Wireless Broadband Alliance

Signalling AP Location

For Wi-Fi Roaming

Source:	Wireless Broadband Alliance
Authors:	Signaling Location Information in RADIUS (SLIR)
Issue Date:	October 2023
Version:	1.0.0
Status:	Exclusively shared with IETF RADEXTRA Members

For other publications, visit our website here

To participate in further projects, contact pmo@wballiance.com

About the Wireless Broadband Alliance

Wireless Broadband Alliance (WBA) is the global organization that connects people with the latest Wi-Fi initiatives. Founded in 2003, the vision of the Wireless Broadband Alliance (WBA) is to drive seamless, interoperable service experiences via Wi-Fi within the global wireless ecosystem. WBA's mission is to enable collaboration between service providers, technology companies, cities, regulators and organizations to achieve that vision. WBA's membership is comprised of major operators, identity providers and leading technology companies across the Wi-Fi ecosystem with the shared vision.

WBA undertakes programs and activities to address business and technical issues, as well as opportunities, for member companies. WBA work areas include standards development, industry guidelines, trials, certification and advocacy. Its key programs include NextGen Wi-Fi, OpenRoaming, 5G, IoT, Testing & Interoperability and Policy & Regulatory Affairs, with member-led Work Groups dedicated to resolving standards and technical issues to promote end-to-end services and accelerate business opportunities.

The WBA Board includes Airties, AT&T, Boldyn Networks, Boingo Wireless, Broadcom, BT, Cisco Systems, Comcast, Intel, Reliance Jio, Turk Telekom and Viasat. For the complete list of current WBA members, click here.

Follow Wireless Broadband Alliance:

www.twitter.com/wballiance

http://www.facebook.com/WirelessBroadbandAlliance

https://www.linkedin.com/company/wireless-broadband-alliance

Undertakings and Limitation of Liability

This Document and all the information contained in this Document is provided on an 'as is' basis without warranty of any kind, either expressed or implied, including, but not limited to, the implied warranties of merchantability, fitness for particular purpose, or non-infringement.

In addition, the WBA (and all other organizations who may have contributed to this document) makes no representations or warranties about the accuracy, completeness, or suitability for any purpose of the information. The information may contain technical inaccuracies or typographical errors. All liabilities of the WBA (and all other organizations who may have contributed to this document) howsoever arising for any such inaccuracies, errors, incompleteness, suitability, merchantability, fitness, and non-infringement are expressly excluded to the fullest extent permitted by law. None of the contributors make any representation or offer to license any of their intellectual property rights to the other, or to any third party. Nothing in this information or communication shall be relied on by any recipient.

The WBA also disclaims any responsibility for identifying the existence of or for evaluating the applicability of any claimed copyrights, patents, patent applications, or other intellectual property rights, and will take no position on the validity or scope of any such rights. The WBA takes no position regarding the validity or scope of any intellectual property or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any effort to identify any such rights.

Neither the WBA nor any of the other organizations who may have contributed to this document will be liable for loss or damage arising out of or in connection with the use of this information. This is a comprehensive limitation of liability that applies to all damages of any kind, including (without limitation) compensatory, direct, indirect, or consequential damages, loss of data, income or profit, loss of or damage to property and claims of third parties.

Confidentiality

Privileged/confidential information may be contained in this document and any files attached in it ('WBA Documentation').

Only WBA member companies who have signed the new WBA IPR Policy (Located at: WBA Extranet and are the intended recipient are entitled to receive, review or comment on this WBA Documentation.

If you are not the intended recipient (or have received this WBA Documentation in error), please notify the sender and WBA (pmo@wballiance.com) immediately and delete this WBA Documentation. Any unauthorized copying, disclosure, use or distribution of this WBA Documentation is strictly forbidden.

Table of Contents

1. Executive Summary

As Wi-Fi networks mature, it has become increasingly important to identify the location of access points. Location information is required for many functions, including network management, troubleshooting, security, enabling location services such as navigation and meeting regulatory obligations.

This white paper explores scenarios involving Wi-Fi roaming, where an Identity Provider (IdP), providing identity and authentication services remote from the Access Network Provider (ANP), can benefit from knowledge of the location of an End-User who is authenticating at the ANP's network, using the IdP's credentials. As Wi-Fi becomes a part of multi-technology networks, ever-more complex financial settlement arrangements and mission-critical applications, location reporting will become an essential function.

This paper has three objectives:

- Identify use-cases where it is important to communicate the location of End-Users or ANP APs to the IdP.
- Identify current standards that apply to a solution, and any gaps where further guidelines or standards work may be necessary.
- Raise awareness in the industry of this need and provide a starting point for addressing the need for both manufacturers and IdPs.

The recommendations at the end of this white paper will ensure that location reports are comprehensive and consistent across the industry.

2. Introduction

For cellular Operator IdPs, AP location information is vital for planning where Wi-Fi roaming should occur when weighed against available cellular connectivity, which may be preferred for reasons of cost, quality or consistency. Offload to Wi-Fi may occur at venues where the Operator has no prior knowledge of the ANP's network configuration, hence the importance of identifying where users are connecting.

Also, regulatory obligations may require the IdP is informed of the country where the ANP's network is located. And in some scenarios, the taxable rates associated with financial settlement arrangements may relate to the location where service is being consumed.

Non-cellular IdPs also require detailed AP location information to evaluate bandwidth requirements, usage patterns and areas where Wi-Fi connectivity is advantageous. Identifying the location where an End-User is authenticating will give these IdPs greater control over where to focus their Wi-Fi roaming investments.

This paper focuses on transmitting AP location from the ANP to the IdP, in the northbound direction from the AP. Because of the limited coverage range of a Wi-Fi AP, the location of the AP can be

considered equivalent to the location of the End-User and signalled by the ANP to the IdP as part of the authentication exchange.

While there are many use-cases where the device can learn its location from the AP, techniques already exist and are commercially available, implemented in the device itself. For this reason, location information transmitted southbound from the AP to associated devices is not covered.

This project is based on the following assumptions:

- The ANP uses RADIUS authentication with the IdP.
- The IdP either includes an AAA (RADIUS) server in its architecture or has the means to recover location information sent to the AAA server.

This paper continues by introducing use-cases that explain the need for signalling location information to the IdP. It then explores the state of the art in WLAN implementations, including configuration and automated discovery of AP locations in both geo-location (latitude-longitude) and civic (street) address formats. A technical discussion of different methods of signalling to the IdP follows, covering an out-of-band technique standardized in WBA WRIX-L (Leonidas, 2020), and a RADIUS-based method using the format specified in IETF RFC 5580 (Tschofenig, 2009).

Finally, the paper lays out recommendations for how ANPs should signal AP locations to IdPs in Wi-Fi Roaming scenarios, including WBA OpenRoaming.

3. Use-cases requiring location signalling

3.1 Network selection (Wi-Fi or cellular) based on AP location

Figure 1: Network selection

An ANP is located in an area where the IdP also manages a cellular network. In this scenario, the IdP's devices (those using the IdP's subscription or SIM card) may, due to device OS or other choices, attempt to connect to Wi-Fi where the IdP would prefer to keep them on the cellular network. For example, the IdP may have built-out 5G mmWave service and would want to maximize use of the 5G mmWave service by limiting offload to Wi-Fi in that geographic area.

A user enters an airport which has Wi-Fi managed by an ANP and cellular coverage provided by the IdP. Gates 1 and 3 are covered by 5G mmWave while other gates are covered by 5G mid-band and 4G service. The IdP prefers to run the user's traffic on 5G mmWave where available but use a Wi-Fi offload strategy in other areas.

Since the offload decision is taken within a building, the prior solution of using Network Access Server Identifier (NAS ID) is not sufficiently granular: a NAS ID will cover the whole building. The IdP needs to know the End-User's location more accurately to decide whether to authorize Wi-Fi access.

The solution is to signal the location of each AP, passing it to the IdP over RADIUS during authentication. This allows the IdP to compare the APs location with its 5G mmWave cell coverage and determine whether this is a location where Wi-Fi offload or cellular service is preferred, Gate 1 or Gate 3 in this example. If the latter, the authentication request can be rejected, and the End-User will stay on the IdP's cellular network.

The solution as described above has known imperfections. For instance, if the End-User authenticates on Wi-Fi, then moves into an area with more robust 5G mmWave coverage without disconnecting, the connection will continue over Wi-Fi. In order to keep the solution relatively simplistic, the IdP should accept this sort of leakage. Assuming an 80/20 rule, the simplistic solution should account for 80% of the desired goal without incurring the cost of complexity required to pick up the other 20%.

This use-case may also be applicable for a private network which runs multiple access technologies.

3.2 Connected vehicle fleet

A delivery company uses Wi-Fi offload to extend the network connection capabilities of its fleet. Offload to Wi-Fi saves costs and improves data transfer rates. The information which is regularly uploaded to the company contains delivery information and vehicle telemetry which is used for customer updates and internal analysis.

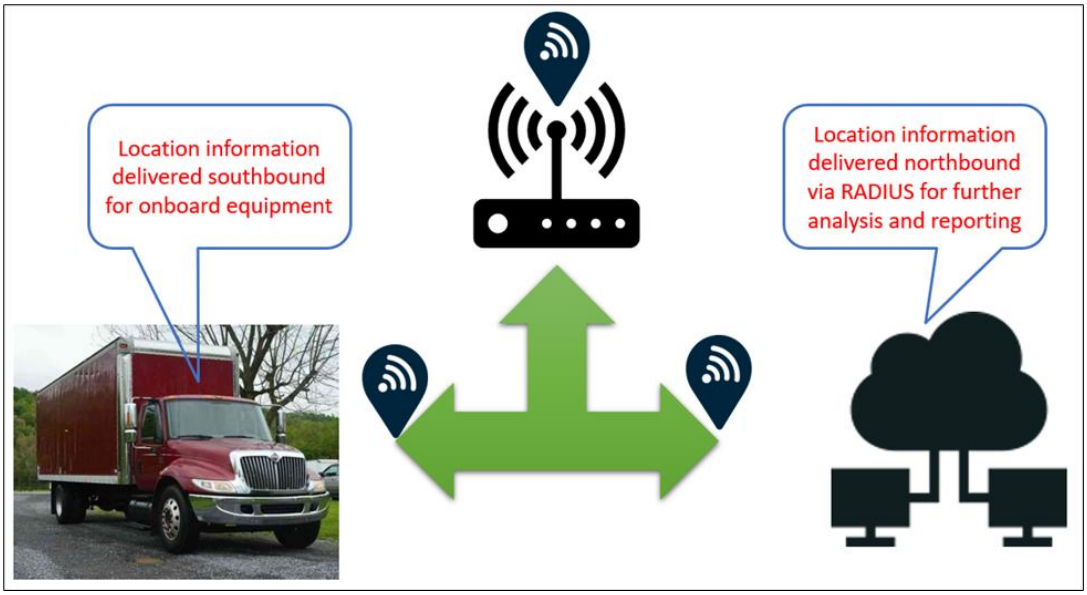

Figure 2: Connected Vehicle Fleet

Since the trucks follow a consistent route, the company can map locations where Wi-Fi coverage is preferred to cellular or other connectivity. This allows for better management of network costs and enables tracking of the fleet's performance day-to-day. Delivery of information from Wi-Fi ANP networks will be merged with cellular network information for a complete view of the fleet's activity.

To accomplish company objectives regarding delivery behaviours, precise location information is required.

3.3 Roaming Hub Policy

In WBA OpenRoaming and other roaming federation scenarios, Roaming Hubs receive RADIUS authentication requests on behalf of the IdP from ANP networks, using Dynamic Discovery as there is no bilateral contract between the ANP and IdP in OpenRoaming. The Roaming Hub manages incoming authentication requests over RADIUS based on the IdP's guidelines, as the IdP may not need offload support in certain areas, preferring to keep their End-User on another network.

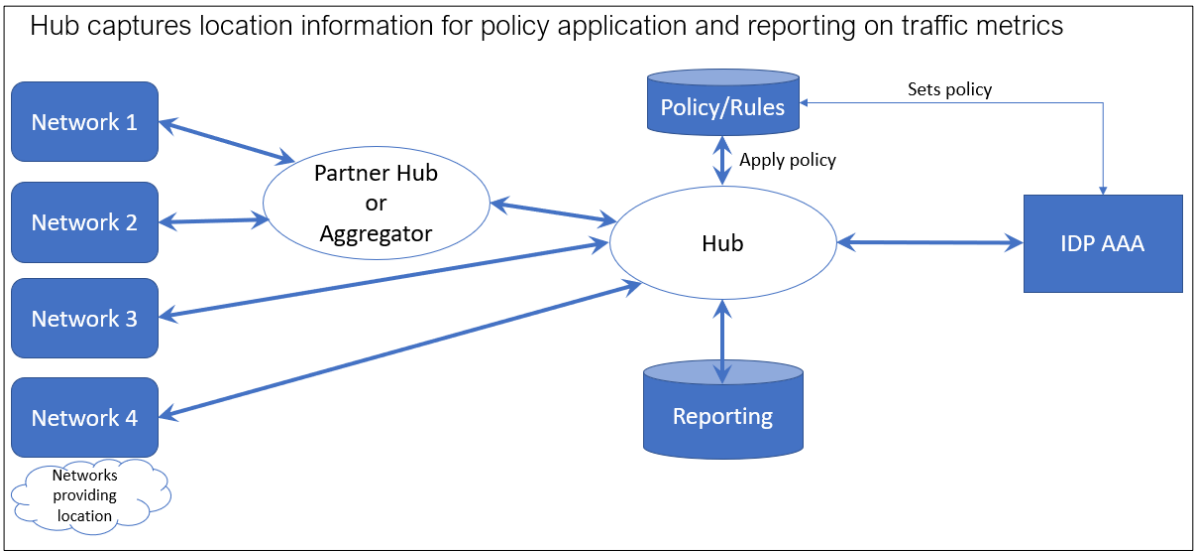

Figure 3: Roaming Hub Policy Enforcement using location information

A Roaming Hub acting on behalf of the IdP provides the initial screening of authentication requests, applying policy for the IdP based on pre-established rules by either forwarding the authentication request to the IdP, or rejecting it. This screening function requires the authentication request to contain sufficient information to determine the user's location. Roaming Hub metrics and reports for their IdPs will include connections accepted and rejected, per-location.

3.4 Emergency call support for Mobile Virtual Network Operators

When a device is connected to Wi-Fi and not the cellular network, access network-based techniques that Mobile Network Operators (MNOs) use for locating the caller are unavailable. However, location information is vital to routing the emergency call the the correct dispatcher location and providing a location to vector first responders.

Several partial solutions exist for providing these location inputs, including on-device location methods such as GPS. Providing location to the IdP may enable use-cases that close some of the gaps, such as indoors when GPS is not available; generally, the location of the AP where a user last authenticated is sufficiently accurate for emergency purposes. One possible architecture is for a call manager function, when identifying an emergency call, to query the IdP's AAA server for the location of the AP where the user authenticated, and to utilize this information when routing the call and appending the user's location.

The WBA has received a proposed ToR for a 2024 project "Mission Critical and Emergency (MCE)". The project deliverable will be a document whose scope spans OpenRoaming and WRIX to describe:

- *the opportunity to use Wi-Fi to support mission critical and emergency services*
- *to review individual regional/nationwide efforts*

- *describe latest 80211be functionality*
- *scope out new requirements for mission critical and emergency service support over Wi-Fi networks*
- *outline a plan to address new requirements within WBA's technical and legal frameworks.*
- *Liaise with RWG, T&I, Policy and OR Working Groups to drive such requirements into separate programs.*

3.5 Emergency calling using the OpenRoaming architecture

A recent IETF Draft (Gundavelli, 2023) proposes using the WBA OpenRoaming architecture to facilitate emergency calling over non-cellular networks.

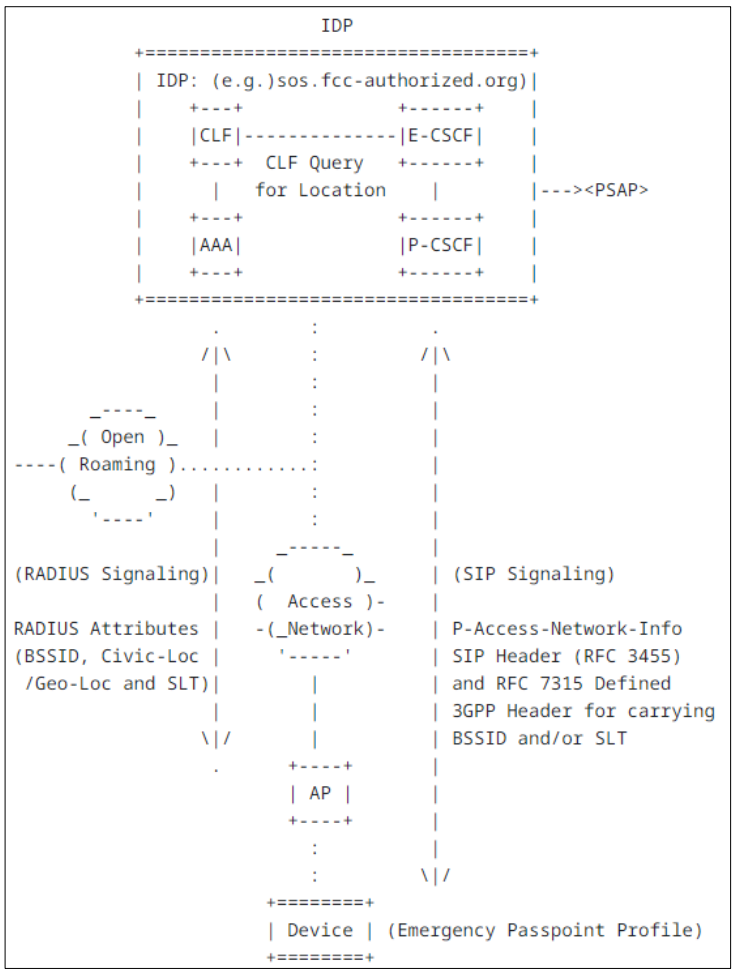

Figure 4: Proposed architecture for supporting 911 services using OpenRoaming

The abstract for this Internet Draft reads:

This document introduces an approach to enable emergency services over Wi-Fi access networks. These services encompass emergency services such as 911 in North America, 112 in the European Union, and equivalent emergency services in other regulatory domains. The proposed approach aims to provide a comprehensive solution for supporting emergency communication across different regions and regulatory frameworks.

Leveraging the legal framework and infrastructure of the OpenRoaming federation, this proposal aims to extend emergency calling capabilities to the vast number of OpenRoaming Wi-Fi hotspots that have already been deployed.

The approach addresses critical challenges related to emergency calling, including discovery and authentication procedures for accessing networks that support emergency services, emergency access credentials, the configuration of emergency voice services, accurate location determination of the emergency caller, and call spoofing.

By providing a comprehensive solution, this proposal ensures that emergency communication services can be seamlessly and effectively supported within the IEEE 802.11-based Wi-Fi ecosystem leveraging Passpoint Profiles.

This architecture would benefit from the option to use AP location information at the IdP, where available.

4. WLAN techniques for determining AP location

WLAN vendors have been incorporating geo-spatial awareness into their products for many years. Uses include network management, troubleshooting, RF management and security.

Initial designs focused on network managers uploading scaled floorplans for their buildings, and creating an overlay of AP locations, usually by drag-and-drop of AP icons to the correct location on the floorplan. This allowed visual identification of AP locations, and End-Users were often mapped to a different layer of the same view in order to facilitate network management functions.

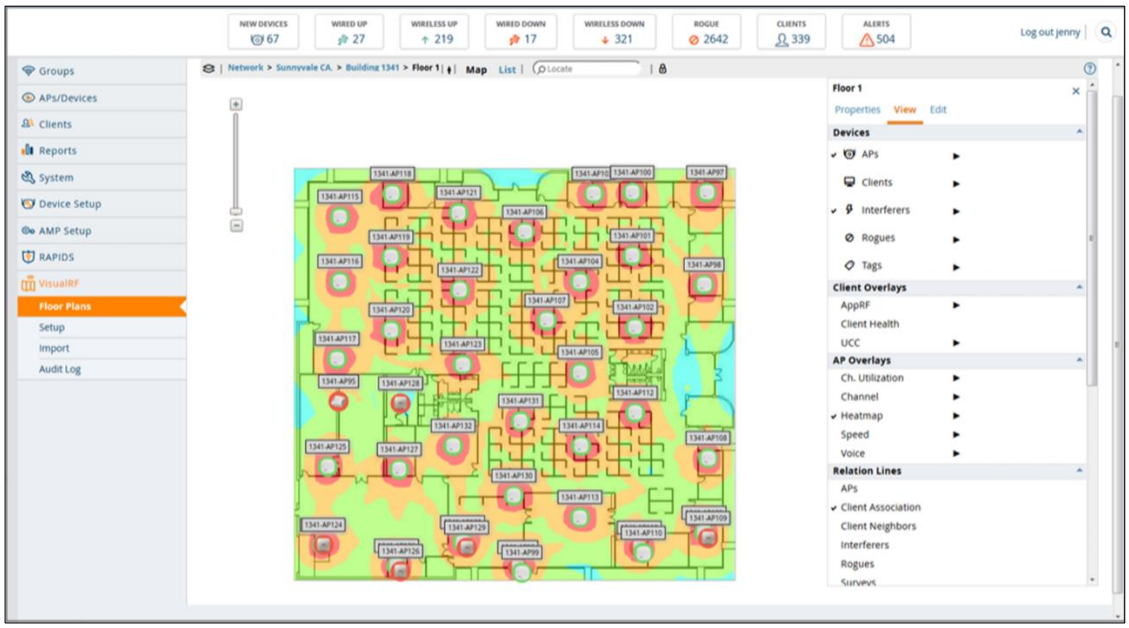

Figure 5: AP Locations overlaid on an uploaded floorplan diagram

As horizons expanded beyond individual floors, many vendors added the capability to configure a civic (street) address for a building, and more recently geo-location (latitude-longitude). With a civic address, an address tag is added to the building object in the database, linking each AP with a building address and sometimes the floor of the building. For geo-location, the usual method is to identify two or more anchor points per floorplan with latitude and longitude, allowing calculation of the geo-location of all APs placed over that view.

While AP location in civic address or geo-location coordinates may be available in a WLAN management system, additional software work may be required to make this information available to a RADIUS connection.

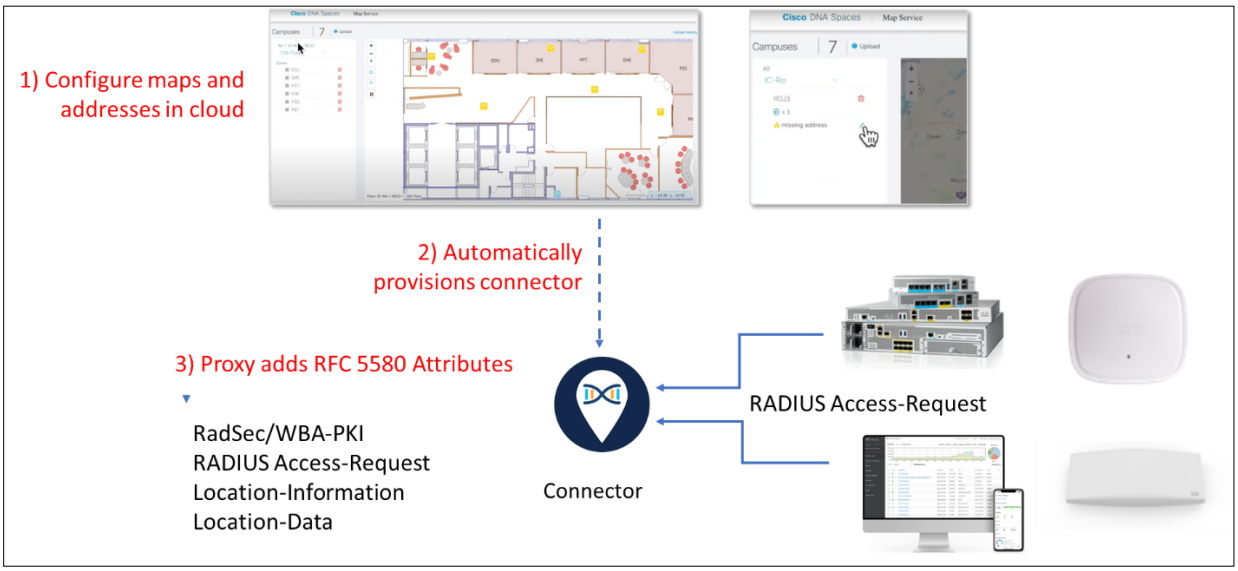

Figure 6: Architecture for adding Civic Address in RFC 5580 format to RADIUS Access-Requests

However, it is well-known that manual processes are error-prone: floorplans can be mis-labelled, APs dragged to the wrong location and geo-locations mis-typed. Automated methods are preferred.

A stimulus for AP self-location arrived recently when national regulators opened the 6 GHz band to Wi-Fi (Wi-Fi 6E). While jurisdictions differ, and many regulators have not finalized their rules, the US Federal Communications Commission (FCC) is typical. The FCC allows unrestricted indoor operation in 6 GHz up to a certain transmit power level, one that is adequate for enterprise, small business, and residential use. However, 'Standard Power' operation, outdoors or with higher power indoors, poses potential interference to incumbent users of the 6 GHz band, mostly point-to-point fixed microwave links. In order to protect these users, the FCC mandates that Standard Power APs must query a frequency allocation server and provide their location; the server will calculate which 6 GHz channels and transmit power levels will not cause interference, and return that list to the AP.

Since the incumbent links use high-gain antennas, interference is very sensitive to AP location, and the FCC mandates that the AP must identify its location by automatic means, to a high level of accuracy. In practice this means the location must be derived from GPS.

Although Standard Power APs may comprise less than 10% of the 6 GHz WLAN market, vendors are beginning to incorporate GPS receivers into some or all of their 6 GHz capable APs, and to develop software to make use of this location, in latitude-longitude form. Some have gone further and used GPS (which, indoors, is useful only near windows, where APs have a view of the sky and can receive satellite signals) in conjunction with AP-to-AP ranging information, derived using methods such as the Wi-Fi Alliance's Location certification, based on Fine Timing Measurement (FTM). This offers a path to fully automatic determination of AP locations to a high level of accuracy.

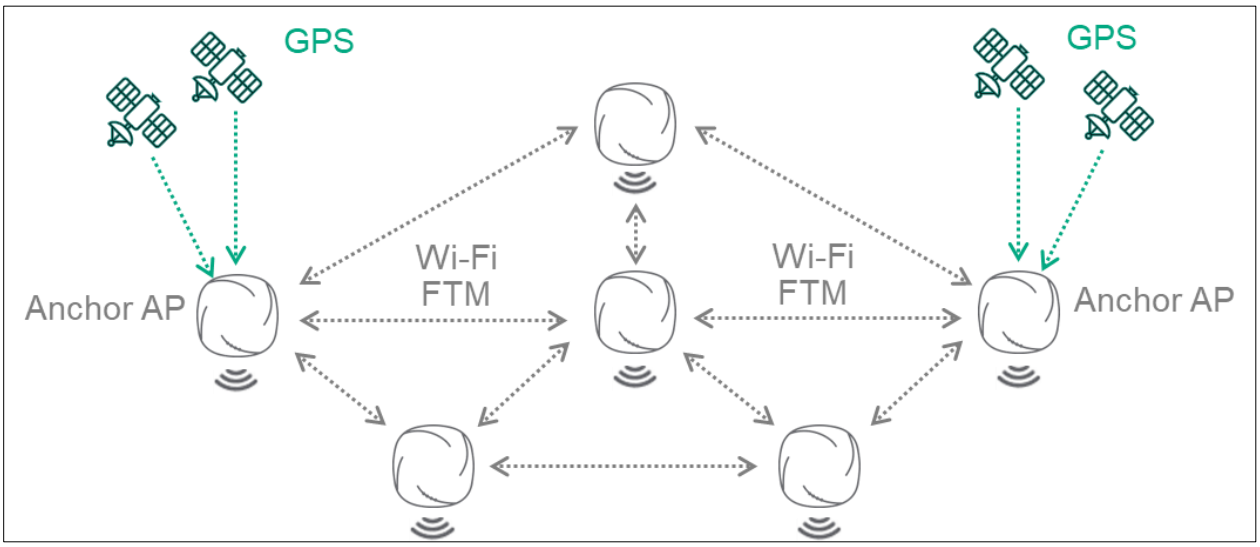

Figure 7: Architecture for automatically locating APs using GPS and Wi-Fi Location

Other methods for locating APs include crowdsourcing, where a device that can locate itself using other methods such as GPS or Bluetooth is able to identify when it is close to an AP and hence tag that AP with a valid location.

5. Techniques for signalling location information

The WBA supports two methods for the IdP to learn the location of APs: WRIX-L file transmission, and RFC 5580 in RADIUS both enable the use-cases listed earlier in this paper.

5.1 WRIX-L out-of-band signalling

WRIX-L is a long-standing WBA Roaming standard that defines a format for ANPs to inform IdPs of the location of individual APs in their networks.

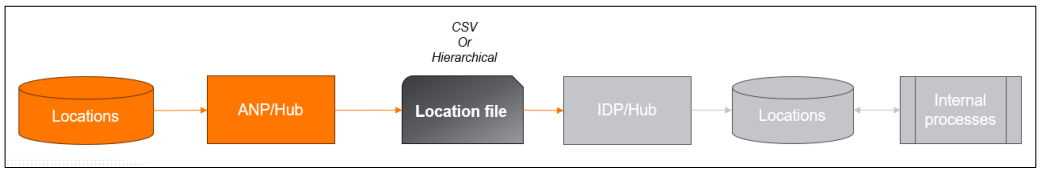

Figure 8: WRIX-L Location File Transmission Procedure

The ANP provides regular updates of location information to its IdP partner or the IdP's Roaming Hub provider. Each WRIX-L file is a complete replacement for any previous files. The schedule for sending updated WRIX-L files is determined by agreement between the IdP and ANP.

The WRIX-L location file can be used to supplement RADIUS information, or even to limit the amount of information (e.g., RFC 5580) passed in RADIUS, as the 'Called-Station' in a RADIUS 'Access-Request' is a Wi-Fi AP BSSID and can be used as a key for the AP location information in WRIX-L.

mandatory values	optional values	
Provider_Identifier	Sub_Venue	Coverage_Area
Location_Identifier	Location_Address2	Open_Monday
Service_Provider_Brand	Location_State_Province_Name	Open_Tuesday
Venue_Description	Location_Phone_Number	Open_Wednesday
English_Location_Name	SSID_Broadcasted	Open_Thursday
Location_Address1	WEP_Key	Open_Friday
English_Location_City	WEP_Key_Entry_Method	Open_Saturday
Location_Zip_Postal_Code	WEP_Key_Size	Open_Sunday
Location_Country_Name	SSID_Secure	UTC_Timezone
SSID_Open_Auth	SSID_1x_Broadcasted	Billing_Attribute
Longitude	Security_Protocol_1X	Billing_ID
Latitude	Client_Support	Radio_Frequency
MAC_Address	Restricted_Access	
Lat_Lng_Quality	Location_URL	
Venue_Group		
Venue_Type		
Location_Floor		
Location_Suite		

Figure 9: Fields Available in WRIX-L

To use WRIX-L, the ANP compiles a list of APs with location information, in CSV or XML/JSON format. This is transmitted to the IdP or Roaming Hub partner as an email attachment, or by some other 'out-of-band' method.

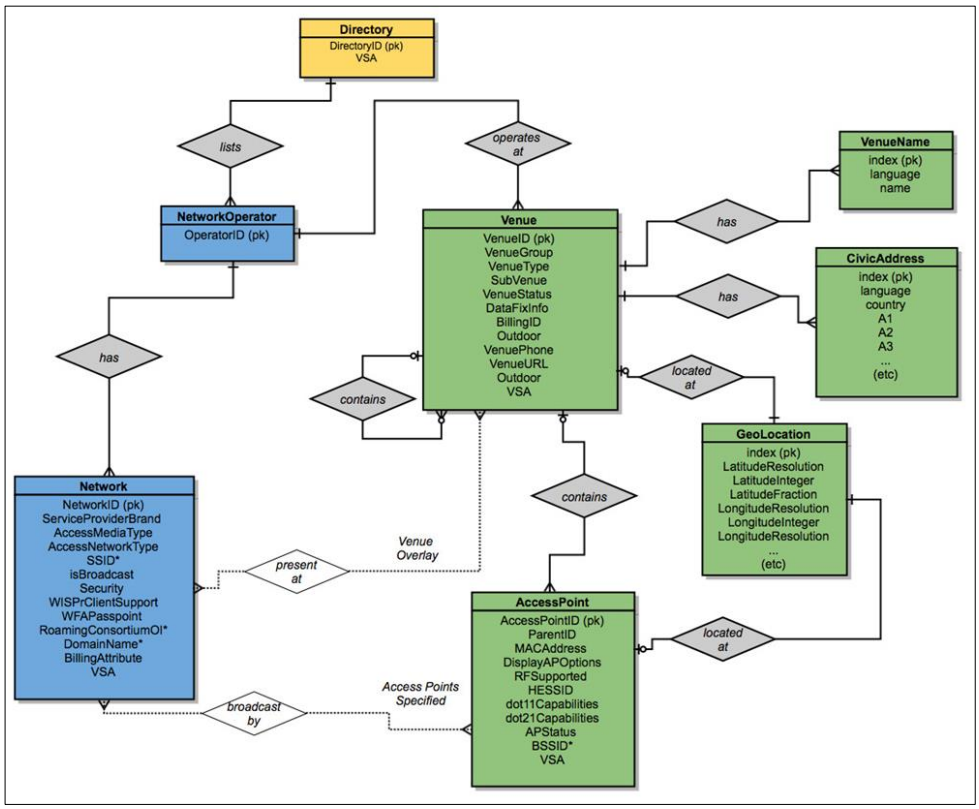

Figure 10: WRIX-L Hierarchical format used for XML/JSON

Because this method uses manual processing, is prone to errors and omissions, and the information may become stale due to infrequent updates, it is generally not preferred. But it may be a solution where, for example, other methods are not supported by the ANP WLAN equipment. The requirement for a further lookup at the AAA may make it difficult to support real-time authentication decisions need for some of the use-cases above.

5.2 RADIUS (in-band) signalling using RFC 5580

RFC 5580 – "Carrying Location Objects in RADIUS and Diameter" - has been adopted by the WBA as the best method for conveying location information for roaming and offload scenarios utilizing Passpoint networks. Other solutions defined previously such as the use of the WISPr location VSA do not provide the flexibility and control of the RADIUS AVPs described in RFC 5580. As a result, for specific use-cases, the WBA mandates the use of certain RFC 5580 attributes in the WRIX Framework.

The Attributes below are mandatory for supporting WRIX-based Passpoint authentication.

Attribute	Description
126	Operator-Name

127	Location-Info
128	Location-Data
131	Location-Capable

All ANPs supporting WRIX-based Passpoint authentication must ensure that the Access-Request message received by the IdP includes RFC 5580 defined location attributes. The ANP may agree with their Roaming Hub provider that the Hub is responsible for including the RFC 5580 attributes.

The Operator-Name attribute (#126) contains the WBAID (or WBA subID) of the ANP.

The Location-Info attribute (#127) indicates the type of location data provided in the Location-Data attribute (#128): either civic address (value 0) or geo-location (value 1).

If the Location-Data (#128) attribute contains a civic address, it must include the country code where the ANP is located.

When supporting OpenRoaming Settled-Service, the Location-Data attribute (#128) must be included, where the location profile is the civic address profile containing Civic Address Type information. The civic address must be sufficient to identify the financial regulatory regime that defines the taxable rates associated with consumption of the ANP's service.

WRIX specifies that the ANP may optionally include additional RFC 5580 defined Location-Information and Location-Data attributes to signal a geo-location profile corresponding to the location at which service is provided. This paper recommends the use of RFC 5580 for the most precise view of where the AP is located and the service is provided.

5.3 Use of Civic Address or Geo-Location

Most location formats, including WRIX-L and RFC 5580, provide two alternatives: geo-location (latitude-longitude), and civic (street) address.

Geo-location is universal across countries, relies on only a few values, is easily obtained from GPS and has an arbitrary level of accuracy.

Geo-Location Elements
Latitude
Longitude
Floor number or elevation above ground level or sea level

RFC 3825 provides the format for conveying geo-location that is used in the RADIUS attributes defined in RFC 5580. The Datum field should be set to 1, designating that the spatial reference system used is

WGS84. The LaRes and LoRes fields should be '22' or higher, to convey a meaningful resolution of the geo-location data. Both fields set to '22' would describe a geo-location area that is approximately 143 square meters (10.5m x 13.6m).

Meanwhile, a civic address has many possible parameters, different formats following national street-addressing schemes, and generally requires manual data entry, introducing potential errors. At a minimum, the WBA considers the following attributes are necessary to uniquely identify a building address (note that this does not identify the location of APs within the building). Where the definition of Zipcode/Postcode supports different resolutions, it is recommended that the highest resolution is signalled, e.g., in the US the signalling of a 9-digit ZIP code in CA Type 24 is recommended, where the additional 4 digits are used to encode street and building information.

CA Type	Description	Notes
19	House Number	If Zipcode / Postcode is insufficient to identify a road/building, include this CA Type.
24	Zipcode / Postcode	
35	Primary Road Name	If Zipcode / Postcode is insufficient to identify a road/building, include this CA Type.

Figure 11: Commonly-used Civic Address attributes

In addition to geo-location and civic address, some IdPs have expressed interest in what3words as a means of identifying location. From what3words.com :

what3words has divided the entire world into 3m squares and given each square a unique identifier made from three words. The words are distributed by a mathematical algorithm; they are fixed and will never change. what3words addresses are accurate to 3m x 3m, enabling them to specify a precise entrance, unlike a street address which identifies an entire building.

We chose 3 metres x 3 metres as it is small enough to be useful for labelling specific areas, such as a water point or a front gate, but not so small that we run out of words to label all the squares or have the squares so small that they become too specific for locations such as houses.

Example:	New York City Hall	(lat 40.71371, long -74.00618)	clip.apples.leap
	Sydney Opera House	(lat -33.85729, long 151.21524)	faced.help.frock

If adoption of what3words continues to grow, the WBA should consider how to add encoding options for WRIX-L and RFC5580.

6. Policy and Privacy Issues

The transmission of AP location, as described in this paper, allows accurate identification of an End-User's location at a moment in time, and transmission of that location to the IdP. To preserve user privacy,

location information must be protected against unauthorized access and distribution. Requirements for access to location information are defined in RFC 3693 (Cuellar, 2004). In addition, the IdP's Terms and Conditions should explain that the IdP is able to track the user, in order to obtain prior consent.

Where there is no a priori agreement on handling of location information, the location-capable attribute (#131) is used in the initial Access-Request message to signal to an IdP that a NAS is location capable. The IdP can then use the Requested-Location-Info attribute (#132) to request the necessary location information be returned by the NAS. In other scenarios, where there is an out-of-band agreement, e.g., based on the OpenRoaming legal framework, the required location information can automatically be included in the initial Access-Request message.

Data protection regulations, e.g., the EU's General Data Protection Regulation (GPDR) (European Union, 2016), typically include rules that govern location data. Under the GDPR, location data is considered to be any information collected by a network or service about where an individual's device is or was located, including the latitude, longitude or altitude of the device and the time the location information was recorded. Businesses can also only process location data with the authority of the network or service provider if it is anonymous or if consent is obtained from the user.

Where there is no out-of-band agreement, RFC 5580 defines the use of the Basic-Location-Policy-Rules attribute (#129) to enable an ANP to signal an IdP the rules that control the distribution of location information, enabling an ANP to indicate that the recipient of the location information is not permitted to share the location information with other parties. However, as described above, the processing of location information requires explicit consent. The preferred approach is for this consent to be agreed between the End-User and their IdP, e.g., when the End-User was provisioned with their Wi-Fi credentials. Such an approach ensures the user has consented to the correct processing by their IdP.

The OpenRoaming legal framework (Wireless Broadband Alliance, 2023) includes default privacy terms that can be used by IdPs that do not want to define their own End-User terms concerning provision of the Wi-Fi service. This privacy policy is being augmented to include terms that govern the baseline handling of the End-User's location. For example, terms are defined covering collection of location data, use of location data, and disclosure of location data.

7. Summary, Recommendations and Conclusion

7.1 Summary

This paper identifies the need for better and more timely AP location information to be provided to IdPs for management, financial and safety scenarios related to Wi-Fi roaming. It is intended to provide guidance to the industry and impetus for adoption, while acknowledging that many have already started to include the required elements in standards, roadmaps and even some product implementations.

The recommendations below are drawn from the expertise of a variety of sources and industry experts concerning how location information is currently collected and used in Wi-Fi roaming.

The paper isolates a small number of important use-cases which serve critical business needs but are not met by current industry deployments. These use-cases require more precise and timely location information than is commonly available today. Following a discussion of use-cases, the paper examines how an ANP's AP can find its current location, and how that location can be communicated upstream to the IdP. Applicable standards and current industry practices are reviewed and, finally, recommendations are provided on how these standards may be implemented within the industry to meet the identified use-cases and similar, emerging needs.

7.2 Recommendations

In order to support the use-cases listed in this paper, the WBA recommends that ANPs should signal AP location information to IdPs. The following methods are preferred, in descending order:

- RFC 5580 in RADIUS Access-Request messages, using geo-location in accordance with the guidelines in this document.
- Where geo-location is not available, RFC 5580 in RADIUS Access-Request messages, using civic address.
- WRIX-L out-of-band file transmission with geo-location. This is not as timely as location information provided through RADIUS and thus may not be suitable for some use-cases.
- WRIX-L with civic addresses is allowed, but not preferred. Where civic addresses are used, they should be highly granular, as defined in this paper.

7.3 Conclusion

The Wi-Fi industry continues to evolve and assume progressively more critical roles. Once considered a "best-effort" technology, Wi-Fi is increasingly used for essential communication, and with this evolution, the need for timely and accurate AP location information has emerged. This paper crystallizes this emerging need by identifying essential use-cases and providing concrete recommendations to aid and accelerate industry adoption of Signalling Location in RADIUS.

8. References

Cuellar, J. e. (2004). *IETF RFC 3693.* Retrieved from https://datatracker.ietf.org/doc/html/rfc3693.

European Union. (2016). *Regulation (EU) 2016/679.* Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504.

Gundavelli, S. (2023, March). *Emergency 911 Services over Wi-Fi, draft-gundavelli-dispatch-e911-wifi-00.txt.* Retrieved from IETF: https://datatracker.ietf.org/doc/draft-gundavelli-dispatch-e911-wifi/

Leonidas, M. (2020, March). *WRIX-L Location Data Exchange.* Retrieved from WBA: https://extranet.wballiance.com/higherlogic/ws/groups/a38e65b5-cb30-4087-b6b7-7fcc3fe08604/documents/wrix1181/document?document_id=18068

Tschofenig, H. e. (2009, August). *Carrying Location Objects in RADIUS and Diameter.* Retrieved from IETF: https://datatracker.ietf.org/doc/rfc5580/

Wireless Broadband Alliance. (2023). *OpenRoaming End-User Privacy Policy*. Retrieved from https://wballiance.com/openroaming/privacy-policy/

9. Appendix A: Useful Civic Address Types

CA Type	Description
1	State
2	County
3	City
4	City Division
5	Block
6	Group of Streets
16	Street Direction
17	Street Suffix
18	Street
19	House Number
20	House Number Suffix

21	Vanity Address
22	Additional Information
23	Name
24	Zipcode / Postcode
26	Unit
27	Floor
28	Room
33	Seat

10. Appendix B: Example of Civic Address in RADIUS

```
RADIUS Protocol
  Code: Access-Request (1)
  Attribute Value Pairs
  > AVP: t=Operator-Name(126), val="414638.DNASPACES.CISCO:US",
  > AVP: t=Location-Information(127), val=0x00030000e7bc12367b22d0e5e7bc193e7b22d0e54d616e75616c
  > AVP: t=Location-Data(128),
val=0x0003494e010e416e6468726120507261646573680309426 56e67756c757275180635363030363 8

Location-Information: 00030000e7bc12367b22d0e5e7bc193e7b22d0e54d616e75616c
  > Index: 0003
  > Code: 00 (Civic)
  > Entity: 00 (client device)
  > Sighting-Time: 2023-03-15 09:45:26
  > Time-to-Live: 2023-03-15 10:15:26
  > Method: "Manual"
Location-Data: 0003494e010e416e6468726120507261646573680309426 56e67756c75727518063536303036 3
  > Index: 0003
  > Country: "IN"
  > CAType: 01 (State)
    CAValue: "Andhra Pradesh"
  > CAType: 03 (City)
    CAValue: "Benguluru"
  > CAType: 24 (Postal)
    CAvalue: "560068"
```

11. Appendix C: Example of Geospatial Address in RADIUS

```
RADIUS Protocol
  Code: Access-Request (1)
  Attribute Value Pairs
  > AVP: t=Operator-Name(126), val="414638.DNASPACES.CISCO:US",
  > AVP: t=Location-Information(127), val=  0x00020101e832f1647ea44321e832f3bc7ea453e84d616e75616c

  > AVP: t=Location-Data(128), val=  0x00025867095fed57fe7de15d278000000001


Location-Information: 00020101e832f1647ea44321e832f3bc7ea453e84d616e75616c
  > Index: 0002
  > Code: 01 (Geospatial)
  > Entity: 01 (NAS)
  > Sighting-Time: 2023-06-13 13:45:08
  > Time-to-Live: 2023-06-13 13:55:08
  > Method: "Manual"
Location-Data: 00025867095fed57fe7de15d278000000001
  > Index: 0002
  > Latitude: 51.5181884765625
  > Longitude: -0.75390625
  > Altitude: 0.0 Floors
  > Datum: WGS84
```

12. Appendix D: Extracts from OpenRoaming Terms & Conditions

1. **Collection of Location Data**

a. In order to provide the Service, each OR Participant operating as an IDP may collect location data related to the ANP's wireless network used by an OpenRoaming End-User.

b. Location data includes the country in which the ANP's wireless network is located and may include the civic address of the wireless access network and/or the geospatial co-ordinates of the ANP's wireless access network.

2. **Use of Location Data**

a. OpenRoaming Participants process location data for certain legitimate business purposes, enabling you to seamlessly log onto participating provider's wireless networks.

b. An OR Participant operating as an IDP that does not separately get agreement from you to its own separate privacy policy, will solely process collected location data for the purposes of:

   i. Making service authorization decisions based on the location of the ANP's wireless network;

   ii. Compliance with applicable law (whether in your jurisdiction or the jurisdiction in which you are accessing the Service) ("**Applicable Law**") or law enforcement requests;

   iii. Sharing location data with the emergency services (if you make an emergency call while connected to an OpenRoaming ANP);

3. **Disclosure of Location Data**

a. Except when complying with law enforcement requests pursuant to clause 2 above, each OR Participant operating as an IDP is prohibited from selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating any location data received as part of its participation in OpenRoaming with any third party.

b. If OR Participant operating as an IDP desires to process or use End User location data in ways not outlined in clause 2-b above, OR Participant shall be required to separately obtain consent from the End User, including stating its requested purpose of use for the location data, and otherwise agrees to treat such location data in accordance with the OR Participant's privacy policy or statement.

c. Notwithstanding the restrictions on disclosure of location data, OR Participant may share aggregated anonymized location data regarding the operation of the Service with WBA.

13. Contributors

Name	Company	Role
Jim Sturges	AT&T	Project Leader
Betty Cockrell	SingleDigits	Project Co-Leader
Peter Thornycroft	HPE Aruba Networking	Chief Editor
Bart Brinckman	Cisco	Editorial Team
Mark Grayson	Cisco	Editorial Team
Sri Gundavelli	Cisco	Editorial Team
Blaz Vavpetic	Galgus	Editorial Team
Roy Want	Google	Editorial Team
Stuart Strickland	HPE Aruba Networking	Editorial Team
Jonathan Segev	Intel	Editorial Team
Michael Sym	Single Digits	Editorial Team
Erinn Hall	AT&T	Project Participant
Rommel Novo	AT&T	Project Participant
Jessie Manik	Bell Mobility	Project Participant
Blair Bullock	Boldyn	Project Participant
Luther Smith	CableLabs	Project Participant
Angelos Mavridis	Deutsche Telekom	Project Participant
Natalia Ermakova	ER-Telecom	Project Participant
Charlie Allgrove	GlobalReach	Project Participant
Mathew George	HPE Aruba Networking	Project Participant
Danny Jump	HPE Aruba Networking	Project Participant
Necati Canpolat	Intel	Project Participant
Edward Wincott	JISC	Project Participant
Ryan Blossom	Single Digits	Project Participant
Yvette Medina	Single Digits	Project Participant
Pedro Mouta	WBA	Project Participant
Bruno Tomás	WBA	Project Participant