WHITE PAPER

CGNAT Isn't a Capability
It's a Lifecycle Strategy

What Service Providers Need to Consider
When Choosing a Carrier-Grade NAT Solution

Table of Contents

Service Providers Utilize Address Translation for Ongoing Business Continuity

With the exponential growth of subscribers and connected devices, service providers have been investing in infrastructure to support increasing traffic growth while implementing new services to attract new subscribers and increase revenue.

Preparing for the Internet of Things (IoT) is also contributing to the demand on the infrastructure and the number of devices connected to the network. With the global exhaustion of free pools of IPv4 addresses and the continuing adoption of IPv6, service providers are facing new challenges in sustaining growth and business continuity.

Many service providers will need to implement an address translation strategy that includes both a short-term plan to address the preservation of their existing IPv4 address allocation, and a long-term plan to seamlessly migrate to an IPv6 infrastructure.

This approach will require a solution that not only provides a robust set of carrier-grade network address translation (CGNAT) capabilities — and IPv6 migration options based on each service provider's existing infrastructure — but one that also addresses the entire lifecycle of the transition from IPv4 to IPv6.

This white paper provides an overview of the various components that are required for a complete CGNAT and IPv6 migration solution, which encompass the entire lifecycle of the transition to IPv6.

IPv4 Addresses Exhausted

"With the global exhaustion of free pools of IPv4 addresses and the continuing adoption of IPv6, service providers are facing new challenges in sustaining growth and business continuity."

Areas to Consider When Implementing CGNAT and IPv6 Migration Techniques

If a service provider doesn't consider all requirements as they build a strategy to migrate to an IPv6 infrastructure, they may end up implementing multiple stop-gap measures that are not addressing the overall long-term strategy.

Most experts agree that IPv4 will be around for at least another 3-5 years. As of October 2016, only about 20 percent of websites can be reached using an IPv6 protocol stack.[1] To provide a smooth transition to IPv6, and to ensure business continuity, providers need to consider several components, including:

- Flexible deployment and integration options
- Performance
- Application integrity
- Visibility and compliance
- Security
- Availability

Deployment Flexibility

Service provider infrastructures vary in size and complexity, so a CGNAT and IPv6 migration solution needs to provide flexible integration options.

Such a platform needs to meet current and future capacity and performance requirements, and is available in a form factor that meets the provider's infrastructure requirements. This may include a dedicated appliance, a virtual machine (VM) that is supported by a leading hypervisor, or bare metal software that can operate on a standardized dedicated server.

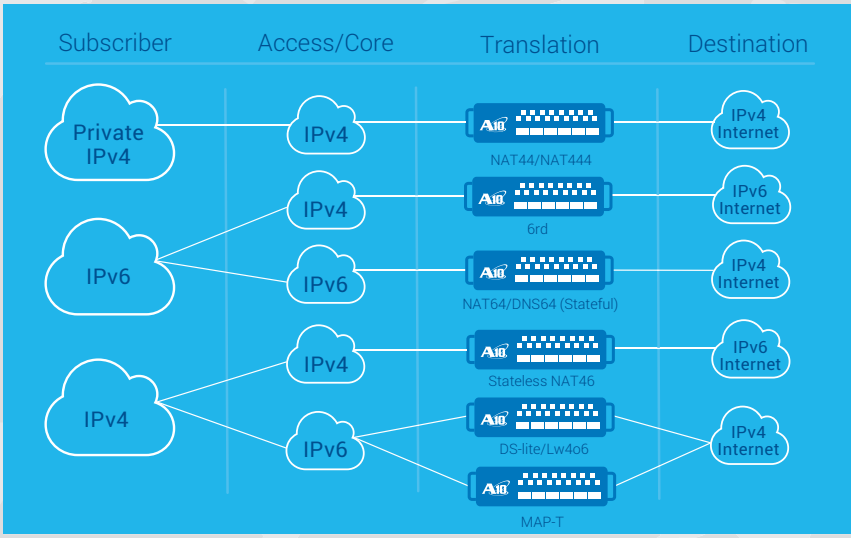
The platform should also include advanced network integration support, such as integrated Layer 2-3 support, and static and dynamic IPv4/IPv6 routing to enable the solution to be easily deployed in an existing environment.

When addressing CGN and IPv6 migration requirements, there are several items to consider, including address translation support for the existing subscriber's customer-premises equipment (CPE), the provider's current and future core and access network IPv6 support, along with the state of the destination server's IPv4/IPv6 protocol support.

Each of these factors will contribute to the type of solution that is implemented. As shown in the figure on the next page, providing a robust set of address and protocol translation techniques is critical in order to properly address an evolving environment.

1 "The Future is Forever." World IPv6 Launch Online. October 13, 2016. http://www.worldipv6launch.org/measurements/

IPv4 PRESERVATION & IPv6 MIGRATION SOLUTIONS



Each address and protocol translation technique provides a solution that allows 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. The available translation techniques support either tunneling or native protocol translation.

Tunneling techniques, such as DS-Lite, encapsulate IPv4 packets over an IPv6 access network, and 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.

The use of a particular translation technique is based on the provider's available IPv4 addresses, the state of the IPv6 support on the access and core networks, and the type of CPE that is used (may be supplied by the subscriber).

The address and protocol translation techniques that are implemented can evolve over time or be used simultaneously to meet the current and future requirements of the CPE, 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 over 150 Gbps and connection setup rates in the millions per second.

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 Enforcement Agency Compliance

Law enforcement agencies (LEA) 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 service providers 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

Service providers design their network infrastructure to provide their subscriber base with consistent performance and reliable connectivity. 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.

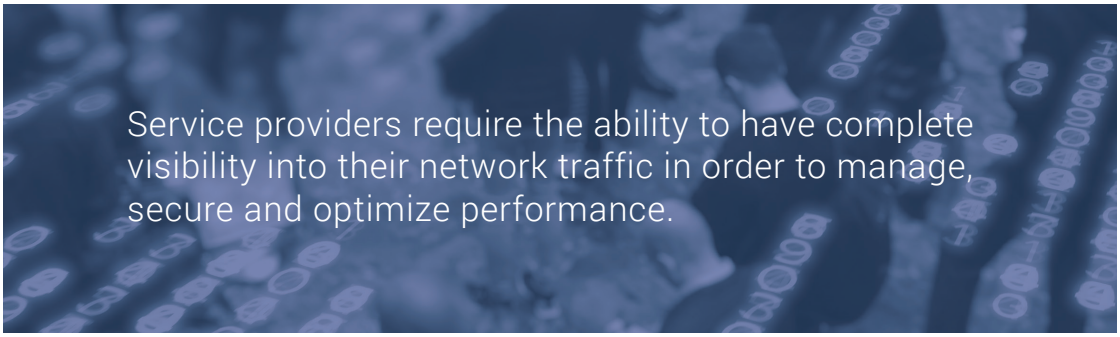
It is also advantageous for the solution to provide the capability to track the health of various network resources, such as gateways and interfaces, along with providing routing protocol awareness, in order to dynamically redirect traffic to prevent user session disconnections.

Visibility

Service providers require the ability to have complete visibility into their network traffic in order to manage, secure and optimize performance. Providers should look for solutions that offer traffic monitoring, mirroring and analytics to support their 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.



Security

Service provider 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.

Multivector DDoS Attacks are Bigger, Smarter, More Devastating

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

- IP anomaly protection to recognize and drop traffic from common attack signatures
- Internet Control Message Protocol (ICMP) rate limiting
- CPU overload protection caused from spoofing attacks
- Connection rate limiting
- Automatic IP address blacklisting to mitigate attacks targeting NAT pool addresses

A10 Provides the Lifecycle Needs of Service Providers

A10 Networks empowers service providers to navigate and prepare for changes within the industry. Based on the effectively architected, highly efficient and powerful Advanced Core Operating System (ACOS®), A10 solutions help service providers maximize their investments and monetize their networks throughout their IPv6 migration lifecycle.

ACOS is at the core of the A10 Thunder® CGN, which enables service providers to mitigate the impact of IPv4 exhaustion, while simultaneously make the transition to IPv6. A10 Thunder CGN allows service providers to address:

- **Different deployment requirements.** Gives providers the choices they need to ensure the solution fits seamlessly within their environment and supports their migration approach. A10 offers physical appliances, virtual and bare metal solutions, and supports the major encapsulation/tunneling and translation protocols to ensure service providers can leverage and extend their investments.

- **Application integrity.** Supports the required ALG to ensure all user applications work seamlessly and use of address and protocol translation is completely transparent to the user experience.

- **Resource allocation.** Ensures a great customer experience without overprovisioning ports to handle bursts. A10 not only provides a user quota, but also a reserve user quota, that delivers on a service provider's service guarantee. This reserve quota allows subscribers to burst into a shared pool of ports, beyond their normal allocation, so providers can be more realistic when allocating ports and don't have to waste ports in reserve, on the off chance they will be needed by a subscriber.

- **Security.** Includes advanced DDoS protection to protect both the NAT gateway and subscribers behind the gateway.

- **Visibility.** Supports sFlow and Netflow to allow service providers to collect and analyze traffic data. Full connection statistics and NAT logging is available to provide capacity planning and monitoring capabilities.

- **Compliance.** Simplifies NAT logging to enable service providers to quickly find the address translation information they need to comply with LEA requests. A10 optimizes logging to reduce volume (e.g., port batching, Fixed-NAT, compact and binary logging) and increase logging efficiency.

  A10 integrates with the service provider's existing infrastructure — supporting ASCII, HEX, Binary, RADIUS and SYSLOG (RFC 5424) — and provides fully customizable logging message formats. It also offers a variety of transport options, such as TCP and UDP, and can send logs to up to 32 servers with hashing and load-balancing support.

- **Performance and reliability.** Delivers performance at an order of magnitude greater than anything else on the market. A10's high-performance ACOS platform separates control and data planes, enables the rapid adoption of new features, provides programmability and delivers greater flexibility and deployment agility.

- **Vendor consulting and support.** Provides elite post-sale support for additional value and peace of mind. There are many CGNAT and IPv6 migration solutions available, but A10 has always taken the consultative approach when working with our service provider customers.

It is easy for a vendor to promote a solution that addresses an immediate requirement, but we prefer to partner with our customers to provide a complete solution that addresses both the immediate and future needs of the entire IPv6 migration lifecycle.

Value of the Complete CGNAT and IPv6 Migration Solution

Providers are highly motivated to optimize their IPv4 investments as they move to IPv6 networks. The A10 Thunder CGN solution makes this possible and helps achieve high-performance, highly transparent address and protocol translation that extends IPv4 network connectivity, while smoothing the migration to IPv6.

- **Increase revenues.** Ensure providers can address changing market demands and build out the differentiated services customers want — now and in the future.
- **Improve customer satisfaction.** Deliver the performance and availability needed to meet the needs of all their global subscriber base.
- **Expand margins.** Lower operating expenses to improve operating income with an advanced solution that reduces the burden on IT.

About A10 Networks

A10 Networks is a leader in application networking, providing a range of high-performance application networking solutions that help organizations ensure that their data center applications and networks remain highly available, accelerated and secure. Founded in 2004, A10 Networks is based in San Jose, California, and serves customers globally with offices worldwide. For more information, visit: **www.a10networks.com**

Corporate Headquarters

A10 Networks, Inc
3 West Plumeria Ave.
San Jose, CA 95134 USA
Tel: +1 408 325-8668
Fax: +1 408 325-8666
www.a10networks.com

Part Number: A10-WP-21136-EN-02
Dec 2016

Worldwide Offices

North America
sales@a10networks.com
Europe
emea_sales@a10networks.com
South America
latam_sales@a10networks.com
Japan
jinfo@a10networks.com
China
china_sales@a10networks.com
Hong Kong
hongkong@a10networks.com
Taiwan
taiwan@a10networks.com
Korea
korea@a10networks.com
South Asia
southasia@a10networks.com
Australia/New Zealand
anz_sales@a10networks.com

To discover how A10 Networks products will enhance, accelerate and secure your business, contact us at a10networks.com/contact or call to speak with an A10 sales representative.