white paper

July 2013

Hotspot 2.0

MAKING WI-FI AS EASY TO USE AND SECURE AS CELLULAR

Today’s cellular networks are being overwhelmed with data traffic, much of it being generated by the rapid proliferation of smartphones. The latest projections are for the industry to ship over 800 million such devices in 2013.

To deal with all this traffic, service providers are looking for technologies that can greatly increase the densification of their networks. Wi-Fi is an excellent option here as it has access to upwards of 600 MHz of spectrum, supports dense AP deployments, is available on all data-centric devices, and it is available in all locations where people congregate. These locations include stadiums, arenas, airports, convention centers, colleges, train stations, downtown city center and the like. Most of these venues are indoors, where Wi-Fi is an especially strong solution because of its enormous capacity and its ability to support neutral host deployments.

Capacity and ease of deployment are only the first steps in enabling a carrier-class solution. The industry is now focused on improving the Wi-Fi user experience while roaming. The goal being to allow users to connect to visited networks as easily as they can connect to their home network. And the easier it is to get connected to a network, the more likely it is to be used. This work is known as Hotspot 2.0 and is being driven by the Wi-Fi Alliance (WFA), which also certifies interoperability as part of their Passpoint™ program. The Wireless Broadband Alliance is also very much involved in the process through their Next Generation Hotspot (NGH) initiative.

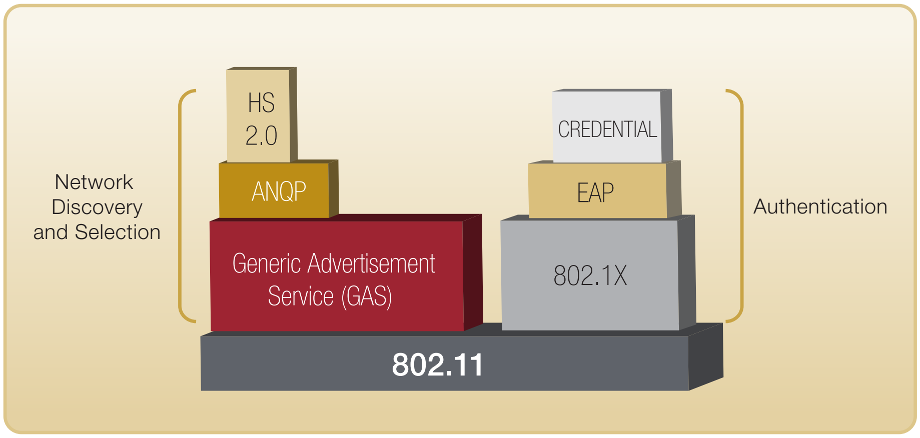
Hotspot 2.0 is focused on enabling a mobile device to automatically “discover” APs that have a roaming arrangement with the user’s home network and then securely connect. This is very much the cellular experience that we all enjoy when getting off an airplane just about anywhere in the world. Wi-Fi roaming would apply anytime a mobile device does not see an AP belonging to its home network provider. A user could roam on a Wi-Fi network that is across town or on the other side of the world. Roaming partners can include MSOs, MNOs, wireline operators, public venues, enterprises, and basically any other entity that has Wi-Fi assets.

Hotspot 2.0 capabilities are emerging in a series of releases, the first of which was completed in June of 2012 and certifications began shortly thereafter.

Hotspot 2.0

MAKING WI-FI AS EASY TO USE AND SECURE AS CELLULAR

Figure 1: Hotspot 2.0 protocol stack


Network Discovery and Selection
HS 2.0
ANQP
Generic Advertisement Service (GAS)
CREDENTIAL
EAP
802.1X
Authentication
802.11

Hotspot 2.0 Release 1

Release 1 is focused squarely on over-the-air security and network discovery and selection. The key enabling protocols are IEEE 802.11u, along with IEEE 802.1X, selected EAP methods, and IEEE 802.11i. The latter three are part of the WPA2-Enterprise certification program in the Wi-Fi Alliance, and are standard on all smartphones. While the certification is called "WPA2-Enterprise", the end result is a process that is every bit as secure and easy to use as what exists in the cellular world.

The IEEE 802.11u protocol enables a mobile device to have a dialog with a Wi-Fi AP "pre-association" to determine the capabilities that the network can support. The two protocols that 802.11u uses to make this happen are the generic advertisement service (GAS) and the access network query protocol (ANQP). These protocols run on top of 802.11 and enable the Hotspot 2.0 experience (see Figure 1).

The Process of Network Discovery and Selection

When a user with an HS2.0 capable mobile device comes within range of a Hotspot 2.0 capable AP, it will automatically open up a dialog with that AP to determine its capabilities. This is done using ANQP packets that are carried at layer 2 by the GAS service (Note: the device has not yet attached and does not yet have an IP address). It is the exchange of ANQP packets that allows the mobile device to automatically learn the capabilities of an AP. A few of the more important capabilities include:

1) The domain name of the network operator. If the AP is part of the user's home network then no roaming is required and the user can move straight to authentication. If the AP is not on the user's home network, then roaming is required.

2) If roaming is required, then the list of roaming partners that are supported by that AP must be passed down to the mobile device via the ANQP protocol. This can be provided in the form of a PLMN (Public Land Mobile Network) ID, realm, or the organizational identifier (OI):

- 3GPP PLMN ID (MCC plus MNC) would be the preferred method for a mobile operator. MCC refers to the mobile country code and MNC to the mobile network code.
- NAI Realm List (username@domain name) would be the preferred method to identify most non-mobile operators like MSOs, wireline operators, and public venues.
- IEEE Organization Identifier (6 hexadecimal digits that many would recognize as the first 3 bytes of a MAC address). The WFA recommends that national and international SPs have an Organization Identifier (OI). The two primary use cases for OI are as follows:
  - A small number of OIs can be put in the AP's beacon; if the mobile device recognizes the OI, it doesn't need to use ANQP to determine if it can successfully authenticate at that AP. This can conserve the mobile's battery as well as reduce the time to associate.
  - Some SPs may wish to sell subscription levels (e.g., gold, silver, bronze) in which not all subscribers have access at every AP. For example, gold users might have access privileges at all APs in an operator's network, but bronze users might not be authorized to use an operator's APs in premium locations.

It is possible that service providers might advertise roaming consortiums in more than one way. A mobile operator might advertise both a PLMN ID and a realm. The former is used for SIM-based devices and the latter for non-SIM devices. A wireline operator or an MSO would only advertise their realm, as they don't have a PLMN ID.

3) Other attributes that can be relayed to the mobile device include backhaul bandwidth and loading on the access network. This is useful information if there is more than one AP that can roam with the user's home network. Other details that are passed down to the phone as part of the HS2.0 process include:

- The operator friendly name (San Jose Airport for instance). This can be displayed on the mobile device once the connection is established and is fairly standard when roaming on cellular networks.
- Venue type (stadium or hospital)
- IP Address Type (v4/v6)
- Internet access or walled garden
- And more

Once the mobile device learns the roaming partners and the identity of the AP operator, it invokes some basic, built-in network selection policies to determine which AP to join. The basic policy provided by Passpoint Release 1 capable mobile devices is, in the absence of [overriding] user-configured preferences, to prefer Hotspot 2.0 compliant APs over legacy APs (i.e., non-Hotspot 2.0 APs) and to prefer an AP operated by the user's home operator over one operated by a visited operator. Users are allowed to specify that certain Wi-Fi networks should always have priority and these would typically include the user's home network and their work network.

The ability of the mobile device to "learn" about Wi-Fi network capabilities pre-association will completely transform the Wi-Fi user experience. It will also completely change the nature of an SSID (Service Set IDentifier). In the past, users and devices had to "remember" SSIDs that have provided connectivity in the past, so that they can be accessed again in the future. These are typically SSIDs for which they have credentials or which provide open access. With HS2.0 the importance of SSIDs will be reduced, and what really matters is *does the visited AP have a roaming arrangement with my home network provider*. In fact the notion of having an AP advertise many different SSIDs for different purposes will also be greatly reduced in favor of Hotspot 2.0 based advertisements. This should also enhance the performance of mobile networks, as it reduces the airlink traffic associated with the beacons generated by these additional SSIDs.

Secure Authentication

Hotspot 2.0 also requires the use of 801.1X authentication. Captive portal based authentication is *not supported in HS2.0.*[1] As part of the 802.1X authentication process, the following EAP methods must be supported:

- If a mobile device has a Subscriber Identity Module (SIM), then EAP-SIM as defined in RFC-4186
- If a mobile device has a UMTS Subscriber Identity Module (USIM), then EAP-Authentication and Key Agreement (AKA) as defined in RFC-4187.
- All mobile devices must support EAP-Transport Layer Security (TLS) as defined in RFC-5216 and which uses an X.509 digital certificate
- All mobile devices must support EAP-Tunneled Transport Layer Security (TTLS) as defined in RFC-5281) along with MS-CHAPv2 which uses username and password, with a server side certificate

TABLE 1

CREDENTIALS AND EAP METHODS IN HOTSPOT 2.0

Credential	EAP Method
Username / Password	EAP-TTLS + MS-CHAPv2
Certificate	EAP-TLS
(U)SIM (if mobile has this credential)	EAP-SIM, AKA

WPA2-Enterprise also requires that the airlink be encrypted using 802.11i. This addresses a security vulnerability with open access or portal based hotspots that don't provide airlink encryption. Hotspot 2.0 plugs this vulnerability with 802.11i, which uses AES (advanced encryption standard) technology. This combination of protocols is what enables Wi-Fi to be every bit as secure and easy to use as a cellular service. In addition, Hotspot 2.0 Release 1 improves upon WPA2-Enterprise security by eliminating the so-called "Hole-196" attack. In these attacks, a device can forge broadcast or multicast frames (as if coming from a legitimate AP) to initiate its attack.

[1] Hotspots using Captive Portal authentication are expected to be used in parallel with Hotspot 2.0-compliant hotspots due to the need to service users' legacy mobile devices.

Figure 2: Authenticating a roaming user to their home network

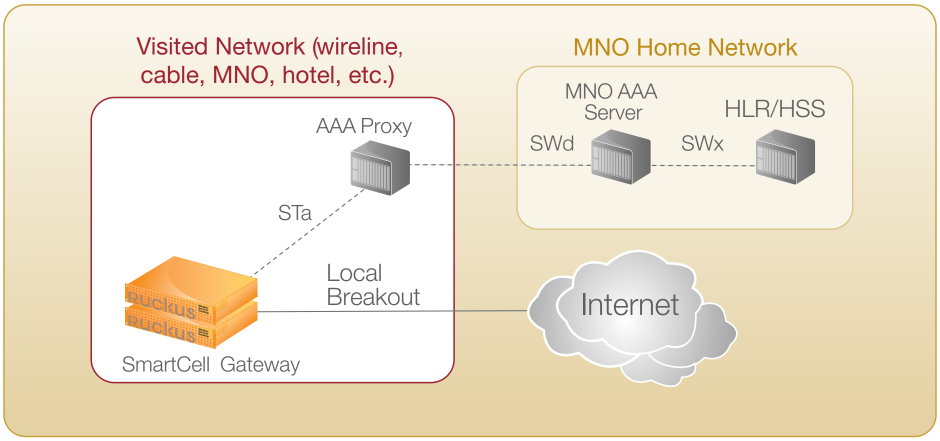


Figure 2 shows the process by which a user in a visited network can have their authentication request proxied back to the home network. In this example the visited network could be an MNO, MSO, a private enterprise, a public venue (such as a hotel, convention center, airport, etc.), or wireline provider. Wi-Fi greatly expands the universe of possible roaming partners, and thus the utility of a Wi-Fi network.

Settlements and the Business of Roaming

Hotspot 2.0 will greatly enhance the opportunities for Wi-Fi operators to monetize their networks through roaming arrangements with other providers. These providers can include MNOs, MSOs, wireline providers, and a wide variety of enterprises including hotels, convention centers, hospitals, airports, etc. This also queues up the very important subject of settlements, which are used to make sure all operators (mobile or wireline) get paid for services rendered, if appropriate. In 2012, WBA updated their WRIX service specifications, which governs settlements and billing. Key elements include WRIZ-i (interconnect), WRIX-d (data clearing), and WRIX-f (financial settlements). These services can be deployed by the home and visited network providers, either directly of through a 3rd party WRIX service provider.

The Impact of Hotspot 2.0

Hotspot 2.0's impact on the industry will be enormous. Mobile operators are already seeing their networks overloaded by data traffic and are looking at all available options to increase densification. At the top of their list are technologies like Wi-Fi and LTE small cells. Cable and wireline operators are taking advantage of their backhaul capabilities to rapidly build-out an extensive Wi-Fi footprint. This technology has also been extensively deployed in public venues like hotels, airports, convention centers, stadiums, hospitals, etc. With Hotspot 2.0, it will now be possible to link together this huge footprint of Wi-Fi APs through a web of roaming arrangements. Users will be able to seamlessly roam onto Wi-Fi networks from almost any location.

The net result for the MNO is much greater network densification then could be achieved by building out a network of APs on their own and a much better experience for the subscriber. Users no longer need to know or care about SSIDs and authentication protocols. Instead, they get an always best-connected experience.

Venue owners and operators can begin to better monetize their Wi-Fi network investments through these roaming arrangements and the settlements that they entail. A mobile operator that deploys a Wi-Fi network in a stadium can now monetize that asset by allowing subscribers of other operators to roam onto that network. Hotels can likewise allow subscribers of all the different mobile operators to roam onto their in-building Wi-Fi networks.

Hotspot 2.0 technology will radically transform the wireless industry, and it is set to emerge in 2013 in a very big way.

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