FMC Working Group C. Xie
Internet-Draft Q. Sun
Intended status: Informational China Telecom
Expires: April 25, 2013 October 22, 2012

Use Cases and Requirements in Fixed Mobile Convergence
draft-sun-fmc-use-case-01

Abstract

This document provides a brief review of use cases in FMC (Fixed Mobile Convergence) architecture from operational point of view. It also provides technical requirements and problems which need be resolved in IETF. It is complementary to the existing problem statement and requirements documents.

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

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust’s Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of

publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction

In the FMC (Fixed Mobile Convergence) architecture, the major FMC could be devided into several aspects, which are the converged business and service, converged infrastructure and network, and converged user management.

The fundamental principle of FMC all starts from the consumers. With a multitude of devices to fit different personal preference, multi heterogeneous networks including fixed, 3GPP, WiFi, etc., and different business models in practice, people are getting more and more confused on how to make the decision to choose their subscriber-id, access network, etc.

The customer needs a life without barriers. 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 infrastructure 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.

While BBF and 3GPP has done a lot of work on architecture model, interface definition, etc., protocol standardization work should still be undertaken in IETF which is acceptable to all parties and cultivates a common ecosystem based on Internet protocol architecture.

The purpose of this document is provides the use cases in FMC ecosystem, together with some technical requirements and problems which need be resolved in IETF process. Some issues have been taken by some existing WGs in IETF, and some can be applied but not specific to FMC scenario. Our purpose can be regarded as a motivation to encouraging those working items to be standardized in IETF.

2. Use case 1: Unified User Identification

Consider a device of the subscriber accessing a network has to be authorised and authenticated as well as to assure reliability of the service,the device must be able to identified and recognized as the first step. That means that the identity of the device must be transferred and acknowledged. In addition, a unique identity has to

be transferred or assigned to the device to maintian the device management.

In real network,ISP assign a subscriber-id to the subscriber always. One subscriber may have multiple devices, including PC, mobile phones, ipad, etc., and may seamlessly cross multiple heterogeneous networks. The subscriber can not only use this subscriber-id to access the network, but also share the subscription between multiple devices. ISP could assign an ID to the customer, any of the devices belonging to the customer can achieve the authentication progress. The cumtomer can use this subcriber-id to connect the same service applications (operator's service or third-party service) without additional appliance. The devices of the same subscriber should be managed in a group. This group could be identified by a identification.With this unified identication, the customer can log in different application systems with a single access control. Besides, operators and content providers can apply the unified access policy, accounting policy, etc., to the customer for the specific set of devices, as illustrated in Figure 1 below.

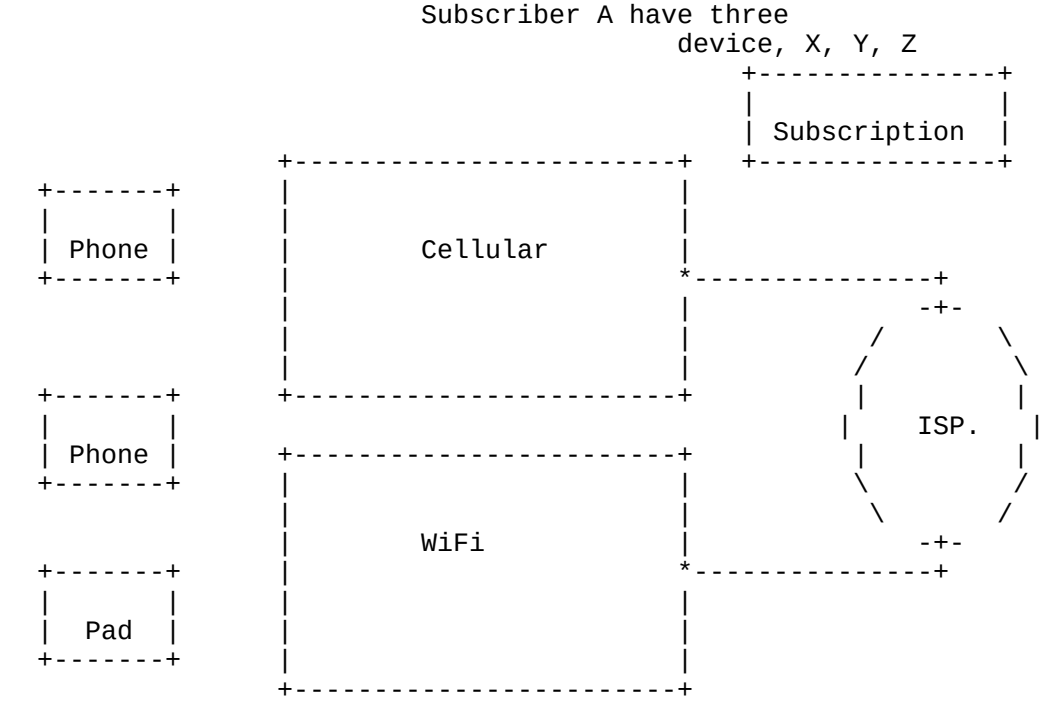

Figure 1

Potencial Technical Issues:

The Device Identifier, such as ISIM, MAC address, IP address etc, is used to indicate each individual device or host for the customer. Currently, IP address can be regarded as a device Identifier from the network layer. However, these identifiers are difficult to be kept consistently with NAT/CGNs(Carrier Grade Network Address Translation) along the path. Addional techniques (e.g. Host_ID, ID/Locator split, Device ID mapping to the network information,etc.)should be introduced to guarantee that a unique device Identifier will not be modified heterogeneous network environment.

Additionally, there is no suitable certain identifier by means of group the customer’s devices for unified control and management. . The group identifier for the devices should be introduced. Based on this kind of identifier, the operator can provide unified policy control on the user-level, irrespective of the devices .It provides a business case with unified subscriber management, policy control, single sign-on for applications, etc.

3. Use case 2: Unified QoS provisioning capability

A customer was firstly watching TV with a smart phone on his way home, and the video stream is smooth. When he arrives home, he switches the same TV channel to the television screen and keep watching. This user experience should not decrease due to the handover between different devices, the QoS feature should remain consistent with customers’ profile all the time, as illustrated in Figure 2 below.

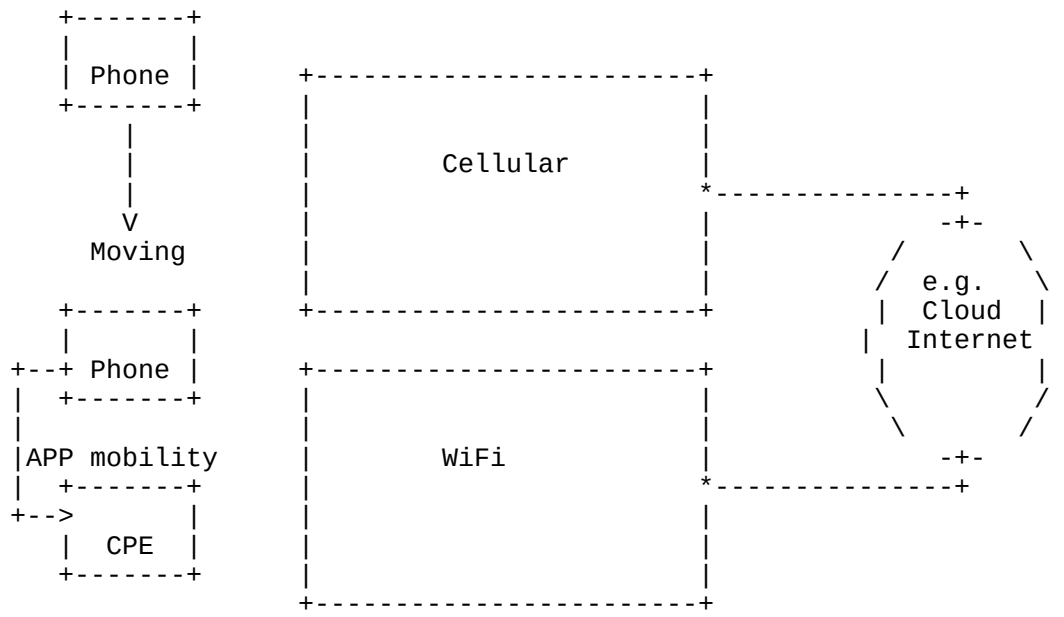

Figure 2

In this scenario, different devices will have the special requirement on display resolution, codec, etc. Addtionally, different networks will also have alternative ways to achieve these requirements.Moreover, content providers may provide differentiated service for subscribers. When a customer roams from one network to another, or from one device or another, the user QoS priority should still be treated uniformly in Content Provider/ Service Provider (CP/SP), including bandwidth guarantee, Content Distribution Network (CDN) policy, etc.

Potential Technical Issues:

1. QoS mapping: Unified user experience can only be achieved when heterogeneous networks interpret QoS parameters uniformly, which is based on the identification of the user.

2. User identification: CP/SP should support to identify the subscribers across different devices and heterogenous network.

4. Use case 3: Seamless handover for VPDN tunnel

A virtual private dial-up network (VPDN) is a network that extends remote access to a private network using a shared infrastructure,

VPDN allows individual users to connect to a remote network such as roaming sales people connecting to their company’s intranet. VPDNs use Layer 2 tunnel technologies (L2F, L2TP, and PPTP) to extend the Layer 2 and higher parts of the network connection from a remote user across an ISP network to a private network. Sometimes, in order to ensure the confidentiality of the data sent to an remote user, IPsec is used to setup a secure tunnel from the VPDN Client to a central router. However, when the user roams from one access point to another one,the network needs to provide a seamless remote access during handover.

Potential Technical Issues:

The issues that should be tackled in this case include device feature identification, seamless handover between different secure tunnels,Qos mapping, etc. Currently, a possible solution is Mobike [RFC4555], which allows the IP addresses of the tunnel endpoints in IPsec tunnel mode to change. However, this solution has a "NAT prohibition" feature which can be used to ensure that IP addresses have not been modified by NATs, IPv4/IPv6 translation agents, or other similar devices. Besides, other kinds of VPDN should also be solved in seamless handover case.

5. Use case 4: Mobility

Mobility is one of the most important items which should be considered in FMC work. We introduce two mobility usecases here, one is mobility between different access technologies (WiFi and 3GPP), and the other is mobility in WiFi scenario, such as between APs, as illustrated in Figure 3 below.

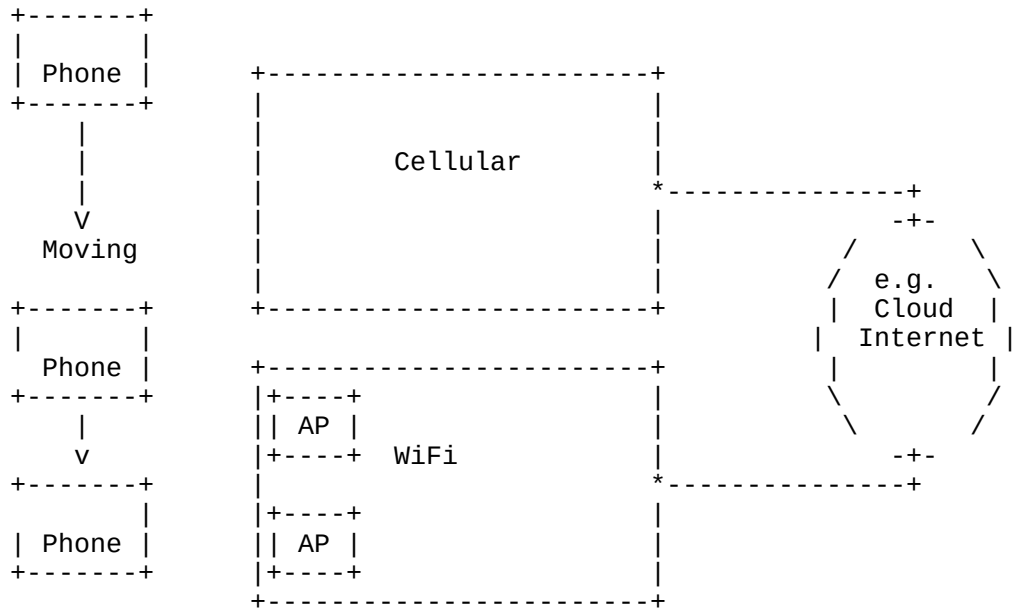

Figure 3

Customer service should be guaranteed 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. Even more we can see all the services depends on the substantive of customer's profile. Move, in the NAT scenario, we need identification for UE behind NAT. It is important to confirm the device identification binding or updated accordingly for the same UE which is moving. It isn't in the scope of mobility protocol.

Additionally, WiFi is one of the most important access technology for operators, it is possible that customer is playing video in the bus via WiFi. The mobility between APs,and in AP overlap area must be considered. Even more, wherever the device access to the service via WiFi, such as at home or in the hotspot, or even roaming to another WiFi operator's network, the QoS and service experience should be uniform.

Potential Technical Issues:

1. In order to provide uniform policy control, the device identification should be uniform or transferred during the device mobility. This is the specical requirement for UE identifier.

2. When the service application from one device to another deivce of a subscriber, the uniform QoS and service experience should be guaranteed, even between different access networks. Based on this requirement, PMIP and MIP can not achieve the QoS uniform during mobility. Additional mechine is needed.

3. In the scenario of WiFi, the service QoS and experience between different APs should be guanrantted during device mobility. In this case, the WiFi connection status and the subscriber information should be tracked during mobility.

6. IANA Considerations

7. Security Considerations

TBD

8. Acknowledgements

TBD

9. References

9.1. 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.

[RFC2460] Deering, S. and R. Hinden, "Internet Protocol, Version 6 (IPv6) Specification", RFC 2460, December 1998.

9.2. Informative References

[RFC2132] Alexander, S. and R. Droms, "DHCP Options and BOOTP Vendor Extensions", RFC 2132, March 1997.

[RFC2661] Townsley, W., Valencia, A., Rubens, A., Pall, G., Zorn,

G., and B. Palter, "Layer Two Tunneling Protocol "L2TP"", RFC 2661, August 1999.

[RFC2865] Rigney, C., Willens, S., Rubens, A., and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

Authors' Addresses

Chongfeng Xie
China Telecom
Room 708, No.118, Xizhimennei Street
Beijing 100084
P.R. China

Email: xiechf@ctbri.com.cn

Qiong Sun
China Telecom
Room 708, No.118, Xizhimennei Street
Beijing 100084
P.R. China

Email: sunqiong@ctbri.com.cn