Whitepaper | AX Series

The End of IPv4?

Migration paths to IPv6

August 2010

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.

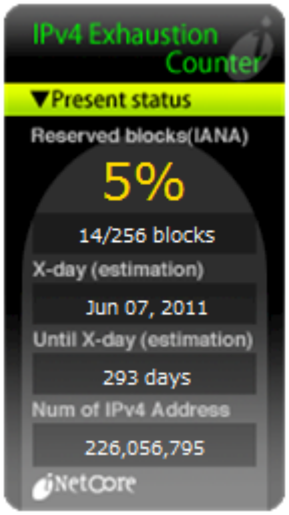
Copyright

Table of Contents

1. The end of IPv4?

For at least 10 years experts have been predicting exhaustion of the assignable IPv4 address space. The timeline for this prediction has never been exact, but an accelerated reduction in the IPv4 address space driven by sharp increase in demand is occurring.

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.


IPv4 Exhaustion Counter

▼Present status

Reserved blocks(IANA)

5%

14/256 blocks

X-day (estimation)

Jun 07, 2011

Until X-day (estimation)

293 days

Num of IPv4 Address

226,056,795

iNetCore

Figure 1: August 17, 2010 - IPv4 Exhaustion Counter developed by Takashi Arano, Intec Netcore to predict the date IPv4 addresses will no longer be available. (http://inetcore.com/project/ipv4ec/index_en.html)

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 versus IPv4.

Many vendors are offering support in network devices for both IPv6 management and IPv6 traffic handling on par with the equivalent IPv4 functionality.

However the transition from IPv4 to IPv6 cannot be achieved overnight. A total switch over is impractical due to the number of hosts and organizations involved with the Internet and associated systems.

Companies now realize that even with IPv6 implementation in their networks, there will still be a need to communicate with existing servers and applications on IPv4 networks.

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.

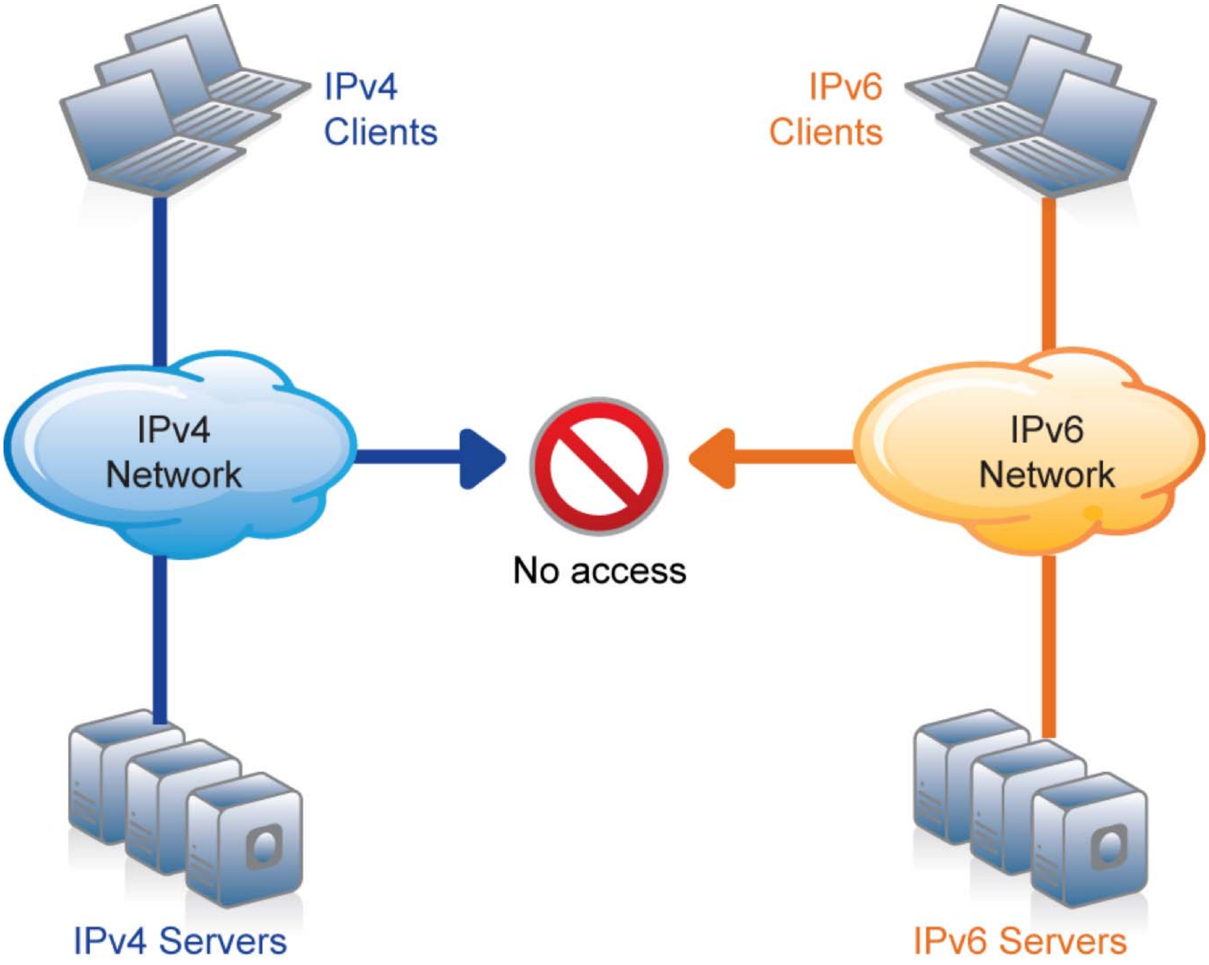


Figure 2: No built-in communication or backward compatibility between IPv4 and IPv6 networks

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 to the content provider. Realistically, all three will not 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 their timeframe for migrating to IPv6.

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

Service Providers – this includes Carriers, 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

Large waves of new customers registered to their services, with new devices such as smart phones and gaming devices, each requiring Internet access, means carriers, ISPs and mobile operators are the first ones to suffer from the negative consequences of IPv4 address exhaustion.

At the time this whitepaper is being written, IANA still has some IPv4 address blocks, but the number of available addresses is quickly dwindling (see Figure 1), making it ever more difficult for organizations to obtain new blocks of IPv4 addresses. With only very small blocks of new IP addresses assigned by IANA, providers may face the challenge of increased management overhead, or in the worst case scenario, the inability to provide new services.

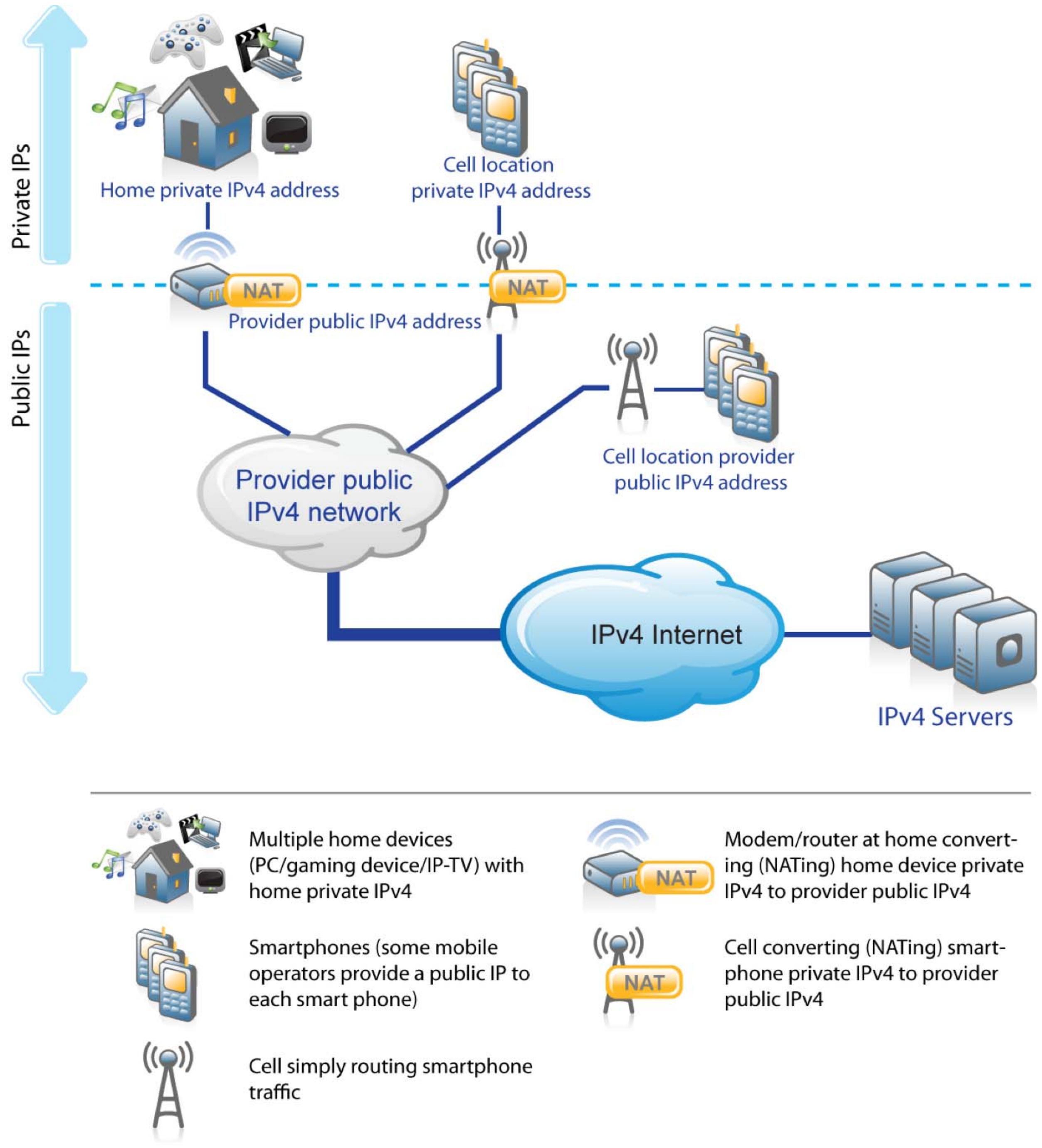

Private IPs
Public IPs
Home private IPv4 address
Cell location
private IPv4 address
NAT
NAT
Provider public IPv4 address
Cell location provider
public IPv4 address
Provider public
IPv4 network
IPv4 Internet
IPv4 Servers
Multiple home devices
(PC/gaming device/IP-TV) with
home private IPv4
Modem/router at home converting (NATing) home device private
IPv4 to provider public IPv4
Smartphones (some mobile
operators provide a public IP to
each smart phone)
Cell converting (NATing) smartphone private IPv4 to provider
public IPv4
Cell simply routing smartphone
traffic

Figure 3: 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 which are the following:

- Large Scale NAT (LSN)
- NAT444
- NAT444 + Tunnel (aka MPLS/VPN based NAT44/LSN)
- Dual-stack Lite (DS-Lite)
- IPv6 rapid deployment (6rd)
- NAT64 and DNS64

4.2.1. Large Scale NAT (LSN)

Large Scale NAT (LSN) is not a technology that in itself solves the IP address scarcity or offers IPv6 services. Instead, LSN is a standard for Network Address Translation (NAT) used by different solutions such as NAT444 and DS-Lite, which can offer additional IPv6 services.[1]

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

LSN formalizes NAT behaviors 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 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: NAT mapping is removed when all of an end user's sessions are terminated.

[1] LSN is formerly known as Carrier Grade NAT (CGN), but LSN has largely replaced the CGN nomenclature.

4.2.2. NAT444

NAT444 is used by Service Providers as a quick, temporary fix for IPv4 exhaustion, to buy time for the correctly 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, NAT444 illustrates the additional layer of NAT.

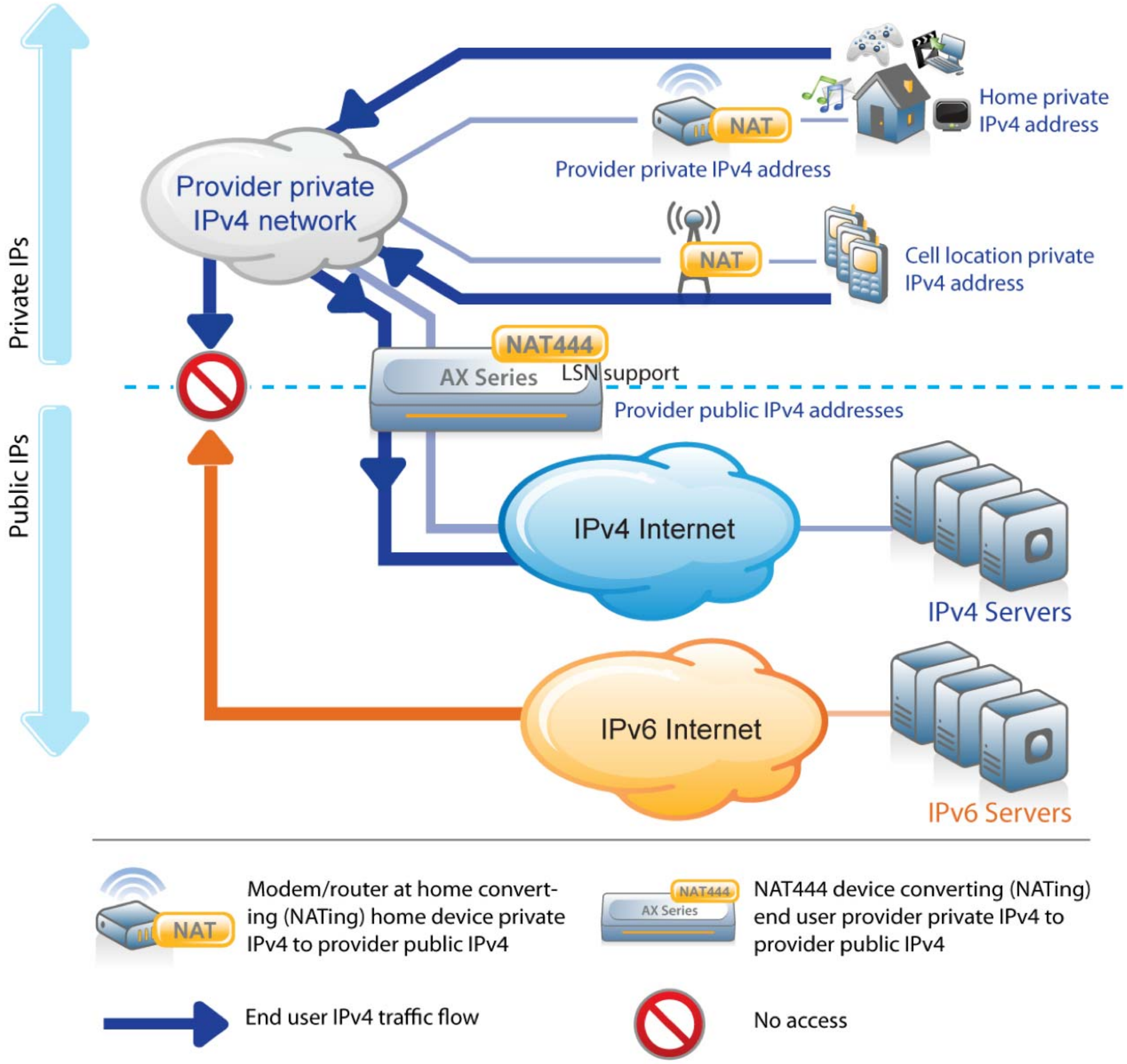

Private IPs
Public IPs
Provider private IPv4 network
NAT
Home private IPv4 address
Provider private IPv4 address
NAT
Cell location private IPv4 address
NAT444
AX Series
LSN support
Provider public IPv4 addresses
IPv4 Internet
IPv4 Servers
IPv6 Internet
IPv6 Servers
NAT
Modem/router at home converting (NATing) home device private IPv4 to provider public IPv4
NAT444
AX Series
NAT444 device converting (NATing) end user provider private IPv4 to provider public IPv4
End user IPv4 traffic flow
No access

Figure 4: Service Provider NAT444 solution

Pros:	**Cons:**
• 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.	• Extends time before migrating to IPv6, but IPv6 migration is still required. • Deployment complexity and conflict are created by the additional layer of NAT (many end users using the same public IP address). • Core infrastructure has no IPv6 benefits (such as efficiency, simplicity and security). • Stateful NAT – 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. • Issues reclaiming IPv4 addresses already statically assigned to users.

NAT444 device requirements

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

Technical Note:

NAT444 uses LSN standards:

- Draft-nishitani-cgn-02 - main RFC for LSN
- 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. NAT444 + tunnel (aka MPLS/VPN based NAT44/LSN)

This solution is also called MPLS/VPN based NAT44/LSN.

This solution is similar to NAT444 but with a couple of key differences. First is the ability for end locations to send their traffic to specific appliances via a tunnel (for example MPLS or VPN) where the second NAT44 (with LSN) is performed. Secondly for the provider, the use of tunnel based technology simplifies the private IPv4 address usage, reducing the total number of unique IPv4 private addresses needed for the first NAT44, while also isolating each host, which facilitates the ability to standardize the IP address.

This solution allows Service Providers to plan their transition to NAT444 and scale easily, sending users from specific cities or regions to specific NAT44 appliances.

But as NAT444 + tunnel is a quick, temporary fix for IPv4 exhaustion and does not offer any IPv6 services; it therefore does not provide any of IPv6's benefits.

NAT444 + tunnel technical walkthrough:

Service Providers provide a private IP address to their customer's router (first NAT IPv4 to IPv4). End users traffic is then sent (via a tunnel, for example MPLS or VPN) to a specific device that will provide the translation to a public IP address (second NAT IPv4 to IPv4). Different locations can send traffic to different devices for higher scalability of the solution.

Note: MPLS/VPN can start on the modem/router at home or afterwards. MPLS/VPN can end on the NAT444 device or before.

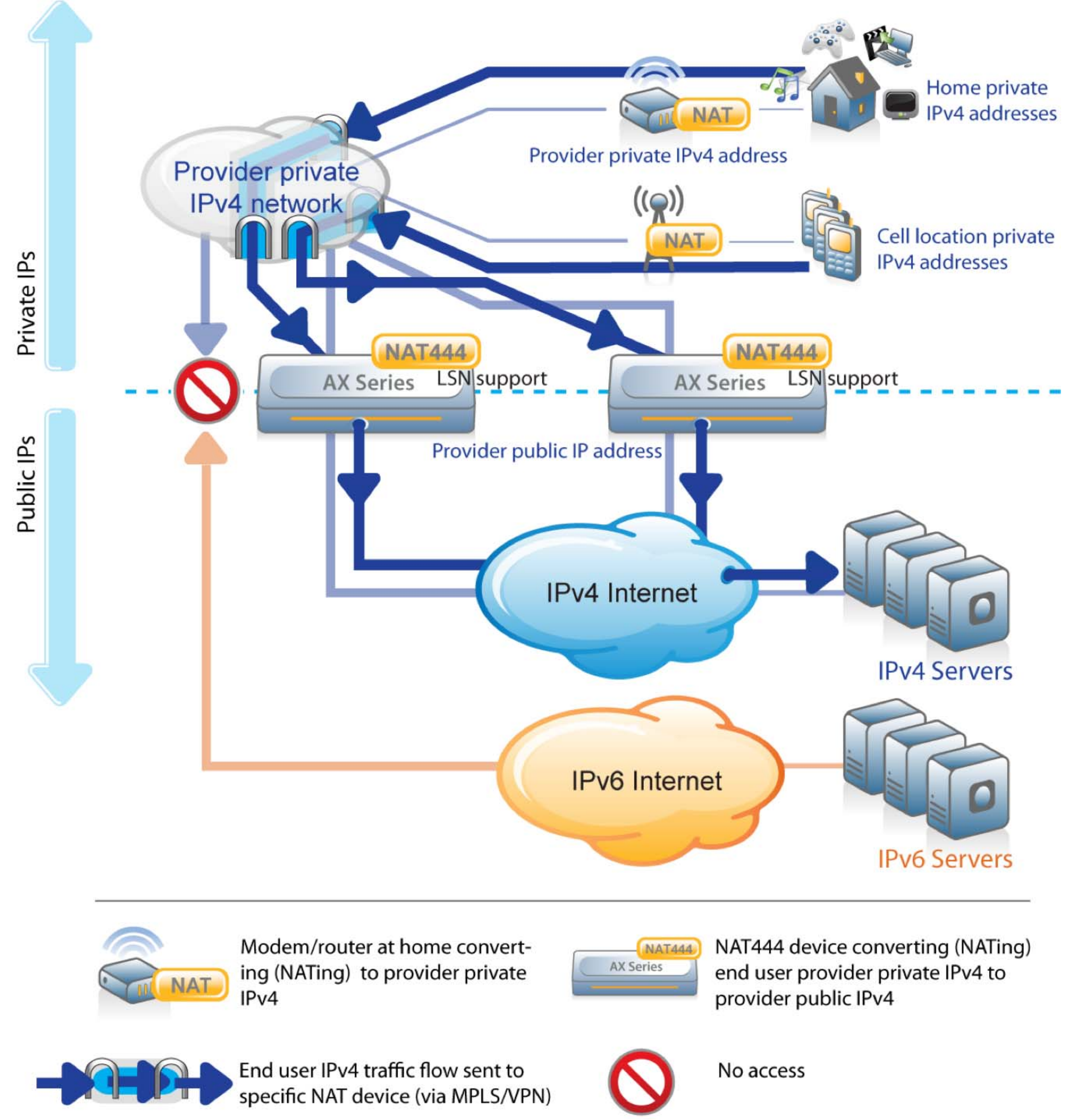

Private IPs
Public IPs
Provider private IPv4 network
NAT
Provider private IPv4 address
Home private IPv4 addresses
NAT
Cell location private IPv4 addresses
NAT444
AX Series
LSN support
NAT444
AX Series
LSN support
Provider public IP address
IPv4 Internet
IPv4 Servers
IPv6 Internet
IPv6 Servers
NAT
Modem/router at home converting (NATing) to provider private IPv4
NAT444
AX Series
NAT444 device converting (NATing) end user provider private IPv4 to provider public IPv4
End user IPv4 traffic flow sent to specific NAT device (via MPLS/VPN)
No access

Figure 5: Service Provider MPLS/VPN based NAT44/LSN solution

Pros:	**Cons:**
• Same as NAT444. • Easy to scale with large networks and large number of end users. • Tunnels enable greater control around private IPv4 addresses assigned on the external side of the home router/modem, reducing overall number of private IPv4 addresses required. • Reduces potential private IPv4 address conflicts and allows standardization. • Optimal LSN device selection via tunnel equipment.	• Same as NAT444. • Extra devices to provide tunnel.

NAT444 + tunnel device requirements

- LSN support
- High scalability for:
  - New connections per second
  - Concurrent connections
  - Throughput
  - Packets per seconds
- High availability for:
  - No service downtime (stateful transition failover)
  - Rapid failover
  - Flexible tracking (not simply remote device and interfaces)
- Tunnel – for example MPLS or VPN support
  Note: The tunnel can be done on a different device for higher flexibility and performance.

Technical Note:

MPLS/VPN based NAT44/LSN uses:

- Draft-kuarsingh-lsn-deployment-00 - NAT44/LSN Deployment Options and Experiences

Plus LSN standards:

- Draft-nishitani-cgn-02 - main RFC for LSN
- RFC 4787 - NAT behavioral requirements for unicast UDP
- RFC 5382 - NAT behavioral requirements for unicast TCP
- RFC 5508 - NAT behavioral requirements for unicast ICMP

4.2.4. Dual-stack Lite (DS-Lite)

DS-Lite is used by the Service Provider to resolve IPv4 exhaustion.

DS-Lite also provides additional benefits. Using an IPv6 core network, the Service Provider provides IPv6 content access to their end users 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 the IPv4 users to connect to the modem/router and access the 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 enabled device environment, the IPv6 end user's traffic is simply routed to the IPv6 resources with the regular IPv6 functionality on the device.

The DS-Lite feature itself encapsulates IPv4 end user traffic into IPv6 and sends it to another DS-Lite device, which de-encapsulates and NATs it with a public IPv4 address before routing it to the IPv4 resources.

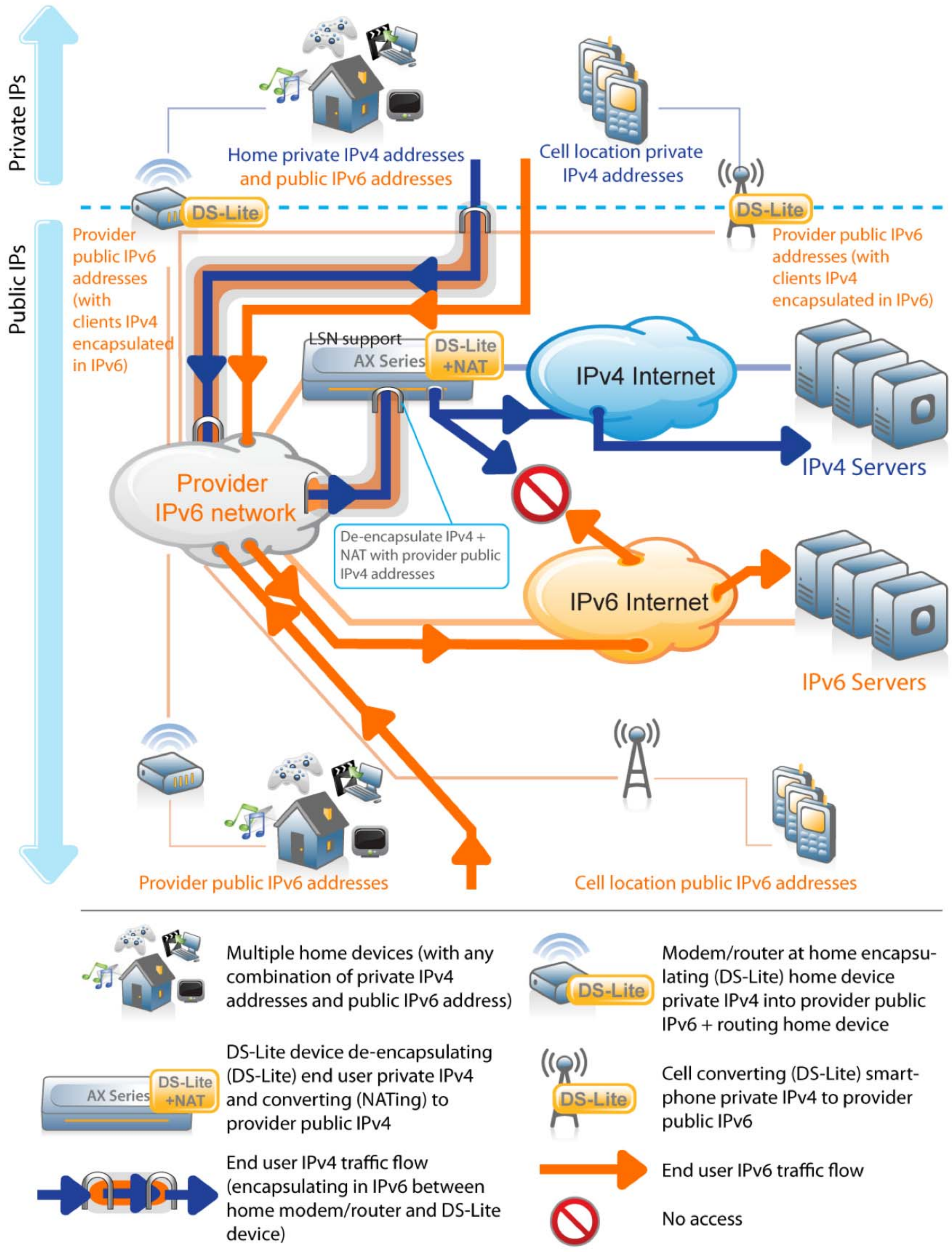

Private IPs
Public IPs
Home private IPv4 addresses and public IPv6 addresses
Cell location private IPv4 addresses
DS-Lite
DS-Lite
Provider public IPv6 addresses (with clients IPv4 encapsulated in IPv6)
Provider public IPv6 addresses (with clients IPv4 encapsulated in IPv6)
LSN support
AX Series
DS-Lite +NAT
IPv4 Internet
IPv4 Servers
Provider IPv6 network
De-encapsulate IPv4 + NAT with provider public IPv4 addresses
IPv6 Internet
IPv6 Servers
Provider public IPv6 addresses
Cell location public IPv6 addresses
Multiple home devices (with any combination of private IPv4 addresses and public IPv6 address)
DS-Lite
Modem/router at home encapsulating (DS-Lite) home device private IPv4 into provider public IPv6 + routing home device
AX Series
DS-Lite +NAT
DS-Lite device de-encapsulating (DS-Lite) end user private IPv4 and converting (NATing) to provider public IPv4
DS-Lite
Cell converting (DS-Lite) smartphone private IPv4 to provider public IPv6
End user IPv4 traffic flow (encapsulating in IPv6 between home modem/router and DS-Lite device)
End user IPv6 traffic flow
No access

Figure 6: Service Provider DS-Lite solution

Pros:	**Cons:**
• Resolves IP address scarcity. • 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 deployment. • Core infrastructure provides IPv6 benefits (efficiency, simplicity and security). • Clients are able to host IPv6 services such as web servers in their locations.	• No formal DS-Lite standard at present. • Requires a DS-Lite enabled device, for example a DS-Lite enabled router, at the end-user location that supports DS-Lite. • Stateful NAT – DS-Lite central device must maintain a table with each active flow, requiring more resource usage.

DS-Lite device requirements

- LSN support
- DS-Lite support
- DS-Lite compatibility with the router/modem/cellular equipment
- High scalability for:
  - New connections per second
  - Concurrent connections
  - Throughput
  - Packets per seconds
- 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 standard for encapsulation:

- Draft-ietf-softwire-dual-stack-lite-06 - Dual-Stack Lite Broadband Deployments Following IPv4 Exhaustion

Plus Large Scale NAT (LSN) standards for the NAT component:

- Draft-nishitani-cgn-02 - main RFC for LSN
- 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. IPv6 rapid deployment (6rd)

Using an existing IPv4 core network, IPv6 rapid deployment (6rd) is used by the Service Provider to provide IPv6 content access to their end users who are already on IPv6.

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 de-encapsulates it before routing it to the IPv6 resources.

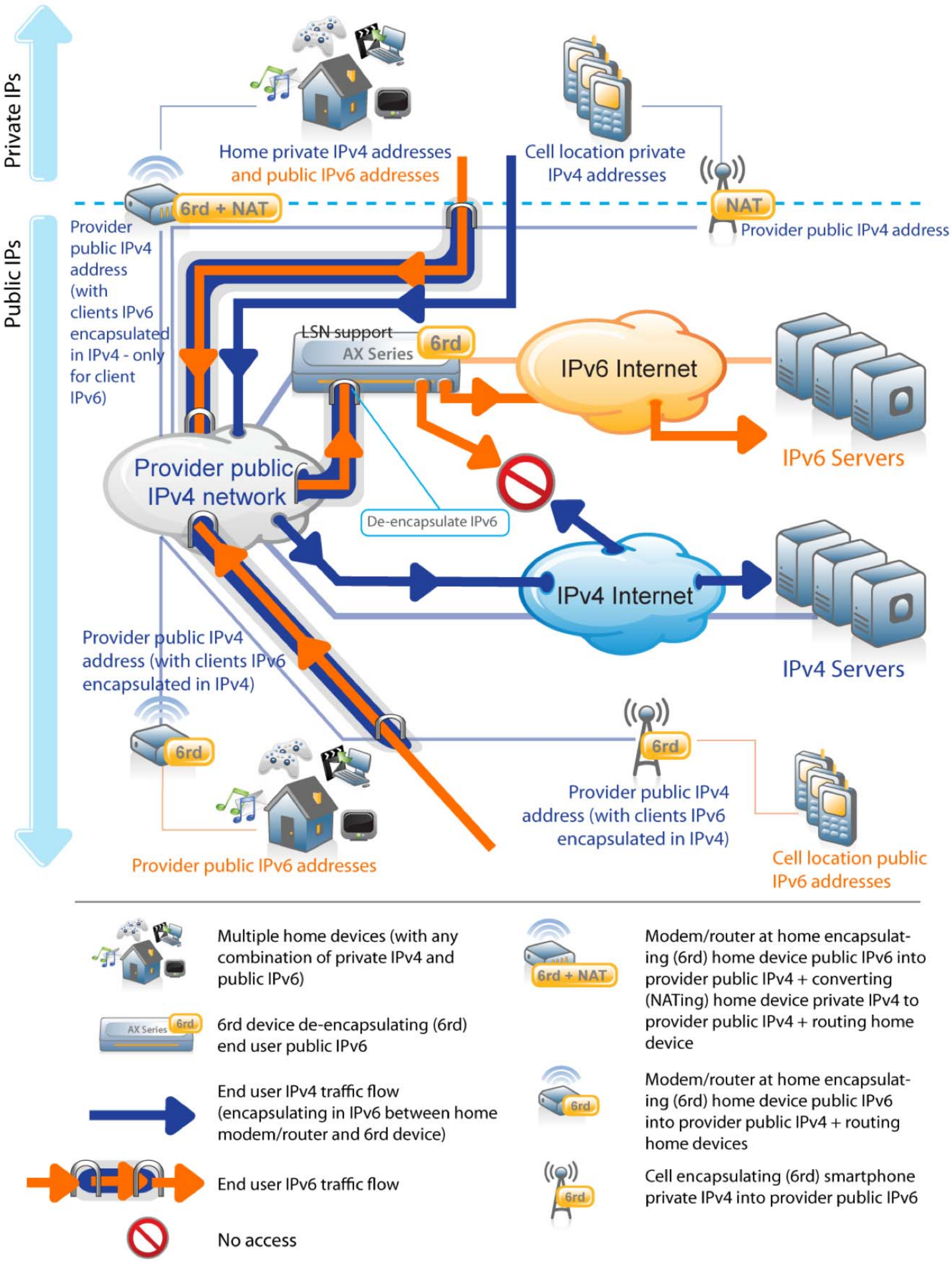

Private IPs
Public IPs
Home private IPv4 addresses
and public IPv6 addresses
Cell location private
IPv4 addresses
6rd + NAT
NAT
Provider public IPv4 address
Provider
public IPv4
address
(with
clients IPv6
encapsulated
in IPv4 - only
for client
IPv6)
LSN support
AX Series
6rd
IPv6 Internet
IPv6 Servers
Provider public
IPv4 network
De-encapsulate IPv6
IPv4 Internet
IPv4 Servers
Provider public IPv4
address (with clients IPv6
encapsulated in IPv4)
6rd
6rd
Provider public IPv4
address (with clients IPv6
encapsulated in IPv4)
Provider public IPv6 addresses
Cell location public
IPv6 addresses
Multiple home devices (with any combination of private IPv4 and public IPv6)
AX Series
6rd
6rd device de-encapsulating (6rd) end user public IPv6
End user IPv4 traffic flow (encapsulating in IPv6 between home modem/router and 6rd device)
End user IPv6 traffic flow
No access
6rd + NAT
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
Modem/router at home encapsulating (6rd) home device public IPv6 into provider public IPv4 + routing home devices
6rd
Cell encapsulating (6rd) smartphone private IPv4 into provider public IPv6

Figure 7: Service Provider IPv6 rapid deployment solution

Pros:	**Cons:**
• 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 needed. • Stateless NAT – 6rd central device does not need to maintain a table with active flows. This results in less resource usage.	• 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). • No formal 6rd standard yet. • Requires a 6rd enabled device, for example a 6rd enabled router, at the end-user location that supports 6rd. • IPv6 end users cannot host services in their locations, such as web servers.

6rd device requirements

- 6rd support
- 6rd compatibility with the router/modem/cellular equipment
- High scalability for:
  - New connections per second
  - Concurrent connections
  - Throughput
  - Packets per seconds
- 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:

- rfc5569 - IPv6 Rapid Deployment on IPv4 Infrastructures

Plus Large Scale NAT (LSN) standards for the NAT component:

- Draft-nishitani-cgn-02 - main RFC for LSN
- RFC 4787 – NAT behavioral requirements for unicast UDP
- RFC 5382 - NAT behavioral requirements for unicast TCP
- RFC 5508 - NAT behavioral requirements for unicast ICMP

4.2.6. NAT64 and DNS64

The majority of Internet content is currently available only on IPv4. While waiting for migration of content to IPv6, IPv6 end users also need a way to access these services on IPv4. NAT64 and DNS64 provide this service.

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

NAT64 and DNS64 are used by Service Providers in addition to other methods such as DS-Lite and 6rd to provide IPv4 content to IPv6 end users.

Note: NAT64/DNS64 is also 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.

If there is no IPv6 address but there is an IPv4 address (A record), 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 that NATs this traffic to the IPv4 server.

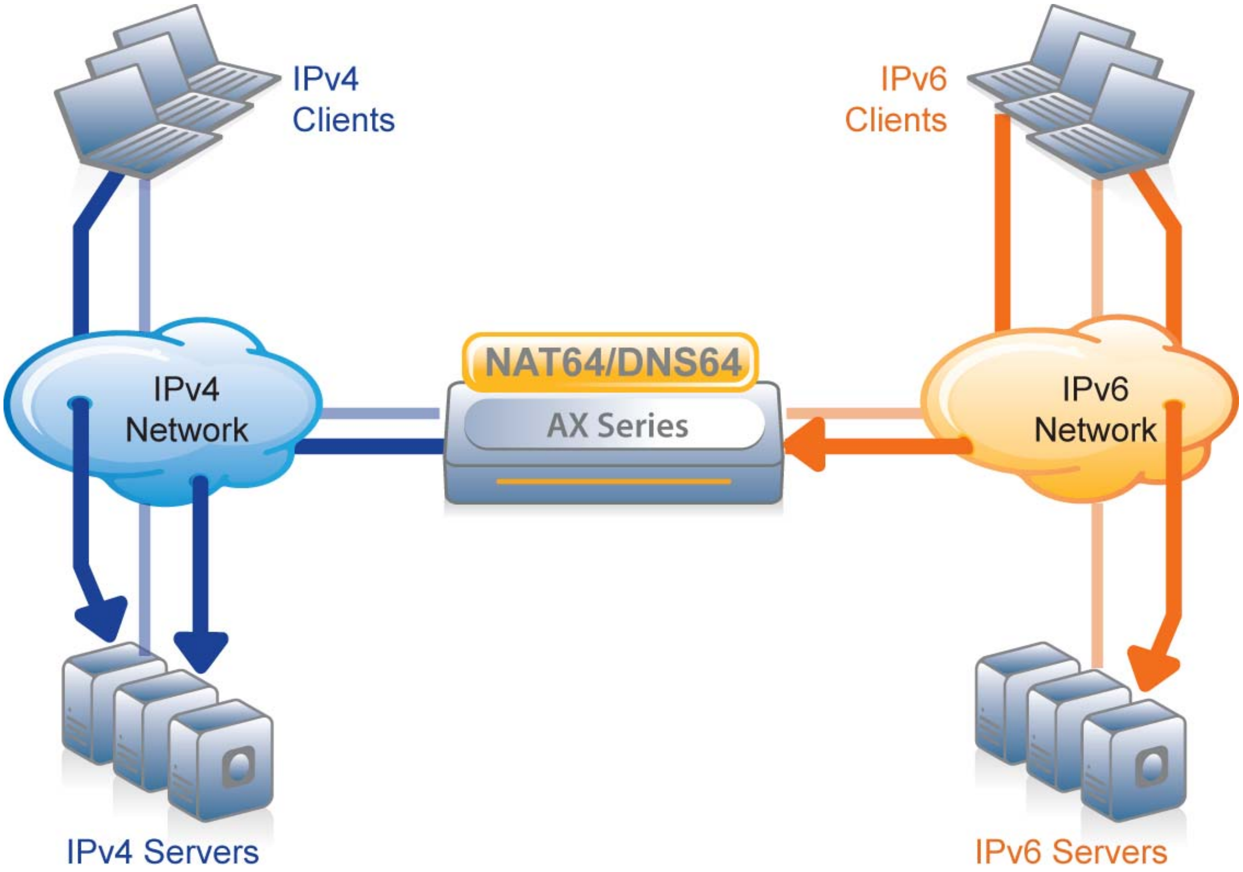


Figure 8: Service Provider NAT64 and DNS64 solution

Pros:	**Cons:**
• Offers IPv6 clients access to IPv4 content. • No disruption to IPv4 infrastructure.	• No solution for IPv4 clients accessing IPv6 content. • Stateful NAT – 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 seconds
- 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:

- Draft-ietf-behave-dns64-10 - DNS64: DNS extensions for Network Address Translation from IPv6 Clients to IPv4 Servers

NAT64 uses the following standard:

- Draft-ietf-behave-v6v4-xlate-stateful-12 - 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 and/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 now support IPv6 natively, and new applications are being developed with IPv6 (such as Microsoft DirectAccess).

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

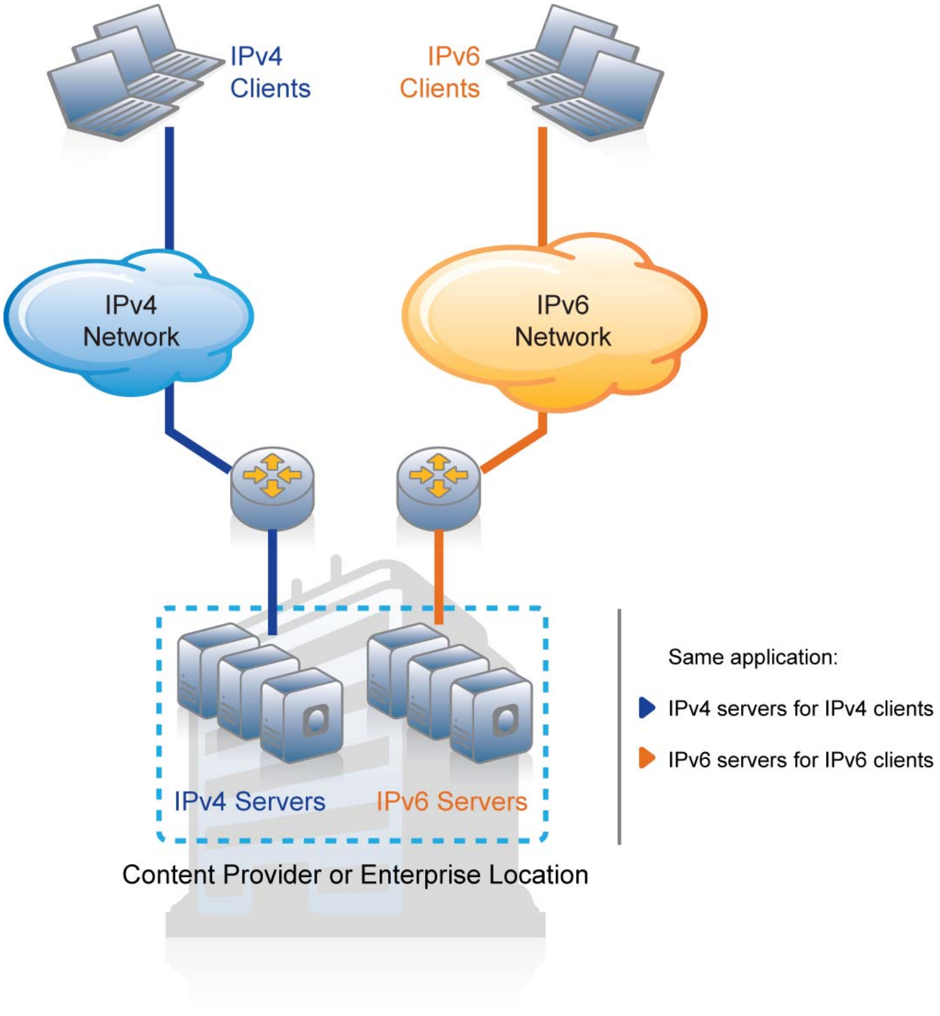

IPv4
Clients
IPv6
Clients
IPv4
Network
IPv6
Network
IPv4 Servers
IPv6 Servers
Content Provider or Enterprise Location
Same application:
IPv4 servers for IPv4 clients
IPv6 servers for IPv6 clients

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 earlier 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. SLB-PT – (Server Load Balancing with Port Translation)

SLB-PT is used by Content Providers and Enterprises to provide content access to both IPv4 and IPv6 end users, using the same IPv4 or IPv6 servers.

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

- Load balancing between multiple services; servers can be all IPv4, all IPv6, or both. For example an SLB-PT device will 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

Content Providers and Enterprises resolve the names of their services with IPv4 and IPv6 addresses. These IPv4 and IPv6 addresses are hosted on the same SLB-PT device, which forwards the IPv4 and IPv6 requests to the same servers, converting if needed to IPv4 or IPv6.

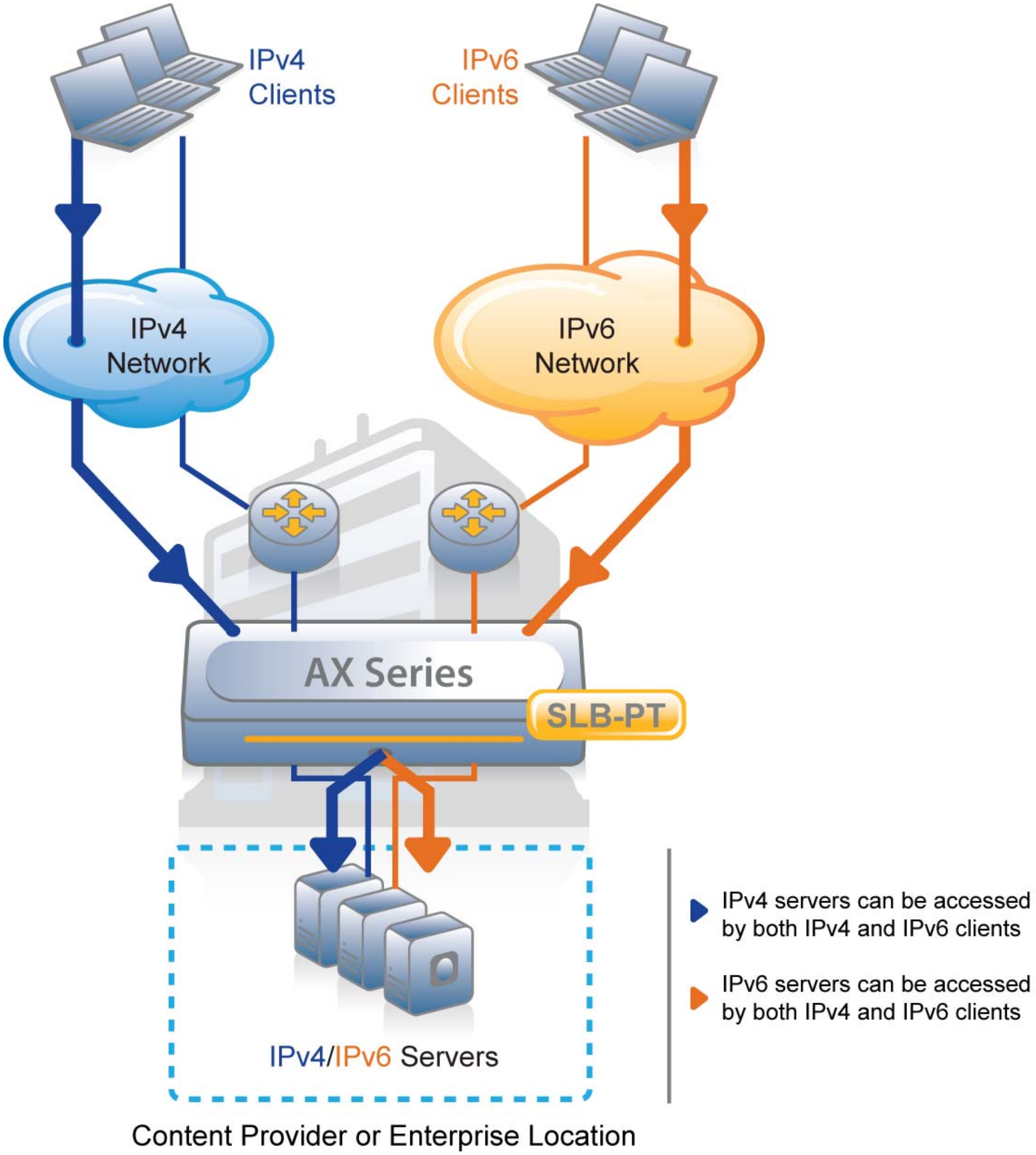

IPv4
Clients
IPv6
Clients
IPv4
Network
IPv6
Network
AX Series
SLB-PT
IPv4/IPv6 Servers
Content Provider or Enterprise Location
▶ IPv4 servers can be accessed by both IPv4 and IPv6 clients
▶ IPv6 servers can be accessed by both IPv4 and IPv6 clients

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

Pros:	**Cons:**
• 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.	• 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 – SLB-PT device must 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 seconds
- 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. NAT-PT – (Network Address Translation with Port Translation)

NAT-PT, although now deprecated, has been used for many years and is still used by some Content Providers and Enterprises.

NAT-PT is used by Content Providers and Enterprises to provide content access to both IPv4 and IPv6 end users, using the same IPv4 or IPv6 servers. But this solution does not provide the extra load balancing services offered by SLB-PT.

NAT-PT optionally can be combined with DNS-PT. DNS-PT offers 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 requests. The server IP address is forwarded to the end user if they both use the same IP version. The NAT-PT device address is forwarded to the end user if they use different IP versions.

The NAT-PT device receives only traffic from end users accessing servers in a different IP version.

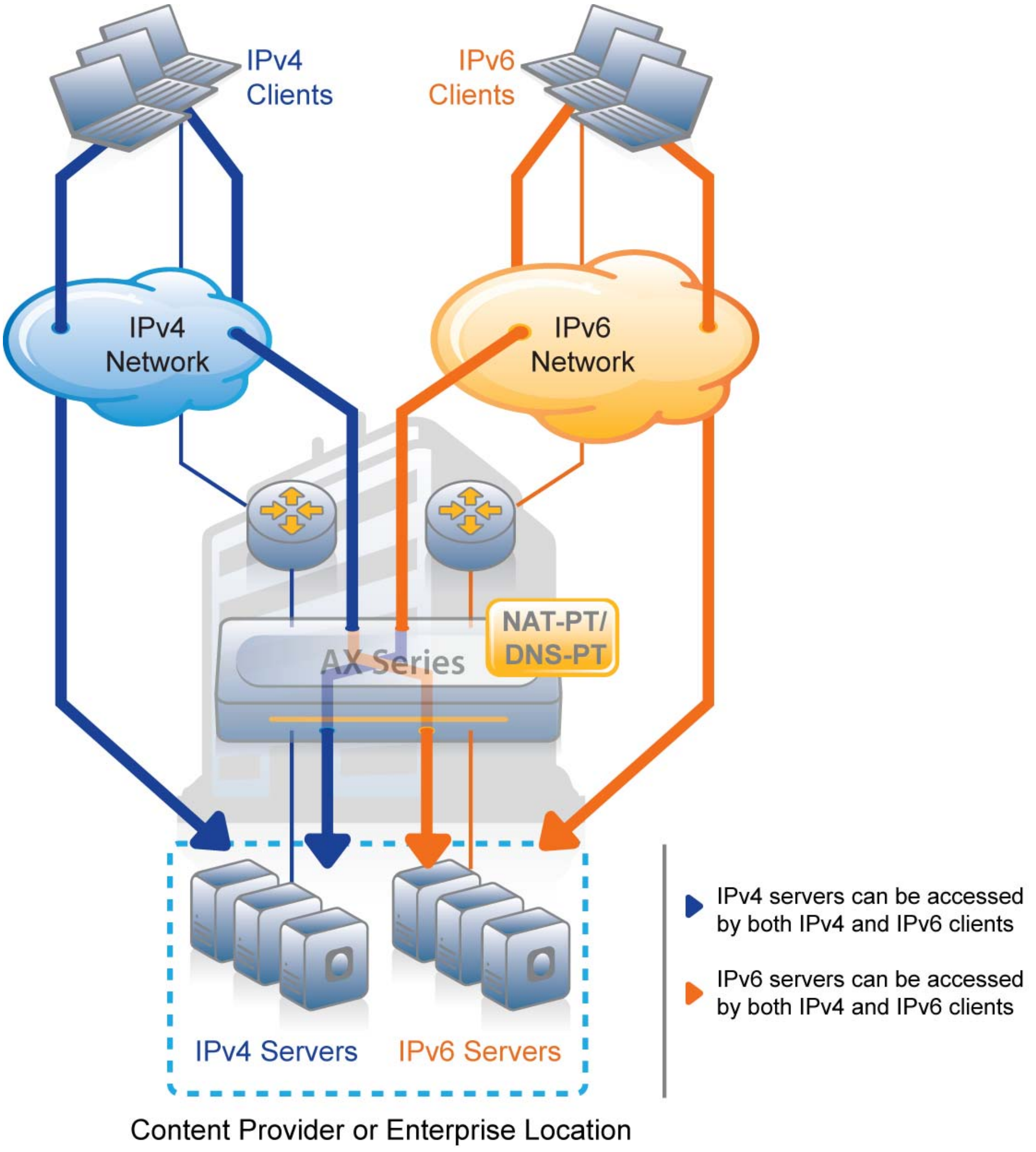

IPv4 Clients
IPv6 Clients
IPv4 Network
IPv6 Network
AX Series
NAT-PT/ DNS-PT
IPv4 Servers
IPv6 Servers
Content Provider or Enterprise Location
IPv4 servers can be accessed by both IPv4 and IPv6 clients
IPv6 servers can be accessed by both IPv4 and IPv6 clients

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

Pros:	**Cons:**
• 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.	• Loses client IP address information when protocol translation is done. • Additional processing overhead for server load balancer/application delivery controller. • Stateful NAT – 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 seconds
- 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 Gbps (gigabits per second) of traffic and millions of concurrent connections. History has shown that scalability needs 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 40 Gbps of throughput and hundreds of millions of sessions. All this is accomplished with a minimal footprint; for example, the AX 5200 appliance is only 2RU in size.

6.2. Flexible solution

Service Providers, Content Providers and Enterprises have different technical solutions available to migrate seamlessly to IPv6 networks. But it should be noted the techniques described in this document are not fully standardized as yet and are still evolving. There are also new technical solutions still being proposed, such as IVI, A+P, and LISP.

Unlike other fixed solutions, AX Series offers high flexibility with a solution based on the combination of its Advanced Core Operating System (ACOS) and field-programmable gate arrays (FPGA). This flexible architecture enables A10 to provide a high performance solution that responds to the current technology requirements for IPv6 migration. AX Series' high scalability also allows the same appliance to be utilized with multiple services such as DS-Lite and NAT64/DNS64. Finally, A10 updates its existing versatile appliances to reply to emerging IPv6 standards' deployment needs 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 in addition to maintaining services for existing IPv4 end users. Challenges include items such as management of both large numbers of IPv4 and IPv6 IP addresses, and security for new 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 countdown to impending exhaustion of IPv4 addresses presents a serious call to action.

The numerous methods 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 server load balancing (SLB) and IPv6 SLB during the exhibition. This resulted in the AX Series receiving Best of Show awards.

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://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 users and companies. The most important ones are:

- IP addresses abundance
- Efficiency
- Security
- Simplicity
- Quality of Service

IP addresses abundance

The total number of IPv6 addresses available would actually 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, 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).

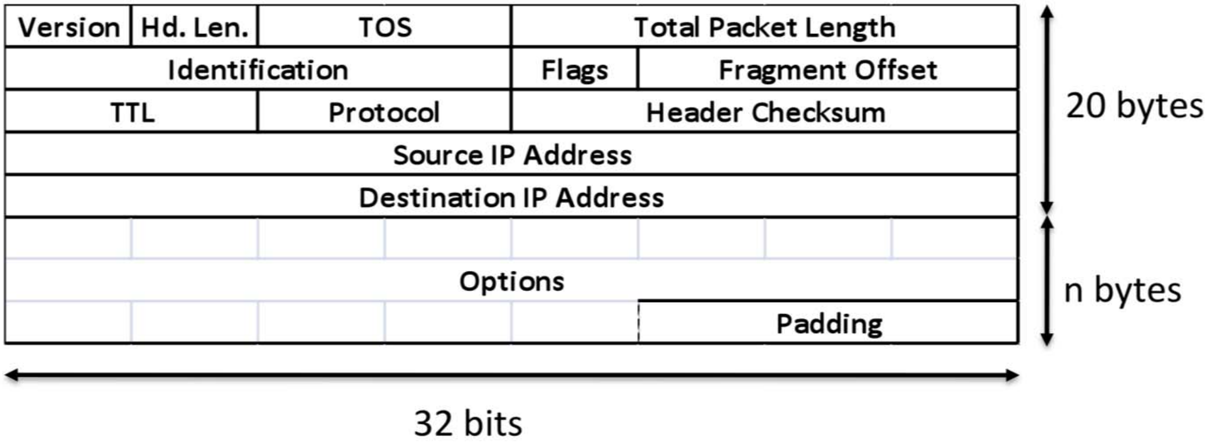


Figure 12: IPv4 address header

In contrast, there are above $3x10^{38}$ IP addresses available in IPv6 (2^128 = 340,282,366,920,938,463,463,374,607,431,768,211,456).

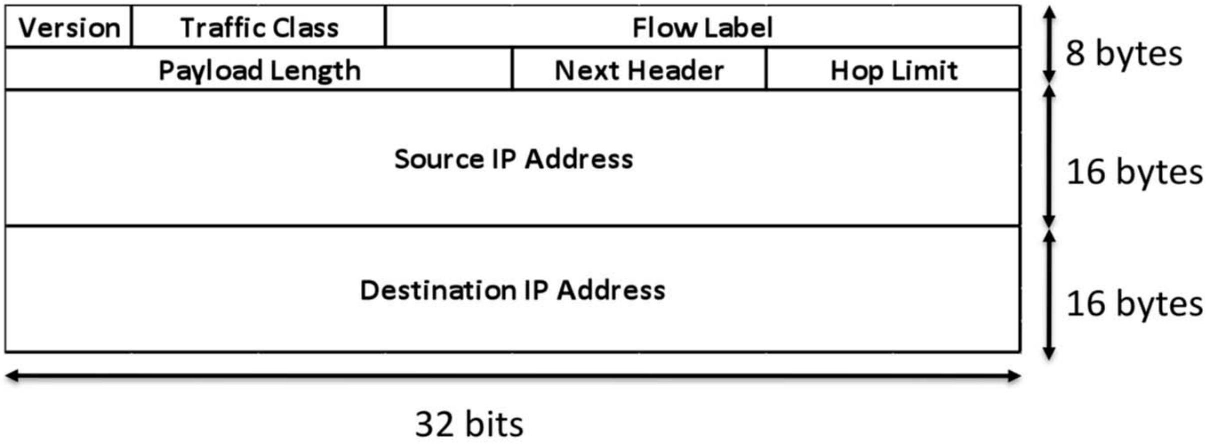


Figure 13: IPv6 address header

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; that is, the 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 like 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.

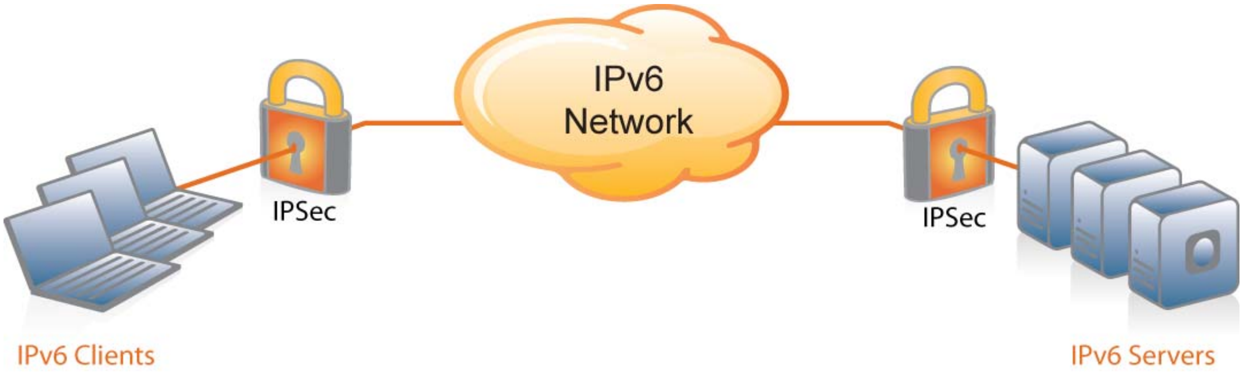


Figure 14: Built-in IPSec support in IPv6

Simplicity

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

- Network Address Translation (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 (QoS)

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 part and parcel of the IPv6 protocol.