White Paper

Managing the Migration to IPv6 Throughout the Service Provider Network

While service providers worldwide are beginning to acknowledge that they need to adopt IPv6, most are still struggling to define a workable strategy around it. F5 solutions provide the flexibility service providers need to devise gradual transition plans, maintain control over the IP network, support their customers, and minimize service disruption and downtime.

by Andrew Hendry
Manager, Solution Marketing

and Alan Murphy
Manager, Technical Marketing

Contents

Introduction

Service providers are feeling increasing pressure to transition from the well-known and universal Internet Protocol version 4 (IPv4) standard to the newer IPv6 standard, while still supporting both network topologies. There are many reasons for this, not the least of which are the continually shrinking number of available IPv4 addresses and the exploding number of devices that require access to Internet applications and services.

Although the IPv6 standard includes important new features beyond the virtually unlimited new address space, such as increased security and reliability, the world still runs largely on IPv4. As new network technologies continue to drive users and services toward what will eventually be an all-IPv6 network, service providers will need to be ready to adapt, manage, and support a dual-network architecture for the duration of the transition.

The Transition Challenge

No service provider will be able to simply flip a switch to make all its applications and equipment IPv6-capable. Indeed, customers and Internet content will continue to run on IPv4 for years to come. To successfully transition to IPv6, service providers must be able to design and manage data centers, network infrastructure, and security systems that simultaneously support both IPv4 and IPv6. But the transition doesn't stop at the network level: most service providers operate a significant number of consumer and enterprise applications and services that must be addressed on a wide range of platforms and within multiple hosting locations. Network firewalls, user access management tools, and advanced application delivery tools are critical components that must also be factored into any IPv6 migration plan.

For most organizations, specific functional needs and customer requirements will be the primary drivers of network migrations to IPv6 as new technologies are introduced into the data center, public IPv4 addresses become scarce, and customers migrate themselves. This type of transition will leave some locations and services on IPv4 while other parts of the network will transition to IPv6, affecting not only the core infrastructure, but the users and services that rely on these networks. Isolated IPv4 networks will still need to be able to seamlessly interoperate with the rest of the organization's users and systems on the IPv6 networks, and vice versa. Unfortunately IPv4 and IPv6 are not inherently interoperable.

Making migration plans even more complex, the new technologies and integration issues associated with a transition can create security challenges and more risk in the service provider network. Firewalls and other network and application security tools must also be able to simultaneously support IPv4 and IPv6 traffic; otherwise, service providers could open themselves up to new threats solely due to interoperability issues at the network level.

To properly handle the burden of introducing and supporting IPv6, service providers need a smart migration plan and tools to help provide an orderly transition between the two standards. These tools should give the organization the freedom to test, move, and migrate its existing infrastructure at a controlled, secure, and manageable pace. F5® BIG-IP® products provide seamless support for both IPv4 and IPv6 networks, allowing service providers to transparently manage application delivery, availability, performance, and security between both network topologies at one central location—all without the need to deploy point products throughout the infrastructure.

Read the case study, F5 Supports IPv6 on Core Network, to learn how F5 IT is managing the transition to IPv6 for its mobile users.

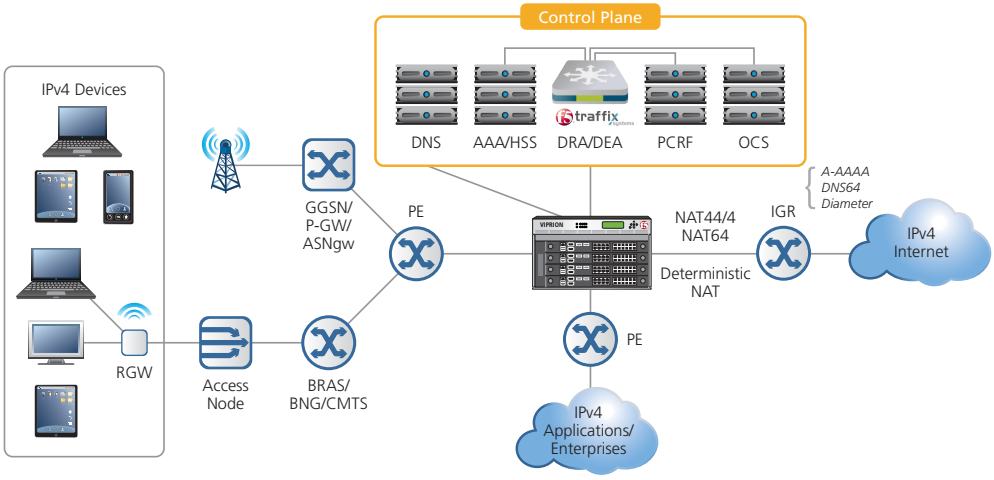

Figure 1: Mitigate IPv4 address depletion with CGNAT.

IPv4 Address Depletion Solution

To mitigate short-term IPv4 address exhaustion while formulating longer-term plans for IPv6, many service providers first implement a carrier-grade network address translation (CGNAT) solution in their core networks. This solution enables translation between private and public IPv4 addresses in N:1 or 1:1 configurations. F5's BIG-IP system provides a high-performance, scalable CGNAT solution for IPv4 address translation, and incorporates other sophisticated functions that provide incremental flexibility and value for service providers. For example, F5 supports high-speed,

reliable system logging with integrated load balancing to a data storage server pool in order to comply with legal intercept and regulatory requirements. F5 solutions support NAPT (PAT) to leverage both the private IPv4 addresses and specific port numbers for translations in order to exponentially scale the available source addresses. F5 solutions also have a deterministic NAT capability that maps specific private IP addresses to public IP addresses within the underlying system configuration and provides high-speed logging in real time.

IPv6 Migration Strategies

While enterprises may be able to stagger their IPv6 implementations by dealing with clients or application content separately, service providers will need to support simultaneous implementations of IPv6-enabled devices, such as broadband modems or mobile devices, as well as IPv6-enabled Internet content, most likely from major web content providers like Google or Facebook and enterprises like Microsoft or Bank of America. The two main scenarios for a smooth, controlled transition are for a service provider to incorporate IPv6-enabled clients while keeping its own servers on IPv4, or to migrate its servers to IPv6 while continuing to support IPv4 clients. Both scenarios have important implications for users and applications alike.

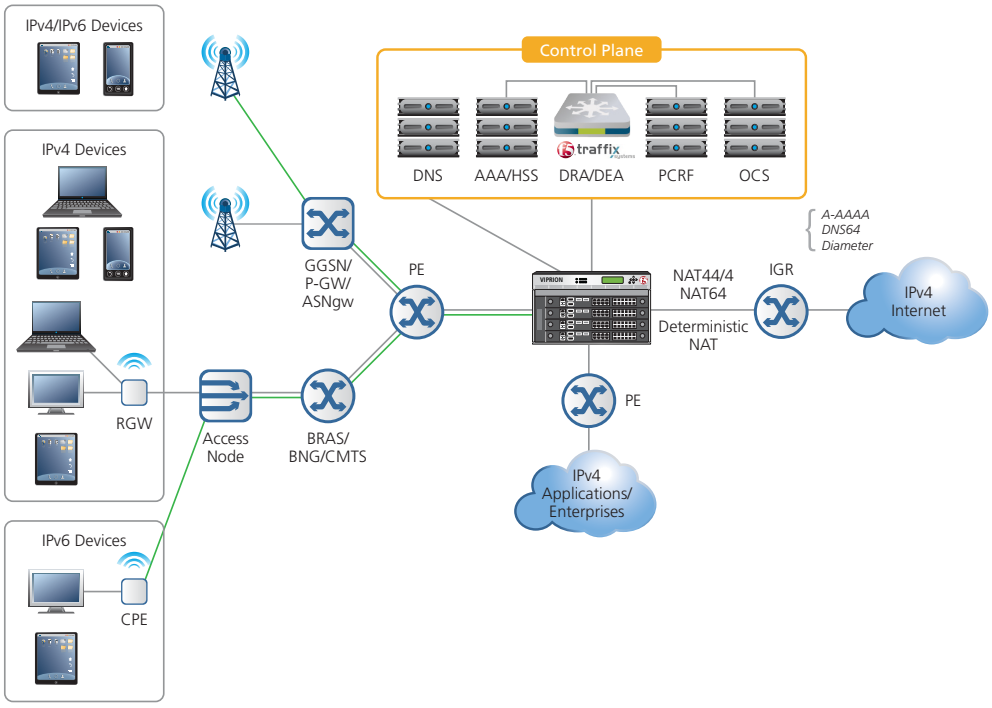

Figure 2: Enable new IPv6 devices to access IPv4 applications and services.

The first scenario, migrating clients to IPv6 or supporting native IPv6 clients such as smartphones and broadband modems, requires that all the clients be able to directly attach to the network and access services via IPv6-enabled pathways. Native IPv6 support for these new devices on the client side involves touching potentially every client device, implementing new access policies across the network, and incorporating new infrastructure services such Dynamic Host Configuration Protocol (DHCP) and Domain Name System (DNS). User access and management tools also need to support an IPv6 environment, or users may lose access to application services that are strictly dependent on an IPv4 network.

Any migration of the installed base of devices will take years to perform due to the replacement lifecycle timeframes. This means that service providers must continue to support existing IPv4 clients as well as new IPv6 devices for network access for the foreseeable future.

In the second scenario of migrating application services to IPv6, it is likely that moving the application servers to IPv6 will reveal some dependencies that potentially affect all users simultaneously if something goes wrong. Even so, most service providers will find it much easier to begin to migrate their applications before their clients, simply because their servers are completely under their control whereas client devices often are not. Because many service providers host a significant number of consumer and enterprise applications such as storefronts, address books, and web portals, they will need to provide support for IPv6 across multiple data centers and externally hosted facilities. In addition, clients will continue for some time to use IPv4 communication for the IPv4-only public Internet.

In reality, migrations are very seldom as clear-cut as either of the scenarios above. More often a combination of IPv6 requirements from different sources will drive the need to migrate: supporting new IPv6-enabled devices while also upgrading application services and the core network infrastructure to support new services running on IPv6. In meeting all of these requirements, maintaining seamless support for all clients across all services is paramount.

As organizations across the globe struggle to transition to IPv6, the critical nature of access and connectivity among devices and services across all networks will increase the complexity of delivering application services. However, some parts of the world, such as parts of Asia, have already migrated to IPv6 and can natively support both clients and applications services—both sides of the network—in an all-IPv6 environment.

The BIG-IP System: A Gateway for Transition

The F5 BIG-IP platform provides application delivery services within service providers' network infrastructure and data centers, ranging from high availability, SSL processing, and caching and compression for server complexes, to more advanced services such as intelligent traffic management, application and network security, and user access management. For all application delivery services, the BIG-IP platform functions as a native IPv4 to IPv6 gateway by transparently managing application delivery in both networking topologies, which enables it to continue supporting advanced services as applications traverse both networks.

IPv6 Migration at the Strategic Point of Control

In a typical deployment, the BIG-IP system is situated in one of two places: in the service provider's core network between the packet gateway and Internet router, or in the data center where applications are hosted. In the core network, the BIG-IP system provides intelligent traffic management, network firewall and other security capabilities, and IPv4/IPv6 solutions. In the data center, the BIG-IP system provides high availability, security, and virtualization services for all application services, making multiple physical servers or hosted services look like a single entity. In either position (both being strategic points of control) the BIG-IP system provides an opportunity to start migrating either clients or servers—or both simultaneously—to IPv6 networks without affecting clients, application services, and both sides of the network all at once.

Initially, most IPv6 migration plans focused on the back-end network moving to IPv6 addresses for application servers and the corporate network. This involved a lot of migrating the private network and on-site application servers in preparation for future IPv6 requirements in applications and with new systems. But as newer IPv6-enabled devices, such as LTE devices that require IPv6 support, begin to penetrate the market, the focus is shifting to supporting those devices in a native IPv6 client-side network. The BIG-IP platform provides centralized IPv6 gateway functions across the entire product suite and on both sides of the network, offering independent and flexible migration solutions regardless of where the organization needs to focus immediate IPv6 support.

Migrating services and application servers

With the BIG-IP system strategically located between clients and servers in the data center, a network administrator can simply add a new "server" network to the BIG-IP system—one that is IPv6-capable. The result is that the network will have IPv4 on the front (client) side of the BIG-IP system and simultaneously support both IPv4 and IPv6 networks behind it.

Once the IPv6 network is established, the service provider can start to migrate its application servers from the IPv4 network. For example, if a particular application uses multiple back-end servers, network administrators can simply take one IPv4 server offline and switch it to IPv6. The BIG-IP platform will handle application delivery requests by load balancing among all servers while continuing to provide IPv4 virtual addresses to the clients. The clients themselves will not realize any difference because they are still contacting and using the IPv4 virtual server being serviced by BIG-IP® Local Traffic Manager™ (LTM) to access their applications.

Once the offline server is switched to IPv6, administrators can bring it back online and add it back to the original load balancing pool with its IPv6 address instead of the old IPv4 address. The BIG-IP system will incorporate new servers in the IPv6 environment, simultaneously providing application availability in this mixed environment, but clients will still use the old IPv4 virtual address to connect to those services. Client requests will now be load balanced across all of the IPv4 and IPv6 servers.

The BIG-IP platform can perform a similar function on a global level across multiple applications and services. As a result, service providers can perform a seamless migration with a centralized IPv6 gateway rather than requiring distributed IPv6 support in multiple internal and external data centers from a number of different vendors.

Supporting IPv6-capable clients in the core network

Service providers can use a similar strategy with the BIG-IP system in the core network to move their clients to IPv6 or support new IPv6 devices while maintaining their existing IPv4 back-end application servers. In this case, along with its IPv4 virtual address that points to its IPv4 servers, the service provider creates a client-facing IPv6 interface with a new IPv6 virtual address that points to those same IPv4 servers. Then, as clients are transitioned to the new IPv6 client network, the BIG-IP system, which provides both NAT64 and IPv6 DNS resolution services, will "hand out" the new IPv6 address of the virtual server, using the same DNS name that previously pointed to the IPv4 address. Because the BIG-IP system supports Dual-Stack Lite (DS-Lite)

termination, service providers can also deploy CPE that uses global IPv6 addresses and encapsulates IPv4 packets into IPv6 tunnels within an IPv6 access network.

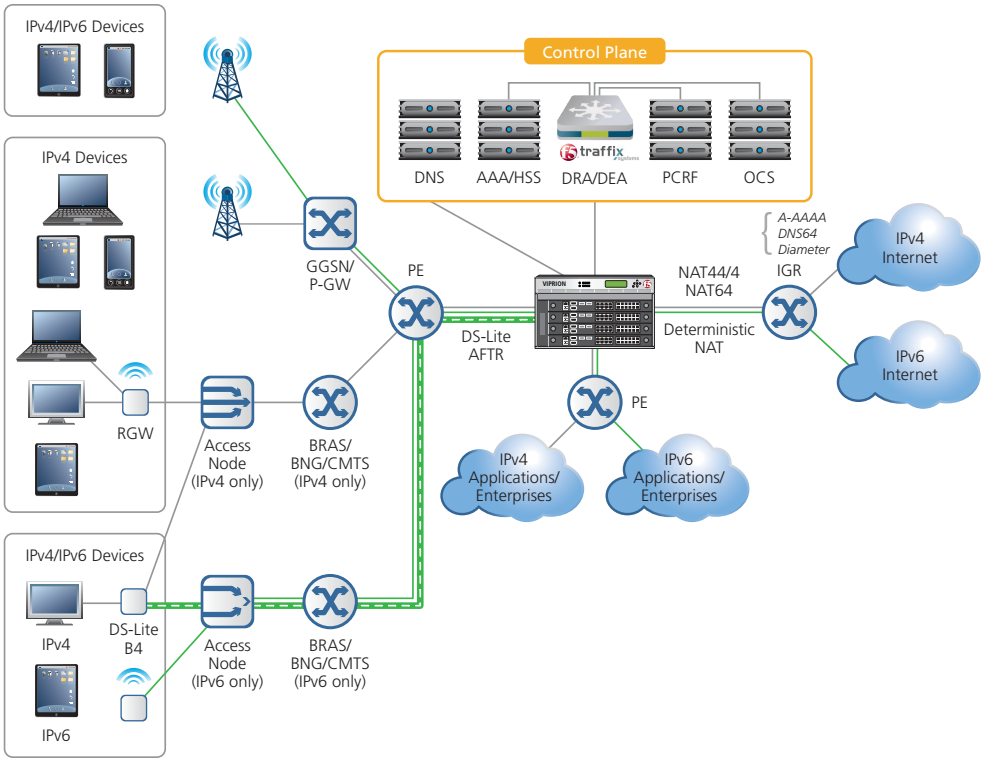

Figure 3: Enable full IPv6 gateway across devices and applications and services.

The BIG-IP platform provides several important additional features that give service providers incremental flexibility and support during their IPv6 migration in the core network. The BIG-IP platform utilizes an event-based scripting language called iRules®, which provides unprecedented control to directly manipulate and manage any IP application traffic. This enables service providers to customize how they intercept, inspect, transform, and direct inbound or outbound application traffic such as adding or adjusting application level gateways on the fly.

BIG-IP solutions also excel at high-performance logging, which is a regulatory compliance requirement for many service providers for IPv6 migrations. In addition, the BIG-IP platform enables very efficient and customizable logs, such as the ability to insert MSISDN/IMSI and destination URL/URI fields into the logs. Another critical factor is the amount of storage space required for such logging, and F5 delivers a very efficient and cost-effective approach.

By using the same host name and back-end servers on both the IPv4 and IPv6 networks, in most cases the clients will be able to start using their old applications as if nothing has changed.

Providing security for IPv4 and IPv6 simultaneously in the network

Throughout the transition to IPv6, service providers must also maintain application and network security. As more types of devices and applications are developed and deployed, more security threats will emerge as well. Seamless and secure application access must be preserved to provide network continuity and prevent new security vulnerabilities from the client side. Meanwhile, as back-end application servers are migrated to the new IPv6 environment, additional services such as network and application firewalls must also be transparently migrated to the IPv6 network. A system that can only provide security for each network topology independently requires that the organization deploy multiple point solutions throughout the mixed networking environment and keep security zones isolated between IPv4 and IPv6 networks.

With the BIG-IP platform, service providers can provide security for both IPv4 and IPv6 servers and applications in a mixed data center environment, where some servers are IPv4-enabled and some are IPv6, regardless of whether those servers and applications require one type of network or the other. The BIG-IP platform enables network administrators to secure access to both IPv4 and IPv6 networks with top-level, high-performance management, including integrated and simultaneous high-speed VPN and SSL connections. As a data center firewall, the BIG-IP platform offers default-deny security and stateful inspection capabilities for defense against more than 30 DDoS attack types at unparalleled scalability.

An ICSA Labs certified firewall, the BIG-IP platform also helps secure the entire service provider network infrastructure and scales to perform under the most demanding conditions. With its TCP Express capabilities, for example, the BIG-IP platform acts as a carrier-grade Gi firewall to protect the radio network from multiple SYN attacks that can result in serious network congestion or even outages. This is a flexible and adaptive solution to the increasing security risks at application and network levels for both IPv4 and IPv6 networks.

IPv6 application awareness

One challenge that service providers often don't deal with until after an application is moved to an IPv6 network is how applications communicate with each other across the network. Many IP-based applications are hard-wired to use IPv4 addresses

and can't work in a mixed IP environment; web-based widgets or HTML5 applications provide an excellent example of application components that are often explicitly bound to one network type or the other. It's not uncommon for a web application to make external calls to other application services for additional functionality, such as "liking" or sharing content, pulling dynamic content from external sources, or calling a specific web-based function such as a java-based chat box. Once the base web application server is transitioned to an IPv6 network, it begins making those external application calls across the same IPv6 network, but the destination applications may not be IPv6-aware or able to function at all on an IPv6 network.

By using the BIG-IP platform, inter-application traffic can be fully proxied between the IPv6 and IPv4 networks, allowing the web application server to make outbound calls over an IPv6 network that are translated to the IPv4 network where the external application data resides. Using the BIG-IP system as a full IPv6 proxy also allows service providers to continue supporting legacy IPv4 applications that would otherwise never work on an IPv6 network. The BIG-IP architecture provides significant flexibility to address service-interrupting migration issues with application level gateways (ALGs), which are configurable filters that enable dynamic mapping of application content to specific IP address and port numbers. Unlike other platforms, the BIG-IP system enables these ALGs to be introduced quickly via on-the-fly configuration updates rather than requiring new software version deployments. In this way, organizations can perform a graceful migration from legacy applications rather than forcing a last-minute crisis as users lose access to those applications.

Consolidating Point Solutions onto the BIG-IP System

The migration to IPv6 does not offer the potential for large new revenue streams like other service deployments. Thus, service providers are motivated to minimize the cost as well as the impact of the migration. At the same time, with the amazing growth and innovation in data networks, service providers have expanded existing legacy platforms and added new ones without a holistic view of the network architecture. In many cases, service providers have needlessly complex networks that cannot scale, have increased deployment and operating costs, and have reduced the ability to add or adapt new services.

The F5 solution offers service providers the opportunity to consolidate multiple service functions into a single platform at strategic points of control to simplify

their networks, reduce their costs and accelerate new services deployment. After deploying the BIG-IP system to support CGNAT and IPv6 migration, service providers can incorporate incremental functions such as network and data center firewall, context-aware traffic steering, and advanced DNS capabilities.

No other IPv6 migration solutions offer this breadth of service functionality on such a high performance and scalable platform.

Conclusion

The transition to IPv6 is something that every service provider will have to deal with. This is due to IPv4 address depletion, but also to new, IPv6-native application services and devices becoming available to end users. The BIG-IP system provides the flexibility for an organization to securely migrate IPv4 network services and clients at its own pace, while maintaining control of the application and network. If some applications can't be moved or don't support IPv6, they can be left on IPv4 until they are replaced or retired. In the same manner, clients that still need to maintain their IPv4 identity can either utilize both networks as needed or can simply continue to use the IPv4 network and access the service provider's IPv6 application services via the BIG-IP platform.

Regardless of when or why IPv6 becomes necessary, F5 provides a seamless, integrated solution for managing a controlled IPv4-to-IPv6 migration throughout the entire service provider network.

F5 Networks, Inc. 401 Elliott Avenue West, Seattle, WA 98119 888-882-4447 www.f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com