ffffff0000fac020c00.`
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:

```
▼ Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 24
  RSN Version: 1
  ▶ Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  ▶ Pairwise Cipher Suite Count: 1
  ▶ Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 2
  ▼ Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
    ▼ Auth Key Management (AKM) Suite: ff:ff:ff Unknown 255
      Auth Key Management (AKM) OUI: ff:ff:ff
      Auth Key Management (AKM) type: 255
    ▼ Auth Key Management (AKM) Suite: 00:0f:ac (Ieee 802.11) PSK
      Auth Key Management (AKM) OUI: 00:0f:ac (Ieee 802.11)
      Auth Key Management (AKM) type: PSK (2)
  ▶ RSN Capabilities: 0x000c
  ▶ Tag: Supported Operating Classes
  ▶ Tag: HT Capabilities (802.11n D1.10)
  ▶ Tag: HT Information (802.11n D1.10)
  ▶ Tag: Extended Capabilities (8 octets)
  ▶ Tag: VHT Capabilities
  ▶ Tag: VHT Operation
  ▶ Tag: MIMO Non-3x3
  ▶ Tag: MIMO 3x3
  ▶ Tag: MIMO 4x4
  ▶ Tag: MIMO 5x5
  ▶ Tag: MIMO 6x6
  ▶ Tag: MIMO 8x8
  ▶ Tag: MIMO 10x10
  ▶ Tag: MIMO 12x12
  ▶ Tag: MIMO 16x16
  ▶ Tag: MIMO 20x20
  ▶ Tag: MIMO 24x24
  ▶ Tag: MIMO 32x32
  ▶ Tag: MIMO 48x48
  ▶ Tag: MIMO 64x64
  ▶ Tag: MIMO 96x96
  ▶ Tag: MIMO 128x128
  ▶ Tag: MIMO 192x192
  ▶ Tag: MIMO 256x256
  ▶ Tag: MIMO 384x384
  ▶ Tag: MIMO 512x512
  ▶ Tag: MIMO 768x768
  ▶ Tag: MIMO 1024x1024
  ▶ Tag: MIMO 1344x1344
  ▶ Tag: MIMO 1792x1792
  ▶ Tag: MIMO 2304x2304
  ▶ Tag: MIMO 3072x3072
  ▶ Tag: MIMO 4096x4096
  ▶ Tag: MIMO 5460x5460
  ▶ Tag: MIMO 7296x7296
  ▶ Tag: MIMO 9728x9728
  ▶ Tag: MIMO 12960x12960
  ▶ Tag: MIMO 17280x17280
  ▶ Tag: MIMO 23040x23040
  ▶ Tag: MIMO 30720x30720
  ▶ Tag: MIMO 40960x40960
  ▶ Tag: MIMO 54600x54600
  ▶ Tag: MIMO 72960x72960
  ▶ Tag: MIMO 97280x97280
  ▶ Tag: MIMO 129600x129600
  ▶ Tag: MIMO 172800x172800
  ▶ Tag: MIMO 230400x230400
  ▶ Tag: MIMO 307200x307200
  ▶ Tag: MIMO 409600x409600
  ▶ Tag: MIMO 546000x546000
  ▶ Tag: MIMO 729600x729600
  ▶ Tag: MIMO 972800x972800
  ▶ Tag: MIMO 1296000x1296000
  ▶ Tag: MIMO 1728000x1728000
  ▶ Tag: MIMO 2304000x2304000
  ▶ Tag: MIMO 3072000x3072000
  ▶ Tag: MIMO 4096000x4096000
  ▶ Tag: MIMO 5460000x5460000
  ▶ Tag: MIMO 7296000x7296000
  ▶ Tag: MIMO 9728000x9728000
  ▶ Tag: MIMO 12960000x12960000
  ▶ Tag: MIMO 17280000x17280000
  ▶ Tag: MIMO 23040000x23040000
  ▶ Tag: MIMO 30720000x30720000
  ▶ Tag: MIMO 40960000x40960000
  ▶ Tag: MIMO 54600000x54600000
  ▶ Tag: MIMO 72960000x72960000
  ▶ Tag: MIMO 97280000x97280000
  ▶ Tag: MIMO 129600000x129600000
  ▶ Tag: MIMO 172800000x172800000
  ▶ Tag: MIMO 230400000x230400000
  ▶ Tag: MIMO 307200000x307200000
  ▶ Tag: MIMO 409600000x409600000
  ▶ Tag: MIMO 546000000x546000000
  ▶ Tag: MIMO 729600000x729600000
  ▶ Tag: MIMO 972800000x972800000
  ▶ Tag: MIMO 1296000000x1296000000
  ▶ Tag: MIMO 1728000000x1728000000
  ▶ Tag: MIMO 2304000000x2304000000
  ▶ Tag: MIMO 3072000000x3072000000
  ▶ Tag: MIMO 4096000000x4096000000
  ▶ Tag: MIMO 5460000000x5460000000
  ▶ Tag: MIMO 7296000000x7296000000
  ▶ Tag: MIMO 9728000000x9728000000
  ▶ Tag: MIMO 12960000000x12960000000
  ▶ Tag: MIMO 17280000000x17280000000
  ▶ Tag: MIMO 23040000000x23040000000
  ▶ Tag: MIMO 30720000000x30720000000
  ▶ Tag: MIMO 40960000000x40960000000
  ▶ Tag: MIMO 54600000000x54600000000
  ▶ Tag: MIMO 72960000000x72960000000
  ▶ Tag: MIMO 97280000000x97280000000
  ▶ Tag: MIMO 129600000000x129600000000
  ▶ Tag: MIMO 172800000000x172800000000
  ▶ Tag: MIMO 230400000000x230400000000
  ▶ Tag: MIMO 307200000000x307200000000
  ▶ Tag: MIMO 409600000000x409600000000
  ▶ Tag: MIMO 546000000000x546000000000
  ▶ Tag: MIMO 729600000000x729600000000
  ▶ Tag: MIMO 972800000000x972800000000
  ▶ Tag: MIMO 1296000000000x1296000000000
  ▶ Tag: MIMO 1728000000000x1728000000000
  ▶ Tag: MIMO 2304000000000x2304000000000
  ▶ Tag: MIMO 3072000000000x3072000000000
  ▶ Tag: MIMO 4096000000000x4096000000000
  ▶ Tag: MIMO 5460000000000x5460000000000
  ▶ Tag: MIMO 7296000000000x7296000000000
  ▶ Tag: MIMO 9728000000000x9728000000000
  ▶ Tag: MIMO 12960000000000x12960000000000
  ▶ Tag: MIMO 17280000000000x17280000000000
  ▶ Tag: MIMO 23040000000000x23040000000000
  ▶ Tag: MIMO 30720000000000x30720000000000
  ▶ Tag: MIMO 40960000000000x40960000000000
  ▶ Tag: MIMO 54600000000000x54600000000000
  ▶ Tag: MIMO 72960000000000x72960000000000
  ▶ Tag: MIMO 97280000000000x97280000000000
  ▶ Tag: MIMO 129600000000000x129600000000000
  ▶ Tag: MIMO 172800000000000x172800000000000
  ▶ Tag: MIMO 230400000000000x230400000000000
  ▶ Tag: MIMO 307200000000000x307200000000000
  ▶ Tag: MIMO 409600000000000x409600000000000
  ▶ Tag: MIMO 546000000000000x546000000000000
  ▶ Tag: MIMO 729600000000000x729600000000000
  ▶ Tag: MIMO 972800000000000x972800000000000
  ▶ Tag: MIMO 1296000000000000x1296000000000000
  ▶ Tag: MIMO 1728000000000000x1728000000000000
  ▶ Tag: MIMO 2304000000000000x2304000000000000
  ▶ Tag: MIMO 3072000000000000x3072000000000000
  ▶ Tag: MIMO 4096000000000000x4096000000000000
  ▶ Tag: MIMO 5460000000000000x5460000000000000
  ▶ Tag: MIMO 7296000000000000x7296000000000000
  ▶ Tag: MIMO 9728000000000000x9728000000000000
  ▶ Tag: MIMO 12960000000000000x12960000000000000
  ▶ Tag: MIMO 17280000000000000x17280000000000000
  ▶ Tag: MIMO 23040000000000000x23040000000000000
  ▶ Tag: MIMO 30720000000000000x30720000000000000
  ▶ Tag: MIMO 40960000000000000x40960000000000000
  ▶ Tag: MIMO 54600000000000000x54600000000000000
  ▶ Tag: MIMO 72960000000000000x72960000000000000
  ▶ Tag: MIMO 97280000000000000x97280000000000000
  ▶ Tag: MIMO 129600000000000000x129600000000000000
  ▶ Tag: MIMO 172800000000000000x172800000000000000
  ▶ Tag: MIMO 230400000000000000x230400000000000000
  ▶ Tag: MIMO 307200000000000000x307200000000000000
  ▶ Tag: MIMO 409600000000000000x409600000000000000
  ▶ Tag: MIMO 546000000000000000x546000000000000000
  ▶ Tag: MIMO 729600000000000000x729600000000000000
  ▶ Tag: MIMO 972800000000000000x972800000000000000
  ▶ Tag: MIMO 1296000000000000000x1296000000000000000
  ▶ Tag: MIMO 1728000000000000000x1728000000000000000
  ▶ Tag: MIMO 2304000000000000000x2304000000000000000
  ▶ Tag: MIMO 3072000000000000000x3072000000000000000
  ▶ Tag: MIMO 4096000000000000000x4096000000000000000
  ▶ Tag: MIMO 5460000000000000000x5460000000000000000
  ▶ Tag: MIMO 7296000000000000000x7296000000000000000
  ▶ Tag: MIMO 9728000000000000000x9728000000000000000
  ▶ Tag: MIMO 12960000000000000000x12960000000000000000
  ▶ Tag: MIMO 17280000000000000000x17280000000000000000
  ▶ Tag: MIMO 23040000000000000000x23040000000000000000
  ▶ Tag: MIMO 30720000000000000000x30720000000000000000
  ▶ Tag: MIMO 40960000000000000000x40960000000000000000
  ▶ Tag: MIMO 54600000000000000000x54600000000000000000
  ▶ Tag: MIMO 72960000000000000000x72960000000000000000
  ▶ Tag: MIMO 97280000000000000000x97280000000000000000
  ▶ Tag: MIMO 129600000000000000000x129600000000000000000
  ▶ Tag: MIMO 172800000000000000000x172800000000000000000
  ▶ Tag: MIMO 230400000000000000000x230400000000000000000
  ▶ Tag: MIMO 307200000000000000000x307200000000000000000
  ▶ Tag: MIMO 409600000000000000000x409600000000000000000
  ▶ Tag: MIMO 546000000000000000000x546000000000000000000
  ▶ Tag: MIMO 729600000000000000000x729600000000000000000
  ▶ Tag: MIMO 972800000000000000000x972800000000000000000
  ▶ Tag: MIMO 1296000000000000000000x1296000000000000000000
  ▶ Tag: MIMO 1728000000000000000000x1728000000000000000000
  ▶ Tag: MIMO 2304000000000000000000x2304000000000000000000
  ▶ Tag: MIMO 3072000000000000000000x3072000000000000000000
  ▶ Tag: MIMO 4096000000000000000000x4096000000000000000000
  ▶ Tag: MIMO 5460000000000000000000x5460000000000000000000
  ▶ Tag: MIMO 7296000000000000000000x7296000000000000000000
  ▶ Tag: MIMO 9728000000000000000000x9728000000000000000000
  ▶ Tag: MIMO 12960000000000000000000x12960000000000000000000
  ▶ Tag: MIMO 17280000000000000000000x17280000000000000000000
  ▶ Tag: MIMO 23040000000000000000000x23040000000000000000000
  ▶ Tag: MIMO 30720000000000000000000x30720000000000000000000
  ▶ Tag: MIMO 40960000000000000000000x40960000000000000000000
  ▶ Tag: MIMO 54600000000000000000000x54600000000000000000000
  ▶ Tag: MIMO 72960000000000000000000x72960000000000000000000
  ▶ Tag: MIMO 97280000000000000000000x97280000000000000000000
  ▶ Tag: MIMO 129600000000000000000000x129600000000000000000000
  ▶ Tag: MIMO 172800000000000000000000x172800000000000000000000
  ▶ Tag: MIMO 230400000000000000000000x230400000000000000000000
  ▶ Tag: MIMO 307200000000000000000000x307200000000000000000000
  ▶ Tag: MIMO 409600000000000000000000x409600000000000000000000
  ▶ Tag: MIMO 546000000000000000000000x546000000000000000000000
  ▶ Tag: MIMO 729600000000000000000000x729600000000000000000000
  ▶ Tag: MIMO 972800000000000000000000x972800000000000000000000
  ▶ Tag: MIMO 1296000000000000000000000x1296000000000000000000000
  ▶ Tag: MIMO 1728000000000000000000000x1728000000000000000000000
  ▶ Tag: MIMO 2304000000000000000000000x2304000000000000000000000
  ▶ Tag: MIMO 3072000000000000000000000x3072000000000000000000000
  ▶ Tag: MIMO 4096000000000000000000000x4096000000000000000000000
  ▶ Tag: MIMO 5460000000000000000000000x5460000000000000000000000
  ▶ Tag: MIMO 7296000000000000000000000x7296000000000000000000000
  ▶ Tag: MIMO 9728000000000000000000000x9728000000000000000000000
  ▶ Tag: MIMO 12960000000000000000000000x12960000000000000000000000
  ▶ Tag: MIMO 17280000000000000000000000x17280000000000000000000000
  ▶ Tag: MIMO 23040000000000000000000000x23040000000000000000000000
  ▶ Tag: MIMO 30720000000000000000000000x30720000000000000000000000
  ▶ Tag: MIMO 40960000000000000000000000x40960000000000000000000000
  ▶ Tag: MIMO 54600000000000000000000000x54600000000000000000000000
  ▶ Tag: MIMO 72960000000000000000000000x72960000000000000000000000
  ▶ Tag: MIMO 97280000000000000000000000x97280000000000000000000000
  ▶ Tag: MIMO 129600000000000000000000000x129600000000000000000000000
  ▶ Tag: MIMO 172800000000000000000000000x172800000000000000000000000
  ▶ Tag: MIMO 230400000000000000000000000x230400000000000000000000000
  ▶ Tag: MIMO 307200000000000000000000000x307200000000000000000000000
  ▶ Tag: MIMO 409600000000000000000000000x409600000000000000000000000
  ▶ Tag: MIMO 546000000000000000000000000x546000000000000000000000000
  ▶ Tag: MIMO 729600000000000000000000000x729600000000000000000000000
  ▶ Tag: MIMO 972800000000000000000000000x972800000000000000000000000
  ▶ Tag: MIMO 1296000000000000000000000000x1296000000000000000000000000
  ▶ Tag: MIMO 1728000000000000000000000000x1728000000000000000000000000
  ▶ Tag: MIMO 2304000000000000000000000000x2304000000000000000000000000
  ▶ Tag: MIMO 3072000000000000000000000000x3072000000000000000000000000
  ▶ Tag: MIMO 4096000000000000000000000000x4096000000000000000000000000
  ▶ Tag: MIMO 5460000000000000000000000000x5460000000000000000000000000
  ▶ Tag: MIMO 7296000000000000000000000000x7296000000000000000000000000
  ▶ Tag: MIMO 9728000000000000000000000000x9728000000000000000000000000
  ▶ Tag: MIMO 12960000000000000000000000000x12960000000000000000000000000
  ▶ Tag: MIMO 17280000000000000000000000000x17280000000000000000000000000
  ▶ Tag: MIMO 23040000000000000000000000000x23040000000000000000000000000
  ▶ Tag: MIMO 30720000000000000000000000000x30720000000000000000000000000
  ▶ Tag: MIMO 40960000000000000000000000000x40960000000000000000000000000
  ▶ Tag: MIMO 54600000000000000000000000000x54600000000000000000000000000
  ▶ Tag: MIMO 72960000000000000000000000000x72960000000000000000000000000
  ▶ Tag: MIMO 97280000000000000000000000000x97280000000000000000000000000
  ▶ Tag: MIMO 129600000000000000000000000000x129600000000000000000000000000
  ▶ Tag: MIMO 172800000000000000000000000000x172800000000000000000000000000
  ▶ Tag: MIMO 230400000000000000000000000000x230400000000000000000000000000
  ▶ Tag: MIMO 307200000000000000000000000000x307200000000000000000000000000
  ▶ Tag: MIMO 409600000000000000000000000000x409600000000000000000000000000
  ▶ Tag: MIMO 546000000000000000000000000000x546000000000000000000000000000
  ▶ Tag: MIMO 729600000000000000000000000000x729600000000000000000000000000
  ▶ Tag: MIMO 972800000000000000000000000000x972800000000000000000000000000
  ▶ Tag: MIMO 1296000000000000000000000000000x1296000000000000000000000000000
  ▶ Tag: MIMO 1728000000000000000000000000000x1728000000000000000000000000000
  ▶ Tag: MIMO 2304000000000000000000000000000x2304000000000000000000000000000
  ▶ Tag: MIMO 3072000000000000000000000000000x3072000000000000000000000000000
  ▶ Tag: MIMO 4096000000000000000000000000000x4096000000000000000000000000000
  ▶ Tag: MIMO 5460000000000000000000000000000x5460000000000000000000000000000
  ▶ Tag: MIMO 7296000000000000000000000000000x7296000000000000000000000000000
  ▶ Tag: MIMO 9728000000000000000000000000000x9728000000000000000000000000000
  ▶ Tag: MIMO 12960000000000000000000000000000x12960000000000000000000000000000
  ▶ Tag: MIMO 17280000000000000000000000000000x17280000000000000000000000000000
  ▶ Tag: MIMO 23040000000000000000000000000000x23040000000000000000000000000000
  ▶ Tag: MIMO 30720000000000000000000000000000x30720000000000000000000000000000
  ▶ Tag: MIMO 40960000000000000000000000000000x40960000000000000000000000000000
  ▶ Tag: MIMO 54600000000000000000000000000000x54600000000000000000000000000000
  ▶ Tag: MIMO 72960000000000000000000000000000x72960000000000000000000000000000
  ▶ Tag: MIMO 97280000000000000000000000000000x97280000000000000000000000000000
  ▶ Tag: MIMO 129600000000000000000000000000000x129600000000000000000000000000000
  ▶ Tag: MIMO 172800000000000000000000000000000x172800000000000000000000000000000
  ▶ Tag: MIMO 230400000000000000000000000000000x230400000000000000000000000000000
  ▶ Tag: MIMO 307200000000000000000000000000000x307200000000000000000000000000000
  ▶ Tag: MIMO 409600000000000000000000000000000x409600000000000000000000000000000
  ▶ Tag: MIMO 546000000000000000000000000000000x546000000000000000000000000000000
  ▶ Tag: MIMO 729600000000000000000000000000000x729600000000000000000000000000000
  ▶ Tag: MIMO 972800000000000000000000000000000x972800000000000000000000000000000
  ▶ Tag: MIMO 1296000000000000000000000000000000x1296000000000000000000000000000000
  ▶ Tag: MIMO 1728000000000000000000000000000000x1728000000000000000000000000000000
  ▶ Tag: MIMO 2304000000000000000000000000000000x23
```


- 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=301a010000fac040100000fac040100000fac020c000000000fac06.
```
 - 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:

```

> Tag: Supported Rates 6(B), 9, 12(B), 18, 24(B), 36, 48, 54, [Mbit/sec]
> Tag: DS Parameter set: Current Channel: 36
> Tag: Traffic Indication Map (TIM): DTIM 0 of 0 bitmap
> Tag: Country Information: Country Code US, Environment Any
> Tag: RSN Information
  Tag Number: RSN Information (48)
  Tag length: 26
  RSN Version: 1
  Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
  Pairwise Cipher Suite Count: 1
  Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
  Auth Key Management (AKM) Suite Count: 1
  Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
  RSN Capabilities: 0x000c
  PMKID Count: 0
  PMKID List
  Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
  Group Management Cipher Suite Count: 1
  Group Management Cipher Suite type: BIP (128) (6)
> Tag: Supported Operating Classes
> Tag: HT Capabilities (802.11n D1.10)
> Tag: HT Information (802.11n D1.10)
-----
0000 00 00 3a 00 2f 40 10 a0 20 08 00 a0 20 08 00 a0  ..:/0.....
0010 20 08 00 00 00 00 00 00 a0 a1 c3 e0 00 00 00 00  ..<.....f...
0020 00 0c 3c 14 40 01 ef 00 00 00 00 00 fc 1c 0a    <<.....f...
0030 0c 00 00 00 e2 00 ec 01 ed 02 00 00 00 ff ff    .....!{7...!{7-
0040 ff ff ff ff 04 f0 21 7b 37 c2 04 f0 21 7b 37 c2  .....!{7...!{7-
0050 a0 12 3b 80 8e 00 00 00 00 00 f0 00 11 00 00 0b  ..;}.....n-
0060 6a 75 69 63 65 72 2d 77 69 66 69 01 08 8c 12 98  juicer-wifi...
0070 24 b0 48 06 0c 03 01 24 05 04 00 02 00 00 07 0c  S-H'l-$.....
0080 55 b3 20 24 08 17 64 0c 17 95 05 1e 30 1a 01 00  US$-d'.....0...
0090 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ac 02  .....;.....n-
00a0 0c 00 00 00 00 0f ac 00 3b 02 80 00 2d 1a 6e 00  .....;.....n-
00b0 1b ff ff ff 00 00 00 00 00 00 00 00 00 01 00 00  .....=S.....
00c0 00 00 00 00 00 00 00 3d 15 24 05 00 00 00 00  .....=S.....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  .....@.....0
00e0 7f 08 04 00 00 02 00 00 00 40 bf 0c b2 01 00 30  .....@.....0
00f0 ea ff 00 00 ea ff 00 00 c0 05 01 2a 00 fc ff c3  .....@.....0
0100 04 02 2e 2e 2e dd 18 00 50 f2 02 01 01 01 00 03  .....P.....
0110 a4 00 00 27 a4 00 00 42 43 5e 00 02 32 2f 00    .....B C^b2/-

```

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=301b010000fac040100000fac040100000fac020c000000000fac0600.
```
 - 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:

```
Tag: RSN Information
Tag Number: RSN Information (48)
Tag length: 27
RSN Version: 1
Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
Pairwise Cipher Suite Count: 1
Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
Auth Key Management (AKM) Suite Count: 1
Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
RSN Capabilities: 0x000c
PMKID Count: 0
PMKID List
Group Management Cipher Suite: 00:0f:ac (Ieee 802.11) BIP (128)
Group Management Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
Group Management Cipher Suite type: BIP (128) (6)
Tag: Supported Operating Classes
Tag: HT Capabilities (802.11n D1.10)
Tag: HT Information (802.11n D1.10)
Tag: Extended Capabilities (8 octets)
Tag: VHT Capabilities
Tag: VHT Operation
Tag: VHT Tx Power Envelope
-----
0000 00 00 3a 00 2f 40 10 a0 20 00 00 a0 20 00 00 a0 .....:/@.....
0010 20 08 00 00 00 00 00 77 1f 15 f0 00 00 00 .....w.....
0020 00 0c 3c 14 40 01 ee 00 00 00 00 6a 6d 1f 0a ...<@.....jm...
0030 0c 00 00 00 e2 00 e9 01 ee 02 80 00 00 ff ff .....
0040 ff ff ff ff 04 f0 21 7b 37 c2 04 f0 21 7b 37 c2 .....!{ 7...{7...
0050 50 12 2b 00 87 00 00 00 00 f0 00 11 00 00 0b P.....
0060 6a 75 69 63 65 72 2d 77 69 66 69 01 08 8c 12 98 juicer-wifi.....
0070 24 b0 48 60 6c 03 01 24 05 04 00 02 00 00 07 0c $-H'L-$.....
0080 55 53 20 24 08 17 64 0c 17 95 05 1e 00 10 01 00 US $-d-.....
0090 00 0f ac 04 01 00 0f ac 04 01 00 00 0f ac 02 .....
00a0 00 00 00 00 0f ac 06 00 30 02 00 00 2d 1a 0e .....
00b0 00 1b ff ff ff 00 00 00 00 00 00 00 00 01 00 .....
00c0 00 00 00 00 00 00 00 00 3d 16 24 05 00 00 00 .....=-$.
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00e0 00 7f 08 04 00 00 02 00 00 00 49 bf 0c b2 01 00 .....@.....
00f0 30 ea ff 00 ea ff 00 00 c9 05 01 2a 00 fc ff .....
0100 c3 04 02 2e 2e 2e dd 18 00 50 f2 02 01 01 01 00 .....-P.....
0110 03 a4 00 00 27 a4 00 00 42 43 5e 00 02 32 2f 00 .....BC^b2/..
```

Candela Technologies, Inc., 2417 Main Street, Suite 201, Ferndale, WA 98248, USA
www.candelatech.com | sales@candelatech.com | +1.360.380.1618