ALCATEL-LUCENT ENTERPRISE IP COMMUNICATIONS :

IPV6 TRANSITION PLANS

APPLICATION NOTE

TABLE OF CONTENTS

INTRODUCTION

Internet Protocol version 6 (IPv6) has been designed by the Internet Engineering Task Force (IETF) to increase the amount of available IP addresses. IPv6 is the long-term replacement for IPv4, the current and widely used Internet routing protocol suite that became the global standard in 1984.

IPv6 will allow every citizen, network operator or organization to have as many IP addresses as they need to connect several devices to the Internet; for example, mobile phones, car navigation systems, home appliances, and industrial equipment. IPv6 would provide more locations in cyberspace than grains of sand on the world's beaches — 3.4×10^{38} IP addresses. In comparison, IPv4 provided $4.3 \times 10^{9} =$ 4.3 billion IP addresses.

This document summarizes the Alcatel-Lucent Enterprise strategy regarding the transition from IPv4 to IPv6 in Enterprise communication networks. The document first explains what the IPv6 promises are for enterprises and large organizations. Then it describes the IPv4 to IPv6 transition phases, the elements that need transformation and what enabling technology is available. Finally, the document describes the Alcatel-Lucent phased approach to IPv4 to IPv6 transition in enterprise networks.

THE PROMISES OF IPV6

The IPv4 exhaustion is becoming real…in the Internet

According to the IANA and RIRs,[1] the Internet organizations that manage and distribute the IPv4 addresses, the existing pool of 4 billion IP addresses provided by the IPv4 will be exhausted in 2011.

In the last several years, two key trends have vastly accelerated the depletion of IPv4 addresses. The first trend is the global rise of consumer home broadband, and the other one is the success of smartphones such as iPhone, BlackBerry and Android handsets. By 2015, 17 percent of the global Internet addresses should be IPv6 with 28 percent of new Internet users running the protocol according to Gartner.[2] A few prevailing actors on the Web have already taken that step (Facebook, YouTube).

To overcome the lack of available IPv4 addresses, technology such as Network Address Translation (NAT) has been deployed for years in enterprises. NAT gateways are devices that modify the IP addresses in IP packets and thus can hide a large private network behind a limited number of public IPv4 addresses.

The IPv4 exhaustion in the Internet is therefore not an immediate issue for large enterprises and organizations.

Besides cost, the major issue with NAT gateways in enterprise communication networks is that they break protocols that transport IP addresses in the messages that protocol agents exchange. Indeed, a basic NAT gateway will not modify the IP addresses that are exchanged inside the protocol messages such as the Session Initiation Protocol (SIP). A NAT gateway will therefore let such a protocol advertise private IPv4 addresses that are not unique in the public Internet address space.

NAT breaks peer-to-peer communication applications such as:

- Instant messaging
- Voice over IP (VoIP) protocols such as dedicated protocols, H.323 or SIP
- Real-time collaboration and sharing

These applications are key enablers for improved collaboration over the Internet between the enterprises and their employees, business partners or customers.

Migrating to IPv6 would help enterprise IT teams to get rid of NAT devices and lower the total cost of ownership (TCO) of the network infrastructure. Besides, migrating to IPv6 would also remove the NAT gateways that block peer-to-peer communication applications between organizations over the Internet.

This is why major analysts such as Burton Group confirmed that enterprises will adopt IPv6 in the mid-term[3] even if IPv6 penetration in enterprises has been slow up to now.

The IPv6 adoption drivers for enterprises

Several IPv6 drivers have been identified:

- Countries deploying entirely new IP infrastructure (for example, Korea and India)
- In APAC and the U.S., vertical markets such as military and government organizations (Ministry of Finance, Education, federal entities) consider IPv6 as mandatory for the renewal of their IT environment
- In Europe, some public organizations ask for IPv6 — mainly large universities and defense departments and European organizations such as Parliament. Seventeen percent of 610 public organizations in EMEA upgraded to IPv6 in 2009 (source: www.pcworld.com)
- Mobile Internet and wireless technologies for mobile handsets. For instance, working groups such as 3GPP recommend IPv6 for all new 3G mobile equipments
- The number of IP-enabled devices grows exponentially in both residential markets (peer-to-peer communications, always-on devices) and industry markets (transportation networks, sensors)
- The Next Generation Networks (NGN) and IP Multimedia Subsystem (IMS) embrace full mobility on whatever device and access network (WLAN, WiMAX, GPRS, GSM, broadband, fiber)

The technical benefits of IPv6

Efficient routing

IPv6 introduces a pure hierarchical addressing scheme, providing enhanced route prefix aggregation.

IPv4 also offers address simplification and hierarchy but then requires additional methodology (CIDR), NAT hardware and software, increasing costs and complex deployments.

Easy to configure

IPv6 provides auto-configuration of IP addresses on IPv6-enabled devices. This greatly improves scalability and manageability of networks. Also, administrators can move a large number of devices from one network to another with ease.

Security enhancements

IPv6 supports IPSec natively, allowing encryption of packets for confidentiality, integrity protection as well as host authentication. In addition, IPv6 provides better protection against address and port scanning attacks.

Note that these technologies are also available on IPv4 architecture, but require the additional hardware and software thus increasing costs and complexity.

Quality of Service enhancements

IPv6 packets contain a field to identify the traffic flows allowing implementation of a wide range of quality of service (QoS) functions, including bandwidth reservations and delay bounds.

Some equivalent fields are present in IPv4 but they are less flexible.

Mobility support

The IPv6 auto-configuration mechanism, neighbor discovery mode, routing headers and anycast addresses scheme enable greater mobility. An additional 'Mobile IPv6' layer has been designed to address further mobility requirements.

Although this technology addresses mobile network service providers' needs, very few application vendors sell products or solutions leveraging IPv6 mobility services. However, mobile IPv6 provides further infrastructure enhancements for today's wireless networks. For instance, the new IPv6 'scope' field for multicast has reduced the management costs of multicast traffic. Similarly, the IPv6 anycast address type improves automatic host location.

Long-term promises and transition time for enterprises

In short, the historical driver for IPv6 transition is IPv4 address depletion, which is accelerating due to global expansion of Internet connectivity, particularly in Asia. Other drivers include rapid deployment and adoption of residential broadband access services, proliferation of smart wired and wireless devices (with connected applications such as My Instant Communicator), and networking of ordinary appliances.

However, most enterprises will not immediately gain a great deal by adopting IPv6 because:

- Most enterprises use NAT or applicative gateways (Proxy, Reverse Proxy or Session Border Controller) to prevent their IPv4 addresses from being directly reachable from the Internet. So IPv4 address space depletion is rather a public Internet and service provider issue
- Few applications today deliver full promises from IPv6 so a migration to IPv6 will not bring many new features for the business user

The benefits of IPv6 for Enterprises are indeed long term. Therefore **enterprises and large organizations must prepare for a transition to IPv6 spanning several years.** Such a transition means designing a phased transformation plan as well as deploying enabling technology that will cope with the IPv4/IPv6 coexistence.

ENTERPRISES AND ORGANIZATIONS TRANSITION TO IPV6

A transition to IPv6 first requires a phased transformation of the infrastructure

Most large organizations have a complex information system with highly connected applications and services (business processes, customer relation management, communications services, intranets, and extranets). The consequence of this complexity leads most enterprises and large organizations to acknowledge the fact that all their infrastructure components cannot instantly migrate toward IPv6. **Most organizations plan an IPv6 transition where IPv4 and IPv6 will coexist for some time.**

Besides, as all applications and services rely on the IP infrastructure, an enterprise can benefit from IPv6- ready applications and services only if the IP infrastructure has been transitioned to IPv6 in a first phase.

This phased transition has to be carefully studied by the IT teams at different levels of their network infrastructure. The following checklist will help to design the IPv6 transformation plan.

IPv6 support hardware

Does hardware such as routers, switches, servers, firewalls, and proxy support IPv6?

Hardware and operating systems are limiting factors for applications and services transition to IPv6.

- If the hardware/OS is IPv6 ready, then the application software that runs on top of the OS can be upgraded to IPv6 in a further step
- If the hardware/OS is IPv4 only, additional enabling technology or hardware upgrade is necessary

Client/Server software usually requires that servers and clients are updated to IPv6. However, in some cases where the software relies on underlying containers such as Web browsers or Web servers, the application may be ported seamlessly to IPv6 if the containers support IPv6 and IPv6 compatible Domain Name System (DNS) records.

Server/Server and peer-to-peer software such as communication servers or devices may exchange IP addresses, and therefore must be updated to handle IPv6 and IPv6/IPv4 translation.

IPv6 WAN service provider

Does the organization's service provider (SP) support IPv6?
The Enterprise WAN or some parts of the WAN may move to IPv6, whereas LAN in branch offices and campuses stay IPv4. This could happen as service providers that run an Enterprise WAN move to IPv6 because of IPv4 address exhaustion.

Some LANs may move to IPv6; for instance, a brand new campus, whereas the WAN stays in IPv4 mode because of cost constraints.

Some enterprises also decide to keep the enterprise LAN and WAN with IPv4 addressing, while a service provider offers IPv6 access to the Internet and to mobile users.

Enterprise WAN site prefixes

To prevent use of NAT technology, a large organization should get a 48-bit site prefix used for routing IPv6 packets within the Enterprise WAN. The IPv6 addresses are then derived from these prefixes.

Enterprise WAN subnets

Large organizations will have to design the entire IPv6 network topology and addressing plan before deploying IPv6 entities. The addressing plan will take the main servers, routers and hosts into account before the actual IPv6 configuration takes place.

Enterprise WAN tunnels

Transition from IPv4 requires that the tunnel topology be planned and updated over time. The plan should indicate which routers or switches will support tunnels to external networks or other subnets. Several tunneling technologies may be deployed at the same time.

IPv6 security design

The organization's security policy will be updated to take into account IPv6 transformation of firewalls, IPSec gateways, Proxy/Reverse Proxy, Session Border Controller, policy servers, authentication repositories and directories.

Organizations should also pay attention to the fact that some of these security applications modify IP packets in flight and therefore are critical in the transition to IPv6. DMZ will also have to fit in the overall IPv6 addressing plan.

IPv6 deployment on routers and hosts

Organizations will then configure IPv6 on all routers and hosts.

IPv6 network and user services

Organizations will have to upgrade the IP infrastructure network services such as DNS, Dynamic Host Configuration Protocol (DHCP) or Lightweight Directory Access Protocol (LDAP) servers that deal with IP addressing translation, leasing or control. These servers must be updated with new IPv6 addresses.

User services such as Network File System (NFS), virtual machines, operating systems, Web servers, communication servers, and e-mail servers will then be transitioned to IPv6. Eventually, endpoints can be transitioned by the IT teams: PCs, desktop phones, wireless access points, wireless phones, printers and so on.

Organizations transitioning to IPv6 should consider all these phases in their IPv6 transformation plan.

Enabling technology is key for a smooth IPv4 to IPv6 transition

As few large networks will transition instantly from IPv4 to IPv6, transition technology has been designed and deployed:

- At the IP infrastructure layer:
  - ¬ DNSs that can serve IPv4 and IPv6 hosts and relay traffic to NATs
  - ¬ NATs that translate IPv6 traffic into IPv4 packets
  - ¬ Tunneling and relaying techniques: Encapsulation in edge NAT equipment helps IPv6 islands exchange through IPv4 or IPv4 LANs to be seamlessly reachable over an IPv6 network
  - ¬ Active dual IPv4-IPv6 stack routers enabling IPv4 and IPv6 routing at the same time

- At the business application layer
  - ¬ Active dual IPv4-IPv6 stack and application logic enabling software servers or clients simultaneously exchanging information with IPv4-only or IPv6-only clients or servers
  - ¬ Application logic to bridge IPv4 and IPv6 communication protocols such as SIP. Indeed, SIP is a standard peer-to-peer communication protocol that transports IP addresses of peers for further signaling or voice, video, instant messaging media exchange. SIP entities have to handle SIP IPv4/IPv6 translation features when connected to IPv4-only SIP endpoints

As the IPv4 to IPv6 transition standards have taken a long time to emerge, a large part of the enabling technology based on relays and application logic has been mostly proprietary leading to architectures that are difficult and costly to transform. However, as standards have been finalized, or in the case of SIP are being finalized, some vendors now issue products that comply with interoperable standards. This enables large organizations with more sustainable transition technology.

IPv4 to IPv6 transition relies on standards compliance and software upgrades

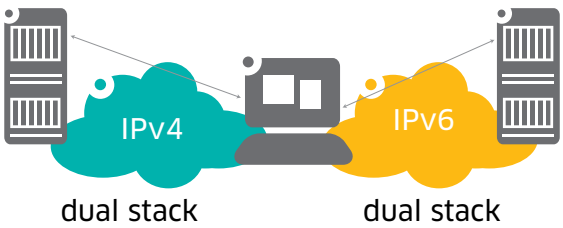
The IPv4 to IPv6 transition will happen through network equipment compliance (hardware and software upgrades) and by enabling technology that allows a phased transformation between network equipment.

Phase 1: Hardware upgrade requires the set-up of hardware devices such as routers, switches, storage equipment, servers, and perimeter security equipment. This task is a fundamental requirement but it remains a complex and costly matter. Software upgrades are then feasible if hardware and operating systems are IPv6 compliant. This can be performed through firmware or software updates depending on the equipment.

Phase 2: IPv6 transition mechanisms enabling technology are then required to meet the challenge of IPv4 and IPv6 coexistence. The following standard technologies are key for Enterprise Communication Services transition to IPv6:

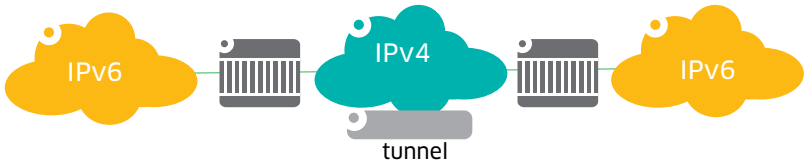
- **Dual stack** (RFC 4213). Each switch, router or host has both stacks implemented and are capable of coping with both protocols by evaluation of the protocol field in the header. Applications can choose the protocol to use or can automatically select it according to address type

Figure 1: Dual stack transition



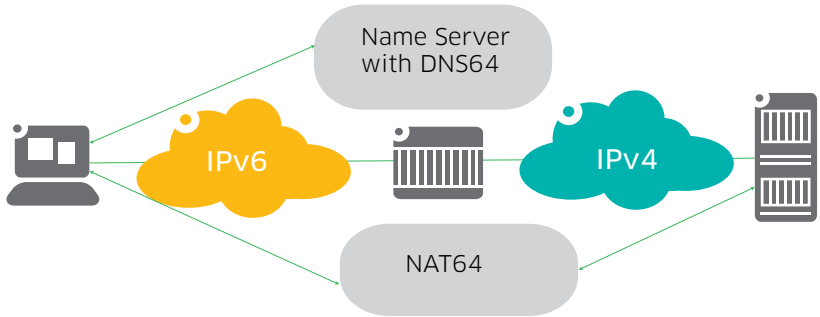
- **Tunneling** consists of encapsulating IPv6 packets within IPv4. ISATAP (RFC 5214) and Teredo (RFC 4380) are candidates for enabling this 6to4 tunneling mechanism. On the opposite 4to6 tunneling allows inter-site connection of IPv4 sites over IPv6 network This can be provided by 4over6 (RFC 5747) and DS-Lite (NAT44 + 4over6)

Figure 2: Tunnels



- Address Family Translation (AFT) replaces deprecated NAT-PT (RFC 4966). This technique is all about replacing headers and addresses of one family of IP with headers and addresses from another IP family, in an IP packet. It is mainly composed of NAT64/NAT46 and DNS64/DNS46. In IPv6-only networks, AFT functionality can be used to enable hosts to establish connections to services in the IPv4-only world, and in some cases, the other way around as well

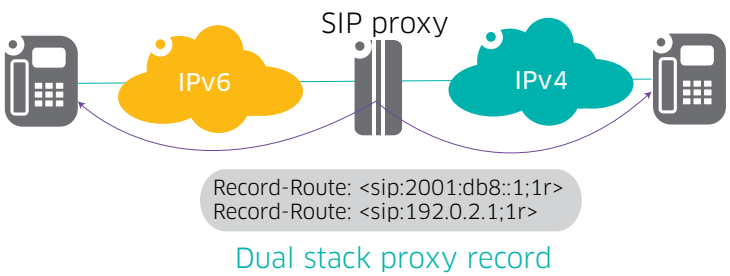
Figure 3: Address Family Translation



- Concerning the SIP protocol, the impact of IPv6 evolution has been recentlyinvestigated by the IETF SIPPING working group (http://tools.ietf.org/html/rfc6157, April 2011). For example, Figure 4 depicts the improved role of a dual stack SIP proxy that manages the IPv4/IPv6 interconnection with addressing both interfaces in transitioning SIP header and SDP body

  The SIP-IPv6 landscape continues to emerge and change and NAT traversal technology such as ICE protocol (RFC 5245) that makes use of STUN/TURN is also leveraged to address the interconnection of IPv6 with IPv4 equipment.

Figure 4: SIP IPv6 transition



Success factors of an IPv4 to IPv6 transition plan

In brief, the key success factor for IPv4 to IPv6 transition is to design a plan that takes into account:

- A phased transformation at the infrastructure and application levels
- A cost/benefit analysis on hardware and/or software upgrade to prioritize the phased transformation
- Standards-based enabling technology to accommodate the network areas or application elements that will not be immediately upgraded to IPv6. Using standards-based technology protects the investments better
- Communication applications and services require additional caution during the transition since many communication protocols and application ecosystem integrations rely on peer-to-peer exchanges that are sensitive to IPv6 transition. SIP standards for IPv4 and IPv6 translation have recently been finalized

ALCATEL-LUCENT PHASED APPROACH TO THE ENTERPRISE IPV4/IPV6 TRANSITION

Alcatel-Lucent acknowledges that a phased transition is the key for IPv6 transformation in large enterprise or organization networks. Enterprises network infrastructure and application upgrades may take place over time as large network 'islands' will remain IPv4 and both address formats may coexist for a long period.

Therefore, Alcatel-Lucent can help customers go through this transition by:

- Providing IPv6-enabling technology in its hardware portfolio and software suites
- Following customers' specific needs and network architecture for enabling IPv6 technology in an effective way

Alcatel-Lucent Communication Services and Applications suite will implement IPv6 transition technology such as:

- Upgrades to dual stack Unified Communication and Collaboration Servers
- Upgrade user devices and applications
- Upgrades to dual stack of the overall communication ecosystem, including communication services and business or vertical application integration
- Upgrades to dual stack management solution platforms

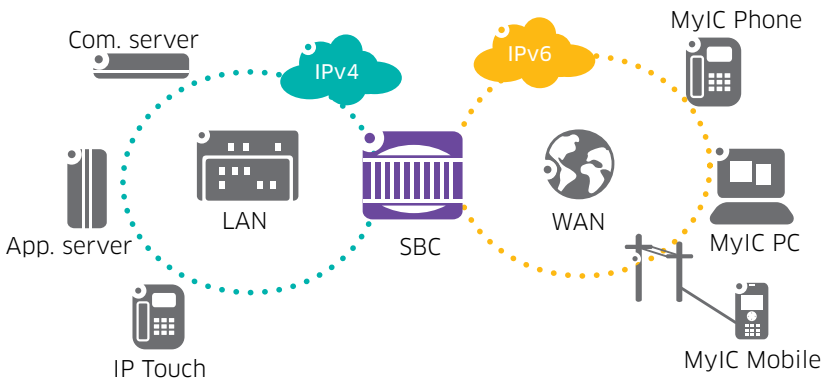
The following section provides examples of a phased transformation that a large enterprise or organization may choose to implement when transitioning to IPv6. Each section also illustrates the Alcatel-Lucent Enterprise portfolio evolutions and when Alcatel-Lucent sees the transformation taking place in enterprise networks.

Transition to IPv6 public connectivity

Enterprises may first leverage IPv6 from service providers public WAN without drastically transforming their enterprise network.

Figure 5 below shows an example where the internal enterprise network architecture remains based on IPv4. However, remote users may reach the enterprise resources having an external IPv6 address by connecting to the public IPv6 network. For example, this is going to be a common situation in APAC regions where the important need of large amounts of IP addresses makes public network move rapidly toward IPv6.

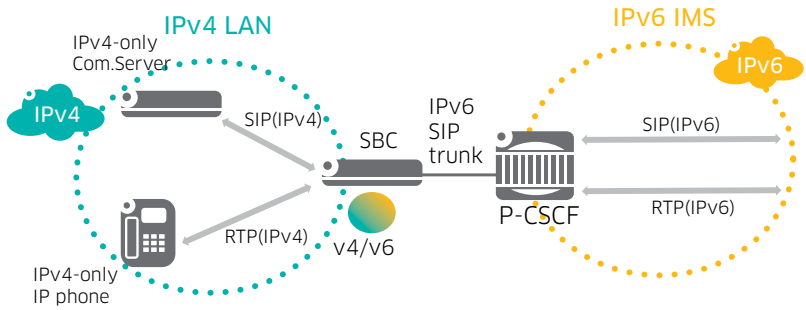
Figure 5: IPv6 public network



In such a topology, Alcatel-Lucent recommends the following first IPv6 transition principles:

- Leverage Address Family Translation (AFT) capabilities of applicative border gateways for communication services (SBC, reverse proxy). It would offer the IPv6 connectivity to enterprise environment to allow communications between IPv6 remote devices connected through the public IPv6 network and the IPv4-based communication services of the enterprise network (see Figure 6)
- LAN communication servers and devices keep IPv4 connectivity. In fact, the above gateways avoid engaging immediately in complex and expansive upgrades of the LAN infrastructure

Figure 6: Address Family Translation for communication services



This solution is a first step for enterprises that want to follow a smooth IPv6 migration while keeping unchanged IPv4-only business and communication services in the LAN.

Our product offer is ready today for supporting a SIP trunking scenario thanks to SBC capabilities.

In the context of the Alcatel-Lucent UC&C mobility solution, full IPv6 support for MyIC clients will be addressed, so nomadic or remote users can reach enterprise communication services from an IPv6 network.

Alcatel-Lucent believes that Enterprise may start evolving toward this step in the next few years.

Enterprise LAN IPv6 migration

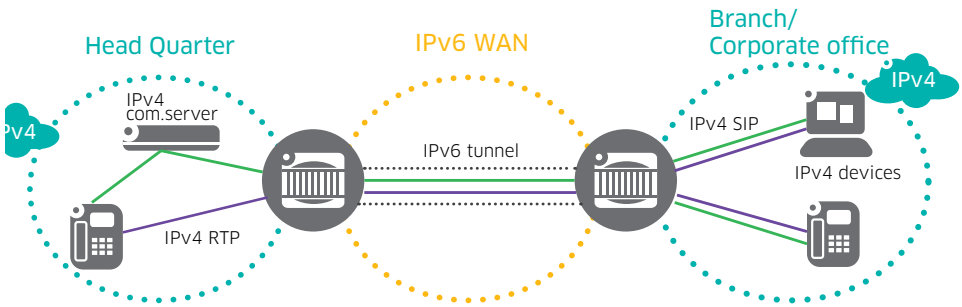
As the Alcatel-Lucent communication services product evolves to IPv6 compatibility, the next section now presents our recommended strategy for a progressive LAN migration of communication services to IPv6.

Step 1: Private WAN phased transition

Alcatel-Lucent acknowledges that IPv6 and IPv4 network infrastructures will coexist for some time, if not indefinitely. Tunneling technologies provide a way for maintaining interoperability between IPv4 islands over IPv6 networks (the Alcatel-Lucent OmniSwitch product range supports this enabling technology). The transition phase then relies entirely on data infrastructure capabilities and there is no impact on Communication and Application services within the customer's network.

Figure 7 shows an IPv6 tunnel bridging two IPv4 LANs.

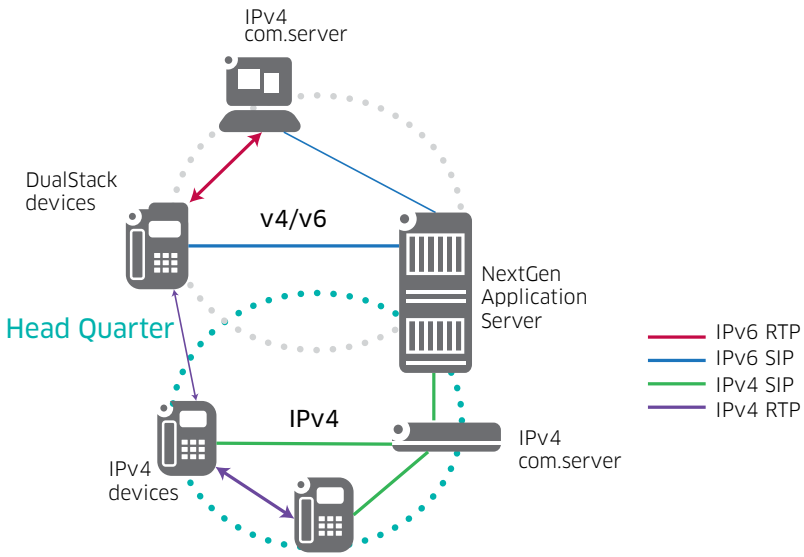
Figure 7: Private WAN transition



Step 2: LAN phased transition

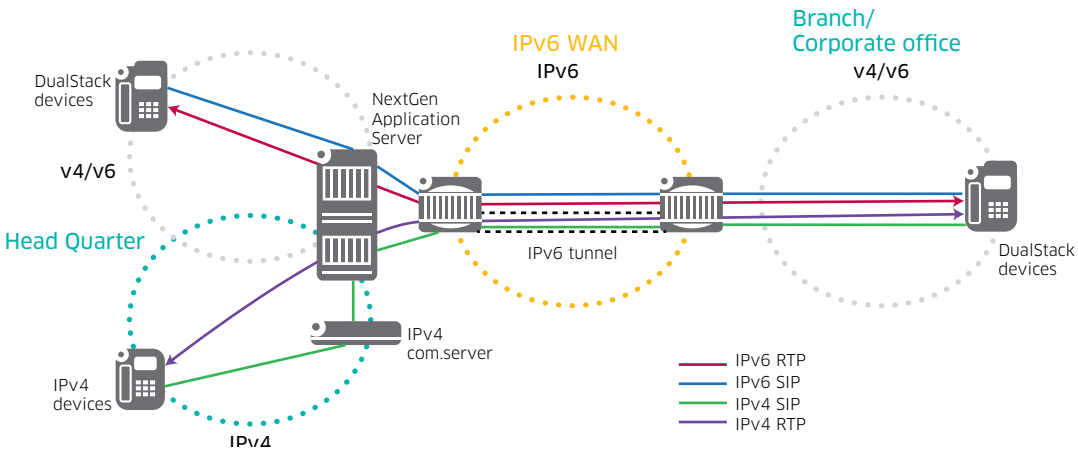
The LAN transition can now occur by introducing IPv6 dual stack servers and devices for enabling communications between these dual stack equipment and IPv4-only services. Figure 8 depicts the evolution of communication and application servers acting as a point of interconnection for this configuration. IPv6 transition mechanisms in the Session Initiation Protocol (SIP) will allow maintaining transparent VoIP communications between IPv4 and IPv6 dual stack equipment.

Figure 8: LAN transition



The execution of this strategy allows, for example, using a Next-Generation Application Server and embedded translation capabilities for connecting indifferently pure IPv4 devices and next-generation ecosystems.

Figure 9: LAN and WAN dual stack transition

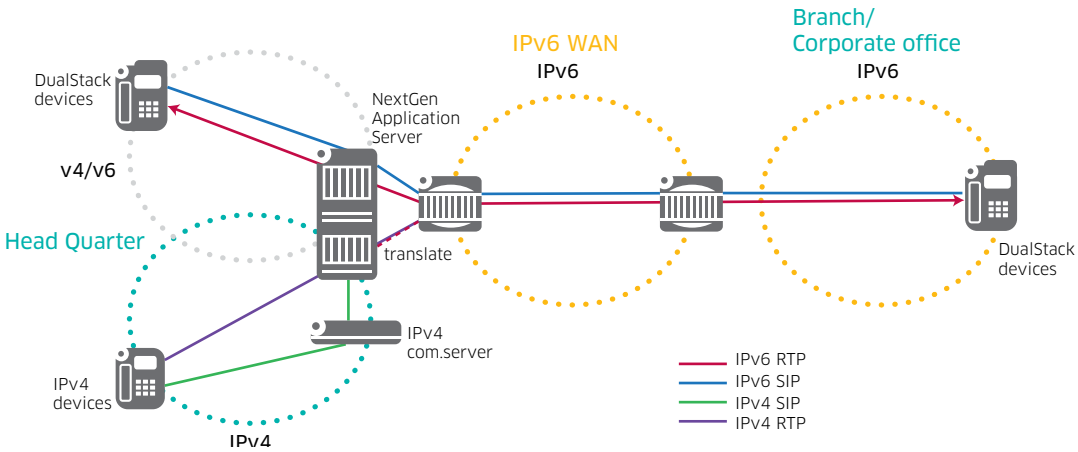


Step 3: IPv6-only regional deployments

The next transition phase consists of slight migration of regional sites. New (or existing) branch/corporate offices may be deployed (or migrated) entirely on IPv6-only architecture. They would then require to be connected to headquarters and other sites that may have IPv4-only or dual capabilities. Alcatel-Lucent next-generation communication and application servers bring the solution to manage, route and adapt SIP and media traffic from IPv6 locations to IPv4. Address Family Translation now brings its full purpose by enabling IPv6-only equipment to continue using IPv4-only services.

Figure 10 illustrates remote IPv6-only devices that can connect to IPv4-only devices through a front SBC in the headquarters.

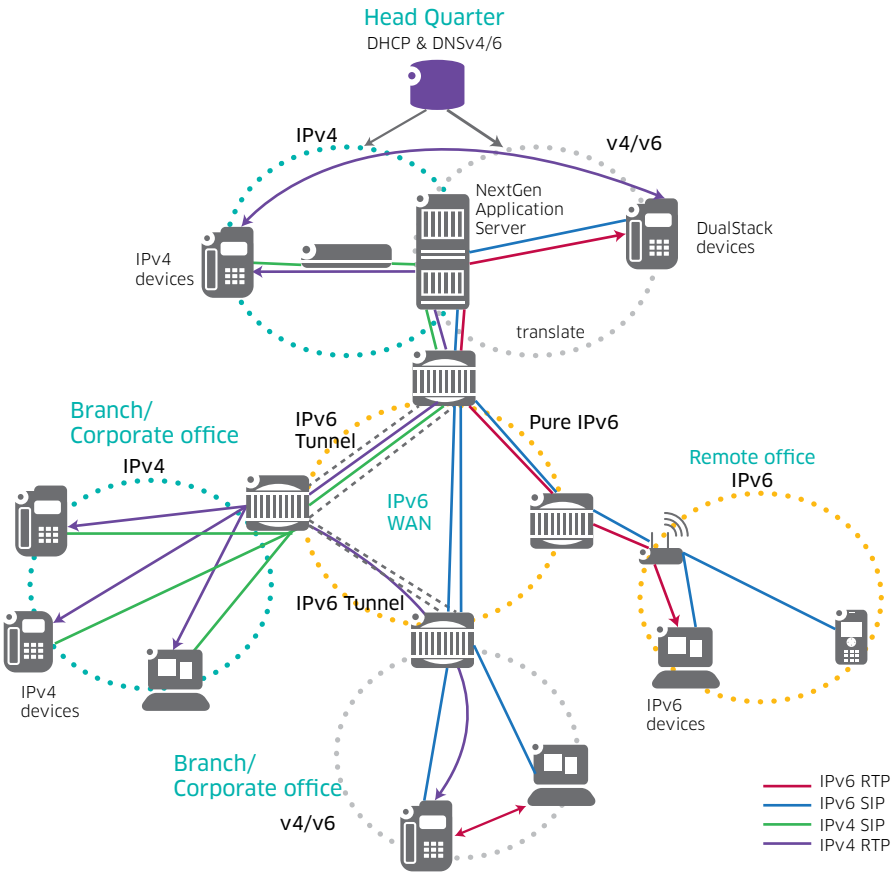
Figure 10: IPv6-only branch offices



Consolidated view of an enterprise-wide IPv6 transition

Figure 11 shows an example where the transition spans the entire enterprise network architecture. The presented transition enabling technology elements allow all the communications between IPv4 networks and IPv6 networks through the above-mentioned mechanisms, dual IPv4/IPv6 stack, IPv6 tunneling and Address Family Translation. All the media flows will be transported between IPv4 and IPv6 networks.

Figure 11: IPv4 islands, IPv6-only WAN and branch offices



Alcatel-Lucent successful IPv4 to IPv6 transformation drivers

The Alcatel-Lucent Enterprise portfolio will enable a successful IPv4 to IPv6 transition of large enterprise communication networks due to:

- A phased transformation allowing a smooth transition over time and protection of current and past investments
- Standards-based enabling technology that allows customer to phase the transition of communication services with the transition of its application ecosystem (CRM applications, industry-specific services such as notification servers, and management hypervisors)

CONCLUSION

The IPv4 address exhaustion in the Internet and public service provider domains will increase the adoption rate of IPv6 by service provider networks and consumer applications and devices in the coming years.

As enterprises and large organizations use NAT technology, IPv4 address space depletion is not as critical for them as in the public Internet. The benefits of IPv6 for enterprises and large organizations are indeed long term. Therefore, enterprises and large organizations must prepare for a transition to IPv6 spanning several years. Such a transition means designing a phased transformation plan as well as deploying enabling technology that will cope with the IPv4/IPv6 coexistence.

A sustainable transformation plan over time requires that IPv4/IPv6 enabling technology relies on standard protocols. The latest backward compatibility issues at the infrastructure level have been solved by standardization bodies in H1 2010. However, communication protocols such as SIP are sensitive to IPv4/IPv6 translation because they exchange IP addresses of media streams between peers. Consequently, SIP IPv4/IPv6 translation standards are required. They have been published very recently by standardization bodies.

Alcatel-Lucent is strongly committed to helping large enterprises and organizations enable sustainable transition plans using standard IPv4/IPv6 enabling technology such as tunnels, dual stack phones and application servers, session border controllers and SIP translation services. This document reviews several steps of Alcatel-Lucent phased approach to migrating communication services in a large enterprise network while minimizing disruption of services and costly major upgrades: SIP trunking, enterprise WAN transformation, LAN and branch office transformation.

As a result of this phased approach, existing and future customers of OmniPCX Enterprise Communication Services can seamlessly insert communication services into their IPv6 strategic plan and transition to IPv6 at their pace.

Footnotes

1 Internet Assigned Numbers Authority (IANA), Regional Internet Registries (RIR)
2 Gartner Group, “Hype Cycle for Networking and Communications,” August 2010.
3 Burton Group, “Changeover to IPv6: The Deadline Approaches,” May 2010.

Sources

1. http://tools.ietf.org/html/rfc6146
2. http://tools.ietf.org/html/rfc6147
3. RIPE: http://www.ripe.net

Note

The information contained in the present document is not binding on Alcatel-Lucent Enterprise and can be modified by Alcatel-Lucent Enterprise at any time without prior notice. Alcatel-Lucent Enterprise makes no warranty or representation of any kind, whether express or implied, with respect to such information. Alcatel-Lucent Enterprise shall have no liability for direct, indirect, special, incidental, punitive or consequential damages of any kind including but not limited to loss of profits, income, business, anticipated savings, reputation as well as financing costs or any other economic loss arising out in relation to the present document.