

White Paper

Enabling the Next Generation of Networking with End-to-End IPv6



Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408.745.2000
1.888 JUNIPER
www.juniper.net



Microsoft Corporation
One Microsoft Way
Redmond, Washington 98052
www.microsoft.com

Table of Contents

Table of Contents	2
Executive Summary	3
Introduction	3
The Changing Expectations of IPv6	3
What Hasn't Changed?	3
What Is Changing?	4
Why?	4
New Applications and Services without Boundaries	5
Classic Applications and Service Limitations	5
Supporting New Applications and Services	5
An Example IPv6 Application	6
Overview of Microsoft Windows Meeting Space in Windows Vista	6
Windows Meeting Space and IPv6	7
Conclusion	8
Components of a Successful IPv6 Implementation	8
IPv6 Capable Applications	8
Production-Quality IPv6 Infrastructure	9
Comprehensive and Performance-Optimized IPv6	9
Flexible IPv6 Transition Mechanisms	9
Comprehensive IPv6 Security	10
Application Layer	10
Customer Premises	10
Infrastructure	11
IPv6 Management Tools	11
IPv6 Deployment Considerations	11
Transition Functionality	12
Transitional Deployment Scenarios	12
IPv6-Capable Products – Today	14
Microsoft	14
Operating Systems -- Windows Vista and Windows Server	14
Juniper Networks	15
Routing and Migration Products	15
Firewalls/VPN Security Devices	16
Conclusion	17
Further Reading	17
About Microsoft	18
About Juniper Networks	18

Executive Summary

As connectivity converges and develops ubiquity many devices are added to the Internet. This trend has created projections of address shortages. Internet Protocol version 6 (IPv6) has promised a solution to this issue. In this paper, Microsoft and Juniper combine their leading networking knowledge to show customers how to adopt IPv6 technology. The paper first looks at the changing expectations of IPv6 with the growth of IPv6-enabled applications like Microsoft Windows Meeting Space in Windows Vista. Next the paper discusses the relationship of each component in an IPv6 implementation. The paper closes with some suggestions on functionality, equipment and deployment scenarios that highlight key aspects of a robust end-to-end IPv6 transition.

Introduction

Since its initial deployment, Internet Protocol version 4 (IPv4) has become the standard network-layer protocol used by the global Internet and a vast majority of computer networks worldwide. This version of IP has served the Internet community well for many years. However, with the increase in global communications and services and the development of many new Internet applications, IPv4 is starting to reach its limitations. The next-generation IPv6 has been designed to replace IPv4 by addressing many of the existing IPv4 limitations, as well as providing a wide range of operational benefits and superior support for advanced applications.

Since 2003, the U.S. Department of Defense (DoD) has been aggressively pushing the planning and adoption of IPv6 technology. As part of its “Network-Centric Warfare” push, the DoD envisions that IPv6 will help with the enablement of worldwide military operations and future defense network transformations. As such, the DoD requires all DoD-purchased networking products be IPv6 capable by 2008. Taking this effort a step further, the Office of Management and Budget (OMB) has started moving government departments and agencies toward IPv6. Another example of government support for IPv6 adoption is Japan’s tax incentives for businesses that deploy IPv6-capable network devices.

Whether driven by necessity or by government mandate, IPv6 is fast approaching. Microsoft and Juniper Networks are working together to help simplify the transition to IPv6 while preserving and enhancing both security and reliability.

The Changing Expectations of IPv6

The original Internet Engineering Task Force (IETF) Requests for Comment (RFC) on IPv6 were written in the early to mid 1990s. Much of this activity was based on concerns with the growing number of computer networks and their associated hosts on the Internet. Various intermediate technologies like Classless Inter-Domain Routing (CIDR), Network Address Translation (NAT), IP security (IPsec), and other extensions helped to address the limitations, but are now reaching their own limits of effectiveness.

What Hasn’t Changed?

As a primary driver of the original IPv6 protocol design, the need for more addresses continues to hold true today. Expanding methods of communication are fueling a global trend to exchange information across the backbone of the Internet. The phenomenon that started with the adoption of the Web has fueled revolutions in consumer electronics, telecommunications, and enterprise computing. With potentially billions of devices communicating across millions of networks, there will be an increased demand for citizenship on the global communication grid.

With widespread growth of networks and communication devices in the Asia Pacific (APAC) region, there is an increased demand for IP addresses. As markets mature and innovate in Japan, Taiwan, and Australia, there is an even faster user adoption rate in countries such as China, Korea, and India. This rapid growth is creating unique challenges for the APAC region due to the very limited number of IP addresses assigned to them during the early days of address allocations.

Forward-thinking IT managers are looking to IPv6 technology for clean integration and coexistence with existing infrastructures through advanced capabilities such as addressing, tunneling, and translation. IPv6 solves this challenge by enabling increased network and application security, which helps protect the handling and transmission of sensitive information.

The U.S. Federal government mandate for implementation of IPv6 in DoD networks is another early IPv6 driver that continues to remain important as the mandated 2008 conformance deadline approaches. A few other original IPv6 drivers include the expanding use of 3G mobile devices, Internet Multimedia Subsystem (IMS) for converged networks, and online gaming – all of which are now adding momentum to attach more devices to the Internet, thus consuming more addresses.

What Is Changing?

So, if the original drivers for IPv6 are still true, then why has it taken so long for any organization to take the next step and transition to IPv6, and why the sudden renewed interest?

One part of the answer can be attributed to a need for breaking in untested IPv6 protocols in laboratories and across various test networks around the world to help make it ready for production environments. Another part of the answer is how successful the intermediate technologies like NAT and CIDR have been in helping to ease the address depletion concerns.

What has really changed from these earlier drivers of IPv6 has been the new expectations service provider and enterprise customers have for the next-generation IPv6 technology. Overall, IPv6 provides a new technology that delivers a strategic platform for flexible network-centric applications. In order to deploy this new system and continue providing mission-critical communications and services, organizations expect IPv6 to enable their global networks to keep pace with new demands for IP-based applications. This requires increased performance, higher availability, and improved quality of service.

Why?

IPv6 is no longer just about future-proofing all aspects of converged communications. Rather, IPv6 deployment is about providing a robust and flexible infrastructure that can support a new generation of applications. IPv6-enhanced applications such as Microsoft Windows Meeting Space (discussed later in this paper) enable even closer collaborative computing experiences for organizations around the globe.

New Applications and Services without Boundaries

The early days of IPv4 networks supported applications that were primarily simple text-based exchanges. With technology advancements, more sophisticated end users, and organizations that are expanding their computer networks, a new breed of applications is emerging. These new applications are enablers for the collaborative computing experience organizations require to fulfill their missions.

Classic Applications and Service Limitations

Most of the initial IPv4 applications that were text-based and normally accessed from a fixed user location include email, newsgroups using Network News Transfer Protocol (NNTP), and Internet text browsers such as Mosaic, Gopher, and LYNX.

The shift from narrowband to broadband technology, and the associated increased bandwidth available to users was driven by the introduction and rapid adoption of graphical Internet browsers such as Netscape Navigator, AOL, and Internet Explorer (IE). This increased bandwidth availability, combined with enhanced remote access technologies such as Secure Socket Layer (SSL), Virtual Private Networks (VPNs), and the growing implementation of Wireless Local Area Networks (WLANs), will continue to enable the emergence of more mobile Internet capabilities and faster adoption of applications such as Voice over IP (VoIP) and IP-based collaboration products.

The introduction and maturation of IPv4 brought many significant developments that enabled instantaneous communication. These include technologies such as dynamic routing, the standardization of IP over all types of transmission media, and the use of Multiprotocol Label Switching (MPLS).

However, the inherent properties of IPv4 present service limitations like, for example, a limited IP address space in the IPv4 datagram's header. With this restriction, many organizations have created private internal addressing schemes and use NAT at the periphery between private and public networks. While NAT has helped to temporarily handle the IP address limitation of IPv4, it also has added complex challenges to network managers. These network managers are struggling with network scaling and management issues as their networks continue to grow both in size and interconnections to other networks.

A final service limitation with IPv4 is the lack of an integrated security mechanism for IPv4 transmitted data, as today's solutions employ a plethora of different approaches.

Supporting New Applications and Services

IPv6's address auto-configuration or plug and play capabilities will make it unnecessary for network managers or end users to configure IPv6 devices when they are connected to a network. This is a huge win for the growing number of mobile networks. With the widespread deployment of IPv6 and the use of its integrated IPsec technology, mobile network users will have the freedom to take advantage of inter-device communication capabilities between PCs, intelligent devices like PDAs, and cell phones. This peer-to-peer networking model will provide a rich environment for new types of communication and collaboration, while also ensuring end-point authentication and data integrity during communications. In addition, ad-hoc peer-to-peer communications will be much easier to establish between co-workers or associates during normal or crisis situations.

The incorporation of Type of Service (ToS) mechanisms into IPv6 will help networks provide better quality of service to new applications by providing lower latency and jitter to these applications during their transport across the network. Through traffic identification using a flow label field in the IPv6 header, routers will be able to identify and provide special handling for packets belonging to a flow (a series of packets between a source and destination). For example, the improved quality experienced by users during the distribution of IP-enabled video and voice collaboration applications will help guarantee user satisfaction and improve employee productivity. The enhanced support for security in IPv6, through integrated IPsec capabilities, will further help ensure a standard and reliable security framework at the IP layer, rather than on a per-application basis. IPsec also enables authenticated communications with integrity protection (end-to-end) without the need to tunnel or encrypt the traffic. This capability can eradicate “man-in-the-middle” or other spoofing attacks.

By taking advantage of these closely integrated IPv6 features, users will be able to expand beyond the constraints of today’s IPv4 networking environments and participate in a much richer set of communication methods.

An Example IPv6 Application

Factors fueling the growth of IPv6 include

- An increasing number of PC users within all types of organizations
- The explosion of non-PC electronic devices
- An increasing amount of time that end users spend online in order to get their jobs done effectively

Of particular interest is the growth of pervasive collaborative computing applications that are enabling new computing and communication experiences for all of these users and new devices.

Overview of Microsoft Windows Meeting Space in Windows Vista

Collaborating across groups can be difficult. The common methods users employ when they need to work together on a document are printing paper handouts, sending files to individuals by email or instant messaging, uploading files to common network shares, or sharing a USB flash drive. Each of these methods has limitations and inconveniences. The Microsoft Windows Meeting Space feature in Windows Vista simplifies common activities faced during business meetings, presentations, and collaborative sessions. Windows Meeting Space gains many advantages from its use of IPv6. Moreover, available transition technologies ensure that this mainstream application can safely rely on IPv6 on existing networks, long before the protocol is deployed natively.

Windows Meeting Space operates entirely peer-to-peer, so it can be used on any network, including enterprise networks and public hotspots. Where connectivity is not available, the feature automatically creates an ad-hoc wireless network among the meeting participants. Windows Meeting Space utilizes several services provided by the Windows peer-to-peer networking platform, including:

- **People nearby and application invite:** The ability to discover nearby people and send invitations to initiate multi-party activities.
- **Serverless name resolution:** The Peer Name Resolution Protocol (PNRP) enables secure advertisement of machine, user, or application resource names either on a local subnet or over the Internet.
- **Multi-party messaging and data synchronization:** The ability to create secure multi-party groups that share a replicated data store.

In addition, the feature uses Web Service Discovery (WSD), Windows Distributed File Replication Service (DFRS), and Windows Remote Desktop Protocol (RDP) to respectively support meeting session discovery, file exchange, and desktop/application streaming. The following figure shows an example of using Windows Meeting Space to modify a presentation.

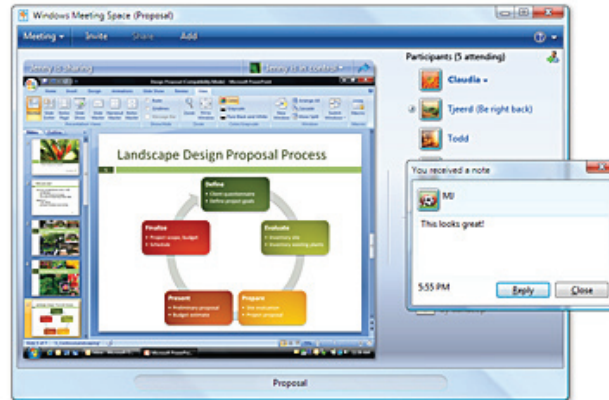


Figure 1: Windows Meeting Space

Windows Meeting Space and IPv6

By using IPv6, Windows Meeting Space gains several advantages:

Ubiquitous addressing: IPv6 allows every Windows Meeting Space participant to have a unique global IP address. Though Windows Meeting Space is typically used on a single LAN or an ad-hoc wireless network, the ubiquitous addressing feature supports meeting sessions that cross subnets or even span the Internet. By allowing each host to have a unique address, IPv6 ensures that all Windows Meeting Space users can ultimately connect to each other without conflict. In the IPv4 world, the lack of available addresses has prompted the use of NAT devices that assign private, or hidden, addresses to each host. Unfortunately, these private IPv4 addresses are not globally unique or routable, so client hosts cannot easily communicate with each other.

- **Improved connectivity:** IPv6 facilitates improved end-to-end connectivity, enabling Windows Meeting Space sessions throughout an enterprise and even over the Internet. Microsoft Windows Vista provides technologies such as Intra-Site Automatic Tunnel Addressing Protocol (ISATAP) and 6to4 that allow IPv6 connectivity to be rapidly deployed over an existing IPv4 enterprise network. For end-user environments that utilize NAT, the Teredo capability in Windows Vista allows IPv6-aware hosts to tunnel traffic to each other, traversing those NATs. By contrast, IPv4 developers must often build and deploy custom solutions to achieve universal connectivity.
- **Automatic address configuration:** IPv6 enables Windows Meeting Space to deliver a fast and smooth ad-hoc networking experience. For each active network interface, clients automatically generate a unique link-local IPv6 address (suitable for communicating with other hosts on the subnet) without relying on the presence of a router or DHCP server to centrally assign addresses on that network. This address allocation scheme ensures that hosts can begin to communicate without any delay upon creating an ad-hoc wireless network or upon plugging into a network hub or switch. Although IPv4 supports ad-hoc networking, automatic network setup is traditionally slow.

- **Native support for security (IPsec):** IPv6 provides native support for IPsec. When IPsec is combined with Microsoft's Active Directory technology, Server and Domain Isolation can be deployed. Server and Domain Isolation enables administrators to dynamically segment their Windows environment into more secure and isolated logical networks based on policy and without costly changes to their network infrastructure or applications. With this additional layer of policy-driven protection, applications are now able to operate with reduced risk over both public and private IP networks. For more information on Server and Domain Isolation, visit <http://www.microsoft.com/sdisolation>.
- **Compatibility with emerging government and national standards:** Several government organizations, like the United States Federal government, have mandated a transition to IPv6 for their internal systems. At the same time, because of the short supply of IPv4 addresses, ISPs in various parts of the world—particularly Asia—are deploying native IPv6 support to their enterprises and consumers. By using IPv6, Windows Meeting Space can be deployed confidently with the knowledge that it will be compatible with these technology mandates.

Windows Meeting Space relies on IPv6 to provide ubiquitous addressing, improved Internet-wide connectivity, and rapid auto-configuration in ad-hoc network environments.

IPv6 helps to future-proof Meeting Space for deployment within evolving network environments worldwide. Though many developers have feared relying on IPv6 because of its limited deployment, Windows Meeting Space demonstrates that IPv6-based applications can still operate in existing IPv4 environments by relying on a combination of transition technologies (such as ISATAP, 6to4, and Teredo) and automatic link-level operation. Most importantly, IPv6-based applications require little or no new network configuration.

Components of a Successful IPv6 Implementation

IPv6 was designed to address the scalability and configuration challenges of IPv4 and to help refocus communication capabilities back to the original TCP/IP goal of global networking. There is no doubt the Internet will continue its exponential growth, and sophisticated end users around the world will quickly adopt more intelligent IP-enabled devices and the applications that support their daily activities.

Some network managers are already in the process of deploying IPv6 into their backbone networks, while many are still finalizing their transition plans. Whether IPv6 implementation is already in process or still in the planning stage, these network managers must clearly understand the components of an IPv6 implementation and how each of the components relate to each other.

IPv6 Capable Applications

Perhaps the most relevant and certainly most pervasive component of the IPv6 implementation will be the actual IPv6-capable applications themselves. The development and deployment of IPv6 protocol-based products is occurring throughout many organizations worldwide. Many of the new capabilities of IPv6 discussed earlier in this paper are expected to drive the rapid adoption of IPv6 throughout these organizations.

New applications will embrace IPv6 across many fronts. In addition to utilizing the increased address space capability from IPv6, new applications will take advantage of the many feature enhancements within IPv6 to help bring back end-to-end controlled communications across a transparent network infrastructure. To ensure optimum performance, applications will need to implement a dual-stack architecture in which IPv4 and IPv6 protocols share a common transport and framing layer. Applications can leverage this new protocol by writing to IP-independent Application Programming Interfaces (APIs) that will automatically use either IPv6 or IPv4. In some cases, where the application exposes network configuration options through the user

interface, extended configuration support for IPv6 networking might be required. Applications will also be able to take advantage of additional capabilities such as the integrated IPsec features for Internet Key Exchange (IKE) and data encryption, as well as the ToS features to provide an array of service levels that are consistent from end to end.

Production-Quality IPv6 Infrastructure

Transitioning from IPv4 to IPv6 will be important, because IPv6 will provide organizations with a network infrastructure that is more scaleable and secure than previously. IPv6 can provide a robust foundation for the 21st Century information age, marked by a global economy and an era of network transformation. Therefore, the second important component of an IPv6 implementation is a robust infrastructure that provides a broad range of IPv6 features covering both network and security functionality to enable real-world deployments.

Comprehensive and Performance-Optimized IPv6

IPv6 has many possible deployment scenarios and its deployment to date in service provider networks, enterprise networks, research networks, and government networks around the world has reinforced that fact. As in IPv4, the deployment paradigm may vary between applications. For example, a service provider may take a different approach to IPv6 adoption than an enterprise.

To accommodate the wide range of deployment scenarios, an IPv6 solution should incorporate a broad set of IPv6-enabled networking and security equipment that can ensure high levels of network reliability and performance, while offering simplified network configuration and operations through a wide range of integrated operational tools such as Command Line Interface (CLI) and APIs.

To help cover an IPv6 implementation throughout an organization (premises/edge/core), networking and security equipment must also extend a full range of IPv6 functionality and simplicity across multiple platform types that are interoperable between themselves and other vendor products. Because IPv6 has moved out of the lab and into mission-critical environments, any solution must deliver production-quality levels of availability along with the necessary tools to help enable a seamless integration and coexistence with existing environments.

As IPv4 and IPv6 will co-exist in networks for some time, a dual-stack implementation that allows simultaneous support for both IPv4 and IPv6 hosts will help provide a smooth transition to all parts of an enterprise network.

Finally, to help ensure an optimum environment for applications, IPv6 networking and security equipment must provide a performance-optimized IPv6 environment through ASIC-based hardware assisted forwarding and a separation of control/forwarding mechanisms.

Flexible IPv6 Transition Mechanisms

Integration and transition tools and mechanisms play a key role in simplifying operations and minimizing costs when introducing IPv6. An IPv6 infrastructure portfolio must provide extensive transition mechanisms like NAT/NAPT (Network Address and Port Translation) as well as a broad range of MPLS-based options for tunneling IPv6 traffic that will ease the burden of converting from IPv4 to IPv6.

Security products located at customer premises must also offer 4 to 6 and 6 to 4 tunneling, as well as 4 to 6 and 6 to 4 translation. These dynamic translation capabilities will allow enterprise organizations to integrate IPv6 without having to replace their existing IPv4 network infrastructure. Platforms will need to ensure IPv4 and IPv6 coexistence will not create any performance trade-offs.

Finally, infrastructure platforms will need to provide service provider and enterprise networks with an IPv6-capable mechanism for transporting existing Time Division Multiplexing (TDM), or circuit-based, traffic across the IP infrastructure. That is because this installed base will still be migrating towards an all-IP environment during this IPv4 to IPv6 transition.

Comprehensive IPv6 Security

As IPv6 is deployed into an existing network, the ability to secure both the information and the systems that carry it is crucial. This is especially true in today's environment of heightened cyber-threats and even more so for critical government network infrastructures.

Thus, another important component of a successful IPv6 implementation is a comprehensive security implementation that can create a trusted IPv6 environment, all the way from the actual application itself, across the customer premises, and across the network, end to end.

Application Layer

Utilizing IPv6, applications can take advantage of the new security features that solve some of the issues discussed earlier. A few of these enhanced IPv6 security features include better protection against address and port scanning attacks and a requirement for all IPv6 implementations to support IPsec for authentication and/or cryptographic protection of IPv6 traffic.

IPsec is centrally controlled with administrative policy, such as Microsoft Group Policy. The configuration of this policy is directly applied to the operating system. This removes the need for applications or administrators to pay special attention to network-level security with new features that configure and control IPsec. It also makes IPsec deployment uniform and consistent across the enterprise or government organization.

Customer Premises

Whether looking at a remote branch, regional office or a central site, the use of production-grade security appliances and systems is paramount. These security appliances are required to implement network security policies, including firewall access control, VPN encryption, and traffic management at all relevant locations.

The firewalls will act as a first layer of security by controlling who and what has access to the network, employing user access control and authentication, providing network segmentation and user containment through secure virtual segments, and protecting against Denial of Service (DoS) attacks by leveraging stateful inspection capabilities. The next layer of protection uses a VPN solution for encryption of communications traversing an untrusted medium that may include the Internet or an internal network segment. Finally, these security appliances will need to provide additional protection from a variety of threats, including viruses, worms, backdoors, Trojans through antivirus, Web filtering, and anti-spam methods.

As organizations transition from IPv4 to IPv6, they will need to implement security appliances that can provide these stateful firewall and IPsec VPN capabilities for IPv4 and IPv6 traffic. These appliances will also need to provide full IPv6 protocol support, many of the transition mechanisms, and traditional networking, routing, and addressing features to enable customers to deploy these products in a production IPv6 or IPv4/IPv6 hybrid network. These security appliances must also provide optimum performance for all applications through the use of integrated hardware acceleration techniques.

Infrastructure

The networking equipment that is utilized across an organization's infrastructure provides critical transport for all applications from end to end. These infrastructure products include a variety of routing platforms for both small and large sites, which are tied together by running a standards-based modular operating system across all of the platforms.

For transitioning to IPv6, these infrastructure products will need to support full routing and MPLS, and provide a rich set of IP services including security, policy, and control for both IPv4 and IPv6 traffic.

The security components of these IPv6 infrastructure products will need to include sophisticated schemes that protect the devices in real time from unauthorized access and unsolicited attacks of either forged routing packets or bogus management traffic. Utilizing hardware-based filtering and IPsec, these products must be able to protect the system and its interfaces, while also protecting both the control plane and data plane during communication between devices.

The use of sophisticated flow monitoring and rate limiting techniques within these infrastructure products will help detect and stop attack flows while also providing the stable operation, routing, and management of important application traffic.

IPv6 Management Tools

While often an afterthought or topic that is discussed late in the planning or implementation stages, IPv6 management tools are a very important component of a successful IPv6 implementation.

As the deployment of IPv6 across an organization will enable a rich new set of collaborative applications and services, the configuration, operations and management of this environment should become simpler and easier to deploy. Across all of the components discussed in this section, from the application to the infrastructure devices, it will be very important to complement IPv4's Simple Network Management Protocol (SNMP) management capabilities with an IPv6 management toolkit that includes an intuitive CLI, flexible APIs, and simplified transition mechanisms.

Support for both IPv4 and IPv6 versions of Internet Control Message Protocol (ICMP) and applications such as Telnet, Ping, Traceroute, FTP and others—as well as extensive support for run-time diagnostics and good system event logging and tracing—will also help ease management of both IPv4 and IPv6 environments during this transition.

IPv6 Deployment Considerations

Significant planning is necessary before a successful transition from IPv4 to IPv6 can be made. With a huge installed base of IPv4, a key consideration to IPv6 deployment will be understanding how to migrate to the “new”, while continuing to support the “old.” Clearly, there will be no flick-of-the-switch way to convert computer and communications systems to an all IPv6 world. Therefore transitional technologies that allow coexistence of both versions and a phased transition to IPv6 will be essential. With the inevitable transition to IPv6, the best thing departments can do today is to plan a transitional strategy that includes both tunneling technologies and the purchase of equipment and software that will support both the IPv6 and IPv4 protocols simultaneously. These next-generation devices should also meet the robust performance and reliability requirements of secure and assured next-generation networks.

Transition Functionality

While providing support for core network routing and security support is of supreme importance, it is not enough. Successfully transitioning networks to IPv6 will require robust transition functionality. As the transition timeline is expected to be a multi-step process, transition planning teams will need to consider coexistence and interoperation. This includes simultaneous support for both IPv4 and IPv6 (dual-IP layer such as that found in Windows Vista and Windows Server, code name “Longhorn,” or dual-stack), in addition to translation and tunneling features. Key transition functionality includes:

- Firewalls that can secure the network during the transition
- The support of a full IPv6 protocol stack in all network devices
- High performing dual-stack routers and hosts that allows simultaneous support for both IPv4 and IPv6 applications
- Provisions for the IPv6-to-IPv4 transition

As a full equipment refresh is not in the scope of some IT budgets, the recommended upgrade path is to first ensure that firewalls support IPv6 functionality. Once this is understood, it is recommended to both disable IPv6 at the perimeter and inspect IPv4 protocol 41. IP protocol 41 is used to mark encapsulated IPv6 packets. Traffic that is entering and leaving a corporate domain through tunnels (IP protocol 41) must have packet inspection enabled similar to the inspection that is enabled on native IPv4 and native IPv6 traffic.

- IPv6 to IPv4 tunneling mechanisms include:
 - Manually configured tunneling of IPv6 over an IPv4 network provides connectivity between two IPv4 points. However, it is difficult to scale and manage, as the configuration is static.
 - 6to4 automatic tunneling based on RFC 3056 provides the method for transmitting IPv6 packets across an IPv4 network. A device must have a globally unique IPv4 address to implement this protocol.
 - ISATAP is defined in RFC 4214 and describes an tunneling mechanism that automatically connects IPv6 hosts/routers over an IPv4 network infrastructure.
- IPv6 using MPLS Circuit Cross-Connect (CCC) enables IPv6 communication over an IPv4/MPLS network on infrastructure products.
- IPv4 over IPv6 and IPv6 over IPv4 IPsec VPN tunneling support on security products enables easy transitioning of IPv4 and IPv6 secure VPNs and allows IPv4 traffic to traverse an IPv6 backbone.

Transitional Deployment Scenarios

The following figures provide some basic steps to IPv6 transitional deployments and highlight key functionality aspects required for a robust end-to-end IPv6 solution. Figure 2 shows the initial transition step in which the IT organization first enables the perimeter firewalls to block IPv6 traffic (both native and tunneled). Secondly, DNS and DHCP servers are deployed in the infrastructure as dual-stack machines.

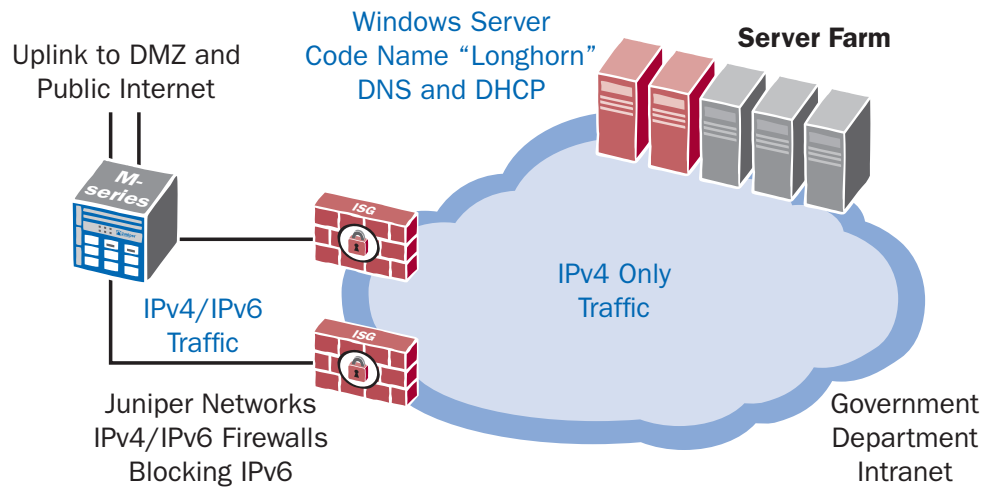


Figure 2 – Enable DNS and DHCP Servers and Configure Firewalls

The second step (Figure 3) shows a typical method for easing IPv6 integration across a government organization. The deployment of an ISATAP server provides transitional connectivity to the hosts. Static IPv6 tunnels are configured between the firewalls to provide tightly controlled IPv6 connectivity to select remote sites. 6to4 is a viable alternative to ISATAP. But 6to4 connectivity requires the enterprise to already use a globally unique IPv4 addressing architecture.

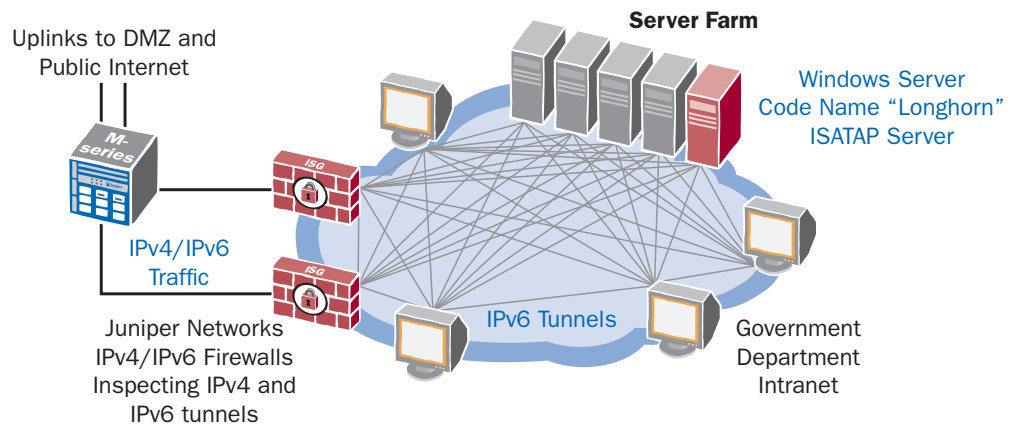


Figure 3 – Enable ISATAP Server; IPv6 Tunnels Across IPv4 Infrastructure

The final deployment scenario is shown in Figure 4. Dual stack routers are enabled across the backbone to provide native IPv6 and IPv4 hosts on the LANs. The security gateways at each location can deliver stateful inspection firewall capabilities at each site. MPLS edge routers are enabled to provide IPv4 and IPv6 connectivity between sites, replacing the static tunnels. New server roles are deployed such as Web, email, and file services.

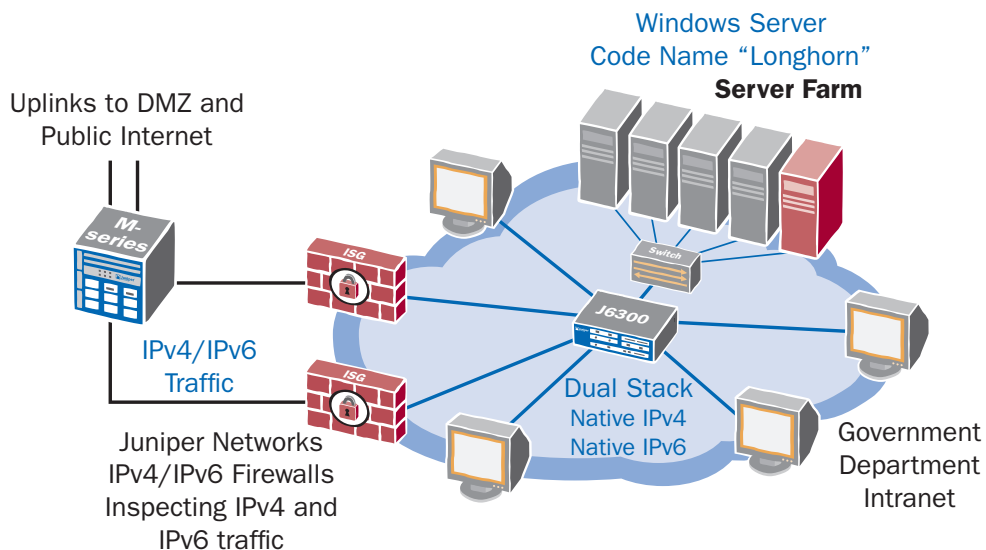


Figure 4 – Native IPv6 and IPv4 Dual-Stack Infrastructure

IPv6-Capable Products – Today

Whether driven by necessity or government mandate, IPv6 is coming to networks worldwide. Juniper Networks and Microsoft can help businesses prepare for this by providing solutions that enable a secure and assured transition to the next generation Internet Protocol.

Microsoft

Microsoft delivers support for IPv6 in the latest versions of Microsoft operating systems and key solutions such as Microsoft Office and SQL Server.

Operating Systems – Windows Vista and Windows Server

Windows Vista introduces powerful new technologies that will help enterprise employees do their best work. It will help them collaborate and communicate more effectively—easily connecting them to corporate resources, to the Internet, and to each other, regardless of their locations. It will also help organizations lower costs, improve security, and comply with regulatory requirements.

Microsoft Windows Server is the next generation of the Windows Server operating system that helps IT professionals maximize control over their infrastructure. It provides unprecedented availability and management capabilities, enabling a significantly more secure, reliable, and robust server environment than ever before.

The next generation TCP/IP stack in Windows Vista and Windows Server represents an evolution of Windows TCP/IP functionality with updated support for both IPv4 and IPv6 to meet the connectivity and performance needs of today's varied networking environments and technologies. This TCP/IP stack provides a dual IP layer architecture in which the IPv4 and IPv6 implementations share common transport and framing layers, as shown below in Figure 5.

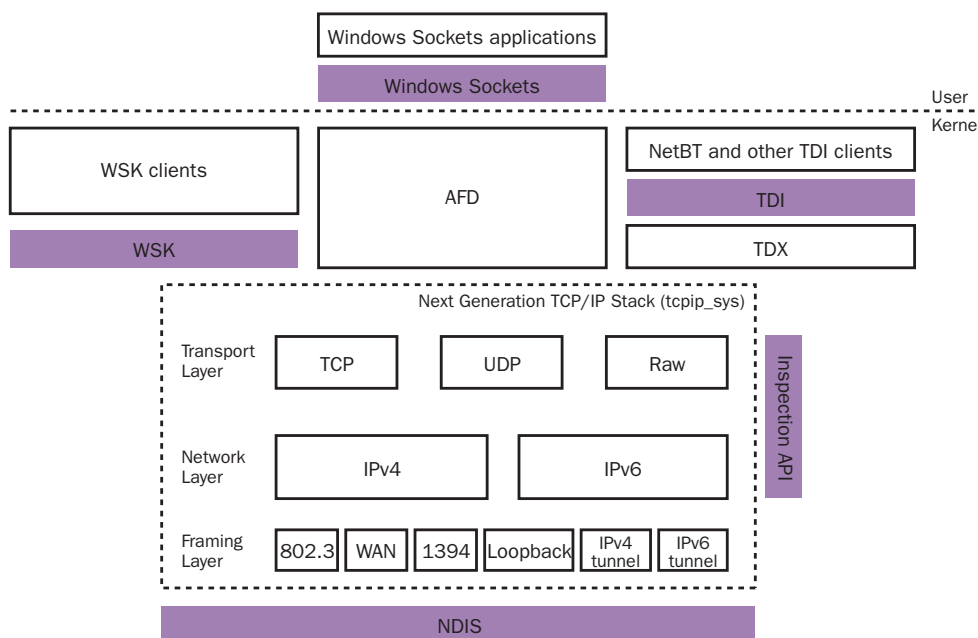


Figure 5: The Dual IP Layer Architecture of the Next Generation TCP/IP Stack

This next generation TCP/IP stack has IPv6 enabled by default and now allows manual configuration of IPv6 settings through familiar administrative interfaces.

Network services in Windows Vista and Windows Server support pure IPv6 environments including host firewall, DNS, DHCP, and Active Directory. This includes IPsec, Multicast Listener Discovery version 2 (MLDv2), Link-Local Multicast Name Resolution (LLMNR), DHCPv6, and IPv6 over PPP for the built-in remote access client. In addition, the WinINet API now supports RFC 2732 and the use of IPv6 literal addresses in URLs.

Juniper Networks

Juniper Networks products support a broad range of IPv6 features covering both network and security functionality to enable real-world deployments today. The key areas required for a smooth migration to a secure and successful IPv6 deployment include core IPv6 network routing support, IPv6 security, and IPv6/IPv4 transition functionality.

Routing and Migration Products

JUNOS on M/T Series Platforms – JUNOS is the standards-based modular operating system for the Juniper Networks routing infrastructure products. JUNOS supports full routing and MPLS, and provides a rich set of IP services, including security, policy, and control for both IPv4 and IPv6. Juniper Networks ASIC-based forwarding and JUNOS software have consistently delivered proven superior performance even when concurrently running both IPv4 and IPv6.

Since integration and transition tools and mechanisms play such an important role in simplifying operations and minimizing costs when introducing IPv6, JUNOS offers a broad number of IPv6 transition, translation, and tunneling features. Juniper Networks also offers a wide range of operational tools to ease IPv6 deployment such as the CLI and the JUNOScript API, enabling IPv6 to be configured and maintained rapidly and efficiently. The following feature summary represents the major IPv6 capabilities of JUNOS.

Addressing and Forwarding	Routing Protocols	Operations and Transition
<ul style="list-style-type: none"> • Forwarding in hardware • Addressing <ul style="list-style-type: none"> – Link, site, global – Stateless autoconfiguration • Neighbor discovery • IPv6 Packet Filtering • EUI 64 Autogeneration • Unicast RPF • FBF and CBF for IPv6 • Destination/Source Class Usage • RF table label for IPv6/IPv6 VPNs 	<ul style="list-style-type: none"> • IS-IS • OSPFv3 • MP-BGP over v4/v6 • RIPng • Static • IPv6 VPN (RFC2547bis) • PIM v2 • PIM – RP/DR • MLD v1, v2 • IPv6 multitopology extensions for ISIS 	<ul style="list-style-type: none"> • Consistent management <ul style="list-style-type: none"> – CLI – JUNOScript API • Path MTU discovery • ICMPv6 • SNMP over v6 + MIBs • IP applications <ul style="list-style-type: none"> – Ping, telnet, ssh, ftp... • Transition <ul style="list-style-type: none"> – Configured tunnels – Dual stack – IPv4/IPv6 – Transport IPv6 in MPLS

JUNOS IPv6 Feature Summary

CTP – The Juniper Networks Circuit to Packet (CTP) family of products provide reliable transport of bit-synchronous circuits across IP networks, sometimes referred to as TDM over IP. The CTP family is designed to both create an IP packet flow from a serial data or analog voice connection at one end, and provide the necessary processing to recreate the serial bit stream or analog signal from the received IP packet flow at the other end on both IPv6 and IPv6 networks.

Firewalls/VPN Security Devices

NetScreen Series – ScreenOS is a real-time, security-specific operating system for all of the Juniper Networks firewall/IPsec VPN devices. Tightly integrated with the hardware platforms, ScreenOS is specifically designed to perform network security tasks in real time. It provides integrated firewall, VPN, attack blocking, and traffic management capabilities across all of Juniper's low-end to high-end firewall/VPN products.

The IPv6 implementation of ScreenOS includes a full IPv6 protocol stack, a dual stack IPv4/IPv6 functionality, many transition mechanisms, and traditional networking, routing, and addressing features that enable enterprise customers to deploy these products in a production IPv6 or IPv6/IPv4 hybrid network. The following feature summary represents the IPv6 capabilities of ScreenOS.

Addressing and Forwarding	Routing and Transition	Security
<ul style="list-style-type: none"> • IPv6 Address • Auto-configuration • DHCPv6 • RADIUSv6 client • Xauth and modeconfig • IPv6 Neighbor Discovery • Virtual System Support • SSH for IPv6 • DNS Proxy • DNS Client 	<ul style="list-style-type: none"> • Full IPv6 protocol stack • Dual stack – IPv4/IPv6 • RIPng • PPPoE v6 support • SNMP MIB • Management similar to IPv4 – WEBUI, CLI • Tunneling <ul style="list-style-type: none"> – 6to4 auto tunnel – 6in4 manual tunnel – 4<->6 IPsec Tunnel 	<ul style="list-style-type: none"> • Firewall functionality • ALGs DNS, FTP, Telnet and ICMPv6 • IPsec and IKE for IPv6 • 3DES IPsec Tunneling • NAP-PT Address Translation 6to4 and 4to6 • Synflood protection • DoS protection

ScreenOS IPv6 Feature Summary

Conclusion

IPv6 offers the promise of both expanded network functionality and technology leadership for organizations around the world. In many nations, IPv6 transition has become a government mandate, and transitional timelines have been set. In order to continue providing mission-critical communications and services, organizations are looking to IPv6-enabled applications and infrastructures that will improve end-to-end productivity. This will enable new applications that provide enhanced performance, improve network availability, and deliver better quality of service. As service providers and enterprises look to move to IPv6, transition functionality and security will be key components of their planning process.

As early pioneers with IPv6 technology, Microsoft and Juniper Networks have been shipping a wide variety of end-to-end IPv6 product and support solutions for many years. Working closely together, both companies share a common vision and are fully committed to helping government agencies and departments achieve a secure and assured transition to IPv6.

Further Reading

Microsoft’s IPv6 TechNet site:

<http://www.microsoft.com/ipv6>

Windows Networking:

<http://www.microsoft.com/networking>

Windows Vista:

<http://technet.microsoft.com/en-us/windowsvista/default.aspx>

Windows Server (“Longhorn”):

<http://www.microsoft.com/windowsserver/longhorn/default.mspx>

Juniper Networks public sector site:

http://www.juniper.net/solutions/public_sector/index.html

Juniper Networks Federal IPv6 site:

<http://www.juniper.net/federal/IPv6/>

About Microsoft

Founded in 1975, Microsoft (Nasdaq "MSFT") is the worldwide leader in software, services and solutions that help people and businesses realize their full potential.

About Juniper Networks

Juniper Networks develops purpose-built, high-performance IP platforms that enable customers to support a wide variety of services and applications at scale. Service providers, enterprises, governments and research and education institutions rely on Juniper to deliver a portfolio of proven networking, security and application acceleration solutions that solve highly complex, fast-changing problems in the world's most demanding networks. Additional information can be found at www.juniper.net.

This is a preliminary document and may be changed substantially prior to final commercial release of the software described herein. The information contained in this document represents the current view of Microsoft Corporation and Juniper Networks, Inc. on the issues discussed as of the date of publication. Because Microsoft and Juniper must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Microsoft or Juniper, and neither Microsoft nor Juniper can guarantee the accuracy of any information presented after the date of publication.

This White Paper is for informational purposes only. NEITHER MICROSOFT NOR JUNIPER MAKES ANY WARRANTIES, EXPRESS, IMPLIED OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, no part of this document may be reproduced, stored in or introduced into a retrieval system, or transmitted in any form or by any means (electronic, mechanical, photocopying, recording, or otherwise), or for any purpose, without the express written permission of Microsoft and Juniper. Microsoft and Juniper may each have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Microsoft or Juniper, the furnishing of this document does not give you any license to any patents, trademarks, copyrights, or other intellectual property of Microsoft or Juniper, respectively.

© 2007 Microsoft Corporation and Juniper Networks, Inc. All rights reserved.

Microsoft, Windows, and Windows Server are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

All rights reserved. Juniper Networks and the Juniper Networks logo are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered trademarks, or registered service marks in this document are the property of Juniper Networks or their respective owners. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.