IGNITION
DESIGN LABS

Passpoint

Technical White Paper V1.1

Disclaimer

Limitation of Liability

Website:

https://ignitiondl.com/

Table of Contents

Chapter 1 Overview

1.1 Introduction

With the popularity of smartphones and tablets, the demand for wireless data greatly exceeds the capacity of operators' networks. Therefore, the operators must think of some way to increase the network capacity. Most operators prefer Wi-Fi to uninstall cellular network traffic. Although the bandwidth of the Wi-Fi is high, the current public hotspots have security risks and are not easy to use.

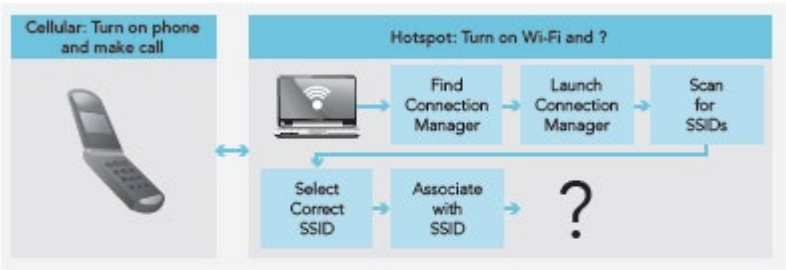
To access a public hot spot, a user must perform the following operations:

Step 1 Check the available SSID list on the equipment, and select a SSID manually.

Step 2 Open a browser and enter web URL, and then the HTTP will be redirected to a portal page, and the portal will return to the login page.

Step 3 Enter the correct username and password to access the public hot spot.

However, the public hot spots often do not enable authentication and encryption, which makes the user's personal information, such as passwords, financial information, and e-mail in danger of leakage.



Users take too many steps to associate to the Wi-Fi network

The June 2012 Wi-Fi Alliance Passpoint certification 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 and IEEE 802.11i amendments. The primary aim of Passpoint is to simplify and automatic access to public Wi-Fi networks, and to provide a more secure Wi-Fi access network.

1.2 Hotspot 2.0 and Passpoint

Passpoint is the brand for the certification program operated by Wi-Fi Alliance. Devices that pass this certification testing can be referred to as "Passpoint devices". Passpoint certification is based on the Wi-Fi Alliance Hotspot 2.0 Specification. This is the underlying technological specification developed by Wi-Fi Alliance members.

Chapter 2 Passpoint Release1

Passpoint will lead a revolution on user experience of Wi-Fi client. Moreover, it will be an important method for operators to share Wi-Fi offloading in public hotspots.

Passpoint release1 defines multiple functions:

- Network scanning and selection: Devices discover and make connection with Passpoint without user actions.
- Seamless network visit: Without registration on a browser or enter a password. Devices can automatically connect to the network through SIM, credential or certification based EAP username/password.
- Security certification and links: All connections are under protection of WPA2╟ - Enterprise, which is able to provide equal security of cellular.

2.1 Passpoint Release1 Typical Scenario

2.1.1 SIM Network Scenarios

A user follows these steps to find network to authenticate in the operator's network:

Step 1 The STA confirms whether it supports hotspot 2.0 by the received beacon frame from the AP.

Step 2 The STA search for the 3GPP SIM network information and the OIs on ANQP server.

Step 3 The STA compares the 3GPP SIM network information and OI with the STA alternative network list to judge whether they match.

Step 4 If they match, the STA will automatically connect to the passpoint AP.

Step 5 The STA uses the EAP-SIM or the EAP-AKA with AAA server to 802.1X authenticate.

Step 6 The AAA server and the HLR cross authenticate the user.

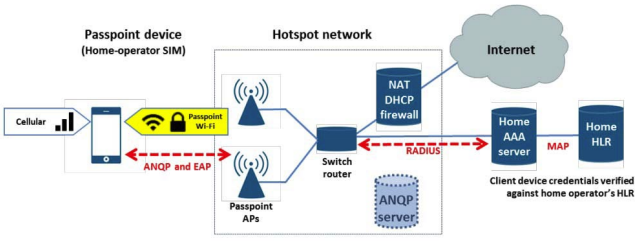


Figure 1. Passpoint hotspot reference architecture: SIM device

2.1.2 Non-SIM Network Scenarios

Step 1 The STA confirms whether it supports hotspot 2.0 by the received beacon frame from the AP.

Step 2 The STA search for the NAI list and the OIs on ANQP server.

Step 3 The STA compares the NAI information and OI with the STA alternative network list to judge whether they match.

Step 4 If they match, the STA will automatically connect to passpoint AP.

Step 5 The STA uses EAP-TLS or supports the MS-CHAPv2 EAP-TTLS and AAA server to 802.1X authenticate.

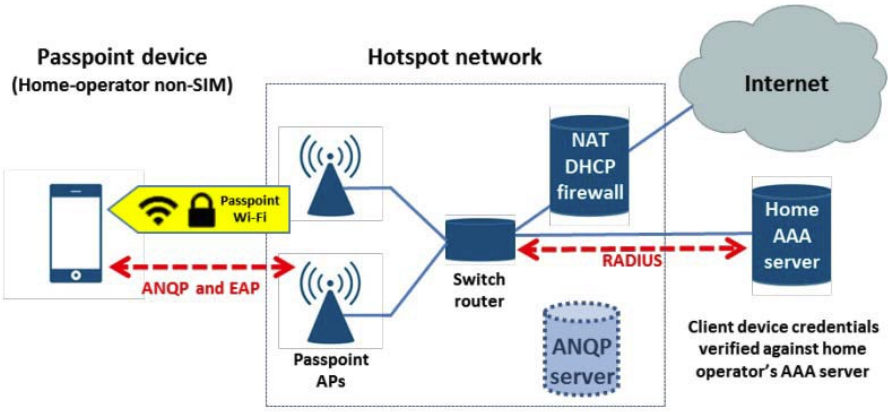


Figure 2. Passpoint hotspot reference architecture: non-SIM device

2.2 Passpoint Release1 Details

2.2.1 Automatic Network Discovery and Selection

This feature allows a mobile device to identify which access points are suitable for its needs. Technical details are summarized as follows:

- New information elements in beacons and probe responses;
- A new GAS/ANQP protocol to allow pre-association queries of a Passpoint's capabilities;
- New information element in GAS/ANQP protocol to allow a mobile device to learn which service providers are reachable via a Passpoints;
- New information element in GAS/ANQP protocol to provide information about a hotspot's operator, venue and configuration.
- The beacon or probe response is the first informative message received by UE to get information of a Wi-Fi network. In Passpoint, a few information elements are added to the beacon and probe response, including:
  - **Access network type**, identifying whether this Wi-Fi network is for public, private or guest access, etc.;
  - **Internet bit**, indicating the Wi-Fi network can be used for internet access;

- **Advertisement protocol**, indicating the Passpoint supports GAS(Generic Advertisement Service)/ANQP(Access Network Query Protocol);
- **Roaming consortium element**, a list of up to 3 names of reachable service providers via this Passpoint;
- **Venue information**, describing the venue where this Passpoint is situated;
- **Homogenous ESSID**, a label identifying Passpoints belonging to a same homogenous extended service set;
- **P2P and cross-connect capability**, describing the support of P2P and crossconnect capability in this Wi-Fi network;
- **BSS load element**, an indication of current load on the Passpoint.

It may be possible for a mobile device to decide whether to use a Passpoint based on the information in beacons or 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 Passpoint. To avoid probe response flooding, 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.

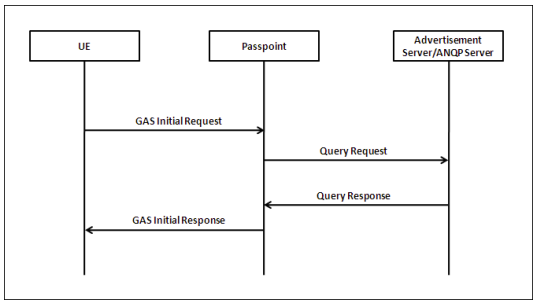
After the device identifies access points in the area via beacon or probe response, then the device proceeds with GAS/ANQP to get a more complete picture of the services and service providers offered, which allows it to select the best match for its needs.

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.

The GAS protocol allows a mobile device to query the access point for configuration and reachability information before association. The basic mechanism of GAS is a client query in a GAS query frame, and the access point responses in a GAS response frame. There are 2-frame exchange and 4-frame exchange mechanisms.

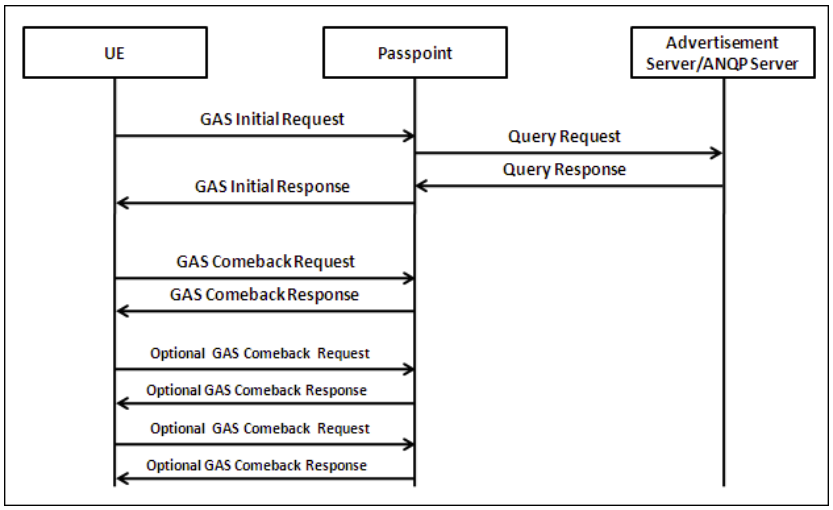
When the requested information is not too long and the Passpoint is set to "pause GAS response for server feedback", a 2-frame exchange mechanisms is used, as shown in the following figure. After sending the GAS initial Request frame to a Passpoint, UE should keep awake and wait for the GAS initial Response frame.

Figure 2-1 GAS 2-frame exchange information query



When the requested information is too big to be included in the GAS initial Response frame and the Passpoint is set to "pause GAS response for server feedback", a 4-frame exchange mechanism and GAS fragmentation are used, as shown in the following figure. When Passpoint finds the requested information obtained from the advertisement server (ANQP server) is too big to be included in the GAS initial response frame, the Passpoint will inform UE of more requested information. UE then will retrieve the rest of the requested information via GAS comeback request/response from the Passpoint.

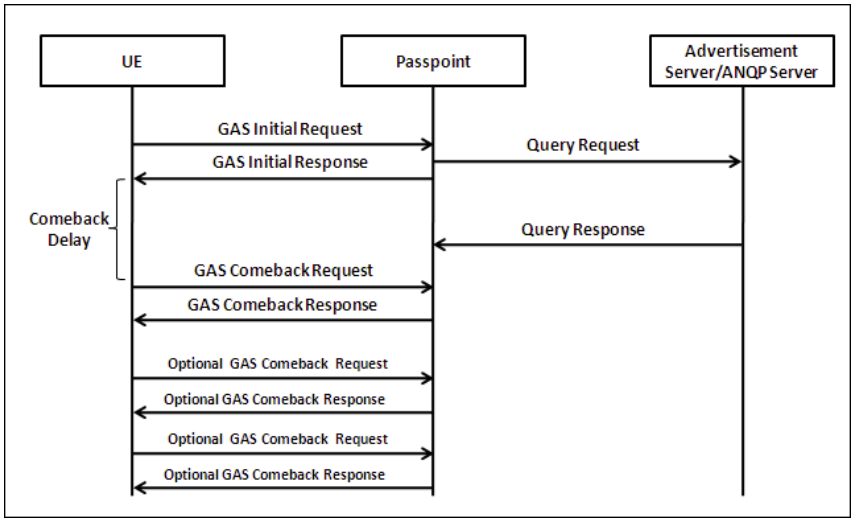
Figure 2-2 GAS 4-frame exchange information query – 1



When the Passpoint is set to "not pause GAS response for server feedback", another

4-frame exchange mechanism is used, as shown in the following figure. When Passpoint received the GAS initial request from UE, Passpoint should estimate the query response time from the advertisement server, then send back a GAS initial response to inform UE of the comeback delay time. UE then will retrieve the requested information via GAS comeback request/response from the Passpoint after the comeback delay time.

Figure 2-3 GAS 4-frame exchange information query – 2



The information in the beacon will not normally be enough for the mobile device to decide whether it wants to connect to the Passpoint, so once it sees the GAS indication in the beacon, it could proceed with a GAS request for more information. In Passpoint, ANQP can return a list of elements as follows.

- 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

Some of these are defined in the original IEEE 802.11u, others are added by the Wi-Fi Alliance. In this white paper, some important elements will be discussed. The information on the rest can be checked in the Passpoint Release 1 specification published by Wi-Fi Alliance.

Check the service provider reachability of a Passpoint is the first thing UE needs to do in automatic access. Before Passpoint, most access points support a Captive Portal web page that offers a list of roaming partners. To connect, a user had to open a browser, pull down the roaming partner menu, select the appropriate partner and enter username/password credentials. This is a cumbersome procedure.

The key question to be answered is "which of the service providers where I have a subscription can be reached through this Passpoint". Passpoint provides the answer to this question in a protocol, with at least 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 the roaming partner for a hotspot is a cellular operator, it will be identified by MCC-MNC. This PLMN list is delivered by the ANQP information element **3GPP Cellular Network information**. A mobile device having SIM or USIM credentials, queries for 3GPP Cellular Network Information and compares it to the PLMD ID stored on its SIM or USIM to determine if the home cellular SP’s network can be accessed through this Passpoint.

Other service providers will be identified by domain name or Network Address Identifier (NAI), the NAI realm, for example, examplecompany.com. This NAI realm list is delivered via the ANQP information element **NAI Realm list**. Also related authentication methods are delivered to the UE at the same time. A mobile device using username/password or certificate credentials queries for the NAI Realm List to get the full list of realms from a Passpoint.

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. This OI list is delivered via the ANQP information element **Roaming Consortium list**. A mobile device using any type of credentials can query for Roaming Consortium list.

These three addressing schemes are not mutually-exclusive. Indeed, one could expect large cellular operators to use all three. Note that the Passpoint operator appears as one of the available service providers, with no particular distinction. To determine which organization owns or manages the Passpoint, it is necessary to check the home operator attributes, and match them to available service providers.

To check the home operator who is operating the Passpoint, ANQP returns the Passpoint operator's domain name (similar to the NAI realm above) via ANQP information element **Domain Name list**, and also an **operator friendly name** which is a human-readable and free-form text field that can identify the operator and also something about the location via ANQP element **Hotspot Operator Friendly Name**.

It's important to know the hotspot operator because if there's a choice of Passpoints, even though the same service providers may be reachable through each, the pricing may be different.

In IEEE 802.11u, whenever UE required for NAI realm list, the hotspot should return all reachable operators' NAI realm information. Since the NAI realm information including more information than NAI name, such as authentication information, it could be a big waste of air-time if the number of reachable operators is huge. Thus, Passpoint allows UE to send out a Home NAI query, which carries the NAI of the operator this UE belongs to. Passpoint will only send back UE's home NAI realm information back to UE if there is a match.

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

Venue name and type 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 cafe 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 Passpoint operator can enter a description.

Passpoint hotspots can use **IP Address Type Availability Information** to indicate they support Ipv4 or Ipv6 addressing, routing and NAT support.

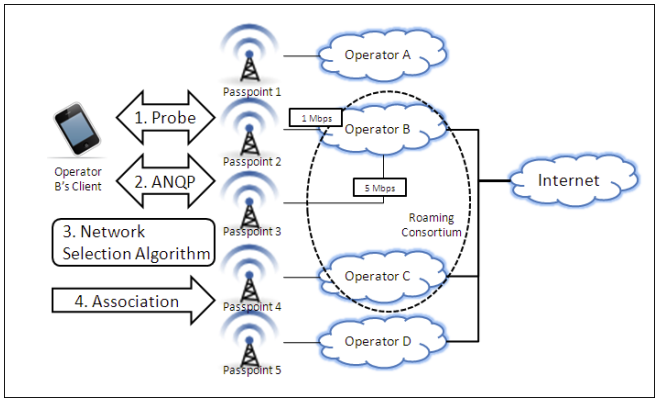
In the same way that residential and enterprise Wi-Fi routers and WLANs can be set up to restrict traffic on some protocols and ports, it is envisaged that some Passpoint networks may have integral or upstream restrictions, and these can be advertised in ANQP via **Connection capability**.

Operating Class 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.

The limiting factor in Internet bandwidth is likely to be the immediate backhaul connection from the Passpoint. ANQP can provide information including the upstream and downstream bandwidths and current traffic and whether the connection is currently at capacity via **Hotspot WAN metrics**. 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.

In summary, the following figure shows an example automatic network discovery and selection procedure. In this scenario, a client from operator B needs to get access to the internet. This UE first sends out a probe asks for Passpoints having the internet access indicated by the interworking information element in probe request frame. Passpoints except Passpoint 1 that does not have the internet access return their probe response frames. Thus UE can build up a list of candidate Passpoints. Then UE starts further information query by ANQP query. Based on the subscription this UE holds for authentication, it asks for 3GPP Cellular Network information, or Roaming Consortium list, or NAI realm list to check via which Passpoints the UE can be authenticated with its subscription. Then UE can exclude Passpoint 5, since it has no roaming relationship with operator B. At the same time, UE will prefer the Passpoints 2 and 3 that are operated by its home operator by asking Domain Name list and Hotspot Operator Friendly Name. It is possible that the application running on the UE has some specific requirements on the network. For instance, a video application asks for at least 2 Mbps bandwidth. Therefore, UE needs to do a further ANQP query to determine the bandwidths it may get from Passpoint 2 and Passpoint 3. After these network selection algorithm, UE decides to connect to Passpoint 3 and starts association procedure. Notably, it is also possible for UE to do all required ANQP information query in one ANQP query procedure. But it will be a big air-time waste if the number of the irrelevant Passpoints around is big. Thus, the ANQP information query algorithm could be very tricky.

Figure 2-4 Example procedure of automate network discovery and selection



2.2.2 Unified Authentication

This feature allows a mobile device to authenticate a remote service provider using suitable credentials. For a cellular client who has a smartphone with both cellular and Wi-Fi modules, this feature allows this client to get access to the Wi-Fi network with the same subscription, the SIM card, as in the cellular network.

Passpoint mandates WPA2-enterprise, using IEEE 802.1x authentication structure and specifying four EAP types within the WPA2-enterprise that are already exercised as part of Wi-Fi Alliance testing. The EAP types mandated in Passpoint are summarized as follows:

- **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 is very similar to authenticating a cellphone

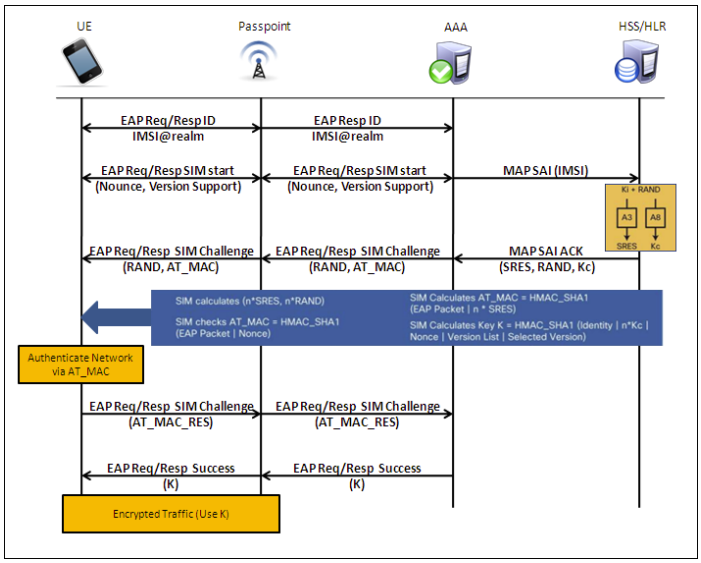
on a cellular network, but the information is carried by the 802.1X protocol in WPA2-enterprise.

- **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 do not issue SIM cards will use one of the other methods. EAP-TLS is attractive because it uniquely identifies the device using a certificate, and does not 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.

The following figure shows a typical procedure for SIM-based authentication when UE attaches to the network via a Passpoint.

Figure 2-5 Typical SIM-based EAP Authentication call flow



Note that EAP-based authentication offers a radio security advantage. Because the authentication is handled on Layer 2, EAP messages can be used to negotiate encryption keys for the IEEE 802.11i-based encryption of the radio interface. This approach provides much stronger security for radio communication compared to the unencrypted radio interface of portal-based authentication and is uniquely able to prevent simple MAC address spoofing attacks.

2.2.3 Security

A secured Wi-Fi access network is the basic requirement for Wi-Fi offloading. Passpoint improves its security 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 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 Passpoints differ from enterprise or home access points in that the various users on a Passpoint 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. Thus it is possible to address one Passpoint 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 is 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 Passpoints. 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 Wi-Fi network

2.2.4 Passpoint Summary

The Passpoint removes many of the obstacles to easy, silent, secure access to public Wi-Fi Passpoints. 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, with whom the consumer has an existing subscription relationship. This allows the service providers to extend their services, while the consumer will be able to leverage existing commercial relationships at many more Passpoints. It becomes much easier for cellular operators to extend their network coverage and enhance their network capacity with Wi-Fi network. When a mobile device encounters a Passpoint, or a number of Passpoints in one location, it can now learn about the service providers available via each passpoint, as well as other characteristics of the Passpoint. The device can match available service providers against its preconfigured subscriptions, prioritize the Passpoints and service providers and proceed to authenticate with the optimum choice.

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 Passpoint. For instance, mutual authentication and over-the-air encryption are guaranteed, as well as restricted peer-to-peer traffic.

Chapter 3 Conclusion

IDL provides the Wi-Fi Passpoint technology, supporting seamless, safe cellular switch, automatic Wi-Fi connection, getting rid of the cumbersome process and freely using Wi-Fi network. It switches the untrusted parts to the trusted in the network for operators.

IDL will support the Passpoint Release 2, providing a new real-time account configuration, safe registration function and operator strategy, and making the technology deeply complete. It not only can ensure the product function and compatibility, but also take greater market efficiency to operators and end users.