Network Working Group
Internet-Draft
Intended status: Informational
Expires: March 11, 2013

H. Chan (Ed.)
Huawei Technologies

September 7, 2012

Requirements for Distributed Mobility Management
draft-ietf-dmm-requirements-02

Abstract

This document defines the requirements for Distributed Mobility Management (DMM) in IPv6 deployments. The traditionally hierarchical structure of cellular networks has led to deployment models which are in practice centralized. Mobility management with logically centralized mobility anchoring in current mobile networks is prone to suboptimal routing and raises scalability issues. Such centralized functions can lead to single points of failure and inevitably introduce longer delays and higher signaling loads for network operations related to mobility management. The objective is to enhance mobility management in order to meet the primary goals in network evolution, i.e., improve scalability, avoid single points of failure, enable transparent mobility support to upper layers only when needed, and so on. Distributed mobility management must be secure and compatible with existing network deployments and end hosts.

Table of Contents

1. Introduction

In the past decade a fair number of mobility protocols have been standardized [RFC6275] [RFC5944] [RFC5380] [RFC6301] [RFC5213]. Although the protocols differ in terms of functions and associated message formats, we can identify a few key common features:

- a centralized mobility anchor providing global reachability and an always-on experience to the user;
- extensions to the base protocols to optimize handover performance while users roam across wireless cells; and
- extensions to enable the use of heterogeneous wireless interfaces for multi-mode terminals (e.g. smartphones).

The presence of the centralized mobility anchor allows a mobile node to remain reachable when it is not connected to its home domain. The anchor point, among other tasks, ensures connectivity by forwarding packets destined to, or sent from, the mobile node. In practice, most of the deployed architectures today have a small number of centralized anchors managing the traffic of millions of mobile nodes. Compared with a distributed approach, a centralized approach is likely to have several issues or limitations affecting performance and scalability, which require costly network dimensioning and engineering to resolve.

To optimize handovers from the perspective of mobile nodes, the base protocols have been extended to efficiently handle packet forwarding between the previous and new points of attachment. These extensions are necessary when applications have stringent requirements in terms of delay. Notions of localization and distribution of local agents have been introduced to reduce signaling overhead [Paper-Distributed.Centralized.Mobility]. Unfortunately, today we witness difficulties in getting such protocols deployed, resulting in sub-optimal choices for the network operators.

Moreover, the availability of multi-mode devices and the possibility of using several network interfaces simultaneously have motivated the development of even more protocol extensions to add more capabilities to the base protocol. In the end, deployment is further complicated with the multitude of extensions.

Mobile users are, more than ever, consuming Internet content; such traffic imposes new requirements on mobile core networks for data traffic delivery. When the traffic demand exceeds available capacity, service providers need to implement new strategies such as selective traffic offload (e.g. 3GPP work items LIPA/SIPTO

[TS.23829]) through alternative access networks (e.g. WLAN) [Paper-Mobile.Data.Offloading]. Moreover, the presence of content providers closer to the mobile/fixed Internet Service Providers network requires taking into account local Content Delivery Networks (CDNs) while providing mobility services.

When demand exceeds capacity, both traffic offloading and CDN mechanisms could benefit from the development of mobile architectures with fewer levels of routing hierarchy introduced into the data path by the mobility management system. This trend towards so-called "flat networks" is reinforced by a shift in user traffic behavior. In particular, there is an increase in direct communications among peers in the same geographical area. Distributed mobility management in a truly flat mobile architecture would anchor the traffic closer to the point of attachment of the user, overcoming the suboptimal route stretch of a centralized mobility scheme.

While deploying today’s mobile networks, service providers face new challenges. Mobility patterns indicate that, more often than not, mobile nodes remain attached to the same point of attachment for considerable periods of time [Paper-Locating.User] . Therefore it is not uncommon to observe that specific IP mobility management support is not required for applications that launch and complete their sessions while the mobile node is connected to the same point of attachment. However, currently, IP mobility support is designed for always-on operation, maintaining all parameters of the context for each mobile subscriber for as long as they are connected to the network. This can result in a waste of resources and ever-increasing costs for the service provider. Infrequent node mobility coupled with application intelligence suggest that mobility can be provided selectively, thus simplifying the context maintained in the different nodes of the mobile network.

The DMM charter addresses two complementary aspects of mobility management procedures: the distribution of mobility anchors towards a more flat network and the dynamic activation/deactivation of mobility protocol support as an enabler to distributed mobility management. The former aims at positioning mobility anchors (HA, LMA) closer to the user; ideally, mobility agents could be collocated with the first-hop router. The latter, facilitated by the distribution of mobility anchors, aims at identifying when mobility support must be activated and identifying sessions that do not require mobility management support -- thus reducing the amount of state information that must be maintained in various mobility agents of the mobile network. The key idea is that dynamic mobility management relaxes some of the constraints of previously-standardized mobility management solutions and, by doing so, it can avoid the establishment of non-optimal tunnels between two topologically distant anchors.

Given this motivational background in this section, this document compares distributed mobility management with centralized mobility management in Section 3. The requirements to address these problems are given in Section 4. Finally, security considerations are discussed in Section 5.

The problem statement and the use cases [I-D.yokota-dmm-scenario] can be found in [Paper-Distributed.Mobility.Review].

2. Conventions used in this document

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL","SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

2.1. Terminology

All the general mobility-related terms and their acronyms used in this document are to be interpreted as defined in the Mobile IPv6 base specification [RFC6275], in the Proxy mobile IPv6 specification [RFC5213], and in Mobility Related Terminology [RFC3753]. These terms include the following: mobile node (MN), correspondent node (CN), and home agent (HA) as per [RFC6275]; local mobility anchor (LMA) and mobile access gateway (MAG) as per [RFC5213], and context as per [RFC3753].

In addition, this draft introduces the following term.

Mobility context

> is the collection of information required to provide mobility management support for a given mobile node.

3. Centralized versus distributed mobility management

Mobility management functions may be implemented at different layers of the protocol stack. At the IP (network) layer, they may reside in the network or in the mobile node. In particular, a network-based solution resides in the network only. It therefore enables mobility for existing hosts and network applications which are already in deployment but lack mobility support.

At the IP layer, a mobility management protocol supporting session continuity is typically based on the principle of distinguishing between identifier and routing address and maintaining a mapping between the two. In Mobile IP, the home address serves as an

identifier of the device whereas the care-of-address (CoA) takes the role of the routing address. The binding between these two is maintained at the home agent (mobility anchor). If packets can be continuously delivered to a mobile node at its home address, then all sessions using that home address are unaffected even though the routing address (CoA) changes.

The next two subsections explain centralized and distributed mobility management functions in the network.

3.1. Centralized mobility management

In centralized mobility management, the mapping information between the persistent node identifier and the changing IP address of a mobile node (MN) is kept at a single mobility anchor. At the same time, packets destined to the MN are routed via this anchor. In other words, such mobility management systems are centralized in both the control plane and the data plane.

Many existing mobility management deployments make use of centralized mobility anchoring in a hierarchical network architecture, as shown in Figure 1. Examples of such centralized mobility anchors are the home agent (HA) and local mobility anchor (LMA) in Mobile IPv6 [RFC6275] and Proxy Mobile IPv6 [RFC5213], respectively. Current cellular networks such as the Third Generation Partnership Project (3GPP) UMTS networks, CDMA networks, and 3GPP Evolved Packet System (EPS) networks employ centralized mobility management too. In particular, Gateway GPRS Support Node (GGSN) and Serving GPRS Support Node (SGSN) in the 3GPP UMTS hierarchical network, and the Packet data network Gateway (P-GW) and Serving Gateway (S-GW) in the 3GPP EPS network, respectively, act as anchors in a hierarchy.

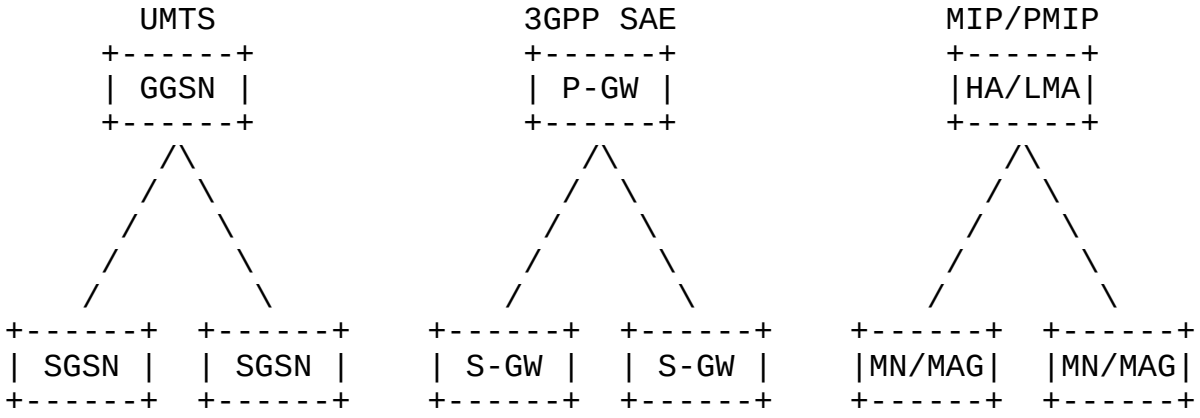

Figure 1. Centralized mobility management.

3.2. Distributed mobility management

Mobility management functions may also be distributed to multiple networks as shown in Figure 2, so that a mobile node in any of these networks may be served by a closeby mobility function (MF).

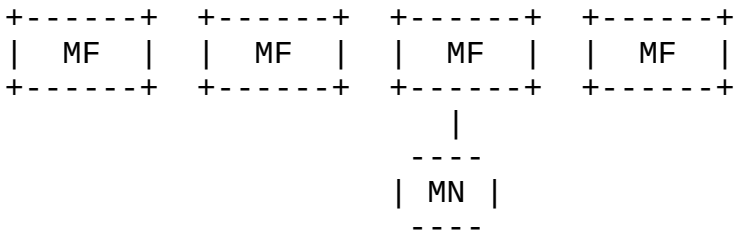

Figure 2. Distributed mobility management.

Mobility management may be partially or fully distributed. In the former case only the data plane is distributed. Fully distributed mobility management implies that both the data plane and the control plane are distributed. These different approaches are described in detail in [I-D.yokota-dmm-scenario].

A distributed mobility management scheme for future flat IP-based mobile network architecture consisting of access nodes is proposed in [Paper-Distributed.Dynamic.Mobility]. Its benefits over centralized mobility management are shown through simulations in [Paper-Distributed.Centralized.Mobility]. Moreover, the (re)use and extension of existing protocols in the design of both fully distributed mobility management [Paper-Migrating.Home.Agents] [Paper-Distributed.Mobility.SAE] and partially distributed mobility management [Paper-Distributed.Mobility.PMIP] [Paper-Distributed.Mobility.MIP] have been reported in the literature. Therefore, before designing new mobility management protocols for a future flat IP architecture, it is recommended to first consider whether existing mobility management protocols can be extended to serve a flat IP architecture.

4. Requirements

After comparing distributed mobility management against centralized deployment in Section 3, this section states the requirements as follows:

4.1. Distributed deployment

REQ1: Distributed deployment

IP mobility, network access and routing solutions provided by DMM MUST enable distributed deployment for mobility management of IP sessions so that traffic does not need to traverse centrally deployed mobility anchors and thus can be routed in an optimal manner.

Motivation: This requirement is motivated by current trends in network evolution: (a) it is cost- and resource-effective to cache and distribute content by combining distributed mobility anchors with caching systems (e.g., CDN); (b) the significantly larger number of mobile nodes and flows call for improved scalability; (c) single points of failure are avoided in a distributed system; (d) threats against centrally deployed anchors, e.g., home agent and local mobility anchor, are mitigated in a distributed system.

This requirement addresses problems PS1, PS2, PS3, and PS4 in the following.

PS1: Non-optimal routes

Routing via a centralized anchor often results in a longer route. The problem is especially manifested when accessing a local server or servers of a Content Delivery Network (CDN).

PS2: Divergence from other evolutionary trends in network architecture

Centralized mobility management can become non-optimal with a flat network architecture.

PS3: Low scalability of centralized route and mobility context maintenance

Setting up routes through a central anchor and maintaining mobility context for each MN therein requires more resources is more difficult to scale in a centralized design, thus reducing scalability. Distributing the route maintenance function and the mobility context maintenance function among different network entities can increase scalability.

PS4: Single point of failure and attack

Centralized anchoring may be more vulnerable to single points of failures and attacks than a distributed system. The impact of a successful attack on a system with centralized mobility management can be far greater as well.

4.2. Transparency to Upper Layers when needed

REQ2: Transparency to Upper Layers when needed

DMM solutions MUST provide transparent mobility support above the IP layer when needed. Such transparency is needed, for example, when, upon change of point of attachment to the Internet, an application flow cannot cope with a change in the IP address. Otherwise, support for maintaining a stable home IP address or prefix during handovers may be declined.

Motivation: The motivation of this requirement is to enable more efficient use of network resources and more efficient routing by not maintaining context at the mobility anchor when there is no such need.

This requirement addresses the problems PS5 as well as the other related problem O-PS1.

PS5: Wasting resources to provide mobility support to nodes that do not need such support

IP mobility support is not always required, and not every parameter of mobility context is always used. For example, some applications do not need a stable IP address during a handover to maintain IP session continuity. Sometimes, the entire application session runs while the terminal does not change the point of attachment.

O-PS1: Mobility signaling overhead with peer-to-peer communication

Wasting resources when mobility signaling (e.g., maintenance of the tunnel, keep alive, etc.) is not turned off for peer-to-peer communication. Peer-to-peer communications have particular traffic patterns that often do not benefit from mobility support from the network. Thus, the assoicated mobility support signaling (e.g., maintenance of the tunnel, keep alives, etc.) wastes network resources for no application gain. In such a case, it is better to enable mobility support selectively.

4.3. IPv6 deployment

REQ3: IPv6 deployment

DMM solutions SHOULD target IPv6 as the primary deployment environment and SHOULD NOT be tailored specifically to support IPv4, in particular in situations where private IPv4 addresses and/or NATs are used.

Motivation: This requirement is to be inline with the general orientation of IETF work. DMM deployment is foreseen in mid- to long-term horizon, when IPv6 is expected to be far more common than today. It is also unnecessarily complex to solve this problem for IPv4, as we will not be able to use some of the IPv6-specific features/tools.

4.4. Existing mobility protocols

REQ4: Existing mobility protocols

A DMM solution SHOULD first consider reusing and extending IETF-standardized protocols before specifying new protocols.

Motivation: Using IETF protocols is easier to deploy and to update.

4.5. Compatibility

REQ5: Compatibility

The DMM solution MUST be able to co-exist with existing network deployments and end hosts. For example, depending on the environment in which DMM is deployed, DMM solutions may need to be compatible with other deployed mobility protocols or may need to interoperate with a network or mobile hosts/ routers that do not support DMM protocols. Furthermore, a DMM solution SHOULD work across different networks, possibly operated as separate administrative domains, when allowed by the trust relationship between them.

Motivation: The motivations of this requirement are (1) to preserve backwards compatibility so that existing networks and hosts are not affected and continue to function as usual, and (2) enable inter-domain operation if desired.

This requirement addresses the following related problem O-PS2.

O-PS2: Complicated deployment with too many MIP variants and extensions

Deployment is complicated with many variants and extensions of MIP. When introducing new functions which may add to the complexity, existing solutions are more vulnerable to break.

4.6. Security considerations

REQ6: Security considerations

DMM protocol solutions MUST consider security aspects, including confidentiality and integrity. Examples of aspects to be considered are authentication and authorization mechanisms that allow a legitimate mobile host/router to use the mobility support provided by the DMM solution; signaling message protection in terms of authentication, encryption, etc.; data integrity and confidentiality; opt-in or opt-out data confidentiality to signaling messages depending on network environments or user requirements.

Motivation: Mutual authentication and authorization between a mobile host/router and an access router providing the DMM service to the mobile host/router are required to prevent potential attacks in the access network of the DMM service. Various attacks such as impersonation, denial of service, man-in-the-middle attacks, and so on, can be mounted against a DMM service and need to be protected against.

Signaling messages can be subject to various attacks since they carry critical context information about a mobile node/ router. For instance, a malicious node can forge a number of signaling messages thus redirecting traffic from its legitimate path. Consequently, the specific node is under a denial of service attack, whereas other nodes do not receive their traffic. As signaling messages may travel over the Internet, end-to-end security could be required.

5. Security Considerations

Distributed mobility management (DMM) requires two kinds of security considerations: First, access network security that only allows a legitimate mobile host/router to access the DMM service; Second, end-to-end security that protects signaling messages for the DMM service. Access network security is required between the mobile host/router and the access network providing the DMM service. End-to-end security is required between nodes that participate in the DMM

protocol.

It is necessary to provide sufficient defense against possible security attacks, or to adopt existing security mechanisms and protocols to provide sufficient security protections. For instance, EAP-based authentication can be used for access network security, while IPsec can be used for end-to-end security.

6. IANA Considerations

None

7. Co-authors and Contributors

This problem statement document is a joint effort among the following participants. Each individual has made significant contributions to this work.

Dapeng Liu: liudapeng@chinamobile.com

Pierrick Seite: pierrick.seite@orange-ftgroup.com

Hidetoshi Yokota: yokota@kddilabs.jp

Charles E. Perkins: charliep@computer.org

Melia Telemaco: telemaco.melia@alcatel-lucent.com

Elena Demaria: elena.demaria@telecomitalia.it

Peter McCann: Peter.McCann@huawei.com

Kostas Pentikousis: k.pentikousis@huawei.com

Tricci So: tso@zteusa.com

Jong-Hyouk Lee: jh.lee@telecom-bretagne.eu

Jouni Korhonen: jouni.korhonen@nsn.com

Sri Gundavelli: sgundave@cisco.com

Carlos J. Bernardos: cjbc@it.uc3m.es

Marco Liebsch: Marco.Liebsch@neclab.eu

Wen Luo: luo.wen@zte.com.cn

Georgios Karagiannis: g.karagiannis@utwente.nl

Julien Laganier: jlaganier@juniper.net

Wassim Michel Haddad: Wassam.Haddad@ericsson.com

Alexandru Petrescu: alexandru.petrescu@gmail.com

Seok Joo Koh: sjkoh@knu.ac.kr

Dirk von Hugo: Dirk.von-Hugo@telekom.de

Ahmad Muhanna: amuhanna@awardsolutions.com

8. References

8.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

8.2. Informative References

[I-D.ietf-netext-pd-pmip]
Zhou, X., Korhonen, J., Williams, C., Gundavelli, S., and C. Bernardos, "Prefix Delegation for Proxy Mobile IPv6", draft-ietf-netext-pd-pmip-02 (work in progress), March 2012.

[I-D.yokota-dmm-scenario]
Yokota, H., Seite, P., Demaria, E., and Z. Cao, "Use case scenarios for Distributed Mobility Management", draft-yokota-dmm-scenario-00 (work in progress), October 2010.

[Paper-Distributed.Centralized.Mobility]
Bertin, P., Bonjour, S., and J-M. Bonnin, "A Distributed or Centralized Mobility", Proceedings of Global Communications Conference (GlobeCom), December 2009.

[Paper-Distributed.Dynamic.Mobility]
Bertin, P., Bonjour, S., and J-M. Bonnin, "A Distributed Dynamic Mobility Management Scheme Designed for Flat IP Architectures", Proceedings of 3rd International Conference on New Technologies, Mobility and Security

(NTMS), 2008.

[Paper-Distributed.Mobility.MIP]
Chan, H., "Distributed Mobility Management with Mobile IP", Proceedings of IEEE International Communication Conference (ICC) Workshop on Telecommunications: from Research to Standards, June 2012.

[Paper-Distributed.Mobility.PMIP]
Chan, H., "Proxy Mobile IP with Distributed Mobility Anchors", Proceedings of GlobeCom Workshop on Seamless Wireless Mobility, December 2010.

[Paper-Distributed.Mobility.Review]
Chan, H., Yokota, H., Xie, J., Seite, P., and D. Liu, "Distributed and Dynamic Mobility Management in Mobile Internet: Current Approaches and Issues, Journal of Communications, vol. 6, no. 1, pp. 4-15, Feb 2011.", Proceedings of GlobeCom Workshop on Seamless Wireless Mobility, February 2011.

[Paper-Distributed.Mobility.SAE]
Fisher, M., Anderson, F., Kopsel, A., Schafer, G., and M. Schlager, "A Distributed IP Mobility Approach for 3G SAE", Proceedings of the 19th International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), 2008.

[Paper-Locating.User]
Kirby, G., "Locating the User", Communication International, 1995.

[Paper-Migrating.Home.Agents]
Wakikawa, R., Valadon, G., and J. Murai, "Migrating Home Agents Towards Internet-scale Mobility Deployments", Proceedings of the ACM 2nd CoNEXT Conference on Future Networking Technologies, December 2006.

[Paper-Mobile.Data.Offloading]
Lee, K., Lee, J., Yi, Y., Rhee, I., and S. Chong, "Mobile Data Offloading: How Much Can WiFi Deliver?", SIGCOMM 2010, 2010.

[RFC3753] Manner, J. and M. Kojo, "Mobility Related Terminology", RFC 3753, June 2004.

[RFC3963] Devarapalli, V., Wakikawa, R., Petrescu, A., and P. Thubert, "Network Mobility (NEMO) Basic Support Protocol",

RFC 3963, January 2005.

[RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K., and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.

[RFC5380] Soliman, H., Castelluccia, C., ElMalki, K., and L. Bellier, "Hierarchical Mobile IPv6 (HMIPv6) Mobility Management", RFC 5380, October 2008.

[RFC5944] Perkins, C., "IP Mobility Support for IPv4, Revised", RFC 5944, November 2010.

[RFC6275] Perkins, C., Johnson, D., and J. Arkko, "Mobility Support in IPv6", RFC 6275, July 2011.

[RFC6301] Zhu, Z., Wakikawa, R., and L. Zhang, "A Survey of Mobility Support in the Internet", RFC 6301, July 2011.

[TS.23829] 3GPP, "Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)", 3GPP TR 23.829 10.0.1, October 2011.

Author's Address

H Anthony Chan (editor)
Huawei Technologies
5340 Legacy Dr. Building 3, Plano, TX 75024, USA
Email: h.a.chan@ieee.org
-
Dapeng Liu
China Mobile
Unit2, 28 Xuanwumenxi Ave, Xuanwu District, Beijing 100053, China
Email: liudapeng@chinamobile.com
-
Pierrick Seite
France Telecom - Orange
4, rue du Clos Courtel, BP 91226, Cesson-Sevigne 35512, France
Email: pierrick.seite@orange-ftgroup.com
-
Hidetoshi Yokota
KDDI Lab
2-1-15 Ohara, Fujimino, Saitama, 356-8502 Japan
Email: yokota@kddilabs.jp
-
Jouni Korhonen
Nokia Siemens Networks
Email: jouni.korhonen@nsn.com

-
Charles E. Perkins
Huawei Technologies
Email: charliep@computer.org
-
Melia Telemaco
Alcatel-Lucent Bell Labs
Email: telemaco.melia@alcatel-lucent.com
-
Elena Demaria
Telecom Italia
via G. Reiss Romoli, 274, TORINO, 10148, Italy
Email: elena.demaria@telecomitalia.it
-
Jong-Hyouk Lee
RSM Department, Telecom Bretagne
Cesson-Sevigne, 35512, France
Email: jh.lee@telecom-bretagne.eu
-
Kostas Pentikousis
Huawei Technologies
Carnotstr. 4 10587 Berlin, Germany
Email: k.pentikousis@huawei.com
-
Tricci So
ZTE
Email: tso@zteusa.com
-
Carlos J. Bernardos
Universidad Carlos III de Madrid
Av. Universidad, 30, Leganes, Madrid 28911, Spain
Email: cjbc@it.uc3m.es
-
Peter McCann
Huawei Technologies
Email: PeterMcCann@huawei.com
-
Seok Joo Koh
Kyungpook National University, Korea
Email: sjkoh@knu.ac.kr
-
Wen Luo
ZTE
No.68, Zijinhua RD,Yuhuatai District, Nanjing, Jiangsu 210012, China
Email: luo.wen@zte.com.cn
-
Marco Liebsch
NEC Laboratories Europe

Email: liebsch@neclab.eu
-
Carl Williams
MCSR Labs
Email: carlw@mcsr-labs.org
-