WHITE PAPER

WI-FI CERTIFIED PASSPOINT ARCHITECTURE FOR PUBLIC ACCESS

aruba
a Hewlett Packard Enterprise company

TABLE OF CONTENTS

INTRODUCTION

Whereas just three or four years ago mobile networks were based solely on licensed spectrum for user access, every mobile operator is now developing a roadmap incorporating unlicensed access using the 802.11 (Wi-Fi) protocol. The major factor driving this change has been the overwhelming demand for video and other high-bandwidth data services that has swamped 3G networks. Most operators, extrapolating demand for data services over the next few years, are recognizing that future data needs cannot be met by enhancements to the traditional mobile network on available licensed spectrum.

The response has been an increasing interest in the Wi-Fi radio that is now provided on all new smartphones. Wi-Fi offers a high-capacity connection, and is generally available at home and in the workplace, the two venues where most mobile data consumption takes place. To these private locations we can add public and semi-public venues such as hotels and conference centers, sports stadiums and airports as well as smaller dining and coffee shops. There will be an increasing need for Wi-Fi infrastructure covering these areas and carrying traffic from devices and users with mobile operator subscriptions.

Current enterprise WLAN infrastructure already allows a single access point to support a number of services. For example, a network for a retail chain can service internal traffic such as point of sale and handheld bar-code scanners, ranging to wireless handsets on the corporate PBX. In addition, the access point provides 3G offload services for the managing operator and roaming services for other operators' subscribers. For public use without an existing subscription, a Web-based captive portal allows credit-card entry for short-term use. By supporting multiple services and uses, the hotspot operator can sell Wi-Fi infrastructure to businesses that services the public as well as supporting their internal data needs.

Although it is possible today to offer a comprehensive Wi-Fi hotspot service from a public or dual-use public-private WLAN, there are impediments to widespread adoption. The existing Wi-Fi standards and device connection manager software were not developed with hotspot applications in mind, so it is not surprising that current services are operator-specific and require significant user-intervention. This can be improved. In the remainder of this paper we will discuss the Wi-Fi Alliance's answer to the question 'Why can't Wi-Fi roaming be like cellular roaming?"

WI-FI ROAMING SHOULD BE LIKE CELLULAR ROAMING

This aphorism has headlined many a keynote speech about Passpoint, but it is no less true for being trite. Cellular phones, when they can't find their home network, automatically identify and register with national and international roaming partners without the need for user intervention. To date, Wi-Fi has lacked a widely implementedprotocol to streamline this function. While it is already possible to set up a Wi-Fi mobile device for hotspot roaming, after a fashion, the process is quite cumbersome and by no means universal.

Today's Wi-Fi access points have only one publicly-accessible label, the SSID. Hence this SSID has to be used to indicate different network types. Most SSIDs reflect the organization operating the local access point, like "PEETS" or "moonrisehotel", while others indicate access to a service provider, "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 cannot 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 and raises questions of privacy and legality.

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.

WHAT'S IN PASSPOINT?

The June 2012 Wi-Fi Alliance Passpoint certification (Wi-Fi CERTIFIED Passpoint) is the first release of Passpoint, incorporating technology from the Wi-Fi Alliance Hotspot 2.0 Specification which in turn references the IEEE 802.11u amendment. Additional Passpoint releases are planned to provide additional functionality, including on-line signup, to obtain credentials from an operator/ service provider, and delivery of policy.

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 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 pre-association 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) which will be used to transport other data in the future, but for our purposes with the initial Passpoint release, GAS and ANQP are used interchangeably.

New beacon and probe response information elements

A few 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 (see below)
- 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

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, with an interval of 15 seconds or more. 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.

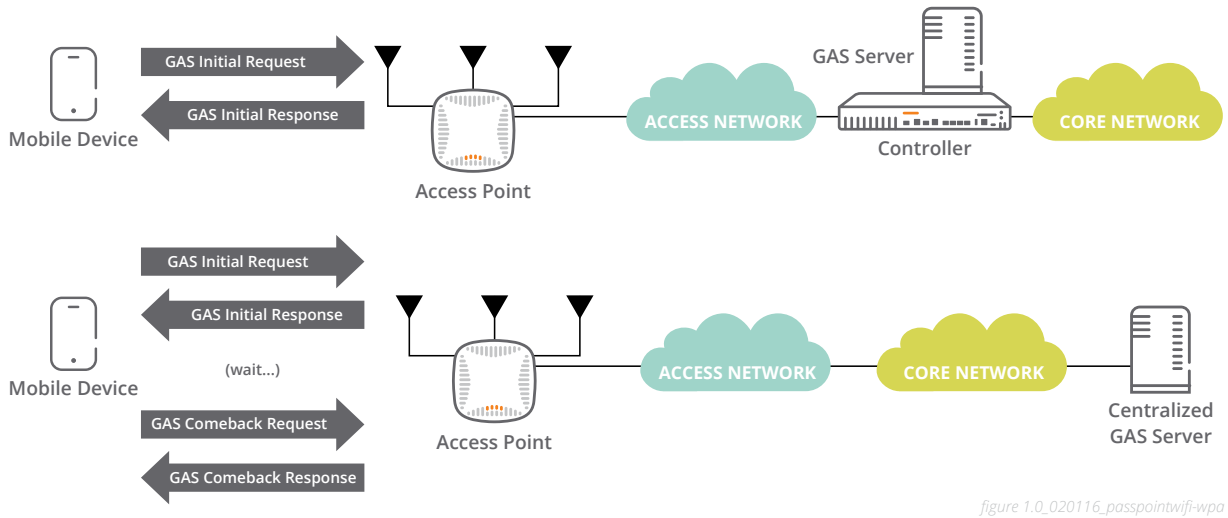

Figure 1. GAS 2-way and 4-way exchanges and back-end architecture (4-way exchange is used when response is too large to fit in one frame or takes too long to assemble)

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.

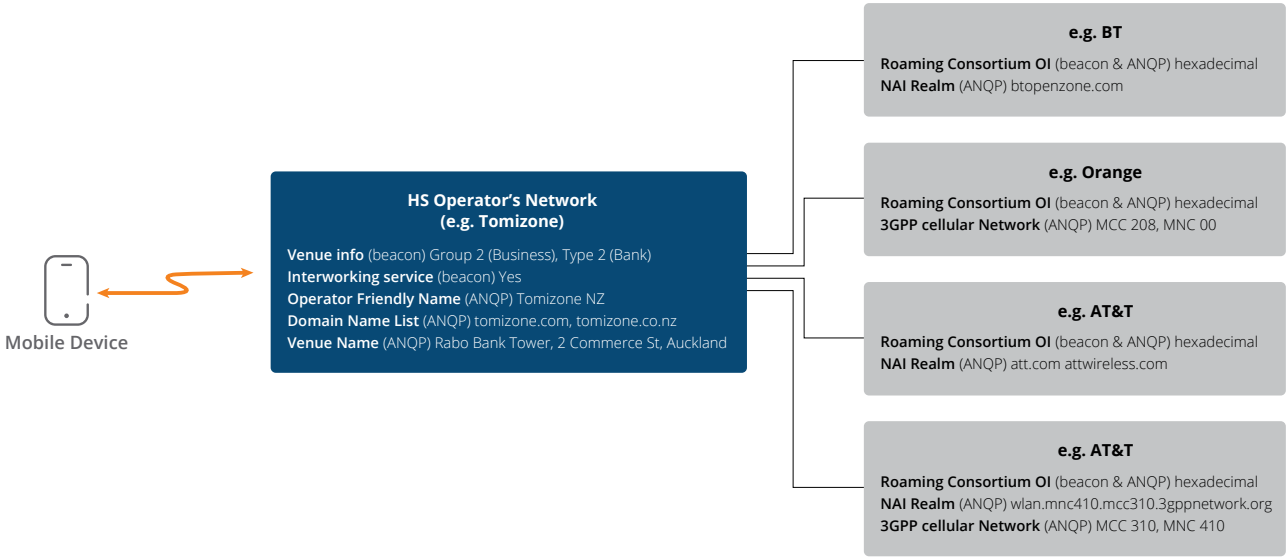

figure 2.0_020116_passpointwifi-wpa

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.

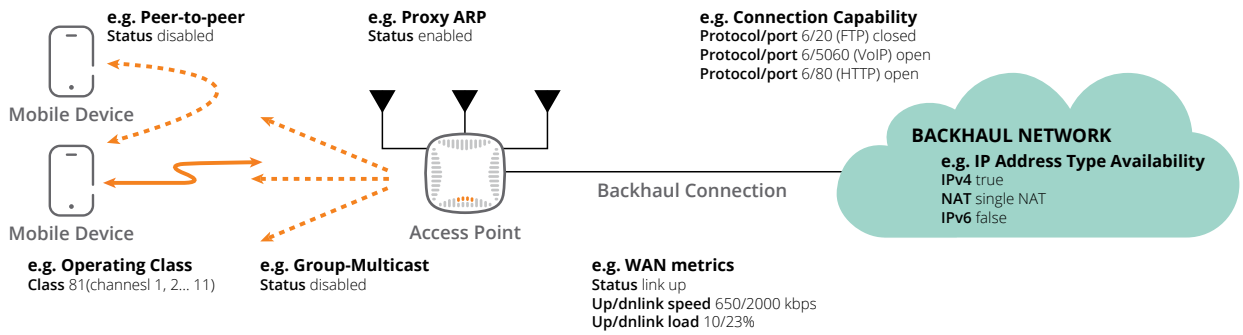

Figure 3. Configuration features and information provided by a Passpoint access point (examples simplified for clarity)

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.

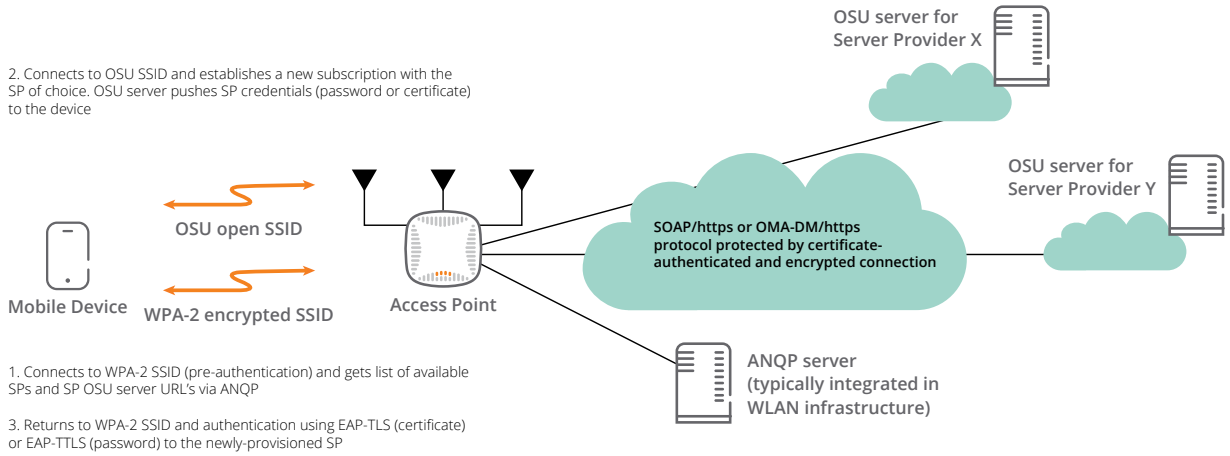

Figure 4. Online sign-up with OSU server associated with a Passpoint WLAN (simplified for clarity)

The user then selects a subscription type, and perhaps enters credit card numbers, and that information is sent securely back to the OSU server, which then issues and returns credentials in the form of an X.509 certificate or username-password. The final act is to automatically install these credentials on the mobile device as a secure authentication profile special to that service provider and including key Passpoint identifiers such as the service provider NAI realm.

Now the device will return to the Passpoint SSID with good credentials and in the future will automatically connect to any access point advertising Passpoint reachability to that service provider, as if the credentials had been entered manually, but without the same degree of user intervention.

Since many subscriptions added by OSU will be limited-time, and for other eventualities, there must be a complementary service that deals with mobile devices connecting to a network with credentials that were once valid but have now expired. The service provider handles this by rejecting the authentication attempt and redirecting the device (via a URL) to the Remediation Server (usually co-located with the OSU server). The Remediation Server uses a secure protocol to inform the user that the subscription or credentials are no longer active, and usually prompts for, and performs, a subscription renewal or pushes new credentials.

The final function in Passpoint v2 is a Policy Server. This is usually a function of the OSU server and can be used during online sign-up to push policy profiles to the mobile device. Most available policy preferences deal with network selection. For instance, when a device can see many available hotspots, policies help it establish priority for connection, based on home-or-visited service provider, current load, backhaul bandwidth (advertised over ANQP) and other parameters. Many service providers have preferred roaming partners which can vary by geography so policies can become quite complex.

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 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 in the same way as it does today.

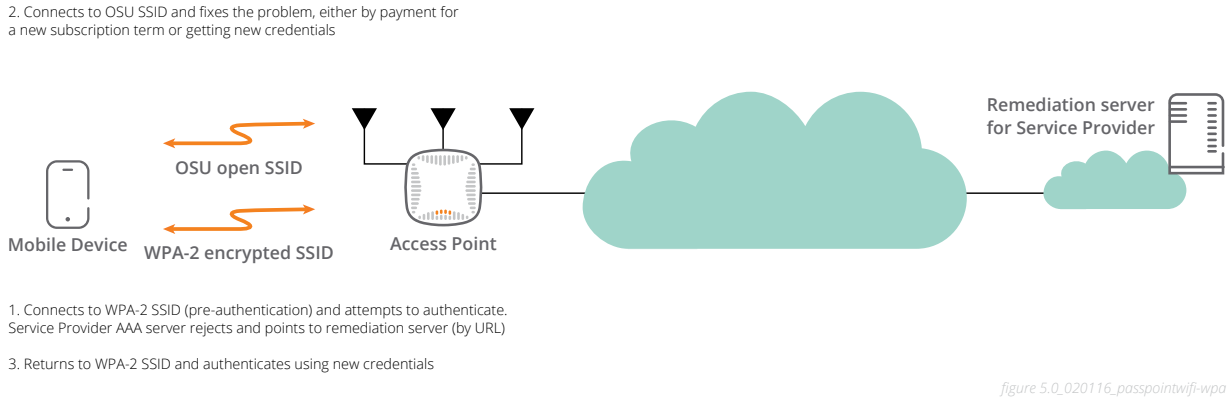

Figure 5. Remediation server associated with a Passpoint WLAN (simplified for clarity)

Passpoint mandates WPA2-enterprise, specifying four EAP types within WPA2-enterprise that are already exercised as part of Wi-Fi Alliance testing: 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.

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 and EAP-AKA are such close cousins 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-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 and EAP-AKA, as they already issue SIM cards and have the matching authentication infrastructure. Common authentication also allows 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. 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.

END-TO-END ARCHITECTURE WITH PASSPOINT

Passpoint enables easy access to public networks by providing information and protocols to assist in discovering and selecting a service provider. After hotspot network selection, the mobile device authenticates, and it is then connected to the Internet or other networks. In this section we discuss the networks that support the authentication and network connection phases. Both of these are outside the Passpoint specifications, but they must be considered by hotspot operators and service providers.

Authentication networks are likely to be quite complex – we show a representative diagram below. All authentication traffic from a Passpoint hotspot using WPA2-enterprise is carried over 802.1X, with RADIUS connections.

As we follow the flow of authentication traffic, it is likely that it will first be routed to a local RADIUS server owned by the hotspot operator. This will allow authentication of the operator's own subscribers, but for roaming users it will act as a proxy and a monitor point for billing and accounting data – if the hotspot operator is authenticating subscribers for other service providers, it will want its own record of this data.

The local proxy RADIUS server will terminate a number of IPSec tunnels, via which authentication traffic will be directed to roaming partners. In some cases this roaming may be a peer-to-peer relationship, as shown in the diagram, with the RADIUS traffic going directly to a partner where it will may be terminated, or converted to DIAMETER to connect to large core networks. Incidentally, this proxy server will also be required to examine mobile device authentication requests and route them to the correct roaming partner, a function that may become complex as the number of roaming partners increases.

However, we believe that Passpoint will broaden the role of existing roaming hub or roaming exchange bureaux. These organizations provide a service where a hotspot operator can reach a large number of roaming partners via a single connection. They can direct the authentication stream to the appropriate service provider, and can also take care of billing and accounting for settlement. As the number of service providers and hotspot operators increases, the number of possible roaming relationships will increase exponentially and the functions provided by roaming hubs will become indispensable.

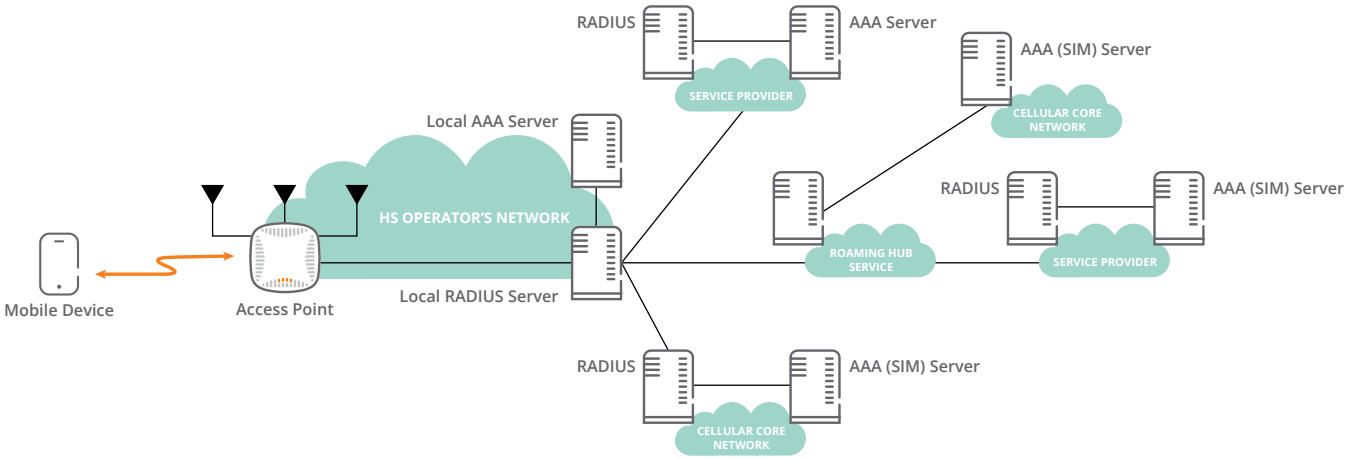

Figure 6. Authentication paths with Passpoint

It is clear that although the authentication, billing and accounting architecture and RADIUS attributes are out of scope of the Passpoint certification, they are essential for a smoothly-functioning hotspot roaming relationship. The Wireless Broadband Alliance and other organizations are working to provide guidelines in this area, as there is currently no universal agreement on required RADIUS attributes for hotspot roaming.

While authentication networks may be extensive and complex, the path followed by data-plane traffic is likely to be much simpler. In most cases, the mobile device will be connected directly to the Internet, probably right at the hotspot's backhaul connection. This is the way most service providers and most subscribers like to work today. However, there will always be circumstances where alternate arrangements are required. Some service providers want subscribers to be connected back to their own network, either because they need to deliver 'walled-garden' services, or to maintain seamless handovers between cellular and Wi-Fi connections, or to monitor users' traffic for other reasons. It is possible to achieve this, as we show in the diagram below. The selection of appropriate network routing can be driven by RADIUS responses from the authenticating service provider.

Corporate networks also need special treatment, but are unlikely to get special routing assistance from hotspot operators and service providers.

HOTSPOT SECURITY WITH PASSPOINT

Current hotspots incorporate relatively weak security so Passpoint improves matters in several areas – mostly using existing Wi-Fi techniques.

The most significant improvement is to mandate WPA2-enterprise for Passpoint hotspots. This implies mutual authentication and strong over-the-air encryption. Whichever EAP-method is used, the access point (or service provider) must identify itself to the mobile device and vice versa. When authentication is complete, unique keys are

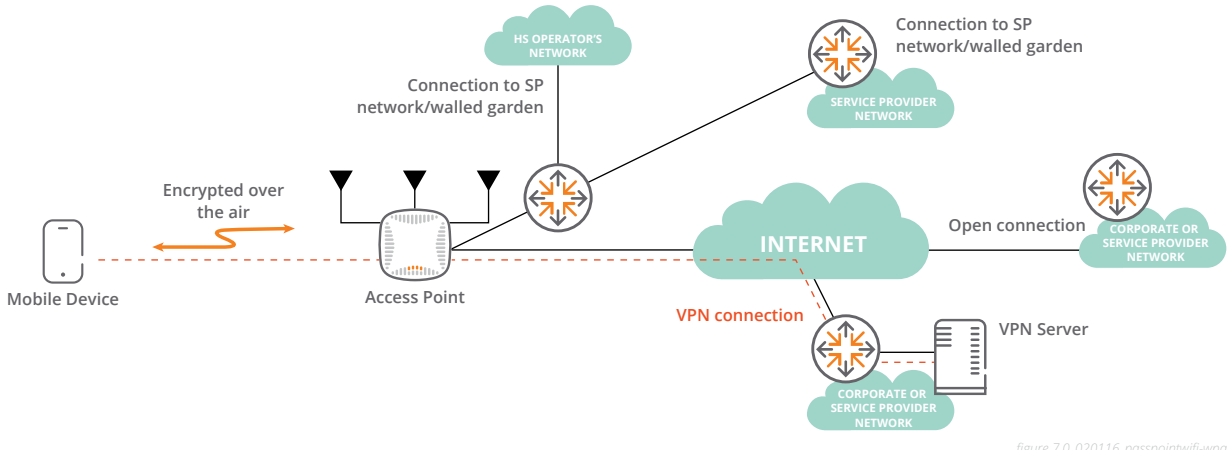

Figure 7. Data paths with Passpoint

distributed to the access point and the device to encrypt the bidirectional traffic – keys are not shared between clients on the same access point. This brings enterprise-grade security to public hotspots.

Public hotspots differ from enterprise or home access points in that the various users on a Passpoint hotspot have no reason to trust one another. Therefore Passpoint requires that when the network type is 'public', whether free or chargeable, individual users are firewalled from each other – it is possible to address one hotspot-connected device from another, but the traffic has to pass through a firewall function either integral to or upstream of the access point before being delivered to the recipient.

Passpoint also requires a proxy-ARP implementation on the access point to prevent ARP spoofing attacks from one client to another. Similarly, multicast or broadcast (it's the same function in Wi-Fi, frames are received by all clients of the AP) requires a Group Key to be shared across all devices and can be disabled on Passpoint hotspots: this represents another need for the proxy ARP function above. And Passpoint prohibits P2P operation, DLS and TDLS methods of peer-to-peer communication within the hotspot.

There are recommendations in Passpoint that a mobile device should provide an indication to the user that link-layer security is in use and that the device is connected to a hotspot using Passpoint. As users become aware of the improved security available on Passpoint hotspots they should become familiar with these indicators (similar in concept to the security-lock displayed on browsers) and notice when they are absent. It's not yet clear whether the industry will develop universal logos for these indications.

Note that even though Passpoint guarantees good over-the-air security when correctly implemented, it is likely that traffic will be decrypted on the access point and forwarded onto the backhaul connection and the Internet en-clair. Users should be aware that if they want privacy over the wired portion of the connection, they will need to implement end-to-end security such as a VPN function. This is no different from a home access point or many small businesses, but it should be borne in mind when considering hotspot use.

BROADER APPLICATIONS FOR PASSPOINT

Passpoint includes so many parameters and options that we will surely find many new and unexpected applications for it in the coming months and years. But the basic public hotspot application will be the most immediate.

Over the coming months and years we will see an explosion in the number of public Wi-Fi hotspots. Some of the impetus will come from cellular service providers eager to offload traffic, particularly high-bandwidth video users in high-density locations such as city centers, airports and stations, sports stadiums and shopping centers. Now that hotspot operators and service providers can rely on known behavior in the client, and mobile device providers can pre-configure handsets, tablets and PCs based on predictable network behavior, the amount of traffic that is automatically passed to Wi-Fi networks will snowball.

Many countries and cities will see a significant increase in service provider-owned hotspots. But Passpoint offers advantages to independent hotspot operators too. Now it is very easy for a single hotspot to accept authenticated traffic from all cellular service providers' subscribers, and if commercial roaming agreements can be put in place this will allow landlords of public areas like shopping centers and airports to use one set of WLAN infrastructure to provide Wi-Fi offload service for every Wi-Fi enabled device that enters their area. Further, these devices will be pre-configured to connect to Wi-Fi without any user intervention.

Stadium operators in particular will benefit from Passpoint, as spectators' mobile devices will automatically seek out the stadium WLAN and authenticate to their home service providers. This will remove the current obstacles to access for delivery of video and images to accompany the game: the spectator will only need to bring up a browser or other client, as Passpoint will take care of the connection mechanisms.

Beyond public access we see an opportunity for dual-use public-private networks, where a single access point can offer private access, perhaps for a small business or retail establishment, while simultaneously advertising Passpoint-based public service. This would be an ideal vehicle for a managed-service solution, where the service provider ships the customer pre-configured access points and manages them remotely, gaining the hotspot footprint while adding revenue from the dedicated private customer.

And Passpoint will tip the scales on a question universities and hospitals, in particular, face with increasing urgency, how to provide cellular service in areas that are too hard to reach or too high in density for the cellular macro network to cover well. Since Wi-Fi interfaces are becoming universal on cellular devices, a single WLAN can potentially support all cellular users, in contrast to solutions such as Distributed Antenna Systems (DAS) which are set up per-carrier, and pico/femtocells that are still immature for large deployments.

The missing piece to this puzzle are those cellular services that do not currently run over Wi-Fi, namely voice and SMS, but it will be easier to make these changes in the future than to perfect the other solutions in licensed spectrum.

Finally, Passpoint has applications in enterprise WLANs. Some are obvious, like providing guest access for authenticated service provider customers without the need to check in and get a special credential. Others may take longer to develop, but we see many opportunities to use Passpoint for guest or contractor access, multi-site or international roaming within the enterprise.

CONCLUSION

The Passpoint certification removes many of the obstacles to easy, silent, secure access to public Wi-Fi hotspots.

Rather than tying each reachable service provider to an SSID, Passpoint allows a single SSID to stand in front of many service providers, including cellular operators, MSOs and other providers with whom the consumer has an existing subscriber relationship. This allows the service providers to extend their services, while the consumer will be able to leverage existing commercial relationships at many more hotspots.

When a mobile device encounters a Passpoint hotspot, or a number of hotspots in one location, it can now learn about the service providers available via each hotspot, as well as other characteristics of the hotspot. The device can match available service providers against its preconfigured subscriptions, prioritize the hotspots and service providers and proceed to authenticate with the optimum choice. Because Passpoint discovery is pre-authentication, there is considerable savings of time and battery life compared with existing methods.

Passpoint makes mandatory a number of existing Wi-Fi and IEEE 802.11 security features, transforming the security posture of a device connected to a hotspot. For instance, mutual authentication and over-the-air encryption are guaranteed, as well as restricted peer-to-peer traffic.

How will Passpoint roll out? The initial Passpoint release 1 certification (known as Wi-Fi Alliance CERTIFIED Passpoint) is released in June 2012, and at that time most of the enterprise WLAN vendors will announce availability of software upgrades with compliance. Mobile devices, particularly cellphones and tablets, may take a little longer but we expect to see many certified devices for the buying season in late 2012, and it is possible that smartphone vendors will offer software upgrades to support Passpoint on existing models.

Meanwhile work continues on future releases of Passpoint. We expect to see a certification for release 2 soon, incorporating features such as on-line sign-up where a user can sign up for service at a hotspot using standard protocols, as well as new work on operator policy for public access.

But the Wi-Fi Alliance has already answered the question “Why can’t Wi-Fi roaming be more like cellular roaming?” With Passpoint, it is.

APPENDIX – INFORMATION AVAILABLE FROM THE ACCESS POINT WITH PASSPOINT RELEASE 1

(This is a summary list, it includes only the important indications from the access point to the client)

INFORMATION AVAILABLE FROM THE ACCESS POINT WITH PASSPOINT RELEASE 1				
Field name	**Beacon/Probe response (802.11u)**	**ANQP (IEEE 802.11u)**	**ANQP (Wi-Fi Alliance)**	**Description**
Access Network Type	✓			6 options… 'private', 'private with guest access', chargeable public', 'free public' 'personal', 'emergency services only'
Internet bit	✓			Set if the hotspot provides access to the Internet
Venue Group	✓			One of 11 codes for 'assembly', 'business', educational', 'factory and industrial'…
Venue Type	✓			The International Building Code defines a number of venue types for each venue group above, so 'educational' group has types 'school, primary', school, secondary', 'university or college'…
HESSID	✓			Identifies a 'homogenous' SSID or zone of coverage, using a BSSID (MAC address) from one access point
Roaming Consortium OI	✓			The beacon has space for 3 OIs, of which one should be the hotspot operator's OI
P2P element	✓			P2P must be disabled
BSS load element	✓			An existing 802.11 function first added in the 802.11e amendment, provides an indication of how much traffic the access point is transmitting/receiving
RSN element	✓			An existing 802.11 function. Must indicate WPA2-enterprise for Passpoint
RSN AKM list	✓			An existing 802.11 function. Must indicate AES encryption for Passpoint
NAI Realm list		✓		A list of network address identifiers for reachable service providers, with optional EAP-type subfield
Venue Name		✓		A text field usually giving the owner/occupier and address of the venue
Network Authentication Type Information		✓		An additional step is required for authentication. The step tested in Passpoint is 'acceptance of terms and conditions is required' with a redirect URL
Roaming Consortium List	✓ (3 RCs)	✓ (Full list)		The RC OI is a value from a registration database maintained by the IEEE
IP Address Type Availability		✓		Reports support for IPv4, NAT, or IPv6
3GPP Cellular Network Information		✓		PLMN IDs are already established for cellular operators, consisting of MCC-MNC values
Domain Name List		✓		The domain name(s) of the hotspot's operator
Operator Friendly Name			✓	A variable-length string identifying the operator of the hotspot
Operating Class			✓	The list of channels an access point can operate on
WAN Metrics			✓	Includes status, whether symmetric, 'at capacity', up/dnlink speed, up/dnlink load
Connection Capability			✓	A list of protocols, ports and open/closed
NAI Home Realm Query			✓	A short-list of reachable NAI Realms that match a list in the client's query

This is a summary list, it includes only the important indications from the access point to the client

ABOUT ARUBA, A HEWLETT PACKARD ENTERPRISE COMPANY

Aruba, a Hewlett Packard Enterprise company, is a leading provider of next-generation networking solutions for enterprises of all sizes worldwide. The company delivers IT solutions that empower organizations to serve the latest generation of mobile-savvy users who rely on cloud-based business apps for every aspect of their work and personal lives. For more information visit www.arubanetworks.com.

To learn more, visit Aruba at http://www.arubanetworks.com. For real-time news updates follow Aruba on Twitter and Facebook, and for the latest technical discussions on mobility and Aruba products visit Airheads Community at http://community.arubanetworks.com.

aruba
a Hewlett Packard Enterprise company

1344 CROSSMAN AVE | SUNNYVALE, CA 94089
1.866.55.ARUBA | T: 1.408.227.4500 | FAX: 1.408.227.4550 | INFO@ARUBANETWORKS.COM

www.arubanetworks.com

WP_PasspointWiFi_020416