Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 30, 2012

L. Howard
Time Warner Cable
T. Chown
University of Southampton
K. Chittimaneni
Google Inc.
Y. Pouffary
Hewlett Packard
E. Vyncke
Cisco Systems
V. Kuarsingh
Rogers Communications
February 27, 2012

Enterprise Incremental IPv6
draft-chkpvc-enterprise-incremental-ipv6-00

Abstract

Enterprise network administrators worldwide are in various stages of preparing for or deploying IPv6 into their networks. The administrators face different challenges than operators of Internet access providers, and have reasons for different priorities. The overall problem for many administrators will be to offer Internet-facing services over IPv6, while continuing to support IPv4, and while introducing IPv6 access within the enterprise IT network. The overall transition will take most networks from an IPv4-only environment to a dual stack network environment and potentially an IPv6-only operating mode. This document helps provide a framework for enterprise network architects or administrators who may be faced with many of these challenges as they consider their IPv6 support strategies.

This Internet-Draft will expire on August 30, 2012.

Copyright Notice

Table of Contents

1. Introduction

An Enterprise Network as defined in [RFC4057] as: a network that has multiple internal links, one or more router connections to one or more Providers, and is actively managed by a network operations entity (the "administrator", whether a single person or department of administrators). Adminstrators generally support an internal network, consisting of users' computers and related peripherals, a server network, consisting of accounting and business application servers, and an external network, consisting of Internet-accessible services such as web servers, email servers, VPN systems, and customer applications. This document is intended as guidance for network architects and administrators in planning their IPv6 deployments.

The business reasons for spending time, effort, and money on IPv6 will be unique to each enterprise. The most common drivers are due to the fact that when Internet service providers, including mobile wireless carriers, run out of IPv4 addresses, they will provide native IPv6 and non-native IPv4. The non-native IPv4 service may be NAT64, NAT444, Dual-stack Lite, or other transition technology, but whether tunneled or translated, the native traffic will be perform better and more reliably than non-native. It is thus in the enterprise's interests to deploy native IPv6 itself.

1.1. Enterprise Assumptions

For the purposes of this document, assume:

- The administrator is considering deploying IPv6 (but see Section 1.2 below).
- The administrator has existing IPv4 networks and devices which will continue to exist.
- The administrator will want to minimize the level of disruption to the users and services by minimizing number of technologies and functions that are needed to mediate any given application. In other words, provide native IP wherever possible.

Based on these assumptions, an administrator will want to use technologies which minimize the number of flows being tunnelled, translated or intercepted at any given time. The administrator will choose transition technologies or strategies which allow most traffic to be native, and will manage non-native traffic. This will allow the administrator to minimize the cost of IPv6 transition technologies, by containing the number and scale of transition systems.

1.2. IPv4-only Considerations

As described in [RFC6302] administrators should take certain steps even if they are not considering IPv6. Specifically, Internet-facing servers should log the source port number, timestamp (from a reliable source), and the transport protocol. This will allow investigation of malefactors behind address-sharing technologies such as NAT44 or Dual-stack Lite. Enabling this additional logging will take a few minutes on each server, and will probably require restarting the service.

Other IPv6 considerations may impact ostensibly IPv4-only networks, e.g. [RFC6104] describes the rogue IPv6 RA problem, which may cause problems in IPv4-only networks where IPv6 is enabled in end systems on that network.

1.3. Reasons for a Phased Approach

Given the challenges of migrating user workstations, corporate systems, and Internet-facing servers, a phased approach allows incremental deployment of IPv6, based on the administrator's own determination of priorities. The Preparation Phases is highly recommended to all administrators, as it will save errors and complexity in later phases. Each administrator must decide whether to begin with the External Phase (as recommended in [RFC5211]) or the Internal Phase. There is no "correct" answer here; the decision is one for each enterprise to make.

Some considerations:

- In many cases, customers outside the network will have IPv6 before the internal enterprise network. For these customers, IPv6 may well perform better, especially for certain applications, than translated or tunneled IPv4, so the administrator may want to prioritize the External Phase.

- Employees who access internal systems by VPN may find that their ISPs provide translated IPv4, which does not support the required VPN protocols. In these cases, the administrator may want to prioritize the External Phase, and any other remotely-accessible internal systems.

- Internet-facing servers cannot be managed over IPv6 unless the management systems are IPv6-capable. These might be Network Management Systems (NMS), monitoring systems, or just remote management desktops. Thus in some cases, the Internet-facing systems are dependent on IPv6-capable internal networks. However, dual-stack Internet-facing systems can still be managed over IPv4.

- o IPv6 is enabled by default on all modern operating systems, so it may be more urgent to manage the internal traffic.

- o In many cases, the corporate accounting, payroll, human resource, and other internal systems may only need to be reachable from the internal network, so they may be a lower priority.

These considerations are in conflict; each administrator must prioritize according to their local conditions.

2. Preparation and Assessment Phase

2.1. Inventory Phase

To comprehend the inventory phase spectrum we recommended dividing the problem space in two: network infrastructure readiness and applications readiness.

2.1.1. Network infrastructure readiness assessment

The network infrastructure readiness assessment for IPv6 as its name state is focused on the network. The goal of this assessment is identify the level of readiness of network equipment. This is an important step as it will help identify the effort required to move to an infrastructure that supports IPv6.

Be able to understand which network devices are already capable, which devices can be made IPv6 ready with a code/firmware upgrade, and which devices will need to be replaced. The data collection consists of a network discovery to gain an understanding of the topology and inventory network infrastructure equipment and code versions with information gathered from static files and IP address management, DNS and DHCP tools.

Remember understanding the starting point and what are the technical issues and challenges is critical as IPv6 might already be present in the environment thus creating inherent security risks.

2.1.2. Applications readiness assessment

Just like network equipment, application software needs to support IPv6. This includes OS, firmware, middleware and applications (including internally developed applications). Vendors will typically handle IPv6 enablement of off-the-shelf products. Enterprises need to request this support from vendors. For internally developed applications it is the responsibility of the enterprise to enable them for IPv6. Analyzing how a given

application communicates of the network will dictate the steps required to support IPv6. Applications should be made to use APIs which hide the specifics of a given IP address family. Any applications that use APIs, such as the C language, which exposes the IP version specificity need to be modified to also work with IPv6.

There are two ways to IPv6-enable your applications. The first approach is to have separate logic for IPv4 and IPv6, thus leaving the IPv4 code path mainly untouched. This approach causes the least disruption to the existing IPv4 logic flow, but introduces more complexity, since the application now has to deal with two logic loops with complex race conditions and error recovery mechanisms between these two logic loops. The second approach is to create a combined IPv4/IPv6 logic, which ensures operation regardless of the IP version used on the network. We recommend using industry IPv6-porting tools to locate the code that need to be updated.

2.1.3. Importance of readiness validation and testing

Lastly IPv6 introduces a completely new way of addressing endpoints, which can have ramifications at the network layer all the way up to the applications. So to minimize disruption during the transition phase we recommend complete functionality, scalability and security testing to understand how IPv6 impacts the services and networking infrastructure will be paramount.

2.2. Training

IPv6 planning and deployment in the enterprise is not an entirely network centric affair. IPv6 adoption will be a multifaceted undertaking that will touch everyone in the organization. While technology and process transformations are taking place is it critical that people training takes place as well. Training will ensure that people and skill gaps are assessed proactively and managed accordingly. We recommend that training needs be analyzed and defined in order to successfully inform, train, and prepare staff for the impacts of the system or process changes.

2.3. Routing

When deploying IPv6, we recommend initially choosing an IGP protocol you are familiar with. That is to say if you are using OSPFv2 you should be using OSPFv3. The main advantage of this approach is that staff do not need to be trained and existing processes can be leveraged.

Enterprises could also take the opportunity the introduction of IPv6 brings to analyze your current environment and to identify which

features you would like to change and what you would like to implement. Then using the validation period as a way to validate your new approach and even applying them to your IPv4 environment.

Either way IPv6 introduces the opportunity to rationalize the environment and to architect it for growth.

2.4. Security and Routing Policy

It is obvious that IPv6 network should be deployed in a secure way. The industry has learned a lot about network security with IPv4, so, network operators should leverage this knowledge and expertise when deploying IPv6. IPv6 is not so different than IPv4: it is a connectionless network protocol using the same lower layer service and delivering the same service to the upper layer. Therefore, the security issues and mitigation techniques are mostly identical with same exceptions that are described further.

2.4.1. Demystifying some IPv6 Security Myths

Some people believe that IPv6 is inherently more secure than IPv4 because it is new. Nothing can be more wrong. Indeed, being a new protocol means that bugs in the implementations have yet to be discovered and fixed and that few people have the operational security expertise needed to operate securely an IPv6 network. This lack of operational expertise is the biggest threat when deploying IPv6: the importance of training is to be stressed again.

One security myth is that thanks to its huge address space, a network cannot be scanned by enumerating all IPv6 address in a /64 LAN hence a malevolent person cannot find a victim. [RFC5157] describes some alternate techniques to find potential targets on a network, for example enumerating all DNS names in a zone.

Another security myth is that IPv6 is more secure because it mandates the use of IPsec everywhere. [RFC6434] clearly states that the IPv6 support is a SHOULD only. Moreover, if all the intra-enterprise traffic is encrypted, then this renders all the network security tools (IPS, firewall, ACL, IPFIX, etc) blind and pretty much useless. Therefore, IPsec should be used in IPv6 pretty much like in IPv4 (for example to establish a VPN overlay over a non-trusted network or reserve to some specific applications).

The last security myth is that amplification attacks (such as http://www.cert.org/advisories/CA-1998-01.html) do not exist in IPv6 because there is no more broadcast. Alas, this is not true as ICMP error (in some cases) or information messages can be generated by routers and hosts when forwarding or receiving a multicast message

(section 2.4 of [RFC4443]). Therefore, the generation and the forwarding rate of ICMPv6 messages must be rate limited as in IPv4.

2.4.2. Similarities between IPv6 and IPv4 security

As mentioned earlier, IPv6 is quite similar to IPv4, therefore several attacks apply for both protocol family:

- Application layer attacks: such as cross-site scripting or SQL injection
- Rogue device: such as a rogue WiFi Access Point
- Flooding and all traffic based denial of services (including the use of control plane policing for IPv6 traffic see [RFC6192])
- Etc

A specific case of congruence is the IPv6 ULA [RFC4193] and IPv4 private addressing [RFC1918] that do not provide any security by 'magic'. In both case, the edge router must apply strict data plane and routing policy to block those private addresses to leave and enter the network. This filtering can be done by the enterprise or by the ISP.

IPv6 addresses can be spoofed as easily as IPv4 addresses and there are packets with bogons IPv6 addresses (see http://www.team-cymru.org/Services/Bogons/). The anti-bogon filtering must be done in the data and routing planes. It can be done by the enterprise or by the ISP.

2.4.3. Specific Security Issues for IPv6

Even if IPv6 is similar to IPv4, there are some differences that create some IPv6-only vulnerabilities or issues.

Privacy extension addresses [RFC4941] are usually to protect individual privacy by changing periodically the interface identifier part of the IPv6 address to avoid tracking a host by its always identical and unique EUI-64. While this presents a real advantage on the Internet, it complicates the task of audit trail when a security officer or network operator wants to trace back a log entry to a host in their network because when the tracing is done the searched IPv6 address could have disappeared from the network. A good way to prevent the use of privacy extension addresses without host configuration is to send the Router Advertisement with the M-bit set (to force the use of DHCPv6 to get an address) and with all advertized prefixes without the A-bit set (to prevent the use of

stateless auto-configuration).

Extension headers complicate the task of stateless packet filters such as ACL. If ACL are used to enforce a security policy, then the enterprise must verify whether its ACL (but also stateful firewalls) are able to process extension headers (this means understand them enough to parse them to find the upper layers payloads) and to block unwanted extension headers (e.g. to implement [RFC5095]).

Fragmentation is different in IPv6 because it is done only by source host and never during a forwarding operation. This means that ICMPv6 packet-too-big must be allowed [RFC4890] through all filters. Fragments can also be used to evade some security mechanisms such as RA-guard [RFC6105], see also [RFC5722]which appears to be widely implemented in 2012.

But, the biggest difference is the replacement of ARP (RFC 826) by Neighbor Discovery Protocol [RFC4861]. NDP runs over ICMPv6 (this means that security policies MUST allow some ICMPv6 messages see RFC 4890) but has the same lack of security as ARP (SeND [RFC3971] and CGA [RFC3972] are not widely implemented). ARP can be made secure with the help of techniques known as DHCPv4 snooping and dynamic ARP inspection by access switches. Therefore, enterprises using those techniques for IPv4 should use the equivalent techniques for IPv6: this is RA-guard (RFC 6105) and all work in progress from the SAVI WG ([I-D.ietf-savi-threat-scope] and others). Another DoS vulnerabilities are related to NDP cache exhaustion ([I-D.gashinsky-v6ops-v6nd-problems]) and they can be mitigated by careful tuning of the NDP cache. In 2012, there are already several vendors offering those features on their switches.

Running a dual-stack network doubles the attack exposure as a malevolent person has now two attack vectors: IPv4 and IPv6. This simply means that all routers and hosts operating in a dual-stack environment with both protocol families enabled (even if by default) must have a congruent security policy for both protocol version. For example, permit TCP ports 80 and 443 to all web servers and deny all other ports to the same servers must be implemented both for IPv4 and IPv6.

2.5. Address Plan

The most common problem encountered in IPv6 networking is in applying the same principles of conservation that are so important in IPv4. IPv6 addresses do not need to be assigned conservatively. In fact, a single larger allocation is considered more conservative than multiple discountiguous small blocks, because a single block occupies only a single entry in a routing table. The advice in [RFC5375] is

still sound, and is recommended to the reader. If considering ULAs, give careful consideration to how well it is supported, especially in multiple address and multicast scenarios, and assess the strength of the requirement for ULA.

The enterprise administrator will want to evaluate whether the enterprise will request address space from its ISP (or Local Internet Registry (LIR)), or whether to request address space from the local Internet Registry (whether a Regional Internet Registry such as AfriNIC, APNIC, ARIN, LACNIC, or RIPE-NCC, or a National Internet Registry, operated in some countries). There may be a registration fee for requesting provider-independent (PI) space from and NIR/RIR, but the enterprise will avoid some complexity if renumbering is required after changing ISPs (it should be noted that renumbering caused by outgrowing the space, merger, or other internal reason might not be avoided with PI space).

Each location, no matter how small, should get at least a /48. In addition to allowing for simple planning, this can allow a site to use its prefix for local connectivity, should the need arise, and if the local ISP supports it. Generally, workstations managed by the enterprise will use stateful DHCPv6 for addressing on corporate LAN segments. DHCPv6 allows for the additional configuration options often employed by enterprise administrators, and by using stateful DHCPv6, administrators correlating system logs know which system had which address at any given time.

In the data center or server room, assume a /64 per VLAN. This applies even if each individual system is on a separate VLAN; in a /48 assignment, typical for a site, there are 65,535 /64 blocks. Addresses are either configured manually on the server, or reserved on a DHCPv6 server, which may also synchronize forward and reverse DNS.

Plan to aggregate at every layer of network hierarchy. Where multiple VLANs or other layer two domains converge, allow some room for expansion. Renumbering due to outgrowing the network plan is a nuisance, so allow room within it. Generally, grow to about twice the current size can be accomodated; where rapid growth is planned, allow for twice that growth. Also, for any part of the network where DNS (or reverse DNS) zones may be delegated, it is important to delegate addresses on nibble boundaries, to ensure propose name delegation.

2.6. Program Planning

As with any project, an IPv6 deployment project will have its own phases. Generally, one person is identified as the project sponsor

or champion, who will make sure time and talent resources are prioritized appropriately for the project. Because enabling IPv6 can be a project with many interrelated tasks, identifying a project manager is also recommended. The project manager and sponsor can initiate the project, determining the scope of work and identifying whose input is required, and who will be affected by work. The scope will generally include the Preparation Phase, and may include the Internal Phase, the External Phase, or both, and may include any or all of the Other Phases identified.

The project manager will need to spend some time planning. It is often useful for the sponsor to communicate with stakeholders at this time, to explain why IPv6 is important to the enterprise. Then, as the project manager is assessing what systems and elements will be affected, the stakeholders will understand why it is important for them to support the effort. Well-informed project participants can help significantly by explaining the relationships between components. For a large enterprise, it may take several iterations to really understand the level of effort required; some systems will require additional development, some might require software updates, and others might need new versions or alternate vendors. Once the projects are understood, the project manager can develop a schedule and a budget, and work with the project sponsor to determine what constraints can be adjusted, if necessary.

It is tempting to roll IPv6 projects into other architectural upgrades - this can be an excellent way to improve the network and reduce costs. Project participants are advised that by increasing the scope of projects, the schedule is often affected. For instance, a major systems upgrade may take a year to complete, where just patching existing systems may take only a few months. Understanding and evaluating these trade-offs are why a project manager is important.

It is very common for assessments to continue in some areas even as execution of the project begins in other areas. This is fine, as long as recommendations in other parts of this document are considered, especially regarding security (for instance, one should not deploy IPv6 on a system before security has been evaluated). The project manager will need to continue monitoring the progress of discrete projects and tasks, to be aware of changes in schedule, budget, or scope. "Feature creep" is common, where engineers or management wish to add other features while IPv6 development or deployment is ongoing; each feature will need to be individually evaluated for its effect on the schedule and budget, and whether expanding the scope increases risk to any other part of the project.

As projects are completed, the project manager will confirm that work

has been completed, often by means of seeing a completed test plan, and will report back to the project sponsor on completed parts of the project. A good project manager will remember to thank the people who executed the project.

2.7. Tools Assessment

Enterprises will often have a number of operational tools and support systems which are used to provision, monitor, manage and diagnose the network and systems within their environment. These tools and systems will need to be assessed for compatibility with IPv6 operation. The compatibility may be related to actual addressing and connectivity of various devices as well as IPv6 awareness in many of tools and processing logic.

The tools within the organization fall into two general categories, those which focus on managing the network, and those which are focused on managing systems and applications on the network. In either instance, the tools will run on platforms which may or may not be capable of operating in an IPv6 network. This lack in functionality may be related to Operating system version, or based on some hardware constraint. Those systems which are found to be incapable of utilizing a IPv6 connection may need to be replaced or upgraded.

In addition to devices working on an IPv6 network natively, or via a tunnel, many tools and support systems may require additional updates to be IPv6 aware. This awareness may include the ability to manage IPv6 elements and/or applications in addition to the ability to store and utilize IPv6 addresses.

Considerations when assessing the tools and support systems may include the fact that IPv6 addresses are significantly larger then IPv4 requiring datastores to support the increased size. Such issues are among those discussed in [RFC5952]. Many organizations may also run dual stack networks, therefore the tools need not only support IPv6 operation, but may also need to support the monitoring, management and intersection with both IPv6 and IPv4 simultaneously. It is important to note that managing IPv6 is not just constrained to using large IPv6 addresses, but also that IPv6 interfaces and nodes may use two or more addresses as part of normal operation. Updating management systems to deal with these additional nuances will likely time time and considerable effort.

For networking focus systems, like node management systems, it is not always necessary to support local IPv6 addressing and connectivity. Operation, such as SNMP MIB polling can occur over IPv4 transport while seeking responses related to IPv6 information. Where this may

seem advantageous to some, it should be noted that without local IPv6 connectivity, the management system may not be able to perform all expected functions - such as reachability and service checks.

Organizations should be aware of changes to older IPv4-Only SNMP MIB specifications have been made by the IETF related to legacy operation in [RFC2096] and [RFC2011]. Updated specifications are now available in [RFC4296] and [RFC4293] which modified the older MIB framework to be IP protocol agnostic supporting IPv4 and IPv6. Polling systems will need to be upgraded to support these updates as well as the end stations which are polled.

3. External Phase

The external phase for Enterprise IPv6 adoption covers topics which deal with how an organization connects their infrastructure to the external world. These external connections may be toward the Internet at larges, or other networks. The external phase covers connectivity, security, monitoring of various elements and outward facing or accessible services.

How an organization connects to the outside worlds is very important as it is often a critical part of how a business functions, therefore must be dealt accordingly.

3.1. Connectivity

The Enterprise will need to work with one or more Service Providers to gain connectivity to the Internet or transport service infrastructure such as a BGP/MPLS IP VPN as described in [RFC4364] and [RFC4659]. On significant factor guiding how an organization may need to communist with the outside world will involve the use of PI (Provider Independent) and/or PA (Provider Aggregatable) IPv6 space.

In the case of PI, the organization will need to support BGP based connectivity for the most part since the address space is assigned direction from the Regional Registry to the local network. In this case, the local network would act as an Autonomous System on the Internet and must advertise routes accordingly. PA space is delegated form the upstream service provider and can then be assigned to the local network. If PA space is used, other forms of route exchange may be possible such as RIPng, OSPFv3 and static. PA assigned space would normally be routed to the general Internet via the upstream providers infrastructure lightening the burden on the local network administrations.

PI and PA space have additional contrasting behaviours when use such

as how dual homing may work. Should an operator choose to dual home, PI space would be routed to both upstream providers and then passed on to other networks. Utilizing more then one upstream Service Provider may introduce challenges since traffic utilizing a given PA assign block would be expected to flow tears the assigning provider for entry to the Internet. Should traffic flow using sources addresses which are not delegated form a given provider, reverse path forwarding rules on the operator side may reject some traffic. These considerations are quite different then those of IPv4 which relied on NAT in most cases.

When seeking IPv6 connectivity to a Service Provider, the Enterprise will want to attempt to use Native IPv6 connectivity. Native IPv6 connectivity is preferred since it provides the most rebuts form of connectivity. If Native IPv6 connectivity is not possible due to technical or business limitations, the Enterprise may utilize readily available tunnelled IPv6 connectivity. There are IPv6 transit providers which provide tunnelled IPv6 connectivity which can operate over IPv4 networks. A Enterprise need not need to wait for their local Service Provider to support IPv6, as tunnelled connectivity can be used.

3.2. Security

The most important part of security for external IPv6 deployment is filtering. Filtering can be done by stateless ACL or stateful firewall. As described in section 2.4.3, the security policies must be congruent for IPv4 and IPv6 except that ICMPv6 messages must be allowed through and to the filtering device (see [RFC4890]):

- unreachable packet-too-big
- unreachable parameter-problem
- neighbor solicitation
- neighbor advertisement

** Add some comment about setting MTU to 1280 to avoid tunnel pMTUd black holes? **

It could also be safer to block all fragments where the transport layer header is not in the first fragment to avoid attack as described in [RFC5722]. Some filtering devices allow this filtering. To be fully compliant with [RFC5095], it can be useful to drop all packet containing the routing extension header type 0.

If Intrusion Prevention Systems (IPS) are used for IPv4 traffic, then

the same IPS should also be used for IPv6 traffic. This is just a generalization of the dual-stack deployment: do for IPv6 what you do for IPv4. This also include all email content protection (anti-spam, content filtering, data leakage prevention, etc).

The peering router must also implement anti-spoofing technique based on [RFC2827].

In order to protect the networking device, it is advised to implement control plane policing as per [RFC6192].

The NDP cache exhaustion (see [I-D.gashinsky-v6ops-v6nd-problems]) attack can be mitigated by two techniques:

- good NDP implementation with memory utilization limits as well as rate-limiters and prioritization of requests.

- else, as the external deployment usually involves just a couple of exposed IPv6 statically configured addresses (virtual address of web, email servers, DNS server), then it is straightforward to build an ingress ACL allowing traffic for those addresses and denying traffic to any other addresses. This actually prevents the attack as packet for random destination will be dropped and will never trigger a neighbor resolution.

3.3. Monitoring

Monitoring the use of the Internet connectivity should be done for IPv6 if it is done for IPv4. This includes the use of IP flow export [RFC5102] to detect abnormal traffic pattern (such as port scanning, SYN-flooding) and SNMP MIB [RFC4293] (another way to detect abnormal bandwidth utilization).

3.4. Servers and Applications

4. Internal Phase

This phase deals with the delivery of IPv6 to the internal user facing side of the IT infrastructure, which comprises of various components such as network devices (routers, switches, etc.), end user devices and peripherals (workstations, printers, etc.), and internal corporate systems.

An important design paradigm to consider during this phase is "Dual Stack when you can, tunnel when you must". Dual stacking allows you to build a more robust IPv6 network that is of production quality as opposed to tunnels that are harder to troubleshoot and support.

Tunnels however do provide operators with a quick and easy way to play with IPv6 and gain some operational experience with the protocol. [RFC4213] describes various transition mechanisms in more detail.

4.1. Network Infrastructure

The typical enterprise network infrastructure comprises of a combination of the following network elements - wired access switches, wireless access points, and routers. Although, it is fairly common to find hardware that collapses switching and routing functionality into a single device. Basic wired access switches and access points that operate only at the physical and link layer, don't really have any special IPv6 considerations other than being able to support IPv6 addresses themselves for management purposes, if the same exists for IPv4. In many instances, these devices possess a lot more intelligence than simply switching packets. For example, some of these devices help assist with link layer security by incorporating features such as ARP inspection and DHCP Snooping.

An important design choice to be made is what IGP to use inside the network. A variety of IGPs (IS-IS, OSPFv3 and RIPng) support IPv6 today and picking one over the other is purely a design choice that will be dictated mostly by existing operational policies in an enterprise network. As mentioned earlier, it would be beneficial to maintain operational parity between IPv4 and IPv6 and therefore it might make sense to continue using the same protocol family that is being used for IPv4. For example, if you use OSPFv2 for IPv4, it might make sense to use OSPFv3 now.

Another important consideration in enterprise networks is first hop router redundancy. This directly ties into network reachability from an end host's point of view. IPv6 Neighbor Discovery (ND), [RFC4861], provides a node with the capability to maintain a list of available routers on the link, in order to be able to switch to a backup path should the primary be unreachable. By default, ND will detect a router failure in 38 seconds and cycle onto the next default router listed in its cache. While this feature does provide with a basic level of first hop router redundancy, most enterprise IPv4 networks are designed to fail over much faster. Although this delay can be improved by adjusting the default timers, care must be taken to protect against transient failures and to account for increased traffic on the link. Another option to provide robust first hop redundancy is to use the Virtual Router Redundancy Protocol for IPv6 (VRRPv3), [RFC5798]. This protocol provides a much faster switchover to an alternate default router than default ND parameters. Using VRRP, a backup router can take over for a failed default router in around three seconds (using VRRP default parameters). This is done

without any interaction with the hosts and a minimum amount of VRRP traffic.

Last but not the least, one of the most important design choices to make while deploying IPv6 on the internal network is whether to use Stateless Automatic Address Configuration (SLAAC), [RFC4862], or Dynamic Host Configuration Protocol for IPv6 (DHCPv6), [RFC3315], or a combination thereof (possible when using a /64 subnet). Each option has its own unique set of pros and cons and the choice will ultimately depend on the operational policies that guide each enterprise's network design. For example, if an enterprise is looking for ease of use, rapid deployments, and less administrative overhead, then SLAAC makes more sense. However, if the operational policies call for precise control over IP address assignment for auditing then DHCPv6 would be the way to go. DHCPv6 also allows you tie into DNS systems for host entry updates and gives you the ability to send other options information to clients. In the long term, DHCPv6 makes most sense for use in a managed environment.

4.2. End user devices

Most operating systems (OS) that are loaded on workstations and laptops in a typical enterprise support IPv6 today. However, there are various out-of-the-box nuances that one should be mindful about. For example, the default behavior of OSes vary, some may have IPv6 turned off entirely by default, some may only have certain features such as privacy addresses turned off while others have IPv6 fully enabled. It is important to note that most operating systems will, by default, prefer to use native IPv6 over IPv4 when enabled. Therefore, it is advised that enterprises investigate the default behavior of their installed OS base and account for it during the implementation of IPv6. Furthermore, some OSes may have tunneling mechanisms turned on by default and in such cases, it is recommended to administratively shut down such interfaces unless required. It is recommended that IPv6 be deployed at the network infrastructure level before it is rolled out to end user devices.

Smartphones and tablets are poised to become one of the major consumers of IP addresses and enterprises should be ready to deploy and support IPv6 on various networks that serve such devices. In general, support for IPv6 in these devices, albeit in its infancy, has been steadily rising. Most of the leading smartphone OSes have some level of support for IPv6. However, the level of configurable options are mostly at a minimum and are not consistent across all platforms. Also, it is fairly common to find IPv6 support on the wifi connection alone and not on the radio interface in these devices. This is sometimes due to the radio network not being ready or device related. An IPv6 enabled enterprise wifi network will

allow the majority of these devices to connect via IPv6. Much work is still being done to bring the full IPv6 feature set across all interfaces (802.11, 3G, LTE, etc.) and platforms.

IPv6 support in peripheral equipment such as printers, IP Cameras, etc. has been steadily rising as well, although at a much slower pace than traditional OSes and Smartphones. Most newer devices are coming out with IPv6 support but there is still a large installed base of legacy peripheral devices that might need IPv4 for sometime to come. The audit phase mentioned earlier will make it easier for enterprises to plan for equipment upgrades, in line with their corporate equipment refresh cycle.

4.3. Corporate Systems

No IPv6 deployment will be successful without ensuring that all the corporate systems that enterprise uses as part of their IT infrastructure, support IPv6. Examples of such systems include, but are not limited to, Email, Video Conferencing, Telephony (VoIP), DNS, Radius, etc. All these systems must have their own detailed IPv6 rollout plan in conjunction with the network IPv6 rollout. It is important to note that DNS is one of the main anchors in an enterprise deployment, since most end hosts decide whether or not use IPv6 based on the presence of AAAA records in a reply to a DNS query. It is recommended that system administrators selectively turn on AAAA records for various systems as and when they are IPv6 enabled. Additionally, all monitoring and reporting tools across the enterprise would need to be modified to support IPv6.

4.4. Security

IPv6 must be deployed in a secure way. This means that all existing IPv4 security policies must be extended to support IPv6; IPv6 security policies will be the IPv6 equivalent of the existing IPv4 ones (taking into account the difference for ICMPv6 [RFC4890]). As in IPv4, security policies for IPv6 will be enforced by firewalls, ACL, IPS, VPN, ...

Privacy extension addresses [RFC4941] pose a real challenge for audit trail. Therefore, it is recommended not to use them within the enterprise network by using the configuration described previously.

But, the biggest problem is probably linked to all threats against Neighbor Discovery. This means that the internal network at the access layer (i.e. where hosts connect to the network over wired or wireless) must implement RA-guard [RFC6105] and the techniques being specified by SAVI WG [I-D.ietf-savi-threat-scope].

5. Other Phases

To be added.

5.1. Guest network

To be added.

5.2. IPv6-only

Although IPv4 and IPv6 networks will coexist for a long time to come, the long term enterprise network roadmap should include steps on gradually deprecating IPv4 from the dual-stack network. In some extreme cases, deploying dual-stack networks may not even be a viable option for very large enterprises due to lack of availability of RFC 1918 addresses. In such cases, deploying IPv6-only networks might be the only choice available to sustain network growth.

If nodes in the network don't need to talk to an IPv4-only node, then deploying IPv6-only networks should fe fairly trivial. However, in the current environment, given that IPv4 is the dominant protocol on the Internet, an IPv6-only node most likely needs to talk to an IPv4-only node on the Internet. It is therefore important to provide such nodes with a translation mechanism to ensure communication between nodes configured with different address families. As [RFC6144] points out, it is important to look at address translation as a transition strategy that will get you to an IPv6-only network.

There are various stateless and stateful IPv4/IPv6 translation methods available today that help IPv4 to IPv6 communication. RFC 6144 provides a framework for IPv4/IPv6 translation and describes in detail various scenarios in which such translation mechanisms could be used. [RFC6145] describes stateless address translation. In this mode, a specific IPv6 address range will represent IPv4 systems (IPv4-converted addresses), and the IPv6 systems have addresses (IPv4-translateable addresses) that can be algorithmically mapped to a subset of the service provider's IPv4 addresses. [RFC6146], NAT64, describes stateful address translation. As the name suggests, the translation state is maintained between IPv4 address/port pairs and IPv6 address/port pairs, enabling IPv6 systems to open sessions with IPv4 systems. [RFC6147], DNS64, describes a mechanism for synthesizing AAAA resource records (RRs) from A RRs. Together, RFCs 6146 and RFC 6147 provide a viable method for an IPv6-only client to initiate communications to an IPv4-only server.

The address translation mechanisms for the stateless and stateful translations are defined in [RFC6052]. It is important to note that both of these mechanisms have limitations as to which protocols they

support. For example, RFC 6146 only defines how stateful NAT64 translates unicast packets carrying TCP, UDP, and ICMP traffic only. The ultimate choice of which translation mechanism to chose will be dictated mostly by existing operational policies pertaining to application support, logging requirements, etc.

There is additional work being done in the area of address translation to enhance and/or optimize current mechanisms. For example, [I-D.xli-behave-divi] describes limitations with the current stateless translation, such as IPv4 address sharing and application layer gateway (ALG) problems, and presents the concept and implementation of dual-stateless IPv4/IPv6 translation (dIVI) to address those issues.

6. Considerations For Specific Enterprises

6.1. Content Delivery Networks

To be added.

6.2. Data Centre Virtualisation

To be added.

6.3. Campus Networks

A number of campus networks have made some initial IPv6 deployment. There are generally three areas in which such deployments may be made, which correspond to the Internal Phase, External Phase and Other Phase (Guest Network) descrobed above.

In particular the areas commonly approached are:

- External-facing services. Typically the campus web presence and commonly also external-facing DNS and MX services.

- Computer science department. This is where IPv6-related research and/or teaching is most likely to occur, so enabling some or all of the campus compauter science department network is a sensible first step.

- The eduroam wireless network. Eduroam is the defacto wireless roaming system for academic networks, and uses 802.1X based authentication, which is agnotic to the IP version used (unlike web-redirection gateway systems).

7. Security Considerations

8. IANA Considerations

There are no IANA considerations or implications that arise from this document.

9. Informative References

[RFC1918] Rekhter, Y., Moskowitz, R., Karrenberg, D., Groot, G., and E. Lear, "Address Allocation for Private Internets", BCP 5, RFC 1918, February 1996.

[RFC2011] McCloghrie, K., "SNMPv2 Management Information Base for the Internet Protocol using SMIv2", RFC 2011, November 1996.

[RFC2096] Baker, F., "IP Forwarding Table MIB", RFC 2096, January 1997.

[RFC2827] Ferguson, P. and D. Senie, "Network Ingress Filtering: Defeating Denial of Service Attacks which employ IP Source Address Spoofing", BCP 38, RFC 2827, May 2000.

[RFC3315] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003.

[RFC3971] Arkko, J., Kempf, J., Zill, B., and P. Nikander, "SEcure Neighbor Discovery (SEND)", RFC 3971, March 2005.

[RFC3972] Aura, T., "Cryptographically Generated Addresses (CGA)", RFC 3972, March 2005.

[RFC4057] Bound, J., "IPv6 Enterprise Network Scenarios", RFC 4057, June 2005.

[RFC4193] Hinden, R. and B. Haberman, "Unique Local IPv6 Unicast Addresses", RFC 4193, October 2005.

[RFC4213] Nordmark, E. and R. Gilligan, "Basic Transition Mechanisms for IPv6 Hosts and Routers", RFC 4213, October 2005.

[RFC4293] Routhier, S., "Management Information Base for the Internet Protocol (IP)", RFC 4293, April 2006.

[RFC4296] Bailey, S. and T. Talpey, "The Architecture of Direct Data Placement (DDP) and Remote Direct Memory Access (RDMA) on Internet Protocols", RFC 4296, December 2005.

[RFC4364] Rosen, E. and Y. Rekhter, "BGP/MPLS IP Virtual Private Networks (VPNs)", RFC 4364, February 2006.

[RFC4443] Conta, A., Deering, S., and M. Gupta, "Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification", RFC 4443, March 2006.

[RFC4659] De Clercq, J., Ooms, D., Carugi, M., and F. Le Faucheur, "BGP-MPLS IP Virtual Private Network (VPN) Extension for IPv6 VPN", RFC 4659, September 2006.

[RFC4861] Narten, T., Nordmark, E., Simpson, W., and H. Soliman, "Neighbor Discovery for IP version 6 (IPv6)", RFC 4861, September 2007.

[RFC4862] Thomson, S., Narten, T., and T. Jinmei, "IPv6 Stateless Address Autoconfiguration", RFC 4862, September 2007.

[RFC4890] Davies, E. and J. Mohacsi, "Recommendations for Filtering ICMPv6 Messages in Firewalls", RFC 4890, May 2007.

[RFC4941] Narten, T., Draves, R., and S. Krishnan, "Privacy Extensions for Stateless Address Autoconfiguration in IPv6", RFC 4941, September 2007.

[RFC5095] Abley, J., Savola, P., and G. Neville-Neil, "Deprecation of Type 0 Routing Headers in IPv6", RFC 5095, December 2007.

[RFC5102] Quittek, J., Bryant, S., Claise, B., Aitken, P., and J. Meyer, "Information Model for IP Flow Information Export", RFC 5102, January 2008.

[RFC5157] Chown, T., "IPv6 Implications for Network Scanning", RFC 5157, March 2008.

[RFC5211] Curran, J., "An Internet Transition Plan", RFC 5211, July 2008.

[RFC5375] Van de Velde, G., Popoviciu, C., Chown, T., Bonness, O., and C. Hahn, "IPv6 Unicast Address Assignment Considerations", RFC 5375, December 2008.

[RFC5722] Krishnan, S., "Handling of Overlapping IPv6 Fragments",

RFC 5722, December 2009.

[RFC5798] Nadas, S., "Virtual Router Redundancy Protocol (VRRP) Version 3 for IPv4 and IPv6", RFC 5798, March 2010.

[RFC5952] Kawamura, S. and M. Kawashima, "A Recommendation for IPv6 Address Text Representation", RFC 5952, August 2010.

[RFC6052] Bao, C., Huitema, C., Bagnulo, M., Boucadair, M., and X. Li, "IPv6 Addressing of IPv4/IPv6 Translators", RFC 6052, October 2010.

[RFC6104] Chown, T. and S. Venaas, "Rogue IPv6 Router Advertisement Problem Statement", RFC 6104, February 2011.

[RFC6105] Levy-Abegnoli, E., Van de Velde, G., Popoviciu, C., and J. Mohacsi, "IPv6 Router Advertisement Guard", RFC 6105, February 2011.

[RFC6144] Baker, F., Li, X., Bao, C., and K. Yin, "Framework for IPv4/IPv6 Translation", RFC 6144, April 2011.

[RFC6145] Li, X., Bao, C., and F. Baker, "IP/ICMP Translation Algorithm", RFC 6145, April 2011.

[RFC6146] Bagnulo, M., Matthews, P., and I. van Beijnum, "Stateful NAT64: Network Address and Protocol Translation from IPv6 Clients to IPv4 Servers", RFC 6146, April 2011.

[RFC6147] Bagnulo, M., Sullivan, A., Matthews, P., and I. van Beijnum, "DNS64: DNS Extensions for Network Address Translation from IPv6 Clients to IPv4 Servers", RFC 6147, April 2011.

[RFC6192] Dugal, D., Pignataro, C., and R. Dunn, "Protecting the Router Control Plane", RFC 6192, March 2011.

[RFC6302] Durand, A., Gashinsky, I., Lee, D., and S. Sheppard, "Logging Recommendations for Internet-Facing Servers", BCP 162, RFC 6302, June 2011.

[RFC6434] Jankiewicz, E., Loughney, J., and T. Narten, "IPv6 Node Requirements", RFC 6434, December 2011.

[I-D.xli-behave-divi]
Shang, W., Li, X., Zhai, Y., and C. Bao, "dIVI: Dual-Stateless IPv4/IPv6 Translation", draft-xli-behave-divi-04 (work in progress), October 2011.

[I-D.gashinsky-v6ops-v6nd-problems]
Jaeggli, J., Kumari, W., and I. Gashinsky, "Operational Neighbor Discovery Problem", draft-gashinsky-v6ops-v6nd-problems-00 (work in progress), October 2011.

[I-D.ietf-savi-threat-scope]
McPherson, D., Baker, F., and J. Halpern, "SAVI Threat Scope", draft-ietf-savi-threat-scope-05 (work in progress), April 2011.

Authors' Addresses

Lee Howard
Time Warner Cable
13820 Sunrise Valley Drive
Herndon, VA 20171
US

Phone: +1 703 345 3513
Email: lee.howard@twcable.com

Tim Chown
University of Southampton
Highfield
Southampton, Hampshire SO17 1BJ
United Kingdom

Email: tjc@ecs.soton.ac.uk

Kiran K. Chittimaneni
Google Inc.
1600 Amphitheater Pkwy
Mountain View, California CA 94043
USA

Email: kk@google.com

Yanick Pouffary
Hewlett Packard
950 Route Des Colles
Sophia-Antipolis 06901
France

Email: Yanick.Pouffary@hp.com

Eric Vyncke
Cisco Systems
De Kleetlaan 6a
Diegem 1831
Belgium

Phone: +32 2 778 4677
Email: evyncke@cisco.com

Victor Kuarsingh
Rogers Communications
8200 Dixie Road
Brampton, Ontario
Canada

Email: victor.kuarsingh@rci.rogers.com