EBOOK

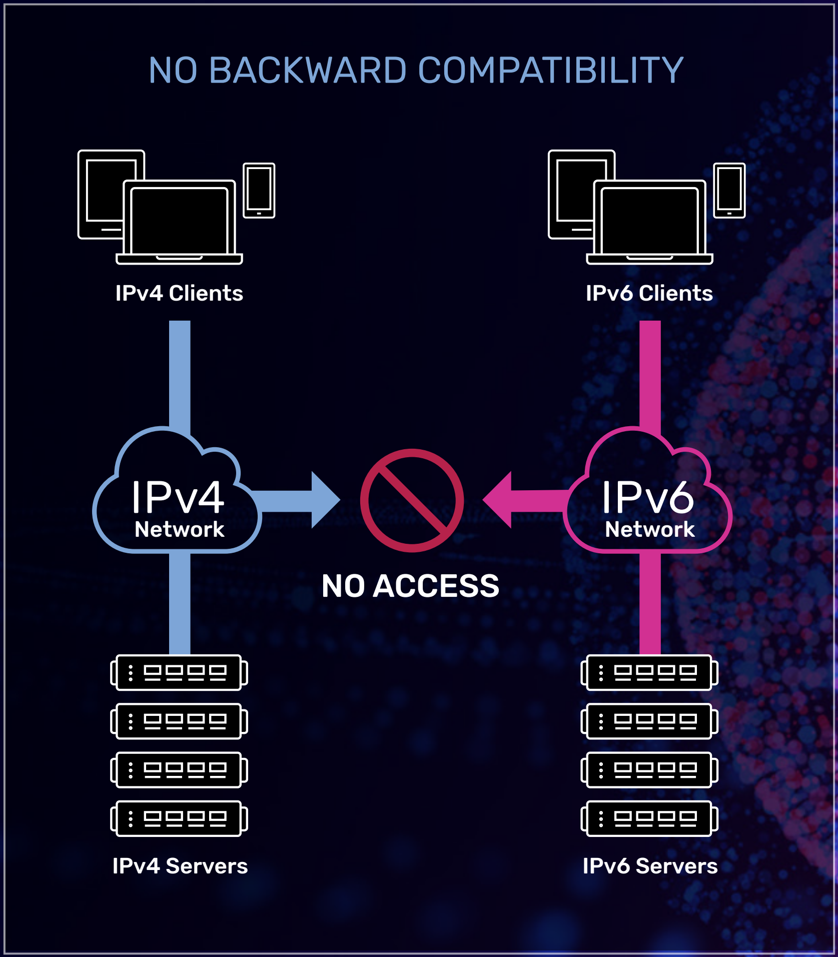
# IPv6 – Are We There Yet?

## How to Co-exist with IPv4 and IPv6 using CGNAT

# Table of Contents

# Your Guide to Managing IPv4 Exhaustion and IPv6 Adoption

IPv6 adoption won't be achieved overnight. While many vendors of enterprise and consumer electronics are offering support for IPv6 management and IPv6 traffic handling that is on par with IPv4 network functionality, a total switchover in the near future is impractical due to the number of hosts and organizations involved with the internet and associated systems. 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, not all three of these links in the IPv6 chain will transition to IPv6 at the same time. As a result, even companies with IPv6 implementation in their networks still need to communicate with legacy IPv4 servers and applications. On the other side of the equation, IPv4 customers need to be able use services developed with IPv6.



The need to support both IPv4 and IPv6 during this transition period is a complicating factor in a broad range of initiatives across the rapidly evolving communications landscape. As organizations move to the cloud, adopt 5G, implement multi-access edge computing (MEC) architectures, and work to support the explosive growth of the Internet of Things (IoT), they will need solutions compatible with both IPv4 and IPv6.

As organizations develop strategies for IPv6 adoption, multiple migration methods have been proposed or standardized. However, it's important to understand that the transition from IPv4 to IPv6 isn't a single event. It's a multi-step process that can involve a series of different methods along the way. Organizations should adopt a lifecycle strategy designed around their business context and the current status of their IPv6 adoption process.

This ebook provides an overview of the components available to support a lifecycle strategy for complete IPv4 – IPv6 migration for ISPs and other broadband service providers, mobile network operators, enterprises, and higher education institutions.

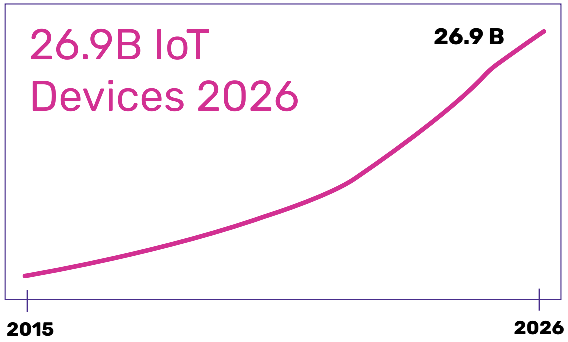
TABLE OF CONTENTS

# IPv4 Exhaustion

At the time of the internet's creation, the IPv4 standard was introduced to allow a unique public IP address to be assigned to each internet-connected computer. Encompassing nearly 4.3 billion different values, IPv4 seemed to be an ample supply at the time, but it soon became apparent that this pool would be depleted sooner rather than later. Indeed, as of November 25, 2019, the last Regional Internet Registry (RIR) made the final allocation from the last remaining addresses in its available IPv4 pool.

IPv4 exhaustion has arrived just as the demand for addresses has never been greater. The advent of new internet-connected locations, from hotels to planes and more worldwide, along with new internet-connected devices such as 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 Internet of Things is another key consideration helping to drive the growth of connected devices to over 26 billion by 2026 according to Ericsson. IPv6 for IoT will be critical to overcoming the constraints of IPv4 exhaustion, increasing the urgency to support IPv6 .

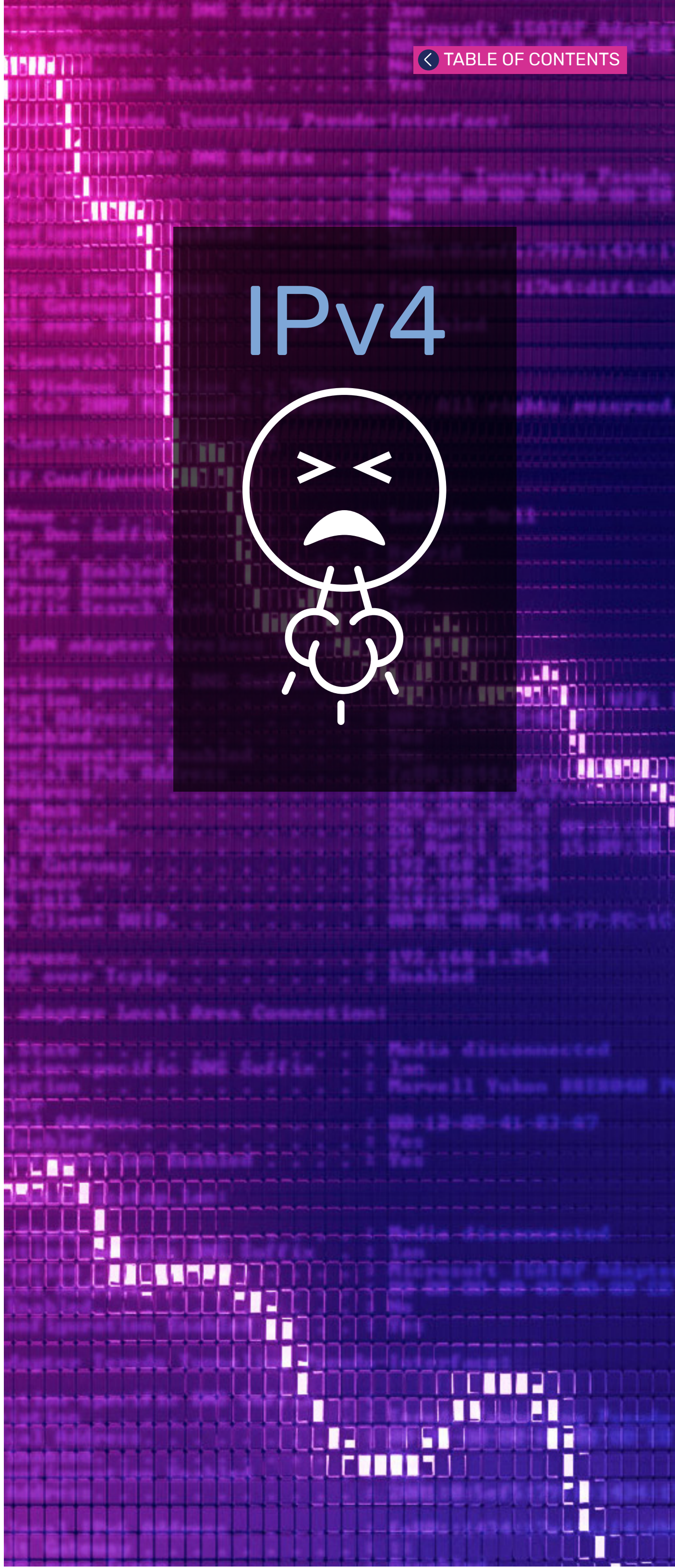
IPv6 promises to remove IP address scarcity by creating a new address space with vastly more potential addresses. IPv6 also provides many other benefits to service providers and end-users, such as improved efficiency, security, simplicity and Quality of Service (QoS) versus IPv4. But it has been over 20 years since IPv6 was introduced as a draft standard by the IETF, and IPv6 adoption remains very much a work in progress. Many, many organizations and users continue to use IPv4 now, and will continue to do so many years into the future.



## IoT Connections (billion)

| IoT | 2020 | 2026 | CAGR |
|---|---|---|---|
| Wide-area IoT | 1.9 | 6.3 | 22% |
| Cellular IoT | 1.7 | 5.9 | 23% |
| Short-range IoT | 10.7 | 20.6 | 12% |
| **Total** | **12.6** | **26.9** | **13%** |

Source: Ericsson Mobility Report, Nov. 2020



# IPv6 Adoption Status

There are several different elements of IPv6 adoption, and all three have to be in alignment on the same standard: content (websites), devices, and networks. Even if organizations have already converted their own infrastructure to IPv6, and most devices support IPv6, most content doesn't—so organizations will still have to provide connectivity for both IPv4 and IPv6.

## Content Remains Largely IPv4-based

However eager operators and organizations are to move forward with IPv6, their subscribers, employees, students, and other users still want to access IPv4-only sites. While high-traffic web destinations such as Google, Yahoo, Wikipedia, Facebook, Netflix and YouTube all support IPv6, at the end of 2020 only 17 percent of websites use IPv6, and globally, only about 32 percent of Google searches use IPv6.

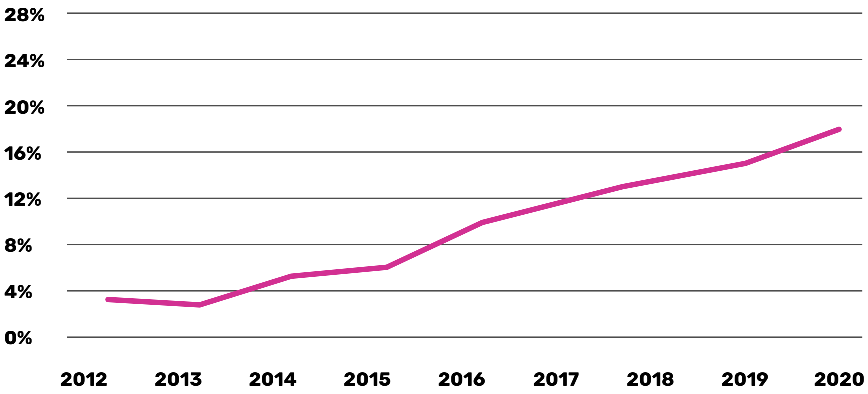
## Devices and Applications aren't Uniformly IPv6 Compatible

IPv6 support has been mandatory in both Android and iOS devices for years, but there are many older devices still connected. Old technologies do not replace new ones; they just overlap. For example, while newer mobile devices and laptops are IPv6 compatible, most 3G and all 2G devices are not. Consider that of the 8.8 billion mobile subscriptions forecast by 2026, 1.4 billion will still be 2G/3G devices, according to Ericsson. In addition, older applications and devices may not be IPv6 compatible. For example, some rural cable operators have postponed IPv6 due to incompatibility of home cable routers, where the cost to change out those devices is too high and the process too disruptive to subscribers.

## Networks have Seen Uneven IPv6 Adoption

Even for service providers that have moved to IPv6 within their networks, the transition is slow. Service providers, especially mobile network operators, expect significant cost benefits from simplifying their networks with IPv6. Top-tier mobile network operators have all aggressively changed to IPv6. Within the U.S., T-Mobile, Verizon, and AT&T have migrated over 70 percent of their traffic, while Reliance, Chunghwa, BT, and others in the global top 20 have migrated around 60 percent of their traffic. However, of the 351 service provider networks measured, only 100 had greater than 50 percent of their traffic on IPv6.

**% of Websites using IPv6**



> *"Each customer wants connectivity to many possible points, and even if 80% of the Internet traffic is over IPv6, nearly every customer will still have numerous IPv4-only sites that they wish to reach"*
>
> **John Curran** | *President and CEO, ARIN*
> North American IPv6 Summit 25 April 2017

## Roadblocks to IPv6 Adoption

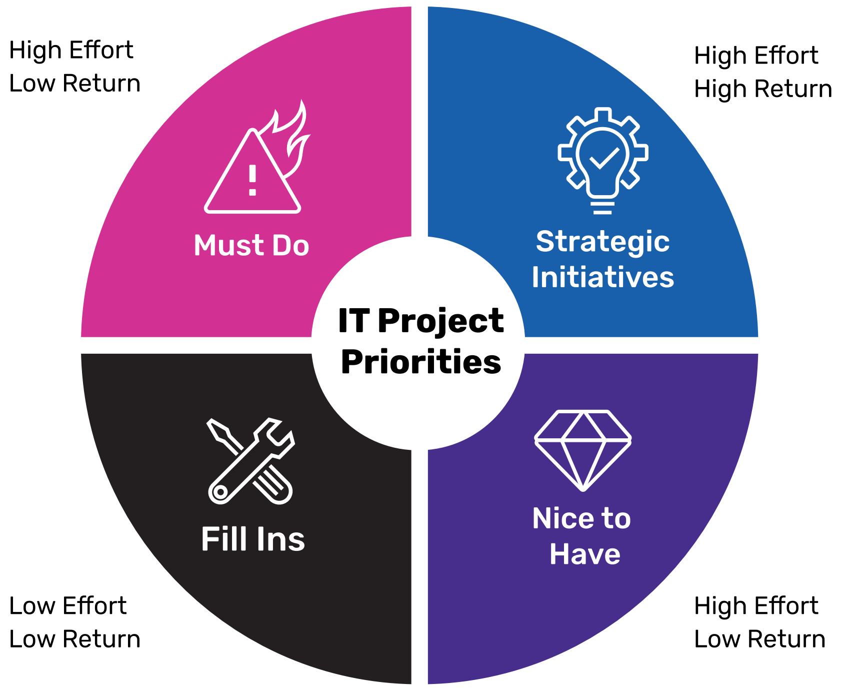
All organizations must balance rapidly increasing IPv6 devices and traffic volume against other network technology initiatives such as software-defined networking, cloud and edge cloud. Connected devices, including cellular IoT devices, are expected to exceed 26 billion by 2026, with most of the new devices likely being IPv6-compatible. As a result, most organizations have to manage a growing base of newer IPv6-enabled devices with older IPv4 devices connecting to both IPv4 and IPv6 content. The two environments will have to co-exist for some time, and both will need to accommodate the other technology transitions now underway.

## The Enterprise Dilemma

Many organizations simply can't always justify the near-term cost and disruption that a data center and network change-out to IPv6 will entail. Switching to IPv6 is costly and time-consuming. All connected devices must be inventoried and changed out or reconfigured. There is a risk that a needed device or application will not work and cause service disruption that will take time to troubleshoot and fix. IPv6 adoption also takes a great deal of detail-oriented effort by network administrators for testing and production; in some cases, they must re-architect entire networks. Balanced against the daily operational demands they face, as well as the need to move forward on strategic initiatives like 5G, cloud, virtualization, edge cloud, and others, IPv6 can be seen as a high-effort, low-return project.

Take the Department of Defense, for example. The DoD's mission requires considerable IP address space—in fact, its 300,149,760 current IPv4 addresses are the most of any organization in the world. The department relies on its current IPv4 networks for enterprise-wide and mission partner wired and wireless communications, including infrastructure, technologies, and devices supporting large-scale, globally dispersed command-and-control systems, naval vessels, aircraft, satellites, and ground operations.

Anticipating that it will exhaust its reserve of unused IPv4 addresses by 2030, the Department has already attempted twice to transition to IPv6 since 2003, only to abandon both efforts due to security concerns and lack of trained personnel. The department's current initiative has been underway since 2017. Even if it succeeds, the DoD expects to have to support IPv4 beyond 2030 due to mission system modernization and replacement timelines, as well as new emerging technologies that may require IPv4 resources while the department transitions to IPv6.



# What Is CGNAT?

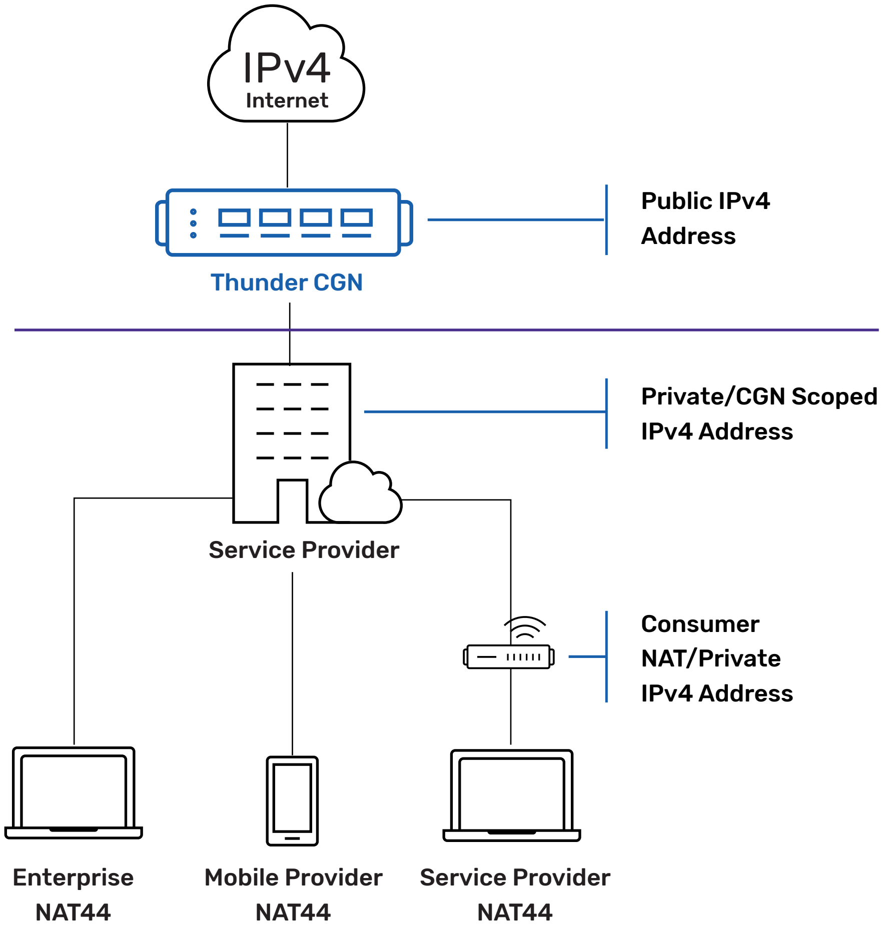
Carrier-grade NAT (CGNAT), also known as large-scale NAT (LSN), is a standard for network address translation (NAT) that helps organizations bridge the transition to IPv6. While CGNAT does not in itself solve the IPv4 exhaustion problem or offers IPv6 services, it can play a critical role in extending existing investment in IPv4 and in enabling the hybrid environment in which IPv4 and IPv6 currently co-exist. With CGNAT, organizations can share a single public IPv4 address with hundreds of subscribers.

Standard NAT enables a single public IPv4 address to be shared across the devices on a private network. CGNAT adds an additional translation layer that allows service providers to share their own public IPv4 addresses across the private IPv4 networks of multiple subscribers or businesses. Created to standardize NAT functions and behavior between network vendors, CGNAT 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** – Internal end-users can communicate directly when the destination endpoint is in the same subnetwork.
- **Endpoint independent mapping and filtering (EIM and EIF)** – Hosts on the inside of the NAT area gain "full-cone," transparent connectivity.

## CGNAT PRESERVES EXISTING IPV4 INVESTMENT



## NAT44 and NAT444 Extends IPv4 Investment

NAT 444 and NAT 44 are models implemented in CGNAT solutions to extend the utility of existing IPv4 addresses. With NAT444, service providers provide a private IP address to a customer's router (first NAT IPv4-to-IPv4). The translation to a public IP address is done further within their network (second NAT IPv4-to-IPv4). Traditional NAT used today, in contrast, can be referred to as NAT44.

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 and does not offer any IPv6 services or provide any of IPv6's benefits.

The advantages of NAT 444 include the ability to support more IPv4 subscribers with fewer IPv4 addresses. No upgrade or enhancement is required on home modems, routers, or cellular phones, and no core infrastructure support for IPv6 is needed. NAT 444 delivers efficiency through features such as hairpinning for eliminating unneeded connections and delay.

On the other hand, while NAT 444 extends the time before migrating to IPv6, it does not allow access to IPv6 content, and IPv6 migration will still ultimately be required. End-to-end connectivity is very complex, especially for IP telephony or file sharing services. The core infrastructure offers none of the benefits for efficiency, simplicity, and security available with IPv6. 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. Finally, governments mandate the capability to track internal-to-external IP associations for extended periods of time, requiring an extensive logging infrastructure.

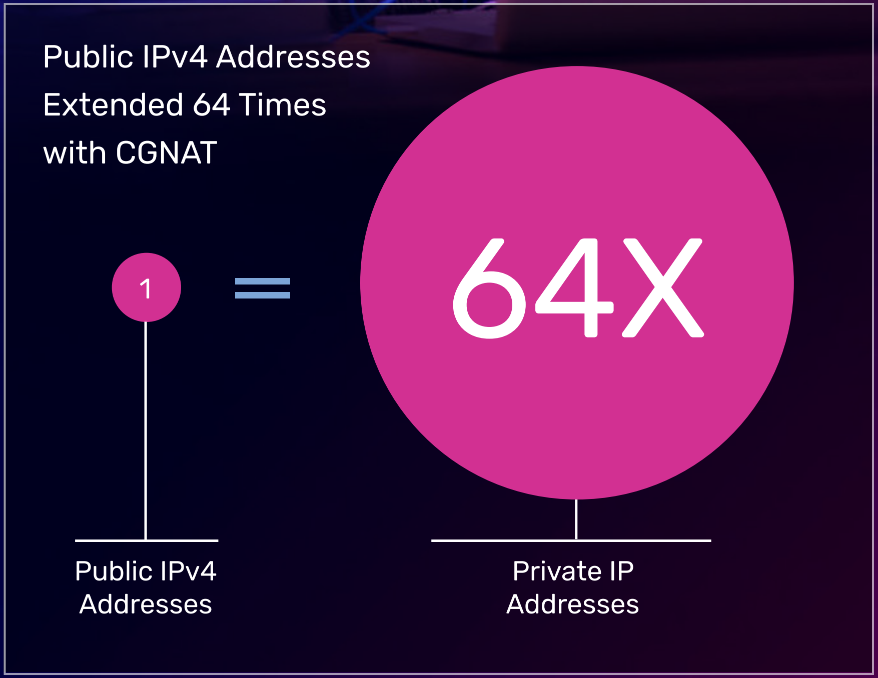
# Case Studies: CGNAT Preserves Infrastructure and Extends IPv4 Address Pools

Given the cost of buying more IPv4 addresses on the open market and the existence of extensive legacy investments in IPv4 infrastructure, many organizations are seeking to extend the utility of their current IPv4 addresses to gain time and flexibility for ongoing IPv6 adoption efforts.

## CGNAT in Higher Education

Many universities were provided years ago with a large set of IPv4 address pools, and subsequently built their network infrastructure to be IPv4-compatible. This allocation has become strained as students and faculty now have five or more devices requiring connectivity to university networks and resources. CGNAT, with NAT44 or NAT444, can expand IP address pools by 64 times or more, with some service providers expanding pools when using CGNAT to support as many as 256 subscriber per IP address, helping budget-constrained organizations extend investment without purchasing costly new IPv4 numbers on the open market or changing out existing infrastructure.

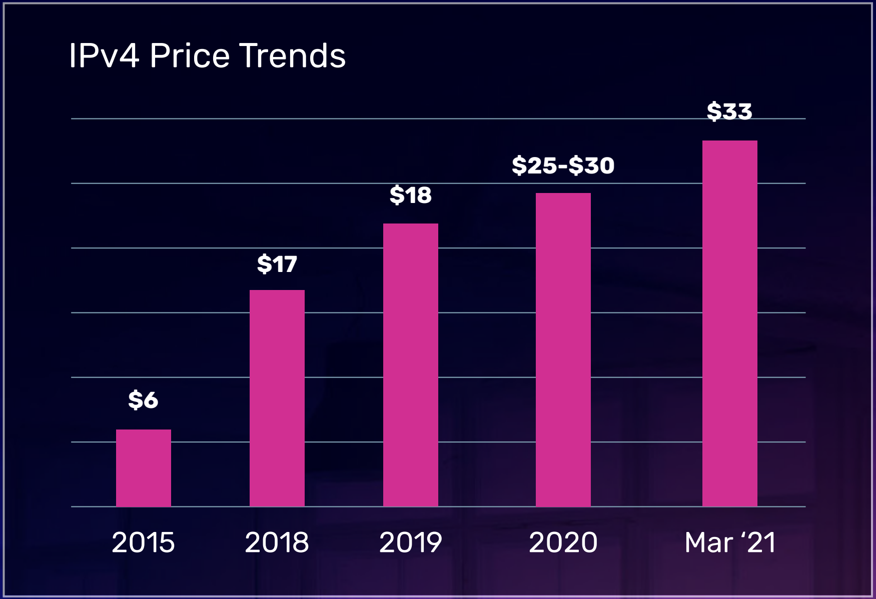
York University is Canada's third largest university, with more than 60,000 students, including 25,000 resident students. Seeking a network infrastructure that could handle its growing student body, the university chose the A10 Networks Thunder® CGN. The solution's NAT44 feature provides large-scale IPv4 address preservation, resulting in a scalable infrastructure that supports 60,000 students and up to 240,000 connected devices.



Public IPv4 Addresses Extended 64 Times with CGNAT

## CGNAT in the Enterprise

A rapidly growing ride-sharing service with nearly 100 million customers and 4 million drivers was consuming more and more of its IPv4 subnet for internal usage. Acquisitions of other companies often resulted in overlapping IP addressing schemes. To make the most of its finite IPv4 resources to support its applications and services, the company deployed A10 Networks Thunder CGN for large-scale network address translation in its two national data centers. The solution manages network address and protocol translation, while automated tooling manages and monitors network configurations and large-scale network address translation. As a result, the company has improved service reliability and operational efficiency while simplifying capacity planning for future innovation.



Source, Heficed

## CGNAT in the CSP Marketplace

MCTV, a regional service provider, provides advanced broadband internet, digital TV, phone, and security to approximately 55,000 homes and businesses in Ohio and West Virginia. The company has built its own optical and cable networks as well as growing by acquisition. As MCTV expanded, it became aware of the steady depletion of its IPv4 addresses. With A10 Networks Thunder CGN, MCTV recovered as many as 31 IPv4 addresses for each customer, resolving its IPv4 exhaustion issue and enabling it to sustain its growth into new service areas.

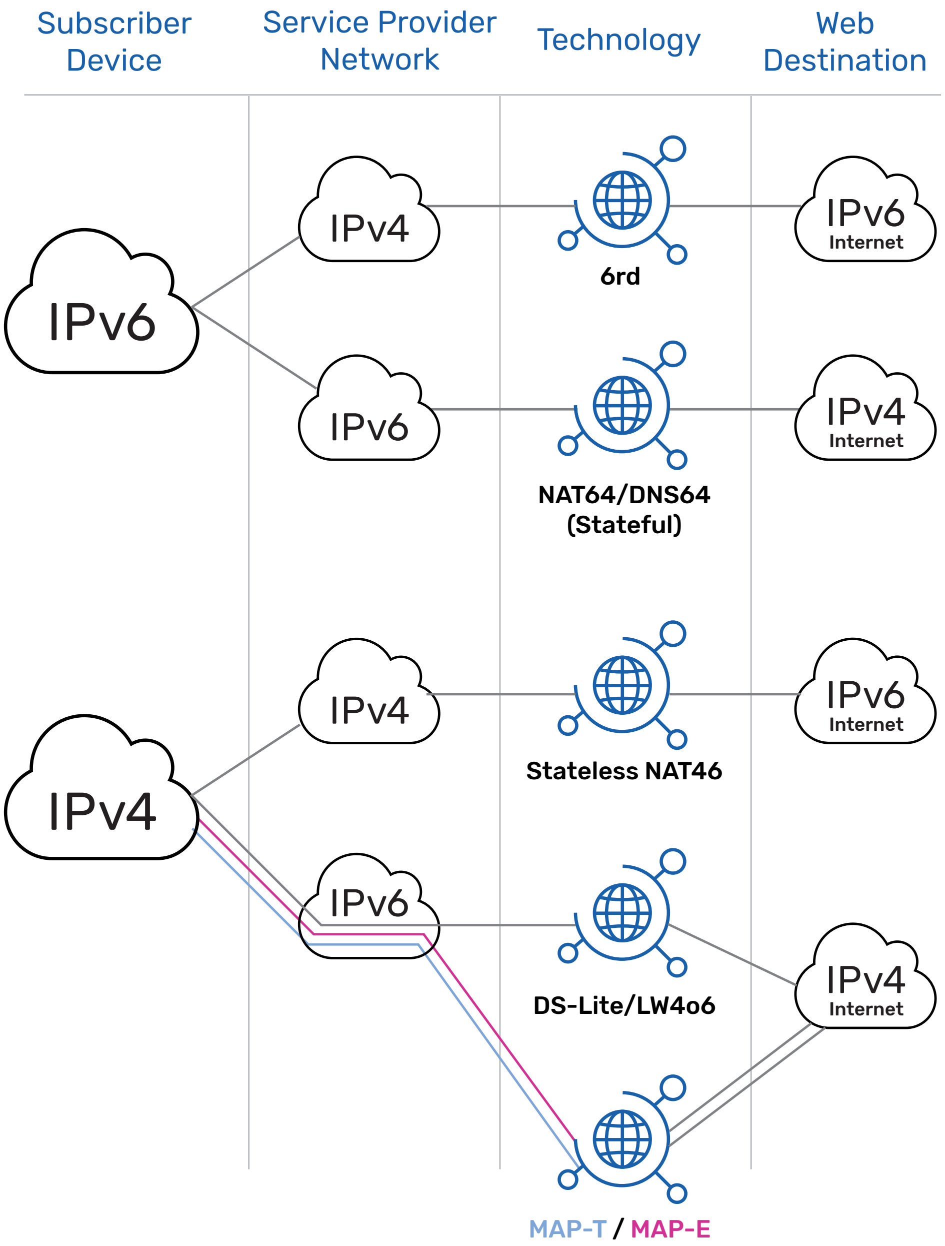
# IPv4 to IPv6 Migration – Translation and Encapsulation Basics

Given the hybrid environment resulting from coexisting IPv4 and IPv6 infrastructure, several technologies have emerged to enable connectivity between IPv4 and IPv6 devices, networks, and Internet destinations. These technologies either translate between IPv4 and IPv6 addresses or encapsulate traffic to enable passage through the incompatible network.

The address and protocol translation techniques available allow a subscriber to transparently access content regardless of the protocol stack their device is using, the provider's access and core network support for IPv4/IPv6, and the destination server support.

Tunneling techniques, such as DS-Lite, encapsulate IPv4 packets over an IPv6 access network, while IPv6 Rapid Deployment (6rd) encapsulates IPv6 packets over an IPv4 access network. Native protocol translation techniques, such as NAT64 or NAT46, translate between the protocol stacks at a gateway within the provider's network when the subscriber and provider networks natively support either IPv4 or IPv6.

These technologies are listed on the next page.



## IPv4 to IPv6 Migration Technologies

| Technology | Type | Subscriber Device | Service Provider Network | Web Destination (Internet) | RFCs |
|---|---|---|---|---|---|
| NAT64/DNS64 | Translation | IPv6 | IPv6 | IPv4 | RFC 6146 (NAT64)<br>RFC 6147 (DNS64) |
| NAT46 | Translation | IPv4 | IPv4 | IPv6 | RFC 6144 |
| MAP-T | Translation | IPv4 | IPv6 | IPv4 | RFC 7599 |
| 464XLAT | Translation (NAT64 + client CLAT) | IPv4 | IPv6 | IPv4/IPv6 | RFC 6877 |
| 6rd | Encapsulation | IPv6 | IPv4 | IPv6 | RFC 6877 |
| DS-Lite | Encapsulation | IPv4 | IPv6 | IPv4 | RFC 6333<br>RFC 6334 |
| LW4o6 | Encapsulation | IPv4 | IPv6 | IPv4 | RFC 7596 |
| MAP-E | Encapsulation | IPv4 | IPv6 | IPv4 | RFC 7597 |

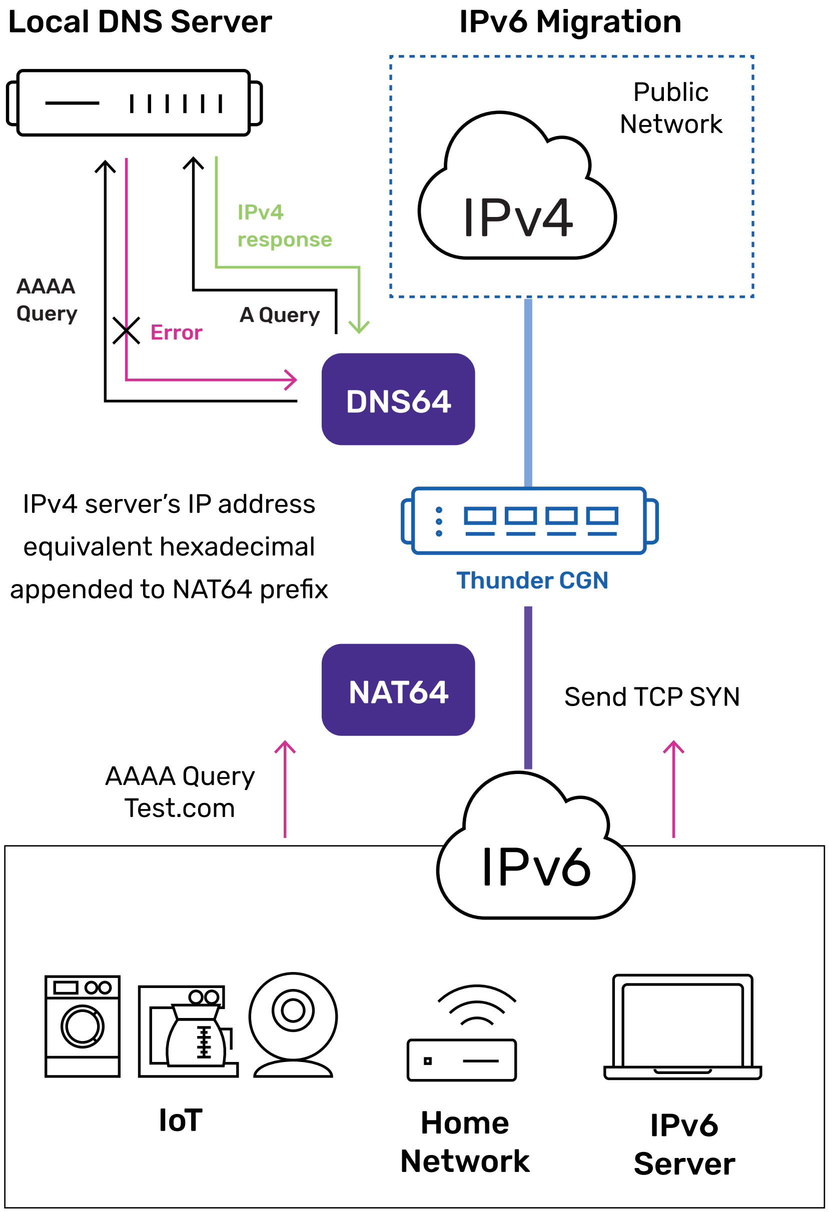
# NAT64 and DNS64

The majority of internet web sites currently are only accessible via 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 IPv6 end-user's DNS requests are received by the DNS64 device, which resolves the requests.

If there is an IPv6 DNS record (AAAA or "quad-A" 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 a 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.

The advantage of NAT64/DNS64 is that it offers IPv6 clients access to IPv4 content with no disruption to IPv4 infrastructure. On the other hand, it does not provide a solution for IPv4 clients accessing IPv6 content. In addition, for stateful NAT, the NAT64 device must maintain a table with each active flow, requiring more resource usage.



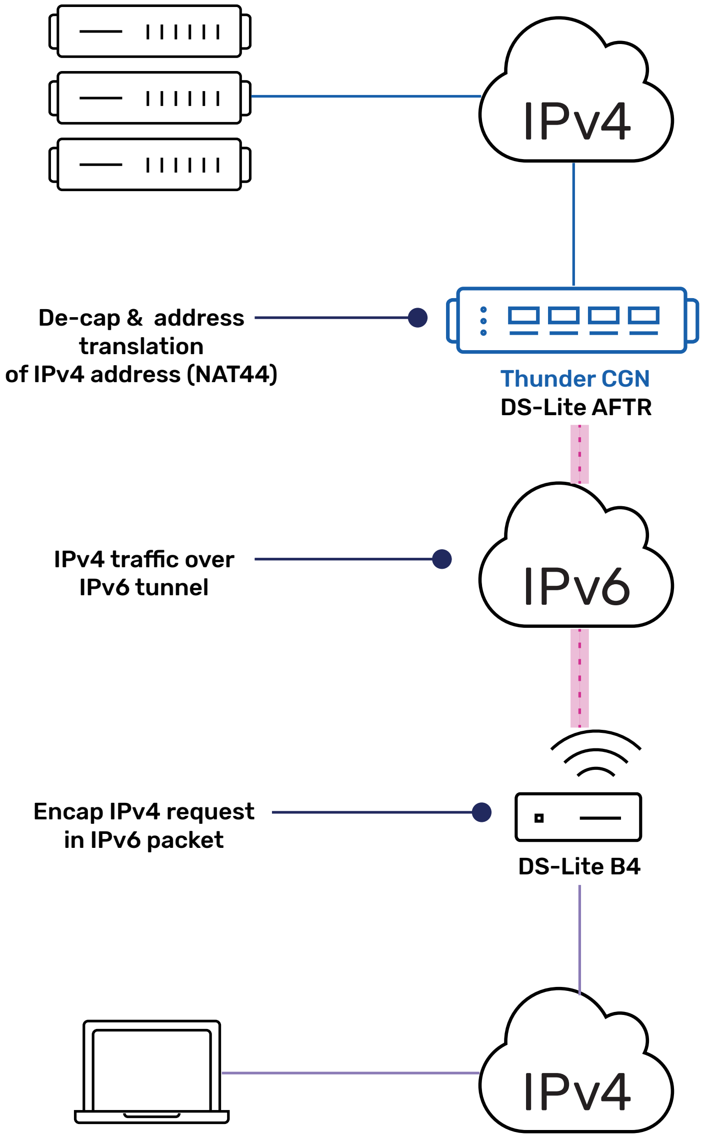
# Dual-Stack Lite (DS-Lite)

Dual-Stack Lite, or DS-Lite, is used by service providers to maintain IPv4 connectivity through an all-IPv6 access network, among other benefits. The service provider's IPv6 core network already allows IPv6 content access to end-users on IPv6. With DS-Lite support, an IPv4 user can use the same network to connect and access the Internet, or any other IPv4 network.

First, the end-user's modem/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.

With DS-Lite, IPv6 end-users have native access to IPv6 content, and can host IPv6 services such as web servers in their locations, while existing IPv4 end-users still have access to IPv4 content. IPv4 and IPv6 end-users can coexist in each end location. This approach enables incremental IPv6 deployment while realizing IPv6 benefits in the core infrastructure including efficiency, simplicity, and security.

However, DS-Lite does not provide any IPv4 content access to IPv6 end-users, or IPv6 content access to IPv4 end-users. It extends the time before IPv6 migration becomes essential, but the migration will still be required eventually. End-to-end connectivity is very complex for IP telephony or file sharing services.


IPv4
De-cap & address translation of IPv4 address (NAT44)
Thunder CGN
DS-Lite AFTR
IPv4 traffic over IPv6 tunnel
IPv6
Encap IPv4 request in IPv6 packet
DS-Lite B4
IPv4

# 464XLAT

One shortcoming of using NAT64 and DNS64 is that some IPv4-only applications, such as Skype and WhatsApp, can't function through NAT64. Using 464XLAT provides a way to keep these applications working with a simple and scalable technique for an IPv4 client with a private address to connect to an IPv4 host over an IPv6 network.

With 464XLAT, the client uses a SIIT translator (Stateless IP/ICMP Translation) to convert IPv4 packets into IPv6 to send over an IPv6-only network to a NAT64 translator. After translation into IPv4, the packets can then be sent over an IPv4-capable network to the IPv4-only server for Skype, WhatsApp, or any other IPv4-only application.

464XLAT eliminates the need to maintain an IPv4 network for this type of IPv4 traffic or assign additional public IPv4 addresses. At the same time, 464XLAT only supports IPv4 in the client-server model, and does not support IPv4 peer-to-peer communication or inbound IPv4 connections.

## SK Telecom Moves into 5G

SK Telecom, the largest mobile operator in South Korea, launched the world's first commercial 5G service. More than one million subscribers signed up in a matter of weeks, by mid year 2020, SK Telecom had exceeded 3.3 million 5G subscribers.

While rebuilding its entire network to support 5G mobile broadband, SK Telecom needed to support subscribers' devices that still used IPv4 addressing, while providing a clear migration path to IPv6 at the edge. The operator also needed to provide subscriber access to internet services and content providers that don't offer IPv6 addressing.

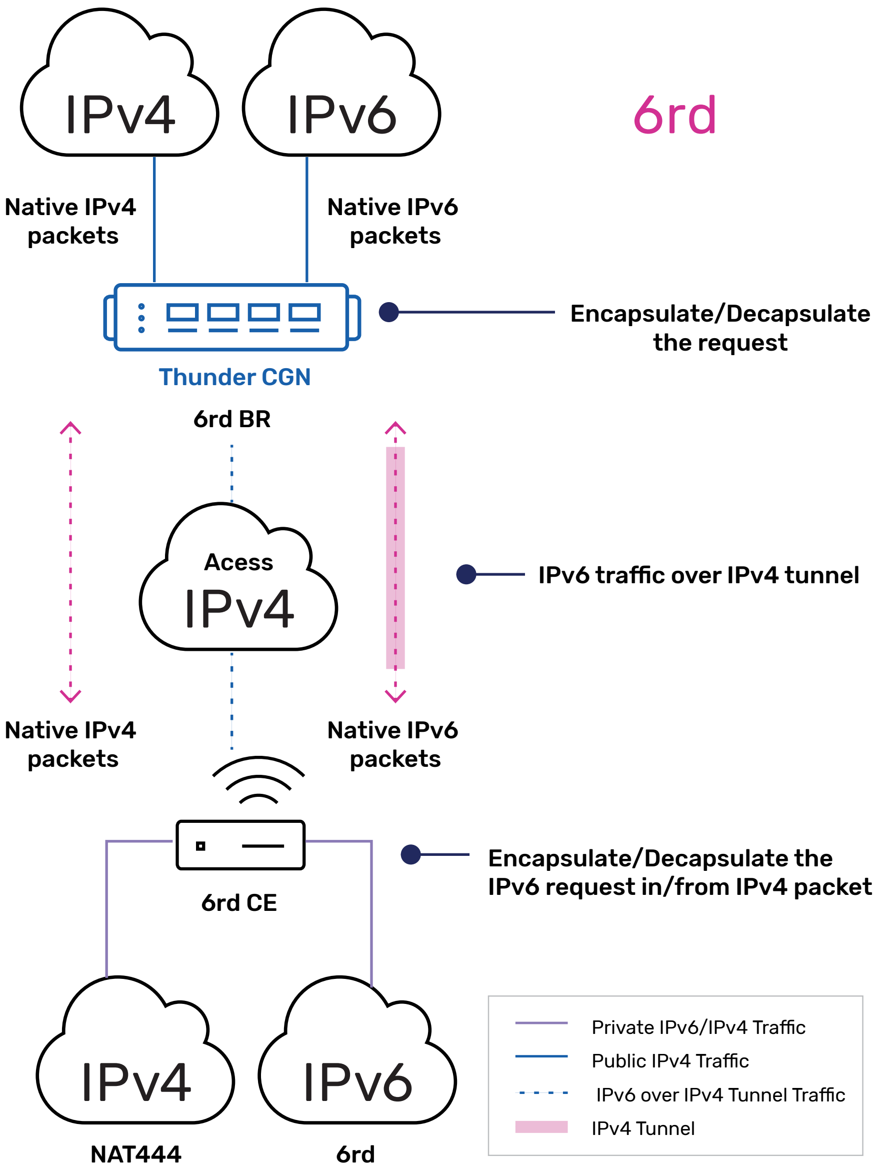
SK Telecom deployed A10 Networks Thunder® CFW for address translations between IPv4 and IPv6. With Thunder CFW, SK Telecom has maintained high reliability and performance for providing uninterrupted access to both IPv4 and IPv6 services.

# Other Transition Options

## IPv6 Rapid Deployment (6rd)

A service provider can use IPv6 rapid deployment (6rd) to leverage an existing IPv4 core network 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. An IPv4 end-user's traffic is simply NATed and routed to the IPv4 resources as normal. An 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.

However, 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.


IPv4
IPv6
6rd
Native IPv4 packets
Native IPv6 packets
Encapsulate/Decapsulate the request
Thunder CGN
6rd BR
Acess
IPv4
IPv6 traffic over IPv4 tunnel
Native IPv4 packets
Native IPv6 packets
Encapsulate/Decapsulate the IPv6 request in/from IPv4 packet
6rd CE
IPv4
IPv6
NAT444
6rd
Private IPv6/IPv4 Traffic
Public IPv4 Traffic
IPv6 over IPv4 Tunnel Traffic
IPv4 Tunnel

## MAP-T and MAP-E

The Mapping of Address and Port using Translation (MAP-T) builds on the Address plus Port method of stateless NAT to translate IPv4 packets to IPv6 and carry on IPv6-only access network in order to provide IPv4 services without deploying a full dual-stack network.

MAP-T is based on stateless NAT64 technique. The end-user's CPE device must support MAP-T CE functionality to provide NAPT (NAT44) and stateless mapping of IPv4 & port to IPv6. MAP-T Border Router (MAP-T BR) translates the address between IPv6 and public IPv4 based on MAP Rules before routing it to the IPv4 resources.

Mapping of Address and Port with Encapsulation (MAP-E) enables service providers to transport IPv4 packets across an IPv6 network using IP encapsulation.

# CGN at the Edge of Digital Transformation

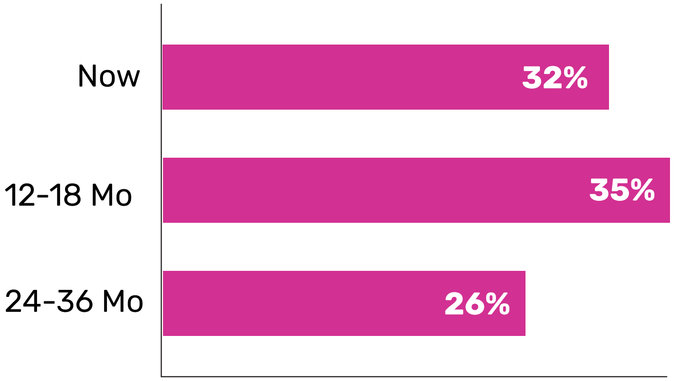
Digital transformation is impacting organizations of all types and driving macro technology trends such as cloud, edge cloud, and 5G. Given its critical function in line with traffic, Carrier Grade NAT (CGNAT) will be required for some time to come, and it must seamlessly integrate with the organization's large architecture plans. In fact, Heavy Reading has reported that 80 percent of mobile network operators will require CGNAT in 2023. As a result, once considered a standalone appliance, the CGN is increasingly deployed as a virtual machine, bare metal, or container, in virtual or cloud-native environments, and it works with the management and orchestration systems for the network.

For example, mobile service providers are quickly launching 5G Core (5GC or standalone), which uses a cloud-native architecture. A 93 percent implementation rate is expected over the next three years.

This is a massive change in the core network technology and will deliver huge benefits to operators in terms of cost reduction and service agility.

Transformation elements also include the migration from 4G to 5G (and 5GC), from hardware-based networks to software-defined networking, from exclusively on-premises infrastructure to hybrid and multi-cloud environments, and from traditional architectures to multi-access edge computing (MEC). Their business success will depend on their ability to deliver these initiatives effectively in tandem while providing a seamless experience for subscribers and value to those creating new applications and services

The IPv4 to IPv6 migration must complement this larger technology transformation and be available in the form factor needed and interoperable with management and orchestration systems.



CGNAT is a Key Requirement in 2023

**By 2023**

**93%**

Implementation Rate for 5GC

Carrier Grade NAT

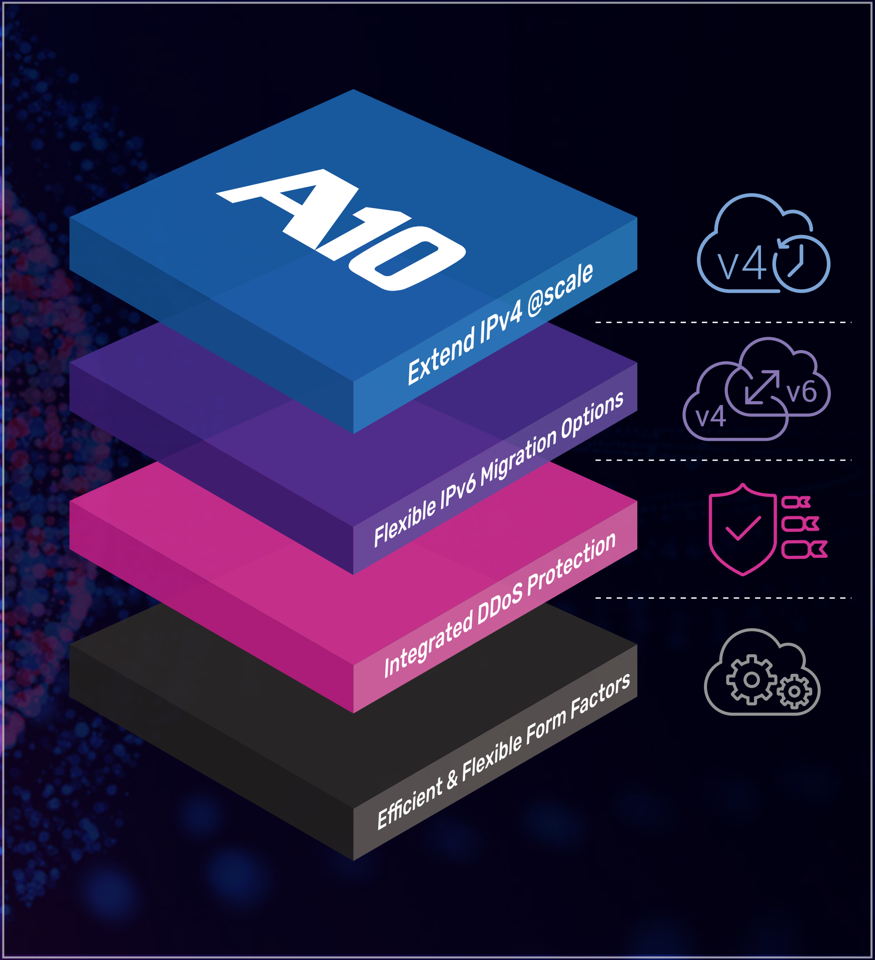
**80%**

% of Operators

Source, Heavy Reading, "Standalone Security – Adoption, Automation, Attributes and Attacks"

# Invest for Continuous Migration

In taking a lifecycle approach to IPv4 – IPv6 migration, service providers and other organizations need to ensure that the technologies they implement will meet both their short-term needs and their long-term requirements.


A10
Extend IPv4 @scale
Flexible IPv6 Migration Options
Integrated DDoS Protection
Efficient & Flexible Form Factors
v4
v4
v6

## Deployment Flexibility

Service provider infrastructures vary in size and complexity, so a CGNAT and IPv6 migration solution needs to provide flexible integration and deployment options, including cloud native (container), virtual machine, bare metal and physical appliances. The platform needs to meet current and future capacity and performance requirements in a form factor that meets the organization's infrastructure.

In evaluating the optimal address and protocol translation techniques for its needs, the provider needs the flexibility to evolve its approach or implement multiple techniques simultaneously to meet the current and future requirements of the CPE data center infrastructure, access and core networks.

## Performance

When implementing CGNAT and IPv6 migration solutions, the subscriber experience should not be affected, and the use of address translation should be completely transparent. This requires the use of a high-performance, scalable and flexible platform that is designed to support tens of millions of concurrent sessions and is also capable of sustaining high throughput levels.

In addition, the platform should provide support for high-speed logging, connection statistics and complete visibility, along with being fully programmable using an open API.

## Logging and Law Enforcement Agency Compliance

Law enforcement agencies generally mandate that network operators provide the details of the location of a particular subscriber—either at the current time or a given moment in the past—and have this information available within a very short timeframe. This requires the ability to quickly map the subscriber's inside address with the address used on the public internet. This can be a very difficult task for a provider given that standard subscriber translation logging can easily exceed a terabyte of storage a day, depending on the number of subscribers supported.

To allow a provider to easily parse and reduce the volume of logs, it is important for the translation logging solution to support advanced logging techniques. This may include log compression features that can significantly reduce the amount of data included in a log or support CGNAT methods that can virtually eliminate logging, such as Deterministic or Fixed NAT, which can provide the details of a connection using a simple algorithm.

## Application Integrity

When organizations implement address and protocol translation solutions, they must ensure that it is completely transparent to their subscribers and that applications don't suddenly stop working. In order to prevent any issues with certain applications that may not operate properly through address or protocol translation, it is critical for the solution to provide complete support for application-level gateways (ALG).

ALG support allows client applications to use dynamic ephemeral TCP/UDP ports to communicate with the known ports used by the server applications, even though a firewall configuration may allow only a limited number of known ports. Without ALG support, application ports would get blocked and the network administrator would need to explicitly open up a large number of ports in the firewall, which would render the network vulnerable to attacks on those ports.

ALGs convert the network-layer information found inside an application payload between the addresses for the hosts on either side of a firewall or NAT function. An ALG can also synchronize the multiple streams and sessions of data between two hosts exchanging data.

## Reliability

When implementing IPv4 preservation and IPv6 migration solutions, the platform used should also be capable of providing a high level of reliability and availability. It should support capabilities such as stateful session failover that can synchronize session information to ensure uninterrupted service disruption by providing sub-second failover to a standby unit in case of a network reachability issue.

It is also advantageous for the solution to provide the capability to track the health of various network resources, such as gateways and interfaces, along with providing routing protocol awareness, in order to dynamically redirect traffic to prevent user session disconnections.

## Visibility

Organizations require the ability to have complete visibility into their network traffic in order to manage, secure and optimize performance. Solutions should offer traffic monitoring, mirroring and analytics to support security, compliance and operational practices.

Tools such as sFlow and Netflow provide traffic visibility with time series data and metrics that enable a CGNAT and IPv6 migration solution to operate as a DDoS probe to uncover potential anomalies that indicate an attack on an individual subscriber or the CGNAT device itself.

Providing visibility within the solution also allows for capacity-planning and resource-tuning. This information should also be available for external systems to analyze traffic patterns, resource usage and alarm/system log information.

TABLE OF CONTENTS

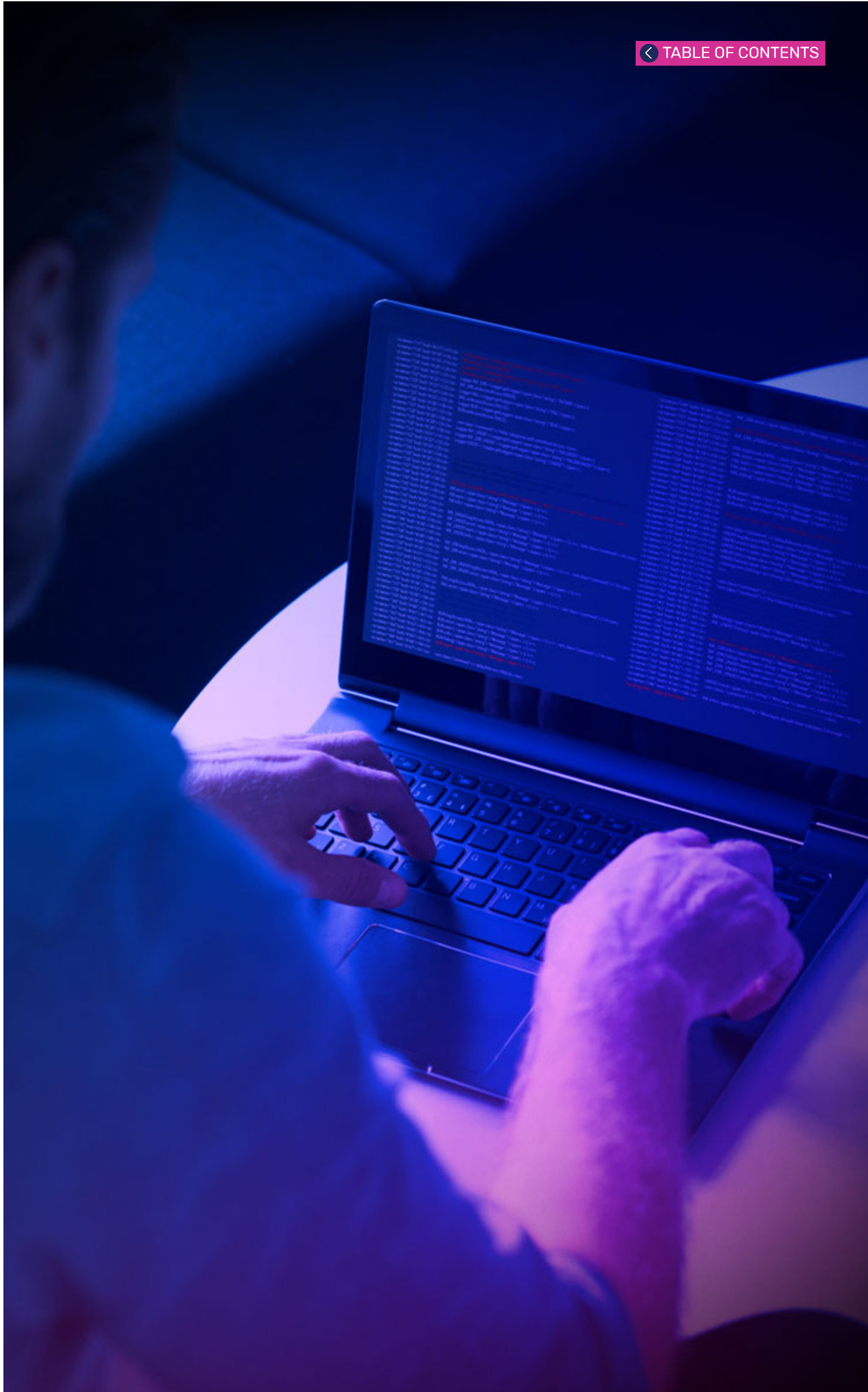
## Security – Integrated DDoS Protection for CGNAT

Service provider, enterprise and higher education networks are big targets for distributed denial of service (DDoS) attacks. Traditionally, a DDoS attack on the service provider's infrastructure was somewhat isolated. If an individual subscriber was targeted, the attack was contained to their service.

With a NAT gateway in place, this is not always the case. Hackers can target the gateway itself to take down the access of large swaths of subscribers. They can also target an individual subscriber and jump to the NAT gateway they are connected to in order to propagate their attack to other subscribers.

Organizations need to have the capability to protect their subscribers, customers, employees and students from DDoS attacks and ensure that the NAT gateway itself is not compromised. A CGNAT and IPv6 migration solution should have the ability to protect itself, and the subscribers behind the gateway, using mitigation techniques such as:

- **IP anomaly filtering**
- **Reduced CPU overhead for CPU round robin**
- **Selective filtering for LSN**
- **Connection rate limiting**
- **IP blacklist for DDoS protection**



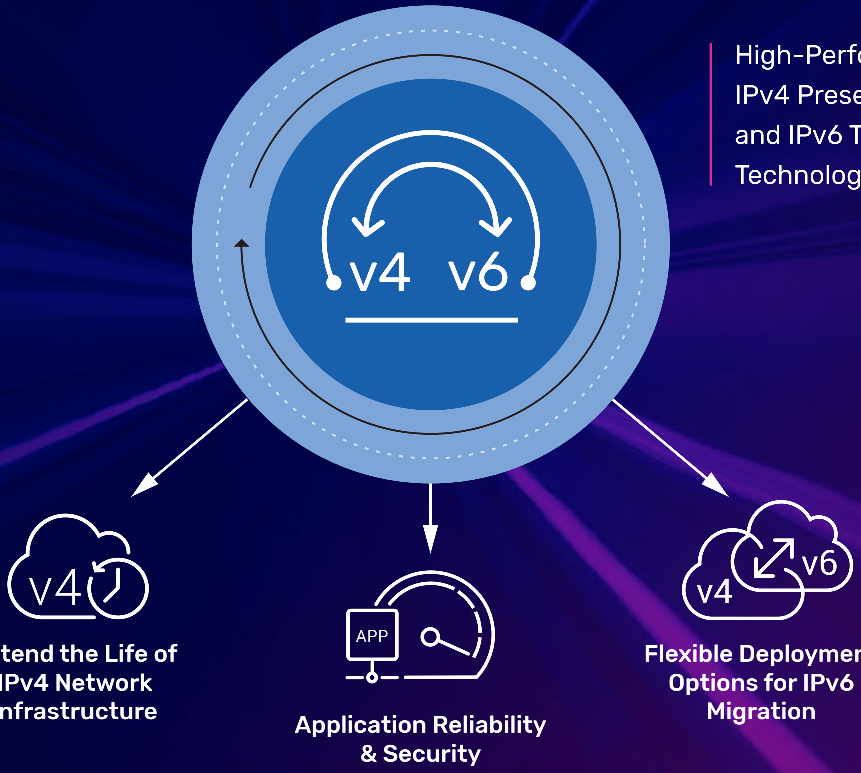
# A10 Networks – Your Partner throughout the IPv6 Lifecycle

A10 Networks Thunder CGN, the most advanced carrier-grade networking solution, provides high-performance CGNAT with protocol translation that allows allow service providers, higher education institutions, and enterprises to extend IPv4 investment while simultaneously transitioning to IPv6 standards.

A10 Networks Thunder CFW provides a unique combination of multiple security functions in a single product—a highly scalable, high-performance firewall, IPsec VPN, secure web gateway, and carrier-grade NAT with integrated DDoS protection. Thunder CFW provides address translations between IPv4 and IPv6 as well as an advanced Gi-LAN firewall.

## A10 Networks Thunder CFW and CGN Solutions Provide:

- High performance in all form factors, including container, virtual, bare metal and physical
- CGNAT (NAT 44/444)
- IPv4 – IPv6 migration through techniques including:
  - NAT 64, DNS 64,
  - LW4o6, MAP-T, MAP-E,
  - DS-Lite
  - 6rd
  - 464XLAT
- Advanced features for logging and compliance to help providers meet requirements for compliance and auditability
- Application-level gateways (ALG) support network growth and a seamless user experience
- Built-in security strengthens defense against cyberthreats including DDoS



High-Performance IPv4 Preservation and IPv6 Transition Technologies

Extend the Life of IPv4 Network Infrastructure

Application Reliability & Security

Flexible Deployment Options for IPv6 Migration

TABLE OF CONTENTS

## About A10 Networks

A10 Networks (NYSE: ATEN) provides secure application services for on-premises, multi-cloud and edge-cloud environments at hyperscale. Our mission is to enable service providers and enterprises to deliver business-critical applications that are secure, available and efficient for multi-cloud transformation and 5G readiness. We deliver better business outcomes that support investment protection, new business models and help future-proof infrastructures, empowering our customers to provide the most secure and available digital experience. Founded in 2004, A10 Networks is based in San Jose, Calif. and serves customers globally.

For more information, visit A10networks.com and follow us @A10Networks.

**LEARN MORE**
**ABOUT A10 NETWORKS**

**CONTACT US**
a10networks.com/contact

Part Number: A10-EB-14140-EN-03 Mar 2021