Internet-Draft
Expires: December, 2002

Yoshihiro Ohba (Editor)
Subir Das
Basavaraj Patil
Hesham Soliman

June 17, 2002

Problem Space and Usage Scenarios for PANA

<draft-ietf-pana-usage-scenarios-02.txt>

Status of This Memo

Abstract

Most of the commercial networks today require users (or devices on behalf of users) to provide their authentication information, such as identity, device identifier, etc., before being allowed access to network resources. Resources here include basic access to the network, specific value added services, different grade of services etc. While such networks are available in the market place, the authentication process and access control mechanisms depend upon the type of network that a user is attaching to and in most cases it is specific to an access technology. Due to the rapid proliferation of access technologies, wireless devices and next generation services offerings, a flexible authentication (which is independent of underlying access technologies) and access control mechanisms are deemed necessary. This document therefore attempts to describe several such scenarios where existing mechanisms are not sufficient

and finally argue the need for a new higher layer protocol called PANA (Protocol for carrying Authentication for Network Access). It also helps to understand the problem space clearly and facilitate the discussion for PANA requirements and framework.

Table of Contents

1 Terms 2
1.1. Acronyms 2
1.2. Terminology 2
2. Problem Space 4
3. PANA Model 6
3.1. Simple PANA Model 6
3.2. Advanced PANA model 7
3.2.1. PAA Co-located with Access Router 8
3.2.2. PAA Separated from Access Router 9
4. Usage Scenarios 9
4.1. Initial Authentication Timing 9
4.2. Multiple Access Routers 10
4.3. Multiple-Interface Device 10
4.4. PANA as a Per-packet Protection Enabler 11
5. Security Consideration 11
6. Acknowledgments 12
7. References 12
8. Authors' Information 12

1 Terms

1.1. Acronyms

AAA: Authentication, Authorization and Accounting

AP: Access Point

AR: Access Router

DSL: Digital Subscriber Line

EAP: Extensible Authentication Protocol

GPRS: General Packet Radio Service

LSA: Local Security Association

PDP: Packet Data Protocol

NAS: Network Access Server

PAA: PANA Authentication Agent

PaC: PANA Client

PPP: Point-to-Point Protocol

1.2. Terminology

Following terminologies are defined for this document. See also [PANAREQ].

Device

A network element (namely notebook computers, PDAs, etc.) that requires access to a provider's network.

Device Identifier (DI)

The identifier used by the network as a handle to control and police the network access of a PANA client. Depending on the access technology, identifier might contain any of IP address, link-layer address, switch port number, etc. of a device. PANA authentication agent keeps a table for binding device identifiers to the PANA clients.

Edge Subnet

The immediate IP subnet that is available to an interface of the device for network access.

PANA Client (PaC)

An entity in the edge subnet who is wishing to obtain network access from a PANA authentication agent within a network. A PANA client is associated with a device and a set of credentials to prove its identity within the scope of PANA.

PANA Authentication Agent (PAA)

An entity in the edge subnet whose responsibility is to authenticate the credentials provided by a PANA client and grant network access service to the device associated with the client and identified by a DI.

Access Point

A first-hop wireless L2 attachment point from the device in the edge subnet.

Access Router

A router in the edge subnet.

Local Security Association (LSA)

A temporary security association between a PaC and a PAA, which is derived from credentials of the PaC during initial authentication.

Initial Authentication

Authentication performed when a device enters into the edge subnet and provides the credentials to be authorized for network access without having any a priori authorization information. This will require a PAA to verify the credentials either locally or by using a back-end authentication infrastructure.

Re-authentication

Authentication that occurs when a device needs to extend the authorization lifetime, changes attributes such as, IP address and/or MAC address, etc., for the same network access after successful initial authentication. This may require a PAA to verify the credentials (used for initial authentication) either locally or by using a back-end authentication infrastructure.

Local re-authentication

A type of re-authentication that occurs locally between a PaC and a PAA by using the LSA established between them. In this type of re-authentication, the PaC does not use the same credentials as used for initial authentication.

Higher Layer

A layer that is higher than layer two.

2. Problem Space

Today's technologies mostly rely on access specific authentication mechanisms (i.e., L2 authentication mechanisms) for network access. For example, PPP has a built-in mechanism for peer authentication [RFC1661] and IEEE 802 networks define a port-based network access control with peer authentication in point-to-point LAN segments [802.1X]. However, it is not guaranteed that L2 authentication is always available in the edge subnet as long as authentication for establishing L2 connectivity is not a mandatory part in the specification of an L2 protocol. For example, the best current practice of Ethernet links that are composed of legacy hubs and switches does not use 802.1X authentication. This leads to the following need:

i) Need for authentication over L2 links that do not support an appropriate authentication mechanism.

In order to satisfy this need where authentication for network access is required, a higher layer protocol for authentication is appropriate. PPP over Ethernet [PPPoE] is currently used for both client authentication and IP packet encapsulation over Ethernet over DSL, however, it was not intended to be used for authentication over multi-access links, and more appropriate authentication carrier protocol that does not require PPP encapsulation over multi-access links is deemed necessary.

It is a common practice to use higher-layer authentication on top of link-layer authentication. For example in 3GPP and 3GPP2, PPP is used for authentication after link-layer authentication succeeds. Or, http-redirect method is used as a higher-layer user authentication in some other network access architectures. This leads to the following need:

ii) Need for L3 authentication separated from L2 authentication

Multi-layer authentication is necessary when each authentication layer is associated with a different level of network access authorization. For example, when an ASP (Access Service Provider) provides hot-spot wireless access service from which a user device can connect to its own ISP(s), it is possible to use L2 authentication to access one of the ASPs in the hot-spot area, but higher layer authentication is needed when connecting to one of its ISPs.

Due to the rapid proliferation of access technologies, wireless devices are becoming very popular. On the other hand, these technologies demands different kinds of authentication, such as:

iii) Need for local re-authentication

Re-authentication is necessary at least in the following situations:

a) If the underlying access network does not have a capability to detect physical disconnection of devices, periodical re-authentication is necessary for minimizing the impact of attacks (e.g., free riding) due to IP address and/or MAC address spoofing, which would possibly occur when the device is shutdown or the user leaves the edge subnet with the device without performing explicit log-off from the local network.

b) If there is a change in attributes (e.g., IP address and/or MAC address) of a device, re-authentication is necessary in order to make sure that the proper change is informed by the entity that was once authenticated successfully.

It is also important that re-authentication is performed locally between the PaC and the PAA without involving other network entities. However, there might be some instances where re-authentication with help of back-end authentication infrastructure is necessary in addition to local re-authentication, considering security for accounting such as non-repudiation.

With regard to case (a), considering mobile and wireless environments, it is possible that a device has multiple wireless interfaces and switches frequently from one interface to another in the same administrative domain. This type of switching can occur with or without changing an IP address based on variable requirements (e.g., power saving vs. throughput). In this

scenario, re-authentication is necessary for the new interface to be authorized for network access, and it is important that re-authentication is performed locally between the PaC and the PAA for fast interface switching. The need for local re-authentication for interface switching immediately leads to a need for another access-independent authentication mechanism that supports:

- an access technology independent authentication protocol for providing a generic method for local re-authentication among different interfaces, AND

- an access independent PaC identifier for associating the different interfaces with the same LSA that is used for local re-authentication.

Local authentication described above should be taken into account when designing and implementing an L3 authentication carrier protocol (and any sort of authentication carrier protocol as well).

In conclusion, we anticipate that a higher layer protocol like PANA (Protocol carrying Authentication for Network Access) will satisfy all of the above needs that are emerging.

3. PANA Model

Following sub-sections capture the PANA usage model in different network architectures with reference to its placement of logical elements such as, PANA Client (PaC) and PANA Authentication Agent (PAA).

3.1. Simple PANA Model

Figure 1 describes a simple architecture in which PAA resides on the first hop access router (AR) and PaC on behalf of a device (D1, D2,.. etc) communicates with PAA for network access. As shown in figure, PaC can use different L2 interfaces to connect to the first hop access router. PAA may or may not use AAA infrastructure to verify the credentials of PaC and grants or deny the device (belongs to that particular PaC) to access the network resources. PANA in this case provides a means to transport the authentication parameters from the PaC to PAA securely. PAA understands how to verify the credentials. After verification, PAA sends back the success or failure to PaC. Although the AR would be the access control enforcement point in this case, PANA does not play any explicit role in performing access control except that it provides a hook to access control mechanisms.

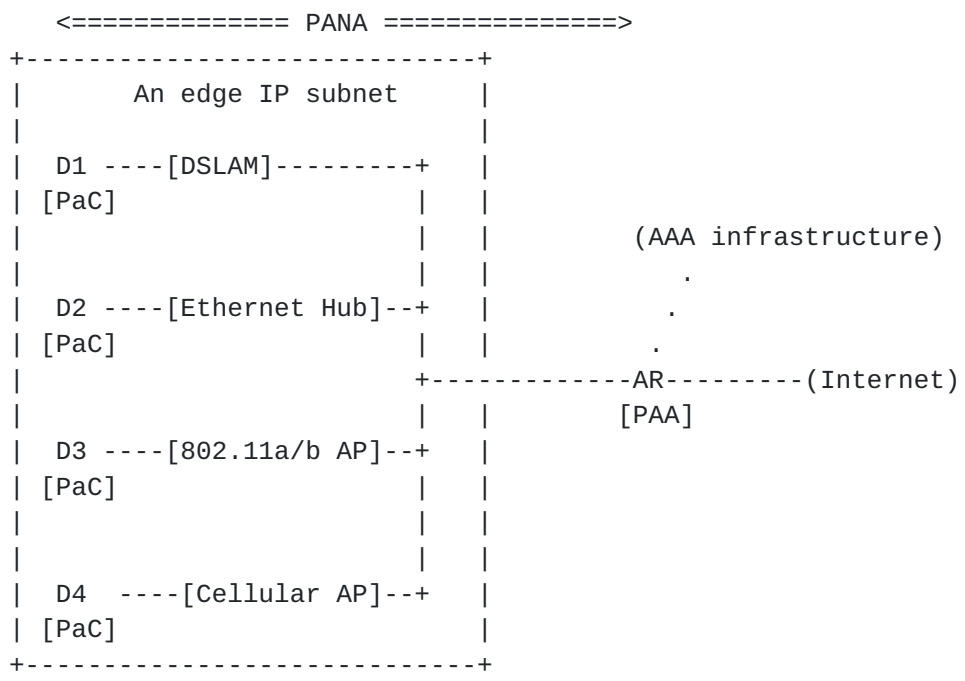


Figure 1: An example of simple PANA model

3.2. Advanced PANA model

Figure 2 presents an advanced architecture where, multiple routers are placed in an edge subnet and the device has one or more interfaces. For simplicity, optional connection to AAA infrastructure is not shown in the figures of this section. Each interface of a device supports a specific L2 type. Thus the edge IP subnet consists of one or more L2 segments, where those segments can be different L2 types. PANA can support this advanced architecture in two different ways: (i) co-location of PAA with access router and (ii) separation of PAA from access router. Although this section describes generic models, more detailed issues on multiple access routers and multiple-interface devices are provided in section "Usage Scenarios".

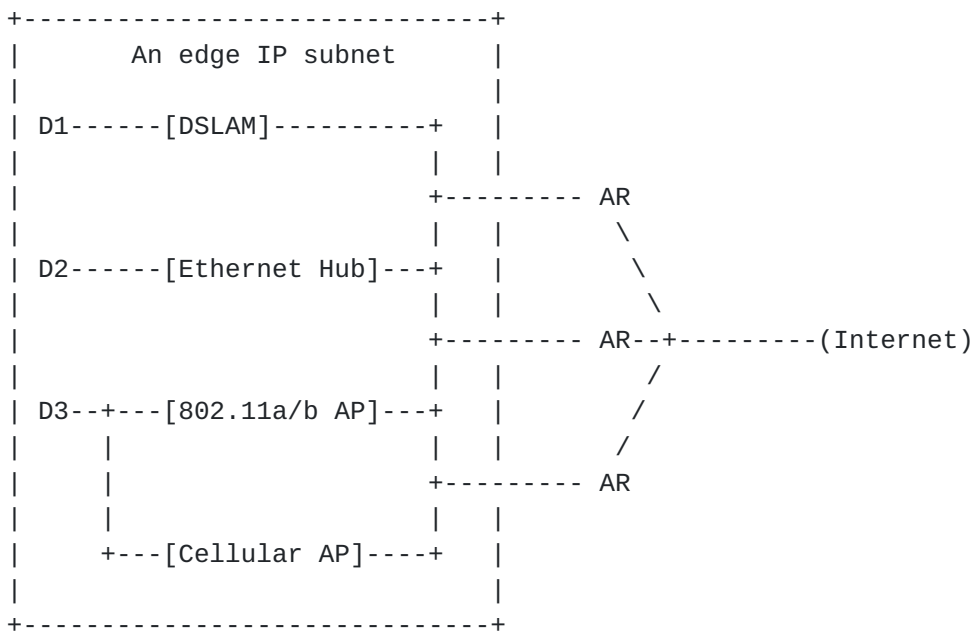
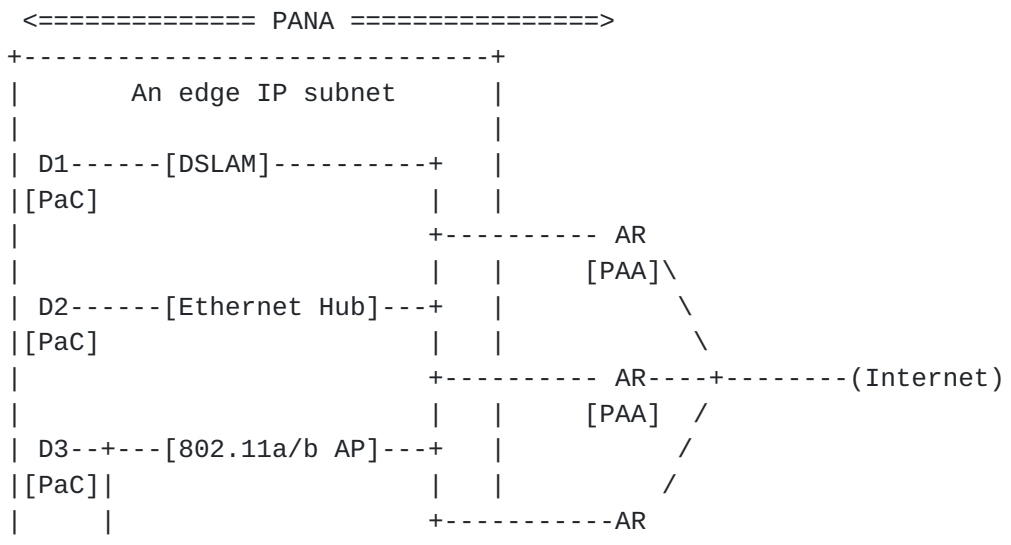


Figure 2: An example of Advanced Architecture

3.2.1. PAA Co-located with Access Router

In this scenario (Figure 3), multiple PAAs can co-exist especially when there are multiple access routers in the edge subnet. PAAs are co-located with these access routers on which access control is performed. When a PaC needs to be authenticated and authorized for network access it exchanges PANA messages (as described above) with a PAA.



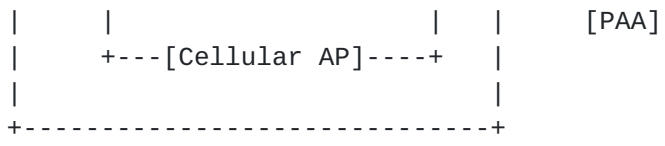


Figure 3: An example of Advanced PANA Model
[PAA co-located with AR]

3.2.2. PAA Separated from Access Router

Figure 4 describes this model. In this scenario, PAA is not co-located with AR but resides on the edge subnet. PaC exchanges the same messages with PAA as discussed earlier. The difference here is when initial authentication for the PaC is successful, access control parameters are to be distributed to all access routers residing in the edge subnet so that the device that PaC resides is authorized at all the access routers. However, PANA does not provide any mechanism how access control parameters are to be distributed. This is in fact outside the scope of PANA.

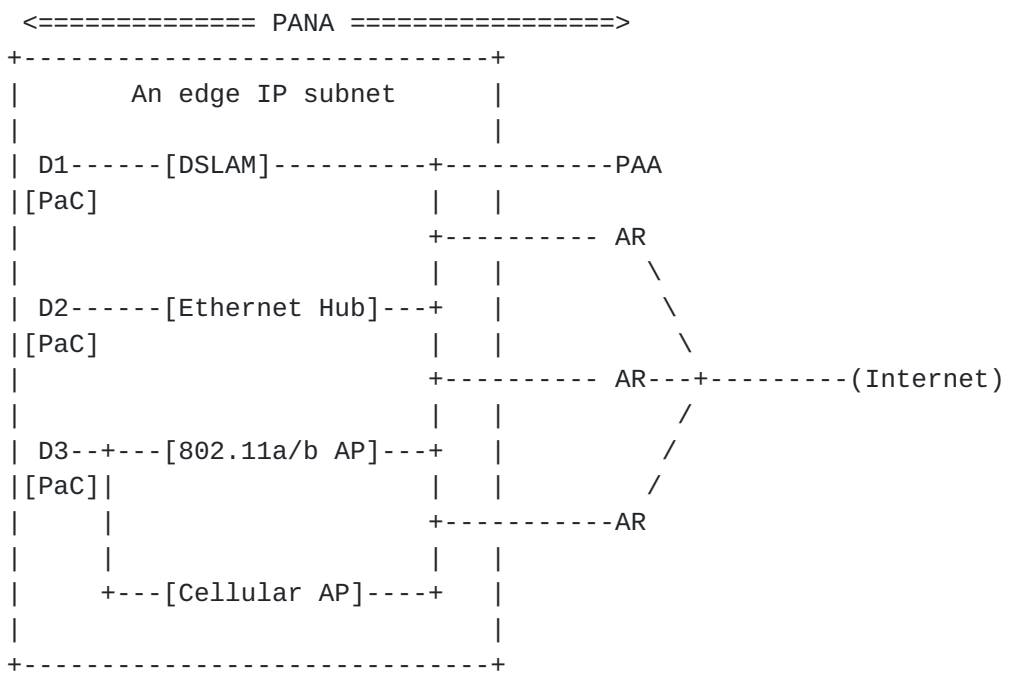


Figure 4: An example of Advanced PANA Model
[PAA separated from AR]

4. Usage Scenarios

4.1. Initial Authentication Timing

There are two possible scenarios with regard to the timing at which initial authentication occurs, i.e., initial authentication can occur before or after IP address configuration. Note that "IP address configuration" in this document means configuration of an IP address that needs to be authorized for network access, and thus configuring an IPv6 link local address or any temporal IP address that is used

only for authentication purpose and not necessarily authorized for network access is excluded from the definition of "IP address configuration."

There are a number of situations where authentication before IP address configuration would be important, for example:

a) If strict access control is required or the IP address resource

used for network access is scarce, authentication should occur before IP address configuration.

b) If an AP supports multiple VLANs and it is possible to dynamically associate a device with one of the VLANs depending on the authentication and authorization result, initial authentication should occur before IP address configuration.

c) If a distinct IPv6 64-bit prefix can be assigned to each PDP context in GPRS[GPRS] or to each subscriber of DSL or cable internet, initial authentication should occur before IP address configuration.

On the other hand, initial authentication after IP address configuration would be useful for providing a network access service in which access to local information such as local-area map and flight information for free of charge, while access to specific external web-sites is subject to charge.

4.2. Multiple Access Routers

In multi-access environments, such as IEEE 802 networks, it is possible for multiple ARs to coexist on the same shared media. In such a scenario, it would be desirable to use multiple ARs in a way that traffic coming from and going to a specific device always goes through a single AR for ease of access control, but traffic from different devices diverges over multiple ARs for the purpose of load balancing and redundancy. If such a routing control is performed, it would be desired to perform authentication via the same AR. This is one scenario where Figure 3 of the advanced PANA model is applied. On the other hand, there are some cases in which such a routing control would not be possible.

For example, if we consider to use "ICMP Redirect or IPv6 Host to Router Load Sharing" [Hinden] mechanism, either Figure 3 or Figure 4 of the advanced PANA model would be applied. Anyway, additional mechanisms would be required for distributing access control parameters from one PAA to other access router(s) that are not physically co-located with the PAA. In other words, the types of routing control would affect the location of PAA as well as the way of access control in multi-AR environments.

The multi-AR scenario also addresses the issue of multiple providers on the same shared media, i.e., each AR may not be administered by the same provider. In this case, it would be necessary for PANA to have a mechanism to provide the identity of PAA(s) for a PaC so that the PaC can choose an appropriate provider to access.

4.3. Multiple-Interface Device

A device can have multiple interfaces of homogeneous or heterogeneous technologies. Thus, there are two possible scenarios for PANA: multi-homing and interface switching.

In case of multi-homing, the multiple interfaces of a device may be activated at the same time for various requirements such as increased bandwidth, load balancing and reliability. PANA should provide a way for the PaC of the device to perform initial authentication and local re-authentication for each interface.

In case of interface switching, it is important to use an access-independent authentication mechanism (as described in section 2). This access-independent authentication mechanism allows a PaC to perform local re-authentication with a PAA when interface switching occurs.

4.4. PANA as a Per-packet Protection Enabler

Although PANA itself does not define key distribution protocol and mechanism, it is possible to use PANA to enable per-packet protection mechanism (such as IPsec and WEP) to secure communication in the edge subnet, if the authentication carrier protocol that is used by PANA supports key distribution mechanism. Note that using PANA for WEP key distribution would be useful (if implemented appropriately) when L2 authentication is null or does not have key distribution capability.

5. Security Consideration

We anticipate following security issues or concerns relating to a higher layer protocol such as PANA.

- Consideration for Eavesdropping

  Since PANA protocol carries authentication information, consideration is necessary for preventing confidential part of the credentials of a PaC from being known by eavesdroppers in the edge subnet. The eavesdroppers include users and operators in the local network.

- Consideration for Denial of Service Attacks

  Since PANA protocol is used for authentication, consideration is necessary for preventing authentication of a legitimate PaC from being denied as a result of processing PANA messages sent from attackers. Next, since both initial authentication and re-authentication would require cryptographic computation on both PaC and PAA, consideration is necessary for both PaC and PAA not to spend CPU and memory resources for processing PANA messages sent from an attacker more than that is spent by the attacker to

attack. The attackers may or may not be on the same link as the PaC or PAA.

Additionally, since during initial authentication PAA may use back-end authentication infrastructure, consideration is necessary to prevent the authentication infrastructure from being attacked via PAA while using PANA.

- Consideration for Man-In-The-Middle Attacks

  Consideration is necessary for preventing the communication between PaC and PAA from being spoofed by an attacker in between. The attacker could be on the same edge subnet as PaC and PAA, e.g., by putting a bogus access point between a PaC and a PAA in the edge subnet.

6. Acknowledgments

The authors would like to thank James Carlson, Jacques Caron, Paal Engelstad, Henry Haverinen, James Kempf, Thomas Narten, Erik Nordmark, Phil Roberts, David Spence, Barani Subbiah, George Tsirtsis, Cliff Wang, Alper Yegin and the rest of the PANA Working Group for the ideas and support they have given to this document.

7. References

[802.1X] IEEE Standard for Local and Metropolitan Area Networks, "Port-Based Network Access Control", IEEE Std 802.1X-2001.

[EAPSRP] J. Carlson, et al., "EAP SRP-SHA1 Authentication Protocol", Internet-Draft, Work in progress, July 2001.

[GPRS] R. Bates, "GPRS", McGraw-Hill TELECOM, ISBN 007138188, 2002.

[Hinden] R. Hinden, "IPv6 Host to Router Load Sharing", Internet-Draft, Work in progress, January 2002.

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

[PANAREQ] A. Yegin, et al., "Protocol for Carrying Authentication for Network Access (PANA) Requirements and Terminology", Internet-Draft, Work in progress, February 2001.

[PPPoE] L. Mamakos, et al., "A Method for Transmitting PPP Over Ethernet (PPPoE)", RFC 2516, February 1999.

[RFC1661] W. Simpson, "The Point-to-Point Protocol (PPP)", RFC 1661 (STD 51), July 1994.

[RFC2284] L. Blunk, et. al., "PPP Extensible Authentication Protocol (EAP)", RFC 2284, March 1998.

8. Authors' Information

Yoshihiro Ohba
Toshiba America Research, Inc.
P.O. Box 136
Convent Station, NJ 07961-0136
USA
Phone: +1 973 829 5174
Fax: +1 973 829 5601

Email: yohba@tari.toshiba.com

Subir Das
MCC 1D210R, Telcordia Technologies
445 South Street, Morristown, NJ 07960
Phone: +1 973 829 4959
email: subir@research.telcordia.com

Basavaraj Patil
Nokia
6000 Connection Dr.
Irving, TX. 75039
USA
Phone: +1 972-894-6709
Email: Basavaraj.Patil@nokia.com

Hesham Soliman
Ericsson Radio Systems AB
Torshamnsgatan 29,
Kista, Stockholm 16480
Sweden
Phone: +46 8 4046619
Fax: +46 8 4047020
E-mail: Hesham.Soliman@era.ericsson.se