IPv6: When, Where and How?

A white paper by Huawei

For more information contact
www.huawei.com

IPv6：When, Where and How?

After a long lull spanning a decade or so, IPv6 is back in the limelight, grabbing the attention of policy makers, governments, service providers, content providers and vendor community alike. This is complemented by the renewed focus on IPv6 among various standard organizations and research communities. The series of IPv6 events/conferences that have sprung up recently further emphasize the importance attached by the industry on the subject.

With more customers and devices being connected using hybrid of fixed/mobile broadband technologies, and plethora of services offered, the decade has experienced huge consumption of IPv4 addresses. The 4 billion+ IPv4 addresses are soon becoming a scarce resource in the networked world with billions of customers and trillions of devices expected to be online. Since 2010, more warning bells have been rung by the address issuing authorities (IANA and RIR). Various counters and prediction charts forecast the end of IPv4 address pools at IANA & RIR in early 2011 & 2012 time frame respectively.

Analogous to a situation where demand exceeds supply, this has led to a gold rush for IPv4 pool requests from service providers in 2010. The address issuing authorities have set up mechanisms and put checks in place to prevent hoarding of IPv4 address pools by the service providers. Newer policy initiatives are being drafted. IPv6 deployment plan and timeline by service provider is considered as a prerequisite for any further IPv4 address allocations. To ensure future entrants will have access to large fraction of IPv4 only customer base, certain percentage of remaining IPv4 pool in RIR has been reserved.

At the outset, the scarcity is a function of the forecasted customer and device additions by the operator in the next few years and the stock of IPv4 addresses in reserve. Given many historical reasons, certain service providers are still sitting on a huge pile of allocated, yet unused IPv4 address pools. Although several operators can afford to ignore the initial warning bells, there is a positive momentum to integrate and enable IPv6 connectivity to end users in one form or the other in a phased way.

The IPv6 transition of the entire ecosystem is a long journey, given that there are multiple stakeholders involved (consumers, service providers, content and application providers), each driven by their own interests, and a cost factor associated for each of them. It's fair to say that service providers carry the maximum burden among all of them. While a certain segment of service providers are excited about the possibilities and benefits in a pure IPv6 world, IPv6 is largely seen as a pain point. The reasons are obvious.

Integration of IPv6: This might seem straightforward; given that IPv6 specifications have been standardized for close to two decades. Modern equipment hardware is expected to implement IPv6 features in hardware with similar performance and scalability as seen in the IPv4 world.

The protocol development efforts under TCP/IP model have never been monolithic. As a result, IP has established it deep roots in all layers, layer 3 towards layer 7. The consequence is that IPv6 integration has huge impact on many higher layers,

Integration of IPv6 in a service provider network, is therefore a daunting task with challenges, not limited to

- Engineering effort for network design & planning, provisioning
- Prepping the service provisioning platforms including OSS/BSS to be IPv6 capable.

- lack of IPv6 skill set and operational experience for network operations
- lack of exhaustive testing for IPv6 features in vendor's hardware
- concern about security risks, etc

Ensuring IPv4 service continuity: IPv6 is not downward compatible with IPv4. In addition to expanding the address space to 2^128 bits, IPv6 protocol has designed to include several new mechanisms and an extended header format.

Operators carry the burden of ensuring that IPv6 enabled devices can continue to communicate with the long tail of IPv4-only applications and services on web for a long time. However, they have minimal control over the pace and time period over which end users and web applications will migrate to IPv6. The uncertainty has resulted in two opinions; one camp which is highly optimistic and the other is very pessimistic about the pace of transition,

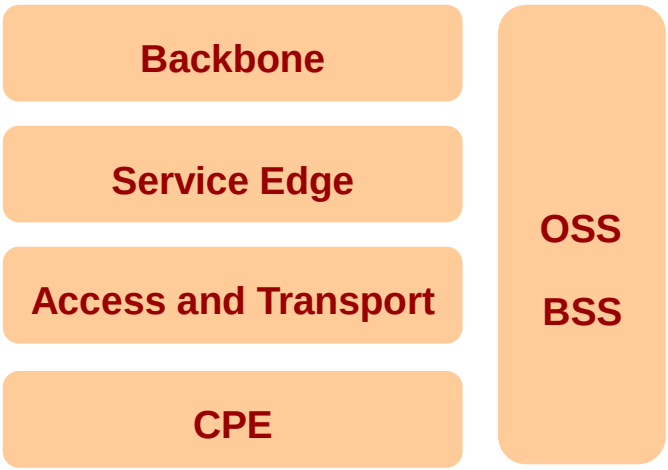
To deal with IPv4 address shortage, requires transition solutions which implement public IPv4 address sharing among multiple users, involves an additional level of NAT in service provider network. This can impact user experience for certain IPv4 applications.

There is a philosophical debate on whether a slight deterioration in user experience for certain IPv4 applications can act as an incentive for end users and web services to accelerate their transition towards IPv6.

Some transition solutions strive hard to minimize the impact on IPv4 applications, while others do not. The transition path chosen and steps involved is to a large extent dependent on the above two opinions.

IPv6 transition in fixed networks

The logical view of various network layers within a fixed network is shown below, and the impact of IPv6 on each of these layers are discussed below.



CPE

CPE/Home Gateway is a layer 3 demarcation device between service provider network and home network. It enables connectivity and offers access to many services after authentication and address assignment by

network infrastructure. In many environments, CPE is bought directly from the retail store by consumer; Operators have no control or limited say over the CPE capabilities.
Even in environment where CPE is by the service provider

a) Much of the existing CPE at customer premises are IPv4 only
Lack support for remote manageability & upgrade,
b) Hardware constraints in CPE to ensure similar performance and functionalities over IPv6 as in IPv4.

Upgrading / swapping these CPEs to support IPv6 involve huge cost and effort, for which the majority of consumers are not willing to shell out any additional money.

The CPE part is complex not because of the technology but because of the costs and logistics involved. With millions of customers in a service provider network, it will be many years before all the customers have IPv6 connectivity.

Operators have to use every other opportunity available either during new customer additions, or during replacements due to failures, to future proof the home network.

Access

Access nodes, which typically implement L2 forwarding for PPP traffic, are agnostic to IPv6.
In IPoE context, access nodes implement L2 DHCP Relay, IP anti-spoofing, IGMP Snooping and IGMP Proxy for multicast. To be IPv6 enabled, DHCPv6 Relay, MLDv2 Snooping, MLDv2 proxy, and related security features are to be supported.

In a typical service provider network, access equipment is from mix of vendors, each with different support for IPv6 capabilities. Enabling IPv6 in access nodes will involve a mix of software upgrade, certain hardware upgrades, or even hardware swap depending on the vendor model and type, currently deployed.

Operators have to capitalize on opportunities such as the rollout of new FTTX networks, ATM DSLAM swap, DSLAM network expansion to ease introduction of IPv6 and reduce the integration cost.

Service Edge

The BNG has to support DHCPv6 procedures for user authentication, prefix delegation. The interaction of service edge with AAA and DHCP servers has to support related IPv6 mechanisms. The service edge also serves as policy enforcement point including QoS, Security, legal interception etc. All these functionalities and related interfaces have to support IPv6 mechanisms.

CGN

While there is general consensus that consumer need to have access to both IPv4 and IPv6 applications for a long time, there are different approaches to realize the same. Operators with sufficient pool of IPv4 addresses have the luxury of offering native dual stack connectivity; many others have to implement IPv4 address sharing during some phase of the transition. A plethora of options involving tunneling and translation among IPv4 and IPv6 address families are being proposed in standard bodies. The standards are relatively new and constantly evolving. Among them, Dual Stack + NAT444, DS_Lite and NAT64 are the prime candidates. Each transition approach is well suited for certain deployment scenarios, specific to current network architecture, and assumptions.

For either of the transition approaches, operators have to give importance to the following factors during CGN deployments

1. The hardware has to scale to support millions of traffic flows, at very high throughputs.
2. support redundancy mechanisms to prevent outage of IPv4 network connectivity, due to NAT device failure
3. include mechanisms to support lawful interception of IPv4 traffic
4. support mechanisms for IPv4 applications which rely on NAT pin holing
5. configurable policies to ensure fair usage of NAT resources by each user

Backbone

In the backbone, operators can leverage on existing MPLS infrastructure to tunnel IPv6 traffic using 6PE and 6vPE mechanisms. Advantage of this approach is only few routers in the periphery of backbone need to be IPv6 capable, while the majority of the routers in the inner periphery can be IPv6 agnostic. This approach minimizes the costs and risks, take advantage of MPLS forwarding and performance. These mechanisms are proven and have been deployed by many operators worldwide for many years.

IPv6 in mobile networks

IPv6 has been incorporated in the 3GPP protocol development and standardization work since a long time. As early as year 2000, 3GPP Rel.99 specifications have included support for IPv6 in GPRS environments. In 2002, IPv6 for IMS networks was included in 3GPP Rel.5 standards. Rel.8 specifications in 2009 have included full support of IPv6 for LTE and EPC networks, including new PDP context type IPv4Ipv6, DSMIPv6, PMIPv6. Rel. 9 specifications include updates to establish single PDP context for IPv4 and IPv6 in GPRS networks.

The mobile network architecture, protocol stack and signaling methods make it much easier to integrate IPv6 in mobile networks. The mobile transport network capability in terms of whether it supports IPv4 or IPv6 on the interfaces in RNC, SGSN, GGSN, eNodeB, SGW and PDN-GW is immaterial.

However, IPv6 migration is relatively a new hot topic in 3GPP as well. A new study item was proposed to investigate the applicability of different IPv6 transition mechanisms for 3GPP network. The recommendations of this study have been documented in as “IPv6 migration guidelines” in TR 23.975

Interestingly, mobile networks have adopted NAT44 solution for a long time to conserve IPV4 address usage. It can therefore be argued that the IPv6 urgency is not so critical. Also, the lack of IPv6 support in terminal hardware and software has been a barrier to consider IPv6 so far.

With increased adoption of USB dongles for mobile data services and new version of operating systems in tablets and computers being IPv6 enabled, there is a scenario fit for IPv6 deployment. LTE specifications recommend IPv6 to be the primary method to offer connectivity. The fast growing M2M market space and the number of devices expected to be connected has created impetus operators to consider IPv6 support in the network and service platforms. These are the main drivers for operators to consider IPV6 integration.

The new network architecture of LTE/EPC presents a green field scenario for introducing IPv6.

Among the various transition mechanisms, NAT64, GI_DS_LITE, IPv6 + NAT44 show great promise for adoption among mobile operators.

Conclusion

With so many variables and stakeholders involved, effective communication, knowledge dissemination and co-ordination within and across organizations are as crucial as the technical aspects of IPv6 itself. Vendors have more work to do introduce/ enhance IPv6 features in their product offerings; Operators have bulk of the work to do beginning with inventory of network equipments, architecture, IT processes, gap analysis, exhaustive lab testing, upgrade of network, service and IT platforms, field trials and commercial rollout; standards/research organizations have to re-evaluate the gaps between standards and deployment scenarios, provide guidelines and document best current practices; Policy makers, and organizations alike have to create more awareness among end users; the list goes on. The industry collectively has begun to take baby steps in this direction; the next few years are exciting to see the pace of development.