CC31xx Connection Policy

Overview

Profiles are designed to allow connection to pre-defined stored Access Points. Connection policy allows automatic and fast connection by controlling how the SimpleLink device attempts to connect to an AP.

A WLAN profile provides the information required to connect to a given AP. This includes the SSID, security type and security keys. Each profile refers to a certain AP. The Profiles are stored in the NVMEM (non-volatile memory), and therefore are preserved during device reset.
The following APIs are available for handling profiles:

- "sl_WlanProfileAdd" - Used for adding a new profile. SSID and security info shall be provided, where returned value refers to the stored index (out of the 7 available)
- "sl_WlanProfileDel" - Used for deleting a certain stored profile, or for deleting all at once. Index shall be the input parameter
- "sl_WlanProfileGet" - Used for retrieving information of certain stored profile. Index shall be the input parameter

For additional information about these APIs, please refer to the doxygen API manual.

WLAN connection policy defines three options to connect the SimpeLink device to a given AP:

- Auto: The device attempts to connect to an AP from the stored profiles based on priority. Up to 7 profiles are supported. Upon connection attempt, the device selects the highest priority profile. If several profiles are within the same priority, decision will be made based on security type (WPA2 -> WPA -> OPEN). If security type is also the same, selection will be based on received signal's strength.
- Fast: The device attempts to connect to the last connected AP. In this mode "probe request" is not transmitted prior to "authentication request", as both the SSID and channel are known in this mode.
- Auto SmartConfig: After booting CC3100 device will start the smartconfig process in case no command is received by host.

The configuration is performed by using the following API: "sl_WlanPolicySet". For additional information about this API, please refer to the doxygen API manual.

Please download the latest SDK for the complete example code.

```
 /* Reset policy settings */
 sl_WlanPolicySet(SL_POLICY_CONNECTION ,
SL_CONNECTION_POLICY(0,0,0,0,0), 0, 0);

 /* Enable auto connect (connection to stored profiles according to
priority) */
 /* Connection should first be established to the higher (secured)
profile */
 sl_WlanPolicySet(SL_POLICY_CONNECTION ,
SL_CONNECTION_POLICY(1,0,0,0,0), 0, 0);

 /* Enable fast connect (connection to last connected AP) */
 sl_WlanPolicySet(SL_POLICY_CONNECTION ,
SL_CONNECTION_POLICY(1,1,0,0,0), 0, 0);

 /* Enable Auto Smartconfig policy */
 sl_WlanPolicySet(SL_POLICY_CONNECTION ,
SL_CONNECTION_POLICY(0,0,0,0,1), 0, 0);
```

WLAN connection policy also defines an options to connect the SimpeLink device to a P2P device. Refer to P2P example for more details.

Application details

The application initializes the device and adds two profiles, one, a unsecured AP profile with priority 6 and the other WPA2 secured AP profile with priority 7 It then enables 'Auto' connect policy. The device shall connect to the available AP of highest priority (secured) profile.

Application deletes all the profiles and sets the policy to 'auto smart config' and resets the device, upon reset after waiting 2 seconds for command, device will go to SmartConfig mode.

Application deletes all the profiles, connects to the open AP, set the connection policy to 'Fast Connect' and resets the device. Upon reset device will connected to last connected AP.

Source Files briefly explained

i. main - Initializes the device, adds profiles and sets connection policies

Usage

- Open 'main.c' and change 'UNSEC_SSID_NAME', 'SEC_SSID_NAME' and 'SEC_SSID_KEY' as per your local n/w
- Build and launch the project

```
   The application adds both secured (priority 7) and unsecured AP
profiles sockets(priority 6) and sets the connection policy to AUTO
   The device tries to connect to AP - Upon connection attempt, the
device selects the highest priority profile. If several profiles are
within the same priority, decision will be made based on security type
(WPA2 -> WPA -> OPEN)
   The application sets the 'Auto SmartConfig' policy and resets the
device
```

- Open the SmartConfig application and complete the provisioning process
- The application then connects to the open AP, enables FAST policy and resets the device

```
   On reset, the device tries to establish connection w/ the last
connected AP, which in our case is the open AP
```

Limitations/Known Issues

None

Article Sources and Contributors

CC31xx Connection Policy *Source*: http://ap-fpdsp-swapps.dal.design.ti.com/index.php?oldid=188573 *Contributors*: A0131814, Giansway