DMM Working Group
Internet-Draft
Intended status: Informational
Expires: 20 April 2026

M. Grayson
Cisco Systems

17 October 2025

# Distributed Roaming and Mobility Problem Statement
## draft-grayson-distributed-roaming-mobility-00

Abstract

This document describes the problem statement for enabling roaming across a distributed set of heterogenous wireless access networks.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at https://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on 20 April 2026.

Table of Contents



## 1. Introduction

Mobility management and roaming are core capabilities of the wireless ecosystem. Whereas the topic of mobility management has often been focused on the functionality deployed in public macro cellular networks, that provide service over wide geographic areas to millions of subscribers, there is increasing interest in how to integrate wide area public macro cellular systems with small, localized, distributed private wireless network deployments. This document describes the challenges with scaling the roaming signaling between these different distributed networks.

### 1.1. Terminology

To Be Completed

## 2. Roaming Architectures

Roaming signaling is sent between a wireless access network and an identity provider to enable the authentication and authorization of an identity provider end-user onto the third-party operated wireless access network.

Conventionally, these approaches have relied on hierarchical schemes to support roaming signaling. For example, the eduroam system described in [RFC7593] scales by having a hierarchy that includes national proxies and global proxies, as illustrated in Figure 1.

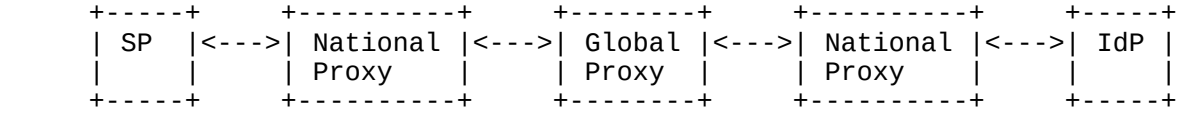


Figure 1: Hierarchical Approach for Roaming across the eduroam federation

Existing 4G roaming solutions are based on a similar hop-by-hop approach. Intermediaries, that may include Roaming Hubs, IPX and Roaming Value Added Services (RVAS) terminate roaming signaling and re-establish signaling between the next hop system, as illustrated in Figure 2.

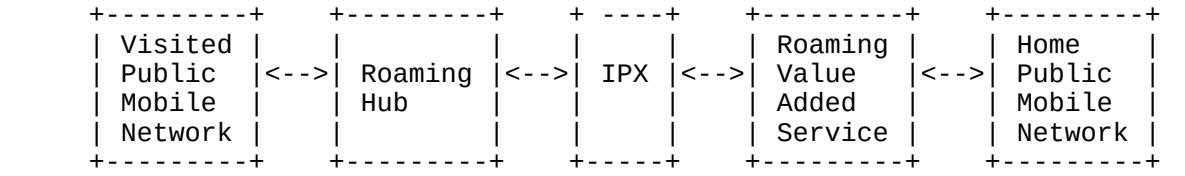


Figure 2: Hierarchical Approach for Roaming across the public 4G Networks

## 3. Scaling Roaming Signaling

The GSMA (www.gsma.com) has been successful in scaling roaming between over 800 public cellular operators. However, how to scale roaming signaling for the switch to small, localized, distributed networks is still a significant issue.

One key aspect of scaling private networks is related to the dimensioning of inter-connected signaling that is a function of the geographical coverage of the private wireless access network and the number of subscribers served by a particular identity provider. Public cellular networks provide nationwide coverage to 10s of millions of subscribers. Such scale drives significant roaming signaling traffic between cellular providers that enable assumptions related to longevity of signaling connections to be embedded into technical procedures that support bidirectional signaling between all public cellular operators. In contrast, early data from the Wireless Broadband Alliance (WBA) on adoption of its OpenRoaming federation [I-D.draft-tomas-openroaming], a system designed to operate with private wireless networks, indicates that dimensioning in private deployments may be as low as one thousandth of that experienced by a conventional public cellular network.

With some forecasting 1 million private cellular networks by the end of the decade [RCRWIRELESSNEWS], a thousand times the current number of public cellular networks, we can anticipate the future scalability challenges of being able to support 1000 times more networks, each with 1/1000th of the signaling load.

## 4. Flattening Roaming Hierarchies

In contrast to traditional hierarchical approaches to roaming signaling, recent developments have seen a switch to flattened architectures. For example, the OpenRoaming federation [I-D.draft-tomas-openroaming] uses Dynamic Peer Discovery for RADIUS/TLS [RFC7585] to enable a flattened architecture with roaming signaling sent directly between the OpenRoaming Access Network Provider (ANP) and the OpenRoaming Identity Provider (IDP), as illustrated in Figure 3.

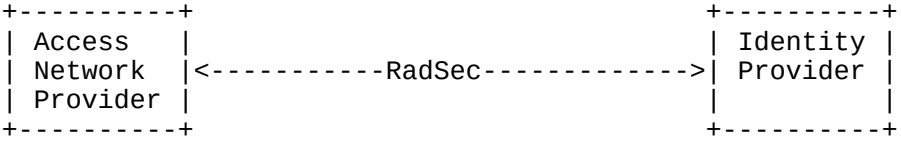


Figure 3: OpenRoaming Federation

5G has introduced a new Service Based Architecture (SBA) that avoids strict signaling hierarchies. Instead, SBA allows signaling consumers to communicate with different signaling producers. Form a roaming perspective, the 5G system has been enhanced whereby there is a direct TLS signaling exchange between Security Edge Protection Proxies (SEPP), deployed by both home and visited networks, used to exchange the SBA-based signaling.

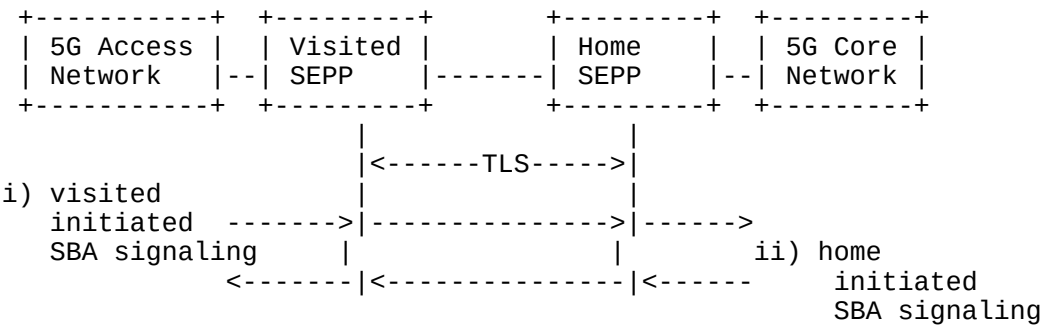


Figure 4: 5G Roaming Architecture

Furthermore, whereas 5G Release 15 introduced the concept of Non Public Networks (NPN) into the 5G architecture (https://www.3gpp.org/technologies/npn), 3GPP Release 16 saw the introduction of Standalone NPN Cellular Hotspots [_3GPPTS22261].

SNPN Cellular Hotspots refers to a connectivity hotspot based on 3GPP 5G network technology that provides services in a similar way as provided by Wi-Fi hotspots. Charging requirements are considered out of scope for this functionality.

Requirements for SNPN Cellular Hotspots include the ability of a Hotspot to interconnect with a large number of identity providers, termed SNPN Credential Providers.

## 5. Bi-Directional Roaming signaling

Roaming signaling used to interconnect wireless access networks with identity provider networks is used to authenticate credentials presented by devices and authorize access onto the specific wireless network. Even if the provision of the wireless service is monetized by some alternative value chain other than charging the end-user, roaming signaling usually includes accounting messages.

While authentication, authorization and accounting messages can be described as access network originated signaling, there are typically requirements for roaming systems to support identity provider initiated signaling. For example, if the end-user is being charged, there can be an identity provider initiated signaling to indicate that the user has consumed all their available credit. In other roaming systems, identity provider initiated signaling can be used to signal a first wireless access network that a user previously authenticated and authorized to access via this first wireless access network has moved and is now being served by a second wireless access network.

## 6. Enterprise networks

All wireless access networks need to configure their perimeter firewall functions to enable roaming signaling to be exchanged between the wireless access network and the identity provider. In public cellular systems, the GSMA is responsible for operating the IR.21 roaming database, used to exchange the IP address ranges used by each operator for connection to the IPX [GSMAIR21]. IP address information for equipment such as Mobility Management Entities (MMEs), Serving Gateways (SGWs), signaling Edge Protection Proxies (SEPPs), User Plane Functions (UPFs) and AAA Servers is exchanged allowing the recipient to use such information to configure firewall and/or border gateway functions.

In contrast to a centralized data based approach that can scale to 100s of public cellular operators, there is no organization responsible for maintaining a centralized registry of signaling systems used to support roaming onto small, localized, distributed, private networks. In contrast in private networks, firewall rules are often configured to permit outbound signaling from enterprise specific functions while prohibiting signaling originating from unknown endpoints on the Internet. While able to support access network provider initiated roaming signaling, such a configuration will block any identity provider initiated roaming signaling, as illustrated in Figure 5.

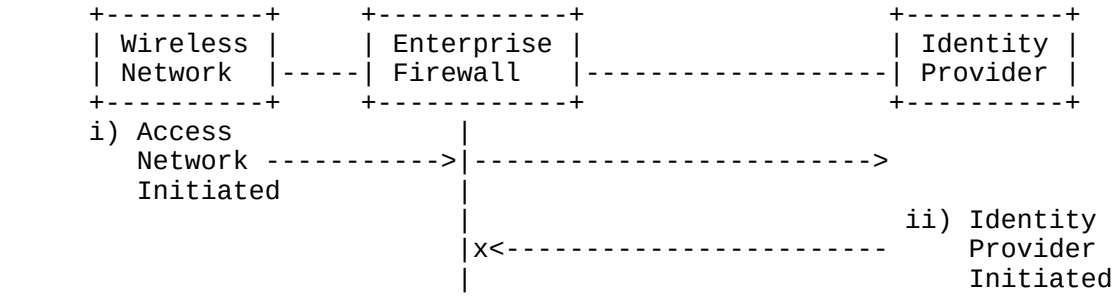


Figure 5: Private Enterprise Firewall Configuration

## 7. The Server-Initiated Roaming Challenge

In order to avoid the need to operate a central database for roaming onto small, localized, distributed, private wireless network deployments, roaming signaling needs to accommodate the typical enterprise firewall configurations that block server-initiated signaling.

### 7.1. Roaming Transport Alternatives

The challenge of how to support server push based signaling across firewall deployments is well understood. Roaming signaling is exchanged using a range of different transports:

* Wi-Fi Networks typically authenticate users using RADIUS [RFC2865] based signaling. More recently, Wi-Fi roaming is increasingly adopting RadSec to secure roaming signaling using secured sessions mutually authenticated using x509v3 PKI certificates [RFC6614].

* 4G Networks typically authenticate users using Diameter [RFC6733] based signaling. [_3GPPTS29272] specifies the S6a reference point. The S6a interface protocol is an IETF vendor specific Diameter application, where the Diameter application identifier assigned to

the application is 16777251. The S6a interface is protected by using 3GPP defined Security Gateways (SEG) used to establish and maintain IPsec secured ESP Security Association in tunnel mode between security domains [_3GPPTS33210].

* 5G Service Based Architecture allows signaling consumers to communicate with different signaling producers. SBA defines the use of RESTful APIs transported using HTTP2 defined methods like GET, POST and PATCH. The 5G System also introduces the Security Edge Protection Proxy (SEPP). The SEPP sits at the perimeter of the 5G public cellular network. The 5G N32 interface is defined by 3GPP for use between two SEPPs to ensure the HTTP2 messages can be securely exchanged. First, N32 control signaling is exchanged to establish N32 forwarding. The N32 forwarding operates by taking the HTTP2 Request or Response messages that need to be exchanged between operators and encoding the HTTP2 header frames and data frames in JSON.

## 7.2. Supporting server-initiated messages

Looking at current solutions for supporting server-initiated messages with these different transports:

* IETF RADEXT has identified the challenge of how a home RADIUS server can send Change of Authorization (CoA) packets to a Network Access Server (NAS) which is behind a firewall or NAT gateway. [I-D.draft-ietf-radext-reverse-coa] defines a "reverse change of authorization (CoA)" path for RADIUS packets, allowing a home RADIUS server to send CoA packets in "reverse" down a RADIUS/TLS connection that was previously established by an access network originated signaling exchange.

* 3GPP is discussing architectural enhancements to support SNPN Cellular Hotspots in 5G. Discussions highlight that in current N32 SBA architecture, the HPLMN initiated signaling to a callback URI may require a separate access network firewall rule configuration. Proposals include studying enhancements to N32 that permit the server initiated signaling towards an SNPN to reuse the same outbound socket as SNPN-initiated signaling towards the server so as to minimize the firewall and border gateway configuration of the SNPN.

* There are no standard Diameter protocol technique that allows a server-initiated message to reuse an existing SCTP or TLS connection from the Diameter server to the Diameter client in a way that avoids the client operator having to configure firewall rules for inbound traffic.

## 8. Problem Statement

The problems that can be addressed with DMM are summarized as follows:

PS1: Re-using outbound sockets when roaming with 5G Service Based Architecture

PS2: Re-using outbound sockets when roaming with 4G Diameter Based Architecture

## 9. Security Considerations

To Be Completed

## 10. IANA Considerations

To Be Completed

## 11. Informative References

[GSMAIR21] "GSM Association Roaming Database, Structure and Updating", n.d., <https://www.gsma.com/newsroom/wp-content/uploads//IR.21-v17.0-2.pdf>.

[I-D.draft-ietf-radext-reverse-coa] DeKok, A. and V. Cargatser, "Reverse Change-of-Authorization (CoA) in RADIUS/(D)TLS", Work in Progress, Internet-Draft, draft-ietf-radext-reverse-coa-08, 27 August 2025, <https://datatracker.ietf.org/doc/html/draft-ietf-radext-reverse-coa-08>.

[I-D.draft-tomas-openroaming] Tomas, B., Grayson, M., Canpolat, N., Cockrell, B. A., and S. Gundavelli, "WBA OpenRoaming Wireless Federation", Work in Progress, Internet-Draft, draft-tomas-openroaming-06, 16 September 2025, <https://datatracker.ietf.org/doc/html/draft-tomas-openroaming-06>.

[RCRWIRELESSNEWS] "A million private 5G networks by 2030? A million just in Europe, says Vodafone", n.d., <https://www.rcrwireless.com/20210127/5g/million-private-5g-networks-in-europe-vodafone>.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, DOI 10.17487/RFC2865, June 2000, <https://www.rfc-editor.org/rfc/rfc2865>.

[RFC6614] Winter, S., McCauley, M., Venaas, S., and K. Wierenga, "Transport Layer Security (TLS) Encryption for RADIUS", RFC 6614, DOI 10.17487/RFC6614, May 2012, <https://www.rfc-editor.org/rfc/rfc6614>.

[RFC6733] Fajardo, V., Ed., Arkko, J., Loughney, J., and G. Zorn, Ed., "Diameter Base Protocol", RFC 6733, DOI 10.17487/RFC6733, October 2012, <https://www.rfc-editor.org/rfc/rfc6733>.

[RFC7585] Winter, S. and M. McCauley, "Dynamic Peer Discovery for RADIUS/TLS and RADIUS/DTLS Based on the Network Access Identifier (NAI)", RFC 7585, DOI 10.17487/RFC7585, October 2015, <https://www.rfc-editor.org/rfc/rfc7585>.

[RFC7593] Wierenga, K., Winter, S., and T. Wolniewicz, "The eduroam Architecture for Network Roaming", RFC 7593, DOI 10.17487/RFC7593, September 2015, <https://www.rfc-editor.org/rfc/rfc7593>.

[_3GPPTS22261] "Service requirements for the 5G system", n.d., <https://www.3gpp.org/ftp/Specs/archive/22_series/22.261/22261-jc0.zip>.

[_3GPPTS29272] "Evolved Packet System (EPS); Mobility Management Entity (MME) and Serving GPRS Support Node (SGSN) related interfaces based on Diameter protocol", n.d., <https://www.3gpp.org/ftp/Specs/archive/29_series/29.272/29272-j30.zip>.

[_3GPPTS33210] "Network Domain Security (NDS); IP network layer security", n.d., <https://www.3gpp.org/ftp/Specs/archive/33_series/33.210/33210-j20.zip>.

## Author’s Address

Mark Grayson
Cisco Systems
10 New Square Park
Feltham
TW14 8HA
United Kingdom
Email: mgrayson@cisco.com