IDC
Analyze the Future

Global Headquarters: 5 Speen Street Framingham, MA 01701 USA P.508.872.8200 F.508.935.4015 www.idc.com

WHITE PAPER

The Business Case for IPv6 Services in Mobile Networks

Sponsored by: Cisco Systems

Nav Chander
March 2013

EXECUTIVE SUMMARY

This IDC white paper examines the economics of an Internet Protocol version 4 (IPv4) transition to an Internet Protocol version 6 (IPv6) network for mobile operators providing mobile broadband service. Mobile operators face important decisions about which transition technologies to use — and when and where to implement them in the network. Mobile operator strategies for alleviating IPv4 address exhaust include continuing to deploy Single Stack IPv4 with large-scale Carrier Grade NAT (NAT44), deploying a combination of Dual Stack IPv6 and NAT44, and deploying a combination of Single Stack IPv6 with NAT from IPv6 clients to IPv4 servers (NAT64). This paper reviews and compares the capex costs associated with these options to deal with IPv4 address exhaust. It is necessary to note, in all cases, this paper examines NAT functionality that is externally located from the packet gateway (PGW). *This analysis is based upon an interview with a major North American tier 1 mobile operator.*

Key findings include:

- Deploying Single Stack IPv4 with NAT44 functionality alone is the most costly way to deal with IPv4 address exhaust due to the combination of increasing per-subscriber bandwidth demands and increasing NAT44 session state in the ISP network over time.
- Building a path to IPv6 remains the most effective way to reduce the per-subscriber capex cost associated with NAT44 functionality.
- Capex is neutral in mobile networks when transitioning to IPv6 by deploying Dual Stack IPv6 with NAT44 versus deploying Single Stack IPv6 with NAT64.
- Opex costs when deploying Dual Stack IPv6 with NAT44 versus deploying Single Stack IPv6 with NAT64 are less clear and likely vary from one operator to another.
- In a Single Stack IPv6 deployment model, 85–90% of smartphone applications worked in a widely deployed beta test either via IPv6 end to end or with the aid of a NAT64 in the network. Remaining applications require the support of "464XLAT" (also known as RFC 6877) on the user endpoint (UE) to operate (source: **docs.google.com/spreadsheet/ccc?key=0AnVbRg3DotzFdGVwZWlWeG5wXzVMcG5qczZEZloxWGc#gid=**).

SITUATION OVERVIEW

This section outlines the important market trends and issues related to IPv6 adoption and IPv4 address exhaustion mobile operators must consider.

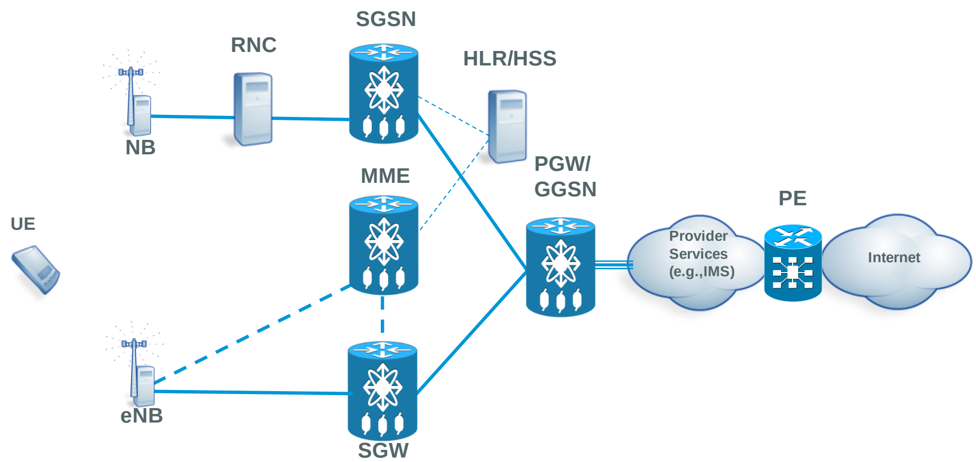
Today's broadband, enterprise, and mobile packet networks primarily use Internet Protocol version 4 addressing to provide a unique numerical identifier for each connected endpoint. This address allows the endpoint to originate traffic and receive traffic from the IP network to which it is connected. The IPv4 address space has a finite limit of approximately 4 billion addresses; it has reached its capacity, with IPv4 address exhaustion occurring in February 2011.

Mobile operators providing Internet access are among the first to have to cope with IPv4 address exhaustion as the growth rate of new subscribers and devices has outpaced the available public IPv4 address reserves. For some time now, mobile operators operating in an IPv4 environment have been using NAT44 functionality to address this issue. For mobile operators where machine-to-machine (M2M) and smartphone growth is exponential, there is not enough private IPv4 address space. Even with the remaining private IPv4 space available in the United States, less than 20 million IP addresses (RFC 1918, 6598) are available, which is not enough addresses for any of the top 5 wireless providers in the United States today, let alone in the future.

A typical scenario in a 3G/4G mobile operator's network consists of the UE, radio equipment, access network, and core network as shown in Figure 1. Each of these network elements of the end-to-end mobile infrastructure has a different timeline on its path to IPv6 enablement. The mobile operator typically has responsibility for the end-user device to the provider edge (PE). Most operators have already enabled some of the network for IPv6 transit. Operators in most cases have shifted focus to ensure all new equipment, including new UEs such as Android and Apple smartphones, tablets, and so forth, is IPv6 capable while the existing install base is left intact.

FIGURE 1

A Typical 3G/4G Mobile Operator's Network



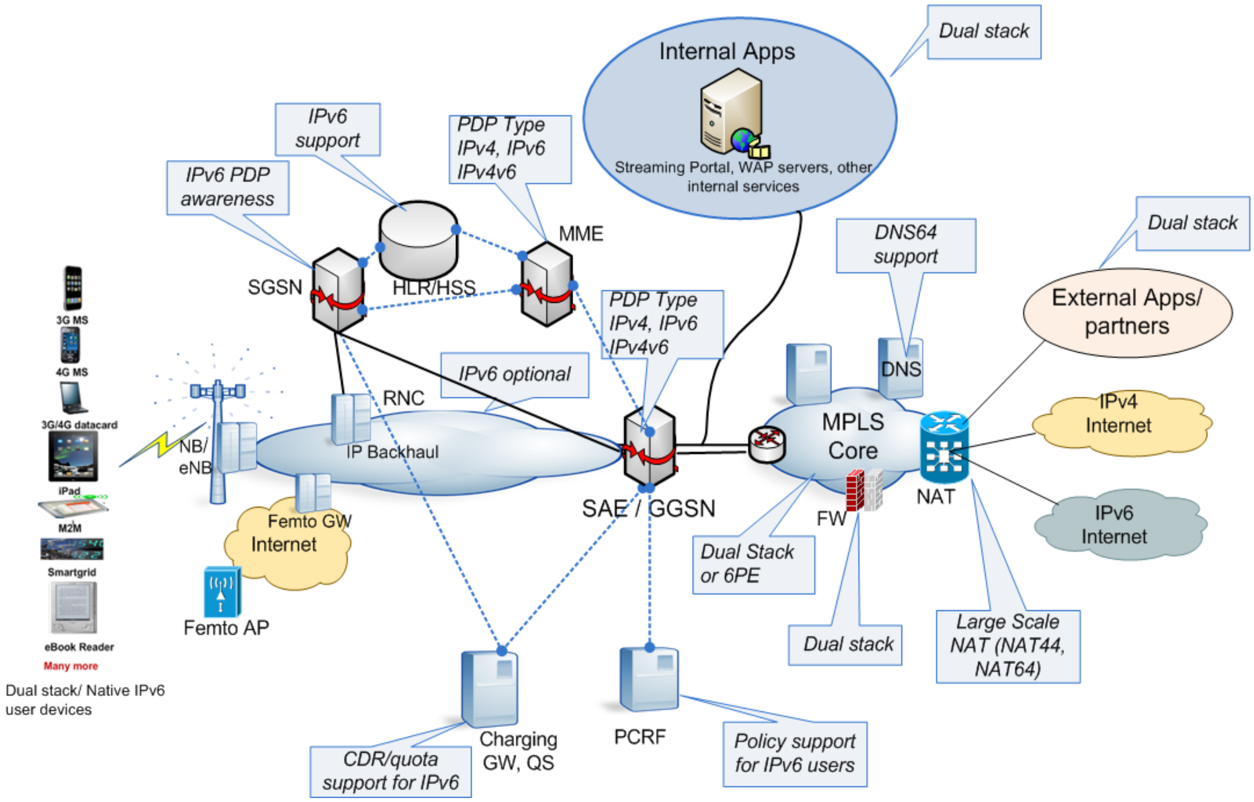
Source: Cisco, 2013

It is widely expected that the majority of the Internet and its applications will eventually be available via IPv6, but as operators transition their networks to support IPv6, they will need to maintain connectivity for their users to the IPv4 Internet as well. Because IPv4 and IPv6 are not interoperable, transitional technologies that can address the needs of both protocols are crucial to ensuring the continued reliability of existing data networks as well as the viability of expanding those networks to account for the massive levels of consumer growth in usage of mobile data.

Mobile operators confront important decisions about their network infrastructure to maintain their current service offerings and continue growth while ensuring a fair profit. The long-term objective for most operators is to completely transition from IPv4 to IPv6 to alleviate the IPv4 address exhaustion situation and reduce opex by having to maintain only one protocol stack. However, implementing a flash cut to a pure IPv6 environment is not realistic because it requires all network equipment as well all IP-based content and applications to work with and be available on IPv6 instantaneously. This is why a well-planned transition strategy is necessary. Figure 2 shows a typical mobile network depicting IPv6 touch points mobile operators must take into consideration when looking at the economics of transitioning the networks to IPv6.

FIGURE 2

IPv6 Touch Points in a Typical Mobile Operator



Source: Cisco, 2013

IPv6 Adoption Trends

Several clear trends show how the growth of IPv6 adoption impacts core, aggregation, and access networks; subscriber user equipment; content providers; and enterprise networks. Consider the following:

- IPv6 traffic growth is expected to grow exponentially as IPv6-capable devices such as smartphones, tablets, and routers increase to over 6 billion by 2015 (according to IDC forecasts).

- The global increase in IPv6 available content is expected to represent more than 95% of all content by 2016.

- In 2012, 14% of all mobile-connected devices/connections (1 billion) were IPv6 capable; by 2017, 41% of all mobile-connected devices/connections (4.2 billion) will be IPv6-capable (source: Cisco Visual Networking Index, Global Mobile Data Traffic Forecast, 2012–2017). Samsung Galaxy devices, iPhone/iPad, and Android and Windows 8 mobile devices all support IPv6.

- T-Mobile USA has IPv6 turned on optionally for GSM/UMTS, and IPv4/v6 will be the default for all LTE production devices in 2013. In the T-Mobile beta test Single Stack IPv6 deployment model, 85–90% of smartphone applications worked via IPv6 end to end or with the aid of a NAT64 in the network. Remaining applications require the support of "464XLAT" on the user endpoint to operate (source: **docs.google.com/spreadsheet/ccc?key=0AnVbRg3DotzFdGVwZWlWeG5wXzVMcG5qczZEZloxWGc#gid=0**).

- Samsung's target is to support the 464XLAT solution for providing IPv4 services over IPv6 networks on the Galaxy S IV (source: **conference.apnic.net/__data/assets/pdf_file/0008/58886/apnic_samsung_20130227_1361841046-1.pdf**).

- Verizon Wireless 4G LTE production network has IPv6 built in, and all LTE devices must be IPv6 compatible. 20% of network traffic is routed via native IPv6 today (source: **conference.apnic.net/__data/assets/pdf_file/0017/50813/vzw_apnic_13462152832-2.pdf**).

- Many new applications and devices that are forming the Internet of Everything, including Internet-enabled wireless devices, home and industrial M2M appliances, Internet-connected transportation, integrated telephony services, sensor networks such as RFID, smart grids, cloud computing, and gaming, are being designed for and enabled by IPv6 networks.

- Applications requiring simple end-to-end reachability by the network, including new services and associated revenue opportunities for operators, should flourish as IPv6 is deployed and could likewise be inhibited by the introduction of NAT44.

Operator segments will face the IPv4 address depletion issue at different times and will have to address the prospect of implementing IPv6 in their network. Each segment has different characteristics dictating the approach taken to accomplish this transition. Key factors contributing to the approach taken include IPv4 address exhaustion status, the availability of IPv6 content and applications, and end-device IPv6 readiness. Table 1 provides the status of these factors for each of the possible segments: mobile, fixed enterprise, and fixed wireline broadband.

In this paper, we focus on these factors as they relate to the mobile broadband segment.

TABLE 1

Key Considerations for Service Providers by Segment

Key Factor	Mobile	Fixed Enterprise	Fixed Wireline Broadband
IPv4 addresses exhaustion?	Now: Devices already deployed with IPv6 addresses	Varies: NAT already used in peering points	Now: Combination of NAT and IPv6-enabled CPE
IPv6 content and application availability?	Rapid growth	Slower growth: Custom enterprise applications and development requirement	Rapid growth
What is the device/CPE refresh frequency?	Short refresh cycle	Longer refresh cycle	Longer refresh cycle

Source: IDC, 2013

As the supply of IPv4 addresses rapidly depletes, network operators are employing unique solutions to optimize current networks to preserve the remaining unallocated IPv4 addresses and implement a transition to IPv6. Today, there are multiple approaches to dealing with IPv4 address exhaustion for operators to consider, including IPv4 Carrier Grade NAT (NAT44), IPv6 rapid deployment (6rd), Native Dual Stack, Dual-Stack Lite (ds-lite), and IPv6 and NAT64 with 464XLAT. Of these approaches, IDC considered two of the most widely deployed mobile IPv6 transition technologies, Dual Stack IPv6 with NAT44 and Single Stack IPv6 with NAT64, and compared these approaches to remaining on a Single Stack IPv4 network and using NAT44 to address IPv4 exhaustion.

MOBILE INTERNET SERVICES: A BUSINESS CASE — THE INTRODUCTION OF IPV6 TRANSITION STRATEGIES VERSUS CONTINUING WITH THE STATUS QUO

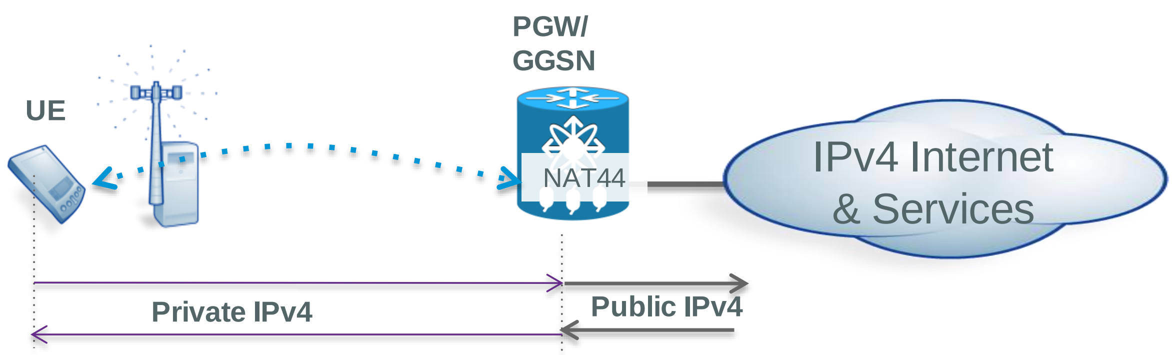
What are mobile operators implementing today? IDC interviewed a major North American tier 1 mobile operator to validate a business model that analyzed various scenarios to deal with IPv4 exhaustion and IPv6 introduction.

IDC analyzed the capex cost of deploying three different modes of operation to address IPv4 address exhaust and, in two of the cases, IPv6 introduction:

1. **Conventional Mode of Operation (CMO) — Single Stack IPv4 with Carrier Grade NAT44 (NAT44)** is the status quo strategy of continuing to deploy IPv4 by using a NAT44 as an approach to IPv4 network design in which the UE, in particular mobile networks, is configured with private IPv4 network addresses that are translated to public IPv4 addresses by routers embedded in the network operator's network, permitting the sharing of small pools of public addresses among many UEs. This shifts the NAT function and configuration from the customer UE to the Internet service provider network. This does not build a path to IPv6 but rather has been the answer to the IPv4 address exhaust challenge for most mobile operators in the industry to date (see Figure 3).

FIGURE 3

CMO — Single Stack IPv4 with NAT44

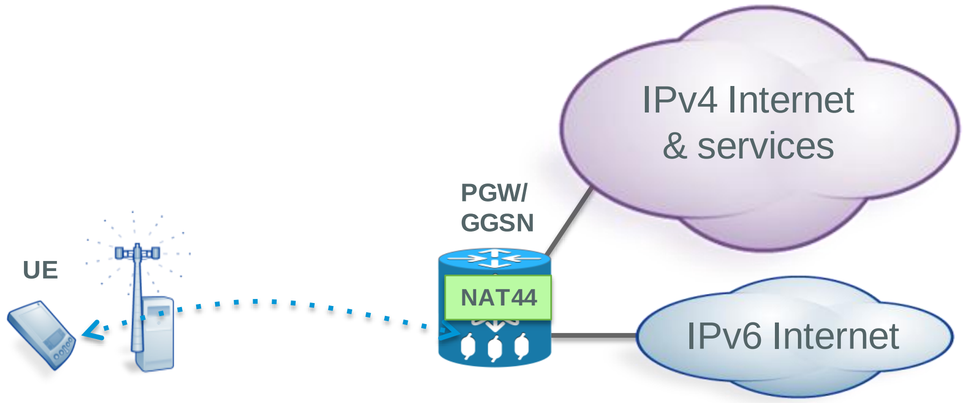


Source: Cisco, 2013

2. **Next Mode of Operation 1 (NMO #1) — Dual Stack IPv6 with Carrier Grade NAT44 (NAT44)** is the IPv4 to IPv6 mobile transition approach to IPv4/IPv6 network design in which the UE, in particular mobile networks, is configured with a public IPv6 address to reach the IPv6 Internet. The UE is also configured with a private network address that is translated to a public IPv4 address by routers embedded in the operator's network, permitting the sharing of small pools of public addresses among many UEs. This shifts the NAT function and configuration from the customer UE to the Internet service provider network. This type of network design allows the customer to reach both the IPv4 and the IPv6 Internet and services (see Figure 4).

FIGURE 4

NMO #1 — Dual Stack IPv6 with NAT44

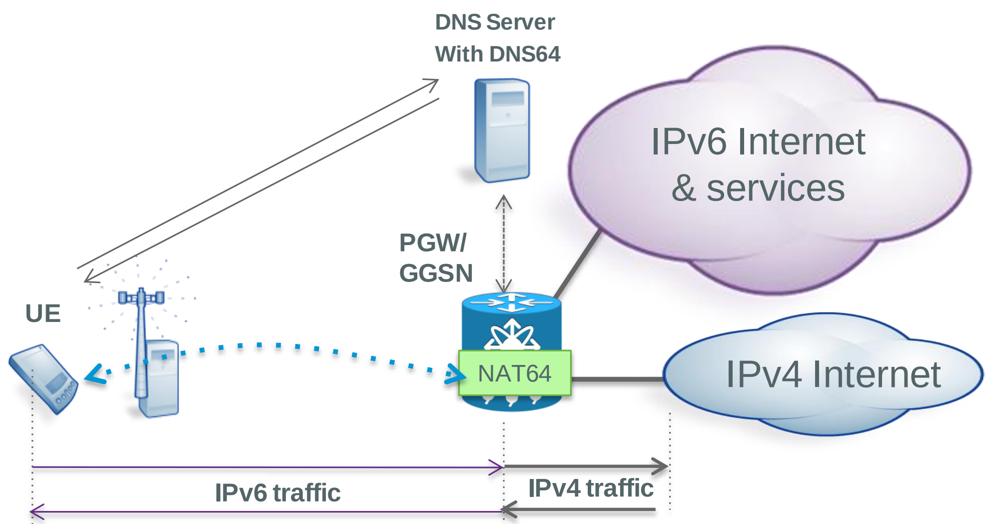


Source: Cisco, 2013

3. **Next Mode of Operation 2 (NMO #2) — Single Stack IPv6 with NAT64 and 464XLAT** is the IPv4 to IPv6 mobile transition approach to IPv6 network design in which the UE, in particular mobile networks, is IPv6 Single Stack and is configured with a public IPv6 address to reach the IPv6 Internet. If the UE needs to reach the IPv4 public Internet, a NAT64 translation is performed by routers embedded in the operator's network, permitting the IPv6 UE to reach IPv4 public Internet devices. This shifts the function and configuration from the customer UE to the Internet service provider network. This type of network design allows the customer to reach both the IPv4 and the IPv6 Internet and services but also allows the mobile operator to operate and maintain a single stacked network from the UE to the PE. Today, this is the mobile network model of choice for T-Mobile and is deployed in T-Mobile's mobile network for customers that have been upgraded into a Single Stack IPv6 UE. In the T-Mobile beta test Single Stack IPv6 deployment model, 85–90% of smartphone applications worked via IPv6 end to end or with the aid of a NAT64 in the network (see Figure 5).

FIGURE 5

NMO #2 — Single Stack IPv6 with NAT64 and 464XLAT



Source: Cisco, 2013

The remaining 10–15% of applications will require the support of "464XLAT" on the user endpoint to operate. For example, two popular applications requiring 464XLAT to operate are Skype and Netflix. By implementing 464XLAT with IPv6 and NAT64, mobile operators will gain 100% smartphone application support, a long-term method for uniquely numbering subscribers; remove the dependency on costly NAT translation; and build more end-to-end traffic over time. For additional information on T-Mobile's IPv6 deployment, go to **sites.google.com/site/tmoipv6/lg-mytouch**.

Summary of Cost Components for IPv6 Transition

Capex and opex business costs are considerations when operators select a strategy to deal with IPv4 address exhaust. The summary of key capex costs components covered in this analysis is shown in Table 2. Some key opex costs *not* covered in this analysis are listed in Table 3. Each operator knows its operating environment best. Because the opex numbers vary so much from operator to operator, these costs are not analyzed in this paper. IDC recommends operators analyze how each IPv6 transition strategy, if implemented, would affect not only capex, as covered in this paper, but also opex projections over a five-year period.

TABLE 2

Key Cost Components Covered in the Analysis

Cost	Description	Type
Core/aggregation/access	Cost of placing NAT44/64 functionality in the network	Capex
UE with IPv6 enabled	Cost of placing IPv6 enabled UE (single or dual stacked) for the subscriber is cost neutral for new subscribers	Capex
State per session	As devices are added, traffic on the network increases, requiring more sessions and state, driving additional NAT44/64 hardware	Capex

Source: IDC, 2013

TABLE 3

Key Cost Components Not Covered in the Analysis That Should Be Considered

Cost	Description	Type
State per session	As devices are added, traffic on the network increases, requiring more sessions and state, driving additional NAT44/64 hardware	Opex
IPv6 lab	Testing, security, training, implementation, and troubleshooting	Opex
Applications	Testing, performance issues, increased NOC level 1 and 3 support calls, subscriber churn, operator-enforced sessions per application, and the cost of not deploying net-new IPv6 applications	Opex

Source: IDC, 2013

Business Case: Mobile Broadband Service

IDC examined a mobile broadband service business scenario: the capex cost of deploying a dual stacked network from the UE to the provider edge with NAT44 versus a Single Stack IPv6 network from the UE to the provider edge to build a path to the IPv6 Internet versus staying with the status quo and continuing with a Single Stack IPv4 network using NAT44 from the UE to provider edge. IDC compared only the NAT44 elements and the resulting capex of each over a five-year time frame. The sections that follow discuss the three alternatives in further detail.

1. Conventional Mode of Operation (CMO) — Single Stack IPv4 with NAT44

- IPv4 public addresses are exhausted.
- UE is single stacked and is configured with a private IPv4 address.
- No path is built to IPv6; NAT44 addresses IPv4 exhaust.
- **IPv4 traffic** is routed from the UE via a private IPv4 address and directed to the NAT44 core node and translated to a public IPv4 address and routed out to the Internet to its destination. *State is held in the NAT44 core node.*
- Simulation is run with the ASR 9000 as NAT44 platform.

This leaves two key metrics that drive cost when scoping the NAT44 portion of the implementation: sessions and throughput per device. It is imperative that both key metrics be considered:

- **Sessions per device:** The key benefit of using NAT44 is the ability to translate multiple private IPv4 addresses into one public IPv4 address; this is done by dividing the port space for the public IPv4 address. The number of ports that will be in turn used for sessions can be provisioned or dynamically allocated. The number of sessions consumed drives the number of NAT44 engines that are required.
- **Throughput per device:** The other key metric used when sizing a NAT44 implementation is how much throughput per device is required. It's possible that a NAT44 engine will be able to satisfy the sessions-per-device requirement for a set number of devices (UEs), but the throughput cannot be met, thus generating the need for more NAT44 engines and driving more capex.

2. Next Mode of Operation 1 (NMO #1) — Dual Stack IPv6 with NAT44

- IPv4 public addresses are exhausted.
- UE is dual stack capable, meaning it is configured with a private IPv4 address and a public IPv6 address.
- **IPv6 traffic** is routed from the UE via a public IPv6 address through the dual stacked core and out to the Internet to its destination. *No state is held in the router.*
- **IPv4 traffic** is routed from the UE via a private IPv4 address and directed to the NAT44 core node and translated to a public IPv4 address and routed out to the Internet to its destination. *State is held in the router.*

When evaluating this option, the only requirement for IPv6 reach ability is a dual stacked UE and provider edge router. Dual stacked UEs will be issued at the time of subscriber churn and will not drive additional cost to the provider. Provider edge routers are for the most part dual stack capable, and IPv6 can be enabled without further cost to the operator.

This leaves two key metrics that drive cost when scoping the NAT44 portion of the implementation: sessions and throughput per device. It is imperative that both key metrics be considered:

- **Sessions per device:** The key benefit of using NAT44 is the ability to translate multiple private IPv4 addresses into one public IPv4 address; this is done by dividing the port space for the public IPv4 address. The number of ports that will be in turn used for sessions can be provisioned or dynamically allocated. The number of sessions consumed drives the number of NAT44 engines that are required.

- **Throughput per device:** The other key metric used when sizing a NAT44 implementation is how much throughput per device is required. It's possible that a NAT44 engine will be able to satisfy the sessions-per-device requirement for a set number of devices (UEs), but the throughput cannot be met, thus generating the need for more NAT44 engines and driving more capex.

3. Next Mode of Operation 2 (NMO #2) — Single Stack IPv6 with NAT64 and 464XLAT

- IPv4 public addresses are exhausted.

- UE is single stacked and configured with a public IPv6 address.

- **IPv6 traffic** is routed from the IPv6 capable UE via a public IPv6 address through the IPv6 core and out to the Internet to its destination. *No state is held in the router.*

- **IPv4 traffic** is routed from IPv6 UE through the provider's network toward the NAT64 mechanism located at the PE, which will then translate the packet from IPv6 to IPv4 and route the packet to its destination and back. *State is held in the NAT64 Node* (binding an IPv6 address and port to an IPv4 address and port).

The single stack IPv6 option is one where the operator's network supports IPv6 or IPv6/v4 and is single stacked from the UE to the provider edge. The UE is assigned a public IPv6 address and can only communicate directly with other IPv6 clients. If the requested communication from the UE is available over IPv6, packets are routed normally via IPv6 through the provider's IPv6 network to the destination. If the requested client communication is IPv4, the traffic is directed from the IPv6 UE through the provider's network toward the NAT64 mechanism located on a router in the provider's network, which will then translate the packet from IPv6 to IPv4. The NAT64 router will translate the packets to IPv4 and forward them through the IPv4 network to the IPv4 receiver. The reverse takes place for packets generated in the IPv4 network for an IPv6 receiver. NAT64, however, is not symmetric. To be able to perform IPv6 to IPv4 translation, NAT64 requires state, binding an IPv6 address and port to an IPv4 address and port. Such a binding state is either statically configured in the NAT64 or created when the first packet flowing from the IPv6 network to the IPv4 network is translated. After the binding state has been created, packets flowing in both directions on that particular flow are translated. The result is that, in the general case, NAT64 supports communications initiated by the IPv6 node toward an IPv4 node. Some additional mechanisms or static binding configuration can be used to provide support for communications initiated by an IPv4 node to an IPv6 node, but they are not covered in this paper. In this option, we have to be aware of the cost of the state that is created to support the communication between IPv6 to IPv4 hosts, *because as state increases, cost will increase.* Again, it is important to note that in a Single Stack IPv6 deployment model, 85–90% of smartphone applications worked in a widely deployed beta test either via IPv6 end to end or with the aid of a NAT64 in the network. Remaining applications require the support of "464XLAT" on the UE to operate.

Key Assumptions Common to Each Mode of Operation

Figure 6 compares the key assumptions for the business case mode of operation.

FIGURE 6

Key Assumptions for the Business Case Mode of Operation Comparison, 2012–2017

Hypothesis	2012	2013	2014	2015	2016	2017
Nbr of Subs	45,000,000	46,350,000	47,740,000	49,173,000	50,648,000	52,167,000
Peak Bw per UE (Mbits/sec)	0.006	0.011	0.019	0.034	0.06	0.107
Avg Session/UE	50	52	55	58	60	63
NMO ramp-up	0	5%	30%	70%	90%	95%
% of Internet Content IPv6-enabled	70%	80%	85%	90%	95%	95%

Source: Cisco, 2013

Additional Assumptions

- 3% compound annual growth rate (CAGR) for subscribers
- 78% CAGR for peak bandwidth (Cisco Visual Network Index)
- 5% CAGR for average session/UE
- Percentage of v6 Internet reaching a plateau
- 20 Carrier Grade NAT (CGN) locations
- 1 UE per subscriber
- Only CGN elements are considered:
  - ✓ Number of NAT44 translations required = subscribers x devices per subscriber x sessions per device
- NMO = Next mode of operation ramp up either NMO #1 or NMO #2:
  - ✓ Simulation run with the Cisco ASR 9000 acting as the Carrier Grade NAT platform (NAT44 or NAT64)
  - ✓ Maximize IPv6 traffic to the extent of IPv6 content availability

Capex Comparison: CMO Will Cost the Most; IPv6 NMO Transition Options Are Capex Neutral

IDC confirms:

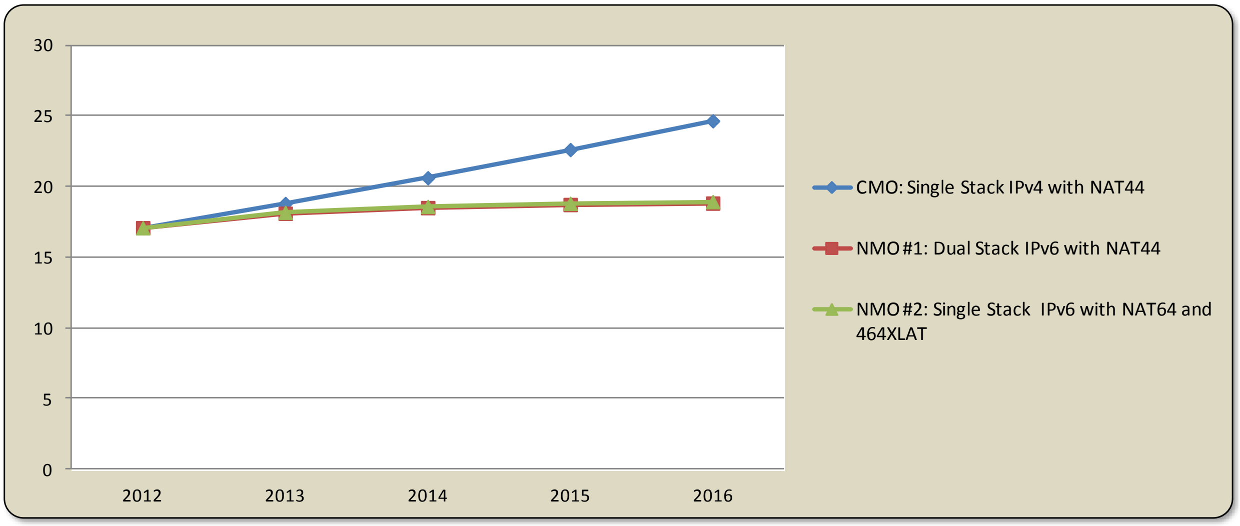
- CMO or the status quo strategy of continuing to deploy IPv4 and NAT44 will be the most costly over the long term because of the ever-increasing cost of NAT44 associated with ever-increasing UE and bandwidth (refer to Figure 10)
- Introducing IPv6 with NMO #1 (Dual Stack UE to provider edge with NAT44) or NMO #2 (Single Stack IPv6 UE to provider edge with NAT64) does not cost any additional capex; rather, it results in a slight reduction of capex over time compared with continuing to deploy CMO (IPv4 with NAT44) (refer to Figure 7).
- Deploying either NMO #1 or NMO #2 results in a capex reduction of 25% over a five-year period (refer to Figure 8).
- Building a path to IPv6 remains the most effective way to reduce the per-subscriber capex cost associated with CGN functionality (refer to Figure 11).
- Opex costs vary on an operator-to-operator basis given the operators' current environment.
- Opex costs and the IPv4 address exhaustion time frame will be the determining factors for operators that are trying to select Single Stack IPv6 UE to PE versus dual stacked UE to PE.
- The burden of maintaining NAT44 address space virtualization and implementation versus implementing IPv6 now must be taken into consideration by the operator.
- In a Single Stack IPv6 UE to PE environment, residual IPv4 applications that are not IPv6 capable and still need to function over the network must be considered.

Results from Mode of Operation Comparison

Figures 7–10 show mode of operation comparisons.

FIGURE 7

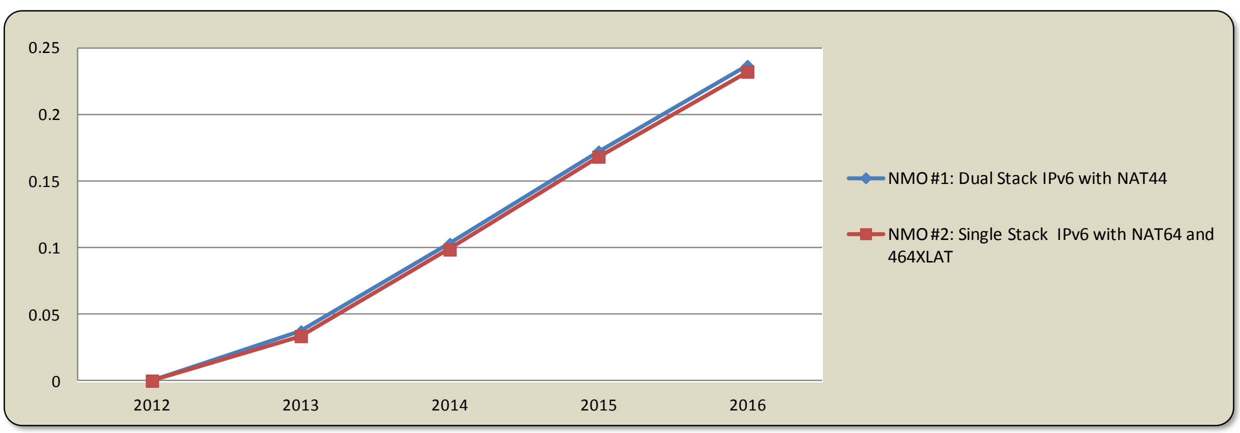
Cumulative Capex Evolution, 2012–2016 ($M)



Source: IDC, 2013

FIGURE 8

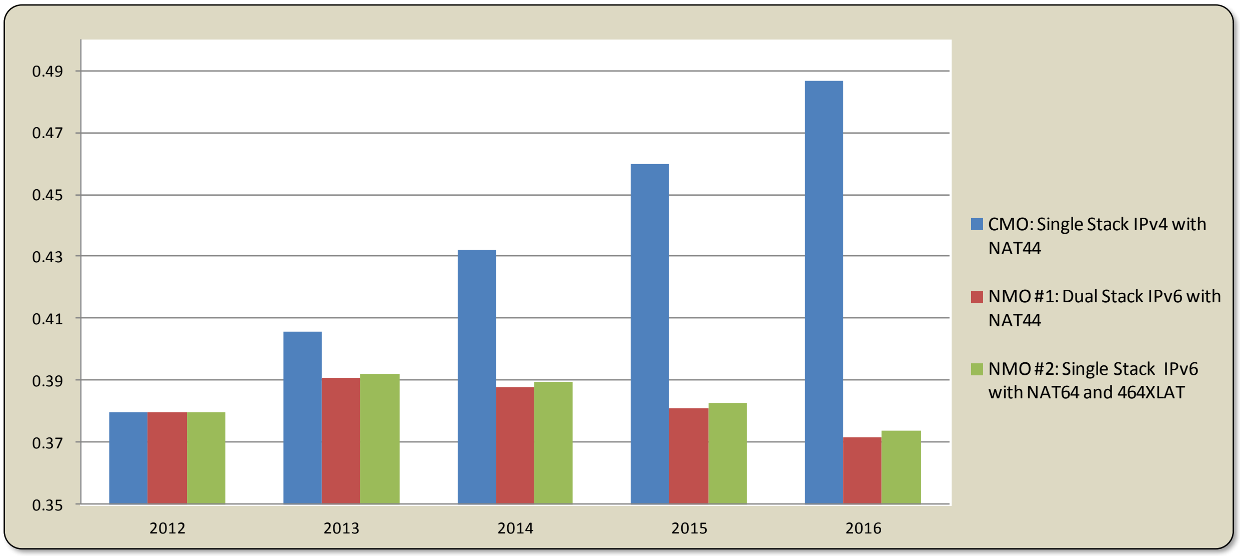
Capex Reduction Over Time Versus CMO, 2012–2016



Source: IDC, 2013

FIGURE 9

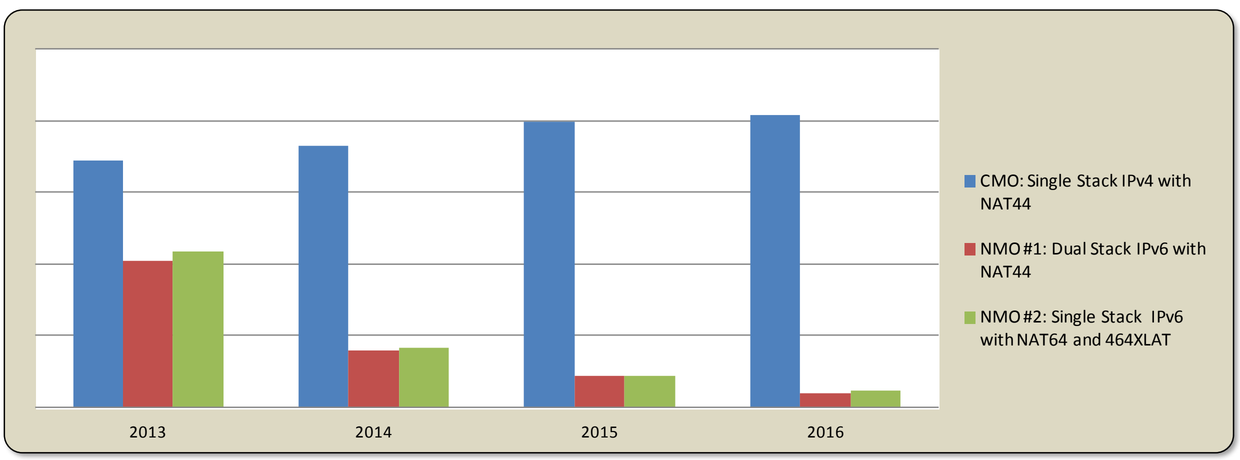
Cumulative NAT Investment, 2012–2016 ($ per Subscriber)



Source: IDC, 2013

FIGURE 10

NAT Investment, 2013–2016 ($M)



Note: Data was validated with a tier 1 North American mobile operator.

Source: IDC, 2013

Key findings for this five-year capex scenario comparison demonstrate capex neutrality for the NMO alternatives, driven by the need to deploy Carrier Grade NAT resources in each case, resulting in an equal capex spend in either scenario to support exactly the same number of subscribers. In NMO #1, IPv4 traffic is routed from the UE via a private IPv4 address directed to the NAT44 core node and translated to a public IPv4 address and routed out to the Internet to its destination. State is held in the router. In NMO #2, IPv4 traffic is routed from the IPv6 single stack UE to the NAT64 core node and the header is translated to a public IPv4 address and routed out to the Internet to its destination. State is held in the router for this translation.

In summary, IDC found the CMO status quo strategy of continuing to deploy IPv4 and NAT44 to be the most costly over the long term due to the ever-increasing cost of NAT44 associated with ever-increasing UEs and bandwidth. IDC found the two IPv4 to IPv6 transition strategies to be capex cost neutral and validated opex expenditures based on the operator's existing environment to be the tipping point for selecting which IPv6 transition option to use to build a path to IPv6. Both IPv6 strategies are capex neutral based on the need for NAT investment, either NAT44 or NAT64 investment in the two scenarios. Both cases are based on incremental growth of IPv6 available content and the availability of either a compliant Dual Stack UE or Single Stack IPv6 capable UE. Furthermore, IDC confirmed the only way to significantly reduce NAT44 cost over time is to introduce one of these IPv4 to IPv6 transition strategies.

Given that capex costs are neutral between NMO scenarios, each operator must examine its own operational environment and then select the IPv6 alternative that best suits its needs. When selecting NMO #1, operators must keep in mind how close they are to IPv4 exhaust and factor in the cost of maintaining NAT44 address space virtualization and implementation versus going with NMO #2, Single Stack IPv6, now. When selecting NMO #2, operators must take into consideration that, in a Single Stack IPv6 environment, there will be residual IPv4 applications on the smartphone device that are not IPv6 capable and will still need to function over the network. At some level, there will be a cost associated with the inability to support some legacy applications.

CHALLENGES/OPPORTUNITIES

In IDC's view, mobile operators face significant challenges in planning an economical and pragmatic transition of their networks, subscribers, and content to IPv6. IPv6 begins to come of age as 4G/LTE networks deployment accelerates, and the high growth of IPv6-capable subscriber devices, additional new IPv6 content, and IPv6 application awareness require careful planning and support from key vendors like Cisco. Future deployments of VoLTE, which will require at least 2 IP addresses per device, further highlight the importance of being proactive. For mobile providers, there is an added challenge because of the expected exponential growth of M2M and smartphone traffic, since there is not enough private IPv4 space. This impacts IPv4 and NAT44 as well as dual-stack and NAT44 equally. Cisco's support for delivering IPv6 service alongside preserving IPv4 service in the face of IPv4 exhaustion mitigates the risk to operators and provides short-term as well as long-term capex savings.

CISCO'S POSITION

Cisco supports IPv6 in the core, aggregation, and subscriber equipment as well as in the network management software it supplies to operators, which ensures an end-to-end, reliable, and fully supportable IPv4 to IPv6 transition. Cisco has a full suite of options for placement of the appropriate transition technology in the network with the CRS in the core, the ASR 9000 and 1000 series routers in the aggregation, and the ASR 5500 series router in the Mobile Packet Core. This allows for strategic placement of the Carrier Grade IPv6 solutions in the network.

Cisco's Carrier-Grade Services Engine (CGSE) is an industry-leading solution for IPv6 support in the core and aggregation network. Powered by a multicore CPU complex, it scales to tens of millions of address translations and gateway functionality with gigabits of throughput for hundreds of thousands of subscribers. In addition, rapid connection setup time boosts performance significantly. The CGSE is a single-slot module supported on all models of Cisco's proven high-end CRS-1/3. The CRS also allows for centralized placement of the 6rd border relay function and takes advantage of its stateless nature to remove session limit bottlenecks.

The ASR 9000 system is a high-end aggregation device that is equipped with the Cisco IOS XR operating system. The ASR 9000 leads the industry, boasting 96Tbps of total capacity alongside carrier grade high availability designed for continuous operations. The ASR 9000 is also outfitted with a multi-functional service module used for Carrier Grade NAT functions to provide a full selection of available transition technologies at the edge of the network.

The Cisco ASR 1000 Series is a highly scalable WAN and Internet edge router platform. Powered by the Cisco QuantumFlow Processor, with parallel processing, it scales to millions of address translations, with gigabits of throughput for Carrier Grade (CGv6) functionality. Highly programmable, it delivers fast feature velocity in a compact form factor. In-service software upgrades make the platform highly reliable.

Cisco Prime Network Registrar provides integrated, scalable, reliable Domain Name System (DNS), Dynamic Host Configuration Protocol (DHCP), and IP Address Management (IPAM) services for IPv4 and IPv6 transition planning.

Cisco Advanced Services have developed a service solution to help operators meet the challenges of IPv4 exhaustion and smoothly integrate IPv6 into their environments. Cisco Advanced Services offer a complete portfolio designed to meet operator needs across all phases of the network life cycle, from preparing and planning to operations and optimization.

As new IPv6 applications emerge and existing services like Netflix and other video-based services migrate to IPv6, it is important and timely for mobile broadband communication providers to become more aggressive with their network transformation and transition to IPv6.

IDC believes that Cisco is well positioned to help mobile operators manage the IPv4 to IPv6 transition costs while also advising the operators to plan for and implement new innovative service opportunities as they open up with the global reachability of all Internet devices.

CONCLUSION

IDC believes that mobile operators have to take a longer-term economic view when it comes to preserving IPv4 addressed services while introducing new IPv6 addresses. A strategy of continuing to deploy IPv4 and NAT44 will be costly over a five-year period because of the ever-increasing cost of NAT44 associated with the significant number of new mobile IPv6-capable devices and supporting higher bandwidth throughput. IDC concludes that selecting either of the two alternative IPv4 to IPv6 transition strategies, Dual Stack IPv6 with NAT44 or Single Stack IPv6 with NAT64, would be capex cost neutral. The capex comparison was validated, and the key factors in deciding which IPv6 transition option to select are the operator's existing operations environment, the availability of IPv4 addresses, and opex cost components.

It is equally important to select a vendor that can allow for gradual IPv6 introduction in parallel to maintaining its existing IPv4-based services and minimize capex expenditures. Each of the two IPv6 transition alternatives to support this IPv6 introduction provide mobile operators with a 25% capex savings over a five-year period with early implementation alongside NAT44. This also enables future plans to implement value-added services based on IPv6.