

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`.

```

> 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)

```

- 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**.

```

> 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: 0x0000
    .....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 (0x3)
    .....00.... = RSN GTKSA Replay Counter capabilities: 1 replay counter per PTKSA/GTKSA/STakeySA (0x0)
    .....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
  Tag Number: Supported Operating Classes (2)
  Tag length: 2
  0000 00 00 3a 00 2f 40 19 a0 20 08 00 a0 20 08 00 a0 .....:/0/
  0010 20 08 00 00 00 00 00 00 2d 3d 30 4a 00 00 00 00 .....#-03-
  0020 00 0c 3c 14 40 01 ed 00 00 00 00 00 a1 d8 24 0a ...<-0.....$-
  0030 0c 00 00 00 e3 00 ea 01 ed 02 00 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 f0 12 3b 08 8e 00 00 00 00 00 f9 00 11 00 00 00 .....
  0060 6a 75 63 68 72 72 77 69 66 69 01 00 00 8c 12 98 juicer-w i f i .....
  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 $-d.....0-
  0090 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ac 02 .....
  00a0 00 0f 3b 02 00 00 2d 1a 00 00 1b ff ff ff 00 00 .....n.....
  00b0 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 .....
  00c0 00 00 3d 16 24 05 00 00 00 00 00 00 00 00 00 .....$-.....
  00d0 00 00 00 00 00 00 00 00 00 00 7f 08 04 00 00 02 .....
  00e0 00 00 00 40 bf 0c b2 01 00 38 ea ff 00 00 ea ff .....0.....0-
  00f0 00 00 c9 05 01 2a 00 fc ff c3 04 02 2e 2e 2e dd .....
  0100 18 00 f0 f2 02 01 01 01 00 03 a4 00 00 27 a4 00 .....P.....
  0110 00 42 43 5e 00 62 32 2f 00 .....BC^b2/

```

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=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:

```

> Frame 38: 259 bytes on wire (2072 bits), 259 bytes captured (2072 bits) on interface mon13a, id 0
> Radiotap Header v0, Length 58
> 802.11 radio information
> IEEE 802.11 Beacon frame, Flags: .....
> IEEE 802.11 Wireless Management
  > Fixed parameters (12 bytes)
  > Tagged parameters (165 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: 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
    > Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element

```

```

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 80 13 b9 ac 00 00 00 00 ...<@.....
0020 00 0c 3c 14 40 01 ec 00 00 00 00 1c 0b 07 0a ...<@.....
0030 0c 00 00 00 e1 00 e8 01 ec 02 80 00 00 00 ff ff .....
0040 ff ff ff ff 04 f0 21 7b 37 c2 04 f0 21 7b 37 c2 .....!{ 7...!{7-
0050 c0 16 3b 40 64 01 00 00 00 00 f0 00 11 00 00 0b ...;@.....
0060 6a 75 69 63 65 72 2d 7f 69 66 69 61 08 8c 12 98 juicer-wifi....
0070 24 b0 48 69 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 02 80 00 US $-d-....
0090 2d 1a 6e 00 1b ff ff ff 00 00 00 00 00 00 00 00 ...-n.....
00a0 00 01 00 00 00 00 00 00 00 00 00 3d 16 24 05 .....-$.
00b0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 .....
00c0 00 00 00 00 7f 08 04 00 00 02 00 00 00 40 bf 0c .....@.....
00d0 b2 01 00 30 ea ff 00 00 ea ff 00 00 c0 05 01 2a ...-0.....*
00e0 00 fc ff c3 04 02 2e 2e 2e dd 18 00 50 f2 02 01 .....-P.....
00f0 01 01 00 03 a4 00 00 27 a4 00 00 42 43 5e 00 62 .....-BC^b
0100 32 2f 00 .....2/-

```

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=30180100000fac040200fffffffff000fac040100000fac020c00.
```

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:

```

  > 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: 24
    > RSN Version: 1
    > Group Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
    > Pairwise Cipher Suite Count: 2
    > Pairwise Cipher Suite List 00:0f:ac (Ieee 802.11) AES (CCM)
      > Pairwise Cipher Suite: ff:ff:ff Unknown 255
        > Pairwise Cipher Suite OUI: ff:ff:ff
        > Pairwise Cipher Suite type: 255
      > Pairwise Cipher Suite: 00:0f:ac (Ieee 802.11) AES (CCM)
        > Pairwise Cipher Suite OUI: 00:0f:ac (Ieee 802.11)
        > Pairwise Cipher Suite type: AES (CCM) (4)
      > Auth Key Management (AKM) Suite Count: 1
      > Auth Key Management (AKM) List 00:0f:ac (Ieee 802.11) PSK
      > 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)

```

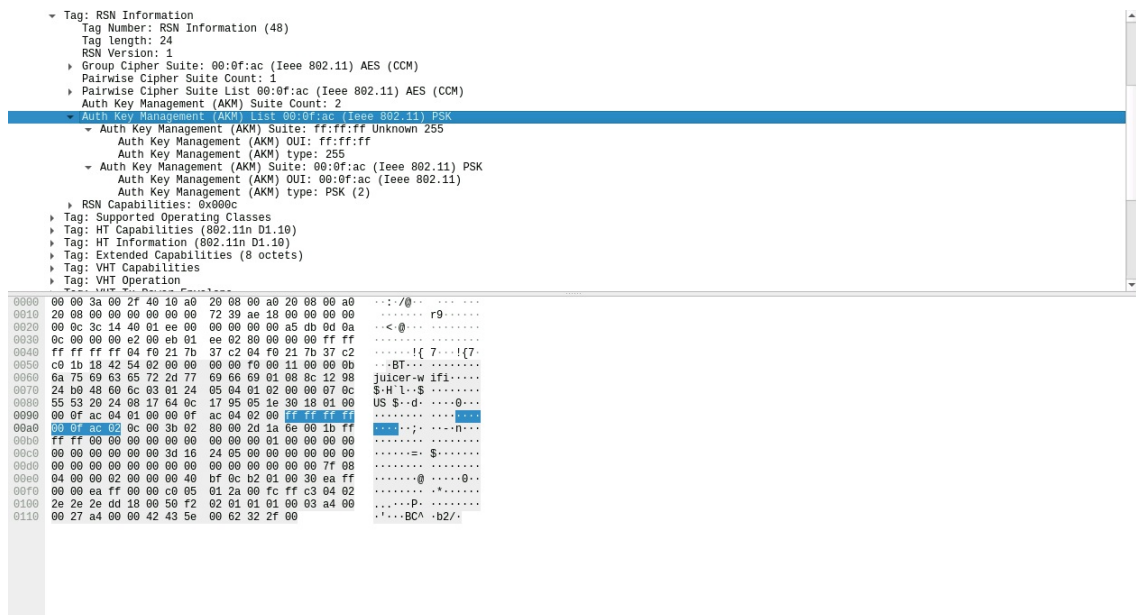
```

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 c2 00 07 f3 00 00 00 00 ...<@.....
0020 00 0c 3c 14 40 01 ed 00 00 00 00 e6 d6 0b 0a ...<@.....
0030 0c 00 00 00 e1 00 e9 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 .....!{ 7...!{7-
0050 80 2c 3b 00 00 05 00 00 00 00 f0 00 11 00 00 0b ...;@.....
0060 6a 75 69 63 65 72 2d 7f 69 66 69 61 08 8c 12 98 juicer-wifi....
0070 24 b0 48 69 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 18 01 00 US $-d-....
0090 00 0f ac 04 02 00 30 02 80 00 2d 1a 6e 00 1b ff .....-0.....
00a0 00 0f ac 04 02 00 30 02 80 00 2d 1a 6e 00 1b ff .....-0.....
00b0 ff ff 00 00 00 00 00 00 00 00 01 00 00 00 00 .....@.....
00c0 00 00 00 00 00 00 3d 16 24 05 00 00 00 00 00 .....-$.
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 02 01 00 30 ea ff .....-0.....
00f0 00 00 ea ff 00 c9 05 01 2a 00 fc ff c3 04 02 .....-P.....
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 .....-BC^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=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:

```

> 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: 22
  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
> 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
> Tag: Vendor Specific: Microsoft Corp.: WMM/WME: Parameter Element
  Tag length: 10
  Vendor ID: 00:00:00
  Vendor Specific: 00 00 00 00 00 00 00 00 00 00
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 00 a3 24 bc 2e 00 00 00 00 ...:.....$.
0020 00 0c 3c 14 40 01 ed 00 00 00 00 3c 5a 0f 0a ...<@.....<Z.
0030 0c 00 00 00 e1 00 e9 01 ed 02 80 00 00 00 ff ff ...:.....
0040 ff ff ff ff 04 f0 21 7b 37 c2 04 f0 21 7b 37 c2 ...!{ 7...{7.
0050 50 13 3b 00 95 01 00 00 00 00 f0 00 11 00 00 0b ...P.....
0060 6a 75 69 63 65 72 2d 77 69 66 69 01 08 8c 12 98 ...juicer-wifi....
0070 24 b0 48 60 6c 03 01 24 05 04 00 02 00 00 07 0c ...$H'L$.
0080 55 53 20 24 08 17 64 0c 17 95 05 1e 30 16 01 00 ...US$.d....0...
0090 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ac 02 ...:.....
00a0 0c 00 00 00 3b 02 80 00 2d 1a 6e 00 1b ff ff ff ...:.....n.....
00b0 00 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 ...:.....
00c0 00 00 00 00 3d 16 24 05 00 00 00 00 00 00 00 00 ...:=$.....
00d0 00 00 00 00 00 00 00 00 00 00 00 00 7f 08 04 00 ...:.....0.....
00e0 00 02 00 00 00 40 bf 9c b2 01 00 30 ea ff 00 00 ...:.....0.....
00f0 ea ff 00 00 c0 05 01 2a 00 fc ff c3 04 02 2e 2e ...:.....*.....
0100 2e dd 18 00 50 f2 02 01 01 01 00 03 a4 00 00 27 ...:P.....!
0110 a4 00 00 42 43 5e 00 62 32 2f 00 ...:BC^b 2/.

```

10. Truncated PMKIDCount field:

- 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**.
- Reset ports and sniff packets:
Repeat steps B through D of [Step 2](#).
- 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:

```

> Fixed parameters (12 bytes)
> Tagged parameters (188 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: 21
    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
  > [Malformed Packet: IEEE 802.11]
    > [Expert Info (Error/Malformed): Malformed Packet (Exception occurred)]
      [Malformed Packet (Exception occurred)]
      [Severity level: Error]
      [Group: Malformed]
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 00 c6 03 84 c9 00 00 00 00 ...:.....;..
0020 00 0c 3c 14 40 01 ee 00 00 00 00 a3 3b 1b 0a ...<@.....;..
0030 0c 00 00 00 e3 00 eb 01 ee 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 ...P.....
0050 50 13 3b c0 b7 00 00 00 00 f0 00 11 00 00 0b ...:.....
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 01 02 00 00 07 0c ...$H'L$.
0080 55 53 20 24 08 17 64 0c 17 95 05 1e 30 15 01 00 ...US$.d....0...
0090 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ac 02 ...:.....
00a0 0c 00 00 3b 02 80 00 2d 1a 6e 00 1b ff ff ff ff ...:.....n.....
00b0 00 00 00 00 00 00 00 00 01 00 00 00 00 00 00 00 ...:=$.....
00c0 00 00 00 3d 16 24 05 00 00 00 00 00 00 00 00 00 ...:=$.....
00d0 00 00 00 00 00 00 00 00 00 00 00 7f 08 04 00 00 ...:.....0.....
00e0 02 00 00 00 40 bf 9c b2 01 00 30 ea ff 00 00 ea ...:.....0.....
00f0 ff 00 00 c0 05 01 2a 00 fc ff c3 04 02 2e 2e 2e ...:.....*.....
0100 dd 18 00 50 f2 02 01 01 01 00 03 a4 00 00 27 a4 ...:P.....!
0110 00 00 42 43 5e 00 62 32 2f 00 ...:BC^b2 /.

```

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:

```

  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 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)
  -----
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  ..c...
0020 00 0c 3c 14 40 0f 00 00 00 00 00 00 00 00 00  ..<...f...
0030 0c 00 00 00 a2 00 ec 01 ed 02 00 00 00 00 ff ff  ..<...f...
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 00 00 11 00 00 0b  ..;.....
0060 6a 75 69 63 65 72 2d 77 69 66 69 01 08 8c 12 98  juicer-wifi...
0070 24 b0 4b 60 6c 03 01 24 05 04 00 02 00 00 07 0c  S-H-L-S .....
0080 55 53 20 24 08 17 64 0c 17 95 05 1e 30 1a 01 00  US S-d .....
0090 00 0f ac 04 01 00 00 0f ac 04 01 00 00 0f ac 02  ..n...n...
00a0 0c 00 00 00 00 0f ac 00 3b 02 00 00 2d 1a 6e 00  ..n...n...
00b0 1b ff ff ff 00 00 00 00 00 00 00 00 00 01 00 00  ..n...n...
00c0 00 00 00 00 00 00 00 00 3d 15 24 05 00 00 00 00  ..n...n...
00d0 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ..n...n...
00e0 7f 08 04 00 00 02 00 00 00 40 bf 0c b2 01 00 30  ..n...n...
00f0 ea ff 00 00 ea ff 00 00 c0 05 01 2a 00 fc ff c3  ..n...n...
0100 04 02 2e 2e 2e dd 18 00 50 f2 02 01 01 01 00 03  ..n...n...
0110 a4 00 00 27 a4 00 00 42 43 5e 00 62 32 2f 00  ..n...n...
```

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:

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 00	77 1f 15 f0 00 00 00 00	W.....
0020	00 0c 3c 14 40 01 ee 00	00 00 00 00 6a 6d 1f 0a	...<@...jm...
0030	0c 00 00 00 e2 00 e9 01	ee 02 80 00 00 00 ff ff	
0040	ff ff ff ff 04 f0 21 7b	37 c2 04 f0 21 7b 37 c2	l{ 7...{7...
0050	50 12 3b 00 87 00 00 00	00 00 f0 00 11 00 00 0b	P.....
0060	6a 75 69 63 65 72 d7 7f	69 66 69 01 08 8c 12 98	juicer-w ifi.....
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 10 01 00	US \$-d-....
0090	00 0f ac 04 01 00 00 0f	ac 04 01 00 00 0f ac 02	
00a0	0c 00 00 00 00 0f ac 06	00 30 02 00 00 2d 1a 0e	P.....
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	00 3d 16 24 05 00 00 00	=-\$....
00d0	00 00 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 40 bf 0c b2 01 00	@.....
00f0	30 ea ff 00 00 ea ff 00	00 c0 05 01 2a 00 fc ff	0.....
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 62 32 2f 00	BC^b2/...