How Microsoft IT has Deployed IPv6 on the Microsoft Corpnet

Internet Protocol version 6 (IPv6) is the replacement for Internet Protocol version 4 (IPv4), the Internet layer of the TCP/IP protocol stack used around the world on the Internet and on private networks. IPv6 restores end-to-end connectivity and ensures the growth of the Internet. Microsoft has deployed IPv6 on its private network for many years. This paper describes the current configuration of IPv6 on the Microsoft corporate network, the short and long-term plans for IPv6, and deployment best practices and lessons learned along the way.

IPv6 on the Microsoft Corpnet

Why Microsoft IT has deployed IPv6 on the Microsoft Corpnet

Microsoft has deployed IPv6 on the Microsoft corporate intranet, hereafter referred to as Corpnet, beginning in 2001. It was introduced into the environment for the following reasons:

IPv6 provides an infrastructure for product development and research

> Microsoft has made and continues to make investments in researching IPv6 technologies and enabling its products and services to fully support IPv6. Therefore, IPv6 capability is required on Corpnet to develop and test current and future products.

IPv6 provides a showcase for IPv6 and IPv6-based solutions

> As an industry proponent of IPv6, Microsoft has deployed IPv6 on its Corpnet as a technology showcase to demonstrate to other enterprise networks a working IPv6 deployment. Additionally, IPv6 on the Microsoft Corpnet enables technologies and solutions that rely on IPv6-based connectivity. For example, DirectAccess deployed across Microsoft acts as a showcase for other enterprise networks.

IPv6 provides public address space for the Microsoft Corpnet

> The Microsoft Information Technology group, MSIT, is in the process of migrating their Corpnet IPv4 address space from public addresses to the private addresses defined in RFC 1918. With IPv6 and Microsoft's eventual IPv6 Internet presence, the public address depletion issue is not an immediate concern.

Microsoft Enterprise Deployment

It is helpful to review two defining characteristics of Microsoft Corpnet:

Microsoft Corpnet is an open network

> The Microsoft Corpnet is “open” in the sense that routers within the Corpnet are not performing firewalling or packet filtering functions. Instead, communication security is enforced at the

endpoints of communication using the built-in Windows Firewall, which protects against unsolicited incoming communication, and a domain isolation deployment, which requires the use of IPsec for incoming connection attempts to corporate resources. Because there is equivalent support for IPv6 in both Windows Firewall and IPsec in versions of Windows starting with Windows Vista and Windows Server 2008, it was relatively easy to implement the same level of host firewalling and protected communication as existed for IPv4.

Microsoft is a homogeneous computing environment

Unlike most enterprises, the Microsoft Corpnet is a largely homogeneous computing environment with almost all computers running a version of Windows on the server and client. Because IPv6 has been supported by built-in applications and services since Windows Vista and Windows Server 2008, many client and server computers are fully IPv6-capable

These two factors have greatly simplified the early adoption of IPv6 within the enterprise network. Eliminating the need to focus on enabling complex security functions and incompatibility issues between multiple vendors stack deployments.

A Brief History of IPv6 in Microsoft

- **2001 - Initial Deployment**
  - Created to support research and development
  - Deployed using experimental 6bone address space.
  - Deployed on dedicated devices due to poor performance on routing platforms
- **2002-2004 – Limited adoption**
  - A single ISATAP instance deployed in each region (Redmond, SVC, Dublin, Singapore)
  - Pockets of native v6 deployed across enterprise
  - Limited to development and research groups with a documented business need
  - “Stitched” together across the enterprise network on a link by link basis
- **2005-2006 - Enterprise backbone upgrade**
  - Obtained new v6 address space from ARIN and RIPE. Entire network readdressed into new address blocks.
  - Requests for native v6 enabled networks grew
  - Operational issues in connecting disparate v6 clouds become commonplace
  - Network hardware capable of routing at performance parity with V6 was introduced during hardware refresh cycle
  - Native v6 was enabled across all backbone and tail site WAN links to resolve issue
  - End user networks still required justification for v6 due lack of security and performance visibility
- **2007-2010 – Expansion**
  - Client and Server OS platforms became v6 capable
  - ISATAP usage grew concurrently, causing scaling/performance issues
  - ISATAP infrastructure was redesigned to distribute service across the backbone
  - IDS infrastructure became v6 aware

Deployment Philosophy

The key elements of the MSIT IPv6 deployment philosophy are the following:

Dual-Stack/Coexistence

Provide parity between v4 and v6 network connectivity wherever possible. While deploying v6 native only segments within the MS network is supported it is not a short or medium term goal to disable v4 on the enterprise network. Ensuring that an end system has the ability to choose either protocol with a base guarantee of parity in both performance and services is the goal.

Enable the network backbone and WAN first and then enable the edge

MSIT follows the methodology of first enabling the routed backbone infrastructure to support v6 and then enable edge connectivity as needed. The history of our deployment has shown that provisioning isolated pockets of native IPv6 connectivity within the enterprise will result in operational/stability issues in the long term.   Ensuring that the entire network can transport the v6 protocol at the beginning of the process streamlines the overall adoption effort and removes the network as the bottleneck/blocker.

Reduce reliance on transition technologies whenever possible

Transition technologies should not be relied upon as the foundation to build your IPv6 deployment. As the name implies they are for a transition. The introduction of transition technologies increases the overall complexity and may reduce the stability of a v6 network deployment.

In the past very few vendors included v6 support in their products. An enterprise such as Microsoft, required to deploy v6 before the industry provided support had limited options. In this case a driving business need forced the introduction of ISATAP as a transition technology. Today most, if not all, network vendors have basic v6 support in their products investing time and effort for native v6.

Current Deployment of IPv6 on the Microsoft Corpnet

Figure 1 shows the deployment of IPv6 on the Microsoft Corpnet.

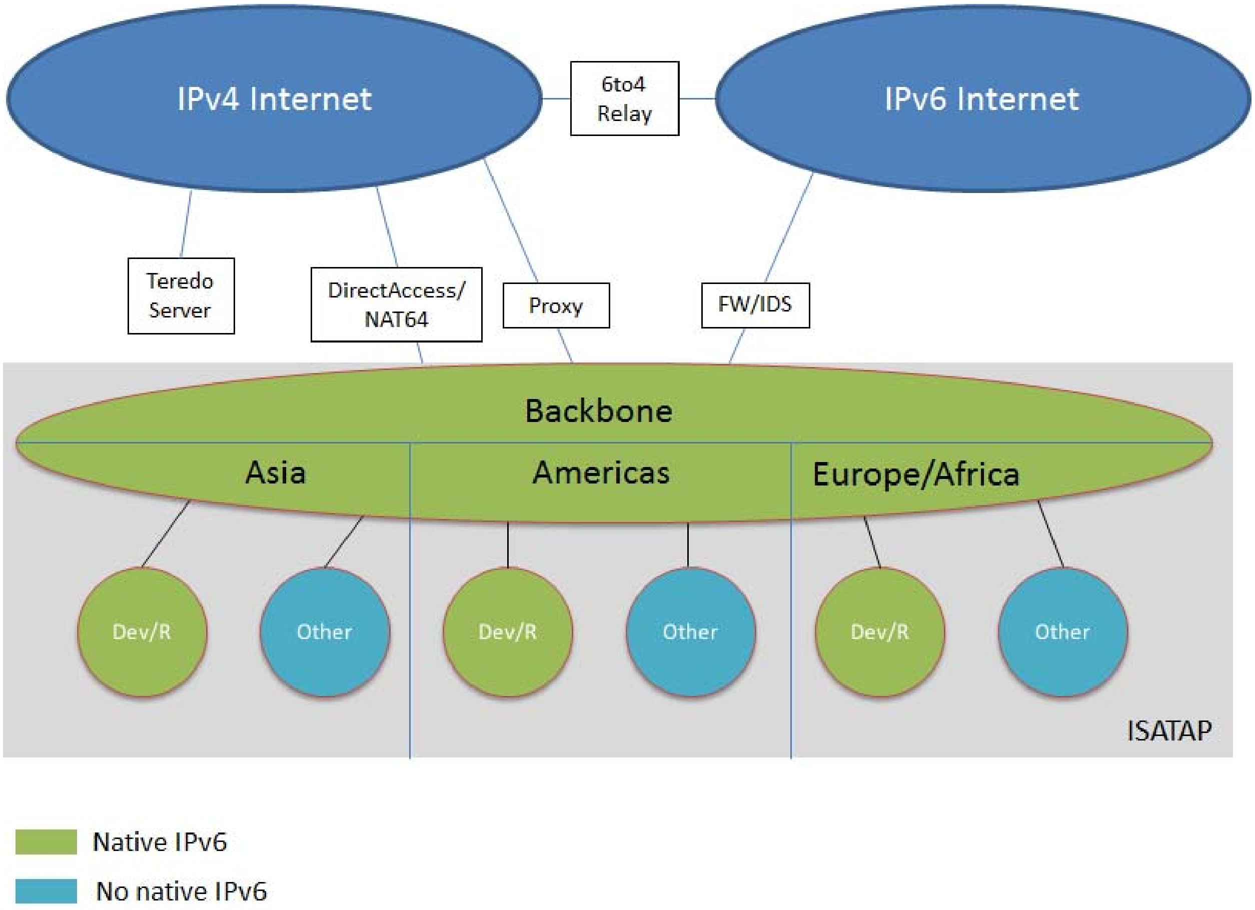

Figure 1 IPv6 deployment on the Microsoft Corpnet

Key elements of the IPv6 deployment on Microsoft Corpnet

IPv6 connectivity in addition to IPv4

It is not a short or long-term goal to migrate the Microsoft Corpnet to an IPv6-only network.

Native IPv6 connectivity across the Corpnet backbone

This is not IPv6-only, but in addition to IPv4.

Native IPv6 connectivity to 40% of subnets

The subnets with native IPv6 connectivity are in locations and buildings that house product development, test, or research teams.

ISATAP connectivity across the entire Corpnet

Multiple ISATAP routers in each region (Asia, Americas, and Europe/Africa in Figure 1) advertise a single ISATAP prefix to ISATAP hosts across the Corpnet.

All of the ISATAP routers are configured for an IPv4 anycast address and the routing infrastructure forwards the Router Solicitation messages sent by ISATAP hosts to the topologically nearest ISATAP router.

NAT64 for DirectAccess

A NAT64 allows DirectAccess clients access to IPv4-only resources on the Corpnet. Forefront Unified Access Gateway (UAG) 2010 provides both DirectAccess and NAT64.

Gaps in management and traffic reporting capabilities

> Lacking IPv4 parity support on its network monitoring equipment, MSIT at this time cannot measure or monitor its native or ISATAP-based IPv6 traffic.

Short and long term plans for IPv6 on the Microsoft Corpnet

In the next three years (to 2014), MSIT is driving toward IPv6 support parity with IPv4 in all of its applications, computers, devices, and networking and traffic management infrastructure. During this period, MSIT is pursuing a strategy of managed coexistence with IPv4, using ISATAP for areas of the Corpnet that are not yet native IPv6-capable and NAT64 for DirectAccess client access to IPv4-only resources.

With IPv6 support parity across all network devices and applications and the preference of IPv6 over IPv4 for network connectivity, beyond 2014 will be a time of IPv6 traffic predominance. At that time, all Corpnet subnets will be native IPv6-capable with no ISATAP and only a small amount of IPv4 traffic will remain.

Deployment Details

Addressing Plan and Routing Infrastructure

Microsoft has received four 32-bit global address prefixes—a 31-bit prefix allocated RIPE, a 32-bit prefix from ARIN, and a 32-bit prefix from APNIC—and uses 64-bit prefixes at the subnet level.

The 32-bit global address prefixes were requested due to current ISP policies, which do not allow an organization to advertise smaller portions of your address space (with a longer address prefix) to Internet routers. To assure an adequate supply of address space going forward, Microsoft requested 32-bit prefixes, rather than a series of 48-bit prefixes.

Microsoft does not perform route summarization in its routing infrastructure, resulting in 3,100 routes in the routing tables of native IPv6 routers. Microsoft uses Open Shortest Path First version 3 (OSPFv3) for their interior gateway protocol (IGP). However, because OSPFv3 is does not have feature parity with OSPFv2 with respect to tuning parameters to control router convergence, Microsoft is investigating the use of the Integrated Intermediate System-to-Intermediate System (IS-IS) IGP in the future.

The Microsoft Corpnet currently uses stateless address autoconfiguration based on local subnet router advertisements and DHCP (for IPv4) for configuration options, including DNS domain suffixes and the IPv4 addresses of DNS servers. At this time, Corpnet hosts do not send or receive DNS traffic over IPv6. MSIT is investigating the deployment of DHCPv6 to support address management and monitoring and for client reservations.

DirectAccess

Microsoft uses DirectAccess as a method for computers to obtain Corpnet connectivity when they are on the Internet. DirectAccess is a feature of Windows 7 and Windows Server 2008 R2 that uses a combination of IPv6, Internet Protocol securing (IPsec), and DNS name request routing to automatically and seamlessly connect DirectAccess client computers to intranet resources without user configuration or initiation.

While on the Internet, Corpnet computers configured for DirectAccess use the following transition technologies:

Teredo

The Teredo component is configured with the name of a Microsoft DirectAccess server on the Internet, which acts as a Teredo server and relay. This allows a DirectAccess client to perform address autoconfiguration and reach IPv6 locations on the Microsoft Corpnet when using Teredo as its IPv6 transition technology.

IP-HTTPS

The IP-HTTPS component is configured with a uniform resource locator (URL) corresponding to the DirectAccess server. This allows a DirectAccess client to perform address configuration and reach IPv6 locations on the Microsoft Corpnet when using IP-HTTPS as its IPv6 transition technology.

6to4

6to4 is disabled through Group Policy on DirectAccess clients because native IPv6 has been deployed internally and the DirectAccess servers are not on the default route path leading outside the Microsoft Corpnet. In this configuration, one cannot route 6to4-addressed traffic, which is summarized with the 2002::/16 route, back to the regional DirectAccess server being used by a specific DirectAccess client. DirectAccess uses IPsec tunnels to a specific DirectAccess server does not support asymmetric routing paths, in which the traffic from the DirectAccess client goes into the intranet through a specific DirectAccess server but the traffic back to the DirectAccess client goes through a different DirectAccess server.

In contrast, traffic for Teredo and IP-HTTPS clients that use a specific DirectAccess can be summarized as 64-bit prefixes and routed back to the regional DirectAccess server being used by the DirectAccess client.

Security for IPv6 Traffic on the Microsoft Corpnet

As previously described, Microsoft uses an open network model in which security for intranet traffic flows is enforced at the endpoints, rather than at intermediate systems within the Corpnet, such as routers. The IPv6 deployment at Microsoft uses the following:

- Windows Firewall on hosts to define allowed inbound and outbound IPv6 traffic.
- Connection security rules for IPsec and domain isolation to define communication protection requirements for IPv6 traffic for domain-joined computers.

Both Windows Firewall and connection security rules are configured for domain member computers through Group Policy.

At the edge, the Microsoft Corpnet does not allow direct traffic to or from the Internet. Access to the Internet from Corpnet is done through proxy servers. Access to the Corpnet from the Internet is done through application gateways—such as Outlook Web Access servers—and DirectAccess and virtual private network (VPN) servers, which are the endpoints of tunneled traffic and require authentication and authorization of the connection and encryption of traffic on the Internet.

Deployment Planning and Best Practices

This white paper is not the forum for a full treatment of IPv6 deployment best practices. However, the following sections describe best practices and lessons learned are based on the experience of deploying IPv6 on the Microsoft Corpnet.

Overall Planning

Planning included of determining the business need, determining the technology gaps that existed across the end to end infrastructure, and operational staff ramp-up.

Determine the business need

When planning for IPv6, you should first establish a business need and an adoption timeframe. Defining these areas is essential to determine the capital and organization investment required to deploy.

Organizations that must comply with regulatory or government mandates. In this case, you should update your computers, applications, and network equipment in the near term to meet that need.

However, for many enterprises, a specific business driver does not exist. Even though there may be no immediate issue with address depletion within the enterprise, it is important to begin early preparation and planning. Early planning allows the enterprise to begin a gradual process of transitioning your intranet to support both IPv4 and IPv6. In this case, IPv6 deployment becomes a longer-term goal that you can achieve as part of your natural computer and infrastructure upgrade lifecycle, in which upgraded computers and equipment support IPv6 capability equivalent to that of IPv4. MSIT has taken this latter approach.

Determine the IPv6 technology gaps that exist across your entire infrastructure

To enable your enterprise for IPv6 connectivity, you must carefully inventory your infrastructure to determine the elements that currently only support IPv4 and create a plan to move them toward IPv6 feature parity. When performing your inventory, analyze your key network traffic flows and management functions by determining all of the components involved in the end-to-end process and their support for IPv6 configuration, IPv6 traffic, and the storage of IPv6 addresses.

The inventory and analysis of IPv6 technology gaps includes the following:

Computers (servers, clients, printers, mobile devices)

Ensure that the computers support a standards-compliant IPv6 stack, which includes support for your current or future address, naming, and directory infrastructure. For example, determine if the stack includes support for DHCPv6 for stateful address autoconfiguration, DNS dynamic update of AAAA and PTR records, and Active Directory Domain Services (AD DS). All three of these essential infrastructure technologies have been supported in Windows since the release of Windows Vista and Windows Server 2008.

Applications that run on those computers (client and server components)

Applications should initiate connections regardless of the version of IP and provide equivalent support for input and storage of IPv6 addresses. For example, typical application support problems include using older WinSock IPv4-specific APIs, using IPv4 addresses and associated 32-bit storage structures within the code of the application, UI support for only IPv4 address configuration, application security based only on IPv4 addresses, reliance on WINS simple names, and database schema that does not allow storage of the 128-bit IPv6 addresses.

Network hardware

Router and switching hardware should provide an equivalent level of support for IPv6, without sacrificing the enhanced features of IPv6 or network throughput.

In addition to basic IPv6 support, it is important to build a comprehensive list of all features that you have enabled on your network infrastructure.   Many vendors will state that they support v6 but experience has shown that support may not be consistent across all features.

When evaluating platform ensure you plan for any additional overhead that IPv6 may introduce in your network device. Increase in routing table size, the addition of 3 128-bit addresses for each host, and impact of processing Neighbor Discovery messages are all examples.

For example, one IPv6-related issue on routers is the use of Ternary Content Addressable Memory (TCAM) entries, which can be used to store addresses or masks, such as address masks in routing tables. On some routers, you must assign the finite TCAM space to specific router features. IPv6-related entries typically use twice the number of TCAM entries as IPv4 and many computers have multiple IPv6 addresses. Therefore, when you deploy IPv6 addressing and routing on such routers, you have to carefully understand the impact the TCAM resources of the router for overall optimal performance.

Another element of router support for IPv6 is whether IPv6 traffic, including traffic with IPv6 extension headers, is processed in hardware or software. When packets are processed by software, it can be dramatically slower than hardware, resulting in sporadic or difficult-to-troubleshoot throughput or performance problems.

Management systems and infrastructure

Ensure that your infrastructure management software and protocols support the input, selection, and storage of IPv6 addresses. Security and traffic monitoring systems, such as intrusion detection systems (IDSs) and intrusion prevention systems (IPSs)

Ensure that your IDS/IPS supports monitoring of native and, for ISATAP traffic, IPv4-encasulated IPv6 traffic. Also, ensure that the database for your IDS/IPS monitoring information allows the storage of 128-bit IPv6 addresses.

Ramp up operations staff

Each dual-stack client and server computer can have multiple addresses (IPv4 and IPv6) and multiple interfaces (LAN and ISATAP) over which to communicate. This can complicate the troubleshooting of connectivity issues. Therefore, sufficient attention to preparing operations staff to support IPv6 connectivity issues on your intranet is important. Without this attention, your operations staff, including helpdesk, can immediately assume that a network connectivity issue is related to IPv6 and either escalate it to engineering (which wastes engineering time) or instruct the user to disable IPv6 (which potentially wastes user time and removes IPv6 capability for that computer).

A recommended course of action to prevent these issues is the following:

- Provide training to operations staff about IPv6, specifically about how Windows uses DNS and address selection to determine the sets of source and destination addresses to use when initiating communication. For more information, see Domain Name System Client Behavior in Windows Vista and Source and Destination Address Selection for IPv6.
- Identify IPv6 experts at the higher tier support levels and provide additional depth training. Use a train-the-trainer approach to distribute deeper IPv6 knowledge across the higher tier teams.
- Provide an IPv6 infrastructure to your IPv6 experts to experiment with IPv6 and build their expertise.

Deployment Recommendations

Use native IPv6 over IPv6 transition technologies

Microsoft recommends that you deploy native IPv6 on your intranet as the primary method of IPv6 connectivity. You should use ISATAP on your intranet for limited testing as needed, rather than an enterprise-wide deployment. If you use ISATAP on your intranet, design for minimal traffic through ISATAP routers, which can become a performance bottleneck.

Use NAT64 only at the edge of your network for DirectAccess clients so they can access IPv4-only applications, computers, or devices. However, note that NAT64 does not allow IPv4-only nodes to access DirectAccess clients and the server hosting NAT64 can become a bottleneck for DirectAccess traffic, depending on the number of concurrent DirectAccess clients and the percentage of intranet resources that are only available over IPv4.

Configure Active Directory Sites and Services for IPv6 subnets

If you define AD DS traffic management in terms of IPv4 subnets and their inter-site transports and costs in the Active Directory Sites and Services snap-in, you must configure the equivalent for IPv6 subnets. For native IPv6, configure an IPv6 subnet object for each of your IPv6 subnets and the appropriate site links and costs for inter-site AD DS traffic over IPv6.

To configure Active Directory sites and services for forwarding within sites when using ISATAP, you must configure an IPv6 subnet object equivalent to each IPv4 subnet object, in which the IPv6 address prefix for the subnet expresses the same range of ISATAP host addresses as the IPv4 subnet. For example, for the IPv4 subnet 192.168.99.0/24 and the 64-bit ISATAP address prefix 2002:836b:1:1::/64, the equivalent IPv6 address prefix for the IPv6 subnet object is 2002:836b:1:1:0:5efe:192.168.99.0/120. For an arbitrary IPv4 prefix length (set to 24 in the example), the corresponding IPv6 prefix length is 96 + *IPv4PrefixLength*.

Deprecate the use of WINS

You might still be using NetBIOS applications and WINS, which provides enterprise-wide NetBIOS name registration and resolution. NetBIOS over TCP/IP (NetBT) is only defined for IPv4, not IPv6. Therefore, as you plan for IPv6 predominance on your intranet, you should also plan to deprecate the use of NetBIOS applications and WINS. For example, update or replace your NetBIOS applications to use Windows Sockets or the .NET Framework Class Library.

WINS is also used to contain static records that provide single-label, unqualified name resolution. To replace this functionality for IPv6, use the GlobalNames zone and functionality in the DNS Server service of Windows Server 2008 and Windows Server 2008 R2. For more information, see Deploying a GlobalNames Zone.

Conclusion

The IPv6 deployment on the Microsoft Corpnet is required by Microsoft product development groups to develop products that are fully IPv6 capable, to provide an example to the IT industry, and to ensure public address space long term. The current implementation consists of a mixture of a native IPv6-capable backbone and subnets for product development and research and a pervasive ISATAP deployment that uses a single ISATAP prefix. This deployment configuration, address selection rules, and the behavior of the Windows client and server computers ensure that traffic is not bottlenecked by ISATAP routers.

Microsoft has taken a long-term approach to IPv6 migration, adding IPv6 capability in addition to and in parity with IPv4 capability as part of the natural upgrade cycle of computers, devices, and network infrastructure and management equipment. Microsoft is driving toward an intranet with a predominance of IPv6 traffic in 2014 and beyond and an eventual presence of Microsoft properties on the IPv6 Internet.

For More Information

For more information about IPv6 in Windows, see the Microsoft IPv6 web site (http://www.microsoft.com/ipv6).

For more information about DirectAccess, see the DirectAccess Getting Started web page (http://www.microsoft.com/directaccess).

For a webcast version of the information in the paper, see the TechNet WebCast: MSIT Enterprise IPv6 Deployment.