hotspot

Overview

Hotspot is a CCSP component that provides the connectivity to the users of Service provider even if not in the range of home device WiFi. This component provides wireless connectivity to a user from a third persons device belonging to a same service provider. This helps the users to stay connected over the service provider WiFi network even outside the home network.

Hotspot offers connectivity over both 2.4GHz and 5GHz frequency range. The SSID for hotspot is same for all the devices. From WEBUI a MSO user can see the exhaustive list of all the client devices connected to the gateway over Hotspot SSID.

What is Passpoint (hotspot 2.0)?

Wi-Fi CERTIFIED Passpoint® is an industry-wide solution to streamline network access in Wi-Fi hotspots and eliminate the need for users to find and authenticate a network each time they connect. In Wi-Fi networks that do not support Passpoint®, users must search for and choose a network, request the connection to the access point (AP), and re-enter authentication credentials each visit to gain access to a hotspot location, such as a restaurant, stadium, airport, or hotel. Passpoint automates the entire process, enabling a seamless connection between Wi-Fi hotspot networks and mobile devices, all while delivering enterprise-level security.

Passpoint features

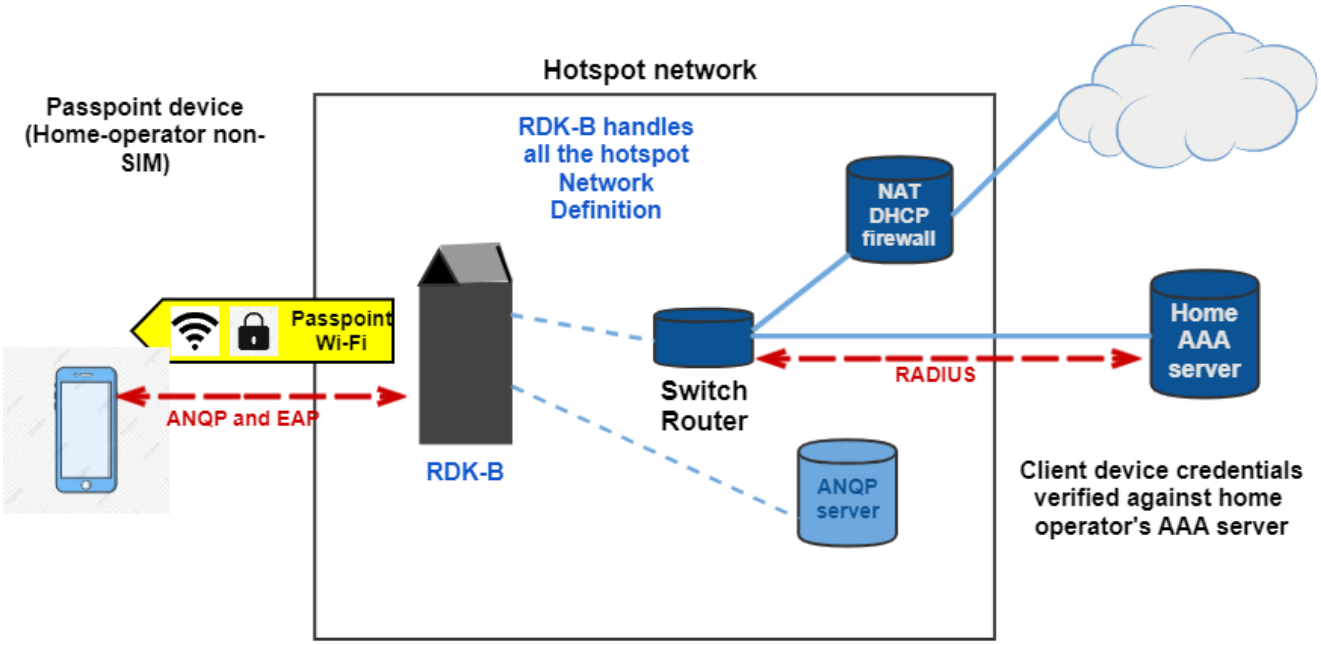
Passpoint improves the mobile user experience by offering:

1. Automatic network discovery and selection
2. Simplified online sign-up and instant account provisioning
    - In the Wi-Fi CERTIFIED Passpoint® certification program, mobile devices use Online Sign-Up (OSU) to accomplish registration and credential provisioning to obtain secure network access. Each Service Provider network has an OSU Server, an AAA Server, and access to a certificate authority (CA).
        - Issues certificates (i.e., creates and signs them)
        - Maintains certificate status information and issues Certificate Revocation Lists (CRLs)
        - Publishes its current (unexpired) certificates and CRLs so users can obtain the information they need to implement security services
        - Maintains archives of status information about the expired or revoked certificates it issued
3. Seamless network access and roaming between hotspots
4. Enhanced WPA2™-Enterprise and WPA3™

Passpoint Benefits

1. Mobile data offload
2. Wi-Fi roaming agreements across carriers and service providers
3. Opportunities to engage users and extract additional value from the network
4. Wi-Fi–based services such as Wi-Fi calling
5. Streamlined, enterprise-class device provisioning and credential management for enterprise and other private networks

Passpoint Architecture



ANQP

A mobile device uses ANQP to perform network discovery. The connection manager within the mobile device compares the information obtained from the hotspot via ANQP to the configuration information stored in the device, including Home SPpolicy and user preferences, to automatically select a hotspot network. The policy information is provisioned using methods that are outside the scope of the Passpoint certification

- To prevent airtime saturation with AP service advertisements, a subset of interworking information is advertised in beacons, but the remaining information is provided to clients only by request.
- The AP communicates the most vital information to all client stations, and then advertises a way for clients to individually discover more, if desired.

Advertisement Protocol Options

- ANQP (Access Network Query Protocol) — support for this protocol is mandatory **(RDK-B Implementation)**
- Media Independent Handover (MIH) Information Service — Defined by 802.21
- MIH Command and Event Services Capability Discovery
- Emergency Alert System (EAS) – supports emergency alerts from external networkstVendor-specific

ANQP Options using GAS (Generic Advertisement Service)

- The Generic Advertisement Service (GAS) is a framework that provides transport for advertisement services like ANQP. When a client must query the AP using an advertisement protocol, it uses GAS to do so. GAS provides a frame exchange process (GAS Request/Response) and a framing format (using 802.11 Action frames) for the advertisement services.

- The reason GAS is used is that prior to association, mobile devices have not obtained an IP address.

- The 802.11 protocol has a special frame type that can be used in this first stage (unauthenticated, unassociated) to invoke a specific action by the recipient. This is called a Public Action frame. 802.11u introduces new Public Action frame subtypes for GAS requests and responses, enabling the client to prompt the AP into action before an association is formed. This is critical for advanced network discovery capabilities and other future advertisement services.

ANQP Elements

These elements are used by the client stations to discover information that is not sent in beacons

.ANQP Query list — the Query List is sent by the client station in a GAS Request, indicating a list of elements (the elements listed below) it would like to receive in a GAS Response.

ANQP Capability list — this element is a bit like a checklist, identifying the ANQP elements that are supported (and will be returned in the GAS Response) by the AP.

EAP

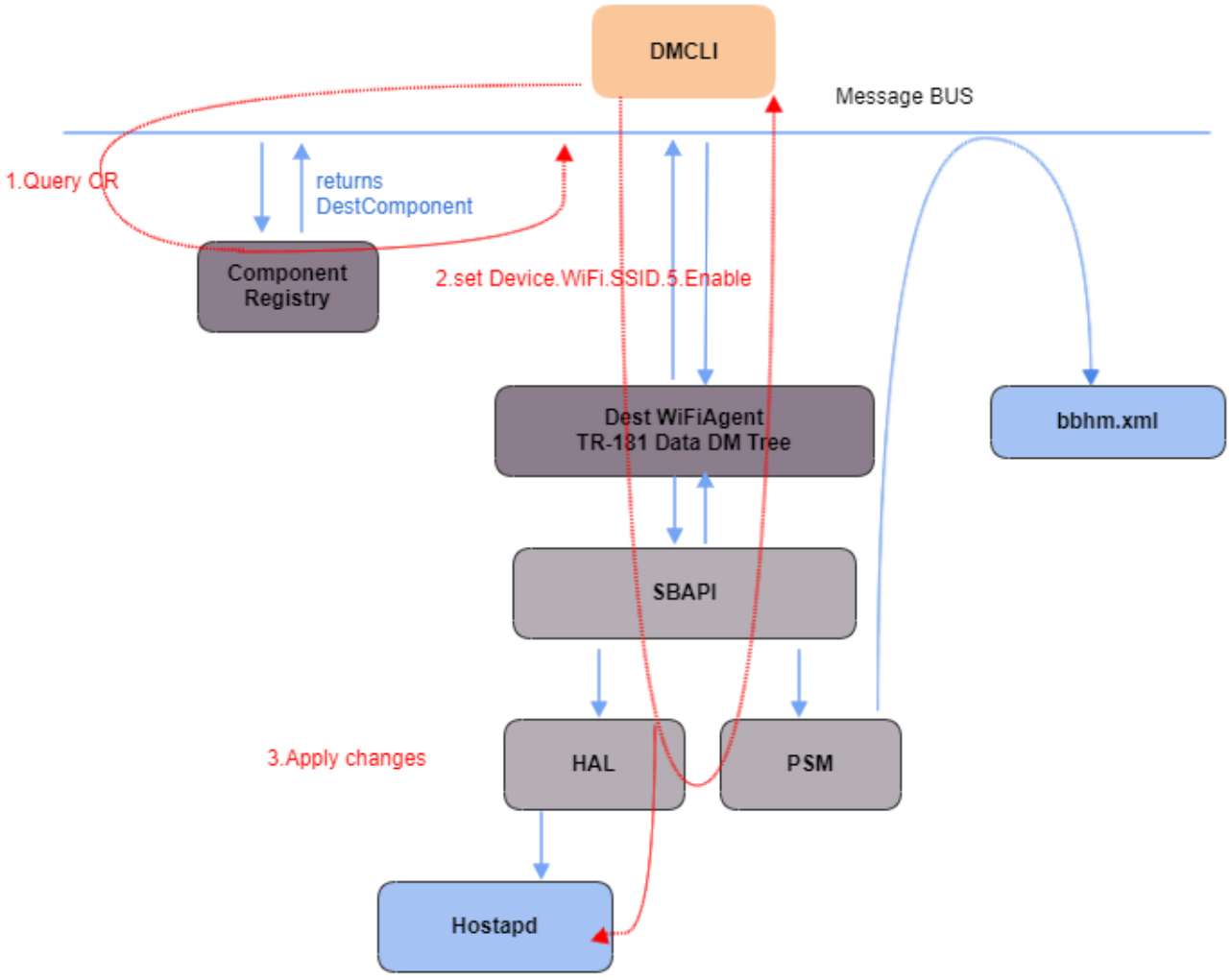
Extensible Authentication Protocol ('EAP') is an authentication framework frequently used in network and internet connections. It is defined in RFC 3748, which made RFC 2284 obsolete, and is updated by RFC 5247.

EAP is an authentication framework for providing the transport and usage of material and parameters generated by EAP methods. There are many methods defined by RFCs and a number of vendor specific methods and new proposals exist. EAP is not a wire protocol; instead it only defines the information from the interface and the formats. Each protocol that uses EAP defines a way to encapsulate by the user EAP messages within that protocol's messages.

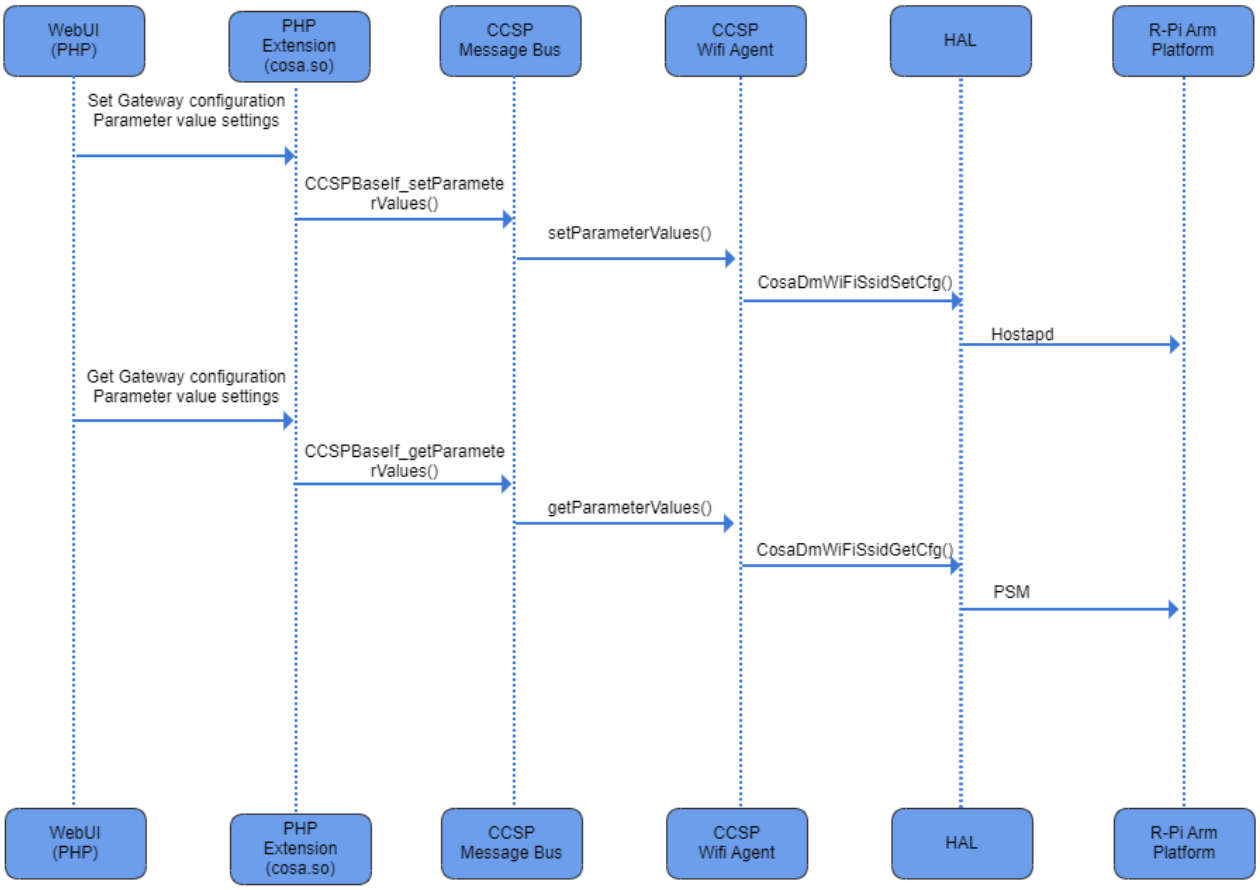
EAP is in wide use. For example, in IEEE 802.11 (WiFi) the WPA and WPA2 standards have adopted IEEE 802.1X (with various EAP types) as the canonical authentication mechanism.

Code Flow

- Configuring parameters using CCspWifiAgent module.



Sequence Flow



Objects

- Device.WiFi.SSID.5.Enable.
- Device.WiFi.SSID.5.SSID.
- Device.WiFi.SSID.5.
- Device.WiFi.SSID.6.Enable.
- Device.WiFi.SSID.6.SSID.
- Device.WiFi.SSID.6.

Retrieve value using dmcli command.

```
dmcli eRT getv Device.WiFi.SSID.5.Enable
CR component name is: eRT.com.cisco.spvtg.ccsp.CR
subsystem_prefix eRT.
getv from/to component(eRT.com.cisco.spvtg.ccsp.wifi): Device.WiFi.SSID.5.Enable
Execution succeed.
Parameter    1 name: Device.WiFi.SSID.5.Enable
              type:       bool,    value: true
```