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

L. Xue
B. Sarikaya
Huawei
D. von Hugo
Telekom Innovation Laboratories

October 22, 2012

Problem Statement for Fixed Mobile Convergence
draft-xue-fmc-ps-03.txt

Abstract

The purpose of this document is to analyze the issues that have arisen so far and to propose several use cases for the Fixed Mobile Convergence. This document gives a brief overview of the assumed Fixed Mobile Convergence architecture and related works and then introduces several Intarea type of use cases based on the partnership in Fixed Mobile Convergence architecture, such as group identification, mobility consideration, such as mobility status reporting in Wi-Fi network.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

Growing availability of intelligent mobile devices and mature networks of operators providing both reliable carrier grade connectivity and affordable high bandwidth access offer to the customer a nice climate of mobile broadband. With widespread availability and easy usability of mobile broadband, mobile broadband applications become more ubiquitous. Subscribers demand for various service applications, especially Internet applications, such as mobile Internet video, mobile Internet real-time communication, etc.

The subscribers requirements lay the foundation of mobile broadband. On the other hand, simultaneously, the subscribers' services promote the evolution of mobile broadband, which will impact the network architecture. The flourishing mobile applications demand more and more bandwidth offered by the operators. Even with wireless networks becoming mature, such as 3G and LTE, the average bandwidth offered is not comparable to data rates offered by fixed networks. With data services rapidly increasing, the traditional cellular network operating at a shared medium and thus being limited in transmission rate often becomes the bottle-neck of mobile broadband. In addition radio network technology generally requires high capital investment and operational expenditures. Cellular network operators are facing the challenge of increasing traffic demand at decreasing revenue and have to provide means of more cost efficient access technology in a highly competitive environment. With parallel availability of different access technologies such as cellular and local wireless networks a selection of the most (e.g. resource) efficient technology is advantageous for both user and operator. Mobile industry has specified functionalities to offload the data traffic to the fixed broadband (FBB) network, via WLAN or a Home (e)NodeB (HNB or eNodeB, aka. Femtocell) [TR23.829], which could alleviate traffic pressure on the mobile network. That is to say, today, operators are able to employ mechanisms to manage the subscriber service over both the mobile and the fixed broadband network. We can say, FMC is emerging on the basis of subscribers and operators requirements.

Fixed Mobile Convergence is a technology trend which aims to provide the subscribers access to services regardless of the access network type they are connecting to and provide the operators with the flexibility to ensure transparency of services to the end user. For a mobile subscriber to access services over both mobile and fixed broadband networks seamlessly, additionally, the subscriber's end-to-end service level agreement (SLA) must be maintained. This is achieved by interworking between the control planes of the fixed broadband network and the mobile network.

In the FMC interworking scenario addressed here, the fixed broadband network must partner with the mobile network to perform authorisation, authentication, and accounting (AAA) and acquire the policies for the mobile subscriber. Please note, a single converged control plane, used for both the fixed broadband and the mobile network, may be used in a truely converged, i.e. integrated convergence scenario. This document only focuses on the interworking scenario in this version. The convergence scenario is for further study.

Figure 1 shows the assumed reference architecture of Fixed Mobile Convergence Interworking for a Mobile (3GPP) Network and a fixed non-3GPP access network as proposed by 3GPP and BroadBand Forum (BBF) as an example in document [TR203].

```
                      +--------------------------------------+
                      | Mobile Network                       |
                      |                                ----  |
                      |                    +------+  /      \|
                      |                +---+ PCRF | |Operator|
                      |                |   +---+--+ | Service|
                      |                |       |     \      /|
                      |                |       |       --+-  |
  +------+  +------+  | +------+   +---+--+    |         |   |
  |  UE  |  | eNB  +----+ SGW  +---+ PGW  +----|---------+----------+
  +------+  +------+  | +------+   +--+---+--+ |     +------+|      |
                      |            +--+---+  +-|-----+M AAA ||    --+-
                      |            | ePDG +--+ |     +---+--+|  /      \
                      +------------+------+----|---------|---+ |Internet
                                      |        |         |     | Service
                      +---------------|--------|---------|---+  \      /
                      | Fixed Network |     +---+--+ +---+--+|    --+-
                      |               | +---+ BPCF | |F AAA ||      |
                      |            +--+-+-+ +------+ +---+--+|      |
            +------+  |            | BNG  +--------------+   |      |
            | Femto+----------+    +--+-+-+                  |      |
            +------+  |       |       | +---------------------------+
  +------+            |       |    +--+---+                  |
  |  UE  |            |       +----+  AN  |                  |
  +------+  +------+  |            +--+---+                  |
            |WiFiAP|------------------+                      |
            |  CPE |  |                                      |
            +------+  |                                      |
                      +--------------------------------------+
  Legend:
   M AAA   Authentication Authorization Accounting in Mobile Network
   F AAA   Authentication Authorization Accounting in Fixed Network
   AN      Access Node
   BPCF    Broadband Policy Control Function
   BNG     Broadband Network Gateway
   ePDG    evolved Packet Data Gateway
   PCRF    Policy Charging Rule Function
   PGW     Packet Data Network Gateway
   SGW     Serving Gateway
   UE      User Equipment
   CPE     Customer Premises Equipment
```

Figure 1: Reference Architecture of Fixed Mobile Convergence

The policy and charging control (PCC) system is an important element in FMC architecture. PCC system of FMC consists of policy decision point (PCRF in the mobile network and BPCF in the fixed broadband network) and the policy enforcement point (PGW and BNG, respectively), shown in Figure 1. PCC should support for controlling the QoS (e.g., QoS class and bit rates) authorized for service, and IP flow based charging. In FMC interworking scenario, these services can be divided into four types.

1. Service via macrocell wireless network

2. Service via WiFi/Femtocell access routed back to 3GPP Evolved Packet Core (EPC), where the fixed broadband network is used as the access network,

   * The service from a mobile UE is connected to WiFi or to Femtocell Access Point (FAP) at the residential gateway (RG), routed back to 3GPP Evolved Packet Core (EPC).

3. Services via WiFi access only fixed broadband routed

   * The service from a mobile UE is connected to WiFi without traversing the mobile network.

   * In this scenario, the UE service may be guaranteed based on subscriber’s policy from the mobile network.

4. LIPA/SIPTO traffic

   * Support of Local IP access (LIPA) and of Selected IP traffic offload (SIPTO) for the Home (e)NodeB Subsystem and for the macro layer network include a more integrated FMC scenario and thus are for further study.

As for the services stated above, only the second and the third type are related to FMC, where both the fixed broadband and the mobile network are involved. The FMC architecture shall be capable to set operator policies to support simultaneous access to these service.

In the network today, deploying FMC is a worthy way for operators to satisfy subscriber’s requirement and ease pressure from bandwidth. In the following sections, we first describe the motivation and then discuss the key issues that are at this time limited to the Intarea and to FMC interworking scenario.

2. Conventions and 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 described in RFC 2119 [RFC2119].

3. Key Issues in Fixed Mobile Converged Interworking

There is a need to highlight and discuss the issues when facilitating FMC. We systematically analyze the issues that have been proposed so far and briefly assess the possible protocol extensions which could solve the problems. In the network architecture, we target and limit the scope to the interworking architecture for FMC.

Regarding the traffic management and control requirements in FMC interworking scenario, these are the issues from an IETF Internet Area and fixed broadband network point of view.

1. Group Id in fixed broadband network,

2. UE mobility status reporting in fixed broadband network.

There are many standardization issues related to FMC and protocol extension work needed. If these issues are fixed, the advantages brought out will be:

1. Optimize traffic management (per-UE granularity in the fixed broadband network)

2. Enhance device management (via IP address synchronization between fixed broadband network and mobile network)

3. Quick Responsiveness based on UE status

These issues are elaborated in the sections that follow.

4. Group Id in Fixed Broadband Network

Consumers in a fixed mobile convergence scenario nowadays are not being limited by a single device such as only smart phone in connecting to fixed broadband network. Increasingly, portable media players, PCs, tablet, and mobile phones all belonging to the same subscriber are being used. It is reported that more than 90 percentage of video streaming customers own more than one device. Therefore, the same set of devices owned by one subscriber will have the same personalized requirement. For example, one subscriber may order the highest priority video streaming service from the operator, an instant bandwidth tune service, security control, etc.

It is expected for consumers to receive network services seamlessly in a convenient and economic way, irrespective of access technologies. For example, consumers prefer to connect to the Internet service via WiFi, instead of cellular access technology when moving into a Wi-Fi hotspot, if their mobile device is equipped with WiFi (IEEE 802.11-based) interface.

Users must be able to access to services irrespective of the access network. Operators need to have suitable user management ability, to reduce the CAPEX and OPEX. For example, operators could apply the unified policy control, and accounting control to the multiple devices owned by one subscriber, or devices with multiple interfaces, etc. This brings the need to identify each subscriber as one group and given a group identifier.

Consider Figure 2 where several hosts are connected to the same RG in a fixed broadband network. These hosts belong to different subscribers. One of the subscribers has only one device shown as UE in the figure. The second subscriber has multiple devices, one Pad, one smart phone and a personal computer (PC). Each subscriber is assigned a group id by the operator. Group Identifier (GroupId) needs to be communicated to fixed broadband network nodes such as the edge router (BNG).

A subscriber signs in the services of an operator. This subscriber has several devices, e.g., two phones and one pad. She/he wishes to share the subscription with these three devices. The operator could assign a group id to the costumer, and any of the devices belonging to the customer can be authenticated with this Id. Then all the other devices can access the service - either in parallel or sequentially - with unified policy control without additional authentication.

A subscriber owns one pad and one Phone. This subscriber may take photos on his trip away from home. It would be desirable that the other device(s) which are left at home to be immediately syncronized with these pictures in order to share them with the family. The operator could ensure the device discovery belonging to one subscriber by keeping an unified subscriber database in the network containing all group ids of the subscribers.

Group id based traffic management changes the granularity of traffic management that is currently in effect in cellular networks which is based on per-UE or per-contract level. In current FMC procedures, the broadband network can be made known of per-phone level traffic control by way of the IP-CAN session [TS23.203] which denotes the association between a UE and an IP network. The operator now will be in a position to provide unified service to all the devices that belong to the same group id, possibly carrying over UE's downloaded traffic quality of service requirements to all other devices.

If several devices access service via multiple access technologies, the access technologies could belong to different network operators. For example, WiFi network could be deployed by a different operator. In this scenario, the subscriber ID semantics must be consistent among these two operators. This can be achieved by agreement between different operators.

Another problem that arises is efficient packet inspection. Operators expect the fixed broadband network could be configured in such a way that the traffic subject to packet inspection is routed via the Traffic Detection Function (TDF) [TS29.212] usually collocated with the edge router. Traffic inspection and then traffic redirection that follows can be facilitated with group id. The same inspection and redirection (to the local home network, to the mobile network or to the Internet) rules can be applied in a unified manner to all devices belonging to the same group.

```
 Group  +----+
   Id   | UE |                                                  Internet
    1   +----+                                                     /
               W                                               ^ Mobile
 Group  +----+ i                                               | Network
   Id   | PC | F +----+                                        |
    2   +----+ i | AP |   +----------+                     +----------+
        +----+   |  & |   |          |                     |          |
        |Pad | L | RG |---|          |   +-------------+   |          |
        +----+ i +----+   | Access   |---| Aggregation |   |  Edge    |
       +-----+ n          |  Node    |   |   Network   |---|  Router  |
       |Phone| k          |          |   +-------------+   |          |
       +-----+            +----------+                     +----------+
               RG
```

Figure 2: Group Identification in Broadband Network

As discussed before, there are many drivers for the identification of GroupId when the same subscriber accesses the broadband network using several devices. They include efficient packet inspection, QoS enforcement, charging. We can note that all these functions in FMC depend on being able to identify the subscriber to which the device belongs, i.e. group identification.

The subscriber ID must be contained in the traffic packet of the subscriber in order to achieve policy enforcement in the device node in the network. Currently the group id is not being communicated in an IP packet. There are several possibilities which provide solutions. IP (v4 or v6) level solution would call for including group identifier in every packet the user sends. Such an approach facilitates packet inspection to provide required Quality of Service since by looking at each packet the subscriber can be identified.

ICMP (both v4 and v6) or TCP/UDP protocol extensions can also be other solution approaches. In this case the group id sent at the beginning needs to be paired with the IP address of the device. Packet inspection can then be conducted by first detecting the address and then identifying the subscriber followed by enforcement specific to this subscriber. It is difficult to foresee which is the suitable solution among the various possibilities, more work needs to be done.

5. UE Mobility in Fixed Broadband Network

The users are the mobile subscribers in FMC. Note that all the services depend on the substantive character of subscriber’s mobility. It is important for operators to capture the user device when it is moving into or outside the network, even in WiFi access. Besides, the application and service from the subscriber must be guaranteed based on the policy of operators.

In mobile network today, there are many mature solutions offered for user’s mobility already. Herein, only mobility in fixed access, i.e., WiFi access, will be considered. For example, the user device is attached to the home LAN (e.g., WiFi) network, and establishes a connection back to the subscriber’s mobile service provider network via the fixed broadband network. The mobile operator should cooperate with the broadband access operator to deliver proper policy for the service from UE.

```
   +----+  +------+    +----------+
   | UE1|  |AP&RG |----|          |
   +----+  +------+    |          |
          W            |    AN    |\
   +----+ i+------+    |          | \
   | UE2| F|AP&RG |----|          |  \
   +----+ i+------+    +----------+   \                   +----------+
                                       \                  |          |
          L                           +-------------+     |          |
          i                           | Aggregation |     |  Edge    |
          n                           |   Network   |-----|  Router  |
          k                           +-------------+     |          |
                      +----------+    /                   +----------+
   +----+  +-----+    |          |  /
   | UE3|  |AP&RG|----|    AN    | /
   +----+  +-----+    |          |
                      +----------+
```

Figure 3: UE Mobility in Broadband Network

The mobility considered in the fixed access does not consider the use of a mobility protocol. Consider Figure 3 where there are many mobile nodes, i.e. UEs connected to the fixed broadband network. Status of these nodes at a given time needs to be communicated to the network by the access points. In this section, we divide the mobility status reporting capability into two cases:

1. UE is moving into or outside the coverage area of WiFi AP

2. UE’s WiFi access is dormant or not.

Figure 3 shows an example of the scenario where mobile UEs are served in WiFi deployment over the fixed broadband network. RG embeds WiFi AP. Each UE is provided with an IPv4/IPv6 address assigned within the local network. A point-to-point link is established between the UE and the edge router.

BPCF in fixed broadband network must have partnership with PCRF in mobile network in order to maintain the service level agreement (SLA). In order to allow the PCRF to retrieve the UE’s policy to be passed onto the BPCF in the fixed broadband network, it is mainly concerned about the traffic and UE identification binding used to achieve the actual traffic control. The BPCF/BNG will perform the policy control based on the binding.

Since plenty of UEs may move into the coverage of WiFi AP, it is possible that large amount of resources will be needed at the BPCF/ BNG. For optimum operation, the resources need to be released when the UE goes out of the coverage of WiFi AP. So timely detection of UE detachments is crucial in fixed mobile convergence environments.

That is to say the configuration must be updated regularly to satisfy that the WiFi AP can serve thousands of UEs and proper resource allocation at the BPCF/BNG.

Possible solutions approaches include extending the Control And Provisioning of Wireless Access Points (CAPWAP) architecture RFC 5415 [RFC5415]. Access Controllers using an extended protocol can be charged to keep track of the mobility status of the UEs that are connected to the fixed broadband network using IEEE 802.11 links. However, in Fixed Mobile Convergence, this information is needed by entities not necessarily co-located with the Access Controller.

In some cases, e.g. home networks, CAPWAP protocol is not commonly used. In such cases, it becomes even more challenging to keep track of the UE mobility status. Protocol solutions need to be developed to solve this problem. During the solution process, CAPWAP protocol could be used as an example.

6. IANA Considerations

This document makes no request to IANA.

7. Security Considerations

Serious concern of mobile operators towards FMC approaches has been the customer access via networks not under control of the operator. Operators would like to keep their own high security measures to prevent various kinds of fraud or attack to the operators services and network entities. Well known risks and vulnerabilities involved in using IEEE 802.11 with the CAPWAP protocol are documented in [RFC5416]. Any additional security considerations arising from FMC are TBD.

8. Acknowledgements

Many people provided comments that have been incorporated into this document including Mohamed Boucadair, David Binet, Pierrick Seite, Daniel Park and Cameron Byrne.

9. References

9.1. Normative References

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

[RFC5415] Calhoun, P., Montemurro, M., and D. Stanley, "Control And Provisioning of Wireless Access Points (CAPWAP) Protocol Specification", RFC 5415, March 2009.

[RFC5416] Calhoun, P., Montemurro, M., and D. Stanley, "Control and Provisioning of Wireless Access Points (CAPWAP) Protocol Binding for IEEE 802.11", RFC 5416, March 2009.

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

[TR23.829]

"3GPP TR23.829, Local IP Access and Selected IP Traffic Offload (LIPA-SIPTO)", October 2011.

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

[TS29.212] "3GPP TS29.212, Policy and Charging Control (PCC) over Gx/Sd reference point", September 2012.

9.2. Informative References

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

[TS24.302] "3GPP TS24.302, Access to the 3GPP Evolved Packet Core (EPC) via non-3GPP access networks", September 2012.

[WT146] "Broadband Forum Working Text WT-146, Subscriber Sessions", June 2012.

Authors' Addresses

Li Xue
Huawei
No.156 Beiqing Rd. Z-park, Shi-Chuang-Ke-Ji-Shi-Fan-Yuan,
Beijing, HaiDian District 100095
China

Email: xueli@huawei.com

Behcet Sarikaya
Huawei
5340 Legacy Dr.
Plano, TX 75024

Email: sarikaya@ieee.org

Dirk von Hugo
Telekom Innovation Laboratories
Deutsche-Telekom-Allee 7
D-64295 Darmstadt
Germany

Email: Dirk.von-Hugo@telekom.de