Network Working Group
Internet-Draft
Expires: March 25, 2013

S. Durel
France Telecom
H. Moustafa
Orange Labs
R. Schott
Deutsche Telekom
C. Perkins
Futurewei

September 21, 2012

Requirements for Fixed Mobile Convergence
draft-schott-fmc-requirements-03

Abstract

Fixed-mobile convergence encompasses a variety of use cases that include situations in which a wireless device travels between a point of attachment in a mobile network (such as a cellular base station) and another point of attachment anchored in a fixed network such as a WiFi hotspot. Convergence then means enabling an end-user to access services or retrieve content whatever the network access conditions (e.g., fixed or mobile access infrastructure), and whether the end-user is in motion or not. This document discusses the issues related to convergence and elaborates a set of requirements.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

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. The 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.

Consequently, Quality of Experience (QoE) has become a crucial determinant of the success or failure of the multimedia and audio-visual applications and services. QoE evaluates the users' perceived quality for the provided services and hence reflects the users' satisfaction. Regarding QoS, 3GPP has made architectural definitions as described in [TS23.203] and [TS29.212]. IETF has also described how QoS can be achieved over IP [RFC5865].

Various meanings can be ascribed to the term Fixed-Mobile Convergence. It is not the intention of this document to give a complete definition regarding business and technical aspects. Fixed-mobile convergence has recently been used to include various use cases in which a wireless device travels between a point of attachment in a mobile network (such as a cellular base station) and another point of attachment anchored in a fixed network such as a WiFi hotspot. [samog]Convergence refers to a perceived unification of the service level available to applications which is, to the extent feasible, independent of the nature of the underlying physical medium.

This document discusses issues raised by convergence and elaborates a set of requirements based on the problem statement and use cases as discussed in [I-D.xue-intarea-fmc-ps] and [I-D.sun-fmc-use-case]. These use cases have been under discussion in BBF [WT203] and 3GPP [3GPP.22.278] respectively [3GPP.22.234]. The requirements discussed in this document are meant to help the IETF community to decide whether it should take part of the corresponding effort or not.

2. Caution

This document is a working tool to help assessing whether additional specification effort is required within IETF. Technical issues mentioned in this document are those which may require carrying out a specification effort within IETF.

The goal of this document to enable the analysis of technical issues and their requirements. These issues are relevant to particular use cases. The relevant use cases and associated requirements need thorough discussion.

Some of these technical issues are already covered by some existing IETF WGs. This document may provide motivation to advance such items in the standardization process.

3. Terminology

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 specified in [RFC2119].

The following additional terms are used in this document.

aggregation node
The access network node which connects CPE and UE devices to the Internet.

Codec
Compression/Decompression of multimedia data using either a hardware device or software.

CPE
Customer Premises Equipment, that is equipment found in the customer’s physical location and provided by the network operator or service providers. DSL routers, Set-Top-Box (STB), and decoders are examples of CPE.

FMC
Fixed Mobile Convergence means enabling an end-user to access services or retrieve content whatever the network access conditions (e.g., fixed or mobile access infrastructure), and whether the end- user is in motion or not. This includes also access conditions with this own service profile although having access by a 3rd party.

host_id
an identifier for the wireless device, as described in [I-D.ietf-intarea-nat-reveal-analysis].

MN

"Mobile Node"; a device that can move from one wireless point of attachment to another. Other standard documents use different terminology for the same idea, for instance "UE" (for User Equipment), or AT (for Access Terminal).

NFC Identifier

Near Field Communications identifier.

Port set

a defined set of ports; in this document "port set" is used as an example of a host_id. Each host under the same external IP address is assigned a restricted port set. These port sets may then be advertised to remote servers. Port sets assigned to hosts may be static or dynamic.

SD

Standard Definition for video using a standard resolution.

HD

High Definition for video using an enhanced resolution.

4. Architecture Overview

In practice multiple scenarios like non-roaming or roaming and access via trusted or untrusted WLAN access are possible. To give a reference architecture we referring to [samog] and [ieee802.11]. The reference architecture describes how access to 3GPP via a GTP-based S2a and PMIP networks is possible.

Requirements of the architecture are :

REQ1: Access to EPC resources/services with access control by the operator

REQ2: Seamless mobility between 3GPP and WLAN for EPS services with IP address preservation

REQ3: Non-seamless mobility services between 3GPP and WLAN for EPS services: no IP address preservation

REQ4: Support of UEs with single PDN connection; support of UEs with multiple PDN connections

REQ5: Access to EPC via WLAN simultaneously with non-seamless WLAN offload

General requirements for FMC are common service and subscriber profiles. Additionally common charging, operational and management procedures are also required. Additional requirements for IP traffic offload are described in [TR23.829]. The benefit of using traffic offload is to save frequency range and to allow access in areas where cellular coverage is not available.

For one, operators see a potential in simplifying their operational/ user support complexity, as well as harmonizing network element functionality around the IP protocol. Operators running multiple access networks also view IP service delivery as the key lowest common denominator towards delivering common services in a converged network. The service provider community have shown significant interest in migrating from a pure PPP access environment towards one with IP subscriber sessions for delivery of all IP broadband services in fixed networks [WT146]. With LTE respectively EPC the mobile networks are also introducing a pure all IP mobile broadband access.

Probably in the end everything is mobile. One can also presume that everything is all IP having only agnostic access networks. For operating those networks appropriate enough IP address space [RFC6264] and security features like Internet Key Exchange Protocol Version 2 [RFC5996] respectively [I-D.so-ipsecme-ikev2-cpext] are required.

The following figure is a brief overview how fixed and mobile networks could interwork:

```
                                                     +---------+
                       +-----------+      +------+   |         |
                       |           |------| TWAP |---|         |
     +----------+      |  WLAN     |      +------+   |   3GPP  |
     |    UE    |------|  ACCESS   |                 |   Home  |
     +----|-----+      |  Network  |      +------+   | Network |
          |            |           |------| TWAG |---|         |
          |            +-----------+      +---|--+   |         |
          |-----------------------------------|      +---------+
                 Trusted non - 3GPP WLAN

            Legend:
            UE   User Equipment
            TWAG Trusted WLAN Access Gateway
            TWAP Trusted WLAN Access Proxy
```

This FMC Architecture described in [samog].

Figure 1: FMC Requirement Architecture

5. Requirements for MN Identification behind a CPE with NAT

A popular deployment model in fixed networks is to provide a host with a single private IPv4 address at the home or small business LAN. Then, each host within the local network will be assigned a private IPv4 address; a NA(P)T function [RFC2663] is responsible for translating the private IPv4 address to the public IPv4 address assigned to the CPE (Customer Premises Equipment). Similar address translation features are also present now in mobile environment; as one example, CPE can be connected to mobile infrastructures.

IP address sharing is motivated by a number of different factors. And today, some servers use the source IPv4 address as an identifier to treat some incoming connections differently. Due to the use of NAT44 [RFC3022] and NAT64 [RFC6146]), that address will be shared. In particular, when a server receives packets from the same source address, because this address is shared, the server does not know which host is the sending host [RFC6269]. To be able to sort out the packets for each sending host, the server must have extra information in addition to the source IP address, to distinguish the sending host. This identifying information is called the "host_id".

As a general matter, the HOST_ID proposals do not seek to make hosts any more identifiable than they would be if they were using a public, non-shared IP address. However, depending on the solution proposal, the addition of host_id information may allow a device to be fingerprinted more easily than it otherwise would be. Should multiple solutions be combined that include different pieces of information in the host_id, fingerprinting may become even easier.

A set of solution candidates to mitigate some of the issues encountered when address sharing is used have been described and compared in [I-D.ietf-intarea-nat-reveal-analysis]. Among or aside this set of solutions, a mechanism will have to be recommended to supply host_id in the use cases described in Section 6 as well as in [I-D.xue-intarea-fmc-ps] and [I-D.sun-fmc-use-case].

A CPE can also be configured to offer a shared WiFi to any visiting host (also called Mobile Node, or simply MN) which does not belong to the subscriber (owning the CPE). A visiting MN uses that shared WiFi facility to access its services. Granting access to the service is usually conditioned by an access control phase (e.g. redirection to captive portal inviting the user to authenticate). Once access to the service is granted, the visiting MN can receive its services. Business model considerations for such service offerings are out of scope for this document.

Among various ways to offer shared WiFi service, operators may elect to re-use the NAT function embedded in the CPE to route the traffic issued from the visiting MN.

When the traffic of a visiting MN is multiplexed behind the same public IP address, upstream devices may be unable to distinguish the the traffic of the visiting MN from other traffic issued by devices belonging to the subscriber owning the CPE. This traffic identification may be required to enforce dedicated policies (e.g., Accounting, QoS policies, legal intercept, legal data storage, etc.). As a result, and in order for the operator to still support traffic management for this service, policy control/decision/enforcement MUST be based on the specific MN. In other words, traffic belonging to a visiting MN MUST be explicitly identified. The host_id jointly with the external IP address can be used for this purpose.

As one example, port sets can be used as a host-id. To illustrate, suppose the CPE assigns a private IPv4 address and a set of ports to a visiting MN. Then, the CPE can report the assigned port set to a aggregation node together with other information such as external IPv4 address, MAC address, etc. This information will be associated with the user-id provided during the authentication phase. The CPE then uses that port set for translating packets to and from that visiting MN. The set of ports (assigned by the CPE) and the external IP address (assigned to the CPE) are then sufficient to uniquely identify a MN. The reporting phase can be avoided if the CPE is pre-configured with a static list of port sets to be used for visiting MNs.

The use of port sets and some other methods to explicitly identify a visiting MN is discussed in [I-D.ietf-intarea-nat-reveal-analysis], but many other methods of identification are also possible. In order to ease the selection of the appropriate host-id solution for the FMC case, below are listed a set of requirements to be met:

- All traffic MUST be identifiable (including TCP, UDP and ICMP)
- The MN SHOULD be authenticated if it injects its own host-id
- Otherwise, the CPE SHOULD inject the host-id
- The CPE SHOULD strip any existing host-id
- The CPE and the aggregation node MUST support at least one common method to convey host-id.

5.1. Recommendations for MN Identification behind NAT

We recommend dedicated efforts to specify a mechanism to supply host-id for MNs behind CPE and NAT.

A solution analysis document for existing solution approaches would help.

6. Requirements for MN Mobility in Fixed Broadband Network

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

- o Handover between networks while the session is active according to the network status with the change in the MN attachment.
- o Mechanisms and interfaces between operators or/and access networks SHOULD be deployed to manage the mobility of the traffic flows of their users.
- o Mobility should be enabled whether or not coverage areas overlap.
- o Differentiated Services for the mobile device (MN)
- o Service guarantee when device is roaming or mobile
- o Resiliency in the network nodes should be provided

7. Requirements for Link Characteristic Information

Today the MN e.g. smart phones are reachable through multiple interfaces and have the possibility to use these interfaces simultaneously. Thus roaming between different access technologies is required. Due to the fact that wireless access link is most likely the bottleneck of end-to-end communication causing a significant portion of end-to-end delay delivery of link respectively sub-path characteristic information from one MN to the other can be used to optimise IP mobility performance by altering the end-to-end path properties.

Unfortunately, existing IP mobility, transport and application layer protocols do not provide any facility to indicate which type of link the MN is currently attached to or what kind of changes there were on the local access link. Local access link characteristic may also vary significantly as a result of handover between links on the same type (horizontal handovers) [I-D.korhonen-mobopts-link-characteristics-ps].

Existing mobility protocols do not provide a mechanism to indicate which type of link the MN is currently attached to. Therefore some new signalling mechanism is needed also avoiding the amount of signalling traffic load.

The benefit of such signalling mechanism is to avoid complications to the IP transport and the service quality as many applications and congestion control mechanisms fail to respond fast enough if path characteristics change suddenly.

7.1. Adaptive Application and Services

Adaptive applications benefit from standardised mechanisms that notifies abrupt changes of link characteristics [I-D.korhonen-mobopts-link-characteristics-ps]. Streaming service e.g. for video or music can adapt to the new connection conditions. Assuming that a mobile device can connect to the network using various access technologies and moves from macro cellular access to 802.11 WLAN an adaptive application could immediately scale the service in an appropriate manner.

7.2. Network-Initiated Handover

In a FMC scenario the MN desires to handover to another access network possibility based on the required service quality or other reasons like administrative policies. With link characteristic information delivery mechanisms the network and the remote MN would have the knowledge to make these decisions.

7.3. End-to-End path characteristics

To deliver link characteristic information, the MN has to get its access link characteristic dynamically [I-D.korhonen-mobopts-link-characteristics-ps]. Providing of event classification, event reporting or event filtering corresponding to dynamic changes in the link characteristic enables the MN to manage and control link behaviour relevant handovers and mobility. Initial measurement results on the end-to-end path characteristics can be used to inform upper layer congestion control mechanisms determining the effective end-to-end path characteristic.

7.4. Requirements for Link and Sub-Path Information delivery

The link characteristic information delivery mechanism SHOULD fulfil the following requirements.

REQ1: The link characteristic information delivery is independent of a certain IP mobility solution.
REQ2: The link characteristic information delivery SHOULD be applicable to existing mobility solutions.
REQ3: It is transport protocol independent.
REQ4: Signalling traffic load MUST be avoided.

REQ5: The mechanism MUST work when the MN is multi-homed or not.
REQ6: Link characteristic information SHOULD be exchanged prior to handover.
REQ7: Link characteristic information MUST be useable for remote peer node and/or remote network control entity.

8. 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.

9. IANA considerations

None.

10. Acknowledgments

Contributions, comments, discussions, and remarks provided by David Binet, Mohamed Boucadair, Christian Jacquenet, Daniel Park, and Pierrick Seite are gratefully acknowledged.

11. References

11.1. Normative References

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

11.2. Informative references

[RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address Translator (NAT) Terminology and Considerations", RFC 2663, August 1999.

[RFC3022] Srisuresh, P. and K. Egevang, "Traditional IP Network Address Translator (Traditional NAT)", RFC 3022, January 2001.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E., and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC5246] Dierks, T. and E. Rescorla, "The Transport Layer Security (TLS) Protocol Version 1.2", RFC 5246, August 2008.

[RFC5865] Baker, F., Polk, J., and M. Dolly, "A Differentiated Services Code Point (DSCP) for Capacity-Admitted Traffic", RFC 5865, May 2010.

[RFC5996] Kaufman, C., Hoffman, P., Nir, Y., and P. Eronen, "Internet Key Exchange Protocol Version 2 (IKEv2)", RFC 5996, September 2010.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6264] Jiang, S., Guo, D., and B. Carpenter, "An Incremental Carrier-Grade NAT (CGN) for IPv6 Transition", RFC 6264, June 2011.

[RFC6269] Ford, M., Boucadair, M., Durand, A., Levis, P., and P. Roberts, "Issues with IP Address Sharing", RFC 6269, June 2011.

[I-D.ietf-intarea-nat-reveal-analysis]
Boucadair, M., Touch, J., Levis, P., and R. Penno, "Analysis of Solution Candidates to Reveal a Host Identifier (HOST_ID) in Shared Address Deployments", draft-ietf-intarea-nat-reveal-analysis-04 (work in progress), August 2012.

[I-D.xue-intarea-fmc-ps]
Xue, L., Sarikaya, B., and D. Hugo, "Problem Statement for Fixed Mobile Convergence", draft-xue-intarea-fmc-ps-02 (work in progress), March 2012.

[I-D.sun-fmc-use-case]
Xie, C. and Q. Sun, "Use Cases and Requirements in Fixed Mobile Convergence", draft-sun-fmc-use-case-00 (work in progress), July 2012.

[I-D.so-ipsecme-ikev2-cpext]
So, T., "IKEv2 Configuration Payload Extension for Private IPv4 Support for Fixed Mobile Convergence",

draft-so-ipsecme-ikev2-cpext-02 (work in progress), June 2012.

[3GPP.22.278]
3GPP, "Service requirements for the Evolved Packet System (EPS)", 3GPP TS 22.278 10.2.0, October 2010.

[3GPP.22.234]
3GPP, "Requirements on 3GPP system to Wireless Local Area Network (WLAN) interworking", 3GPP TS 22.234 10.0.0, December 2009.

[I-D.korhonen-mobopts-link-characteristics-ps]
Korhonen, J., "Link Characteristic Information for IP Mobility Problem Statement", draft-korhonen-mobopts-link-characteristics-ps-01 (work in progress), June 2006.

[TS29.212]
"3GPP TS29.212, Policy and Charging Control (PCC) over Gx/Sd reference point", December 2011.

[TS23.203]
"3GPP TS23.203, Policy and Charging control architecture", December 2011.

[TR23.829]
"3GPP TR23.829, Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)", October 2010.

[WT146] "Broadband Forum Working Text WT-146, Subscriber Sessions", June 2011.

[WT203] "Broadband Forum Working Text WT-203, Interworking between Next Generation Fixed and 3GPP Wireless Access", December 2011.

[samog] "3GPP TR 23.852 V1.2.0, Study on S2a Mobility based On GTP & WLAN access to EPC (SaMOG) (Release 12)", July 2012.

[ieee802.11]
"Information technology - Telecommunications and information exchange between systems - Local and metropolitan area networks - Specific requirements - Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) specifications", IEEE Standard 802.11, 2008", 2008.

Appendix A. Requirements for Content Adaptation

In this case, adaptation of content format (HD/SD, codec, ...) SHOULD be possible when delivering the same content (e.g. video streaming) regardless of the access network type and of the mobile node (MN) characteristics.

A.1. Recommendations for Content Adaptation

To be able to meet above high level requirement, the content adaptation function needs to:

1. identify the user connection by identifying each MN in a separate manner. The MN identity MUST be updated during the session each time a new terminal is used. The characteristics of each MN being used needs to be known also (e.g. supported resolution, screen size, available network connectivity "WiFi, 3G, .." and the cost of using each type of available network).
2. distinguishing the MN and the CPE identification (MOTIVATION?).
3. rely on service layer monitoring (for instance through MPEG2 layer monitor for video content) SHOULD exist to choose the network best matching the service requirements.

Authors’ Addresses

Sophie Durel
France Telecom
Rennes, 35000
France

Phone:
Email: sophie.durel@orange.com

Hassnaa Moustafa
Orange Labs
Issy-Les-Moulineaux,
France

Phone:
Email: hassnaa.moustafa@orange.com

Roland Schott
Deutsche Telekom
Darmstadt,   64295
Germany

Phone:
Email: Roland.Schott@telekom.de

Charles E. Perkins
Futurewei
Santa Clara, California 94053
USA

Phone:
Email: charlie.perkins@huawei.com