

INTAREA Working Group
Internet-Draft
Intended status: Informational
Expires: April 20, 2013

M. Boucadair
D. Binet
S. Durel
France Telecom
T. Reddy
Cisco
October 17, 2012

HOST_ID: Use Cases
draft-boucadair-intarea-host-identifier-scenarios-01

Abstract

This document describes a set of scenarios in which host identification is required.

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 20, 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	3
2. Scope	3
3. Use Case 1: CGN	4
4. Use Case 2: A+P	4
5. Use Case 3: Application Proxies	5
6. Use Case 4: Open Wi-Fi or Provider Wi-Fi	6
7. Use Case 5: Policy and Charging Control Architecture	7
8. Use Case 6: Cellular Networks	8
9. Use Case 7: Femtocells	9
10. Security Considerations	10
11. IANA Considerations	10
12. Acknowledgments	10
13. Informative References	10
Authors' Addresses	11

1. Introduction

The ultimate goal of this document is to enumerate scenarios which encounter the issue of uniquely identifying a host among those sharing the same IP address. Examples of encountered issues are:

- o Blacklist a misbehaving host without impacting all hosts sharing the same IP address.
- o Enforce a per-subscriber/per-UE policy (e.g., limit access to the service based on some counters such as volume-based service offering); enforcing the policy will have impact on all hosts sharing the same IP address.
- o If invoking a service has failed (e.g., wrong login/passwd), all hosts sharing the same IP address may not be able to access that service.
- o Need to correlate between the internal address:port and external address:port to generate and therefore to enforce policies.

It is out of scope of this document to list all the encountered issues as this is already covered in [RFC6269].

The generic concept of host identifier, denoted as HOST_ID, is defined in [I-D.ietf-intarea-nat-reveal-analysis].

The analysis of the use cases listed in this document indicates two root causes for the host identification issue:

1. Presence of address sharing (NAT, A+P, application proxies, etc.).
2. Use of tunnels between two administrative domains.
3. Combination of NAT and presence of tunnels in the path.

2. Scope

It is out of scope of this document to argue in favor or against the use cases listed in the following sub-sections. The goal is to identify scenarios the authors are aware of and which share the same issue of host identification.

This document does not include any solution-specific discussion. This document can be used as a tool to design solution(s) mitigating the encountered issues. Having a generic solution which would solve

the issues encountered in these use cases is preferred over designing a solution for each use case. Describing the use case allows to identify what is common between the use cases and then would help during the solution design phase.

The first version of the document does not elaborate whether explicit authentication is enabled or not.

3. Use Case 1: CGN

Several flavors of stateful CGN have been defined. A non-exhaustive list is provided below:

1. NAT44
2. DS-Lite NAT44 [RFC6333]
3. NAT64 [RFC6146]
4. NPTv6 [RFC6296]

As discussed in [I-D.ietf-intarea-nat-reveal-analysis], remote servers are not able to distinguish between hosts sharing the same IP address (Figure 1).

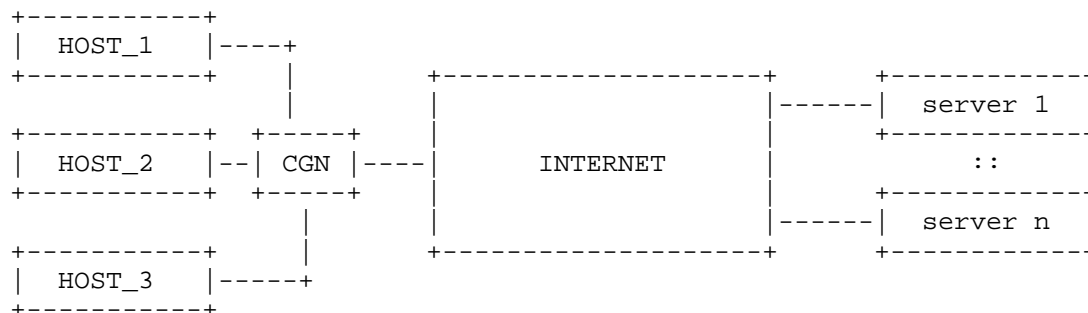


Figure 1

4. Use Case 2: A+P

A+P [RFC6346] denotes a flavor of address sharing solutions which does not require any additional NAT function be enabled in the service provider's network. A+P assumes subscribers are assigned with the same IPv4 address together with a port set. Subscribers assigned with the same IPv4 address should be assigned non

overlapping port sets. Devices connected to an A+P-enabled network should be able to restrict the IPv4 source port to be within a configure range of ports. To forward incoming packets to the appropriate host, a dedicated entity called PRR (Port Range Router, [RFC6346]) is needed (Figure 2).

Similar to the CGN case, the same issue to identify hosts sharing the same IP address is encountered by remote servers.

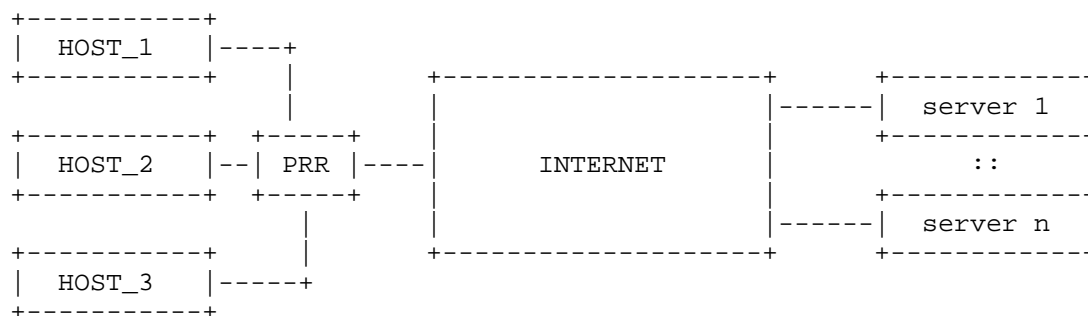


Figure 2

5. Use Case 3: Application Proxies

This scenario is similar to the CGN scenario. Remote servers are not able to distinguish hosts located behind the PROXY. Applying policies on the perceived external IP address as received from the PROXY will impact all hosts connected to that PROXY.

Figure 3 illustrates a simple configuration involving a proxy. Note several (per-application) proxies may be deployed.

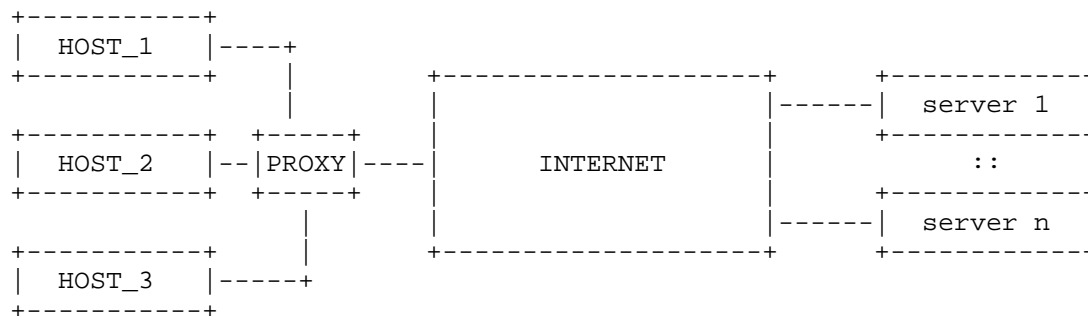


Figure 3

6. Use Case 4: Open Wi-Fi or Provider Wi-Fi

In the context of Provider Wi-Fi, a dedicated SSID can be configured and advertised by the RG (Residential Gateway) for visiting terminals. These visiting terminals can be mobile terminals, PCs, etc.

Several deployment scenarios are envisaged:

1. Deploy a dedicated node in the service provider's network which will be responsible to intercept all the traffic issued from visiting terminals (see Figure 4). This node may be co-located with a CGN function if private IPv4 addresses are assigned to visiting terminals. Similar to the CGN case discussed in Section 3, remote servers may not be able to distinguish visiting hosts sharing the same IP address (see [RFC6269]).
2. Unlike the previous deployment scenario, IPv4 addresses are managed by the RG without requiring any additional NAT to be deployed in the service provider's network for handling traffic issued from visiting terminals. Concretely, a visiting terminal is assigned with a private IPv4 address from the pool managed by the RG. Packets issued from a visiting terminal are translated using the public IP address assigned to the RG (see Figure 5). This deployment scenario induces the following identification concerns:
 - * The provider is not able to distinguish the traffic belonging to the visiting terminal from the traffic of the subscriber owning the RG. This is needed to apply some policies such as: accounting, DSCP remarking, black list, etc.
 - * Similar to the CGN case Section 3, a misbehaving visiting terminal is likely to have some impact on the experienced service by the customer owning the RG (e.g., some of the issues are discussed in [RFC6269]).

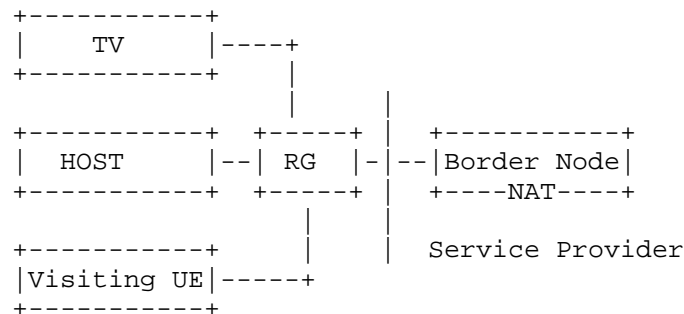


Figure 4

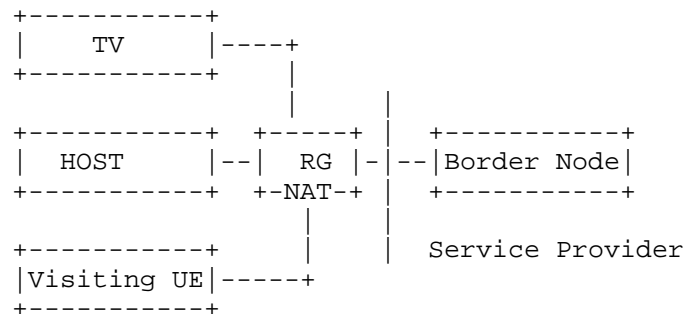


Figure 5

7. Use Case 5: Policy and Charging Control Architecture

This issue is related to the framework defined in [TS.23203] when a NAT is located between the PCEF (Policy and Charging Enforcement Function) and the AF (Application Function) as shown in Figure 6.

The main issue is: PCEF, PCRF and AF all receive information bound to the same UE but without being able to correlate between the piece of data visible for each entity. Concretely,

- o PCEF is aware of the IMSI (International Mobile Subscriber Identity) and an internal IP address assigned to the UE.
- o AF receives an external IP address and port as assigned by the NAT function.

- o PCRF is not able to correlate between the external IP address/port assigned by the NAT and the internal IP address and IMSI of the UE.

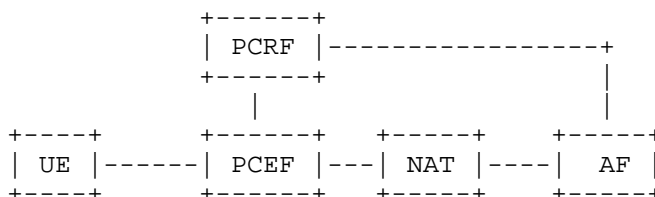


Figure 6

This scenario can be generalized as follows (Figure 7):

- o Policy Enforcement Point (PEP, [RFC2753])
- o Policy Decision Point (PDP, [RFC2753])

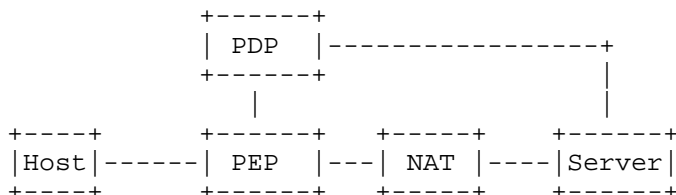


Figure 7

8. Use Case 6: Cellular Networks

Cellular operators allocate private IPv4 addresses to mobile customers and deploy NAT44 function, generally co-located with firewalls, to access to public IP services. The NAT function is located at the boundaries of the PLMN. IPv6-only strategy, consisting in allocating IPv6 prefixes only to customers, is considered by various operators. A NAT64 function is also considered in order to preserve IPv4 service continuity for these customers.

These NAT44 and NAT64 functions bring some issues very similar to those mentioned in Figure 1 and Section 7. This issue is particularly encountered if policies are to be applied on the Gi interface: a private IP address may be assigned to several UEs, no correlation between the internal IP address and the address:port assigned by the NAT function, etc.

9. Use Case 7: Femtocells

This issue is discussed in [I-D.so-ipsecme-ikev2-cpext]. This use case can be seen as a combination of the use cases described in Section 6 and Section 7.

The reference architecture, originally provided in [I-D.so-ipsecme-ikev2-cpext], is shown in Figure 8.

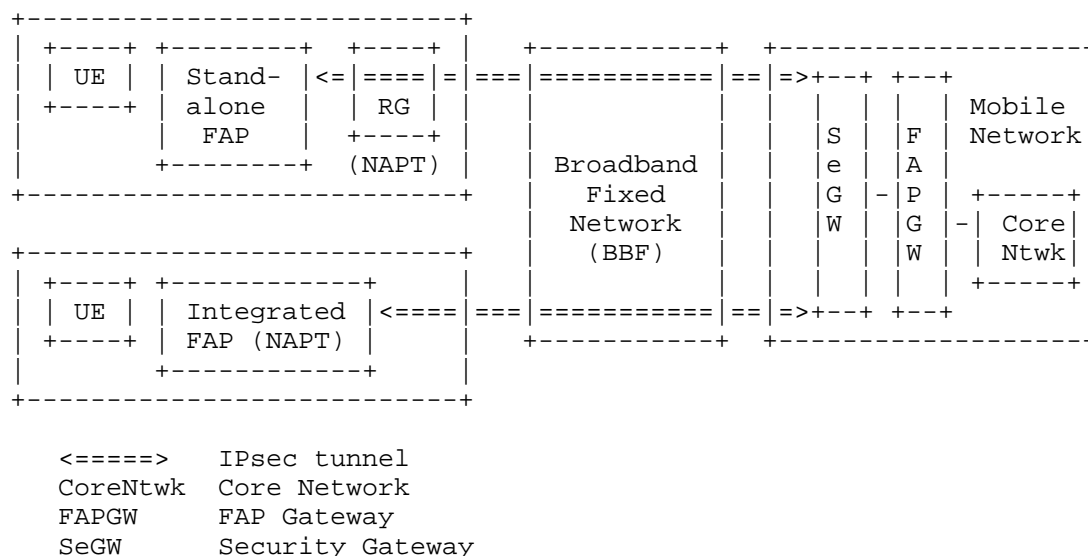


Figure 8

UE is connected to the FAP at the residential gateway (RG), routed back to 3GPP Evolved Packet Core (EPC). UE is assigned IPv4 address by the Mobile Network. Mobile operator's FAP leverages the IPSec IKEv2 to interconnect FAP with the SeGW over the BBF network. Both the FAP and the SeGW are managed by the mobile operator which may be a different operator for the BBF network.

An investigated scenario is the mobile network to pass on its mobile subscriber's policies to the BBF to support remote network management. But most of today's broadband fixed networks are relying on the private IPv4 addressing plan (+NAPT) to support its attached devices including the mobile operator's FAP. In this scenario, the mobile network needs to:

- o determine the FAP's public IPv4 address to identify the location of the FAP to ensure its legitimacy to operate on the license spectrum for a given mobile operator prior to the FAP be ready to

serve its mobile devices.

- o determine the FAP's public IPv4 address together with the translated port number of the UDP header of the encapsulated IPsec tunnel for identifying the UE's traffic at the fixed broadband network.
- o determine the corresponding FAP's public IPv4 address associated with the UE's inner-IPv4 address which is assigned by the mobile network to identify the mobile UE to allow the PCRF to retrieve the UE's policy (e.g., QoS) to be passed onto the Broadband Policy Control Function (BPCF) at the BBF network.

SecGW would have the complete knowledge of such mapping, but the reasons for unable to use SecGW for this purpose is explained in "Problem Statements" (section 2 of [I-D.so-ipsecme-ikev2-cpext]).

This use case makes use of PCRF/BPCF but it is valid in other deployment scenarios making use of AAA servers.

The issue of correlating the internal IP address and the public IP address is valid even if there is no NAT in the path.

10. Security Considerations

This document does not define an architecture nor a protocol; as such it does not raise any security concern.

11. IANA Considerations

This document does not require any action from IANA.

12. Acknowledgments

Many thanks to F. Kamm for the review.

Figure 8 and part of the text in Section 9 are inspired from [I-D.so-ipsecme-ikev2-cpext].

13. 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 (HOST_ID) in Shared Address Deployments",
draft-ietf-intarea-nat-reveal-analysis-04 (work in
progress), August 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.

[RFC2753] Yavatkar, R., Pendarakis, D., and R. Guerin, "A Framework
for Policy-based Admission Control", RFC 2753,
January 2000.

[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.

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

[RFC6296] Wasserman, M. and F. Baker, "IPv6-to-IPv6 Network Prefix
Translation", RFC 6296, June 2011.

[RFC6333] Durand, A., Droms, R., Woodyatt, J., and Y. Lee, "Dual-
Stack Lite Broadband Deployments Following IPv4
Exhaustion", RFC 6333, August 2011.

[RFC6346] Bush, R., "The Address plus Port (A+P) Approach to the
IPv4 Address Shortage", RFC 6346, August 2011.

[TS.23203]

3GPP, "Policy and charging control architecture",
September 2012.

Authors' Addresses

Mohamed Boucadair
France Telecom
Rennes, 35000
France

Email: mohamed.boucadair@orange.com

David Binet
France Telecom
Rennes,
France

Email: david.binet@orange.com

Sophie Durel
France Telecom
Rennes
France

Email: sophie.durel@orange.com

Tirumaleswar Reddy
Cisco Systems, Inc.
Cessna Business Park, Varthur Hobli
Sarjapur Marathalli Outer Ring Road
Bangalore, Karnataka 560103
India

Email: tiredddy@cisco.com

V6OPS WG
Internet-Draft
Intended status: Informational
Expires: April 25, 2013

S. Gundavelli
M. Grayson
Cisco
P. Seite
France Telecom - Orange
Y. Lee
Comcast
October 22, 2012

Service Provider Wi-Fi Services Over Residential Architectures
draft-gundavelli-v6ops-community-wifi-svcs-05.txt

Abstract

The tremendous growth in Wi-Fi technology adoption over the last decade has met the ultimate possible goal of 100% adoption rate. All most every new mobile device is now equipped with IEEE 802.11-based wireless interface and with pre-configured policy to prefer Wi-Fi to cellular access. Matching this evolution is every service provider's desire to offer Wi-Fi based broadband services; a new business opportunity even for fixed line operators. Operators are exploring options to monetize their existing networks, most with nation-wide footprint, to build a high-speed Wi-Fi service that can be the basis for offering new wireless broadband services. This document identifies the requirements for supporting these new Wi-Fi community services and the mobility tools which have been standardized in IETF that can be used for enabling these architectures.

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	4
2. Conventions and Terminology	5
2.1. Conventions	5
2.2. Terminology	5
3. Deployment Models	7
4. Requirements	8
4.1. IPv6 Addressing Model for SP WiFi Architectures	9
4.2. Subscriber Authentication & Service Authorization	9
4.3. Location-based Services	9
4.4. Local Services Access & Internet Traffic Offload	10
4.5. Web-based Authentication Support	10
4.6. Transparent Auto Login (TAL)	10
4.7. Multiple WLAN SSID Support	11
4.8. Multiple Home Network Service (APN) Access	11
4.9. CPE Identity and Authorization	11
4.10. Mobility within the WLAN Access Network	11
4.11. Mobility across WLAN and Macro Access	12
4.12. Differentiated Services for Users behind RG	12
4.13. Lawful Intercept (LI)	12
4.14. Subscriber Management and Charging	13
4.15. Handling the Walk-by Users	14
4.16. Overlapping IPv4 Address Support	14
4.17. Service Provisioning & Monitoring	14
5. Solution Approaches & Considerations	15
5.1. PMIPv6 MAG on the RG: Layer-3 Encapsulation between CPE and Access Gateway	15
5.2. Ethernet-over-IP Support on the RG: Layer-2 Encapsulation between CPE and Access Gateway	15
5.3. Local Aggregation for Subscriber Control and Internet Offload	15
5.4. Mobility Chaining: Integration with Mobile Packet Core	15
6. IANA Considerations	15
7. Security Considerations	15
8. Acknowledgements	16
9. References	16
9.1. Normative References	16
9.2. Informative References	16
Authors' Addresses	17

1. Introduction

The tremendous growth in Wi-Fi technology adoption over the last decade has met the ultimate possible goal of 100% adoption rate. All most every new mobile device is now equipped with IEEE 802.11-based wireless interface and these devices are typically pre-configured with a policy to prefer Wi-Fi to cellular access. This so called, "cheap access based on unlicensed spectrum", is no longer considered an unreliable access, but with all the available protocol tools and with maturity in technology, building a reliable broadband service that can meet the committed service-level agreements is proving to be a non-issue.

Matching this evolution is every service provider's desire to offer Wi-Fi based broadband services; a new business opportunity even for both fixed and mobile operators. The demand for bandwidth is only growing with the availability of new smart devices, new technology applications and with all the content in the Internet. Furthermore, an increasing percentage of mobile consumption is happening in the home and so DSL/Cable operators are exploring options to monetize their existing networks, most with nation-wide footprint, to build a high-speed, nation-wide Wi-Fi service that can be the basis for offering new wireless broadband services and for building roaming agreements with traditional mobile operators, who are unable to meet the mobile subscriber growth due to the finite licensed spectrum available for macro-cell deployments. Every residential CPE device that the operator owns can now be enabled to provide Wi-Fi service and new community Wi-Fi hotspots can be built in any location where there is fixed line coverage. A wireless service based on unlicensed spectrum, and leveraging existing transport is a huge incentive for operators to enter this new market.

To support these business goals, operators are looking at mobility architectures for supporting various requirements. Not all requirements are well understood, and neither are the implications with the chosen solution approaches for each of those requirements. The choice of the architecture has an implication on the CPE evolution and on the core infrastructure feature requirements. Therefore, the sole purpose and the goal of this document is to present all the requirements, identify the protocol tools and any potential gaps. This analysis is important for enabling the network vendors and the mobile operators to make the right design choices and leverage the existing tools that the mobility groups in IETF have already developed and discourage them from adopting proprietary, non-standard mechanisms or developing redundant alternatives.

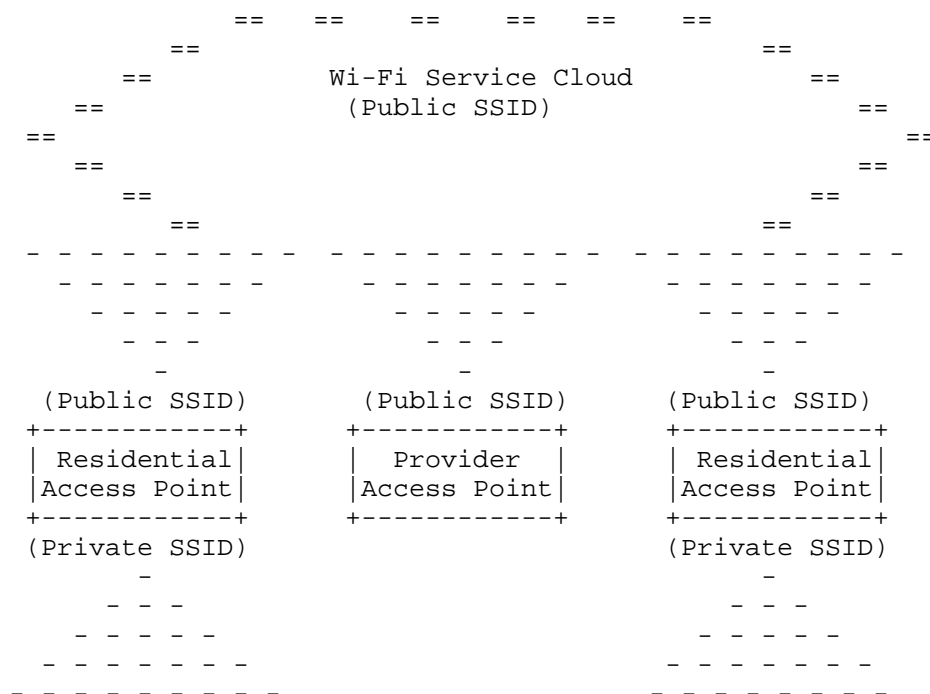


Figure 1: Wi-Fi Cloud Over Residential Gateways

2. Conventions and Terminology

2.1. Conventions

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].

2.2. Terminology

This document uses the following abbreviations and definitions:

Community Wi-Fi Service

It is a Wi-Fi based broadband service offered by a service provider. The Wi-Fi Access Points that are part of this service are owned and managed by the operator, and physically located in carrier premises. These operator owned CPE's typically have a large Wi-Fi coverage area, operated on a higher signal power.

There could also be the residential Access Points that are part of this service, located in the subscriber homes, that are part of this service and allowing community access to a public SSID along with a private SSID for their personal access.

Wi-Fi Operator

A service provider that offers Community Wi-Fi services. Wi-Fi operator can be a wireline operator, mobile operator or an operator offering both wireline and mobile services.

Residential Gateway (RG)

It is a network device that is located in the Customer premises and is also referred to as Residential CPE (Customer Premises Equipment). This device is connected to service providers network and defines the demarcation point between the provider and the customer. In the context of this document this is hosting the 802.11 Access Point function.

WLAN controller (WLC)

It is an entity responsible for performing radio resource management (RRM) on the Access Points, system-wide mobility policy enforcement and centralized forwarding function for the user traffic.

Mobile Gateway

It is network entity anchoring IP traffic in the mobile core network. This entity allocates an IP address which is topologically valid in the mobile network and may act as a mobility anchor if handover between mobile and Wi-Fi is supported.

Home/Roaming User

The home user is the owner of the network where the Residential Gateway is located and is paying for the service associated with that Residential Gateway. A Roaming User is a visitor from the operator's home network, or from a partner's network and is allowed to access broadband services using that Residential Gateway and over a Public SSID.

Access Point Name (APN)

Its the name of a packet data network. This APN concept was first introduced in GPRS by 3GPP to enable legacy Intelligent Networking (IN) approaches to be applied to the newly deployed IP packet data services. In roaming deployments, the APN construct was visible to the visited network and allowed legacy IN charging solutions to be supported. Defining an application specific APN then allowed application charging to be supported.

Addressing Models

The term Per-MN-Prefix model [RFC5213] is used to refer to an addressing model where there is a unique network prefix or prefixes assigned for each mobile node. The term Shared-Prefix model [RFC5213] is used to refer to an addressing model where the prefix(es) are shared by more than one node.

3. Deployment Models

Figure 2 illustrates the most common residential and hotspots Wi-Fi deployment models.

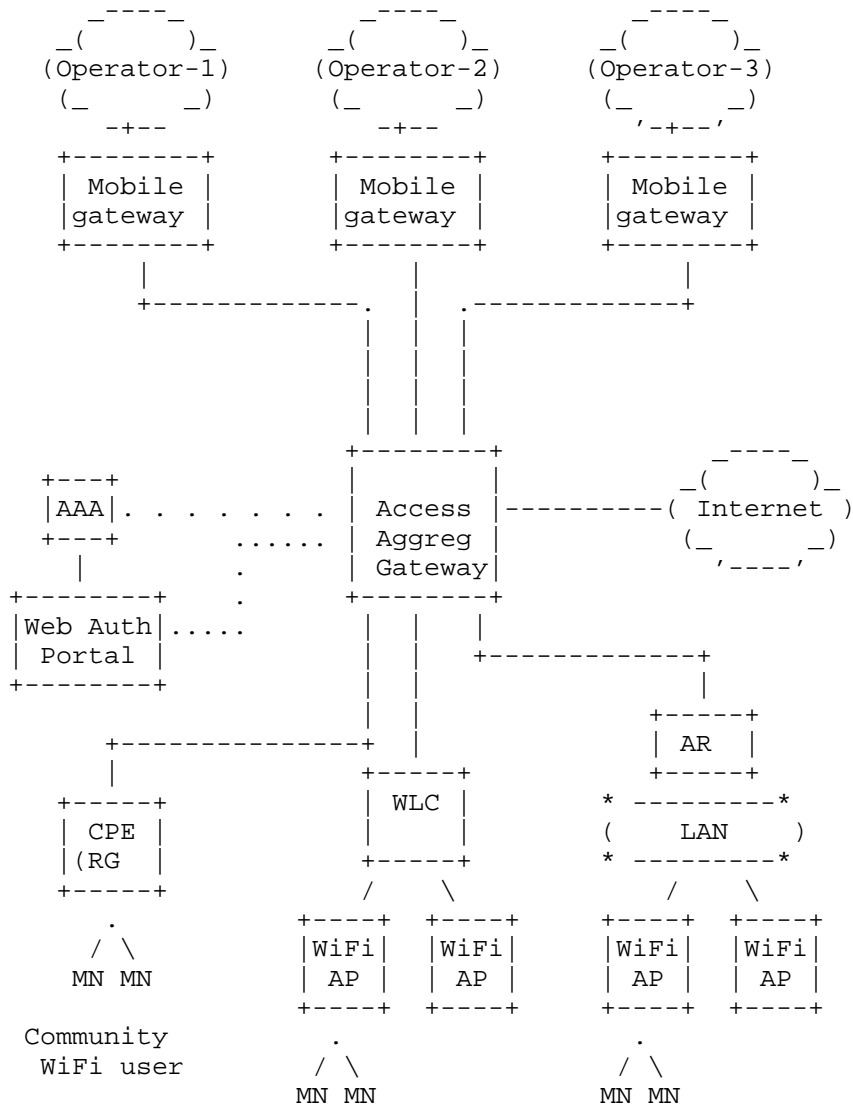


Figure 2: WLAN Service for Retail Model

4. Requirements

4.1. IPv6 Addressing Model for SP WiFI Architectures

The selection of the right IPv6 addressing model for the SP WiFI architectures is an important consideration. There are these two IPv6 addressing models:

- o Unique-Prefix Model - As per this addressing model, home network prefix(es) assigned to a mobile node are for its exclusive use and no other node shares an address from that prefix (other than the Subnet-Router anycast address [RFC4291] that is used by the IPv6 access router hosting that prefix on that link). There could be multiple unique IPv6 prefixes assigned to each mobile node.
- o Shared-Prefix model - The IPv6 prefix that is assigned to the mobile node is a shared prefix. There can be more than one mobile node that can be using IPv6 addresses from that prefix.

3GPP architecture supports Unique-Prefix model for the mobile node's PDN connections. This decision was largely influenced by the IETF recommendation to 3GPP to support this specific addressing model. In the context of SP WiFI, there are clearly scenarios where a mobile node may perform an inter-technology handover from the macro network to the WLAN access network and handoff the session and is important that the addressing model is the same in both the access architectures. Even in deployment models where such handovers are not envisioned, such as an WLAN access aggregation architecture with no mobile packet core integration, there are sufficient reasons for adopting the Unique Prefix model.

4.2. Subscriber Authentication & Service Authorization

Community Wi-Fi service is designed to be available for public access. Wi-Fi operator must authenticate users before offering services to them. Once a user is authenticated, Wi-Fi operator will authorize services based on the user identity. There are many authentication mechanisms, such as 802.1x, Web-authentication, WISPr that the operator may deploy for this purpose.

4.3. Location-based Services

In many deployments, there is a need for the mobile operator to provide differentiated services and policing to the mobile nodes based on the access network to which they are attached. Policy systems in mobility architectures such as PCC and ANDSF in 3GPP system allow configuration of policy rules with conditions based on the access network information. For example, the service treatment for the mobile node's traffic may be different when they are attached to a access network owned by the home operator than when owned by a

roaming partner. The service treatment can also be different based on the configured Service Set Identifiers (SSID) in case of IEEE 802.11 based access networks. Other examples of location services include the operator's ability to display a location specific Web Page, or apply tariff based on the location.

4.4. Local Services Access & Internet Traffic Offload

In the integrated WLAN-EPC architectures, the mobile node's IP traffic is always tunneled back from the access network to the mobile gateway in the home network. However, with the exponential growth in the mobile data traffic, mobile operators are exploring new ways to offload some of the IP traffic flows at the nearest access edge where ever there is an internet peering point, as supposed to carrying it all the way to the mobility anchor in the home network. Not all IP traffic need to be routed back to the home network, some of the non-essential traffic which does not require IP mobility support can be offloaded at the mobile access gateway in the access network. This approach provides greater leverage and efficient usage of the mobile packet core which help lowering transport cost.

4.5. Web-based Authentication Support

Most Public Wireless LAN (PWLAN) deployments today use web-based authentication for authorizing the user for network access. Web-based mode of authentication is considered a legacy mode, for its weak security properties, and there are efforts to replace it with 802.1x-based security mechanisms. However, a very high percentage of the PWLAN deployments are still using using this authentication mode and operators are not willing to move away from this mode any time soon. The reason being, lack of support for 802.1x/EAP support on the 100's of millions of handsets that are out there, and for the lack of client software in the laptops running various operating systems versions. This is forcing the operators to support web-based authentication.

4.6. Transparent Auto Login (TAL)

In many deployments, there is a need to support Transparent Auto Login capability. This is essentially an approach for maintaining Authenticated state for a user, for a duration of time. Once an authenticated user disconnects and re-attaches to the network, the network should allows instant access without forcing the user to re-authenticate.

4.7. Multiple WLAN SSID Support

A Wi-Fi Operator may broadcast multiple SSIDs. In case Residential Wi-Fi hotspots, there can be one set of private SSIDs specific to that home user and there can be another set of public SSIDs for wider community use. In case of public hotspots, the operator can advertise the public SSID for its own subscribers and also public SSID's belonging to other operators with whom the operator has roaming relationships.

4.8. Multiple Home Network Service (APN) Access

The 3GPP system architecture supports the concept of an Access Point Name (APN). An APN can identify a particular routing domain and can be used by 3GPP operators to segment user traffic. APNs are included in the session establishment signaling sent by 3GPP User Equipments (UEs), identifying which routing domain they want to be connected to. Furthermore, 3GPP has defined a system architecture which supports the ability of a single UE to have simultaneous connectivity to a plurality of APNs, and be allocated multiple IPv4 addresses and/or IPv6 prefixes from the network.

There is a need to ensure multiple APN access for a subscriber in the community Wi-Fi network.

4.9. CPE Identity and Authorization

There are two known models with respect to CPE roll out. The consumer may purchase a device off the shelf and plugin to the network, or the operator at the time of service creation may have shipped a new device with the pre-provisioned service configuration. In either case, the operator needs to be able to identify the device based on the IP address and associate that to a given location.

The Wi-Fi network performs access control of UEs, via the CPE acting as AAA supplicant. As a result, the mobile network does not authenticate directly the user but shall trust the CPE performing the authentication.

4.10. Mobility within the WLAN Access Network

The mobile node should have the ability to roam within the Wi-Fi domain. Depending on the deployment model, the mobile node may roam across different IP subnets. To survive to such handover, some applications (e.g. VPN, streaming) need the IP address to be preserved.

A WLAN network may include a large number of Wi-Fi base stations. In

some occasions, two or more Wi-Fi base stations may cover the same area. When a subscriber receives Wi-Fi service in this overlapped area, the device may bounce between different base stations. This is typical Proximity problem. In this scenario, it is important for the WLAN to offer mobility to the subscriber as such the subscriber can continue the services without changing its IP address.

4.11. Mobility across WLAN and Macro Access

A mobile node should have the ability to handover from macro network to the Wi-Fi network and be able to retain IP address configuration and be able to access the home operator services.

4.12. Differentiated Services for Users behind RG

A Wi-Fi operator enabling Hotspot Services on a residential gateway is required to ensure the service levels for the home user is not impacted as a result of opening up the service for public usage. The home user should always have preferred access over public users and the operator may be bound to meet the Service Level Agreements. This essentially requires the operator to be able to differentiate the service flows and apply differentiated service treatment. The operator should be able to enforce QoS policing and labeling of packets to enforce QoS differentiation.

A single operator has deployed both a fixed access network and a mobile access network. In this scenario, the operator may wish a harmonized QoS management on both accesses. However the fixed access network does not implement a QoS control framework. So, the operator may choose to rely on the mobile network, specifying the standard framework to provide a QoS control, to enforce the QoS policy from the mobile gateway to the Wi-Fi Access network.

4.13. Lawful Intercept (LI)

Lawful Intercept [RFC2119] stands for legally authorized interception and monitoring of communications to and from a subscriber under Surveillance by a Law Enforcement Agency. In most of the countries, there are legal obligations for Service Providers to facilitate the intercept of any subscriber's communication if requested by law enforcement agencies. Communications Assistance for Law Enforcement Act (CALEA), the United States wiretapping law passed in 1994 is an example for such legal mandates. This section talks about Lawful Intercept solution requirements that are operators are required to support when offering WLAN services.

The following are the key considerations with respect to supporting Lawful Intercept capability in Wi-Fi architectures.

- o The operator should have the ability to capture IP traffic from any of the mobile nodes for which the operator is offering Wi-Fi services.
- o The ability to identify the Geo-location of the mobile node to the nearest WLAN access point.
- o The ability to track the mobile node's roaming within the network, even when there are no active IP flows.
- o The ability to pre-provision Lawful Intercept for an inactive mobile node so that that the capture of IP traffic can be initiated anytime new IP flows associated to that mobile node are detected.
- o Lawful Intercept (LI) should be undetectable by the intercept subject
- o Mechanisms should be in place to limit unauthorized personnel from performing or knowing about lawfully authorized intercepts
- o If the information being intercepted is encrypted by the service provider and the service provider has access to the keys, then the information should be decrypted before delivery to the Law Enforcement Agency (LEA) or the encryption keys should be passed to the Law Enforcement Agency to allow them to decrypt the information.

4.14. Subscriber Management and Charging

It refers to the capability to manage network resources on a per subscriber, and eventually on a per-flow, basis. Subscriber management should be able to maintain a user context associating the user identifier with specific network resource (e.g. IP address, default router, mobility/traffic anchoring point,...), QoS profile, billing context and specific network functions (e.g. legal interception). The user context includes traffic selectors if subscriber management is on a per flow basis. Subscriber management should be done according to the user subscription, the user preferences and/or operator policies.

The ability to charge the subscriber is the fundamental business requirement before an operator can deploy the Wi-Fi service. The operator should have the ability to enforce charge the subscriber by usage and enforce quota policies. This is the basis for keeping the service operational and managing inter-operator roaming agreements.

4.15. Handling the Walk-by Users

In the case of community Wi-Fi, the network is an open network with the SSID visible to any wireless LAN device. This essentially creates a situation where any walk-by user's mobile terminal automatically gets connected to the Wi-Fi network and results in a subscriber session creation. The user may not be having any intention in connecting to the Wi-fi network and infact may not be using the mobile device, but the device gets attached to the network and a subscriber session and other network resources get locked up for that user session. The situation is especially worse in public hotspots such as train stations, or Airports where there is high traffic. This is important that this situation is correctly handled.

4.16. Overlapping IPv4 Address Support

The transition from IPv4 to IPv6 is a long process, and during this period of transition, the Wi-Fi operators will have to continue to offer IPv4 services. However, these operators may not have sufficient public IPv4 addresses for all the Wi-Fi devices in their network. For addressing this IPv4 exhaust issue, operators may have to leverage transitioning technologies such as NAT64, Dual-Stack Lite, 6rd or other approaches. These operators may also choose to segment the network into regions and two regions may use overlapped IPv4 address space to provide IPv4 services to users.

In a different scenario, a roaming user from a partners network, with an established mobility session with her home network, may be using a private IPv4 address and this IPv4 address may be overlapping with the address space that is being used in this access network. Furthermore, the IPv4 address space that is used for assignment to Wi-Fi subscribers should not conflict with the IPv4 addresses used on the Cable/DSL transport network.

The Wi-Fi operator should be able to handle all these scenarios related to overlapping private IPv4 address usage.

4.17. Service Provisioning & Monitoring

Deployment of any community based Wi-Fi access will require additional Wi-Fi specific configuration on a per Residential Gateway basis. In order to support scalable deployment, the Service Providers should be able to provision these configuration options remotely. This remote provisioning frame work must support the following:

- o Secure provisioning of the RG with community WiFi parameters to minimize the theft of service
- o Ability to separate the private home subscriber traffic from the community WiFi traffic in the access network
- o Privacy and protection of private Residential subscriber traffic from the community WiFi users
- o Ability to remotely shut down an Residential Gateway which has been hijacked by hackers and is being used for DoS attacks.
- o Ability to temporarily disable services for the community based WiFi support while maintaining service to the Residential fixed broadband subscriber
- o Seamless integration of the WiFi provisioning aspects of the Residential Gateway into the existing RG provisioning infrastructure implemented by the Fixed Broadband Providers
- o Dynamic Service Monitoring Capability for managing the Wi-Fi Service.

5. Solution Approaches & Considerations

The following section identifies the different mobility approaches that Wi-Fi operator can leverage for deploying this Wi-Fi services.

- 5.1. PMIPv6 MAG on the RG: Layer-3 Encapsulation between CPE and Access Gateway
- 5.2. Ethernet-over-IP Support on the RG: Layer-2 Encapsulation between CPE and Access Gateway
- 5.3. Local Aggregation for Subscriber Control and Internet Offload
- 5.4. Mobility Chaining: Integration with Mobile Packet Core

6. IANA Considerations

This document does not require any IANA actions.

7. Security Considerations

This specification identifies the requirements for enabling Community

Wi-Fi Services over Residential architectures and the potential solution approaches for addressing those requirements. The security analysis for each of those requirements are covered in those respective sections.

8. Acknowledgements

The authors would like to thank Bill Choinski, John Coppola and Sangeeta Ramakrishnan for all the discussions related to Service Provider Wi-Fi Service requirements. The authors would also like to thank Byju Pularikkal for all the discussions and text contributions related to Lawful Interception and Service Provisioning.

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.

9.2. Informative References

- [I-D.gundavelli-netext-multiple-apn-pmipv6]
Gundavelli, S., Grayson, M., Lee, Y., Deng, H., and H. Yokota, "Multiple APN Support for Trusted Wireless LAN Access", draft-gundavelli-netext-multiple-apn-pmipv6-01 (work in progress), February 2012.
- [I-D.gundavelli-netext-pmipv6-wlan-applicability]
Gundavelli, S., "Applicability of Proxy Mobile IPv6 Protocol for WLAN Access Networks", draft-gundavelli-netext-pmipv6-wlan-applicability-03 (work in progress), April 2012.
- [I-D.ietf-netext-pmipv6-qos]
Liebsch, M., Seite, P., Yokota, H., Korhonen, J., and S. Gundavelli, "Quality of Service Option for Proxy Mobile IPv6", draft-ietf-netext-pmipv6-qos-00 (work in progress), June 2012.
- [I-D.ietf-netext-pmipv6-sipto-option]
Gundavelli, S., Zhou, X., Korhonen, J., and R. Koodli, "IPv4 Traffic Offload Selector Option for Proxy Mobile IPv6", draft-ietf-netext-pmipv6-sipto-option-07 (work in progress), October 2012.

- [I-D.liebsch-netext-pmip6-authiwb]
Gundavelli, S., Liebsch, M., and P. Seite, "PMIPv6 inter-working with WiFi access authentication",
draft-liebsch-netext-pmip6-authiwb-05 (work in progress),
September 2012.
- [RFC2663] Srisuresh, P. and M. Holdrege, "IP Network Address
Translator (NAT) Terminology and Considerations",
RFC 2663, August 1999.
- [RFC3924] Baker, F., Foster, B., and C. Sharp, "Cisco Architecture
for Lawful Intercept in IP Networks", RFC 3924,
October 2004.
- [RFC4291] Hinden, R. and S. Deering, "IP Version 6 Addressing
Architecture", RFC 4291, February 2006.
- [RFC5213] Gundavelli, S., Leung, K., Devarapalli, V., Chowdhury, K.,
and B. Patil, "Proxy Mobile IPv6", RFC 5213, August 2008.
- [RFC5844] Wakikawa, R. and S. Gundavelli, "IPv4 Support for Proxy
Mobile IPv6", RFC 5844, May 2010.
- [RFC6757] Gundavelli, S., Korhonen, J., Grayson, M., Leung, K., and
R. Pazhyannur, "Access Network Identifier (ANI) Option for
Proxy Mobile IPv6", RFC 6757, October 2012.
- [TS23402] 3GPP, "Architecture enhancements for non-3GPP accesses",
2010.

Authors' Addresses

Sri Gundavelli
Cisco
170 West Tasman Drive
San Jose, CA 95134
USA

Email: sgundave@cisco.com

Mark Grayson
Cisco
11 New Square Park
Bedfont Lakes, FELTHAM TW14 8HA
ENGLAND

Email: mgrayson@cisco.com

Pierrick Seite
France Telecom - Orange
4, rue du clos courtel BP 91226
Cesson-Sevigne, 35512
France

Email: pierrick.seite@orange-ftgroup.com

Yiu L. Lee
Comcast
One Comcast Center
Philadelphia, PA 19103
U.S.A.

Email: yiu_lee@cable.comcast.com
URI: <http://www.comcast.com>

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

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 March 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	3
2. Caution	3
3. Terminology	4
4. Architecture Overview	5
5. Requirements for MN Identification behind a CPE with NAT	7
5.1. Recommendations for MN Identification behind NAT	8
6. Requirements for MN Mobility in Fixed Broadband Network	9
7. Requirements for Link Characteristic Information	9
7.1. Adaptive Application and Services	10
7.2. Network-Initiated Handover	10
7.3. End-to-End path characteristics	10
7.4. Requirements for Link and Sub-Path Information delivery	10
8. Security Considerations	11
9. IANA considerations	11
10. Acknowledgments	11
11. References	11
11.1. Normative References	11
11.2. Informative references	11
Appendix A. Requirements for Content Adaptation	14
A.1. Recommendations for Content Adaptation	14
Authors' Addresses	14

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

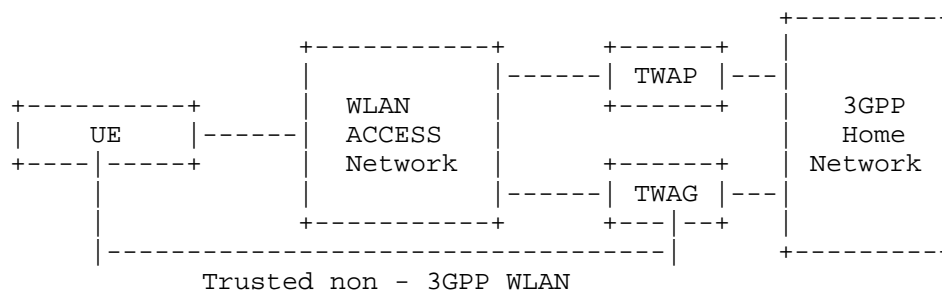
General requirements for FMC are common service and subscriber profiles. Additionally common charging, operational and management procedures are also required. Additional requirements for IP traffic

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:



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:

- o All traffic **MUST** be identifiable (including TCP, UDP and ICMP)
- o The MN **SHOULD** be authenticated if it injects its own host-id
- o Otherwise, the CPE **SHOULD** inject the host-id
- o The CPE **SHOULD** strip any existing host-id
- o 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

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

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	3
2. Use case 1: Group Identification	3
3. Use case 2: Requirements for UE Mobility in Fixed Broadband Network	5
4. IANA Considerations	5
5. Security Considerations	5
6. Acknowledgements	6
7. References	6
7.1. Normative References	6
7.2. Informative References	6
Authors' Addresses	6

1. Introduction

In the FMC (fix/mobile convergence) network, the major converged aspects include the converged business and service, converged network and infrastructure, 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 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 [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 Identification, 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 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 technology. 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 technology, 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

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

C. Xie
Q. Sun
China Telecom
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	3
2. Use case 1: Unified User Identification	3
3. Use case 2: Unified QoS provisioning capability	5
4. Use case 3: Seamless handover for VPDN tunnel	6
5. Use case 4: Mobility	7
6. IANA Considerations	9
7. Security Considerations	9
8. Acknowledgements	9
9. References	9
9.1. Normative References	9
9.2. Informative References	9
Authors' Addresses	10

1. Introduction

In the FMC (Fixed Mobile Convergence) architecture, the major FMC could be divided 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 maintain 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 customer can use this subscriber-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 identification, 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.

Subscriber A have three
device, X, Y, Z

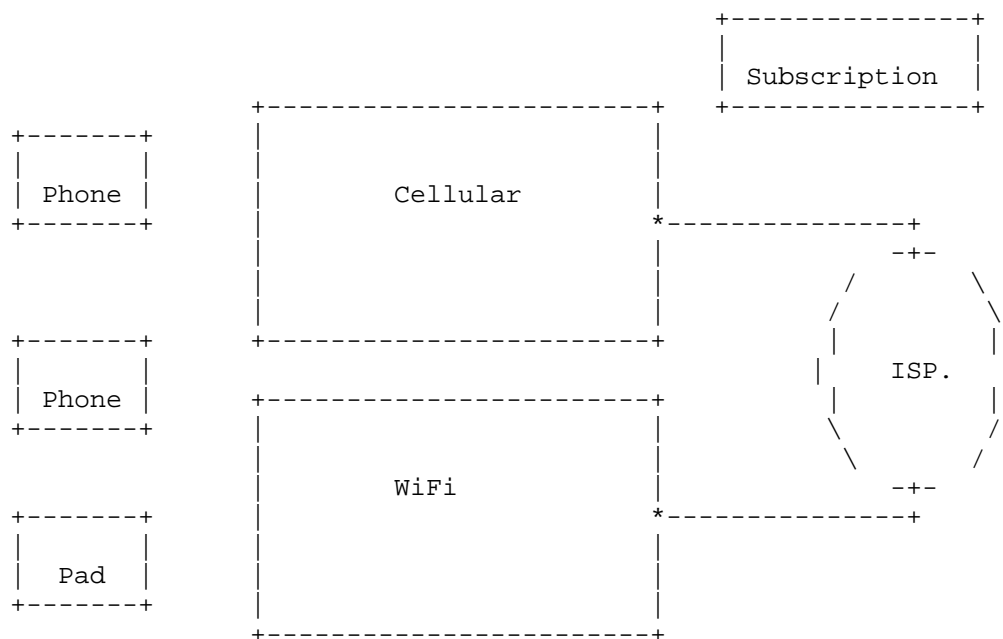


Figure 1

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. Additional 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.

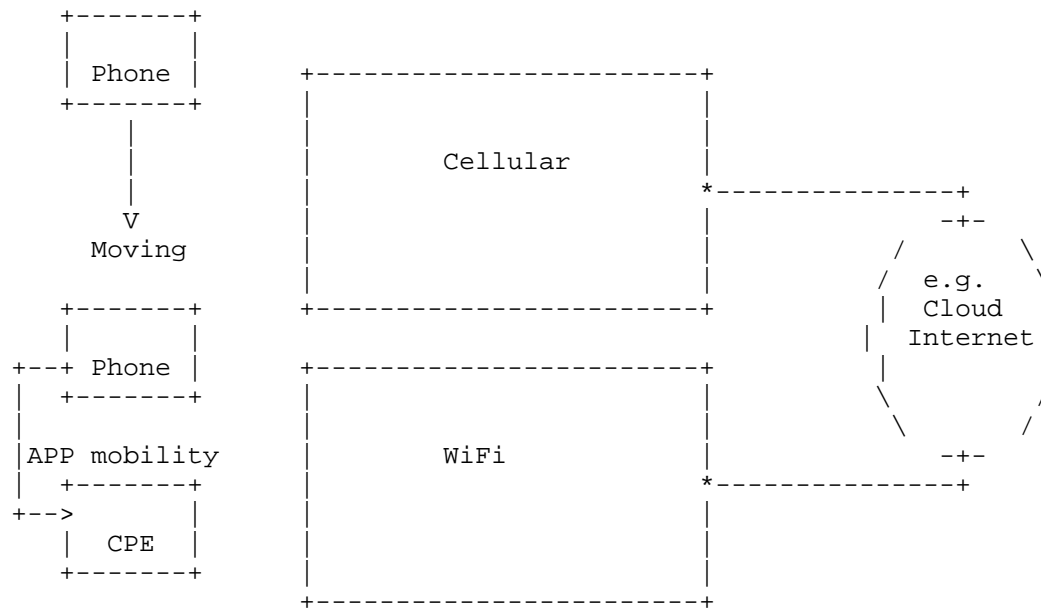


Figure 2

In this scenario, different devices will have the special requirement on display resolution, codec, etc. Additionally, 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 to 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 heterogeneous 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 a 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.

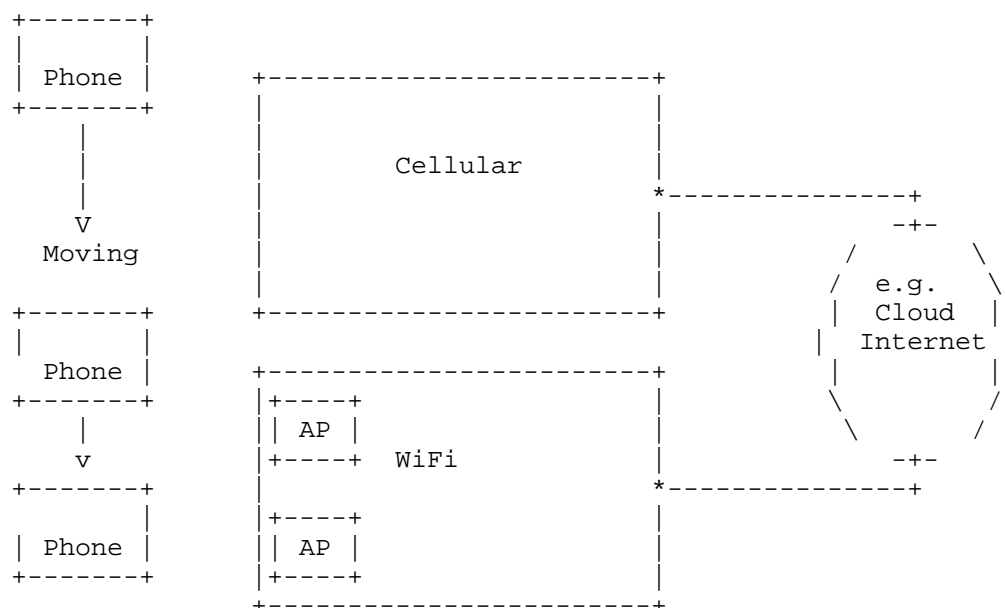


Figure 3

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 technology. 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 special requirement for UE identifier.

2. When the service application from one device to another device 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 mechanism is needed.
3. In the scenario of WiFi, the service QoS and experience between different APs should be guaranteed 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

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

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	3
2. Conventions and Terminology	6
3. Key Issues in Fixed Mobile Converged Interworking	7
4. Group Id in Fixed Broadband Network	7
5. UE Mobility in Fixed Broadband Network	10
6. IANA Considerations	12
7. Security Considerations	12
8. Acknowledgements	12
9. References	12
9.1. Normative References	12
9.2. Informative References	13
Authors' Addresses	13

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. Femto cell) [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 truly 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].

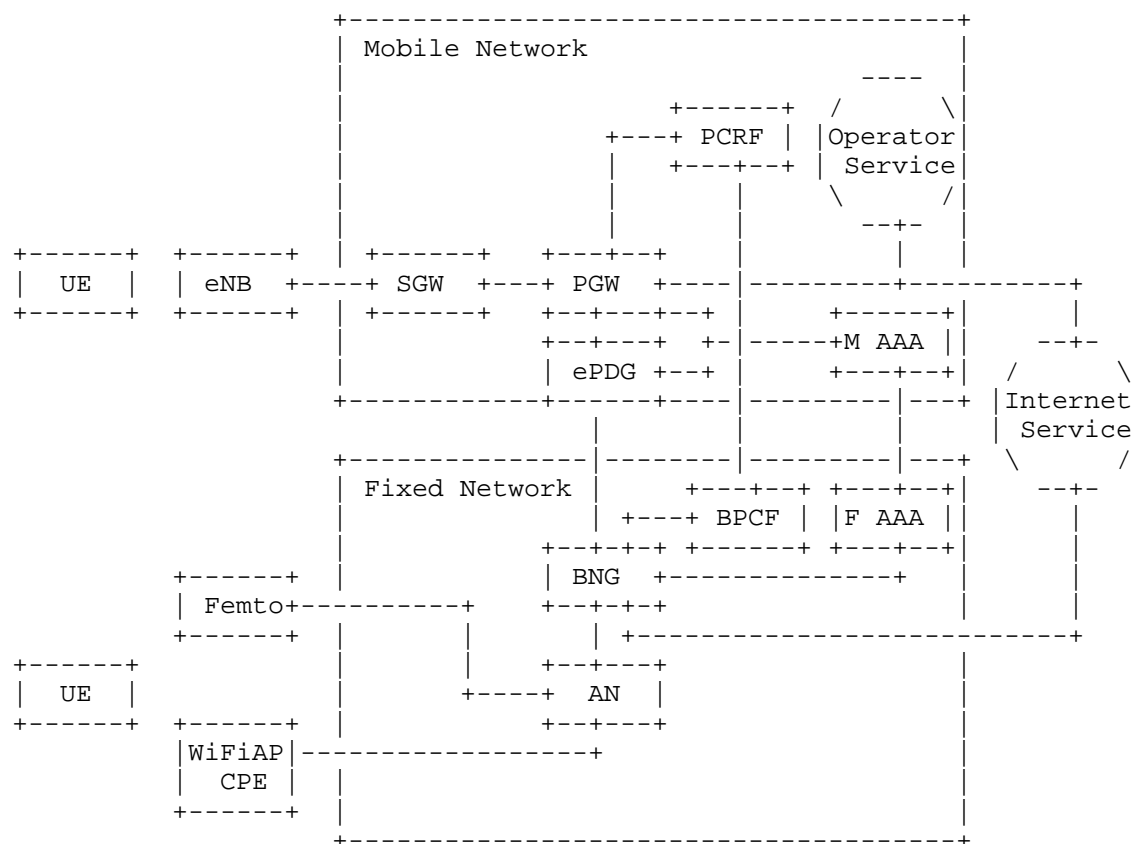


Figure 1: Reference Architecture of Fixed Mobile Convergence

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 synchronized 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.

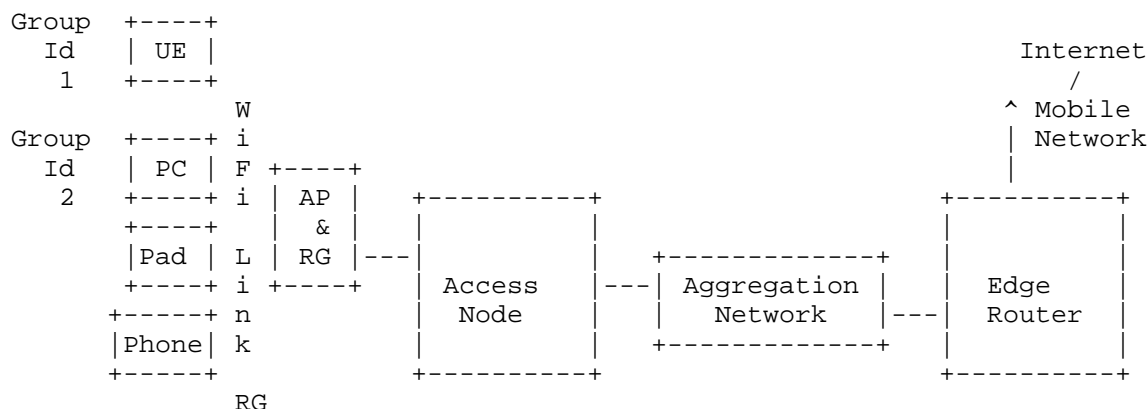


Figure 2: Group Identification in Broadband Network

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.

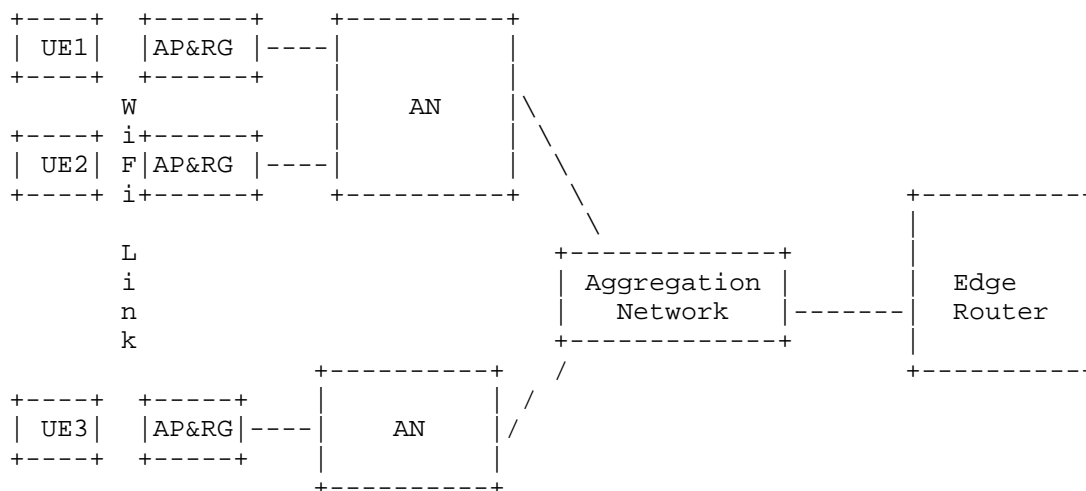


Figure 3: UE Mobility in Broadband Network

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

