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.

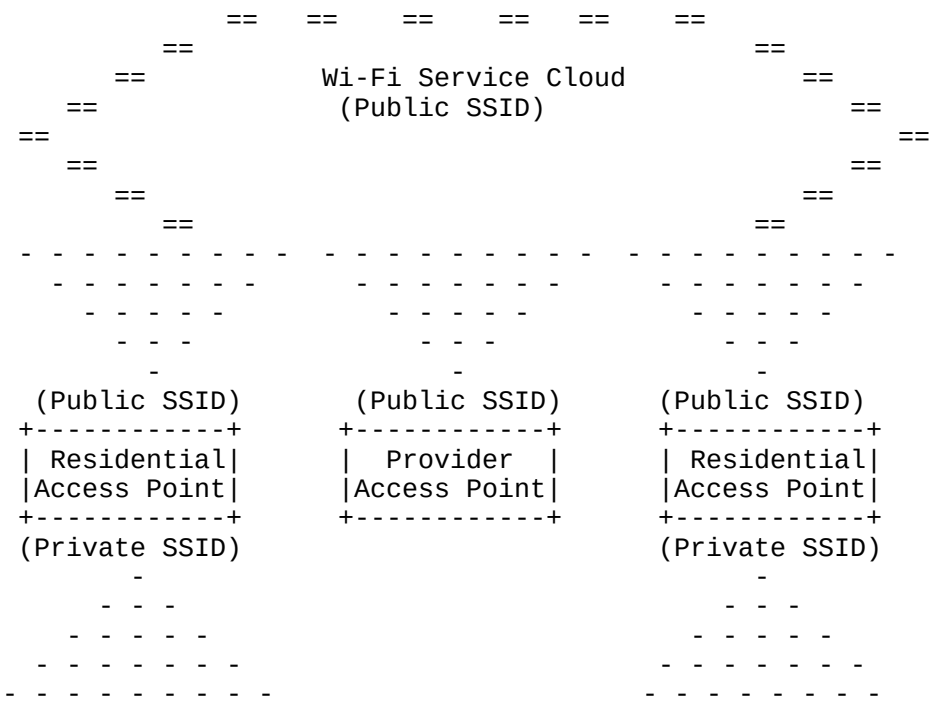

Figure 1: Wi-Fi Cloud Over Residential Gateways

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.

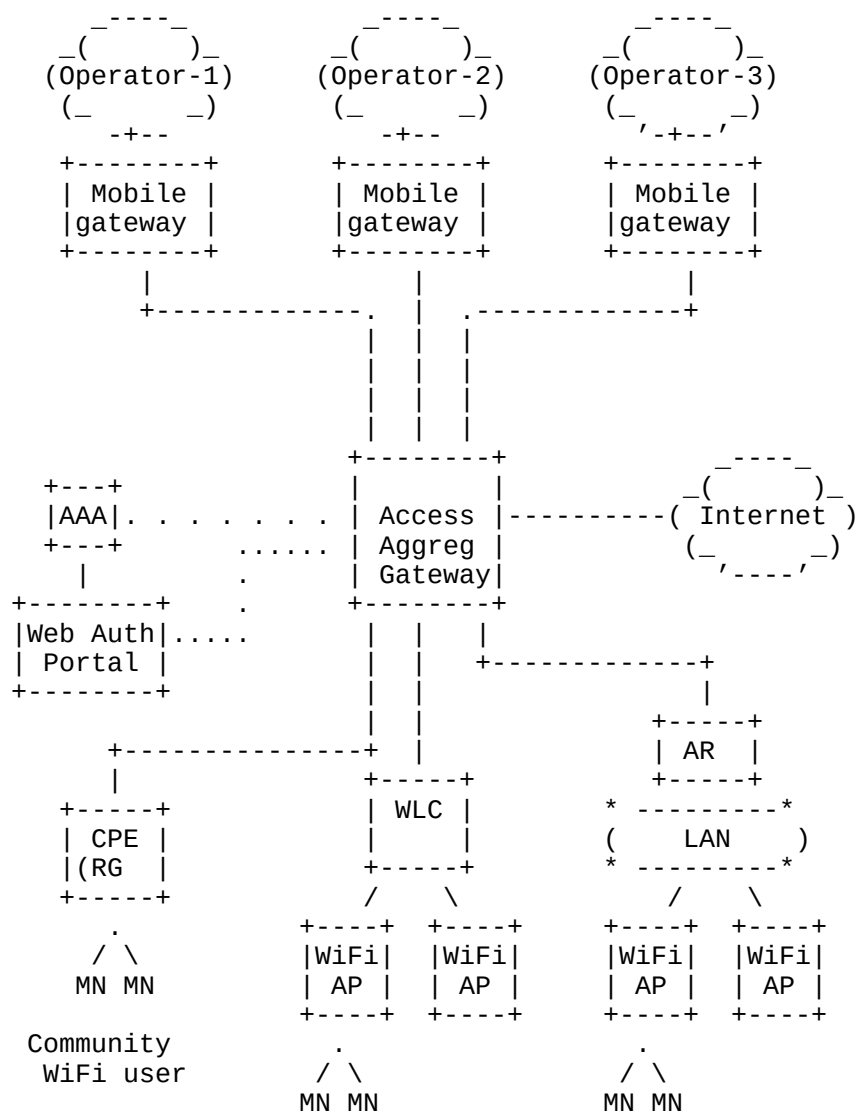

Figure 2: WLAN Service for Retail Model

4. Requirements

4.1. IPv6 Addressing Model for SP WiFI Architectures

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

- 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.

- 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 no 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.

- 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.
- The ability to identify the Geo-location of the mobile node to the nearest WLAN access point.
- The ability to track the mobile node’s roaming within the network, even when there are no active IP flows.
- 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.
- Lawful Intercept (LI) should be undetectable by the intercept subject
- Mechanisms should be in place to limit unauthorized personnel from performing or knowing about lawfully authorized intercepts
- 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:

- Secure provisioning of the RG with community WiFi parameters to minimize the theft of service
- Ability to separate the private home subscriber traffic from the community WiFi traffic in the access network
- Privacy and protection of private Residential subscriber traffic from the community WiFi users
- Ability to remotely shut down an Residential Gateway which has been hijacked by hackers and is being used for DoS attacks.
- Ability to temporarily disable services for the community based WiFi support while maintaining service to the Residential fixed broadband subscriber
- Seamless integration of the WiFi provisioning aspects of the Residential Gateway into the existing RG provisioning infrastructure implemented by the Fixed Broadband Providers
- 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-pmip6-qos]
Liebsch, M., Seite, P., Yokota, H., Korhonen, J., and S. Gundavelli, "Quality of Service Option for Proxy Mobile IPv6", draft-ietf-netext-pmip6-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-authiwk]
Gundavelli, S., Liebsch, M., and P. Seite, "PMIPv6 inter-working with WiFi access authentication", draft-liebsch-netext-pmip6-authiwk-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