Ruckus
Simply Better Wireless.

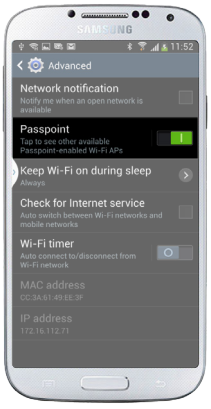
white paper

July 2013

How Interworking Works:
A Detailed Look at 802.11u and Hotspot 2.0 Mechanisms

Wi-Fi is entering a new phase in worldwide popularity, with high user expectations to match. New protocols will help the technology live up to the challenge.

Introduction



In the face of a changing wireless industry, network operators, venue owners, and enterprises are all looking for ways to offer new services to customers. Many organizations are leaning into unlicensed Wi-Fi technologies to address their needs, and the industry is abuzz with messages of new protocols. Analysts and product vendors have been at work talking about business drivers, consumer behavior, spectrum problems, and some of the technical initiatives that are enabling Wi-Fi to meet business needs. But, technical readers are less interested in charts, graphs, and trend analysis.

The purpose of this paper is to focus on the 802.11u/Hotspot 2.0 protocol enhancements that will enable Wi-Fi to live up to the next wave of business requirements being asked of it, especially as it relates to enhanced security, easier access, and more user-friendly operation. Both the Hotspot 2.0 (Wi-Fi Alliance) and 802.11u (IEEE) tech specs spell out the mechanisms and protocols that will be used to enhance Wi-Fi capabilities, but a translator is often necessary. This paper will serve as translator, sorting through the key elements in the specifications and explaining them in plain English.

ORGANIZATION	INITIATIVE	DETAILS
IEEE	802.11u	802.11u amendment to 802.11 standard published in February 2011
Wi-Fi Alliance	Hotspot 2.0	Technical program and specification that defines technical requirements for Passpoint™ interoperability certification
Wireless Broadband Alliance	Next Generation Hotspot	End-to-end roaming trials establish common commercial framework for interoperability across networks and devices

How Interworking Works:
A Detailed Look at 802.11u and HotSpot 2.0 Mechanisms

We will focus on discussing how the Wi-Fi protocols will achieve the benefits that are casually mentioned in many industry articles:

- How is the network discovery and selection process by a client device improved?
- How does a client device or user positively and reliably identify specific networks and their owners/operators?
- How does a mobile device or user know about the roaming partnerships, agreements, and possibly costs associated with a specific Wi-Fi network?
- What other contextual insight can a mobile device obtain about each Wi-Fi network, and how does it do so?
- How do these protocols fix the many security and privacy problems with today's Hotspots and public networks?
- How will Wi-Fi handle QoS for operator networks?
- What about emergency services?

In wireless trade publications, we hear about 802.11u and Hotspot 2.0 "network discovery and selection," "offload," "seamless handoffs," "secure Hotspots," and many of the other key terms associated these initiatives. Those concepts are the what, but this paper is here to address the how.

NOTE: This paper assumes that the reader is already familiar with 802.11 networking and the existence of 802.11u and Hotspot 2.0 initiatives. We do provide some background along with a cursory introduction of the specifications, but this paper is directed to a semi-technical audience.

The Specifications

The 802.11u specification was ratified by the IEEE in February 2011. It defines a number of enhancements to the 802.11 (WLAN) protocol to address the process of "interworking with external networks." One of the motivations for 802.11u is to allow Wi-Fi client devices to learn more about a network before deciding to join it. There are many relevant uses for this additional insight by the mobile device, such as network selection, automated roaming and offload, secure user authentication, emergency services, and QoS integration with operator networks carrying user traffic. Likely the most important use is to enhance network selection processes both by the human user as well as automated connection policies applied to the connection manager on the device.

On the heels of the IEEE's work, the Wi-Fi Alliance has also been at work creating a certification framework and specification that complements, and utilizes a subset of, the 802.11u interworking protocols. The Wi-Fi Alliance program is called Hotspot 2.0, as is the technical specification, which spells out the Passpoint™ certification requirements. Wi-Fi Certified Passpoint™ is a Wi-Fi Alliance certification (based on Hotspot 2.0 technology) for clients and Wi-Fi infrastructure equipment. Hotspot 2.0 was completed (v1.0) in the first half of 2012, and device interoperability testing has been in progress since the summer of 2012.

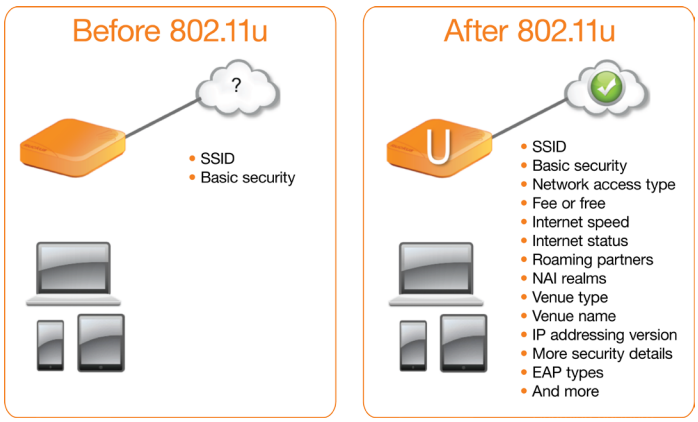
The Passpoint™ initiative will come to market in phases, with Release 1 delivering the heart of the technical features (network discovery/selection, smooth mobility, secure connectivity) and the beginning of product certifications. Release 2 is expected to come in 2014, and will introduce automated credential and network-selection policy provisioning that will allow users to easily subscribe to Hotspot 2.0 services.

Network Discovery and Selection

One of the most significant and fundamental functions of any Wi-Fi network is the process by which client stations (laptops, tablets, phones, etc.) discover access points (APs) and determine their capabilities. Clients can use active (probes) or passive (beacons) scanning techniques to discover APs, learn about the network, determine which network is best, and make a connection. Unfortunately, this process today depends on user recognition of the network name: the SSID.

802.11u does not fundamentally alter the basic discovery process; however, it does enable the discovery of new information during the scanning process and it allows the client to query the AP for more information.

FIGURE 1: Network Discovery With and Without 802.11u



How Interworking Works:

A Detailed Look at 802.11u and HotSpot 2.0 Mechanisms

A significant change with 802.11u is that connectivity to multiple "home" networks can be advertised using a single SSID. For example, the "PublicHotspot" SSID could be used to advertise that a Hotspot has the ability to automatically authenticate subscribers of a number of fixed or mobile operators.

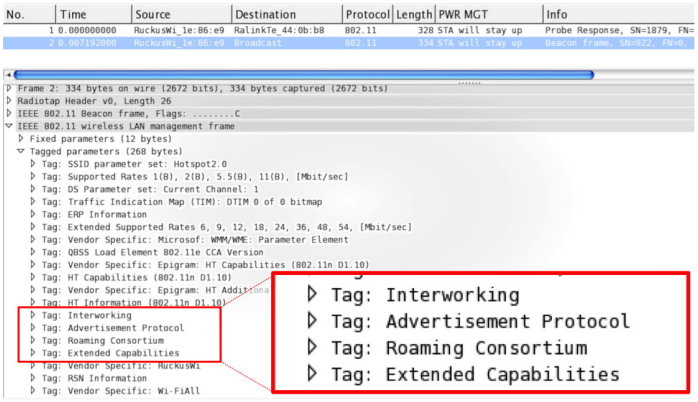
In 802.11, clients learn about AP networks via beacons and probe response frames. Each beacon or probe response carries information about the AP's capabilities in a component of the frame called an information "element." Naturally, the 802.11u protocol focuses on enhancing network discovery by adding new information elements to these frames. The most noteworthy of the new elements are shown in Table 1.

TABLE 1

Information Element Name	Description
Extended Capabilities	Indicates whether an AP supports 802.11u interworking features.
Interworking	Identifies the interworking service capabilities of the AP or client
Advertisement Protocol	Identifies the network's support for particular advertisement protocols, such as ANQP, which allow the client to learn more about the network by querying the AP prior to forming a connection
Roaming Consortium	Identifies service providers or groups of roaming partners whose security credentials can be used to connect to a network

These elements warrant a deeper look to help us understand exactly how they are used and what they communicate about the network.

FIGURE 2: 802.11u Information Elements in a Beacon Frame



Extended Capabilities Element

This element existed prior to 802.11u; some of the previously unused bits are now used to indicate AP support for interworking features:

- Interworking — Bit is set (to 1) to indicate interworking support
- QoS Map — Bit set to indicate support for QoS mapping from 802.11 to external networks
- SSPN Interface — Bit set to indicate that the AP has a logical backend interface to external service providers (SSPN – Subscription Service Provider Network)

NOTE: The Hotspot 2.0 specification has also defined a new information element called the Hotspot 2.0 Indication element. This element serves a similar purpose as the Extended Capabilities element; its basic purpose is to indicate support for, and compliance with, Passpoint™ (Hotspot 2.0) certification.

Interworking Element

The interworking element communicates basic features related to interworking services. Anytime we see this element in a frame, we know the AP or client sending the frame supports 802.11u. APs include the Interworking element in beacons and probe responses and clients include it in probe requests and (re)association requests.

FIGURE 3: Interworking Element Format

	Element ID	Length	Access Network Options	Venue Info (Optional)	HESSID (optional)
Octets	1	1	1	0 or 2	0 or 6

In this element, we learn some important things about the network.

Access Network Options

What type of access network is this?

- Private — home and enterprise networks
- Private with guest access — enterprises offering guest connectivity
- Chargeable public network — available to anyone, but requires a fee

How Interworking Works:
A Detailed Look at 802.11u and HotSpot 2.0 Mechanisms

- Free public network — available to anyone, no fees
- Personal device network — for peripherals in an ad-hoc mode
- Emergency services only

Does this network provide access to the Internet?

- Yes
- Unspecified

If this is an unsecured network (open authentication), are there additional steps required for access (ASRA)?

- Yes
- No

The interworking protocols are interested in solving problems with modern Hotspots, notably security problems. However, the ASRA information is for unsecured networks that are akin to today's open public networks. The ASRA field tells the higher layer protocols on the client device what steps to take (e.g. URL redirection, terms and conditions, etc.) after the connection is made.

Does the AP support Emergency Services?

- Yes
- Unspecified

Venue Info

Including venue information in the Interworking element is optional, but it may be used to improve network selection behavior by users or client devices. Users or operators may be able to more precisely control network connection preferences by using venue types in the decision criteria. Mobile device manufacturers can also provide venue-specific device behaviors (e.g., turning off their ring tone when in a movie theater or place of worship).

What is the venue type for this network?

Venue Groups — this field identifies the general class of venue (a sample of possible groups are listed)

- Assembly
- Business
- Educational
- Industrial
- Residential
- Vehicular
- Outdoor

Venue Types — this field identifies the specific type of venue within each group (a sample of possible types within the "Assembly" group are listed below)

- Arena
- Stadium
- Place of Worship
- Library
- Restaurant

HESSID

A homogenous extended service set (ESS) is a group of basic service sets that all provide access to the same external networks. A homogenous ESS is identified by its HESSID, which takes the form of a MAC address (6 bytes). The value used as the HESSID must be the Basic Service Set Identifier (BSSID) of an AP within the homogenous ESS.

Because the HESSID is based on a BSSID, it is a globally unique value. As such, it could be used in concert with the SSID to identify a specific service provider network. Client devices could also use the HESSID value to ensure that a mobility event (Wi-Fi roaming) would not disrupt a specific application service. The client would know if the new service set is in the same homogenous ESS as its existing connection. Advertising an HESSID is optional.

FIGURE 4: A Sample Interworking Element

```
▽ Tag: Interworking
    Tag Number: Interworking (107)
    Tag length: 9
    .... 0010 = Access Network Type: Chargeable public network (2)
    ...0 .... = Internet: 0
    ..0. .... = ASRA: 0
    .0.. .... = ESR: 0
    0... .... = UESA: 0
    Venue Group: Business (2)
    Venue Type: 8
    HESSID: RuckusWi_1e:86:e9 (58:93:96:1e:86:e9)
```

Roaming Consortium Element

A roaming consortium is a group of service providers (SP) with which a user's credentials can be used for authentication. Service providers in a roaming consortium have user roaming agreements

How Interworking Works:
A Detailed Look at 802.11u and HotSpot 2.0 Mechanisms

FIGURE 5: Roaming Consortium Element Format

	Element ID	Length	Number of ANQP OIs	OI # 1 and #2 Lengths	OI #1	OI #2	OI #3
Octets	1	1	1	1	variable	variable	variable

with one another. Naturally, the Roaming Consortium Element tells a mobile device which roaming consortiums or service providers are available through an AP.

Roaming consortiums are identified by an organization identifier (OI) that is assigned by the IEEE—similar to the first half of a MAC address. An OI is often 24 bits in length, but can also be 36 bits (i.e. OUI-36). OIs are globally unique, identifying a manufacturer, operator, or other organization. Passpoint™ certification requires that large network operators (i.e. national or regional)—who will be providing credential authentication for their subscribers at visited Hotspots—register for and advertise an OI for their network operations. Smaller venue operators are not required to do so.

During network discovery and selection, the client device will receive this list of OIs and determine if any of them meet the device's connection and roaming policies. The Roaming Consortium element can include up to 3 OIs in the beacon, but will also notify clients if additional OIs are available via ANQP query (e.g. "Number of ANQP OIs").

FIGURE 6: Sample Roaming Consortium Element

```
▽ Tag: Roaming Consortium
    Tag Number: Roaming Consortium (111)
    Tag length: 10
    Number of ANQP OIs: 0
    .... 0011 = OI #1 Length: 3
    0101 .... = OI #2 Length: 5
    OI #1: 506f9a - Wi-FiAll
    OI #2: 001bc504bd
```

Advertisement Protocol Element

With each new enhancement to the 802.11 protocols, APs must communicate more information in beacons and probe responses. 802.11u is no exception. In fact, the purpose of 802.11u is primarily to improve network selection by advertising more information about the network services behind the AP. With that purpose in mind, APs that support interworking could consume a lot of airtime just by advertising their services in beacons. However, some or all of the interworking information will be irrelevant to some clients and users, especially those that do not support 802.11u.

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

The Advertisement Protocol element facilitates this function by identifying the advertisement protocol(s) by which a client may query the AP for more information.

FIGURE 7: Advertisement Protocol Element Format

	Element ID	Length	Advertisement Protocol Tuple #1	Advertisement Protocol Tuple #2 (optional)	--	Advertisement Protocol Tuple #n (optional)
Octets	1	1	variable	variable		variable

When the AP receives such queries from a station, it may either reply directly or proxy the request to an external Advertisement Server.

What are the Advertisement Protocol options?

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

802.11u and Hotspot 2.0 querying functionality is built around ANQP, but as you can see, 802.11u also provides room for vendor-specific advertisement protocols that can be used to enable other pre-association services other than network advertisement and selection. For instance, an advertisement service integrated with location-based systems could be used to "push" a targeted promotion to a station, even prior to association (assuming client support).

For now, let's take a more detailed look at the advertisement protocols.

How Interworking Works:
A Detailed Look at 802.11u and HotSpot 2.0 Mechanisms

FIGURE 8: Sample Advertisement Protocol Element

```
▽ Tag: Advertisement Protocol
    Tag Number: Advertisement Protocol (108)
    Tag length: 2
  ▽ Advertisement Protocol element: ANQP
    ▽ Advertisement Protocol Tuple: Access Network Query Protocol
        .111 1111 = Query Response Length Limit: 127
        0... .... = PAME-BI: 0
        Advertisement Protocol ID: Access Network Query Protocol (0)
```

GAS

The Generic Advertisement Service (GAS) is a framework that provides transport for advertisement services like ANQP. When a client must query the AP using an advertisement protocol, it uses GAS to do so. GAS provides a frame exchange process (GAS Request/Response) and a framing format (using 802.11 Action frames) for the advertisement services. The advertisement protocols listed in the previous section would be transported by GAS. GAS Action frames contain fields used by the transported advertisement protocol to fulfill its purposes, as we will show later. One reason GAS is used is that prior to association, mobile devices have not obtained an IP address.

ANQP

The Access Network Query Protocol (ANQP) is—quite simply—a query protocol used by stations to discover information about the network. ANQP would be used to discover network information that is not advertised in beacons. ANQP is the advertisement protocol upon which 802.11u and Hotspot 2.0 are built, and support for it is mandatory for both 802.11u and Hotspot 2.0. As you'd expect, it will be heavily used in vendor products and will become the standard WLAN query protocol. GAS frames are used to transport the Access Network Query Protocol (ANQP).

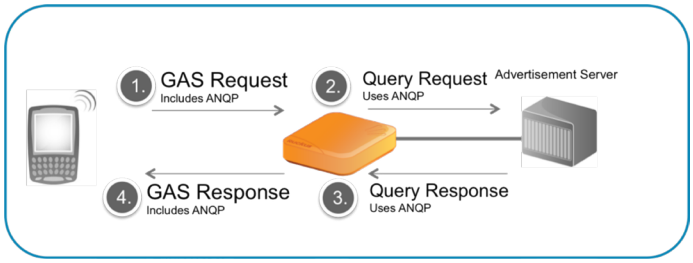
GAS, ANQP, and the Query Process

Thus far, we've looked at the network selection elements and fields in beacons and probe responses. Now let's expand the network selection concept and explore how GAS and ANQP are implemented in the query process.

In 802.11 networks, at any point in time, a Wi-Fi client and AP may be in one of several different states of connectivity. The network discovery and selection process occurs when the AP and client are in an unauthenticated and unassociated state—the initial stage. Prior to 802.11u, a client station selected a network based on basic info in beacons and probe responses. Clients had no way to see beyond the AP into the wired network prior to association. That's where 802.11u and the query process come into play.

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

FIGURE 9: A Logical Overview of the Advertisement Protocol Process



Previously, we noted that ANQP information is carried within GAS Action frames. Specifically, the GAS frames include ANQP elements. The client sends a GAS Request, providing a list of ANQP elements that it wants to receive from the AP. The AP either satisfies the query out of its own configured datastore or relays the client's query to backend advertisement servers—the backend encapsulation protocols are not specified by 802.11u or Hotspot 2.0. The AP replies to the client with a GAS Response, which includes the ANQP elements requested by the client.

As we did earlier in the paper with the 802.11 interworking frame elements and fields, let's look closer at the ANQP elements and the information available by client query.

ANQP Elements

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

- ANQP Query list — the Query List is sent by the client station in a GAS Request, indicating a list of elements (the elements listed below) it would like to receive in a GAS Response
- ANQP Capability list — this element is a bit like a checklist, identifying the ANQP elements that are supported (and will be returned in the GAS Response) by the AP

How Interworking Works:
A Detailed Look at 802.11u and HotSpot 2.0 Mechanisms

- Venue Name information — indicates the name of the venue for the network, which may be useful to a user for network selection (e.g., Ella's Coffee Shop, 5/3 Ballpark, etc.)
- Emergency Call Number information — provides a list of location-specific emergency numbers
- Network Authentication Type Information — if this is an unsecured network (following the legacy Hotspot model), what additional steps are required for access (ASRA)?
  - Acceptance of terms and conditions
  - On-line enrollment supported — may require the user to create an account of some type
  - HTTP/HTTPS redirection — the URL to which the browser is redirected is indicated
  - DNS redirection — Note that the Hotspot 2.0 specification forbids network operators from supporting protocols that are not interoperable with DNSSEC. DNS redirection for captive portals violates this requirement.
- Roaming Consortium list — provides the same information as the Roaming Consortium information element in beacons and probe responses (which has a max of 3 Organization Identifiers (OIs)), but this list can contain many more OIs. This ANQP element acts as overflow if more than three roaming consortiums are supported, which is more likely in the long-term vision of 802.11u/ Hotspot 2.0 networks.
- IP Address Type Availability information
  - IPv6
    - Available
    - Not available
    - Availability unknown
  - IPv4
    - Available
    - Public IPv4 available
    - Port-restricted IPv4 available
    - NAT
    - Double NAT
    - Port-restricted and NAT
    - Port-restricted and double NAT
    - Availability unknown
- NAI Realm list — identifies all NAI realms available through the BSS (and its service providers) and (optionally) the EAP types supported by each realm

  A network access identifier (NAI) is a standardized (RFC 4282) format for identifying users requesting access to a network (e.g. user@realm.com). Thus, an NAI Realm identifies the proper authentication server or domain for the user's authentication exchange. By discovering which authentication realms are supported by a network, a mobile device can selectively authenticate to its preferred networks.

  The NAI Realm list can also optionally indicate the Extensible Authentication Protocol (EAP) types supported by each realm as well as the authentication parameters for that EAP type. An example authentication parameter is the client credential type (token, certificate, username/password, SIM, etc.) or inner authentication method (PAP, CHAP, MSCHAP, MSCHAPv2).
- 3GPP Cellular Network information — identifies the 3GPP cellular networks available through the AP. Specifically, this field identifies the Public Land Mobile Network (PLMN) ID, comprised of the Mobile Country Code (MCC) and Mobile Network Code (MNC) of the mobile operator. When the client is a mobile device with a cellular subscription (containing a SIM or USIM for cellular authentication), the PLMN ID will be used if the Hotspot provides credential authentication with the subscriber's mobile operator.
- AP Geospatial Location — provides the AP's location in longitude, latitude, and elevation (LCI format)
- AP Civic Location — provides the AP's location in civic format (country, province, state, city, district, street, house number, unit, etc.)
- AP Location Public Identifier URI — provides a reference URI at which location information can be retrieved
- Domain Name list — lists one or more domain names for the entity operating the AP. This is a critical for Hotspot 2.0 network selection policy, as it identifies the operator of the network. It indicates to the mobile device whether they are at a home or visited Hotspot.
- Emergency Alert Identifier URI — provides a URI for Emergency Alert System (EAS) message retrieval
- Emergency NAI —provides an NAI string that the client can use with EAP authentication to access emergency services
- ANQP vendor-specific list — as usual, the IEEE has made accommodations for vendors to implement their own elements using a standardized format

The above list of ANQP elements come from the 802.11u amendment.

How Interworking Works:
A Detailed Look at 802.11u and HotSpot 2.0 Mechanisms

FIGURE 10: GAS Initial Request with ANQP requesting a Roaming Consortium list

```
▽ IEEE 802.11 wireless LAN management frame
  ▽ Fixed parameters
      Category code: Public Action (4)
      Public Action: GAS Initial Request (0x0a)
      Dialog token: 0x01
      Tag Number: Advertisement Protocol (108)
      Tag length: 2
    ▽ Advertisement Protocol element: ANQP
      ▷ Advertisement Protocol Tuple: Access Network Query Protocol
    ▽ Query Request: ANQP Request - ANQP Query list
        Query Request Length: 6
      ▽ Info ID: ANQP Query list (256)
          Length: 2
          ANQP Query ID: Roaming Consortium list (261)
```

Hotspot 2.0 ANQP Elements

The Wi-Fi Alliance has also introduced its own Hotspot 2.0 ANQP elements to extend the querying functionality. To do so, the Hotspot 2.0 elements utilize the vendor-specific ANQP format. You'll notice that some of these elements are similar to 802.11u elements, while others are important functions unaddressed by 802.11u.

- HS Query List — like the 802.11u Query List, this list identifies the Hotspot 2.0 ANQP elements being requested
- HS Capability List — indicates the Hotspot 2.0 ANQP elements that will be returned by the AP
- Operator Friendly Name element — an open text field used to identify the Hotspot venue operator. The field can be repeated multiple times in different human languages.
- WAN Metrics element —provides details about the WAN connection available through the WLAN
  - WAN Info
    - Link Status (Up / Down / Test)
    - Symmetric Link (yes / no)
    - At Capacity (yes / no) — determines whether new mobile clients will be permitted to associate to the AP
  - Downlink Speed
  - Uplink Speed
  - Downlink Load
  - Uplink Load
  - Load Measurement Duration — indicates the time value over which the downlink and uplink load calculations were made

    This element could be extremely useful for network selection, particularly in cellular offload scenarios. Despite the many potential benefits of Wi-Fi connectivity, one occasional problem at public access networks is an under-provisioned (or poorly functioning) WAN connection—to end-users, the experience is still a "Wi-Fi problem." The WAN Metrics information could help client devices select the least congested and highest bandwidth portal to the Internet, which is usually (but not always) Wi-Fi.

    Unfortunately, for many venue owners and network operators, announcing Internet speeds could result in bad press if the network is under-provisioned. For political/marketing reasons, the WAN Metrics information may not see wide use.
- Connection Capability element —this element provides connection status for commonly used communication ports and protocols. It identifies the availability of common IP protocols (TCP, UDP, IPsec) and ports (21, 80, 443, 5060). This element will be important for clients attempting to determine whether a particular service is available, such as HTTP/HTTPS, VPN protocols, FTP, ICMP, or others. If an upstream firewall in the access network blocks these protocols or they are otherwise unavailable, this element will make that known to the client station, allowing it to manage connections based on application needs.
- NAI Home Realm Query —this element is a query sent by clients to discover supported realms. In its request, the client includes the NAI realms for which it has authentication credentials. The AP compares the list in the client's query to the NAI Realms it can reach and then responds to the client accordingly. This query could be used exclusively to answer the core question "can you authenticate me against the following realms, yes or no?"
- Operating Class Indication element —provides a list of Wi-Fi frequencies supported by the APs in the ESS.

Network Selection in Real Life

As you can see, 802.11u and Hotspot 2.0 take big strides in making more information available to client devices prior to association. With the rich information made available, network administrators, operators, and device owners will be able to tailor their network selection profiles and policies with much more precision.

How Interworking Works:
A Detailed Look at 802.11u and HotSpot 2.0 Mechanisms

The exact way in which these capabilities will be implemented in mobile devices is still unclear. Industry pundits have justifiable concerns about how this discovery information will be displayed to the user or incorporated into connection policies on the device's connection manager. Cellular service providers certainly have a vested interest in controlling the connection manager and will require some control of devices, but since Wi-Fi connections may be at home, work, or public venues, end-users still want control and visibility.

The Wi-Fi Alliance has provided one requirement on the network selection function of the mobile device in the HS 2.0 Tech Spec. This requires that the mobile device shall give preference to connect to a Hotspot operated by its home SP over a Hotspot operated by a visited SP, except when overridden by user preference.

Other connection management issues will need a graceful solution as well, such as how a user configures initial connectivity preferences, how those preferences are applied and used thereafter, and ensuring that this process is intuitive for the non-technical user. In the end, several participants in the ecosystem (users, device manufacturers, network operators/owners, service providers) may influence the selection process, but it depends in large part on the device manufacturer and their user interface design. Regardless of its exact form, the prize comes in the form of performance improvements, a better overall connectivity experience for users, operator control, and automated security—which is where we'll turn now.

Secure Hotspots

With today's Hotspots, manual—and blind—network selection is a major problem. An interrelated and possibly more acute problem is the utter lack of security. Fixing this problem was a primary objective of the 802.11u and Hotspot 2.0 initiatives; however, WLAN security has many layers that need to be addressed.

Hotspots today could be secured—and some are—but today's solutions are not cost-effective, simple, or user-friendly. Simple passphrases can be issued (WPA2-Personal) in some cases, but if all users share the same password, its privacy value is lessened. Further, many public network venues lack an effective method to distribute the password to new users. Similar ease-of-use problems exist with 802.1X, and there are additional issues including configuration complexity of end devices, credential distribution, certificate management, and backend solution support.

Today's Hotspots are already very difficult to use (manual network selection, terms and conditions, captive web portals, etc.). Adding security to today's model would make Hotspots completely unusable. Lacking an easy and comprehensive security solution, Hotspot operators forego security altogether, and customers use the network at their own risk.

	Today's Hotspot	Hotspot 2.0
Network Discovery/ Selection	Manual (SSID)	802.11u
Subscriber Authentication	Captive Portal, WISPr	802.1X
Over-the-Air Encryption	none	AES-CCMP (802.11i)
Mutual Authentication	none	EAP-SIM/AKA, EAP-TLS, EAP-TTLS
Rogue/Hijacking Protection	none	Yes (802.1X/EAP)

802.11u and Hotspot 2.0

One of the key requirements for automated client connectivity to Wi-Fi is the assurance of robust security. Neither end-users nor carriers want mobile devices to thoughtlessly prioritize unsecured Wi-Fi networks over secure cellular networks—for many applications, anyway. For cellular offload, operators are expected to match both the security and ease-of-use of cellular networks. The interworking protocols pave the way for automated, robust security by first providing information to the client. Specifically, during the network selection process (as discussed earlier), the client discovers the operator domains, roaming consortiums, authentication realms, and EAP types supported by a Wi-Fi network prior to joining. Then, if the network services match the client's security requirements and connectivity policies, it will associate using 802.1X/EAP authentication. The AP provides backend connectivity to an authentication entity and forwards client authentication frames as necessary.

To ensure that Passpoint™-certified networks are optimally secured, Hotspot 2.0 mandates that certified APs support WPA2-Enterprise (802.1X/EAP authentication with AES-CCMP encryption). Hotspot 2.0 certified devices must also support EAP types from the following list:

- TLS
- TTLS/MSCHAPv2
- SIM
- AKA

HS 2.0 certified APs must support all of the EAP types listed above.

How Interworking Works:
A Detailed Look at 802.11u and HotSpot 2.0 Mechanisms

FIGURE 11: Example Certificate of a Passpoint™-certified AP

All certified client devices are required to support EAP-TLS and EAP-TTLS. Client devices with cellular subscriptions and credentials (SIM or USIM) must also support EAP-SIM and EAP-AKA.

EAP-SIM and EAP-AKA (as well as AKA') are used for cellular authentication today. EAP-TLS and -TTLS are popular enterprise EAP types, and were chosen to broaden the client credential options, particularly for devices like Wi-Fi enabled tablets that do not support a cellular credential. EAP-TLS supports certificates for both client and server authentication while EAP-TTLS/MSCHAPv2 supports client-side username/password pairs and a server-side certificate.

Other EAP types (EAP-FAST and PEAP, as examples) will be used at Hotspots as well, but the four EAP types listed above are both commonly supported and standardized.

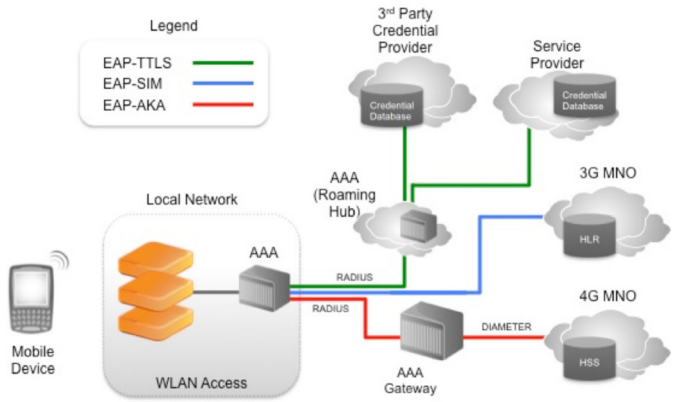
Other Industry Initiatives

802.11u and Hotspot 2.0 provide necessary, but not sufficient, pieces in solving the Hotspot security problem. Mandatory support for 802.1X at Hotspot 2.0 networks requires that the network operator integrate its access points with a AAA server and user database. However, to make these security services useful to users, the AAA server(s) must provide access to authentication realms for which users have valid credentials.

A sample use case for this technology is for service provider Wi-Fi at public venues. A mobile phone may have a valid credential (e.g. a SIM card) with the service provider, but the Hotspot must have access to the service provider's authentication services. Hotspot APs could integrate directly with the service provider's authentication servers; of course, not all Hotspot venues will be able to integrate directly with large service providers or other widely used credential databases, so roaming aggregators will be used as hubs to ease this process.

In the roaming hub model, an authentication brokerage service is provided by a third-party company. The brokerage company forms relationships with credential providers and integrates with their systems. Then the network operator integrates with the brokerage company's authentication service, thereby gaining access to the credential stores through the brokerage hub.

FIGURE 12: Overview of Authentication Concepts (samples only: not exhaustive or all-inclusive)



In addition to wireless carriers, any organization that offers a credential to its traditional customers could act as a credential store (aka Identity Provider) for public Wi-Fi usage. Such companies include device manufacturers, email service providers, social media companies, retailers, fixed broadband service providers, and many others.

In addition to the IEEE and WI-FI Alliance, other industry organizations are working to promote and test this complex ecosystem. The Wireless Broadband Alliance, in partnership with the Wi-Fi Alliance, is a part of this effort with its Next Generation Hotspot (NGH) program. It has conducted trials to test the use and interoperability of backend integration between operators and AAA providers. "End-to-end international roaming," and "seamless interoperability across home and visited network operators" are two main elements of the NGH trials.

Much of the integration work with 802.11u depends on partnerships and platform integration in a way that appeals to all parties—service providers, roaming aggregators, network

operators, device manufacturers, and end-users. To that end, one of the major hurdles in bringing this solution to market is creating such business relationships.

QoS and Emergency Services

Two additional features are enabled by the interworking enhancements that were not included in the Hotspot 2.0 Release 1 specification. QoS mapping with external networks and emergency services don't hold the same publicity appeal as network discovery/selection and security, but could be useful enhancements nonetheless. This section will be a brief introduction only.

QoS Mapping

Changes in the cellular industry have been a major driver for interworking protocols in Wi-Fi. And even though some cellular services will be offloaded to Wi-Fi, service providers still have a vested interest in the quality of the user's wireless experience. Further, some service providers may still require Wi-Fi voice and data services to be tunneled through their core data network. To that end, 802.11u incorporates a method by which the QoS policies of a service provider's network can be mapped to the WLAN for proper end-to-end QoS. The primary objective with 802.11u QoS is to map the Layer-3 QoS priorities of an SSPN to the over-the-air Layer 2 Wi-Fi priority.

To accomplish this goal, 802.11u introduces the QoS Map Set Information element. This element contains a list of 802.11 user priorities (UP), to which a range of DSCP (i.e. IP QoS) values are mapped.

When 802.11u-compatible client stations receive the QoS map, they use it to map the IP-layer priority (i.e. DSCP field) to an 802.11 priority. As frames are passed from the IP layer of the device's networking stack to the MAC layer, they are mapped according to the 802.11u policy provided by the AP. Likewise, APs follow these maps on downlink QoS frames received from the wired network and sent to the client. This mapping enables the consistent end-to-end policies desired by service providers.

FIGURE 13: QoS Map Set Information Element

	Element ID	Length	DSCP Exception #n (optional)	UP 0 DSCP Range	UP 1 DSCP Range	...	UP 7 DSCP Range
Octets	1	1	2	2	2	...	2

Emergency Services

In some previous sections of this paper, we have already introduced various fields and elements that facilitate client discovery of emergency services. 802.11u provides a means for the client devices to learn about emergency services prior to association and then to support them at the link-level. Though many Wi-Fi Hotspots will not provide emergency services, networks that are designed to offload/replace cellular voice services are likely to do so.

Link-level support of emergency services is provided via a few primary functions:

- Emergency service discovery by unassociated client devices (does the AP support emergency services?)
- Advertisement of important emergency details, such as notifications of emergency alerts, URIs that provide more information about a specific emergency alert, and emergency contact numbers
- Optional support for unauthenticated emergency services, making emergency services available to any user, with or without a valid authentication credential

Conclusion

802.11u and Hotspot 2.0 are bridging opportunities in public access networks everywhere, and their impact will have broad implications for end-users, small businesses, enterprises, and carriers. As this technology proliferates, the reality of secure and universal wireless connectivity will become more tangible. The Wi-Fi Certified Passpoint™ program stepped forward in the second half of 2012 and will see broader adoption throughout 2013 and later.

These technologies create a framework that provides rich contextual information during network discovery. With the extensive information obtained, client devices and end users can intelligently, automatically, and accurately select the right network supporting the right services the first time. With improved network discovery and selection as an underpinning, Hotspot security is revitalized. WPA2-Enterprise will become the norm, as it should, and end-users can safely use public networks without fear.

Stakeholders everywhere should be pleased. 802.11u, Hotspot 2.0, and Passpoint™, along with other industry initiatives like the WBA's Next Generation Hotspot, were developed with a broad scope in mind. They were designed to accommodate many distinct business models, which will serve to increase Wi-Fi's usability and further solidify its place as the most important wireless technology in history. The solutions described in this paper benefit everyone. Service innovators win. Hotspot operators win. Enterprises win. End-users win. Wi-Fi wins.

How Interworking Works:

A Detailed Look at 802.11u and HotSpot 2.0 Mechanisms

Acronyms	
3GPP	3rd Generation Partnership Project
AAA	Authentication, Authorization and Accounting
AES-CCMP	Advanced Encryption Standards (AES) - Counter Cipher Mode with Block Chaining Message Authentication Code Protocol (CCMP)
AKA	Authentication and Key Agreement
ANQP	Access Network Query Protocol
ASRA	Additional Steps Required for Access
BSS	Basic Service Set
BSSID	Basic Service Set Identifier
CHAP	Challenge Handshake Authentication Protocl
DNSSEC	Domain Name System Security Extensions
DSCP	Differentiated Services Code Point
EAP	Extensible Authentication Protocol
EAS	Emergency Alert System
ESR	Emergency Services Reachable
ESS	Extended Service Set
GAS	Generic Advertisement Service
GSM	Global System for Mobile Communications (originally Groupe Special Mobile)
HESSID	Homogenous Extended Service Set Identifier
LCI	Location Configuration Information
MCC	Mobile Country Code
MNC	Mobile Network Code
MIH	Media Independent Handover
MSCHAP	Microsoft Challenge Handshake Authentication Protocol
MSCHAPv2	Microsoft Challenge Handshake Suthentication Protocol Version 2
NAI	Request-to-Send/Clear-to-Send
NAT	Network Address Translation
OCSP	Online Certificate Status Protocol
PAP	Password Authentication Protocol
PLMN	Public Land Mobile Network
OI	Organization Identifier
OUI	Organizationally Unique Identifier
QoS	Quality of Service
SIM	Subscriber Identity Module
SP	Service Provider
SSID	Service Set Identifier
SSPN	Subscription Service Provider NEtwork
TLS	Transport Layer Security
TTLS	Tunneled Transport Layer Security
UESA	Unauthenticated Emergency Service Accessible
UMTS	Universal Mobile Telecommunications System
UP	User Priority
USIM	Universal Subscriber Identity Module
URI	Uniform Resource Identifier
WAN	Wide Area Network

Ruckus®
Simply Better Wireless.

Ruckus Wireless, Inc.
350 West Java Drive
Sunnyvale, CA 94089 USA
(650) 265-4200 Ph \ (408) 738-2065 Fx

www.ruckuswireless.com