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.