VERISIGN™

WHITE PAPER

PREPARING FOR IPv6:
VERISIGN'S PERSPECTIVE

VerisignInc.com

VERISIGN™

UNITED STATES' CHIEF TECHNOLOGY OFFICER, ANEESH CHOPRA AND NTIA ADMINISTRATOR LAWRENCE E. STRICKLING STRESSED, "THE IPV6 TRANSITION IS CRITICAL TO THE CONTINUED GROWTH OF THE INTERNET, AN ENGINE FOR FACILITATING COMMERCE AND ECONOMIC GROWTH. WE WILL CONTINUE TO HIGHLIGHT THE IMPORTANCE OF THIS ISSUE AND ENCOURAGE COMPANIES TO SHARE BEST PRACTICES TO FURTHER IPV6 UPTAKE."

THE ROAD TO IPV6

Starting in 2000, after a relatively uneventful Y2K transition, many network operators turned their attention to the depletion of IPv4 addresses. At the time, the final IPv4 address allocation was predicted for 2009 and the consensus plan was to implement a dual-stack solution where IPv4 and IPv6 would operate simultaneously until IPv4 phased out. Instead, several technologies to bridge the gap came to market and slowed the consumption of IPv4 by a considerable amount. As a result, between 2004 and 2007, only 50 percent of the existing /8 (or IPv4) space was consumed, and the attitude shifted from conversion to IPv6, to conservation of the remaining IPv4 addresses. But now that IANA has allocated the last of the remaining IPv4 addresses as of February of this year, the realization that a migration to IPv6 is unavoidable is starting to sink in for everyone.

OPERATIONAL EXCELLENCE

Verisign has had the ability to handle IPv6 addresses in the .com and .net registries as well as the root zone for nearly ten years. Because these three zones are the most significant on the Internet, Verisign has been steadfast in preparing well ahead of the projected dates for IPv4 address exhaustion. Verisign is committed to ensuring that its services and internal infrastructure are capable not only to transition to IPv6, but also to continuously exceed needs as global connectedness increases.

Gartner, Inc. predicts that by 2015, 17 percent of global Internet users will use IPv6, with 28 percent of new Internet connections running on the protocol. An underlying framework for this transition is the DNS itself – required for provisioning and access to IPv6 content. As a critical provider of DNS infrastructure, "Verisign was an early leader in the DNS registry community supporting the use of AAAA (quad-A) records in our DNS registries," explains Verisign's Vice-President of Product Development, Dan Schonfeld. "As our registrars and other customers accelerate their adoption of IPv6, we will be ready to support not only web sites that use IPv6, but our non-DNS related infrastructure will be ready to support IPv6 as well."

Verisign and most of the world's Internet organizations recommend that companies clear the way for IPv6 by preparing for the interim dual use of both protocols on their networks and systems. While Verisign is committed to dual-stacked operations in the coming years, it has currently adopted a dual-legged approach in order to protect the more mature IPv4 network from the less mature IPv6. "We are in a period of transition, where IPv4 is prominent but IPv6 will be growing rapidly due to the exhaustion of the IPv4 address space," Schonfeld continued.

VERISIGN™

"Verisign's infrastructure will be fully IPv6 enabled to support the next wave of Internet growth. We are prepared to support both IPv4 and IPv6 for all of our customers."

Meanwhile, Verisign is moving forward with plans for native IPv6 support for our customer-facing portals, but are doing so in a cautious and methodical manner to ensure a smooth transition. As Verisign has learned from its broad IPv6 provisions, everyone from infrastructure operators and service providers to application developers and users will have to work together to support and develop IPv6 capabilities, debug issues with new software and applications that are IPv6 only, and refine interworking and transitional co-existence with IPv4. "We have taken a programmatic approach to implementing IPv6 across all of our products and services," explains Mike Kaczmarek, director of Verisign's Program Management Office.

"Our planning and execution is being conducted at both the strategic and tactical levels to ensure that every facet of such an all-encompassing change is accounted for and will support future needs and growth. Even though we have supported IPv6 for a number of years, we recognize that a full dual-stack implementation across all of our products and services has the potential to be disruptive. To that end, we are leveraging our expertise, best practices, structures and agility to ensure our internal and external customers experience a smooth transition as well as service parity between IPv4 and IPv6."

Gartner recommends that all categories of organizations should aim to establish an IPv6 Internet presence and begin to develop a roadmap based on the ability to communicate with external IPv6 endpoints.

The pressure is growing for companies to take action on IPv6. For some, the pressure is internal with a goal to be as technologically current and future-proofed as possible. For others, the pressure is external – a need to keep up with the increasing number of devices requiring IP addresses as consumers adopt mobile and streaming technologies at a blistering pace. For many startups, new services and emerging markets, IPv6 will be the only option and consumers around the world will expect to connect seamlessly with those companies, services and markets.

STRATEGIC PROGRAM FRAMEWORK

Verisign's objective for transition has been to create a dual-legged then dual-stack environment to enable either protocol to work across its products and services. From the beginning, Verisign brought together a team of experts from across the company to ensure that all aspects of the business would be addressed – from the most technical and operational, to our customer-facing services.

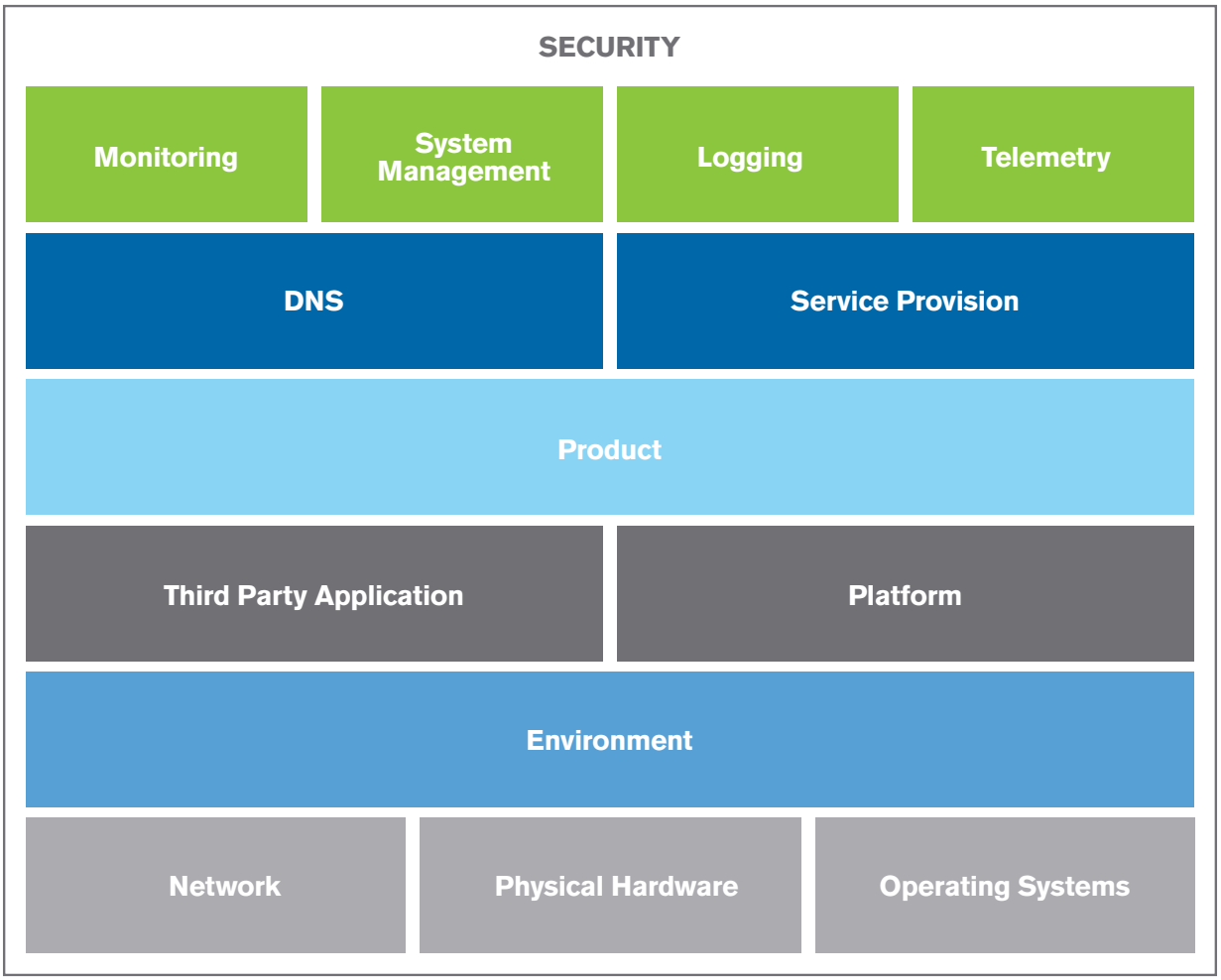
Verisign developed a layered framework to be sure it incorporates all aspects of IPv6 for its business and system environments as it transitions from a dual-legged to a dual-stack infrastructure.

Verisign defined the dual purpose of the layered framework as follows:

- To provide structure for how to think about IPv6 and
- Apply that structure to an approach to address the various efforts it involves

Like most complex efforts, it's daunting to look at the total amount of work all at once. Instead, Verisign has defined a framework that addresses all areas of both an Internet and Enterprise IT infrastructure that need to be addressed when implementing IPv6. The completion of only a single layer or component of this framework does not constitute full IPv6 readiness. The framework addresses the components necessary to operate any Internet or Enterprise IT implementation. This framework can be applied to any business with few changes – no matter the size or the industry. Taken together, this framework helps a company prepare for the transition in a systematic way, while keeping an eye on the big picture. The following tables provide details for each major layer of the framework and the considerations that Verisign has encountered in our work, as well as other considerations to the process.

STRATEGIC PROGRAM FRAMEWORK



VERISIGN™

INFRASTRUCTURE

The base layer of the framework is your principal infrastructure. Infrastructure serves as the primary physical, logical and network building blocks upon which any IT service functions. For any Internet or Enterprise implementation, ensuring your key components are capable of supporting IPv6 in the manner for which you intend to deploy is paramount for a successful implementation.

Framework Layer	Definition	Examples	Areas of Investigation	Key Considerations
Network	The essential components of an Internet or Enterprise IT environment that interconnects all systems and services facilitating the sharing of resources and information. Composed of, but not limited to the following components: routers, switches, load-balancers, and quality of service devices.	• DMZ • Protected Network • Management Interface	• IPv6 network devices and transport • Load balancing, routing and transit/circuits • IP management • Dual-stacked or dual-legged approach	1. Is IPv6 being offered by your service providers for transit? 2. As you refresh hardware across your enterprise, are your vendors offering IPv6 support for upgrades of devices? 3. What will your test and certification cycle for IPv6 support of hardware look like? 4. Which attributes does your team consider most critical to test for? 5. What is your approach to IP address management with IPv6? 6. Are you familiar with server settings such as Path MTU and it's implications? 7. To what extent is your network, both internal and external, IPv6 ready? 8. What is the priority of infrastructure upgrades; e.g. are you looking at "barrier" devices such as intrusion detection services and firewalls first before addressing servers and operating systems?
Physical Hardware	A physical host installed to perform a specific function or combination of functions in support of a service offering. Includes virtualization of systems on a single server.	• Intel-Based Server • Commodity Server • Hypervisor • Virtual Machine	• Readiness of physical systems • Readiness of virtual systems	
Operating System	Primary building blocks implemented on servers and/or network components to perform a specific purpose or allow for the implementation of additional applications and services.	• Linux • Windows • BSD • AIX • Solaris	• Specific routing settings required within operating systems	

VERISIGN™

ENVIRONMENT

The environment layer is the combination of the base infrastructure components that perform either a specific purpose, function, or meet the need of a specific audience. No environment is the same. Therefore, it is essential that you address the implementation of IPv6 across your architectures and implement it in a manner that ensures you can validate the deployment as well as test for anomalies that may arise.

Framework Layer	Definition	Examples	Areas of Investigation	Key Considerations
Environment	The combination of systems built within a network framework to serve a specific purpose or function.	• Development • Quality Assurance • Production	• Architecture designs reflecting IPv6 related changes	1. How far are you ready to extend native IPv6 transport into your organization? 2. Are each of your teams capable of implementing IPv6 with assurance? 3. Do your developers have the access and tools they need to build IPv6 capable services? 4. Are your testers working in an environment that replicates the manner in which you plan to deploy IPv6 for your products and services? 5. Will your production environments support end users accessing services over native IPv6 transport?

VERISIGN™

APPLICATION

The application layer is the most diverse layer for IPv6 consideration. IPv6 implementations here can range from third-party products that serve a function or purpose to custom applications that contribute to your unique business value or the delivery of your products and services. Regardless of the type or combination of applications implemented, taking future IPv6 considerations into account now instead of deploying what works for now may minimize substantial rework down the road.

Framework Layer	Definition	Examples	Areas of Investigation	Key Considerations
Third-Party Applications and Platforms	A product or service (commercial or open source) implemented in an environment performing a specific function for the development and implementation of additional processes or components.	• ORACLE • SQL Server • Apache • .NET • MQ	• Versioning to provide necessary IPv6 support • Library revisions for either dual-legged or dual-stacked implementations	1. What do your application developers require from their environment to execute their full SDLC when introducing IPv6 readiness to your products? 2. What are the architectural decisions that you have to take into account when assessing software platforms, addressing both the capabilities of your infrastructure and the needs of your applications? 3. What is the priority of third party software upgrades with respect to your overall product life-cycle roadmap? 4. What third party software will your application developers need in order to engineer applications with IPv6 support?
Platforms	An application framework developed internally and specifically designed for the development and implementation of additional processes or components associated with a specific product or service offering.	• ATLAS (a Verisign technology)	• Internal versioning to provide necessary IPv6 support • Internal library revisions for either dual-legged or dual-stacked implementations	

VERISIGN™

PRODUCT

Products are the aggregation of a service, protocol or function offered directly to the market. IPv6 impacts in this area are substantial. As more and more end-users and customers migrate to, enter or integrate IPv6 into their everyday usage, it becomes essentially important that your offerings do the same.

Framework Layer	Definition	Examples	Areas of Investigation	Key Considerations
Product	An offering made directly to the market.	• Web Hosting • Email • Managed DNS • Ecommerce	• IPv6 interactions between all other services within your network • IPv6 interactions between all other services outside of your network (partners, customers, etc.) • IPv6 integration with end-user's products and services	1. Is what you sell affected by the migration to IPv6? 2. To what extent do the unique attributes of IPv6 and the state of its global implementation allow your products to be extended into new markets? 3. Does IPv6 provide you with new markets in which to operate?

VERISIGN™

INTERNET-FACING INTERFACES

The most critical component of the framework, your Internet-facing interfaces are those that will be affected by the transition to IPv6 first. As the fifth layer of the framework, it is very easy to address this first and stop. For many, this may be the only area that requires change. However, to be certain that your products and service are fully IPv6 capable, investigating the impacts of IPv6 at all layers is the most sound approach.

Framework Layer	Definition	Examples	Areas of Investigation	Key Considerations
DNS	The primary Internet routing mechanism that ensures end-users can access your protocol, website, portals, application programming interface (API) or any other service required to operate and maintain your business.	• Verisigninc.com • Anycompany.com • Anyservice.net	• Implementation of both A-records and AAAA-records (Quad-A) for DNS resolution	1. What is your principal business and what public interfaces does it offer? 2. Which contracts govern your business and which stipulations do they make about IPv6 delivery? 3. Are there any Service Level Agreements that you need to consider maintaining as you begin to incorporate IPv6 into your organization? 4. For your public interfaces, have you evaluated all of the options for offering IPv6 in a dual-legged or dual-stacked manner?
Service Provision	The principal service that your business offers to the market through protocols, websites, portals, APIs, etc. or all of the above.	• Website • Data transfer portal • Product provisioning API	• Extending the dual-legged IPv6 service already offered • Ensuring no degradation of service or service level agreements (SLAs) while migrating customer-facing interfaces to being dual-stacked	

VERISIGN™

HYGIENE SERVICE

The most overlooked component of any environmental or product implementation, hygiene services provide the necessary information on an environment, system or service allowing you to determine if they are performing to expectations. The components of hygiene services are an indispensable part of conducting business. While many of these services do not impact customers directly, their disruption could be highly problematic by resulting in an inability to determine your service's availability or performance.

Framework Layer	Definition	Examples	Areas of Investigation	Key Considerations
Monitoring	Tools and processes in place to ensure that critical applications and services perform as expected.	• SNMP • Nagios • Netcool • Tivoli	• Monitoring for IPv6 network and systems equivalent to IPv4	1. Which tools does your operational staff require in order to ensure your business is running? 2. Are the tools you use able to identify and manage IPv6 hosts and traffic? 3. How significant is identifying a client IP address to your business and your applications? 4. At the network and traffic layer, which metrics and forms of telemetry are valuable and drive decisions in your enterprise?
Systems Management	Utility servers and/or services that enable management of hosts and applications.	• NetIQ • System Center	• Distributed system access over IPv6 networks in concert with IPv4 networks • Under what protocol will new equipment be deployed and managed	
Logging	Periodic and real-time data on the activity of a particular device or service.	• Syslog • Chronlog	• Writing and interpretation of IPv6 hosts consistent with those that are IPv4 • Alignment between IPv6 and IPv4 hosts from a specific customer or provider	
Telemetry	Metrics used to measure and auge valuable information, specifically related to network traffic.	• Source location • Route	• Volume of requests originating from IPv6 networks vs. IPv4 networks • Network route of services on both IPv6 and IPv4	

VERISIGN™

SECURITY

Security must be a primary consideration for IPv6 operations. Sean Leach, Vice-President of Product Development at Verisign explains, "The deployment of IPv6, from a security perspective, must be done with caution. We have heard several stories of enterprises not taking the same precautions with IPv6 as they have with IPv4, and it opened up a huge hole in their defenses. Bad guys know that enterprises are not locking the doors on IPv6 like they have on IPv4 and are adjusting their tactics to take advantage of that." Leach also advises, "DDoS (distributed denial of service) protection is just as important for IPv6 as it is for IPv4. If an enterprise's DDoS defenses are not designed for IPv6 (either done in-house or outsourced), it's as bad as not having DDoS defense at all."

Framework Layer	Definition	Examples	Areas of Investigation	Key Considerations
Network Security	Policies, processes and/or monitoring intended to prevent unauthorized access to an Internet or Enterprise IT environment, service, system or application.	• Access Control Lists • Authentication • Firewall	• Auditing of both IPv4 and IPv6 access reducing unauthorized access	1. What is your information security strategy for addressing potential new IPv6 originating attack vectors? 2. Are you informed of IPv6 related vulnerabilities and do you have a strategy for addressing them? 3. Do you have the necessary tools to analyze your enterprise today? 4. Given the scale of IPv6 address space, what is your approach to security scanning?
Application Security	Tools, policies, processes and/or procedures deployed as part of application implementations intended to minimize or prevent the unauthorized use and/or access to critical data.	• Input validation • Authentication • Session management	• Hardening application to minimize IPv6 related exploits	

TARGET STANDARDS

Transition to IPv6 is a project where the adage "measure twice, cut once" holds true. The primary undertaking to help ensure success is to prepare your plan well. First of all, gather a team with members from every area of the business. The National Telecommunications and Information Administration (NTIA) names IT as one of the primary teams of course, but it is also important to involve customer care, internal application developers, website managers, product management and any other group that you think may be impacted. The project manager should assign the department representatives the task of naming every function, process or service that may be affected by the transition. It's crucial that this is handled by those from each respective department because, as the experts within their area, they will be able to identify key considerations, spot abnormalities and propose solutions.

It's critical that in addition to cross-department input, companies assure that necessary in-house budget support and tools are provided for testing and monitoring of IPv6 applications using dual-legged or dual-stacked systems and network configurations.

Of course no project can be complete until the stated objectives are met. For the IPv6 transition, Verisign developed a set of specific goals to help define success and mark completion of certain tasks. While the ultimate goal is to ensure that internal and external customers do not see a difference in service whether they connect over IPv4 or IPv6, the following checklist of Target Standards have been helpful guideposts as Verisign works toward the finish line:

- All customer-facing services are reachable over IPv6 transport, including protocols, user interfaces, and portals
- Monitoring for IPv6 traffic is of the same caliber as IPv4
- Service level agreements are not adversely impacted
- Required internal environments such as quality assurance and pre-production are provisioned as dual-stack to support necessary re-architecting
- Both information and system security across services are adapted for the IPv6 network
- Systems are able to identify and mitigate IPv6-originating vulnerabilities and threats
- Compliance with industry standards, regulations and government mandates for IPv6 readiness
- Training conducted for handling IPv6 for engineering, production services and customer care staff

RESOURCES FOR NEXT STEPS

The time has come to get to work – The global hunger for digital mobility, social connectedness and on-demand entertainment will not abate. Emerging countries are modernizing rapidly and the Internet is playing a critical role in their advancement politically, socially and commercially. The Internet blurs our global borders and people continue to connect from every facet and corner of the world. The use of IPv6 will inevitably increase and consumers will demand uninterrupted access to all that the Internet brings.

"Coupled with the continued deployment of DNS Security Extensions (DNSSEC), IPv6 will ultimately provide the stable and secure base for the future Internet," said Danny McPherson, Verisign Chief Security Officer. "But, for the transition from IPv4 to IPv6 to be successful, everyone from infrastructure operators and service providers to application developers and users will have to work together on a range of activities."

As an experienced operator of IPv6 technologies, Verisign will be actively involved in the global adoption of IPv6. We will be releasing additional resources and information for enterprises planning their own transitions.

LEARN MORE

For more information, please visit www.verisigninc.com/IPv6

ABOUT VERISIGN

Verisign is the trusted provider of Internet infrastructure services for the digital world. Billions of times each day, companies and consumers rely on our Internet infrastructure to communicate and conduct commerce with confidence.