ArubaOS (stand-alone) OpenRoaming configuration snippets

ArubaOS OpenRoaming configuration snippets

This configuration was tested on ArubaOS 8.7.1.1 (Vela build). Configuration of OpenRoaming (and Passpoint in general) is not possible via the UI, one needs to resort to CLI mode. The total configuration consists of multiple building blocks, each of which has its own section below. Much of it is copy&paste - the bits to adapt are marked with ⚠️.

Main body: "wlan ssid-profile" definition

```
wlan ssid-profile PasspointAruba
  enable
  type employee
  ⚠️essid PasspointAruba                                 # ANPs choice and irrelevant for OpenRoaming
purposes
  opmode wpa2-aes
  max-authentication-failures 0
  auth-server OR_Proxy_eduroamOT                         # we will only connect you if you are an eduroam
SP! Definition see below.
  rf-band all
  captive-portal disable
  dtim-period 1
  broadcast-filter arp
  dmo-channel-utilization-threshold 90
  local-probe-req-thresh 0
  max-clients-threshold 64
  hotspot-profile OpenRoaming                            # the important bit. Definition see below.
```

Passpoint with OpenRoaming RCOIs: "hotspot-profile" definition

```
hotspot hs-profile OpenRoaming
  enable
  no comeback-mode
  no asra                                                # no captive portal on this network
  internet                                               # internet access is provided
  no pame-bi
  no group-frame-block
  no p2p-dev-mgmt
  no p2p-cross-connect
  addtl-roam-cons-ois 0                                  # there are not more than 3 roaming consortium OIs
(-> no ANQP queries to be run)
  gas-comeback-delay 500
  query-response-length-limit 6
  access-network-type private                            # eduroam networks are private to the R&E community
  ⚠️venue-group business                                  # adjust to the classification of your hotspot
  ⚠️venue-type research-and-dev-facility                  # adjust to the classification of your hotspot
  roam-cons-len-1 5                                      # OpenRoaming RCOIs are always 4.5 bytes long (5
octets rounded)
  roam-cons-oi-1 5a03ba0000                             # the main OpenRoaming RCOI: "OpenRoaming-All"
(unsettled access, all identities welcome, baseline QoS)
  roam-cons-len-2 3                                      # Cisco's legacy OpenRoaming RCOI is 3 bytes long
  roam-cons-oi-2 004096                                 # Cisco's legacy OpenRoaming RCOI, still needed for
their OpenRoaming app and Samsung OneUI onboarding workflow
  roam-cons-len-3 0
  advertisement-profile anqp-venue-name YourVenueInfo   # description of the venue in ANQP. Definition see
below.
  advertisement-profile anqp-roam-cons OpenRoaming      # in case a station does run ANQP for the list of
RCOIs, also add the same RCOIs as an ANQP element
  advertisement-profile anqp-roam-cons OpenRoamingCiscoLegacy # in case a station does run ANQP for the list of
RCOIs, also add the same RCOIs as an ANQP element
  advertisement-profile anqp-nai-realm OpenRoaming_ANY_Realm # likely to be optional, but found to make the AP
work when it didn't without it. Advertises the realms allowed to connect to this hotspot
```

Uplink to authentication server: "auth-server"

The uplink can be realised over "good old" RADIUS/UDP, but then a shared secret and static IP address need to be negotiated with eduroam OT. Or, as a holder of a eduPKI RADIUS/TLS certificate, the connection can be established over RADIUS/TLS ("RadSec"). Pick one of the two variants below.

RADIUS/UDP

```
wlan auth-server OR_Proxy_eduroamOT
  ⚠️ip ...                                                    # IP address of the preliminary OpenRoaming ANP-
side proxy of eduroam OT
  port 1812
  acctport 1813
  ⚠️key ...                                                   # your shared secret for the preliminary
OpenRoaming ANP-side proxy of eduroam OT
  service-type-framed-user 1x
```

RADIUS/TLS

```
wlan auth-server OR_Proxy_eduroamOT
  radsec
  ip openroaming-ap.eduroam.org                              # this is the real hostname
  port 1812                                                  # these don't matter, it is an ArubaOS artifact.
The port used is TCP/2083.
  acctport 1813                                              # these don't matter, it is an ArubaOS artifact.
The port used is TCP/2083.
  rfc5997 auth-only
  service-type-framed-user 1x


# the certificates themselves need to be uploaded in the web interface (Maintenance -> Certificates -> Upload ->
Client/Trusted CA)

wlan cert-assignment-profile
  pki-cert-assign application radsec cert-type ClientCert certname RADIUS-TLS-Cert # "RADIUS-TLS-Cert" is the
friendly name given to the client certificate during upload
  pki-cert-assign application radsec cert-type TrustedCA certname eduPKI-Root      # "eduPKI-Root" is the
friendly name given to the Trusted CA certificate during upload
```

Venue information in ANQP: "anqp-venue-name"

```
hotspot anqp-venue-name-profile YourVenueInfo
  enable
  ⚠️venue-group business                                     # repeats beacon info (see above) in ANQP
  ⚠️venue-type research-and-dev-facility                     # repeats beacon info (see above) in ANQP
  venue-lang-code eng                                        # a descriptive name for the venue in English
language follows
  ⚠️venue-name "RESTENA Offices"                             # the name in English
```

RCOI information in ANQP: "anqp-roam-cons"

```
hotspot anqp-roam-cons-profile OpenRoaming
  enable
  roam-cons-oi-len 5
  roam-cons-oi 5A03BA0000

hotspot anqp-roam-cons-profile OpenRoamingCiscoLegacy
  enable
  roam-cons-oi-len 3
  roam-cons-oi 004096
```

Realm information in ANQP: "anqp-nai-realm"

```
hotspot anqp-nai-realm-profile OpenRoaming_ANY_Realm
  enable
  nai-realm-name *
  nai-realm-eap-method peapmschapv2
  nai-realm-auth-id-1 reserved
  nai-realm-auth-value-1 reserved
  nai-realm-auth-id-2 reserved
  nai-realm-auth-value-2 reserved
  nai-realm-encoding utf8
  no nai-home-realm
```