FMC Working Group
Internet-Draft
Intended status: Informational
Expires: April 25, 2013

S. Durel
France Telecom
H. Moustafa
Intel Corporation
R. Schott
Deutsche Telekom
October 22, 2012

Requirements in Fixed Mobile Convergence
draft-schott-fmc-requirements-04

Abstract

This document provides provides technical requirements in Fixed Mobile Convergence for the two use cases of group identification and user equipment mobility in fixed network.

Requirements Language

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 RFC 2119 [RFC2119].

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 http://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 April 25, 2013.

Copyright Notice

Table of Contents

1. Introduction

In the FMC (fix/mobile convergence) network, the major convergenced aspects include the converged business and service, converged network and infrustructure, and converged user management and terminals [TR203].

With network heterogeneity and huge demand of multimedia and audio-visual services and applications as a given, users' satisfaction is the aim of each service provider to reduce churn, promote new services and improve the ARPU (Average Revenue per User). The market is crowded. Many players provide Internet and entertainment services, which motivates new business models considering users' experience and considering roaming agreement between different operators. New expectation for users' consumption style focuses on personalized and interactive usage. This allows users on one hand to share content across many devices and with other users, but on the other hand to access all content seamlessly at the touch of a button.

The converged business will provide the customer with a uniform policy and user experience. It can be seamlessly and intuitively accessible across all devices and all networks. The converged network and infrustructure will reduce the CAPEX and OPEX for operators, and incur minimal additional costs with the ever-changing business model. The converged user management and terminals will offer a more simple and convenient user experience, which will deliver broadband connectivity and standardized multimedia services to a wide range of devices, including media servers, video cameras, portable media players, PCs and mobile phones [TS23.203].

The purpose of this document is to provide some technical requirements specific to FMC scenario. It can be regarded as a motivation to encouraging standardization work in IETF in those areas.

2. Use case 1: Group Identification

The goal of our model is to enforce certain unified policy control for consumer's service by means of grouping the consumer's devices for management. This enforcement allows control over the subscriber level who can share the subscription among several devices. This group can be configured in the subscription server of the operator. This device group for subscriber management could be defined as subscriber ID.

Subscriber ID used for unified service management can be constructed based on the requirements of:

1. Subscriber ID is assigned by the ICP/ISP or operators, and

2. Subscriber ID determine which traffic policy such as QoS are enforced by the nodes inside the network, and

3. Subscriber ID could be configured in the subscription server of the operator or ICP/ISP, and

4. Subscriber ID is combined with the subscriber information.

5. Subscriber ID may correspond to the device identifiers, such as ISIM, etc. And the ID should be kept unchanged in the Carrier Grade Network Address Translation (CGN) devices.

The rules of this ID could be set through administrative rules, which is out the scope of this document. The devices of the consumer and the operator must have the consistent ID for the same management group. A differentiated service-compliant network node can provide differentiated policy enforcement and packet scheduling mechanism based on this kind of ID.

Consider an ISP assign a subscriber-id to the customer, the customer can not only use this subscriber-id to access the network, but also use some applications (operator’s service or third-party service) without additional appliance or authentication.

One subscriber may have multiple devices, including PC, mobile phones, ipad, etc., and may seamlessly move across multiple heterogeneous networks. With this unified user Identication, the customer can log in different application systems with a single access control. Besides, operators and Content providers can also apply the unified access policy, accounting policy, etc., to the customer for the specific set of devices.

Potencial Technical Issues:

Two different types of identifiers play an important role in this case: Device Identifier and Subscriber Identifier. The Device Identifier is used to indicate each individual devices for the customer, and the Subscriber Identifier is used to indicate a customer under the same policy, e.g. accouting policy, priority profile, etc. One Subscriber Identifier may correspdent to multiple Devices Identifiers. These Identifiers should be kept unchanged in the CGNs.

3. Use case 2: Requirements for UE Mobility in Fixed Broadband Network

Regarding the requirements for MN (Mobile Node) mobility in fixed broadband networks two use cases can be distinguished. One is the mobility between different access technologies e.g. WiFi and 3 GPP access and the other is the mobility in a WiFi scenario.

Customer service should be guanranted during the switch between one access network to another. For example, customer’s call or video service shouldn’t be interrupted when moving from 3GPP access to WiFi access techonology. The services depend on the substantive of customer’s profile and it is important to confirm the device identification binding or updated accordingly for the same moving device.

The following are the requirements for the User Equipment Mobility in Fixed Broadband Network:

- Handover between networks while the session is active according to the network status with the change in the MN attachment.

- Mechanisms and interfaces between operators or/and access networks SHOULD be deployed to manage the mobility of the traffic flows of their users.

- Mobility should be enabled whether or not coverage areas overlap.

- Differentiated Services for the mobile device (MN)

- Service guarantee when device is roaming or mobile

- Resiliency in the network nodes should be provided

Potential Technical Issues:

The potential issues for the mobility use case is device identification suitable for mobility requirements, IP address reserved techonology, QoS or UE information communication between different access networks, mobility technology in WiFi scenario.

4. IANA Considerations

5. Security Considerations

This document focuses on FMC requirements and the interworking of "WiFi, 3G, etc..." and should not give rise to any new security

vulnerabilities beyond those described in IPSec [RFC4301], TLS [RFC5246] or SRTP [RFC3711]. Nevertheless an open network architecture aimed at fulfilling the requirements listed in this document may give rise to security issues not yet identified.

6. Acknowledgements

TBD

7. References

7.1. Normative References

[RFC0768] Postel, J., "User Datagram Protocol", STD 6, RFC 768, August 1980.

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

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

[TS23.203] "3GPP TS23.203, Policy and Charging control architecture", September 2012.

7.2. Informative References

[TR203] "Broadband Forum Technical Report TR-203, Interworking between Next Generation Fixed and 3GPP Wireless Access", August 2012.

Authors' Addresses

Sophie Durel
France Telecom
Rennes, 35000
France

Phone:
Email: sophie.durel@orange.com

Hassnaa Moustafa
Intel Corporation
Hillsboro, OR,
United States

Phone:
Email: hassnaa.moustafa@intel.com

Roland Schott
Deutsche Telekom
Darmstadt, 64295
Germany

Phone:
Email: Roland.Schott@telekom.de