Network Working Group
Internet-Draft
Intended status: Informational
Expires: September 10, 2012

L. Xue
B. Sarikaya
Huawei
D. von Hugo
Telekom Innovation Laboratories
March 9, 2012

Problem Statement for Fixed Mobile Convergence
draft-xue-intarea-fmc-ps-01.txt

Abstract

The purpose of this document is to analyze the issues that have arisen so far and then to propose a set of requirements for the Fixed Mobile Convergence. The term Fixed Mobile Convergence spans several scenarios from true integration of fixed and mobile terminals, services, and network infrastructure on both technical and management level down to pure interworking between fixed and mobile networks in serving access for multi-interface terminals like todays' smartphones. In the interworking scenario, the mobile network passes on the mobile subscribers policies to the fixed broadband network in order to maintain the end-to-end service level agreement and to support remote terminal and access network management. Explicitly, the fixed broadband network must have partnership with the mobile network in Fixed Mobile Convergence interworking scenario. This document gives a brief overview of the assumed Fixed Mobile Convergence architecture and related works and then introduces several requirements based on the partnership in Fixed Mobile Convergence architecture, such as User Equipment identification and authentication, Femto Access Point management, device type identification and mobility considerations.

This Internet-Draft will expire on September 10, 2012.

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.

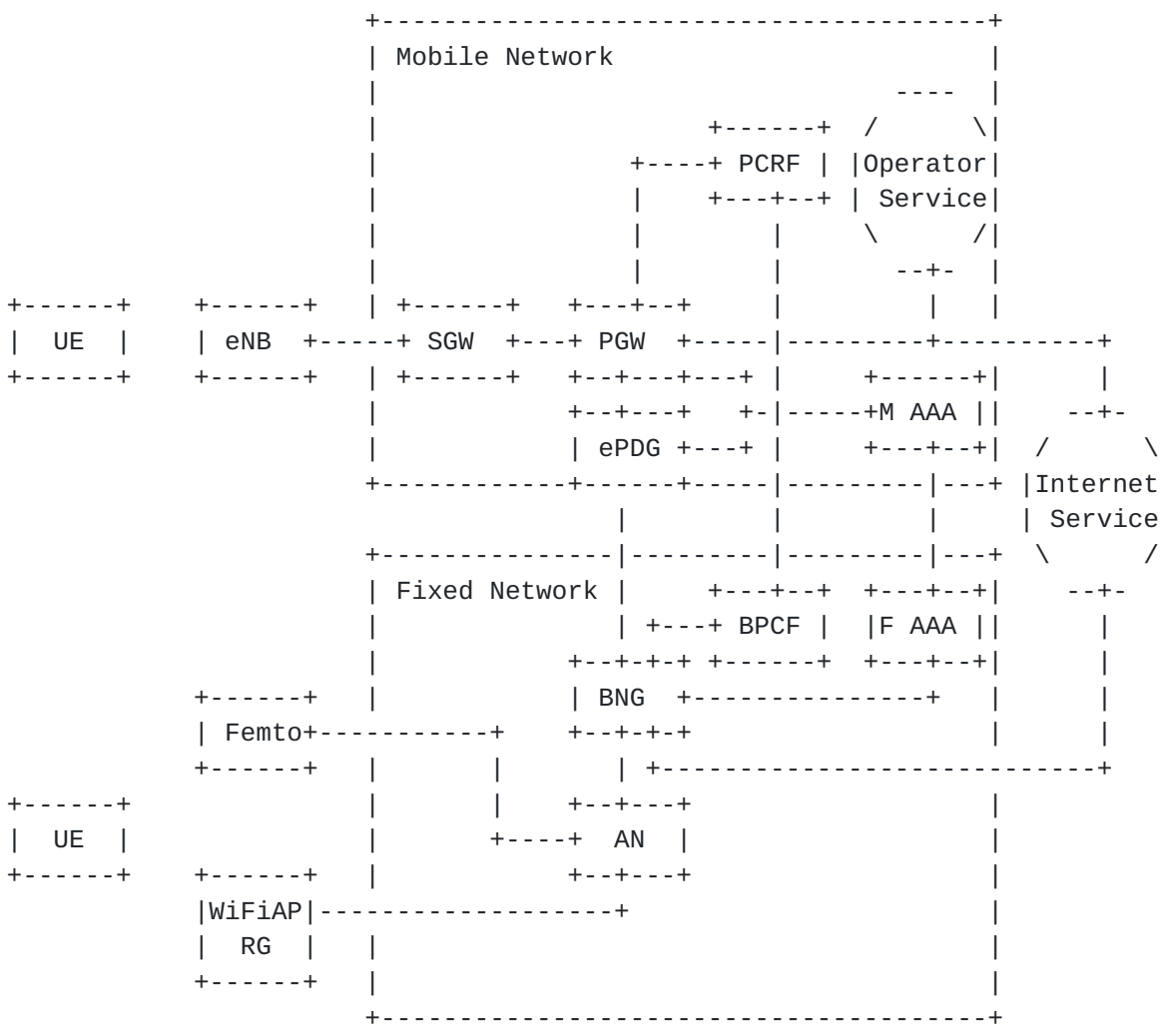
The subscribers requirements lay the foundation of mobile broadband. On the other hand, simultaneously, the subscribers' services promote the evolution of mobile broadband, which will impact the network architecture. The flourishing mobile applications demand more and more bandwidth offered by the operators. 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. The trend of offloading the traffic to fixed broadband network is emerging. 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 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 [WT203].



Legend:

M AAA	Authentication Authorization Accounting in Mobile Network
F AAA	Authentication Authorization Accounting in Fixed Network
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
RG	Residential Gateway

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 in 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. Motivation

The motivation is 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 extensions which could solve the problems. In the network architecture, we target and limit the scope to the interworking architecture for FMC. The convergence architecture is out of scope.

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

1. UE identification in fixed broadband network

2. Femto Access Point management

3. Device type identification

4. UE Mobility in fixed broadband network

5. Flow Mobility

In Section 4 below, we discuss the key issues and some problems based on the FMC architecture. There are many standardization issues related to FMC and protocol extension work needed are stated in this document.

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. Reduce operators load on Deep Packet Inspection (DPI) (bypass the unnecessary traffic)

4. Quick Responsiveness based on UE status

4. Key issues in Fixed Mobile Converged Interworking

This section provides some key issues related to FMC when deployed. These issues, which motivate the FMC, must be resolved. It is difficult to foresee the most suitable solutions to resolve these issues now, but in any event, some possibilities need to be analysed

based on the scenarios. Mobile network solutions of these issues are out of scope.

4.1. UE identification and AAA management in fixed broadband network

A user accessing a network point of attachment has to be authorised and authenticated by the network as well as vice versa to assure reliability of service as well as proper exchange of accounting information. That is the identity of the user and the AAA credentials have to be transferred and acknowledged. In addition a unique identity has to be assigned to the customer and/or his terminal, i.e. to maintain a session, a routable IP address has to be provided. Detailed consideration of AAA issues is out of sccope of this document.

Nowadays, a subscriber is always provided with a single private IPv4 address at their home or small business, which should reduce the pressure on the available public IPv4 addresses which are now exhausted. For instance, in the fixed broadband network, each host within the local network will be assigned a private IPv4 address, then NA(P)T function is responsible for translating the private IPv4 address to the public IPv4 address assigned to the CPE (Customer Premises Equipment) by operators, and vice versa.

As a result of maintaining growth of IPv4 service, private addressing plan will require address sharing, which will cause issues for operators, such as traffic management, QoS enforcement, etc. in the FMC scenarios, where the policy control must be based on the fundamental concept of per-UE granularity. Note that ultimately, deploying IPv6 is the only perennial way to ease pressure on the public IPv4 address without the need for address sharing mechanisms that give rise to the issues identified herein. But in the interim, however, IPv4 services are also very important for end-users, and service providers, which can not be ignored.

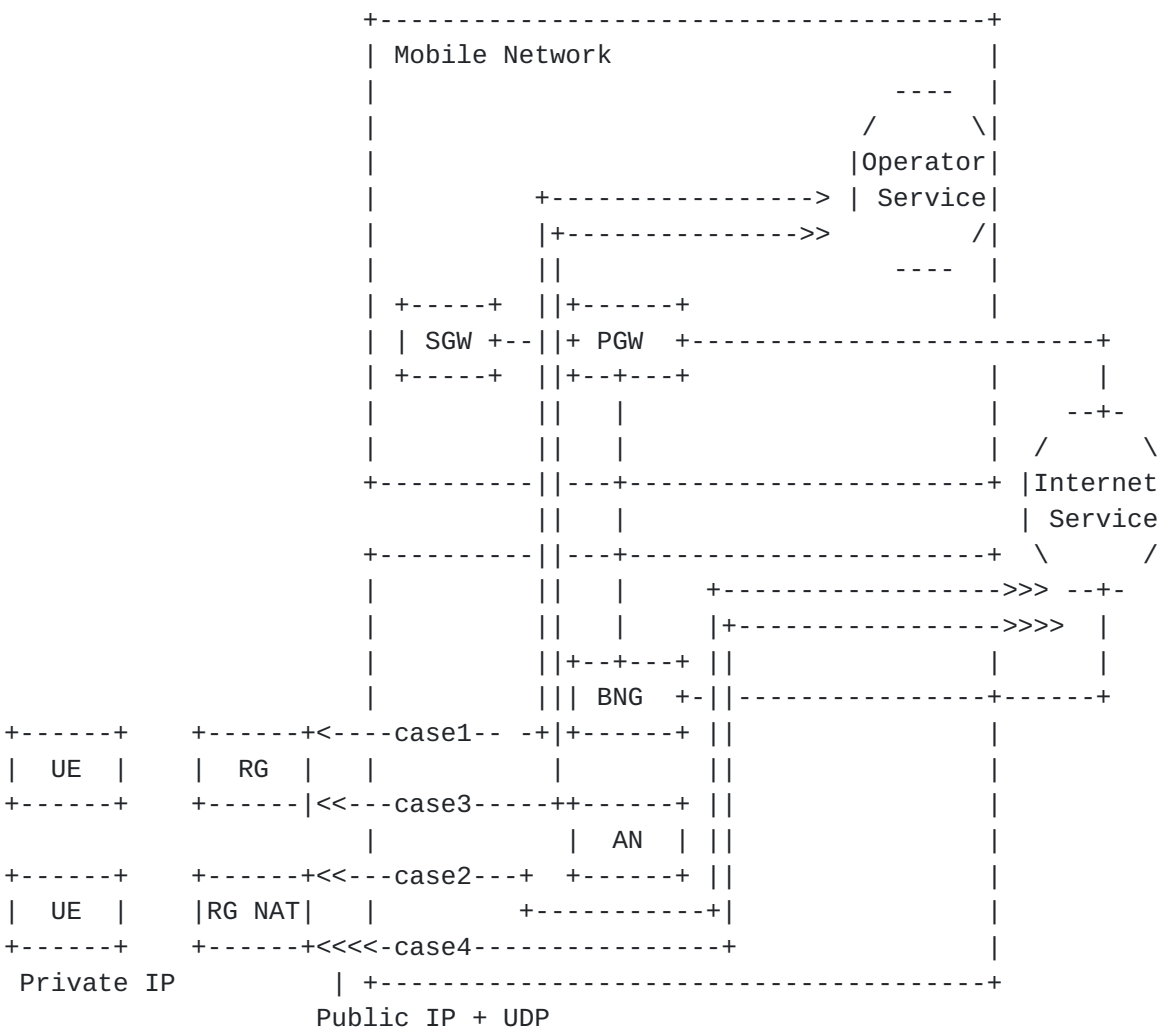
The FMC architecture shall be capable to set operator policies to support simultaneous access to mobile services and traffic offloading to the fixed broadband network. Accordingly, regarding policy and QoS interworking between the fixed broadband and mobile architectures, we consider the following scenarios:

1. Mobile UE with mobile-routed traffic and no NAT in Residential Gateway (RG)

2. Mobile UE with mobile-routed traffic with NAT in RG

3. Mobile UE with offloaded traffic and no NAT in RG

4. Mobile UE with offloaded traffic with NAT in RG



Currently PCC can support case 1 and 3, but issues will be introduced in cases 2 and 4 because of address sharing via NA(P)T. The important consideration is that today's PCC (including QoS control and IP flow based charging) must be based on the fundamental concept of IP Connectivity Access Network (IP-CAN) in per-UE granularity. IP-CAN session [TS23.203] is the association between a UE and an IP network. So in FMC network, it is assumed that fixed broadband network could manage the traffic in per-UE granularity.

Obviously, the fixed broadband network and mobile network must support inter-operator subscribers policy exchange, this introduces a major challenge on how to coordinate UE identification across the operators' domains so that the mobile network can inform the suitable policy to the serving fixed broadband access network that its mobile user equipment (UE) is attached to. So that the fixed broadband

network can provide the appropriate FMC interworking policy and bearer control on UE's traffic.

There may be limitations with BNG implementations with respect to the level of granularity (per-UE) of the enforcement. Take case 4 for an example, a key problem is to identify offloaded traffic from a special UE, i.e. UE identification substantively, behind the NA(P)T embedded into RG, there is no longer a unique IP address per UE, in addition, the UDP port behind NA(P)T is not bound to the special UE.

Another factor that contributes to UE identification 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], otherwise, the traffic that is not subject to packet inspection may bypass the TDF. This assumption only holds if it is possible to identify individual UEs behind NA(P)T embedded into the RG in fixed broadband network, shown in Figure 2. Issues may arise if there is a NA(P)T in or beyond the RG, even a NA(P)T in or beyond the BNG. As a result, additional mechanisms are needed to enable this.

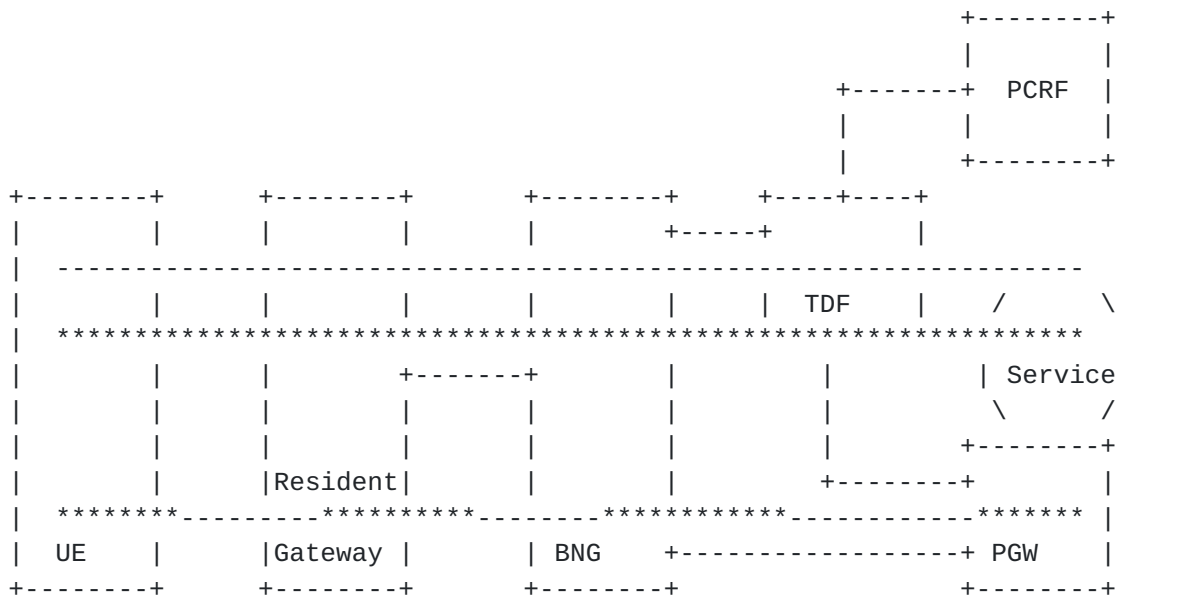


Figure 2: UE's Traffic Route with TDF

As discussed before, there are many drivers for the UE identification in the broadband network. They include efficient packet inspection, QoS enforcement, charging. We can note that all these functions in FMC depend on being able to identify UEs behind the NA(P)T.

There are several possibilities which provide solutions. One recommendation from fixed broadband, defined in [WT146], is to bind the UDP port (after NA(P)T) to the special UE. This solution has limitations because it may not be feasible due to static configuration in RG, to provide unique UDP port numbers to all the devices on user side. This is the overload scenario for operators.

Beside 3GPP-defined algorithms to derive unique identities for use within a fixed access network from 3GPP-specified SIM (Subscriber Identity Module) such as in [EAP-SIM, RFC 4186] or [EAP-AKA, RFC 4187 or EAP-AKA', RFC 5448] there are several possible IP or TCP protocol extensions, discussed in [I-D.ietf-intarea-nat-reveal-analysis]. In that draft, TCP host identifier option is also discussed. Additionally, there may be other possibilities, such as some other new identifier to be defined, etc. It is difficult to foresee which is the suitable solution, more work needs to be done.

4.2. Femto Access Point Management

Femtocells (FAPs), whose architecture is specified in the mobile standards (e.g., 3GPP, Femto Forum, etc.), are an exemplary feature of an FMC network. The access network to which Femtocells are attached is the fixed broadband network as depicted in Figure 3. As mentioned before, in order to achieve PCC, there is a need for the fixed broadband network to have partnership with mobile network to maintain the service level agreement (SLA). Here, the private IPv4 addressing plan in fixed broadband network introduces the limitations, which was described in the draft [I-D.so-ipsecme-ikev2-cpext]. In today's generic FAP architecture, it is difficult to guarantee a unique mapping, shown as follows:

1. Determine the UE attached FAP's public IPv4 address together with the translated port number of the UDP header of the encapsulated IPsec tunnel between the FAP and the Security Gateway (SeGW) which are assigned by the fixed broadband network. The FAP's public IPv4 address is:

    * used for identifying the location of the FAP,

    * used for identifying the UE's traffic at the fixed broadband network.

2. Determine the corresponding FAP's public IPv4 address's association with the UE's inner-IPv4 address which is assigned by the mobile network. The association is:

   * used for identifying the mobile UE that is attached to the FAP in order to allow the PCRF to retrieve the UE's policy to be passed onto the BPCF at the fixed broadband network.

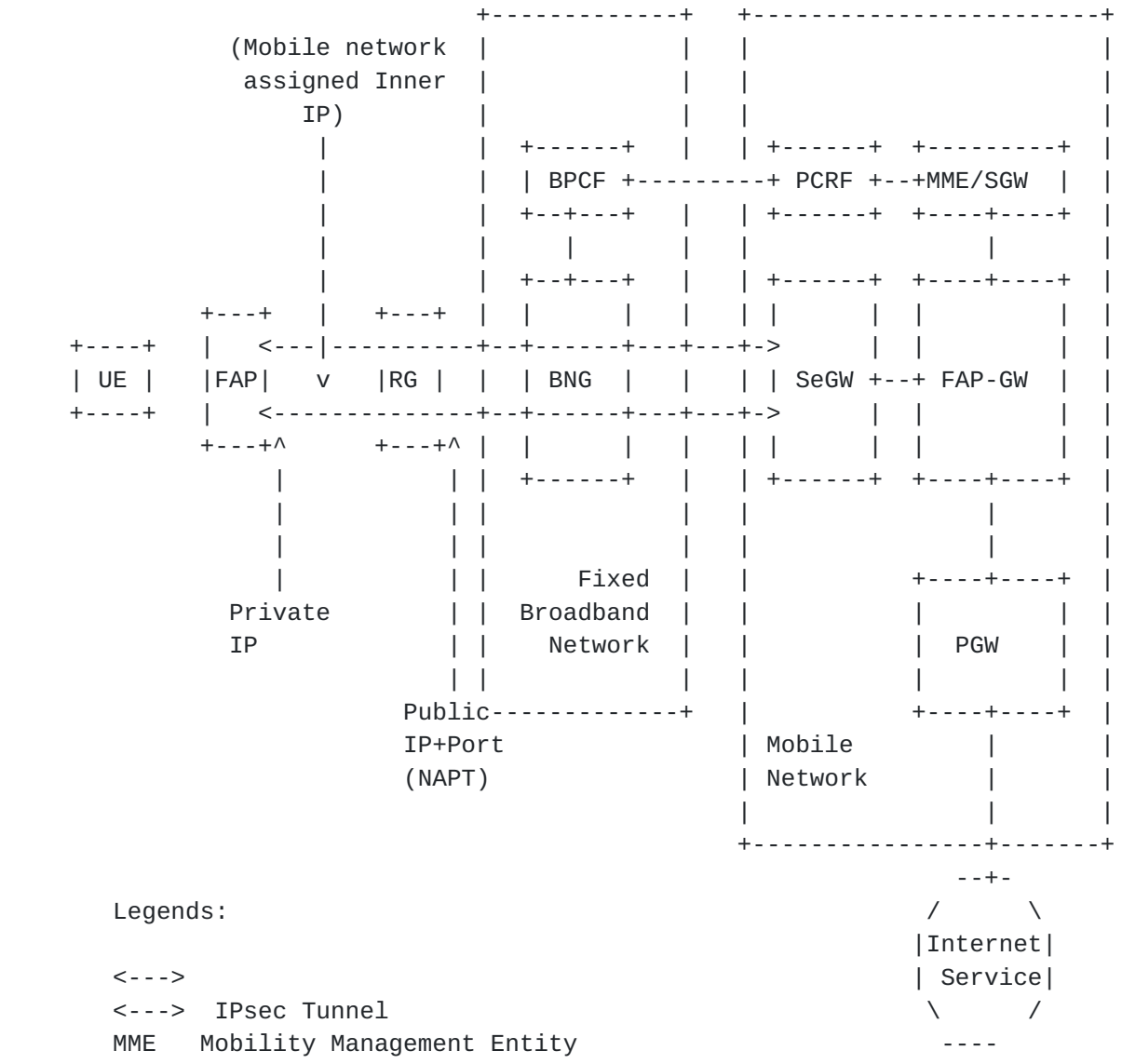


Figure 3: FMC Femto Access Architecture

Due to the requirement for inter-operators subscribers policy exchange, the private and public addressing which rely on NA(P)T, must be coordinated cross the operators domains. Additionally, FAP location must be identified for management. These major factors

drive the solutions in interworking architecture with Femtocell scenario such as extending IKEv2 [RFC5996], so that the overall service performance and the user experience could be enhanced.

4.3. Device type identification

As there are multiple types of user terminal devices, e.g. PDA, mobile phone, personal computer, etc. with different characteristic capabilities (portability, screen size, audio output etc.) for some service applications and corresponding QoS and management requirements, it is important for operators to capture the service-specific terminal device type, especially in FMC interworking scenario. In such cases, different rules for policy control and traffic routing are needed to be provided by the operators to ensure acceptable SLA to the device.

When WiFi is deployed for traffic offload, the terminal devices, such as mobile phone and personal computer could be used for service. In this case, only the traffic from the 3GPP service, such as mobile voice may need policy control and management. The best effort traffic will not be routed via the mobile core (EPC) and thus has no impact to the FMC at all. With this method, the traffic management optimization generally occurs based on selecting suitable types of device which need special policy control and management.

In the current WiFi network, the device type information is transparent to the fixed broadband network, because only IP and port information is used for identification. It is difficult for BNG to distinguish the traffic from UE device, and then route it specially. So a solution is needed to identify the device type, especially at the BNG.

4.4. Carrier Grade NAT Related Issues

Referring to Figure 3, FAP is usually behind a Carrier Grade NAT (CGN) box. CGN may be used as part of architecting the support of NAT44 or NAT444 [RFC6264]. CGN could be colocated with BNG in Figure 3. In such a configuration, UE maintains long lived IPsec or TLS connection across the CGN.

Carrier Grade NAT may flush the long lived session after a certain timeout period. Currently most NAT implementations would flush all sessions after they reach 24 hours, regardless of the state of the session.

CGN terminating all existing sessions of a UE does present a number of problems. One problem is that this will cause more attachment signaling to be introduced in order to reestablish UE's sessions.

More serious problem may occur though. UEs all active phone calls are possibly disrupted. UE may even be involved in calls to emergency services like 911 which would be disrupted as well.

4.5. 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.

The mobility considered in the fixed access is a little different. In this section, we divide the mobility 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.

The following figure shows an example of the scenario where mobile UEs are served in WiFi deployment over the fixed broadband network. RG embeds WiFi AP and NA(P)T function. Each UE is provided with a single private IPv4 address assigned within the local network. NA(P)T in RG is responsible for translating the private IPv4 address to the public IPv4 address assigned by the fixed operator.

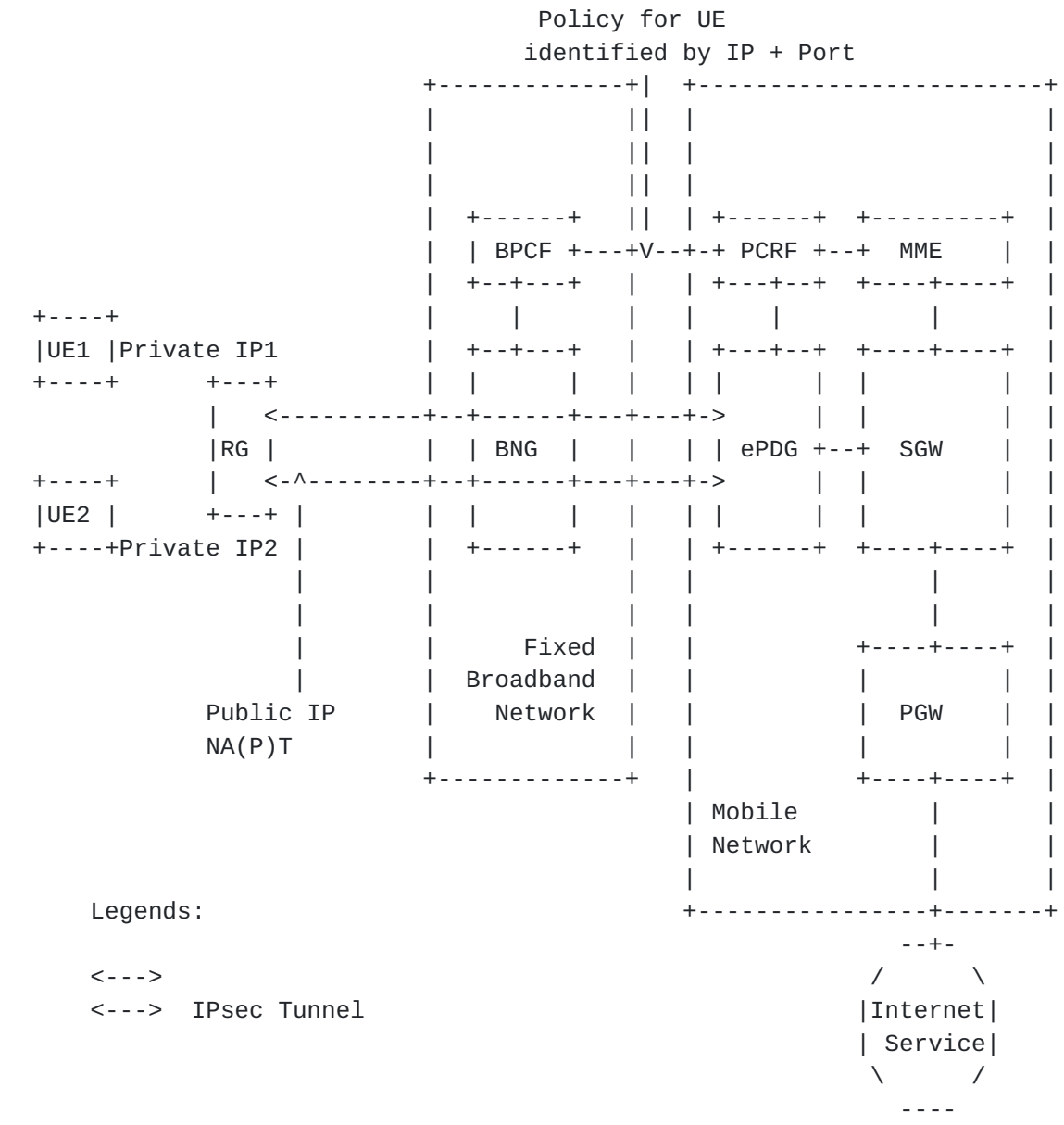


Figure 4: Mobility in the Fixed Broadband Network

As described previously, 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.

Based on the UE's mobility, issues will arise. For example, the PCRF will retrieve the wrong policy to the BPCF, if the UE identification can not be updated in time. For instance, there are two UEs, shown

in Figure 4. UE1 and UE2 are assigned different private IP addresses within the local network, IP1 and IP2 accordingly. After NAPT, BPCF/BNG will be based on the public IPv4 address and the different UDP port numbers assigned by NAPT to perform the admission control and policy enforcement on the UE's traffic.

Since plenty of UEs may move into the coverage of WiFi AP, it is possible that the same UDP port will be used for both UE1 and UE2 at the different time period. For example, UE1 moved out of the WiFi coverage and later the UE2 moved in. The same UDP port used by UE1 before is assigned to UE2 again. As mentioned, the identification must be consistent between fixed broadband network and the mobile network for policy exchange. So the UDP port used as part of UE identification must be updated in time based on the status of UE, otherwise the PCRF will confused about which policy is used.

Especially, there may be a requirement to binding the UDP port to a special UE described in Section 4. The UDP ports must be cleared if the UEs corresponding to prior port binding are out of coverage of the WiFi AP. That is to say the configuration must be updated regularly to satisfy that the WiFi AP can serve thousands of UEs. Other solutions to solve the issue in Section 4 may also fix this challenge introduced by the mobility of UE.

Based on the discussion, for UE's mobility in WiFi network, we can recognize that the important requirement for the fixed broadband network is to update the UE identification based on UE mobility. In this scenario, the fixed broadband network must be able to update the record for UE during the UE mobility.

4.6. Flow Mobility between different interface

Traffic offloading requires the ability to move the traffic flows from one interface to the other interface of the UE. The type of flows to be moved depends on the policy and should be dictated by the mobile operator.

Several IP flow mobility protocol approaches are under discussion some of which have been already adopted for use in mobile networks, e.g. by 3GPP, but currently no such flow mobility protocol has been applied for use in an fixed broadband network, e.g. by BBF. Without an overarching commonly agreed on flow mobility protocol, offloading traffic from mobile network to fixed broadband network can simply not be achieved.

5. IANA Considerations

This document makes no request to IANA.

6. 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 which are common to any NA(P)T application are documented in the NAT specification [RFC2663]. Any additional security considerations arising from FMC are TBD.

7. Acknowledgements

Many people provided comments that have been incorporated into this document including Mohamed Boucadair, David Binet, Pierrick Seite. Special thanks to Cameron Byrne for providing the text in Section 4.4.

8. References

8.1. Normative References

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

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

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

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

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

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

8.2. Informative References

[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 in Shared Address Deployments", draft-ietf-intarea-nat-reveal-analysis-01 (work in progress), March 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-01 (work in progress), February 2012.

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

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

[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.

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 75074

Email: sarikaya@ieee.org

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

Phone:
Email: Dirk.von-Hugo@telekom.de