

v6ops Working Group
Internet-Draft
Intended status: Informational
Expires: November 20, 2011

Rajeev. Koodli
Cisco Systems
May 19, 2011

Mobile Networks Considerations for IPv6 Deployment
draft-ietf-v6ops-v6-in-mobile-networks-05.txt

Abstract

Mobile Internet access from smartphones and other mobile devices is accelerating the exhaustion of IPv4 addresses. IPv6 is widely seen as crucial for the continued operation and growth of the Internet, and in particular, it is critical in mobile networks. This document discusses the issues that arise when deploying IPv6 in mobile networks. Hence, this document can be a useful reference for service providers and network designers.

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 November 20, 2011.

Copyright Notice

Copyright (c) 2011 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. Reference Architecture and Terminology	3
3. IPv6 Considerations	5
3.1. IPv4 Address Exhaustion	5
3.2. NAT Placement in the mobile networks	7
3.3. IPv6-only Deployment Considerations	10
3.4. Fixed - Mobile Convergence	13
4. Summary and Conclusion	15
5. Security Considerations	16
6. IANA Considerations	16
7. Acknowledgement	16
8. Informative References	16
Appendix A. Change Log	18
Author's Address	18

1. Introduction

The dramatic growth of the Mobile Internet is accelerating the exhaustion of the available IPv4 addresses. It is widely accepted that IPv6 is necessary for the continued operation and growth of the Internet in general, and that of the Mobile Internet in particular. While IPv6 brings many benefits, certain unique challenges arise when deploying it in mobile networks. This document describes such challenges and outlines the applicability of the existing IPv6 deployment solutions. As such, it can be a useful reference document for service providers as well as network designers. This document does not propose any new protocols or suggest new protocol specification work.

The primary considerations that we address in this document on IPv6 deployment in mobile networks are:

- o Public and Private IPv4 address exhaustion and implications to mobile network deployment architecture;
- o Placement of Network Address Translation (NAT) functionality and its implications;
- o IPv6-only deployment considerations and roaming implications;
- o Fixed-Mobile Convergence and implications to overall architecture.

In the following sections, we discuss each of these in detail.

For the most part, we assume the 3GPP 3G and 4G network architectures specified in [3gpp.3g] and [3gpp.4g]. However, the considerations are general enough for other mobile network architectures as well [3gpp2.ehrpd].

2. Reference Architecture and Terminology

The following is a reference architecture of a mobile network.

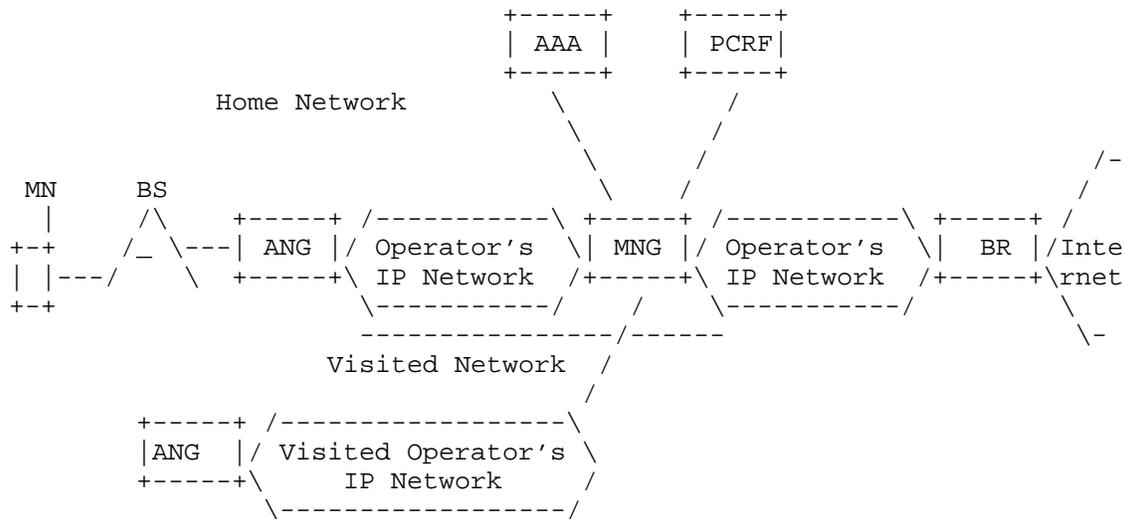


Figure 1: Mobile Network Architecture

A Mobile Node (MN) connects to the mobile network either via its Home Network or via a Visited Network when the user is roaming outside of the Home Network. In the 3GPP network architecture, a MN accesses the network by connecting to an Access Point Name (APN), which maps to a mobile gateway. Roughly speaking, an APN is similar to an SSID in wireless LAN. An APN is a logical concept which can be used to specify what kinds of services, such as Internet access, high-definition video streaming, content-rich gaming, and so on, a MN is entitled to. Each APN can specify what type of IP connectivity (i.e., IPv4, IPv6, IPv4v6) is enabled on that particular APN.

While an APN directs a MN to an appropriate gateway, the MN needs an end-to-end "link" to that gateway. In the Long-Term Evolution (LTE) networks, this link is realized through an Evolved Packet System (EPS) bearer. In the 3G UMTS networks, such a link is realized through a Packet Data Protocol (PDP) Context. The end-to-end link traverses multiple nodes which are defined below:

- o Base Station (BS): The radio Base Station provides wireless connectivity to the MN.
- o Access Network Gateway (ANG): The ANG forwards IP packets to and from the MN. Typically, this is not the MN's default router, and the ANG does not perform IP address allocation and management for the mobile nodes. The ANG is located either in the Home Network or in the Visited Network.

- o The Mobile Network Gateway (MNG): The MNG is the MN's default router which provides IP address management. The MNG performs functions such as offering Quality of Service (QoS), applying subscriber-specific policy, and enabling billing and accounting; these functions are sometimes collectively referred to as "subscriber-management" operations. The mobile network architecture, as shown in the figure, defines the necessary protocol interfaces to enable subscriber management operations. The MNG is typically located in the Home Network.

- o Border Router (BR): As the name implies, a BR borders the Internet for the mobile network. The BR does not perform subscriber management for the mobile network.

- o Authentication, Authorization and Accounting (AAA): The general functionality of AAA is used for subscriber authentication and authorization for services, as well as for generating billing and accounting information.

In the 3GPP network environments, the subscriber authentication and the subsequent authorization for connectivity and services is provided using the "Home Location Register" (HLR)/"Home Subscriber Server" (HSS) functionality.

- o Policy and Charging Rule Function (PCRF): The PCRF enables applying policy and charging rules at the MNG.

In the rest of this document, we use the terms operator, service provider or provider interchangeably.

3. IPv6 Considerations

3.1. IPv4 Address Exhaustion

It is generally agreed that the pool of public IPv4 addresses is nearing its exhaustion. The IANA has exhausted the available '/8' blocks for allocation to the Regional Internet Registries (RIRs). The RIRs themselves have either "run-out" of their blocks or are projected to exhaust them in the near future. This has led to a heightened awareness among the service providers to consider introducing technologies to keep the Internet operational. For providers, there are two simultaneous approaches to addressing the run-out problem: delaying the IPv4 address pool exhaustion (i.e., conserving their existing pool) and introducing IPv6 in operational networks. We consider both in the following.

Delaying the public IPv4 address exhaustion for providers involves assigning private IPv4 addressing for end-users, or extending an IPv4 address with the use of port ranges which requires tunneling and additional signaling. A mechanism such as the Network Address Translator (NAT) is used at the provider premises (as opposed to customer premises) to manage the private IP address assignment and access to the Internet. In the following, we primarily focus on translation based mechanisms such as NAT44 (i.e., translation from public IPv4 to private IPv4 and vice versa) and NAT64 (i.e., translation from public IPv6 to public IPv4 and vice versa). We do this because the 3GPP architecture already defines a tunneling infrastructure with the GPRS Tunneling Protocol (GTP), and the architecture allows for dual-stack and IPv6-only deployments.

In a mobile network, the IPv4 address assignment for a MN is performed by the MNG. In the 3GPP network architecture, this assignment is performed in conjunction with the PDN connectivity establishment. A PDN connection implies an end-end link (i.e., an EPS bearer in 4G LTE or a PDP context in 3G UMTS) from the MN to the MNG. There can be one or more PDN connections active at any given time for each MN. A PDN connection may support both IPv4 and IPv6 traffic (as in a dual-stack PDN in 4G LTE networks) or it may support only one of the two traffic types (as in the existing 3G UMTS networks). The IPv4 address is assigned at the time of PDN connectivity establishment, or is assigned using the DHCP protocol after the PDN connectivity is established. In order to delay the exhaustion of public IPv4 addresses, this IP address needs to be a private IPv4 address which is translated into a shared public IPv4 address. Hence, there is a need for private - public IPv4 translation mechanism in the mobile network.

In the Long-Term Evolution (LTE) 4G network, there is a requirement for an always-on PDN connection in order to reliably reach a mobile user in the All-IP network. This requirement is due to the need for supporting Voice over IP service in LTE which does not have circuit-based infrastructure. If this PDN connection were to use IPv4 addressing, a private IPv4 address is needed for every MN that attaches to the network. This could significantly affect the availability and usage of private IPv4 addresses. One way to address this is by making the always-on PDN (that requires voice service) to be IPv6. The IPv4 PDN is only established when the user needs it.

The 3GPP standards also specify a deferred IPv4 address allocation on a dual-stack IPv4v6 PDN at the time of connection establishment. This has the advantage of a single PDN for IPv6 and IPv4 along with deferring IPv4 address allocation until an application needs it. The deferred address allocation requires support for a dynamic configuration protocol such as DHCP as well as appropriate triggers

to invoke the protocol. Such a support does not exist today in mobile phones. The newer iterations of Smartphones could provide such support. Also, the tethering of Smartphones to laptops (which typically support DHCP) could use deferred allocation depending on when a laptop attaches to the Smartphone. Until appropriate triggers and host stack support is available, the applicability of the address deferring option may be limited.

On the other hand, in the existing 3G UMTS networks, there is no requirement for an always-on connection even though many Smartphones seldom relinquish an established PDP context. The existing so-called pre-Release-8 deployments do not support the dual-stack PDP connection. Hence, two separate PDP connections are necessary to support IPv4 and IPv6 traffic. Even though some MNs, especially the Smartphones, in use today may have IPv6 stack, there are two remaining considerations. First, there is little operational experience and compliance testing with these existing stacks. Hence, it is expected that their use in large deployments may uncover software errors and interoperability problems which inhibit providing services based on IPv6 for such hosts. Second, only a fraction of current phones in use have such a stack. As a result, providers need to test, deploy and operationalize IPv6 as they introduce new handsets which also, continue to need, access to the predominantly IPv4 Internet.

The considerations from the preceding paragraphs lead to the following observations. First, there is an increasing need to support private IPv4 addressing in mobile networks because of the public IPv4 address run-out problem. Correspondingly, there is a greater need for private - public IPv4 translation in the mobile networks. Second, there is support for IPv6 in both 3G and 4G LTE networks already in the form of PDP context and PDN connections. To begin with, the operators can introduce IPv6 for their own applications and services. In other words, the IETF's recommended model of dual-stack IPv6 and IPv4 networks is readily applicable to mobile networks with the support for distinct APNs and the ability to carry IPv6 traffic on PDP/PDN connections. The IETF dual-stack model can be applied using a single IPv4v6 PDN connection in Release-8 and onwards, but requires separate PDP contexts in the earlier releases. Finally, operators can make IPv6 as the default for always-on mobile connections using either the IPv4v6 PDN or the IPv6 PDN, and use IPv4 PDNs as necessary.

3.2. NAT Placement in the mobile networks

In the previous section, we observed that the NAT44 functionality is needed in order to conserve the available pool and delay public IPv4 address exhaustion. However, the available private IPv4 pool itself

is not abundant for large networks such as mobile networks. For instance, the so-called NET10 block [RFC1918] has approximately 16.7 million private IPv4 addresses starting with 10.0.0.0. A large mobile service provider network can easily have more than 16.7 million subscribers attached to the network at a given time. Hence, the private IPv4 address pool management and the placement of NAT44 functionality becomes important.

In addition to the developments cited above, NAT placement is important for other reasons as well. Access networks generally need to produce network and service usage records for billing and accounting. This is true also for mobile networks where "subscriber management" features (i.e., QoS, Policy, and Billing and Accounting) can be fairly detailed. Since a NAT introduces a binding between two addresses, the bindings themselves become necessary information for subscriber management. For instance, the offered QoS on private IPv4 address and the (shared) public IPv4 address may need to be correlated for accounting purposes. As another example, the Application Servers within the provider network may need to treat traffic based on policy provided by the PCRF. If the IP address seen by these Application Servers is not unique, the PCRF needs to be able to inspect the NAT binding to disambiguate among the individual MNs. And, the subscriber session management information and the service usage information also need to be correlated in order to produce harmonized records. Furthermore, there may be legal requirements for storing the NAT binding records. Indeed, these problems disappear with the transition to IPv6. For now, it suffices to state that NAT introduces state which needs to be correlated and possibly stored with other routine subscriber information.

Mobile network deployments vary in their allocation of IP address pools. Some network deployments use the "centralized model" where the pool is managed by a common node, such as the PDN's BR, and the pool shared by multiple MNGs all attached to the same BR. This model has served well in the pre-3G deployments where the number of subscribers accessing the mobile Internet at any given time has not exceeded the available address pool. However, with the advent of 3G networks and the subsequent dramatic growth in the number of users on the mobile Internet, the service providers are increasingly forced to consider their existing network design and choices. Specifically, the providers are forced to address private IPv4 pool exhaustion as well as scalable NAT solutions.

In order to tackle the private IPv4 exhaustion in the centralized model, there would be a need to support overlapped private IPv4 addresses in the common NAT functionality as well as in each of the gateways. In other words, the IP addresses used by two or more MNs (which may be attached to the same MNG) are very likely to overlap at

the centralized NAT, which needs to be able to differentiate traffic. Tunneling mechanisms such as Generic Routing Encapsulation (GRE) [RFC2784], [RFC2890], MPLS [RFC3031] VPN tunnels or even IP-in-IP encapsulation [RFC2003] which can provide a unique identifier for a NAT session can be used to separate overlapping private IPv4 traffic as described in [gi-ds-lite]. An advantage of centralizing the NAT and using the overlapped private IPv4 addressing is conserving the limited private IPv4 pool. It also enables the operator's enterprise network to use IPv6 from the MNG to the BR; this (i.e., the need for an IPv6-routed enterprise network) may be viewed as an additional requirement by some providers. The disadvantages include the need for additional protocol to correlate the NAT state (at the common node) with subscriber session information (at each of the gateways), suboptimal MN - MN communication, absence of subscriber-aware NAT (and policy) function, and of course the need for a protocol from the MNG to BR itself. Also, if the NAT function were to experience failure, all the connected gateway service will be affected. These drawbacks are not present in the "distributed" model which we discuss in the following.

In a distributed model, the private IPv4 address management is performed by the MNG which also performs the NAT functionality. In this model, each MNG has a block of 16.7 million unique addresses, which is sufficient compared to the number of mobile subscribers active on each MNG. By distributing the NAT functionality to the edge of the network, each MNG is allowed to re-use the available NET10 block which avoids the problem of overlapped private IPv4 addressing at the network core. In addition, since the MNG is where subscriber management functions are located, the NAT state correlation is readily enabled. Furthermore, an MNG already has existing interfaces to functions such as AAA and PCRF, which allows it to perform subscriber management functions with the unique private IPv4 addresses. Finally, the MNG can also pass-through certain traffic types without performing NAT to the application servers located within the service provider's domain, which allows the servers to also identify subscriber sessions with unique private IPv4 addresses. The disadvantages of the "distributed model" include the absence of centralized addressing and centralized management of NAT.

In addition to the two models described above, a hybrid model is to locate NAT in a dedicated device other than the MNG or the BR. Such a model would be similar to the distributed model if the IP pool supports unique private addressing for the mobile nodes, or it would be similar to the centralized model if it supports overlapped private IP addresses. In any case, the NAT device has to be able to provide the necessary NAT session binding information to an external entity (such as AAA or PCRF) which then needs to be able to correlate those records with the user's session state present at the MNG.

The foregoing discussion can be summarized as follows: First, the management of available private IPv4 pool has become important given the growth of the mobile Internet users. The mechanisms that enable re-use of the available pool are required. Second, in the context of private IPv4 pool management, the placement of NAT functionality has implications to the network deployment and operations. The centralized models with a common NAT have the advantages of continuing their legacy deployments and the re-use of private IPv4 addressing. However, they need additional functions to enable traffic differentiation and NAT state correlation with subscriber state management at the MNG. The distributed models also achieve private IPv4 address re-use and avoid overlapping private IPv4 traffic in the operator's core, but without the need for additional mechanisms. Since the MNG performs (unique) IPv4 address assignment and has standard interfaces to AAA and PCRF, the distributed model also enables a single point for subscriber and NAT state reporting as well as policy application. In summary, providers interested in readily integrating NAT with other subscriber management functions, as well as conserving and re-using their private IPv4 pool, may find the distributed model compelling. On the other hand, those providers interested in common management of NAT may find the centralized model more compelling.

3.3. IPv6-only Deployment Considerations

As we observed in the previous section, the presence of NAT functionality in the network brings multiple issues which would otherwise be absent. NAT should be viewed as an interim solution until IPv6 is widely available, i.e., IPv6 is available for mobile users for all (or most) practical purposes. Whereas NATs at provider premises may slow down the exhaustion of public IPv4 addresses, expeditious and simultaneous introduction of IPv6 in the operational networks is necessary to keep the "Internet going and growing". Towards this goal, it is important to understand the considerations in deploying IPv6-only networks.

There are three dimensions to IPv6-only deployments: the network itself, the mobile nodes and the applications, represented by the 3-tuple {nw, mn, ap}. The goal is to reach the co-ordinate {IPv6, IPv6, IPv6} from {IPv4, IPv4, IPv4}. However, there are multiple paths to arrive at the goal. The classic dual-stack model would traverse the co-ordinate {IPv4v6, IPv4v6, IPv4v6}, where each dimension supports co-existence of IPv4 and IPv6. This appears to be the path of least disruption, although we are faced with the implications of supporting large-scale NAT in the network. There is also the cost of supporting separate PDP contexts in the existing 3G UMTS networks. The other intermediate co-ordinate of interest is {IPv6, IPv6, IPv4}, where the network and the MN are IPv6-only, and

the Internet applications are recognized to be predominantly IPv4. This transition path would, ironically, require interworking between IPv6 and IPv4 in order for the IPv6-only MNs to be able to access IPv4 services and applications on the Internet. In other words, in order to disengage NAT (for IPv4 - IPv4), we need to introduce another form of NAT (i.e., IPv6 - IPv4) to expedite the adoption of IPv6.

It is interesting to consider the preceeding discussion surrounding the placement of NAT for IPv6 - IPv4 interworking. There is no overlapping private IPv4 address problem because each IPv6 address is unique and there are plenty of them available. Hence, there is also no requirement for (IPv6) address re-use, which means no protocol is necessary in the centralized model to disambiguate NAT sessions. However, there is an additional requirement of DNS64 [dns64] functionality for IPv6 - IPv4 translation. This DNS64 functionality must ensure that the synthesized AAAA record correctly maps to the IPv6 - IPv4 translator.

The IPv6-only deployments in mobile networks need to reckon with the following considerations. First, both the network and the MNs need to be IPv6-capable. Expedited network upgrades as well as roll-out of MNs with IPv6 would greatly facilitate this. Fortunately, the 3GPP network design for LTE already requires the network nodes and the mobile nodes to support IPv6. Even though there are no requirements for the transport network to be IPv6, an operational IPv6 connectivity service can be deployed with appropriate existing tunneling mechanisms in the IPv4-only transport network. Hence a service provider may choose to enforce IPv6-only PDN and address assignment for their own subscribers in their Home Networks, see Figure 1. This is feasible for the newer MNs when the mobile network is able to provide IPv6-only PDN support and IPv6 - IPv4 interworking for Internet access. For the existing MNs however, the provider still needs to be able to support IPv4-only PDP/PDN connectivity.

Migration of applications to IPv6 in MNs with IPv6-only PDN connectivity brings challenges. The applications and services offered by the provider obviously need to be IPv6-capable. However, a MN may host other applications which also need to be IPv6-capable in IPv6-only deployments. This can be a "long-tail" phenomenon; however, when a few prominent applications start offering IPv6, there can be a strong incentive to provide application layer (e.g., socket interface) upgrades to IPv6. Also, some IPv4-only applications may be able to make use of alternative access such as WiFi when available. A related challenge in the migration of applications is the use of IPv4 literals in application layer protocols (such as XMPP) or content (as in html or xml). Some Internet applications expect their clients to supply IPv4 addresses as literals, and this

will not be possible with IPv6-only deployments. Some of these experiences and the related considerations in deploying IPv6-only network are documented in [arkko-v6]. In summary, migration of applications to IPv6 needs to be done, and such a migration is not expected to be uniform across all subsets of existing applications.

Voice over LTE (VoLTE) also brings some unique challenges. The signaling for voice is generally expected to be available for free while the actual voice call itself is typically charged on its duration. Such a separation of signaling and the payload is unique to voice, whereas an Internet connection is accounted without specifically considering application signaling and payload traffic. This model is expected to be supported even during roaming. Furthermore, the providers and the users generally require the voice service regardless of roaming whereas the Internet usage is subject to subscriber preferences and roaming agreements. This requirement to ubiquitously support voice service while providing the flexibility for Internet usage exacerbates the addressing problem, and may hasten provisioning of VoLTE using the IPv6-only PDN.

As seen earlier, roaming is unique to mobile networks and it introduces new challenges. The service providers can control their own network design but not their peer's networks which they rely on for roaming. The users expect uniformity in experience even when they are roaming. This imposes a constraint on providers interested in IPv6-only deployments to also support IPv4 addressing when their own (outbound) subscribers roam to networks which do not offer IPv6. For instance, when an LTE deployment is IPv6-only, a roamed 3G network may not offer IPv6 PDN connectivity. Since a PDN connection involves the radio base station, the AN and the MNG (See Figure 1), it would not be possible to enable IPv6 PDN connectivity without the roamed network support. These considerations also apply when the visited network is used for offering services such as VoLTE in the so-called Local Breakout model; the roaming MN's capability as well as the roamed network capability to support VoLTE using IPv6 determine whether fallback to IPv4 would be necessary. Similarly, there are inbound roamers to an IPv6-ready provider network whose MN's are not capable of IPv6. The IPv6-ready provider network has to be able to support IPv4 PDN connectivity for such inbound roamers. There are encouraging signs that the existing deployed network nodes in the 3GPP architecture already provide support for IPv6 PDP context. It would be necessary to scale this support for a (very) large number of mobile users and offer it as a ubiquitous service which can be accounted for.

In summary, IPv6-only deployments should be encouraged along-side the dual-stack model which is the recommended IETF approach. This is relatively straightforward for an operator's own services and

applications, provisioned through an appropriate APN and the corresponding IPv6-only PDP or EPS bearer. Some providers may consider IPv6-only deployment for Internet access as well, and this would require IPv6 - IPv4 interworking. When the IPv6 - IPv4 translation mechanisms are used in IPv6-only deployments, the protocols and the associated considerations specified in [xlate-stateful] and [xlate-stateless] apply. Finally, such IPv6-only deployments can be phased-in for newer mobile nodes, while the existing ones continue to demand IPv4-only connectivity.

Roaming is important in mobile networks and roaming introduces diversity in network deployments. Until IPv6 connectivity is available in all mobile networks, IPv6-only mobile network deployments need to be prepared to support IPv4 connectivity (and NAT44) for their own outbound roaming users as well as for inbound roaming users. However, by taking the initiative to introduce IPv6-only for the newer MNs, the mobile networks can significantly reduce the demand for private IPv4 addresses.

3.4. Fixed - Mobile Convergence

Many service providers have both fixed broadband and mobile networks. Access networks are generally disparate, with some common characteristics but with enough differences to make it challenging to achieve "convergence". For instance, roaming is not a consideration in fixed access networks. An All-IP mobile network service provider is required to provide voice service, whereas this is not required for a fixed network provider. A "link" in fixed networks is generally capable of carrying IPv6 and IPv4 traffic, whereas not all mobile networks have "links" (i.e., PDP/PDN connections) capable of supporting IPv6 and IPv4. Indeed roaming makes this problem worse when a portion of the link (i.e., the Home Network in Figure 1) is capable of supporting IPv6 and the other portion of the link (i.e., the Visited Network in Figure 1) is not. Such architectural differences, as well as policy and business model differences make convergence challenging.

Nevertheless, within the same provider's space, some common considerations may apply. For instance, IPv4 address management is a common concern for both of the access networks. This implies that the same mechanisms discussed earlier, i.e., delaying IPv4 address exhaustion and introducing IPv6 in operational networks, apply for the converged networks as well. However, the exact solutions deployed for each access network can vary for a variety of reasons. For instance:

- o Tunneling of private IPv4 packets within IPv6 is feasible in fixed networks where the end-point is often a cable or DSL modem. This is not the case in mobile networks where the end-point is a MN itself.
- o Encapsulation-based mechanisms such as 6rd [RFC5969] are useful where the operator is unable to provide native or direct IPv6 connectivity and a residential gateway can become a tunnel end-point for providing this service. In mobile networks, the operator could provide IPv6 connectivity using the existing mobile network tunneling mechanisms without introducing an additional layer of tunneling.
- o A mobile network provider may have application servers (e.g., an email server) in its network that require unique private IPv4 addresses for MN identification, whereas a fixed network provider may not have such a requirement or the service itself.

These examples illustrate that the actual solutions used in an access network are largely determined by the requirements specific to that access network. Nevertheless, some sharing between access and core network may be possible depending on the nature of the requirement and the functionality itself. For example, when a fixed network does not require a subscriber-aware feature such as NAT, the functionality may be provided at a core router while the mobile access network continues to provide the NAT functionality at the mobile gateway. If a provider chooses to offer common subscriber management at the MNG for both fixed and wireless networks, the MNG itself becomes a convergence node that needs to support the applicable transition mechanisms for both fixed and wireless access networks.

Different access networks of a provider are more likely to share a common core network. Hence, common solutions can be more easily applied in the core network. For instance, configured tunnels or MPLS VPNs from the gateways from both mobile and fixed networks can be used to carry traffic to the core routers, until the entire core network is IPv6-enabled.

There can also be considerations due to the use of NAT in access networks. Solutions such as Femto Networks rely on a fixed Internet connection being available for the Femto Base Station to communicate with its peer on the mobile network, typically via an IPsec tunnel. When the Femto Base Station needs to use a private IPv4 address, the mobile network access through the Femto Base Station will be subject to NAT policy administration including periodic clean-up and purge of NAT state. Such policies affect the usability of the Femto Network, and has implications to the mobile network provider. Using IPv6 for

the Femto (or any other access technology) could alleviate some of these concerns if the IPv6 communication could bypass the NAT.

In summary, there is interest in fixed-mobile convergence at least among some providers. While there are benefits from harmonizing the network as much as possible, there are also idiosyncrasies of disparate access networks which influence the convergence. Perhaps greater harmonization is feasible at the higher service layers, e.g., in terms of offering unified user experience for services and applications. Some harmonization of functions across access networks into the core network may be feasible. A provider's core network appears to be the place where most convergence is feasible.

4. Summary and Conclusion

IPv6 deployment in mobile networks is crucial for the mobile Internet. In this document, we discussed the considerations in deploying IPv6 in mobile networks. We summarize the discussion in the following:

- o IPv4 address exhaustion and its implications to mobile networks: As the mobile service providers begin to deploy IPv6, conserving their available IPv4 pool implies the need for network address translation in mobile networks. At the same time, providers can make use of the 3GPP architecture constructs such as the APN and PDN connectivity to introduce IPv6 without affecting the predominantly IPv4 Internet access. The IETF dual-stack model [RFC4213] can be applied to the mobile networks readily.
- o The placement of NAT functionality in mobile networks: Both the centralized and distributed models of private IPv4 address pool management have their relative merits. By enabling each MNG to manage its own NET10 pool, the distributed model achieves re-use of available private IPv4 pool and avoids the problems associated with the non-unique private IPv4 addresses for the MNs without additional protocol mechanisms. The distributed model also augments the "subscriber management" functions at an MNG, such as readily enabling NAT session correlation with the rest of the subscriber session state. On the other hand, the existing deployments which have used the centralized IP address management can continue their legacy architecture by placing the NAT at a common node. The centralized model also achieves private IPv4 address re-use, but needs additional protocol extensions to differentiate overlapping addresses at the common NAT as well as to integrate with policy and billing infrastructure.

o IPv6-only mobile network deployments: This deployment model is feasible in the LTE architecture for an operator's own services and applications. The existing MNs still expect IPv4 address assignment. And, roaming which is unique to mobile networks, requires that a provider support IPv4 connectivity when their (outbound) users roam into a mobile network that is not IPv6-enabled. Similarly, a provider needs to support IPv4 connectivity for (inbound) users whose MNs are not IPv6-capable. The IPv6 - IPv4 interworking is necessary for IPv6-only MNs to access IPv4 Internet.

o Fixed-Mobile Convergence: The examples discussed illustrate the differences in the requirements of fixed and mobile networks. While some harmonization of functions may be possible across the access networks, the service provider's core network is perhaps better-suited for converged network architecture. Similar gains in convergence are feasible in the service and application layers.

5. Security Considerations

This document does not introduce any new security vulnerabilities.

6. IANA Considerations

This document does not require any actions from IANA.

7. Acknowledgement

This document has benefitted from discussions with and reviews from Cameron Byrne, David Crowe, Hui Deng, Remi Despres, Fredrik Garneij, Jouni Korhonen, Teemu Savolainen and Dan Wing; thanks to all of them. Mohamed Boucadair provided an extensive review of individual draft version 01 of this document; many thanks Mohamed. Cameron Byrne, Kent Leung, Kathleen Moriarty and Jari Arkko provided reviews which have helped improve this document. Thanks to Nick Heatley for providing valuable review and input on VoLTE.

8. Informative References

[3gpp.3g] "General Packet Radio Service (GPRS); Service description; Stage 2, 3GPP TS 23.060, December 2006", .

- [3gpp.4g] "General Packet Radio Service (GPRS);enhancements for Evolved Universal Terrestrial Radio Access Network (E-UTRAN) access", 3GPP TS 23.401 8.8.0, December 2009.",
.
- [3gpp2.ehrpd]
"E-UTRAN - eHRPD Connectivity and Interworking: Core Network Aspects", http://www.3gpp2.org/Public_html/Misc/X.P0057-0_v0.13_E-UTRAN-eHRPD_Interworking_VV_Due_5_December-2008.pdf.
- [RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.
- [RFC2003] Perkins, C., "IP Encapsulation within IP", RFC 2003, October 1996.
- [RFC2784] Farinacci, D., Li, T., Hanks, S., Meyer, D., and P. Traina, "Generic Routing Encapsulation (GRE)", RFC 2784, March 2000.
- [RFC2890] Dommety, G., "Key and Sequence Number Extensions to GRE", RFC 2890, September 2000.
- [RFC3031] Rosen, E., Viswanathan, A., and R. Callon, "Multiprotocol Label Switching Architecture", RFC 3031, January 2001.
- [RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.
- [RFC5969] Townsley, W. and O. Troan, "IPv6 Rapid Deployment on IPv4 Infrastructures (6rd) -- Protocol Specification", RFC 5969, August 2010.
- [arkko-v6]
Arkko, J. and A. Keranen, "Experiences from an IPv6-Only Network", draft-arkko-ipv6-only-experience-01, Jul 2010.
- [dns64] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", draft-ietf-behave-dns64-11, Mar 2010.
- [gi-ds-lite]
Brockners et al., F., "Gateway Initiated Dual-stack Lite Deployment", draft-ietf-softwire-gateway-init-ds-lite, Oct 2009.

[xlate-stateful]

Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers",
draft-ietf-behave-v6v4-xlate-stateful-11, Mar 2010.

[xlate-stateless]

Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", draft-ietf-behave-v6v4-xlate-20, May 2010.

Appendix A. Change Log

Revisions (from draft-koodli-**), descending chronological order

- o: More IESG reviews
- o: Addressed IESG reviews
- o: VoLTE related text
- o: FMC, Femto Networks text
- o: Dedicated NAT device model (in addition to the centralized and distributed models)
- o: IPv6-only deployment considerations: - IPv4 literals discussion and reference, - IPv6 prefix assignment clarification, - DNS64 requirement and reference
- o: Overall revisions based on comments from reviews (C. Byrne, K. Leung)
- o: Dual-stack being the recommended model, while encouraging IPv6-only deployments.
- o: Clarifications on on-demand IPv4 PDN usage, DHCP usage and on-demand IPv4 assignment.
- o: Clarifications regarding IPv6-only deployment: Roaming and Applications considerations.

Author's Address

Rajeev Koodli
Cisco Systems
USA

Email: rkoodli@cisco.com

