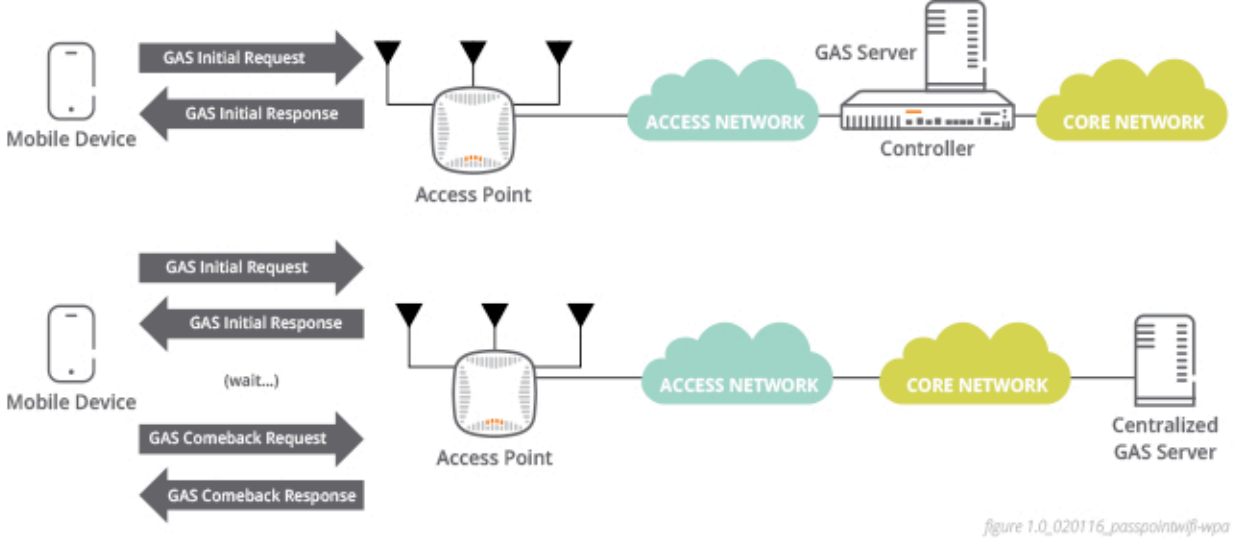

Figure 1. GAS 2-way and 4-way exchanges and back-end architecture (4-way exchange is used when response is too large to fit in one frame or takes too long to assemble)

The GAS request – response protocol

The GAS protocol allows a mobile device to query the access point for configuration and reachability information before association. The basic format of GAS is a client query transmitted in a GAS query frame, and the access point response in a GAS response frame. Since we envisage the ANQP-provided lists of service providers and capabilities may become extensive, Passpoint includes an outline architecture where a dedicated GAS server can be centralized in a hotspot network.

Whether due to a centralized server or large amounts of information, the GAS lookup behind the access point may incur delays or fill more than one frame, in which case the GAS query can be answered with a 'GAS initial response' where the access point says 'I'll get your information, but come back in X seconds', or 'it will take N frames'. This sets up the 4-frame exchange where the client pauses if necessary, then sends a number of 'GAS comeback request' frames, each triggering a GAS comeback response frame from the access point.

While we don't expect the comeback mechanism to be used very much in initial Passpoint networks, support for the longer 4-frame GAS exchanges is an option available in Passpoint Release 1.

ANQP elements

The information in the beacon will not normally be enough for the mobile device to decide it wants to connect to the hotspot, so once it sees the GAS indication in the beacon it will proceed with a GAS request for more information. Even in the initial release of Passpoint, ANQP can return a long list of elements:

- Venue Name information
- Network Authentication Type information
- Roaming Consortium list
- IP Address Type Availability Information
- NAI Realm list
- 3GPP Cellular Network information
- Domain Name list
- Hotspot Operator Friendly Name
- Operating Class
- Hotspot WAN Metrics
- Hotspot Connection Capability
- NAI Home Realm

Some of these are defined in the original 802.11u, others were added by the Wi-Fi Alliance, and the discussion below will not dwell on the detail of the specification, but rather the important capabilities. We will mention only those elements that are part of Passpoint Release 1, and only those we see as important in the short-term will be discussed in detail.

Service provider reachability

The most important function of Passpoint is to automate connection to subscription-authorized Internet hotspots. Before Passpoint, most hotspots supported a Captive Portal web page that offered a list of roaming partners. To connect, a user had to bring up a browser, pull down the roaming partner menu, select the appropriate partner and enter username/password credentials. This is already cumbersome for a PC user opening a laptop on a table, but it won't work at all for a smartphone or tablet in a pocket or purse. The key question to be answered is 'which of the service providers where I have a subscription can be reached through this hotspot'. Passpoint provides the answer to this question in a protocol, with no fewer than three different ways to identify a service provider

Cellular operators already use a unique addressing scheme for roaming. Each operator is identified by a PLMN ID, a combination of Mobile Country Code (MCC) and Mobile Network Code (MNC), where for instance T-Mobile in the US is MCC 310 MNC 026. Where the roaming partner for a hotspot is a cellular operator, it will be identified by MCC-MNC.

Other service providers will be identified by a domain name or Network Address Identifier (NAI), the NAI realm, for example 'attwireless.com'.

A third addressing scheme is the Organization Identifier (OI) for a Roaming Consortium (RC). The idea here is that all significant players in the hotspot business will register for an OI in a database maintained by the IEEE, identifying one organization or a group with shared authentication capabilities.

These three addressing schemes are not mutually-exclusive. Indeed, one could expect large cellular operators to use all three. Normally, each will lead to a particular authentication protocol as we will see later. And there are twists – most cellular providers will prefer to use EAP-SIM for SIM-capable mobile devices, but they may also offer password- or certificate-based authentication for non-SIM clients. This means they may appear as different options in the various ANQP responses.

Note that the hotspot operator appears as one of the available service providers, with no particular distinction. To determine which organization owns or manages the hotspot, it is necessary to check the home operator attributes explained below, and match them to available service providers.

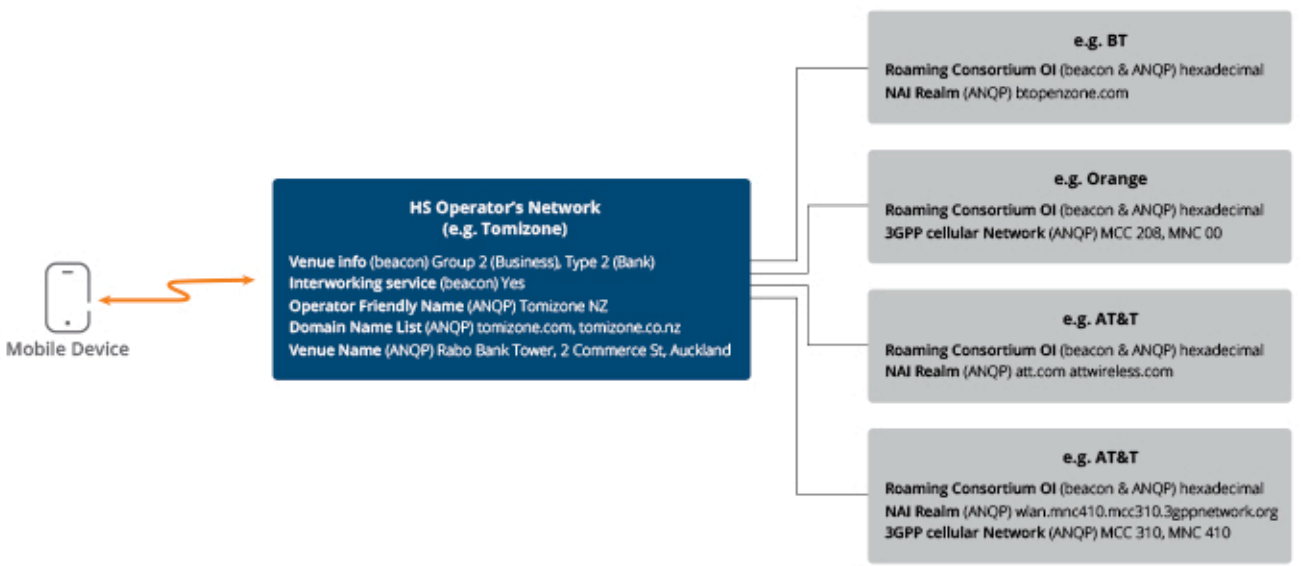

figure 2.0_020116_passpointwifi-wpa

Figure 2. Passpoint service provider addressing and labels available in the beacon and via ANQP

When a mobile device identifies a Passpoint hotspot, it will examine beacons and probe responses, then probably initiate a GAS/ANQP exchange to learn which service providers can be reached. It will then compare the list with its internal configuration. If there are multiple matches, a prioritization function will be required to determine the best choice.

Identification of the hotspot operator

It may be important to know who is operating the hotspot, so ANQP returns the hotspot operator's domain name (similar to the NAI realm above) and also an 'operator friendly name' which is a free-form text field that can identify the operator and also something about the location.

It's important to know the hotspot operator because if there's a choice of hotspots, even though the same service providers may be reachable through each, the pricing may be different. Similarly, an operator providing a device or subscription – assuming it has the ability to configure the device – would want to stay on its own network rather than a roaming partner's, all other factors being equal.

Other factors related to hotspot capabilities

Beyond service provider and hotspot operator identification, Passpoint provides many parameters that may be important in hotspot selection. We'll briefly describe each below:

Venue name and type. It may be important to connect to a particular hotspot because of its location. A stadium network may offer special services, so a fan would want to make sure the connection is to the arena Wi-Fi rather than a café next door. Passpoint provides space in the beacon for venue group and venue type codes, taken from the International Building Code. These are pre-defined generic codes like 'residential', 'educational', library' or 'museum'. There is also a text field for the 'venue name' in ANQP where the hotspot operator can enter a description.

IP addressing. Passpoint hotspots can indicate they support Ipv4 or Ipv6 addressing and routing and whether the address is NAT'd.

Internet reachability. Normally a mobile device is looking for an Internet connection. Where would one not want an Internet connection? Perhaps in a museum where there's a 'walled-garden' with services for visitors.

Peer-to-peer cross connect. This is a security consideration. A hotspot allowing P2P is effectively giving its users inside-the-firewall access to each others' devices. So Passpoint recommends that all user-to-user traffic be directed through a firewall, either behind or inside the access point, to reduce the risks, and provides an indication that this is in place.

Connection capability - Protocol filtering. In the same way that residential and enterprise Wi-Fi routers and WLANs can be set up to restrict traffic on some protocols and ports, it is envisaged that some Passpoint networks may have integral or upstream restrictions, and these can be advertised in ANQP.

ARP Proxy. The hotspot AP provides an ARP proxy service. This is useful for limiting broadcast traffic, and also improves security. It may be useful for the mobile device to know ARP proxy is in use.

Group-address restrictions. Even though WPA2-Enterprise is mandated for Passpoint (see below) the hotspot application differs somewhat from enterprise or home WLANs. Even though each user on a hotspot will have authenticated in some way and is trusted by their service provider, they should not necessarily trust each other or be allowed to share traffic. A WPA2 access point encrypts all data traffic, but in order to support multicast it needs to distribute a common multicast key to all clients – so every client can read every multicast frame. To prevent this and other attacks, it is suggested that when possible, Passpoint 2.0 access points disable multicast; this may not always be possible, for example in venues where multicast applications are commonly used.

Operating Class. This is a list of the channels the hotspot is capable of operating on. It may be useful where, for instance, a mobile device discovers a hotspot in the 2.4 GHz band but finds it is dual-band and prefers the 5 GHz band.

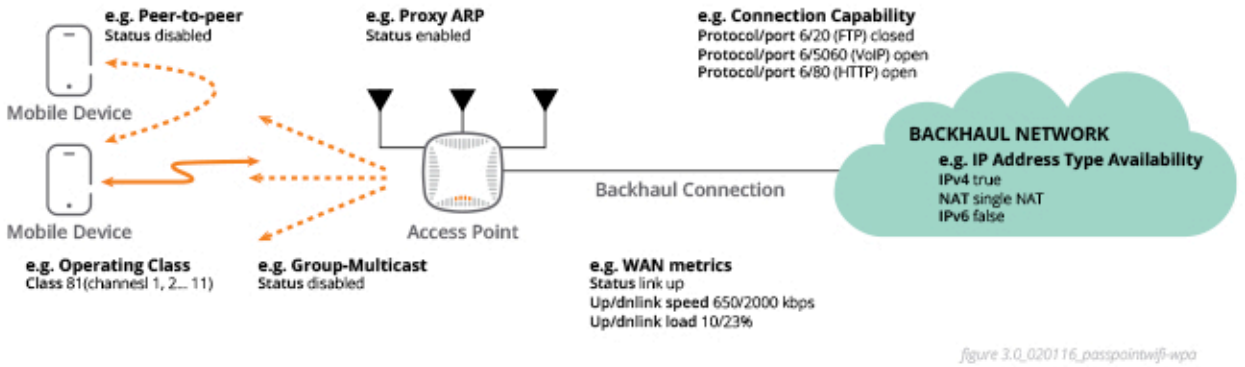

Figure 3. Configuration features and information provided by a Passpoint access point (examples simplified for clarity)

WAN metrics. The limiting factor in Internet bandwidth is likely to be the immediate backhaul connection from the AP. ANQP can provide information including the upstream and downstream bandwidths and current traffic and whether the connection is currently at capacity. This might be useful for a mobile device with a minimum (and large) bandwidth requirement for a particular application, or it could be used as a tie-breaker between two otherwise equivalent hotspot access points.

HESSID. Sometimes a number of hotspots will provide overlapping coverage for a zone, perhaps in a sports stadium or large shopping center. For this scenario, Passpoint provides a label for the zone so mobile devices have an easy way to recognize which access points offer the same capabilities. The HESSID needs to be a unique label, so it is chosen as one of the BSSIDs (MAC addresses) of the access points in the zone.

The Online Sign-Up Server

A new version of the Passpoint certification was launched in October 2014. It contains extensions to the original certification which are presently optional (i.e. a Wi-Fi device can be certified to Passpoint v1 or Passpoint v2) but will become mandatory early in 2016 (when Passpoint v1 certification will be discontinued).

Changes in Passpoint v2 are incremental and specify functionality for Online Sign-Up, Remediation and Policy services. These protocols provide service providers with standard ways to reach devices that may not have subscriptions, and to perform provisioning-related tasks.

The most popular function is Online Sign-Up (OSU). This performs a task known to many travelers and others who encounter hotspots where the captive-portal "splash" page invites them to sign up to get service on the network. Whereas this function is currently performed by Web pages, Passpoint v2 OSU uses a standard, secure protocol to exchange the required information between the mobile device and OSU server, across the WLAN.

If a user encounters a Passpoint hotspot which does not provide access to any service provider subscription configured on the mobile device, but the hotspot advertises "OSU service" in its beacon, the device should automatically make an ANQP request that returns a list of service provider OSUs that are available. The user selects a service provider and connects to an open "OSU SSID" – normally on the same access point as the Passpoint SSID – and then uses the URL to reach the service provider's OSU server, receiving a list of subscription options.

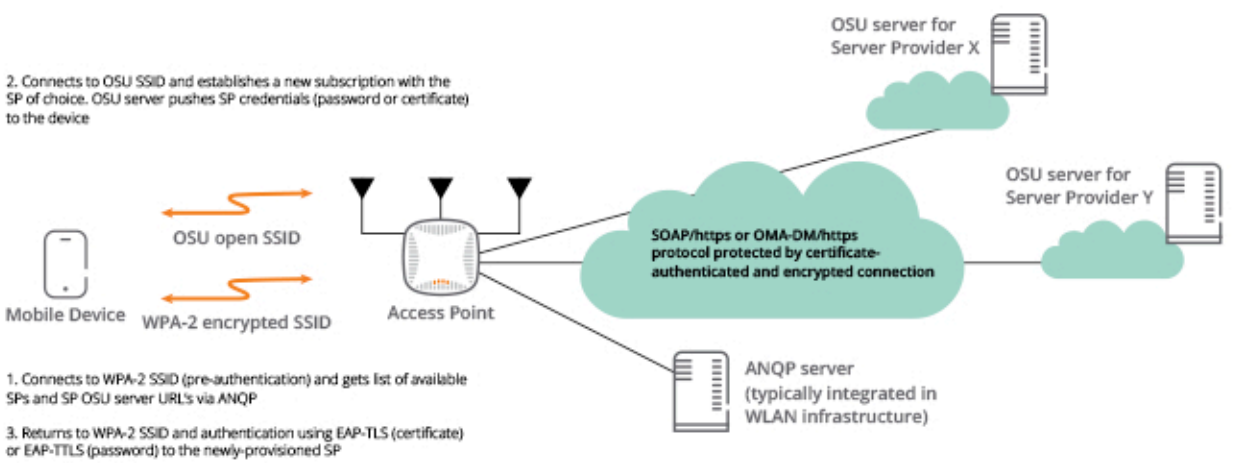

Figure 4. Online sign-up with OSU server associated with a Passpoint WLAN (simplified for clarity)