Accelerating Wi-Fi Offload – Strategies for Solving Roaming Interworking Challenges
Executive Summary

The explosion of mobile data traffic is driving the viability of Wi-Fi networks as a way to improve coverage and capacity for mobile carriers. This is opening new opportunities for not only pure-play Wi-Fi providers, but also Mobile Network Operators (MNOs) implementing complementary Wi-Fi networks as a means to expand coverage, lower the cost per delivered bit [1], and ease congestion on strained spectrum and backhaul resources. Wi-Fi operators want to provide a seamless user experience for their customers across a broader range of home and visited hotspots and better monetize their network investment through roaming agreements with other wireless operators and MNOs. This is also creating opportunities for Wi-Fi roaming hub operators that want to provide value to the ecosystem by enabling multilateral connectivity between multiple Wi-Fi network operators. In this white paper we’ll explore how operators can leverage interworking solutions to address the challenges they face when it comes to delivering services across diverse network technologies.
Table of Contents

Roaming Strategies ................................................................. 4
GSMA and WBA Alignment ......................................................... 6
Interworking Is Fundamental in Roaming Architectures ................. 6
Message Flows for Roaming Authentication and Accounting .......... 7
Any-to-Any Services Interworking – The Key To Seamless Roaming, ........................................ 7
  Interworking RADIUS to facilitate Wi-Fi roaming...................... 8
  Centralized routing and interworking for 3GPP operators ............ 8
  Enhancing user experience while optimizing core traffic load ...... 9
  Interworking and enhancing policy and charging ...................... 10
Conclusions ........................................................................... 11
Bibliography ........................................................................... 11
Roaming Strategies

Roaming in mobile and wireless networks is the process by which customers can use the network of a “visited” network operator to access the services in their home network. Roaming is an important component to mobile data offload strategies that can help operators cost effectively increase footprint and provide users a seamless and improved quality of experience. As standards and technology evolve, operators are employing various approaches to provide their customers with a seamless experience as they move between mobile networks and Wi-Fi hotspots. While there are several ways to actually implement networks to support roaming, there are basically a couple of broad architectural options Wi-Fi operators have when it comes to interconnecting with other networks to enable customers to roam [2]. One is for Wi-Fi operators to connect directly with other operators and establish bilateral agreements to enable customers to roam. Alternatively, they can use the services of a third party hubbing provider - like an IPX - that has established a Wireless Roaming Intermediary eXchange (WRIX).

The Wireless Broadband Alliance (WBA) has established roaming guidelines to provide its member operators a reference for facilitating customer roaming. The benefits to Wi-Fi operators include better potential to monetize network investment through increased traffic and improved user experience by making roaming easier and seamless for customers in more places around the globe.

Wi-Fi operators, of course, can establish arrangements with each other on a one-to-one basis, but that approach does not scale or provide ubiquitous coverage. To help with the situation the WBA created the WRIX framework to facilitate roaming across different Wi-Fi technology implementations.

Figure 1. Roaming interconnection options for Wi-Fi networks can include direct connections between operators or the use of a third party intermediary.

The Wireless Broadband Alliance (WBA) has established roaming guidelines to provide its member operators a reference for facilitating customer roaming. The benefits to Wi-Fi operators include better potential to monetize network investment through increased traffic and improved user experience by making roaming easier and seamless for customers in more places around the globe.

Wi-Fi operators, of course, can establish arrangements with each other on a one-to-one basis, but that approach does not scale or provide ubiquitous coverage. To help with the situation the WBA created the WRIX framework to facilitate roaming across different Wi-Fi technology implementations.

Figure 2. The various WRIX modules (WRIX-i, WRIX-d, and WRIX-f) are broken down into specific interactions that occur between the visited network provider and the home service provider to facilitate seamless roaming. The interactions, protocols, and authentication mechanisms between the public connections and the private connections are defined in the WBA specifications for the various WRIX modules [3].
The WRIX is broken into three levels that cover the various interactions needed between operators to support roaming. The WRIX-i or interconnect specifies the interface between the visited network provider (VNP) and the home service provider (HSP). This specification outlines the proxy functionality and protocols used between the visited and home network. Part of the specification also includes defining the information in user data records that would be generated on a per session basis and passed up to the WRIX-d Data Clearing function for processing.

The WRIX specification also identifies the authentication methods that operators should support [7]. Some of the authentication methods specified are based on the Extensible Authentication Protocol or EAP. EAP-SIM and EAP-AKA are SIM (Subscriber Identity Module) based authentication methods that the WRIX specifications encourage operators to support. Within a GSM compatible handset or smartphone is a SIM card that contains information specific to the subscriber like the International Mobile Subscriber Identity (IMSI) and the device’s authentication key. Authentication methods in 3GPP networks utilize the SIM based IMSI information making them critical in facilitating seamless roaming for 3GPP-based customers. While not called out in the WRIX specifications, EAP-AKA’ is another SIM-based authentication method that can be used to access AAA resources in networks that have migrated to an Evolved Packet Core (EPC). Some devices like a laptop will not have a SIM card and will need to use an alternative authentication method such as EAP-TLS (Transport Layer Security) or EAP-TTLS (Tunneled Transport Layer Security) to gain access.

Wi-Fi operators have the flexibility to deploy WRIX functions on either an “in-source” basis or “out-source” basis and the tables below provides some information on the basic services supported by the various WRIX modules [3].

- **WRIX-i for RADIUS interaction**

<table>
<thead>
<tr>
<th>Visited Network Provider</th>
<th>Home Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Proxy routing of RADIUS messages to appropriate WRIX-i</td>
<td>Proxy routing of RADIUS messages</td>
</tr>
<tr>
<td>Collect RADIUS records</td>
<td>Collect RADIUS records</td>
</tr>
<tr>
<td>Send records to WRIX-d</td>
<td>Send records to WRIX-d</td>
</tr>
<tr>
<td>Dispute resolution support</td>
<td>Dispute resolution support</td>
</tr>
</tbody>
</table>

- **WRIX-d for data clearing or wholesale accounting**

<table>
<thead>
<tr>
<th>Visited Network Provider</th>
<th>Home Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive data records from WRIX-i</td>
<td>Receive data records from WRIX-d VSP</td>
</tr>
<tr>
<td>Rating based on IOT agreement and send to the WRIX-d HSP</td>
<td>Validate and reconcile records</td>
</tr>
<tr>
<td>Extract and send financial data to WRIX-f VNP module</td>
<td>Perform IOT check as required</td>
</tr>
<tr>
<td>Dispute resolution support</td>
<td>Dispute resolution support</td>
</tr>
</tbody>
</table>

- **WRIX-f for financial clearing or wholesale billing**

<table>
<thead>
<tr>
<th>Visited Network Provider</th>
<th>Home Service Provider</th>
</tr>
</thead>
<tbody>
<tr>
<td>Receive data records from WRIX-d</td>
<td>Receive data records from WRIX-d</td>
</tr>
<tr>
<td>Send financial data to WRIX-f (HSP)</td>
<td>Reconcile financial data with WRIX-f (VSP)</td>
</tr>
<tr>
<td>Reconciliation between operators</td>
<td>Receive invoices, administer settlements, and dispute resolution support</td>
</tr>
<tr>
<td>Invoicing, settlement and dispute resolution</td>
<td>Dispute resolution support</td>
</tr>
</tbody>
</table>

WRIX-i requires use of RADIUS authentication, authorization and accounting (AAA) procedures and some specific attributes associated with access and accounting services. The WRIX specifications provide a high degree of interoperability between Wi-Fi operators. However, real world implementations may still require RADIUS-to-RADIUS mediation and the need for interworking functionality with other signaling protocols as part of the overall solution to correct for incompatibilities between operator networks.
GSMA and WBA Alignment

The 3GPP has developed specifications for GSM operators on how Wi-Fi networks can integrate with 3G and 4G mobile networks. The GSMA and WBA are working together to harmonize efforts technically on Wi-Fi roaming and to make the integration of 3GPP mobile and Wi-Fi seamless and transparent to the end user [6]. Another initiative, Hotspot 2.0, led by the Wi-Fi Alliance is focusing on ways to help devices improve the detection and selection of Wi-Fi networks and reduce the traffic impact on core facilities.

The GSMA’s WLAN Roaming Guidelines [4] provide details of a technical solution for enabling roaming between Wi-Fi networks and 3GPP 3G and 4G networks. The GSMA roaming reference model consists of two sets of interfaces. One of the interfaces is between the mobile device and the Wi-Fi access network which provides functions like user authentication. The other set of interfaces (Wd/SWd) is between the visited Wi-Fi network and the home service provider network. The SWd and Wd interfaces use Diameter and RADIUS respectively to provide the underlying capabilities for interconnection between a 3G hotspot provider and a Wi-Fi operator.

Interworking Is Fundamental in Roaming Architectures

In order to accommodate roaming over a diverse set of user devices and network implementations, Wi-Fi and 3GPP network architectures will need to provide interworking between different protocols used for AAA as well as mediate between variations of the same protocol. The diagram below shows one such example where the HSP is a Wi-Fi operator and the roaming customer is using the network of a 3GPP-based VNP.

![Interworking Diagram](image)

In Figure 3, a customer with a Wi-Fi device would need to authenticate back to the HSP network. Authentication messages would be sent over the Wd or SWd interface between the 3GPP network’s AAA proxy and the Wi-Fi operator’s AAA server. For operators on a pre-Release 8 version of 3GPP specifications, it would be the Wd interface which uses RADIUS; for operators using 3GPP release 8 or higher it would use the specifications for the SWd interface which requires Diameter. There would be a need for interworking with the WRIX-i interface of the Wi-Fi operator in order for both of these scenarios to properly interwork.

Conversely, shown in Figure 4 is the situation where a customer in a 3GPP network wants to roam and use services from a Wi-Fi operator. The subscriber’s device would utilize SIM based authentication methods that would need to proxy through the Wi-Fi operator’s network. Authentication messages would go through the AAA proxy of the VSP over the WRIX-i interface and would require interworking with the Wd or SWd interface of the 3GPP operator.

![Interworking Diagram](image)
Interworking is also required in many cases in the 3GPP operator’s mobile core. In pre-release 8 3GPP networks, SS7/MAP is used for connecting the Home AAA server to the Home Location Register (HLR) to authenticate the user. A RADIUS to MAP gateway function is needed to interwork the RADIUS-based Home AAA server with the SS7 based HLR. In the case of 4G networks or Release 8 or greater 3GPP networks, there would be a Home Subscriber Server (HSS) in the place of the HLR that would connect to the AAA Proxy/Server. The HSS uses Diameter as the enabling protocol and thus would require an interworking function that would convert the RADIUS to Diameter signaling.

Message Flows for Roaming Authentication and Accounting

The specific messages and nodes involved in the authentication flows will differ between operator implementations. RADIUS is extensively used as the AAA protocol for Wi-Fi networks; however other protocols are involved when the home network belongs to a mobile 3G operator. The diagram in Figure 5 provides an example, at a high level, of the authentication, authorization and accounting flows and the corresponding nodes involved in establishing roaming between a WLAN and a 3GPP network. In this case, EAP is used to automatically authenticate the user by validating IMSI-specific information in the SIM with the corresponding credentials obtained from a Home Location Register (HLR) in the 3G network.

Any-to-Any Services Interworking – The Key To Seamless Roaming

In order to enable interoperability between the different architectures, a mediation and interworking platform is required to support the different scenarios where RADIUS, Diameter and SS7 are used [6]. The Dialogic® Helix™ Signaling Controller is a platform that is well suited to take on the interworking and mediation challenges Wi-Fi operators have in implementing their roaming and mobile data offload strategies. The Helix™ Signaling Controller (HSC) is uniquely architected with an intuitive and flexible service orchestration framework that enables seamless multiprotocol interworking along with Diameter Edge Agent (DEA) and Diameter Routing (DRA) functionality. The HSC enables service providers to structurally enable and adapt service scenarios to changing needs and circumstances. It represents the next generation of Diameter signaling controllers developed to give operators more control in routing, securing and interworking services based on Diameter, RADIUS and MAP. In addition to enabling diverse networks to communicate, its unique framework and ability to enhance message flows gives Wi-Fi, mobile operators and IPX/WRIX providers a service innovation platform that allows them to orchestrate services in a way that had not been available to them previously.
Let’s explore a few example use cases where the HSC can help address the interworking and operational challenges with Wi-Fi roaming and mobile data offload.

**Interworking RADIUS to facilitate Wi-Fi roaming**

Authentication and authorization of roaming subscribers is performed through RADIUS messages over an inter-operator interface between the visited network provider and home service provider. The interface can be implemented directly between two operators or through an intermediary, like an IPX or WRIX provider, that need to exchange RADIUS access and accounting messages. The interworking functionality can be placed within either of the visited and home operator’s networks, an IPX/WRIX provider or all three locations.

![Diagram showing interworking functionality](image)

**Figure 6. The Dialogic® Helix™ Signaling Controller can provide RADIUS routing, mediation and interworking with other Wi-Fi providers to help accelerate interconnection with roaming partners.**

By providing the interworking functionality to support WRIX-i or IR 61 [4] roaming requirements, service providers can gain control in how they establish roaming with both pure-play and MNO-based Wi-Fi network providers. The HSC supports RFC 2865 RADIUS proxy capabilities to enable realm-based routing of RADIUS messages to the appropriate destination. However, even in scenarios where 3GPP, GSMA and WBA defined interfaces are used, the RADIUS attributes might not be the same [6]. To address this, RADIUS-to-RADIUS mediation capability of the HSC can help to quickly align differences in interface implementations to support seamless roaming. Service providers benefit by saving considerable time and expense since they do not have to go back to their infrastructure vendors to solve interoperability issues or have their corresponding roaming partners modify their interface implementations.

**Centralized routing and interworking for 3GPP operators**

We’ve discussed previously the flow of RADIUS access messages used to authenticate subscribers with SIM based approaches. While most of the authentication and authorization traffic is RADIUS-based, many 3GPP operators are moving to an Evolved Packet Core (EPC) as they prepare and implement LTE in the Radio Access Network (RAN). This results in the need to interwork RADIUS and Diameter messages when establishing roaming with Wi-Fi operators. Also, incompatibility in signaling protocols can occur not only between a pure-play Wi-Fi operator and a 3GPP based wireless operator at the Network-to-Network Interface (NNI), but also between two 3GPP operators where one is utilizing the RADIUS based Wd interface with its AAA proxy and the other is using the Diameter SWd interface when connecting to its roaming partners.
Finally, a 3GPP operator may need to interwork RADIUS, Diameter or even HTTP in some cases between its AAA proxy and its HLR or HSS depending on what the proxy uses to request information on authorized IMSIs for validation purposes. Often, service providers have to deploy stand-alone gateways to remedy any interworking issues between their AAA server and HSS/HLR or hope their AAA vendor can accommodate their migration to 4G interfaces or need for RADIUS support.

The HSC provides a single, manageable platform for routing and interworking of Diameter, RADIUS, HTTP and SS7 traffic to address the incompatibility challenges service providers face when trying to implement a seamless roaming and Wi-Fi offload strategy. Service providers can use the Any-to-Any service orchestration capabilities of the HSC to:

- Interwork Wi-Fi interfaces based on WRIX-i or IR 61 with 3GPP based networks utilizing Diameter
- Interwork RADIUS-based authentication and authorization (RFC 2865) and accounting (RFC 2866) with the corresponding Diameter-based services
- Eliminate the need for separate gateways between the AAA proxy/server and an HSS or HLR to interwork RADIUS to Diameter or RADIUS to MAP/SS7
- Support HTTP based connections to EAP-SIM AAA servers
- Provide extensive traffic reporting based on configurable event detail records

The HSC accomplishes interworking through an intuitive and easy to use service orchestration framework that leverages a template driven approach to make the task straightforward. In addition, the template driven architecture makes the platform extensible to support interface variations and proprietary attribute value pairs (AVPs) without the need for costly and time consuming development work. The extensive interworking capabilities of the HSC helps service providers protect existing infrastructure investment by extending the life of existing platforms that would otherwise have to be upgraded or replaced to support the newer protocols and architectures.

**Enhancing user experience while optimizing core traffic load**

The unique service orchestration and enhancement features of the HSC integrated into the flow management procedures allow service providers the flexibility to inspect and alter message flows directly through the web based GUI. For example, as a roaming Wi-Fi subscriber moves from one access point to another, there is a flurry of authentication messages going back into the core. Multiply this by hundreds of people moving between busy hotspots, like in airports or in stadiums, and the result is a mini signaling storm that can jeopardize user experience. The HSC can inspect message flows and extract and cache key attributes like IMSI information and use it to compare against subsequent requests. This can be used to set up a mechanism to potentially reduce the number of messages sent towards the HLR.
The HSC also provides access to all message parameters for all protocols involved which allows service providers to share subscriber level policy and charging information across network domains to enhance existing services and help them offer new promotional type services targeted to high value customers.

Interworking and enhancing policy and charging

In some Wi-Fi implementations, a WLAN Access Gateway (WAG) interfaces an Online Charging System (OCS) to retrieve and update real-time rating and charging information. In many cases, the WAG might not support the Diameter Credit Control messages but does support RADIUS accounting messages. Also, there may even be some vendor specific attributes added to the RADIUS and Diameter messages, making interworking, as well as mediation scenarios, complex and unwieldy.

The issue where one platform talks RADIUS while the corresponding node is expecting Diameter is not uncommon, and represents a real world scenario that challenges service providers on a daily basis. RADIUS is the predominant protocol in Wi-Fi roaming implementations for both WRIX-i and IR 61, and traditional approaches to interworking RADIUS and Diameter have included proprietary schemes, costly stand-alone gateways or home grown implementations using stack based methods. These interworking approaches introduce a high degree of complexity and management overhead to what is likely an already burdened operational staff.

The HSC can provide RADIUS to Diameter interworking to help service providers eliminate the need for stand-alone RADIUS-to-Diameter gateways, defer requirements to upgrade infrastructure, and offer new and innovative services to their customers.
This HSC can interwork RADIUS (RFC 2866) Accounting messages with the Diameter Credit Control Application (RFC 4006) to enable interoperability between Wi-Fi infrastructure and Online Charging Platforms by converting the RADIUS messages to the corresponding Diameter messages per the Gy or Wo reference specifications. The HSC can also enhance the message flows by:

- Inspecting the message contents of the incoming flows
- Evaluating conditional statements against other events or static values
- Initiating an LDAP lookup to an external database to correlate various informational elements such as username with subscriber MSISDN (Mobile Subscriber Integrated Services Digital Network-Number) in case it is not present in the original message flows

**Conclusions**

The demand for Wi-Fi Hotspots is literally heating up. Mobile operators are turning to Wi-Fi as a means to improve coverage and capacity to meet consumer demand for mobile data services. Organizations like the WBA, Wi-Fi Alliance, GSMA and 3GPP are working to set the standards for improving the overall user experience for customers to move seamlessly between 3G, 4G and Wi-Fi networks. But in order to get to that point, there are several challenges along the way service providers will have to face to implement seamless mobile data coverage.

When it comes to Wi-Fi offload and roaming, by applying technology that includes interworking of RADIUS, Diameter and SS7/MAP interfaces, today’s Wi-Fi operators can accelerate connectivity between different types of networks, better leverage existing investments in infrastructure, and upgrade to new technology and architectures in a more controlled manner. The BorderNet Diameter Services HSC combines high availability Diameter Edge Agent and Routing capabilities with advanced and intuitive service orchestration to provide unparalleled multi-protocol service interworking, security, and routing. The Helix™ Signaling Controller (HSC) provides operators with an interworking and service innovation platform that can help lower costs and more rapidly connect networks to provide roaming customers with the user experience and coverage they look for.

**Bibliography**


