BUSINESS PAPER

aruba
a Hewlett Packard Enterprise company

Solving the Indoor Wireless Coverage Problem: Passpoint and Wi-Fi Calling

NEXT-GENERATION HOTSPOT FOR THE ENTERPRISE

TABLE OF CONTENTS

SUMMARY

This paper describes an approach to the in-building cellular coverage problem that allows an enterprise to provide dependable service for any cellular mobile device. It is supported by all major cellular operators in the US and is based on existing Wi-Fi infrastructure. By modifying the configuration of an existing wireless local-area network (WLAN) to enable Passpoint service and adding a secure RADIUS authentication link from the WLAN to a node in the operator roaming exchange ecosystem, enterprises can enable the large and growing population of Passpoint-configured smartphones to automatically connect to the WLAN and thereby gain access to data, Wi-Fi Calling, and SMS (text) services.

This approach requires no new hardware beyond ensuring seamless voice-grade Wi-Fi coverage across the desired area, and offers an effective alternative to complex, expensive DAS (Distributed Antenna System) build-outs that are the traditional remedy for gaps in cellular coverage. Wi-Fi, unlike DAS or cellular small cells, is inherently multi-operator and Passpoint profiles are found on the majority of SIM-based devices. Experience at Aruba trials and customer events has shown that enabling Passpoint results in an immediate connection for the majority of the devices that the public carry in their pockets with no action by the user.

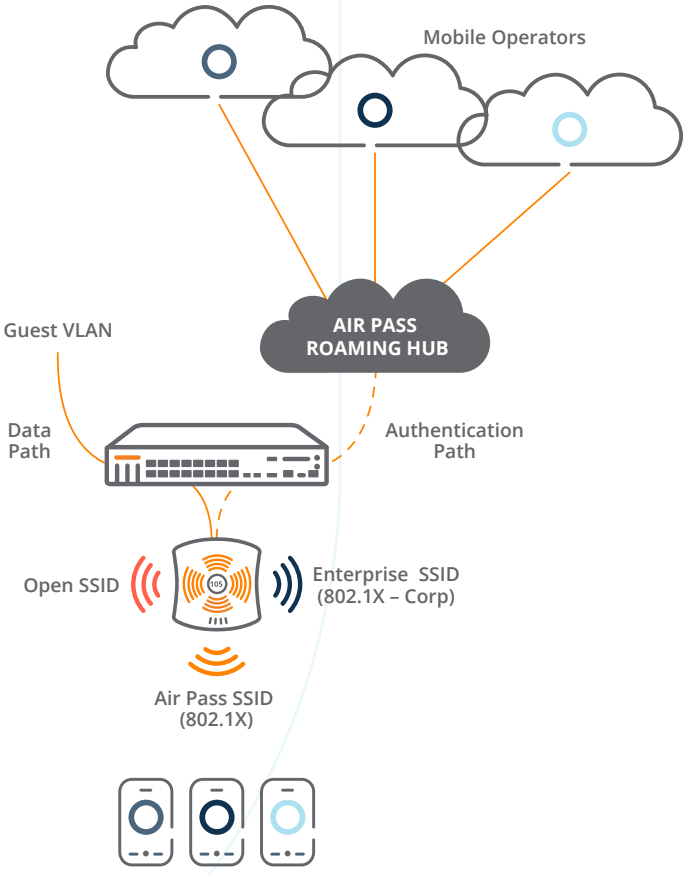
Passpoint, a Wi-Fi Alliance certification based on the 802.11 standard, offers possibilities beyond local cellular offload. International roaming for many major operators can be supported, a growing community of smart-cities is already starting to use Passpoint to offer roaming across the world, and enterprises can configure their own Passpoint profiles on devices for private guest-access purposes.

HOW IT WORKS

Using Wi-Fi to provide robust in-building or campus cellular coverage requires Passpoint to automatically discover and attach to an authorized Wi-Fi network and Wi-Fi Calling (WFC) for making and receiving voice calls. WFC is now pervasive globally – with over 92 operators in 49 countries active as of June 2019.[1] In the US alone, WFC is supported by 18 operators, while Canada has 10. Europe has 26 operators who support WFC, while the Asia-Pacific region has at least 23 operators. Eight operators in Latin America currently support WFC.

Passpoint traces its origins to the IEEE 802.11u amendment (also known as 'Hotspot 2.0') and subsequent Wi-Fi Alliance (WFA) 'Passpoint' certification program. Following the initial Passpoint launch, the Wireless Broadband Alliance (WBA), with Aruba participation, conducted a series of international "Next Generation Hotspot" carrier trials to verify performance in real-world networks and applications. Thus, this technology is well-understood and established. Over the last few years it has been adopted by AT&T Wireless as its preferred protocol for national Wi-Fi offload and international roaming, and it is supported by all major North American service providers. Internationally, operators in Europe and Asia are beginning to deploy Passpoint profiles as well.

A Passpoint-enabled cellular offload service requires three functions. Smartphones must be Passpoint-capable and configured with profiles that identify service providers; Wi-Fi access points must advertise a list of supported service providers; and a secure link must be established to the roaming exchange for authentication.



[1] https://support.apple.com/en-us/HT204040

For the first component, configured smartphones, the popular smartphone families (Android, Apple iOS and even Microsoft, with Windows 10) have incorporated Passpoint capabilities for some years now. All that remains is for cellular operators to specify Passpoint-certified devices, and to add the appropriate configuration profiles: each profile contains information identifying the service provider. For example, a smartphone could identify an AT&T-capable access point by

- 'MCC-MNC' (Mobile Country Code – Mobile Network Code, e.g. 310-410)
- 'NAI realm' (e.g. attwifi.com or wlan.mnc410.mcc310.3gppnetwork.org)
- 'OI' (Organization Identifier, not widely used)

The profile for the service provider will contain at least one of these elements, together with login credentials which, for most cellular operators, will point to the device's SIM card.

The smartphone OS vendors have added functionality to allow network-based configuration of Passpoint profiles, based on clicking links. But mobile operators prefer to configure Passpoint profiles on the special software builds they load on or push to subscriber devices.

Once a smartphone has a Passpoint profile, it regularly scans for Wi-Fi access points that use Passpoint to advertise their service provider reachability. This is done before association, so the smartphone can pick a suitable access point and know it will be able to get service before initiating authentication.

One key advantage of the Passpoint profile is that it is not linked to a particular SSID, so a single client profile will work across any WLAN that has appropriate Passpoint configuration. Organizations can add Passpoint service to any existing SSID that uses WPA2 or WPA3 authentication.

Aruba access points are Passpoint certified and can be easily configured to advertise Passpoint profiles, using the labels listed above. For cellular operators, typically MCC-MNC and NAI realm are used. An access point can advertise a very long list of service providers without burdening the beacon because Passpoint includes a new protocol, 'ANQP' (Access Network Query Protocol), that allows a device to query for particular service provider profiles, before associating.

Once the device has detected a match between a pre-configured profile and an access point's advertisements, it starts to authenticate. For this it needs a path to the service provider's authentication server, which is provided by an IPSec-encrypted RADIUS connection from the Aruba mobility controller to the service provider via the cloud. Authentication protocols supported by Passpoint include:

- EAP-SIM/AKA/AKA', using SIM credentials
- EAP-TTLS, using username-password
- EAP-TLS, using X.509 certificates

All these options use the WPA2/WPA3-Enterprise 802.1X protocol which protects credentials and encrypts over-the-air traffic.

The cloud RADIUS/RadSec link is used only for authentication traffic following the 802.1X protocol. Data-plane traffic remains on-campus and is routed by the WLAN. Most Aruba customers place Passpoint-attached clients in a guest role on the existing guest VLAN. This ensures that offload traffic is completely segregated from the corporate network, leveraging Aruba's built in role-based access control capability. Aruba's experience suggests that for most traditional office environments, enabling Passpoint-based cellular offload adds a minimal amount of new traffic, even while greatly increasing the number of devices attached to the WLAN.

The combination of Passpoint authentication and Wi-Fi calling enables robust in-building and campus cellular coverage, delivered over Wi-Fi. With this proven technology, it is not necessary to deploy costly and complex small cells, Citizen's Band Radio Service (CBRS), private LTE or 5G or, in most cases, distributed antenna solutions. Since cellular data and messaging services are carried over Wi-Fi without user intervention, Information Technology departments can address coverage problems and increase capacity with minimal additional investment.

By dramatically increasing the attach rate of smartphone devices to the WLAN, the utility of the Wi-Fi infrastructure as a sensor system is also enhanced. Applications such as shopper analytics in the retail vertical, space and energy/lighting optimization for facilities departments, and network security systems have greater visibility of visitor data traffic, location, and behavior.

ARUBA'S IMPLEMENTATION OF PASSPOINT

Aruba provides the functionality that allows an enterprise to launch a Passpoint service over its WLAN and support in-building cellular coverage for the devices in employees' and guests' pockets. It does this through:

- Wi-Fi Alliance CERTIFIED Passpoint functionality on mobility controller-based WLANs
- Fast configuration of the controller with per-operator predefined config
- Guidance on establishing a RADIUS/RadSec connection to route authentication traffic to the appropriate operators
- Control of user traffic through role-based management
- Tools to monitor Passpoint usage and assess Quality of Service (QoS)

FUTURE DEVELOPMENTS

While many operators support Passpoint based on SIM credentials. Passpoint also supports non-SIM credentials that may be issued by an enterprise and recognized across groups of enterprise networks. Since all current smartphones are Passpoint-capable, guest provisioning can take advantage of this standard feature: click-link or app-based provisioning can be used to install a Passpoint profile. This allows a multi-site or multi-brand enterprise to enable universal roaming across different campus network domains.

In the future, enterprises may form public or private roaming federations where members of one organization are allowed to roam onto the networks of others. Hotel chains, for instance, are starting to use Passpoint to give their loyalty-club members automatic connections at all properties in a federation, regardless of the locally-advertised SSID.

As Passpoint adoption progresses, more applications will be found for this secure, automatic, neutral host, SSID-independent network identification and connection functionality.

WIRELESS BROADBAND ALLIANCE NGH TRIALS

The underlying 802.11 specifications are developed in the IEEE, and the Wi-Fi Alliance is responsible for Passpoint certifications, but a third organization, the Wireless Broadband Alliance (WBA) has been most involved in moving Passpoint out of the lab and into production networks. The WBA, an industry group comprising service providers, equipment vendors and authentication services organizations, has been at the forefront of testing the technology under real-world conditions under its 'Next Generation Hotspot' (NGH) program.

A series of four NGH trials were conducted between 2011 and 2016, where mobile operators exchanged SIM cards and tested Wi-Fi roaming across the world. The WBA has published various reports from the NGH trials (e.g. https://www.wballiance.com/major-telcos-to-trial-next-generation-hotspots-using-firstcommercially-ready-equipment/) and lists of participating service providers, including the one below from the Phase 1 NGH trial. While not all these service providers have progressed to a commercial Passpoint service, they and others have used the WBA NGH trials to gain experience with Wi-Fi roaming using Passpoint.

Aircel	AT&T	Boingo Wireless	BT
BskyB (The Cloud)	China Mobile	Deutsche Telekom	DOCOMO InterTouch
Everything Everywhere	FON Wireless	Gowex	Indosat M2
HK CSL	KDDI	iBAHN	KT Corporation
Meteor Network	NTT DOCOMO	Oi Wi-Fi	Orange
PCCW Mobile	Portugal Telecom TMN	SK Telecom	Shaw Communications
Smart Communications	Softbank Mobile	StarHub	Swisscom
Talk Talk	TeliaSonera	Telefónica	TIM Brasil
Time Warner Cable	Tomizone	True Corp.	Trustive

Aruba was a significant participant in all phases of the NGH trials, and continues its engagement with the WBA, especially the Carrier Wireless Services Certification (CWSC) program https://www.wballiance.com/certification/, where testing labs are equipped to certify client devices, infrastructure and authentication services for carrier-specific NGH compatibility.

The WBA also coordinates member companies to provide NGH roaming over the Mobile World Congress industry conference and show in Barcelona. The graphic below shows dramatic growth of Passpoint-configured devices in recent years.

APPENDIX – PASSPOINT PROTOCOL AND OPERATION

Today's Wi-Fi access points have only one publicly-accessible identifier label, the SSID. Hence this must be used for multiple purposes. Most SSIDs reflect the organization operating the local access point, like "PEETS" or "moonrisehotel", while others indicate access to a service provider such as "attwifi". If one wished to show that the hotel also supported AT&T service, it would be necessary to advertise both SSIDs. While it's possible to broadcast several SSIDs on each physical access point, this is inefficient of airtime and should not be extended very far.

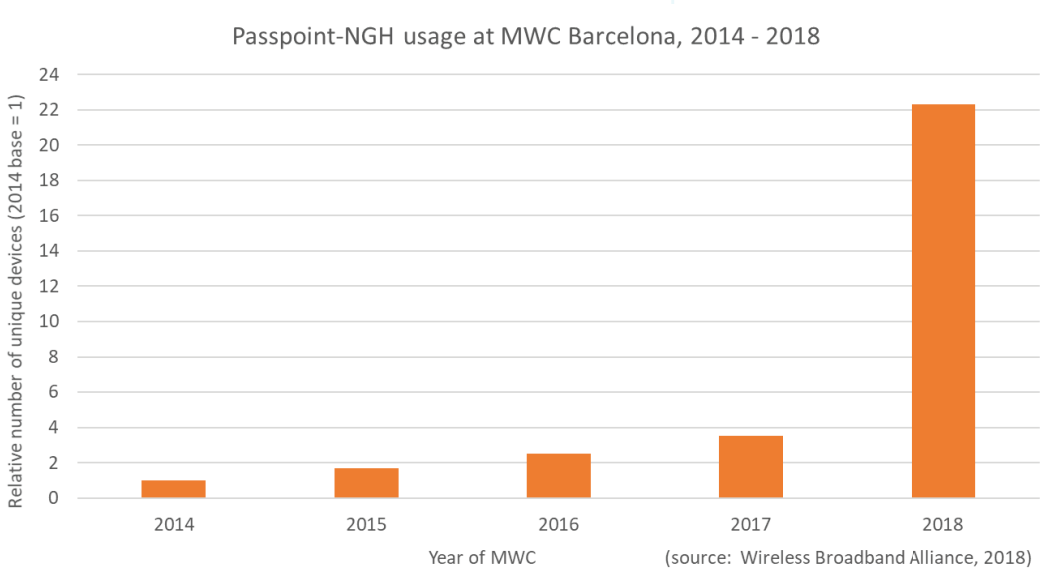
When a mobile device seeks an access point for Internet access, it has two options. Either it takes an internally configured list of SSIDs like 'attwifi' and looks for a match, or it tries to associate with every open SSID it sees, and tests to see if it can reach the Internet. In the former case it can miss opportunities, as it can't know about SSIDs which haven't been configured, while the latter is very time and power-consuming.

With Passpoint, the information about the services and service providers that are reachable via a hotspot are separated from the SSID. A new protocol allows the mobile device to discover a comprehensive profile of the hotspot before it associates, so it can quickly identify and prioritize hotspots suitable for its needs. The use of unambiguous, standard service provider names simplifies the task of matching a suitable hotspot to the device's available subscriptions.

With Passpoint, the mobile device can silently identify suitable access points and select the best match while still in the user's pocket. It can then automatically authenticate and start using the service while protected by state-of-the-art security.

The primary aim of Passpoint is to simplify and automate access to public Wi-Fi networks. The features allow a mobile device to identify which access points are suitable for its needs, and to authenticate to a remote service provider using suitable credentials. Technical details include:

- New information elements in beacons and probe responses
- A new GAS/ANQP protocol to allow pre-association queries of a hotspot's capabilities
- New information fields to allow a mobile device to learn which service providers are reachable via a hotspot
- New information fields to provide information about a hotspot's operator, venue and configuration
- Security features to further secure hotspots, clients and user traffic against attack



The structure of Passpoint – GAS and ANQP

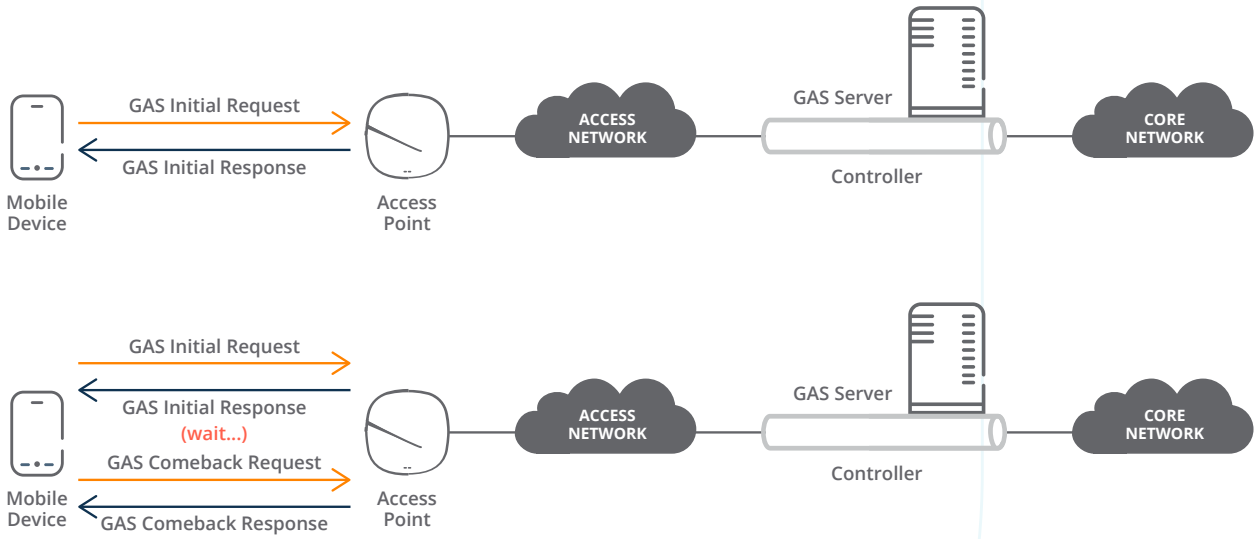
The key innovation in Passpoint is a new pre-association protocol that allows a mobile device to query the hotspot for various parameters. A pre-association protocol is considerably faster than requiring authentication before information can be learned, and saves battery life. But since the only preassociation capabilities to date are the beacon and probe response, and these are limited in how far they can be extended, it was necessary to invent a new protocol for capability discovery. This is called Access Network Query Protocol (ANQP).

ANQP is delivered inside the Generic Advertisement Service (GAS) protocol which will be used to transport other data in the future, but for our purposes with the current Passpoint release, GAS and ANQP may be used interchangeably. The IEEE 802.11 architecture allows the GAS/ANQP server to be centralized, separate from the WLAN architecture but in Aruba's architecture, the GAS/ANQP server function is always located in the controller.

New beacon and probe response information elements

Information elements are added to the beacon and probe response, including:

- Access network type, identifying whether hotspot is for public, private or guest access, etc.
- Internet bit, indicating the hotspot can be used for Internet access
- Advertisement protocol, indicates the hotspot supports GAS/ANQP
- Roaming consortium element, a list of up to 3 names of reachable service providers
- Venue information, describing the venue where the hotspot is situated
- Homogenous ESSID, a label identifying hotspots in a continuous zone
- P2P and cross-connect capability (more later)
- BSS load element, an indication of current load on the access point originally from 802.11e



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)

It may be possible for a mobile device to decide whether to use a hotspot based just on the information in beacons and probe responses. A quick scan will allow the device to build a list of Passpoint-capable access points, whether they provide Internet access and a (possibly incomplete) list of service providers available via that hotspot.

Passive radio use – listening for beacons – is less battery-consuming than active probing where frames are transmitted, but the long interval between beacons (usually ~100msec) means that in practice, devices follow an active-scan regime, sending probes every minute or so. Passpoint allows probe requests to be directed: for instance, if a flag is set in the probe request, only those access points supporting Internet access will respond. This reduces frames on the air and potentially means the mobile device can spend less time listening for responses.

In most cases the device will identify access points in the area using probe requests, then proceed with GAS/ANQP to get a more complete picture of the services and service providers offered, allowing it to select the best match for its needs.

ANQP elements

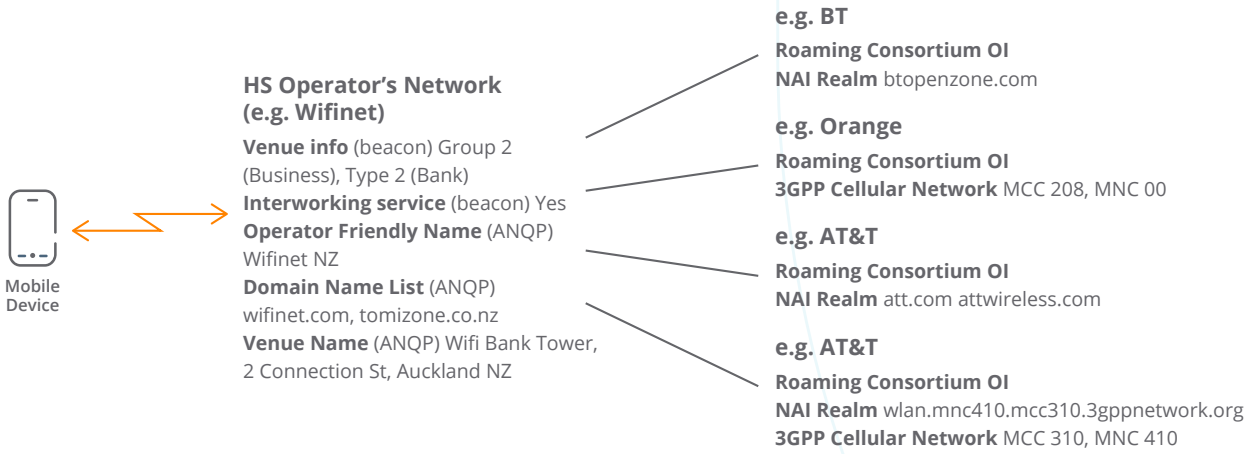
The information in the beacon will not normally be enough for the mobile device to decide it wants to connect to the hotspot, so once it sees the ANQP indication in the beacon it will proceed with an ANQP request for more information. Even in the initial release of Passpoint, ANQP can return a long list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

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 an over-the-air protocol, with no fewer than three different ways to identify a service provider.



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

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 realm), for example 'attwireless.com'.

A third addressing scheme is the Organization Identifier (OI) for a Roaming Consortium (RC). This is intended for significant players in the hotspot business, who will register for an OI in a database maintained by the IEEE, identifying a single organization or a group with shared authentication capabilities. The OI is not widely used at this time.

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. And there are twists – most cellular providers will prefer to use EAP-AKA 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.

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 determines the best choice.

Identification of the home operator

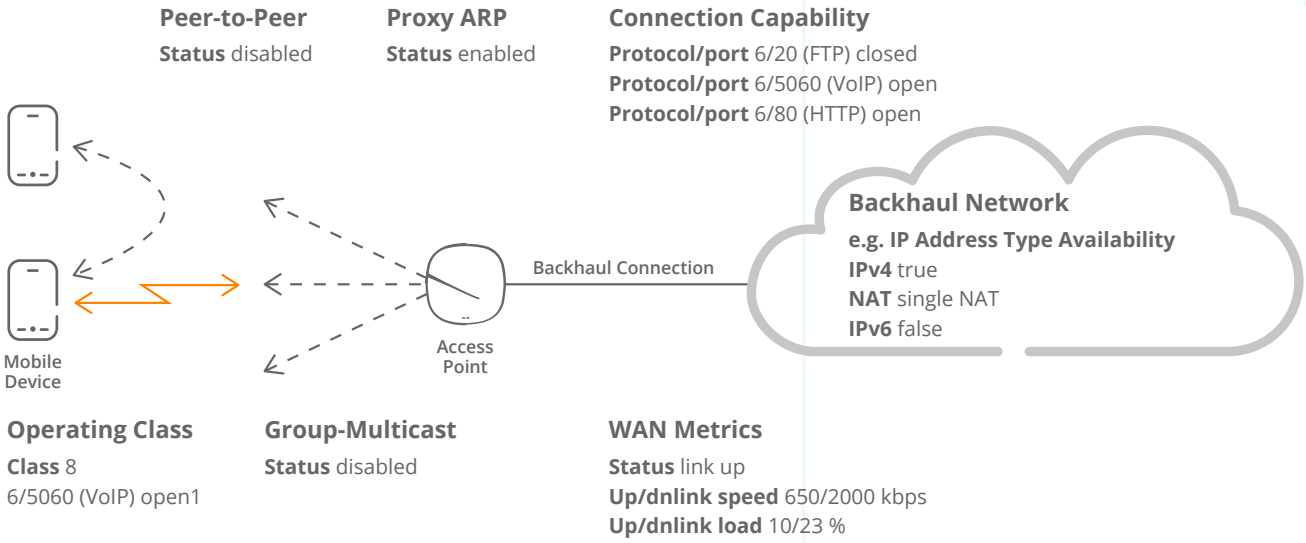
It may be important to know who is operating the hotspot, so ANQP returns the hotspot operator's domain name (similar to the NAI realm above) and also an 'operator friendly name' which is a free-form text field that can identify the operator, and also something about the location.

Other factors related to hotspot capabilities

Beyond service provider and hotspot operator identification, Passpoint provides many parameters that may be important in hotspot selection.

- **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 spectator 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 other's 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 may provide 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**. While WPA2/WPA3-Enterprise is mandated for Passpoint, 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/WPA3 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 Passpoint 2.0 access points disable multicast, instead converting multicast frames to unicast over-the-air, where each will be protected by a key unique to the respective client.
- **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 2.4GHz band but finds it is dual-band and prefers the 5GHz band.
- **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, current traffic levels 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.



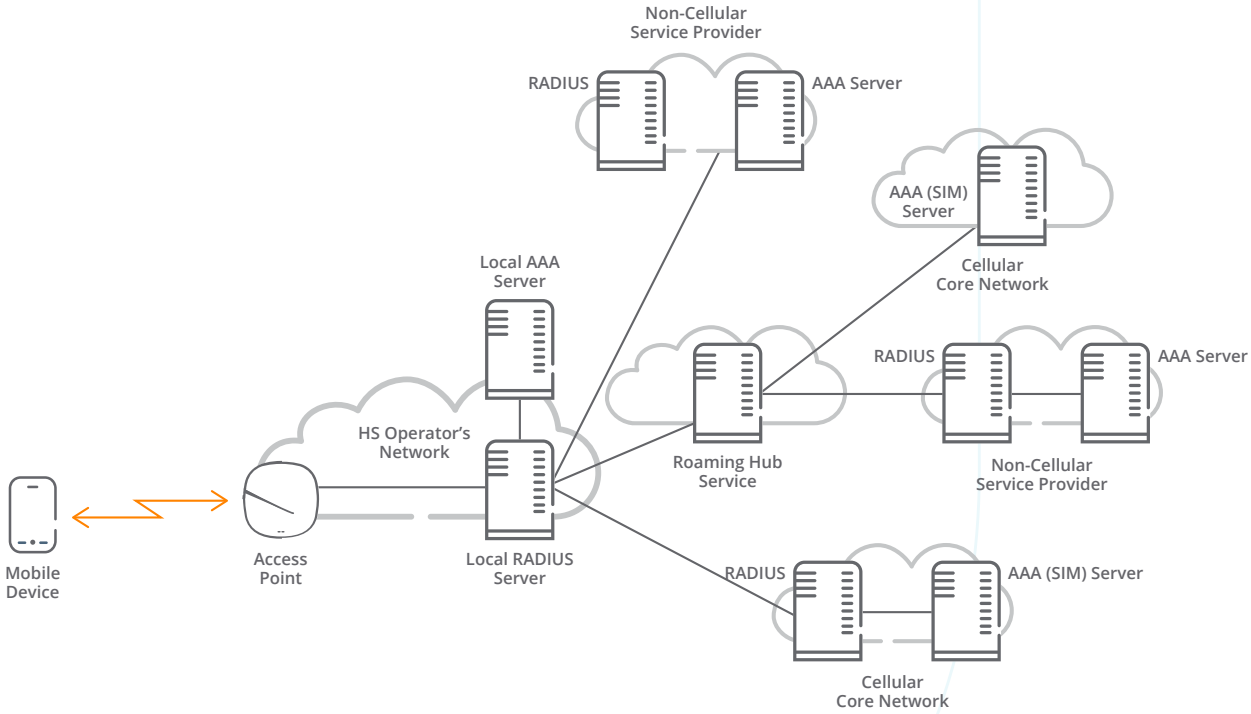
Configuration features and information provided by a Passpoint access point
(examples simplified for clarity)

- **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.

Authentication to remote service providers

Despite its focus on authentication and authenticator choices and capabilities, Passpoint makes no changes to authentication protocols. The new information in the beacon and ANQP allows the mobile device to determine if a particular hotspot has connections to a service provider who can authenticate it, given its choice of credentials, and to choose between hotspots if more than one match exists. But at the end of the hotspot discovery and selection phase, the Passpoint involvement is over, and the mobile device initiates a 'normal' authentication.

Passpoint mandates WPA2/WPA3-Enterprise, specifying five EAP types within WPA2/WPA3-Enterprise that are already tested and certified by the Wi-Fi Alliance: the innovation in Passpoint is in allowing the mobile device to identify the service providers and capabilities of a hotspot before association and authentication, rather than the authentication itself. We will continue here with the authentication phase because it's an integral part of the hotspot experience.



Authentication paths with Passpoint

When ANQP returns a list of reachable service providers ready to authenticate clients, it optionally attaches an authentication protocol to each. The EAP types mandated in Passpoint:

- **EAP-SIM, EAP-AKA and EAP-AKA'** ("AKA prime") are so close they are identical from our Wi-Fi viewpoint. They take credentials stored in the SIM (or USIM) card on a cellular device, and use them to authenticate with the AAA server in the cellular network which issued the SIM. In essence it's the same as authenticating a cellphone on a cellular network, but the information is carried by the 802.1X protocol in WPA2/WPA3-enterprise.
- **EAP-TLS** is an existing EAP type that relies on X.509 certificates to authenticate the network to the client and vice versa. No extra userid or password is required.
- **EAP-TTLS** uses an X.509 certificate on the server, but the client authenticates using a userid/password combination.

Generally, we expect cellular operators to use EAP-SIM (still in use, but recently deprecated by 3GPP) and EAP-AKA or EAP-AKA', as they already issue SIM cards and have the matching authentication infrastructure. Common credentials also allow operators to keep track of users and devices as they move between the cellular network and Wi-Fi. Organizations that don't issue SIM cards will use one of the other methods, and obviously SIM-less devices won't support EAP-SIM, EAP-AKA or EAP-AKA' and so will rely on one or both of the other EAP-types. EAP-TLS is attractive because it uniquely identifies the device using a certificate, and doesn't require any user configuration (setting the userid/password), but generating large numbers of certificates and installing them on devices (and eventually revoking them) can be cumbersome. EAP-TTLS is the default password-based authentication.

When the Passpoint hotspot reports reachable service providers, the field showing available EAP types is optional. Indeed, it should not normally be required, as the mobile device should be pre-provisioned with a list of service providers, their names or realms, and the respective EAP-type and credentials. Thus the EAP-type information should be redundant, as the device already associates authentication type and service provider address.

APPENDIX – PASSPOINT FAQ

What is Passpoint?

Passpoint is a standardized method to seamlessly discover and securely authenticate to Wi-Fi networks with no explicit user intervention. The Aruba Gemini service pilot leverages Passpoint to enable mobile devices to automatically authenticate to enterprise Wi-Fi networks using their cellular credentials (SIM/eSIM). Devices that associate with an enterprise network using Passpoint may then use their Wi-Fi connection to make and receive cellular calls and text messages, effectively eliminating gaps in cellular coverage, providing local networks with better visibility of visitor activity, and providing mobile network operators (MNOs) with continuous access to their subscribers.

How is Passpoint related to Wi-Fi Calling (WFC)?

Passpoint allows a mobile device to discover and authenticate itself on a Wi-Fi network. WFC enables a device to create a secure tunnel to its home cellular network so that it can send and receive calls and SMS/RCS messages over a Wi-Fi network. Both Passpoint and WFC are widely supported by MNOs' mobile devices but remain independent services. WFC is available to any properly configured device, regardless of how it associates to a Wi- Fi network, but it only works if a device is already connected to a Wi-Fi network, making Passpoint a prerequisite for WFC in many environments where visiting devices may lack local credentials. By connecting devices using Passpoint, Aruba can also share quality of service information between the local network and the mobile carrier to improve the experience of WFC and the mobility between local Wi-Fi and the surrounding cellular networks.

How are E9-1-1 requirements satisfied?

Voice calls are controlled by the mobile device and the operator's network. The data traverses the local network in an encrypted tunnel. While Aruba has added heuristic rules to identify WFC-based calls, it cannot know which numbers dialed.

Operators have developed protocols to handle emergency WFC-based calls and route them to the appropriate response center based on the caller's location. Operators who support e911 over WFC do so in compliance with current regulatory requirements.

Is Passpoint secure?

Passpoint uses WPA2/WPA3-Enterprise with AES encryption ensuring all user traffic is encrypted over-the-air.

Does Passpoint support multiple operators on the same SSID?

Passpoint is a neutral host technology that supports the discovery and authentication of local networks using a wide variety of credentials from any number of sources on a single ESSID. As Passpointcapable clients search for Passpoint-enabled networks, they ignore the SSID name and instead focus on a beacon and/or pre-association exchange that advertises Passpoint support and offers a list of recognized providers/credential types.

Do all operators support Passpoint?

Passpoint profiles have been pushed to the client devices by all major North American operators and many others globally. The Wireless Broadband Alliance (WBA) is actively promoting Passpoint in the global operator community.

Do all operators support WFC?

All major North American operators support WFC. The link below provides an overview of operator support for iPhone. While the list is maintained by Apple, WFC carrier support is not specific to iPhones and a majority of flagship Android devices have support. As of this writing, WFC is supported on over 100 operators in over 40 countries.

What analytics can a network extracxt from Passpoint traffic?

Generally speaking, the local network will have visibility of the same client traffic it would see on any guest network, but it will not have visibility of the subscriber identity or any persistent identifiers other than the associated device's MAC address. From an analytics perspective, the major benefits of Passpoint are that it creates a much larger and more complete picture of visitor activity. Since a much higher percentage of visitors will be automatically associated with the network and their behavior and traffic will be visible to the local network, the value of any location, business, and security analytics in use will be improved.

Can Passpoint service be enabled per-AP?

Yes. Passpoint is part of the AP configuration and can be applied to groups or individual AP's.

Can Passpoint service be enabled selectively?

Yes. Passpoint can be configured across a campus, in a specific location, or on specific access points. It can be enabled for all participating operators or for any subset.

BP_Passpoint_RVK_021122 a00090761enw