

White Paper | AX Series

The End of IPv4?

Migration paths to IPv6

February 2013

Disclaimer

This document contains confidential materials proprietary to A10 Networks, Inc. This document and information and ideas herein may not be disclosed, copied, reproduced or distributed to anyone outside A10 Networks, Inc. without prior written consent of A10 Networks, Inc.

This information may contain forward looking statements and therefore is subject to change without notice.

Copyright

©2013 A10 Networks, Inc. All rights reserved.

ACOS, aFleX, aXAPI, Virtual Chassis, SoftAX and SmartFlow are registered trademarks of A10 Networks.

Table of Contents

1. The end of IPv4?	5
2. Migration paths to IPv6	6
3. How to transition seamlessly to IPv6?.....	7
4. Service Provider transition to IPv6: The challenges.....	8
4.1. Service Provider challenges	8
4.2. Service Provider solutions.....	10
4.2.1. Carrier Grade NAT (CGN or CGNAT)	10
4.2.2. NAT444	11
4.2.3. Dual-stack Lite (DS-Lite).....	13
4.2.4. IPv6 rapid deployment (6rd).....	16
4.2.5. NAT64 and DNS64	19
5. Content Provider and Enterprise transition to IPv6	22
5.1. Content Provider and Enterprise challenges	22
5.2. Content Provider and Enterprise solutions.....	23
5.2.1. SLB-PT – (Server Load Balancing with Protocol Translation).....	23
5.2.2. NAT-PT – (Network Address Translation with Port Translation).....	26
6. Why select A10 to help you to migrate to IPv6?	29
6.1. High performance	29
6.2. Flexible solution	29
6.3. Value added	29
7. Summary and Conclusion	30
Appendix – IPv6 benefits overview	31
IP addresses abundance	31
Efficiency	32
Security.....	32
Simplicity	33

Quality of Service (QoS)..... 33

1. The end of IPv4?

On February 3, 2011, the Internet Assigned Numbers Authority (IANA) allocated the last five remaining /8s of IPv4 address space to the Regional Internet Registries (RIRs); the local registries are running low on IPv4 addresses, rapidly.

The advent of new Internet-connected locations (from hotels to planes and more world-wide) and new Internet-connected devices (notable examples include smartphones, smart meters, gaming devices and other household appliances) has exacerbated the shortage. Each of these extra devices places greater pressure on the existing IPv4 infrastructure.

The adoption rate of IPv6 is increasing rapidly. On each annual IPv6 Launch Day, in June 2011 and 2012, the world turned on IPv6 and left it on. It was a success according to the event organizers. For example, in 2012, over 60 access providers and more than 3,000 websites publicly participated in the Launch event. Those participants all have committed to keeping IPv6 running as part of normal business operations.

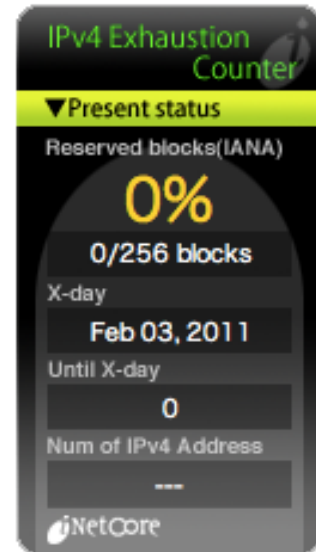


Figure 1: IANA IPv4 address pool is depleted. (http://inetcore.com/project/ipv4ec/index_en.html)

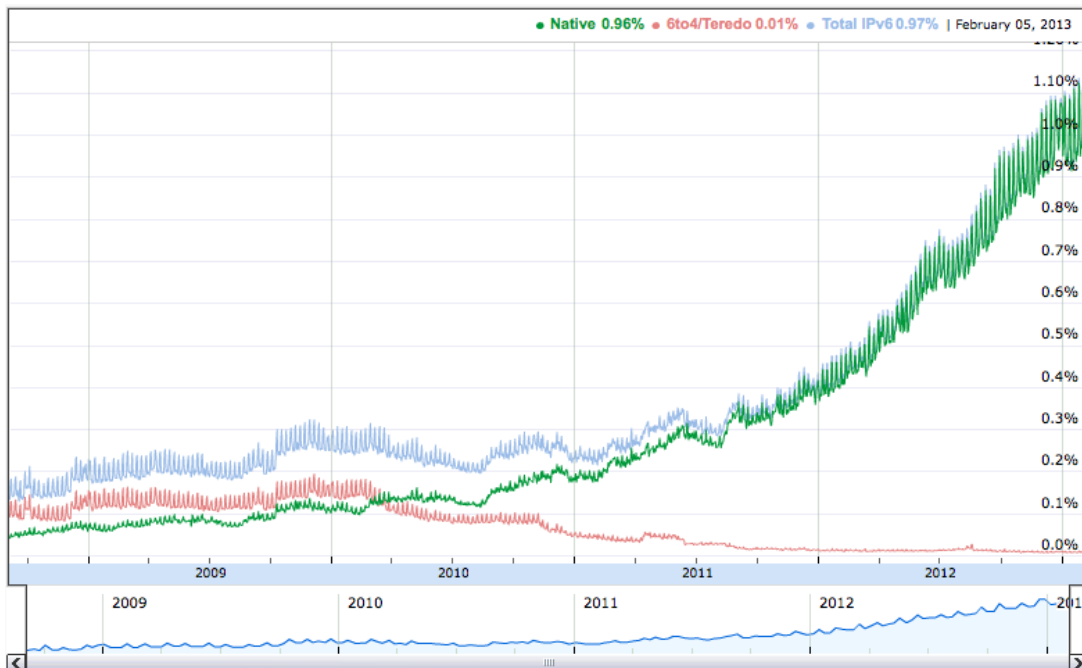


Figure 2: IPv6 access statistics. Source: Google

2. Migration paths to IPv6

IPv6 removes the IP address scarcity by creating a new address space with vastly more potential addresses. IPv6 also provides many other benefits to Service Providers and end-users, such as improved efficiency, security, simplicity and Quality of Service (QoS) versus IPv4.

Many vendors of enterprise and consumer electronics are offering support for IPv6 network connectivity, for both IPv6 management and IPv6 traffic handling, that is on par with IPv4 functionality.

However, the transition from IPv4 to IPv6 cannot be achieved overnight. A total switchover is impractical due to the number of hosts and organizations involved with the Internet and associated systems. Companies realize that even with IPv6 implementation in their networks, there still will be a need to communicate with legacy IPv4 servers and applications. On the other side of the equation, companies also realize their IPv4 customers will need to use services developed with IPv6, such as Microsoft DirectAccess.

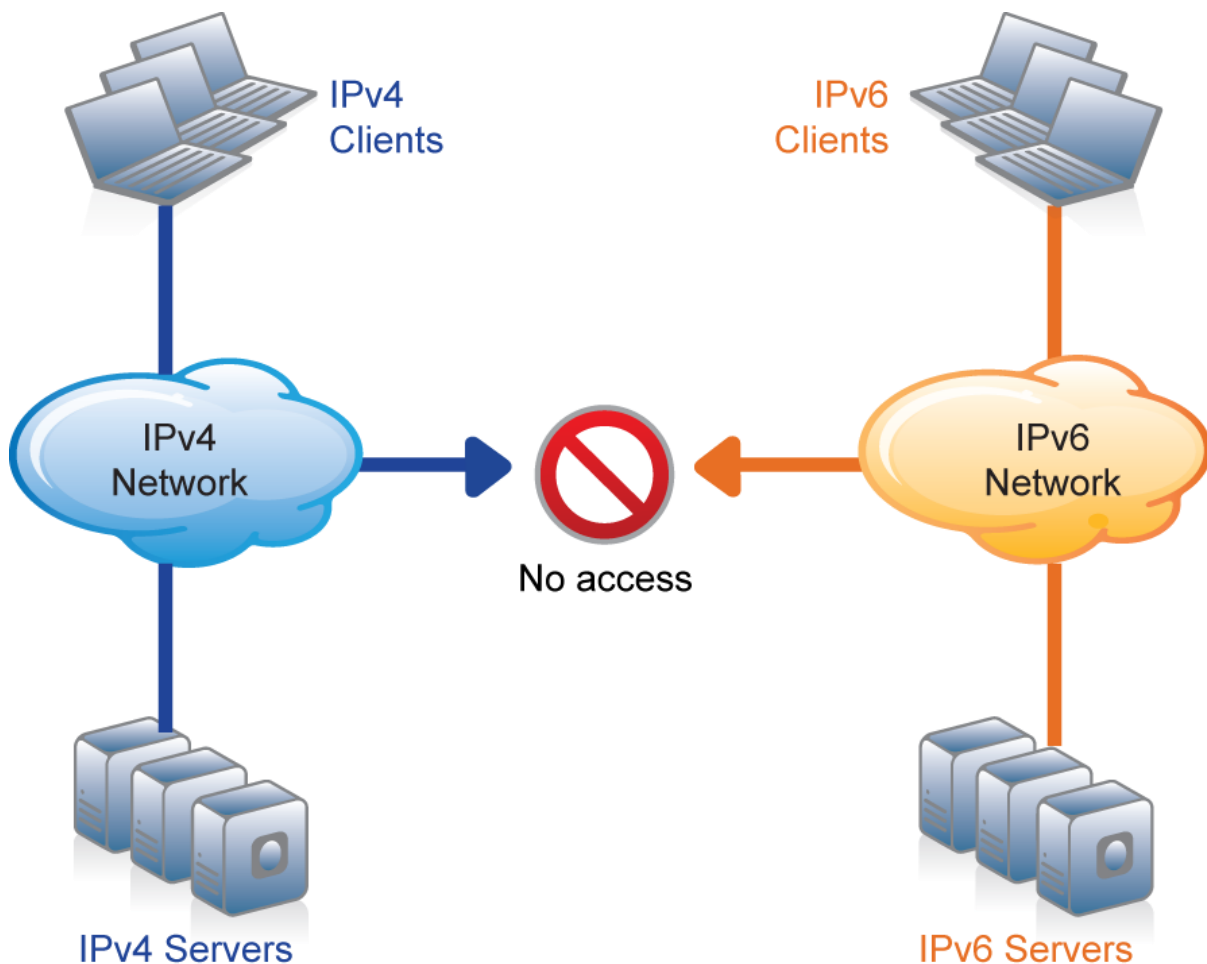


Figure 3: No built-in communication or backward compatibility between IPv4 and IPv6 networks

3. How to transition seamlessly to IPv6?

To provide a complete IPv6 service, each link in the chain must be running IPv6, from the end-user, to the carrier, and to the content provider. Realistically, not all three of these links in the IPv6 chain will transition to IPv6 at the same time. IPv4 is still required during the transition to IPv6.

Network organizations, network vendors, large network carriers and large enterprises have been working on strategies to migrate seamlessly from IPv4 to IPv6 networks. Multiple methods have been proposed and some are being standardized, but there is no single solution that fits the needs of all customers.

The best solution for a given organization varies depending on their existing infrastructure and the organization's timeframe for migrating to IPv6.

This white paper details the different solutions being standardized for both groups of customers:

- Service Providers, including cCarriers, Internet Service Providers (ISPs), and Mobile operators
- Content Providers and Enterprises

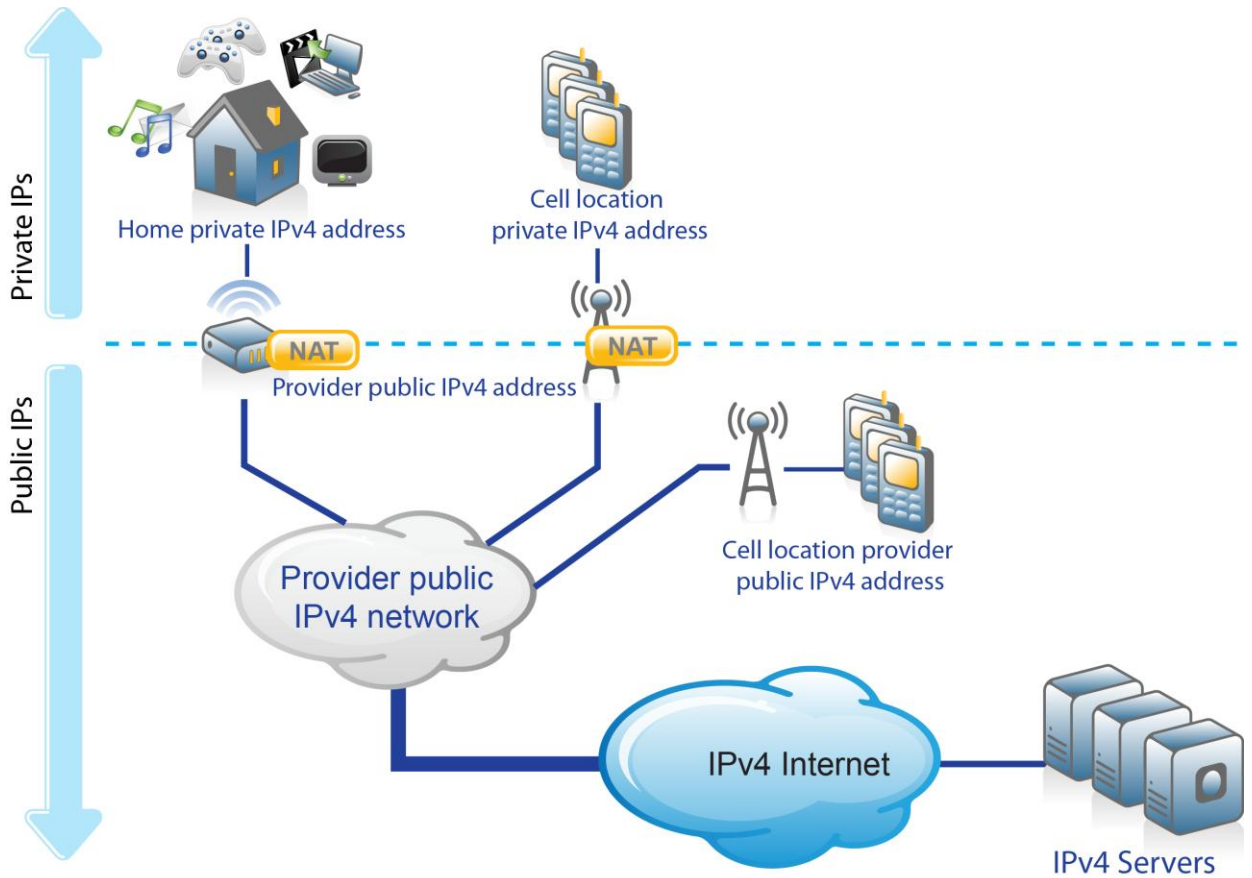
4. Service Provider transition to IPv6: The challenges

One of the main roles of Carriers, ISPs and Mobile Operators is to provide Internet access; here we examine the applicable challenges.

4.1. *Service Provider challenges*

Service providers are grappling to accommodate large waves of new customers registered to their services, with new devices such as smart phones and gaming devices, each requiring Internet access. This means Carriers, ISPs and Mobile Operators are the first ones to suffer from the negative consequences of IPv4 address exhaustion.

As IANA has depleted its IPv4 address space (see Figure 1), it is getting ever more difficult for organizations to obtain new blocks of IPv4 addresses. With only very small blocks of new IP addresses assigned by RIRs, for as long as this is even possible, providers are facing the challenge of increased management overhead, or in the worst-case scenario, the inability to provide new services.



Multiple home devices (PC/gaming device/IP-TV) with home private IPv4



Modem/router at home converting (NATing) home device private IPv4 to provider public IPv4



Smartphones (some mobile operators provide a public IP to each smartphone)



Cell converting (NATing) smartphone private IPv4 to provider public IPv4



Cell simply routing smartphone traffic

Figure 4: Service Provider current network

4.2. Service Provider solutions

The solution is to start planning for alternatives now, in the shape of IPv6 and associated transition technologies. IPv4 hosts will persist for some time, thus making co-existence and translation technologies essential.

Multiple solutions are being reviewed to extend the life of IPv4 networks or enable the adoption of IPv6 services; the most prevalent of these include the following:

- Carrier Grade NAT (CGN or CGNAT), a.k.a. Large Scale NAT (LSN)
- NAT444
- Dual-stack Lite (DS-Lite)
- IPv6 rapid deployment (6rd)
- NAT64 and DNS64

4.2.1. Carrier Grade NAT (CGN or CGNAT)

Carrier Grade NAT, also known as Large Scale NAT (LSN), is not a technology that in itself solves the IPv4 address scarcity or offers IPv6 services. Instead, CGN is a standard for Network Address Translation (NAT) used by different solutions such as NAT444 and DS-Lite, which can offer additional IPv6 services.

CGN was created to standardize the NAT functions and behavior between network vendors.

CGN formalizes NAT behavior, while guaranteeing a transparent NAT service for end-users' applications, for example:

- Stickiness: End-users first NATed with address IP1 will have all subsequent flows NATed with address IP1.
- Fairness: All end-users can be guaranteed to have NAT resources reserved for their future needs.
- Hairpinning: Enables direct communication between internal end-users, when the destination endpoint is in the same subnetwork.
- End-point independent mapping and filtering (IEM and IEF): Provides "Full-cone", transparent connectivity to hosts on the inside of the NAT area.

4.2.2. NAT444

NAT444 is used by Service Providers as a quick, temporary fix for IPv4 exhaustion, to buy time for the correct implementation of their migration to IPv6.

NAT444 is IPv4 only, thus it does not offer any IPv6 services, and therefore does not provide any of IPv6's benefits.

NAT444 technical walkthrough:

Service Providers provide a private IP address to their customer's router (first NAT IPv4-to-IPv4). The translation to a public IP address is done further down their network (second NAT IPv4-to-IPv4). Traditional NAT used today, in contrast, can be referred to as "NAT44. Figure 5 illustrates this additional layer of NAT.

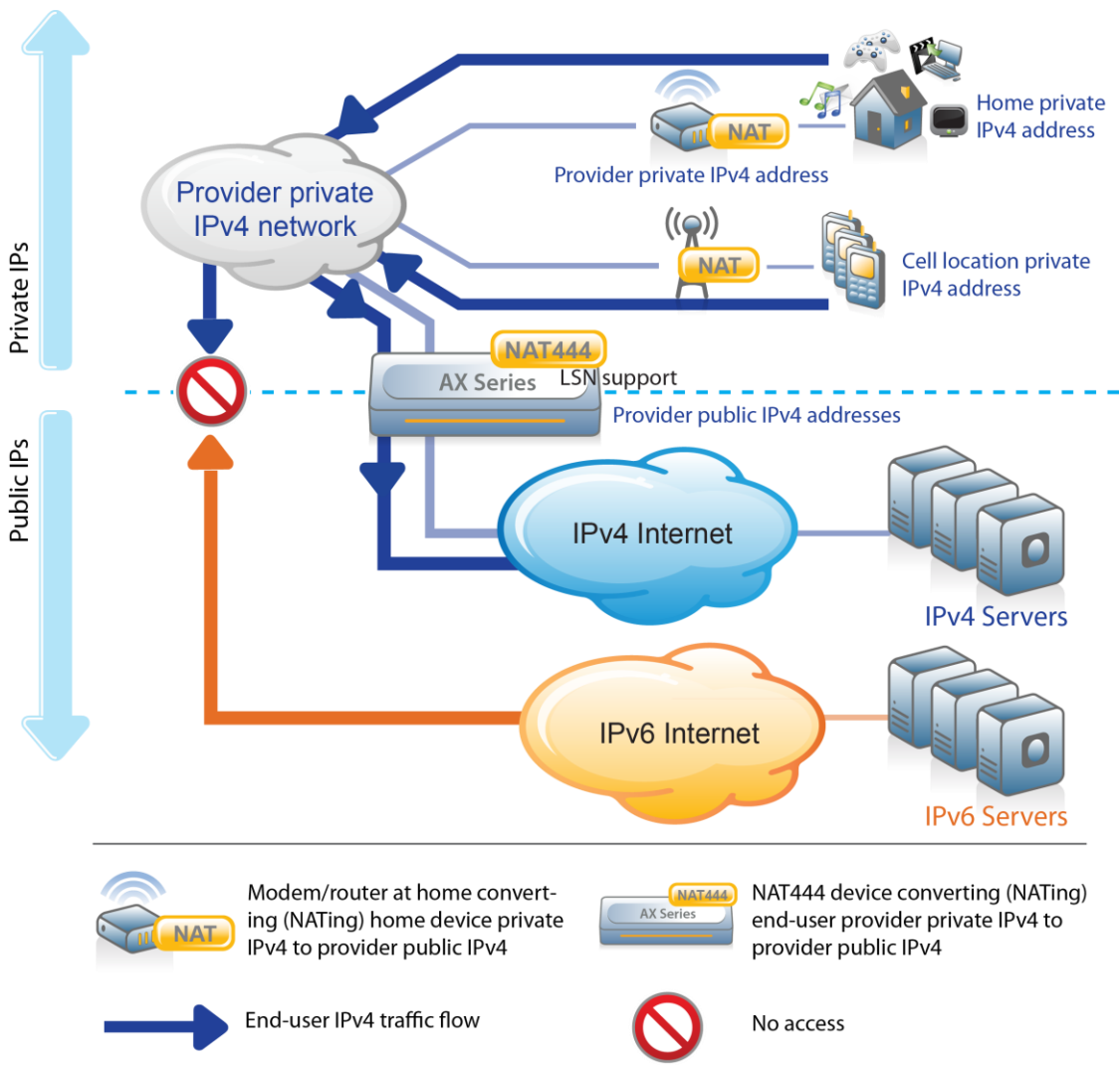


Figure 5: Service Provider NAT444 solution

Pros:	Cons:
<ul style="list-style-type: none">• More IPv4 subscribers can be supported with fewer IPv4 addresses.• No upgrade or enhancement is required on home modems/routers and cellular phones.• No core infrastructure support for IPv6 is needed.• Delivers efficiency through features, for example hairpinning for eliminating unneeded connections and delay.	<ul style="list-style-type: none">• Extends time before migrating to IPv6, but IPv6 migration is still required.• End-to-end connectivity is very complex (for IP telephony, or file sharing services).• Core infrastructure has no IPv6 benefits (such as efficiency, simplicity and security).• For stateful NAT, the NAT444 device must maintain a table with each active flow, requiring more resource usage.• End-users cannot host services such as web servers in their locations.• Does not allow access to IPv6 content.• Governments mandate the capability to track internal-to-external IP associations for extended periods of time, requiring an extensive logging infrastructure.

NAT444 device requirements

- CGN support
- High scalability for:
 - New connections per second
 - Concurrent connections
 - Throughput
 - Packets per second
- High availability for:
 - No service downtime (stateful failover)
 - Rapid failover
 - Flexible tracking (not simply remote device and interfaces)

Technical Note:

NAT444 uses CGN standards:

- draft-ietf-behave-lsn-requirements-10 (the main standard for CGN)
- RFC 4787, NAT Behavioral Requirements for Unicast UDP
- RFC 5382, NAT Behavioral Requirements for Unicast TCP
- RFC 5508, NAT Behavioral Requirements for Unicast ICMP

4.2.3. Dual-stack Lite (DS-Lite)

DS-Lite is used by Service Providers to maintain IPv4 connectivity through an all-IPv6 access network.

DS-Lite provides additional benefits. Using an IPv6 core network, the Service Provider provides IPv6 content access to their end-users, who are now on IPv6. However, at the same time, the Service Provider needs to provide IPv4 content access to their end-users who are still on IPv4. The Service Provider's IPv6 modem/router with DS-Lite support allows IPv4 users to connect to their modem/router and access the Internet, or any other IPv4 network.

DS-Lite does not provide any IPv4 content access to IPv6 end-users, or IPv6 content access to IPv4 end-users.

DS-Lite technical walkthrough:

In a DS-Lite environment, traffic for an IPv6 end-user with a device enabled for DS-Lite is simply routed to the IPv6 resources, using the regular IPv6 functionality on the device.

The end-user's DS-Lite router encapsulates IPv4 end-user traffic into IPv6 and sends it to the Service Provider's Address Family Translation Router (AFTR); the DS-Lite concentrator then decapsulates and NATs the IPv4 traffic with a public IPv4 address before routing it to the IPv4 resources. (The end-user DS-Lite router also is referred to as the *Basic Bridging Broadband (B4)* element.)

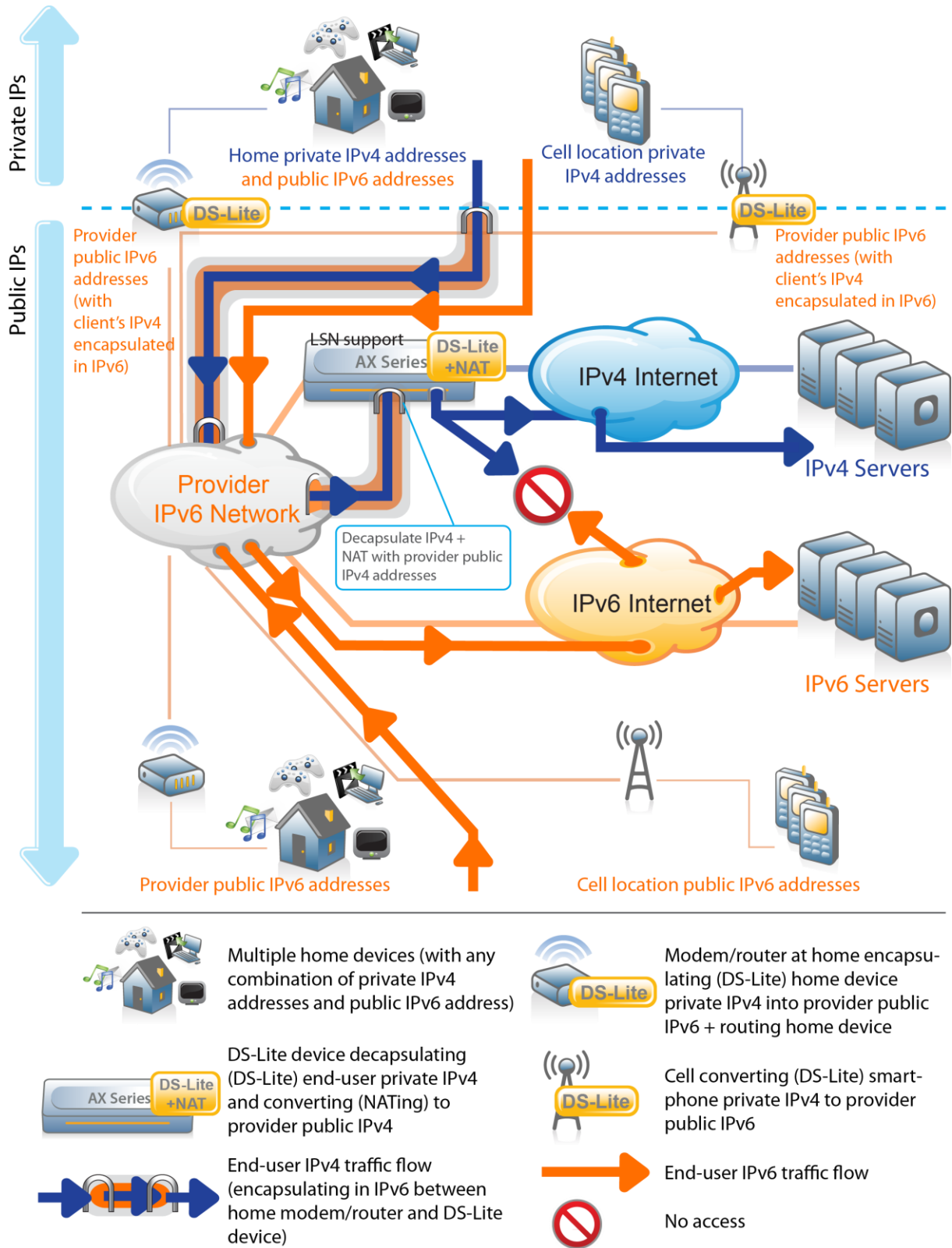


Figure 6: Service Provider DS-Lite solution

<p>Pros:</p> <ul style="list-style-type: none">• Resolves IP address scarcity.• IPv6 end-users have native access to IPv6 content.• Existing IPv4 end-users still have access to IPv4 content.• Allows co-existence of IPv4 and IPv6 end-users in each end location.• Enables incremental IPv6 deployment.• Core infrastructure provides IPv6 benefits (efficiency, simplicity and security).• End-users are able to host IPv6 services such as web servers in their locations.	<p>Cons:</p> <ul style="list-style-type: none">• Requires a DS-Lite router at the end-user location.• Stateful NAT requires a central DS-Lite device to maintain a table with each active flow, requiring more resource usage.
--	--

DS-Lite device requirements

- CGN support (for the Address Family Transition Router [AFTR] element)
- DS-Lite support (for both B4 and AFTR elements)
- High scalability for:
 - New connections per second
 - Concurrent connections
 - Throughput
 - Packets per second
- High availability with:
 - No service downtime (stateful transition failover)
 - Rapid failover
 - Flexible tracking (not based simply on remote device and interface)

Technical Note:

DS-Lite uses the following standards:

- RFC 6333, Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion

Plus Carrier Grade NAT (CGN) standards for the NAT component:

- draft-ietf-behave-lsn-requirements-10 (main standard for CGN)
- RFC 4787, NAT Behavioral Requirements for Unicast UDP
- RFC 5382, NAT Behavioral Requirements for Unicast TCP
- RFC 5508, NAT Behavioral Requirements for Unicast ICMP

The first RFC is used for encapsulation. The NAT component of each of the other standards, which are for CGN, is used.

4.2.4. IPv6 rapid deployment (6rd)

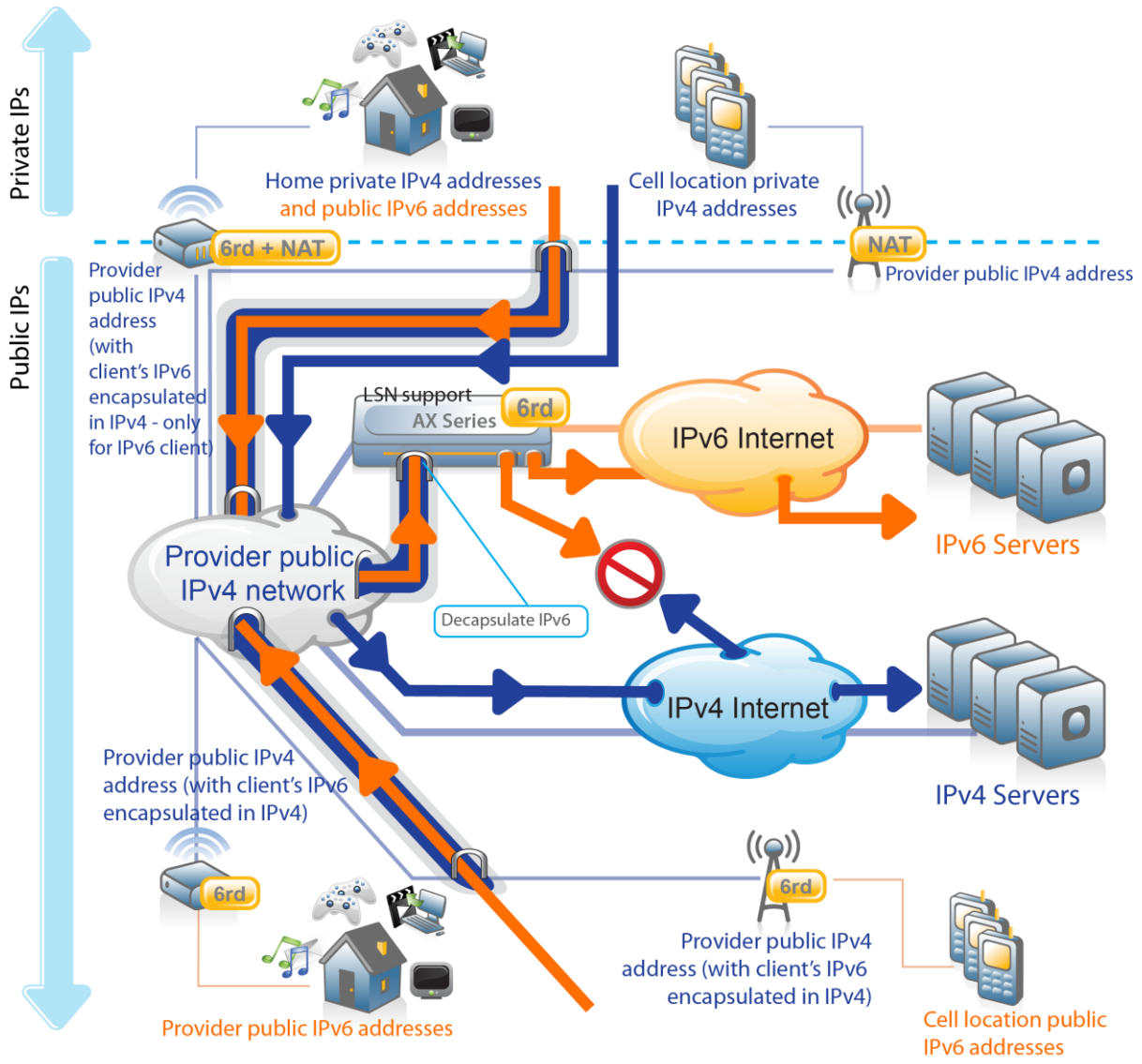
Leveraging an existing IPv4 core network, IPv6 rapid deployment (6rd) is used by the Service Provider to provide IPv6 content access to end-users that have IPv6-capable devices. The advantage for the Service Provider is that IPv6 Internet access is provided over an IPv4 access network.


But 6rd does not resolve the IPv4 exhaustion issue, nor does it provide any IPv4 content access to IPv6 end-users or IPv6 content access to IPv4 end-users.

6rd technical walkthrough:


The IPv4 end-user's traffic is simply NATed and routed to the IPv4 resources as normal.


The IPv6 end-user's traffic is encapsulated into IPv4 and sent to a 6rd device, which decapsulates it before routing it to the IPv6 resources.




- 


Multiple home devices (with any combination of private IPv4 and public IPv6)




Modem/router at home encapsulating (6rd) home device public IPv6 into provider public IPv4 + converting (NATing) home device private IPv4 to provider public IPv4 + routing home device
- 


6rd device decapsulating (6rd) end-user public IPv6




Modem/router at home encapsulating (6rd) home device public IPv6 into provider public IPv4 + routing home devices
- 

End-user IPv4 traffic flow (encapsulating in IPv6 between home modem/router and 6rd device)



Cell encapsulating (6rd) smartphone private IPv4 into provider public IPv6
- 

End-user IPv6 traffic flow
- 

No access

Figure 7: Service Provider IPv6 rapid deployment solution

Pros:	Cons:
<ul style="list-style-type: none">• New IPv6 end-users have access to IPv6 content.• Existing IPv4 end-users still have access to IPv4 content.• Allows co-existence of IPv4 and IPv6 end-users in each end location.• Enables incremental IPv6 end-user support at end locations.• No core infrastructure support for IPv6 necessary.• Stateless NAT does not need a central 6rd device that maintains a table with active flows. This results in less resource usage.	<ul style="list-style-type: none">• Does not resolve IP address scarcity – does not allow more subscribers.• Extends time before migrating to IPv6, but IPv6 migration is still required.• Core infrastructure has no IPv6 benefits (efficiency, simplicity and security).• Requires a 6rd router at the end-user location.

6rd device requirements

- 6rd support
- High scalability for:
 - New connections per second
 - Concurrent connections
 - Throughput
 - Packets per second
- High availability with:
 - No service downtime (stateful transition failover)
 - Rapid failover
 - Flexible tracking (not based simply on remote device and interface)

Technical Note:

6rd uses the following standard for encapsulation:

- rfc5969, IPv6 Rapid Deployment on IPv4 Infrastructures

The NAT component within each of the following CGN standards also is used::

- Draft-nishitani-cgn-02 (the main RFC for CGN)
- RFC 4787, NAT Behavioral Requirements for Unicast UDP
- RFC 5382, NAT Behavioral Requirements for Unicast TCP
- RFC 5508, NAT Behavioral Requirements for Unicast ICMP

4.2.5. NAT64 and DNS64

The majority of Internet content currently is available only on IPv4. While waiting for migration of content to IPv6, IPv6 end-users also need a way to access IPv4 services. NAT64 in combination with DNS64 provides this access.

The methods detailed above provide solutions for IPv4 exhaustion or provide IPv6 end-users with access to IPv6 content, but do not provide IPv4 content to IPv6 end-users.

Service Providers can, in addition to Nat64 and DNS64, use DS-Lite to provide IPv4 access for IPv4-only end-users.

Note: NAT64/DNS64 also is called NAT 6-to-4 or AFT (Address Family Translation).

NAT64 and DNS64 technical walkthrough

The IPv6 end-user's DNS requests are received by the DNS64 device, which resolves the requests.

If there is an IPv6 DNS record (AAAA record), then the resolution is forwarded to the end-user and they can access the resource directly over the Service Provider's IPv6 infrastructure.

If there is no IPv6 address, but there is an IPv4 address (A record) available, then DNS64 converts the A record into an AAAA record using its NAT64 prefix and forwards it to the end-user. The end-user then accesses the NAT64 device, which NATs the traffic to the IPv4 server.

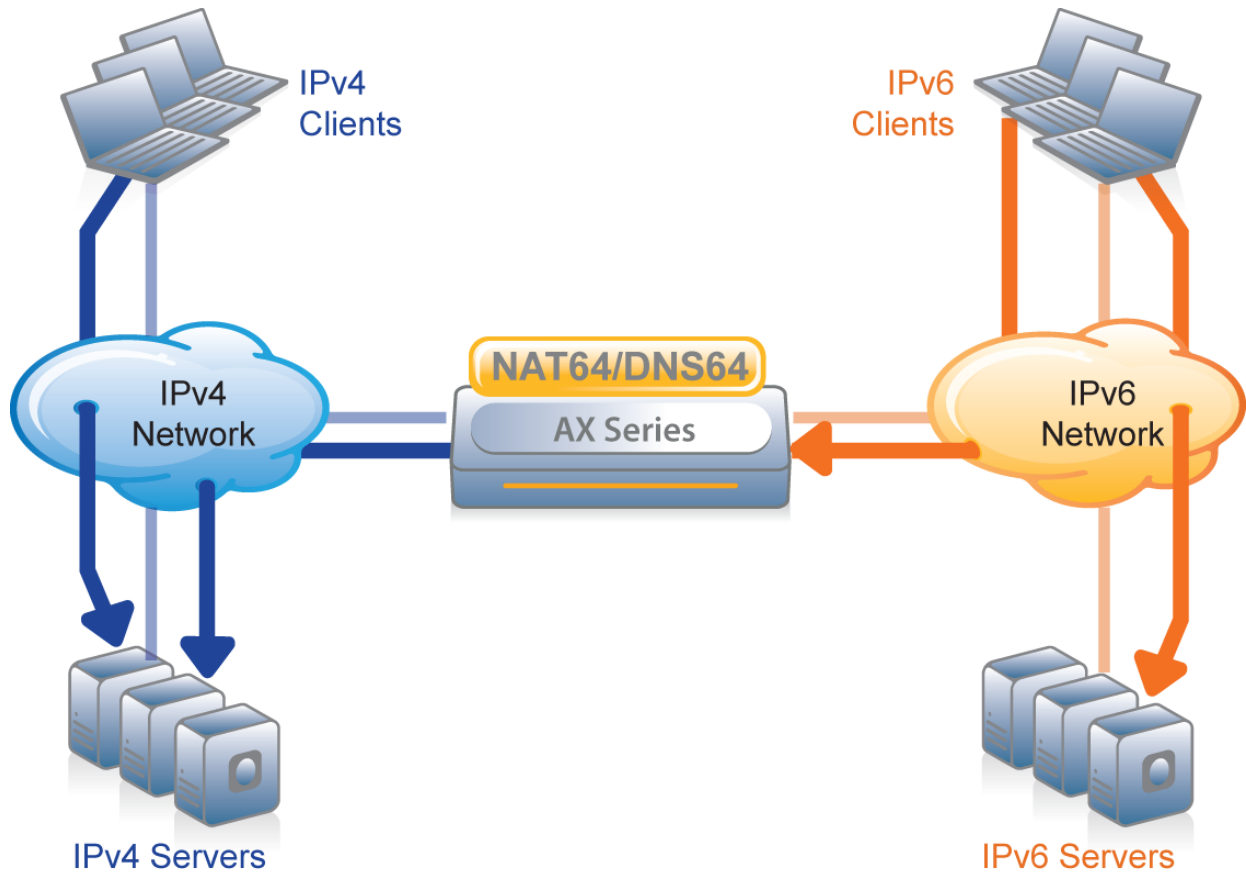


Figure 8: Service Provider NAT64 and DNS64 solution

Pros:

- Offers IPv6 clients access to IPv4 content.
- No disruption to IPv4 infrastructure.

Cons:

- No solution for IPv4 clients accessing IPv6 content.
- For stateful NAT, the NAT64 device must maintain a table with each active flow, requiring more resource usage.

NAT64/DNS64 device requirements

- NAT64 and DNS64 support
- High scalability for:
 - New connections per second
 - Concurrent connections
 - Throughput
 - Packets per second

- High availability with:
 - No service downtime (stateful transition failover)
 - Rapid failover
 - Flexible tracking (not based simply on remote device and interface)

Technical Note:

DNS64 uses the following standard:

- [RFC 6147 - DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers](#)

NAT64 uses the following standard:

- [RFC 6146 - Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers](#)

5. Content Provider and Enterprise transition to IPv6

One of the main roles of Content Providers and most Enterprises is to provide application access to end-users (customers or employees).

5.1. Content Provider and Enterprise challenges

End-users are today mostly IPv4 clients, but new operating systems (such as Microsoft Windows 7) can support IPv6 natively, and new applications, such as Microsoft DirectAccess, are being developed with IPv6.

Also, Service Providers either are deploying or are considering deploying, IPv6 networks, creating a need for Content Providers and Enterprises to offer services and applications on both IPv4 and IPv6 networks.

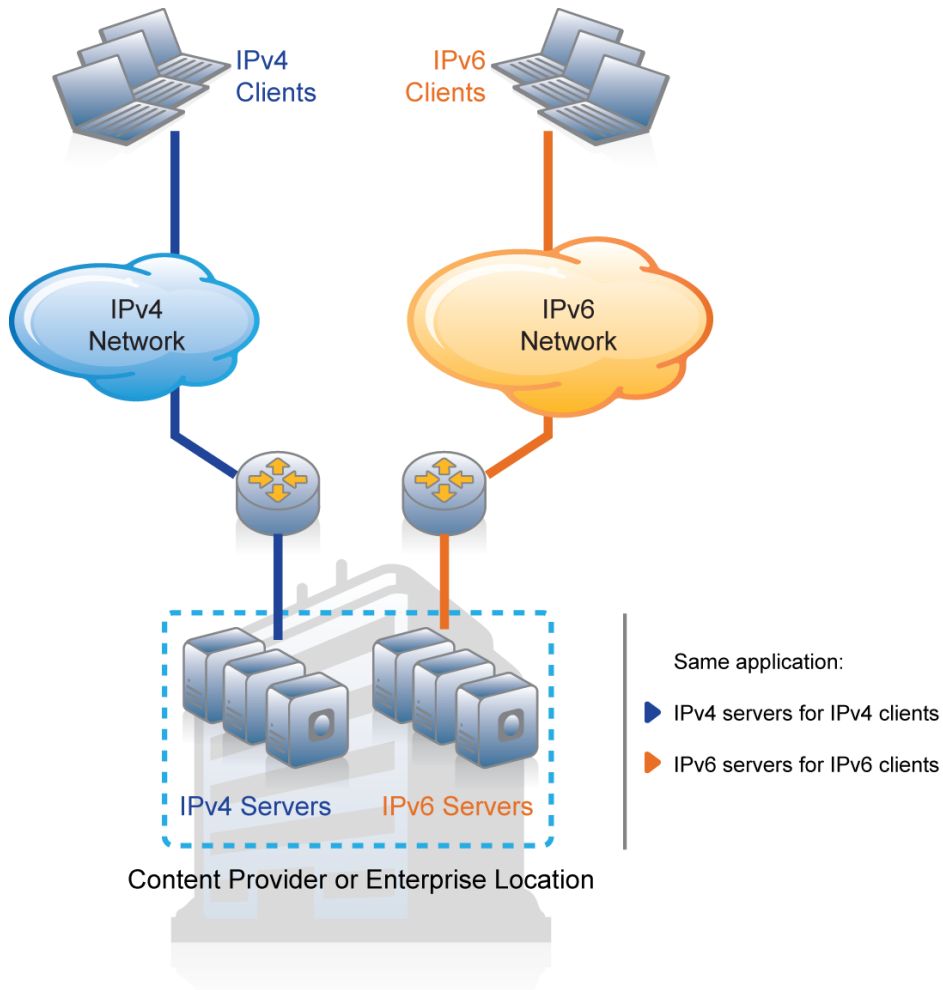


Figure 9: Content Provider or Enterprise with IPv4 and IPv6 networks

This simple approach has significant challenges and inconveniences:

- Twice the infrastructure and twice the number of servers must be supported.
- Existing IPv4 applications must be altered to support IPv6.
- Each application must be maintained and supported for both IPv4 and IPv6.

Note: If all Service Providers offered NAT64 and DNS64 services (see NAT64 and DNS64 section), Content Providers and Enterprises would not need to offer their services on IPv6. But very few offer NAT64 and DNS64 services. Additionally, most do not provide visibility when they offer it.

5.2. Content Provider and Enterprise solutions

5.2.1. Server Load Balancing with Protocol Translation (SLB-PT)

SLB-PT is used by Content Providers and Enterprises to provide content access to both IPv4 and IPv6 end-users, without the need to change the servers; they can keep running IPv4 or IPv6.

In addition, SLB-PT provides all the services provided by load balancers, including:

- Load balancing between multiple services; servers can be all IPv4, all IPv6, or a mix of both. For example, an SLB-PT device can facilitate an IPv4 client retrieving content from an IPv6 server behind it, or vice versa.
- Server and service high availability.
- Service acceleration with functions such as SSL Offload and HTTP Compression.

SLB-PT technical walkthrough

End-users resolve the names of the services they want to reach through a DNS server, which provides the client with IPv4 or IPv6 addresses, as is typical. These IPv4 or IPv6 addresses are configured as a Virtual IP (VIP) address on the front end of the SLB-PT device. The SLB-PT device converts the IP protocol to IPv4 or IPv6 as needed in order to communicate with the back-end servers. Return traffic is similarly translated to IPv4 or IPv6 as needed by the requesting client. This protocol translation is transparent and unknown to the end-user client.

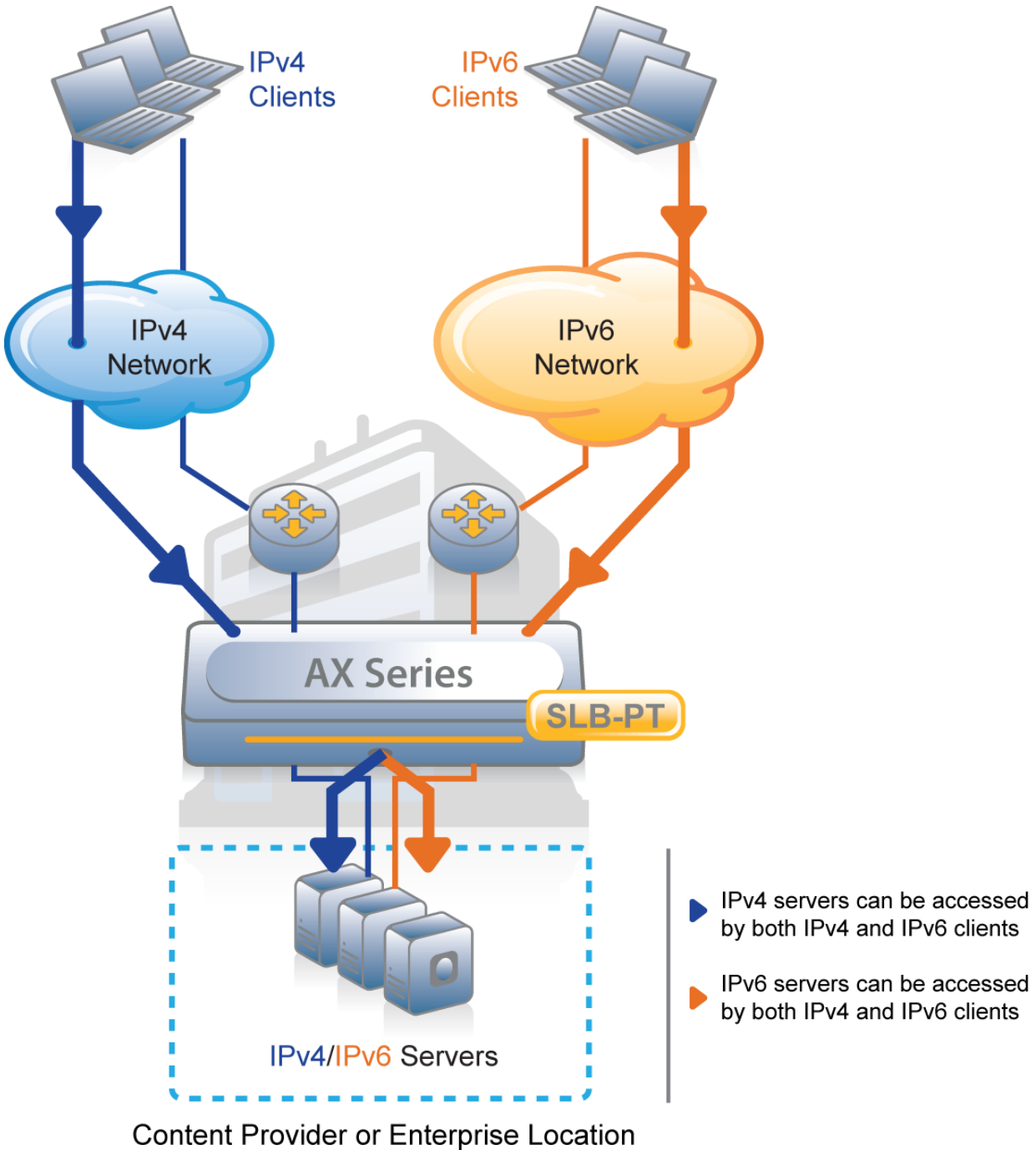


Figure 10: Content Provider and Enterprise SLB-PT solution allowing access to IPv4 or IPv6 resources

<p>Pros:</p> <ul style="list-style-type: none">• Reduced number of servers. Same servers are used for both IPv4 and IPv6 clients.• No need to migrate existing IPv4 applications to IPv6.• No need to downgrade new IPv6 applications to IPv4.• Fast path to providing IPv6 content.• Load balancing services.	<p>Cons:</p> <ul style="list-style-type: none">• Loses client IP address information when protocol translation is done. (This limitation does not apply to web traffic.)• Additional processing overhead for server load balancer/application delivery controller.• Stateful NAT requires SLB-PT device to maintain a table with each active flow, requiring more resource usage.
---	--

SLB-PT device requirements

- SLB-PT support (bi-directional translation from IPv4 to IPv6 and IPv6 to IPv4)
- High scalability for:
 - New connections per second
 - Concurrent connections
 - Throughput
 - Packets per second
- High availability with:
 - No service downtime (stateful transition failover)
 - Rapid failover
 - Flexible tracking (not based simply on remote device and interface)

Technical Note:

There is no specific standard for SLB-PT. Instead, it leverages other RFCs that formalize translation from IPv4 to (and from) IPv6.

5.2.2. Network Address Translation with Port Translation (NAT-PT)

NAT-PT, although deprecated for some time, was used by Content Providers and Enterprises to provide content access to both IPv4 and IPv6 end users, without the need to make changes to the IPv4 or IPv6 servers. However, this solution does not provide the extra load balancing services offered by SLB-PT.

NAT-PT, when used in combination with DNS-PT, offered automatic IPv4 name resolution for IPv6 servers and automatic IPv6 name resolution for IPv4 servers.

NAT-PT + DNS-PT technical walkthrough

If DNS-PT is used, the IPv4 and IPv6 end-user's DNS requests are received by the DNS-PT device, which resolves the domain name requests to an IP address. The server's IP address is forwarded to the end-user, if they both use the same IP version. The NAT-PT device's address is forwarded to the end-user instead, if the server and end-user use different IP versions.

The NAT-PT device receives traffic only from end-users attempting to access servers on a different IP version.

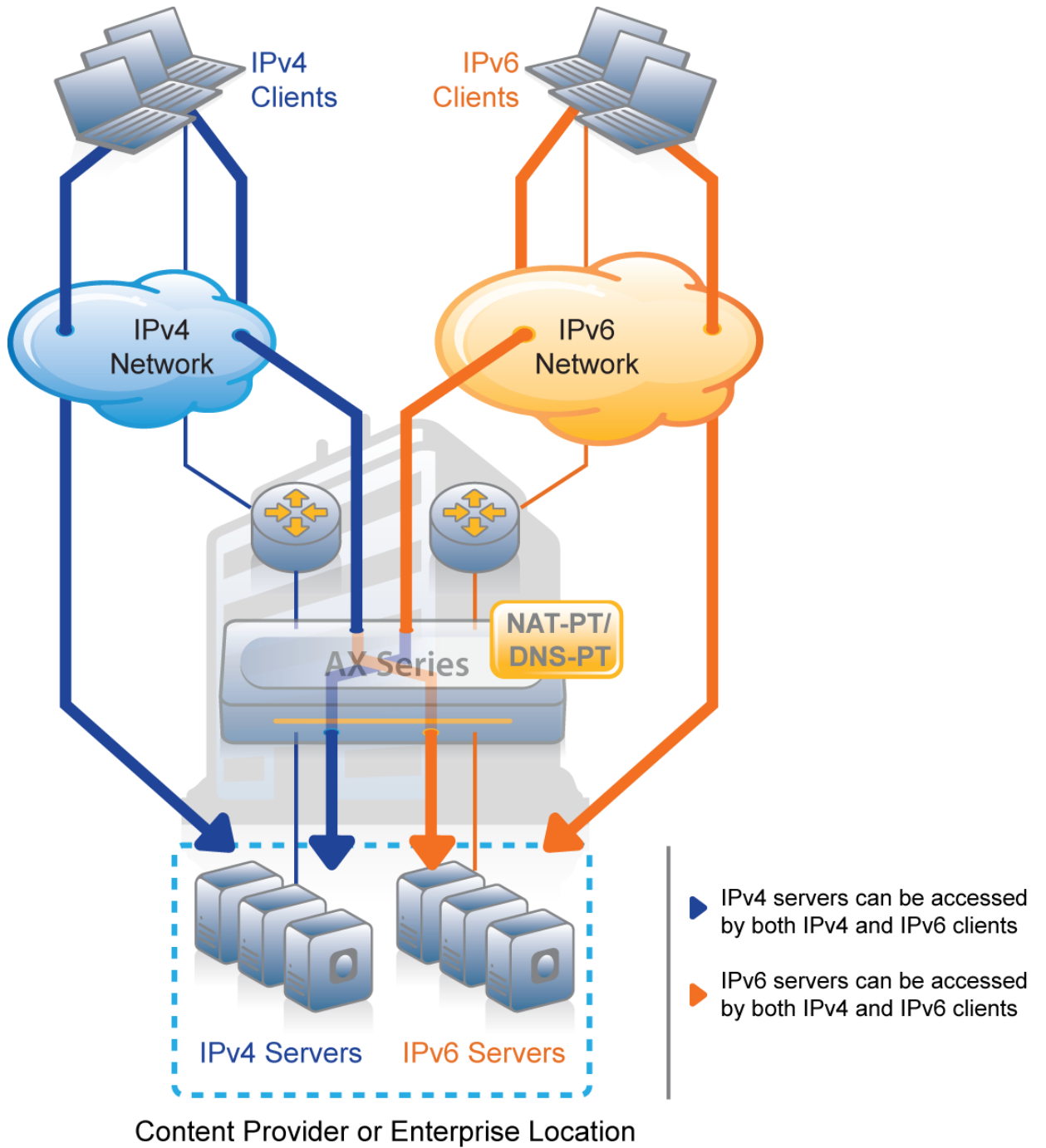


Figure 11: Content Provider and Enterprise NAT-PT and DNS-PT solution allowing access to IPv4 or IPv6 resources

Pros:	Cons:
<ul style="list-style-type: none">• Reduced number of servers. The same servers are used for both IPv4 and IPv6 clients.• No need to migrate existing IPv4 applications to IPv6.• No need to downgrade new IPv6 applications to IPv4.• Fast path to providing IPv6 content.	<ul style="list-style-type: none">• Loses client IP address information when protocol translation is done.• Additional processing overhead for server load balancer/application delivery controller.• For stateful NAT, the SLB-PT device must maintain a table with each active flow, requiring more resource usage.• No load balancing services.

NAT-PT and DNS-PT device requirements

- NAT-PT support (bi-directional translation from IPv4 to IPv6 and IPv6 to IPv4)
- High scalability for:
 - New connections per second
 - Concurrent connections
 - Throughput
 - Packets per second
- High availability with:
 - No service downtime (stateful transition failover)
 - Rapid failover
 - Flexible tracking (not based simply on remote device and interface)

Technical Note:

NAT-PT uses the following standard for encapsulation:

- RFC 2766, Network Address Translation - Protocol Translation (NAT-PT)

Note: RFC 4966 moved RFC 2766 to historical status.

There is no specific standard for DNS-PT.

6. Why select A10 to help you to migrate to IPv6?

6.1. *High performance*

Service Providers, Content Providers and Enterprises already process gigabits per second (Gbps) of traffic and millions of concurrent connections. History has shown that scalability requirements only increase.

A10's AX Series Carrier Class Advanced Traffic Managers are specifically built for processor-intensive high volume networking tasks, including NAT, and already can scale to hundreds of Gbps of throughput and hundreds of millions of concurrent sessions. All this is accomplished with a minimal footprint; for example, this can be done in a 1-RU AX device.

6.2. *Flexible solution*

Service Providers, Content Providers and Enterprises have different technical solutions available to migrate seamlessly to IPv6 networks. There also are new technical solutions still being proposed, such as Stateful NAT64, LightWeight 4over6 (LW6o4) , and LISP.

Unlike other fixed solutions, the AX Series offers a highly flexible and high-performance solution based on the combination of its Advanced Core Operating System (ACOS) and purpose-built, carrier-grade hardware. This flexible architecture enables A10 to respond to current and future technology requirements for IPv6 migration. AX Series' high scalability also allows the same appliance to provide Interplay between multiple services; for example, to run DS-Lite, CGN and NAT64/DNS64 concurrently. Finally, A10 updates its existing versatile appliances to aptly respond to emerging IPv6 standards without requiring a physical upgrade.

6.3. *Value added*

Sooner or later, Service Providers, Content Providers and Enterprises will be compelled to migrate to IPv6. But this migration implies a lot of challenges to maintain services for existing IPv4 end-users. Challenges include items such as management of large numbers both of IPv4 and IPv6 IP addresses, and security for new end-users with public IPv6 addresses.

A10 offers various management and security services in addition to migration to IPv6.

7. Summary and Conclusion

IPv6 migration has long been delayed due to the complexities of migrating large numbers of users, devices and applications to the new IPv6 protocol. The inevitable complete exhaustion of new IPv4 addresses presents a serious call to action.

The numerous methods available for extending the life of the IPv4 address space present viable short-term solutions; however, they merely provide a brief stop gap before the inevitable. The advent of multiple evolving IPv6/IPv4 co-habitation and translation technologies allows organizations to select viable alternatives to the infeasible overnight wholesale switch from IPv4 to IPv6.

IPv6 solutions were already predicted to be a major issue when A10 Networks was formed in late 2004. In response, A10 Networks focused on early leadership. Highlights include:

- Support for native IPv6 (management and traffic handling) in 2007 – at no additional charge.
- Deployment by Hikari-TV, the first large-scale IPTV-over-IPv6 service, in 2008.
- Frequent participation in IPv6-related NANOG and IETF events.
- Support for DS-Lite and LSN in 2009.
- In 2009, the AX Series ran live traffic to support IPv4-to-IPv6 translation for the Interop Tokyo ShowNet. Live 40-Gbps throughput demonstrations were conducted for IPv4 SLB and IPv6 SLB during the exhibition. This resulted in the AX Series receiving Best of Show awards.
- In a 2012 Network World Clear Choice Test, A10 received the highest rating in a comparative review of ADC vendors for IPv6 migration capabilities. The AX Series achieved maximum scores in each category. This test was performed in a real-world hands-on test.
- In 2012, A10 received the Best of Show award at Interop Tokyo for showcasing multiple IPv4 preservation and IPv6 migration methods simultaneously, demonstrating the power of Interplay.

The AX Series offers a seamless migration to IPv6 for Service Providers, Content Providers and Enterprises, with a wide range of options. In pace with emerging standards for IPv6, the AX Series offers current and future compatibility in the highest performance and most cost effective solution.

For more information about AX Series products, please see:

http://www.a10networks.com/products/axseries-IPv6_migration.php

<http://a10networks.com/products/axseries.php>

<http://a10networks.com/resources/solutionsheets.php>

<http://a10networks.com/resources/casestudies.php>

Appendix – IPv6 benefits overview

IPv6 provides a large number of advantages that will benefit all end-users and organizations. The most important of these are the following:

- IP addresses abundance
- Efficiency
- Security
- Simplicity
- QoS

IP addresses abundance

The total number of IPv6 addresses available actually would be enough to provide an IPv6 address to every single object that exists today; not just computers, kitchen appliances, cars, and any other electronic devices but also non-electronic devices such as pens, books, cups, dentures, and so on.

Note: For more on the emerging concept of interconnected everyday objects, the “Internet of Things”, see http://en.wikipedia.org/wiki/Internet_of_Things.

There are just above 4 billion IP addresses available in IPv4 ($2^{32} = 4,294,967,296$).

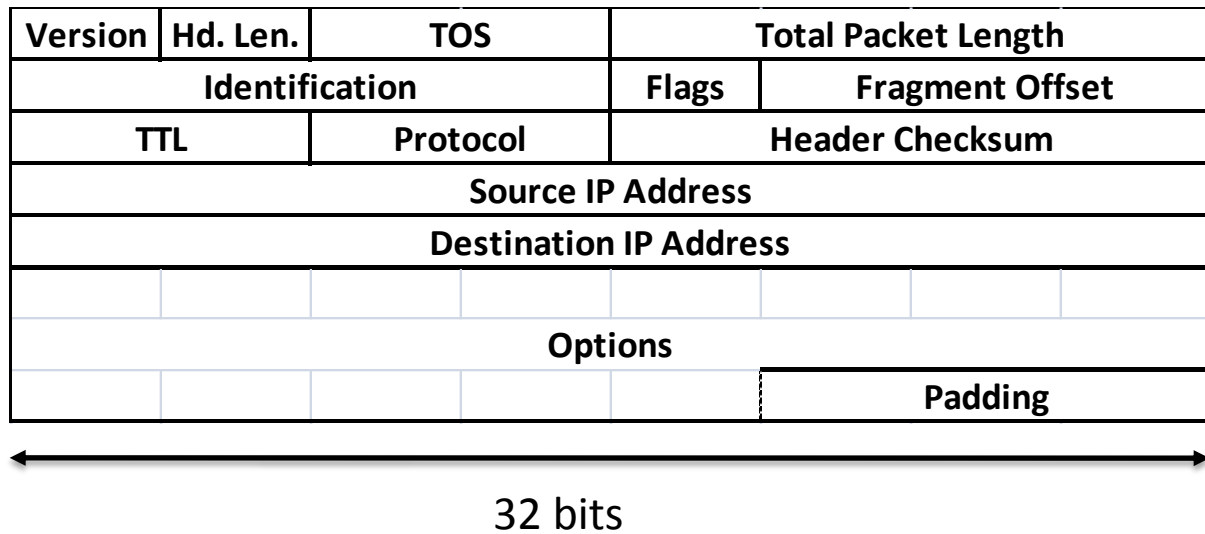


Figure 12: IPv4 address header

In contrast, there are above 3×10^{38} IP addresses available in IPv6 ($2^{128} = 340,282,366,920,938,463,463,374,607,431,768,211,456$).

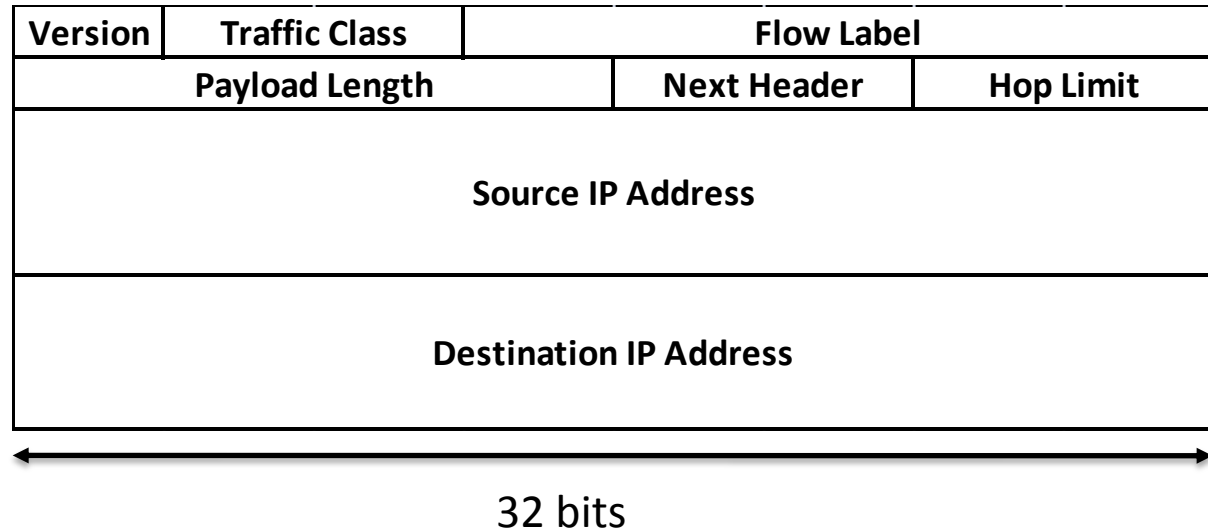


Figure 13: IPv6 address header

Efficiency

IPv6 is designed to allow routers and other devices to process IPv6 traffic very efficiently. Here are some examples:

- The IPv6 header is streamlined for efficiency. IPv6-relevant information is simply placed at specific offsets in the packet header.
- IPv6 does not use traditional IP broadcasts (transmission of packets to all hosts on an attached link using a special broadcast address). IPv6 instead uses more efficient multicast addresses.

Security

Private communication over a public medium such as the Internet requires secured services that protect the data from being viewed or modified while in transit. Although an IPv4 standard exists for providing security for data packets (known as *Internet Protocol Security*, or *IPsec*), this standard is only optional, and proprietary solutions are prevalent.

IPsec forms an integral part of the base protocol suite in IPv6. This standards-based solution offers built-in security for devices, applications and services, and promotes interoperability among different IPv6 implementations.

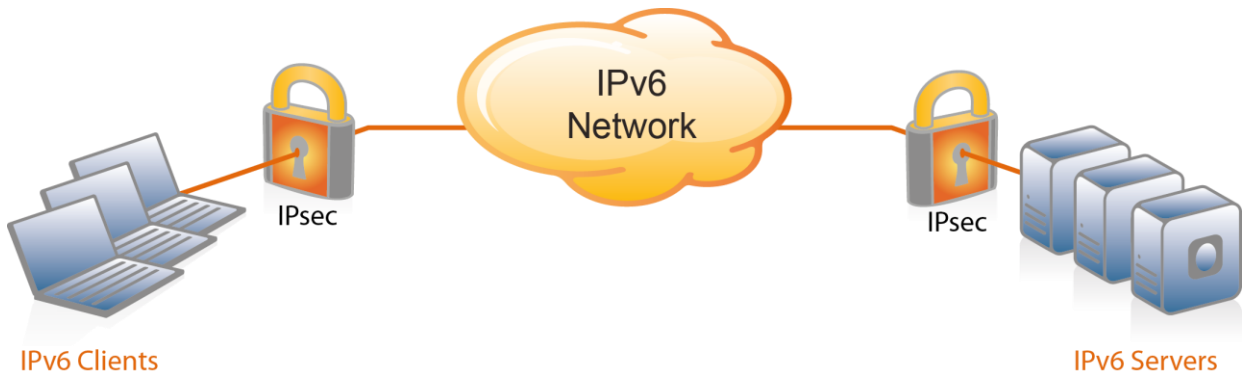


Figure 14: Built-in IPsec support in IPv6

Simplicity

IPv6 design allows a lot of simplification in applications and management. Here are some examples:

- NAT works perfectly for client-server applications such as Web browsing or email. But NAT does not always work well with client-to-client applications such as peer-to-peer applications, and often requires complex workarounds. IPv6 and its very large number of IP addresses eliminates the need for NAT and its many compatibility requirements for applications to function properly.
- IPv6 also supports stateless address auto-configuration to allow an end device to automatically configure its IPv6 address without human intervention.

Quality of Service

New fields in the IPv6 header define how traffic is handled and identified. Traffic identification using a Flow Label field in the IPv6 header allows routers to identify and provide special handling for packets belonging to a given flow (a series of packets between a source and destination). Because the traffic is identified in the IPv6 header, support for QoS is an integral part of the IPv6 protocol.