

IPv6 Enterprise Network Scenarios

Status of This Memo

This memo provides information for the Internet community. It does not specify an Internet standard of any kind. Distribution of this memo is unlimited.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document describes the scenarios for IPv6 deployment within enterprise networks. It defines a small set of basic enterprise scenarios and includes pertinent questions to allow enterprise administrators to further refine their deployment scenarios. Enterprise deployment requirements are discussed in terms of coexistence with IPv4 nodes, networks and applications, and in terms of basic network infrastructure requirements for IPv6 deployment. The scenarios and requirements described in this document will be the basis for further analysis to determine what coexistence techniques and mechanisms are needed for enterprise IPv6 deployment. The results of that analysis will be published in a separate document.

Table of Contents

1.	Introduction.....	2
2.	Terminology.....	3
3.	Base Scenarios.....	4
3.1.	Base Scenarios Defined.....	4
3.2.	Scenarios Network Infrastructure Components.....	5
3.3.	Specific Scenario Examples.....	8
3.4.	Applicability Statement.....	10
4.	Network Infrastructure Component Requirements.....	10
4.1.	DNS.....	11
4.2.	Routing.....	11
4.3.	Configuration of Hosts.....	11
4.4.	Security.....	11
4.5.	Applications.....	12
4.6.	Network Management.....	12
4.7.	Address Planning.....	12

4.8. Multicast.....	12
4.9. Multihoming.....	12
5. Security Considerations.....	12
6. Normative References.....	13
Acknowledgements.....	13

1. Introduction

This document describes the scenarios for IPv6 deployment within enterprise networks. It defines a small set of basic enterprise scenarios and includes pertinent questions to allow enterprise administrators to further refine their deployment scenarios. Enterprise deployment requirements are discussed in terms of coexistence with IPv4 nodes, networks and applications, and in terms of basic network infrastructure requirements for IPv6 deployment. The scenarios and requirements described in this document will be the basis for further analysis to determine what coexistence techniques and mechanisms are needed for enterprise IPv6 deployment. The results of that analysis will be published in a separate document.

The audience for this document is the enterprise network team considering deployment of IPv6. The document will be useful for enterprise teams that will have to determine the IPv6 transition strategy for their enterprise. It is expected those teams include members from management, network operations, and engineering. The scenarios presented provide an example set of cases the enterprise can use to build an IPv6 network scenario.

To frame the discussion, this document will describe a set of scenarios each with a network infrastructure. It is impossible to define every possible enterprise scenario that will apply to IPv6 adoption and transition.

Each enterprise will select the transition that best supports their business requirements. Any attempt to define a default or one-size-fits-all transition scenario, simply will not work. This document does not try to depict the drivers for adoption of IPv6 by an enterprise.

While it is difficult to quantify all the scenarios for an enterprise network team to plan for IPv6, it is possible to depict a set of abstract scenarios that will assist with planning. This document presents three base scenarios to be used as models by enterprises defining specific scenarios.

The first scenario assumes the enterprise decides to deploy IPv6 in conjunction with IPv4. The second scenario assumes the enterprise decides to deploy IPv6 because of a specific set of applications that

it wants to use over an IPv6 network. The third scenario assumes an enterprise is building a new network or restructuring an existing network and decides to deploy IPv6 as the predominant protocol within the enterprise coexisting with IPv4. This document then briefly reviews a set of network infrastructure components that must be analyzed, which are common to most enterprises.

This document then provides three specific scenario examples using the network infrastructure components to depict the requirements. These are common enterprise deployment cases to depict the challenges for the enterprise to transition a network to IPv6.

Next, supporting legacy functions on the network (while the transition is in process), and the network infrastructure components requiring analysis by the enterprise are discussed. The interoperation with legacy functions within the enterprise will be required for all transition except possibly by a new network that will be IPv6 from inception. The network infrastructure components will depict functions in their networks that require consideration for IPv6 deployment and transition.

Using the scenarios, network infrastructure components, and examples in this document, an enterprise can define its specific scenario requirements. Understanding the legacy functions and network infrastructure components required, the enterprise can determine the network operations required to deploy IPv6. The tools and mechanisms to support IPv6 deployment operations will require enterprise analysis. The analysis to determine the tools and mechanisms to support the scenarios will be presented in subsequent document(s).

2. Terminology

- Enterprise Network - 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.
- Provider - An entity that provides services and connectivity to the Internet or other private external networks for the enterprise network.
- IPv6 Capable - A node or network capable of supporting both IPv6 and IPv4.
- IPv4 only - A node or network capable of supporting only IPv4.

- IPv6 only - A node or network capable of supporting only IPv6. This does not imply an IPv6 only stack in this document.

3. Base Scenarios

Three base scenarios are defined to capture the essential abstraction set for the enterprise. Each scenario has assumptions and requirements. This is not an exhaustive set of scenarios, but a base set of general cases.

Below we use the term network infrastructure to mean the software, network operations and configuration, and methods used to operate a network in an enterprise.

For the base scenarios it is assumed that any IPv6 node is IPv6 capable.

3.1. Base Scenarios Defined

Scenario 1: Wide-scale/total dual-stack deployment of IPv4 and IPv6 capable hosts and network infrastructure. Enterprise with an existing IPv4 network wants to deploy IPv6 in conjunction with their IPv4 network.

Assumptions: The IPv4 network infrastructure used has an equivalent capability in IPv6.

Requirements: Do not disrupt existing IPv4 network infrastructure assumptions with IPv6. IPv6 should be equivalent or "better" than the network infrastructure in IPv4. However, it is understood that IPv6 is not required to solve current network infrastructure problems, not solved by IPv4. It may also not be feasible to deploy IPv6 on all parts of the network immediately.

Scenario 2: Sparse IPv6 dual-stack deployment in IPv4 network infrastructure. Enterprise with an existing IPv4 network wants to deploy a set of particular IPv6 "applications" (application is voluntarily loosely defined here, e.g., peer to peer). The IPv6 deployment is limited to the minimum required to operate this set of applications.

Assumptions: IPv6 software/hardware components for the application are available, and platforms for the application are IPv6 capable.

Requirements: Do not disrupt IPv4 infrastructure.

Scenario 3: IPv6-only network infrastructure with some IPv4-capable nodes/applications needing to communicate over the IPv6 infrastructure. Enterprise deploying a new network or restructuring an existing network, decides IPv6 is the basis for most network communication. Some IPv4 capable nodes/applications will need to communicate over that infrastructure.

Assumptions: Required IPv6 network infrastructure is available, or available over some defined timeline, supporting the enterprise plan.

Requirements: Interoperation and Coexistence with IPv4 network infrastructure and applications are required for communications.

3.2. Scenarios Network Infrastructure Components

This section defines the network infrastructure that exists for the above enterprise scenarios. This is not an exhaustive list, but a base list that can be expanded by the enterprise for specific deployment scenarios. The network infrastructure components are presented as functions that the enterprise must analyze as part of defining their specific scenario. The analysis of these functions will identify actions that are required to deploy IPv6.

Network Infrastructure Component 1

Enterprise Provider Requirements

- Is external connectivity required?
- One site vs. multiple sites and are they within different geographies?
- Leased lines or VPNs?
- If multiple sites, how is the traffic exchanged securely?
- How many global IPv4 addresses are available to the enterprise?
- What is the IPv6 address assignment plan available from the provider?
- What prefix delegation is required by the Enterprise?
- Will the enterprise be multihomed?
- What multihoming techniques are available from the provider?
- Will clients within the enterprise be multihomed?
- Does the provider offer any IPv6 services?
- Which site-external IPv6 routing protocols are required?
- Is there an external data center to the enterprise, such as servers located at the Provider?
- Is IPv6 available using the same access links as IPv4, or different ones?

Network Infrastructure Component 2

Enterprise Application Requirements

- List of applications in use?
- Which applications must be moved to support IPv6 first?
- Can the application be upgraded to IPv6?
- Will the application have to support both IPv4 and IPv6?
- Do the enterprise platforms support both IPv4 and IPv6?
- Do the applications have issues with NAT v4-v4 and NAT v4-v6?
- Do the applications need globally routable IP addresses?
- Do the applications care about dependency between IPv4 and IPv6 addresses?
- Are applications run only on the internal enterprise network?

Network Infrastructure Component 3

Enterprise IT Department Requirements

- Who "owns"/"operates" the network: in house or outsourced?
- Is working remotely (i.e., through VPNs) supported?
- Are inter-site communications required?
- Is network mobility used or required for IPv6?
- What are the requirements of the IPv6 address plan?
- Is there a detailed asset management database, including hosts, IP/MAC addresses, etc.?
- What is the enterprise's approach to numbering geographically separate sites that have their own Service Providers?
- What will be the internal IPv6 address assignment procedure?
- What site internal IPv6 routing protocols are required?
- What will be the IPv6 Network Management policy/procedure?
- What will be the IPv6 QOS policy/procedure?
- What will be the IPv6 Security policy/procedure?
- What is the IPv6 training plan to educate the enterprise?
- What network operations software will be impacted by IPv6?
 - DNS
 - Management (SNMP & ad-hoc tools)
 - Enterprise Network Servers Applications
 - Mail Servers
 - High Availability Software for Nodes
 - Directory Services
 - Are all these software functions upgradeable to IPv6?
 - If not upgradeable, then what are the workarounds?
 - Do any of the software functions store, display, or allow input of IP addresses?
 - Other services (e.g., NTP, etc.)

- What network hardware will be impacted by IPv6?
 - Routers/switches
 - Printers/Faxes
 - Firewalls
 - Intrusion Detection
 - Load balancers
 - VPN Points of Entry/Exit
 - Security Servers and Services
 - Network Interconnect for Platforms
 - Intelligent Network Interface Cards
 - Network Storage Devices
 - Are all these hardware functions upgradeable to IPv6?
 - If not, what are the workarounds?
 - Do any of the hardware functions store, display, or allow input of IP addresses?
- Are the nodes moving within the enterprise network?
- Are the nodes moving outside and inside the enterprise network?

Network Infrastructure Component 4

Enterprise Network Management System

- Performance Management required?
- Network Management applications required?
- Configuration Management required?
- Policy Management and Enforcement required?
- Security Management required?
- Management of Transition Tools and Mechanisms?
- What new considerations does IPv6 create for Network Management?

Network Infrastructure Component 5

Enterprise Network Interoperation and Coexistence

- What platforms are required to be IPv6 capable?
- What network ingress and egress points to the site are required to be IPv6 capable?
- What transition mechanisms are needed to support IPv6 network operations?
- What policy/procedures are required to support the transition to IPv6?
- What policy/procedures are required to support interoperation with legacy nodes and applications?

3.3. Specific Scenario Examples

This section presents a set of base scenario examples and is not an exhaustive list of examples. These examples were selected to provide further clarity for base scenarios within an enterprise of a less abstract nature. The example networks may use the scenarios depicted in 3.1 and the infrastructure components in 3.2, but there are no direct implications specifically within these example networks. Section 3.1, 3.2, and 3.3 should be used in unison for enterprise IPv6 deployment planning and analysis.

Example Network A:

A distributed network across a number of geographically separated campuses.

- External network operation.
- External connectivity required.
- Multiple sites connected by leased lines.
- Provider independent IPv4 addresses.
- ISP does not offer IPv6 service.
- Private Leased Lines no Service Provider used.

Applications run by the enterprise:

- Internal Web/Mail.
- File servers.
- Java applications.
- Collaborative development tools.
- Enterprise Resource applications.
- Multimedia applications.
- Financial Enterprise applications.
- Data Warehousing applications.

Internal network operation:

- In house operation of the network.
- DHCP (v4) is used for all desktops; servers use static address configuration.
- The DHCP server that updates naming records for dynamic desktops uses dynamic DNS.
- A web based tool is used to enter name to address mappings for statically addressed servers.
- Network management is done using SNMP.
- All routers and switches are upgradeable to IPv6.
- Existing firewalls can be upgraded to support IPv6 rules.

- Load balancers do not support IPv6, upgrade path unclear.
- Peer-2-Peer Application and Security supported.
- IPv4 Private address space is used within the enterprise.

Example Network B:

A bank running a large network supporting online transaction processing (OLTP) across a distributed multi-sited network, with access to a central database on a remote network from the OLTP network.

- External connectivity not required.
- Multiple sites connected by VPN.
- Multiple sites connected by Native IP protocol.
- Private address space used with NAT.
- Connections to private exchanges.

Applications in the enterprise:

- ATM transaction application.
- ATM management application.
- Financial Software and Database.
- Part of the workforce is mobile and requires access to the enterprise from outside networks.

Internal Network Operation:

- Existing firewalls can be upgraded to support IPv6 rules.
- Load balancers do not support IPv6, upgrade path unclear.
- Identifying and managing each node's IP address.

Example Network C:

A Security Defense, Emergency, or other Mission Critical network operation:

- External network required at secure specific points.
- Network is its own Internet.
- Network must be able to absorb ad-hoc creation of sub-networks.
- Entire parts of the network are completely mobile.
- All nodes on the network can be mobile (including routers).
- Network high-availability is mandatory.
- Network must be able to be managed from ad-hoc location.
- All nodes must be able to be configured from stateless mode.

Applications run by the Enterprise:

- Multimedia streaming of audio, video, and data for all nodes.
- Data computation and analysis on stored and created data.
- Transfer of data coordinate points to sensor devices.
- Data and Intelligence gathering applications from all nodes.

Internal Network Operations:

- All packets must be secured end-2-end with encryption.
- Intrusion Detection exists on all network entry points.
- Network must be able to bolt on to the Internet to share bandwidth as required from Providers.
- VPNs can be used, but NAT can never be used.
- Nodes must be able to access IPv4 legacy applications over IPv6 network.

3.4. Applicability Statement

The specific network scenarios selected are chosen to depict a base set of examples, and to support further analysis of enterprise networks. This is not a complete set of network scenarios. Though Example Network C is a verifiable use case, currently the scenario defines an early adopter of enterprise networks transitioning to IPv6 as a predominant protocol strategy (i.e., IPv6 Routing, Applications, Security, and Operations), viewing IPv4 as legacy operations immediately in the transition strategy, and at this time may not be representative of many initial enterprise IPv6 deployments. Each enterprise planning team will need to make that determination as IPv6 deployment evolves.

4. Network Infrastructure Component Requirements

The enterprise will need to determine which network infrastructure components require enhancements or need to be added for deployment of IPv6. This infrastructure will need to be analyzed and understood as a critical resource to manage. The list in this section is not exhaustive, but contains the essential network infrastructure components for the enterprise to consider before beginning to define more fine-tuned requirements such as QOS, PKI, or Bandwidth requirements for IPv6. The components are only identified here and their details will be discussed in the analysis document for enterprise scenarios. References currently available for components are provided.

4.1. DNS

DNS will now have to support both IPv4 and IPv6 DNS records and the enterprise will need to determine how the DNS is to be managed and accessed, and secured. The range of DNS operational issues is beyond the scope of this document. However, DNS resolution and transport solutions for both IP protocols are influenced by the chosen IPv6 deployment scenario. Users need to consider all current DNS IPv4 operations and determine if those operations are supported for IPv6 [DNSV6].

4.2. Routing

Interior and Exterior routing will be required to support both IPv4 and IPv6 routing protocols, and the coexistence of IPv4 and IPv6 over the enterprise network. The enterprise will need to define the IPv6 routing topology, any ingress and egress points to provider networks, and transition mechanisms that they wish to use for IPv6 adoption. The enterprise will also need to determine what IPv6 transition mechanisms are supported by their upstream providers.

4.3. Configuration of Hosts

IPv6 introduces the concept of stateless autoconfiguration in addition to stateful autoconfiguration, for the configuration of hosts within the enterprise. The enterprise will have to determine the best method of host configuration for its network, if it will use stateless or stateful autoconfiguration, and how autoconfiguration will operate for DNS updates. It will also need to determine how prefix delegation will be done from their upstream provider and how those prefixes will be cascaded down to the enterprise IPv6 network. The policy for DNS or choice of autoconfiguration is out of scope for this document [CONF, DHCPF, DHCPPL].

4.4. Security

Current existing mechanisms used for IPv4 to provide security need to be supported for IPv6 within the enterprise. IPv6 should create no new security concerns for IPv4. The entire security infrastructure currently used in the enterprise needs to be analyzed against IPv6 deployment effect to determine what is supported in IPv6. Users should review other current security IPv6 network infrastructure work in the IETF and within the industry. Users will have to work with their platform and software providers to determine which IPv6 security network infrastructure components are supported. The security filters and firewall requirements for IPv6 need to be determined by the enterprise. The policy choice of users for security is beyond the scope of this document.

4.5. Applications

Existing applications will need to be ported or provide proxies to support both IPv4 and IPv6 [APPS].

4.6. Network Management

The addition of IPv6 network infrastructure components will need to be managed by the enterprise network operations center. Users will need to work with their network management platform providers to determine what is supported for IPv6 while planning IPv6 adoption, and which tools are available to monitor the network. Network management will not need to support both IPv4 and IPv6 and view nodes as dual stacks.

4.7. Address Planning

The address space within the enterprise will need to be defined and coordinated with the routing topology of the enterprise network. It is also important to identify the pool of IPv4 address space available to the enterprise to assist with IPv6 transition methods.

4.8. Multicast

Enterprises utilizing IPv4 Multicast services will need to consider how these services may be implemented operationally in an IPv6-enabled environment.

4.9. Multihoming

At this time, current IPv6 allocation policies are mandating the allocation of IPv6 address space from the upstream provider. If an enterprise is multihomed, the enterprise will have to determine how it wishes to support multihoming. This also is an area of study within the IETF and work in progress.

5. Security Considerations

This document lists scenarios for the deployment of IPv6 in enterprise networks, and there are no security considerations associated with making such a list.

There will be security considerations for the deployment of IPv6 in each of these scenarios, but they will be addressed in the document that includes the analysis of each scenario.

6. Normative References

- [DNSV6] Durand, A., Ihren, J., and P. Savola, "Operational Considerations and Issues with IPv6 DNS", Work in Progress.
- [CONF] Thomson, S. and T. Narten, "IPv6 Stateless Address Autoconfiguration", RFC 2462, December 1998.
- [DHCPF] Droms, R., Bound, J., Volz, B., Lemon, T., Perkins, C., and M. Carney, "Dynamic Host Configuration Protocol for IPv6 (DHCPv6)", RFC 3315, July 2003
- [DHCPL] Nikander, P., Kempf, J., and E. Nordmark, "IPv6 Neighbor Discovery (ND) Trust Models and Threats", RFC 3756, May 2004.
- [APPS] Shin, M-K., Hong, Y-G., Hagino, J., Savola, P., and E. Castro, "Application Aspects of IPv6 Transition", RFC 4038, March 2005.

Acknowledgements

The Authors would like to acknowledge contributions from the following: IETF v6ops Working Group, Alan Beard, Brian Carpenter, Alain Durand, Bob Hinden, and Pekka Savola.

Authors' Addresses

Yanick Pouffary (Chair of Design Team)
HP Competency Center
950, Route des Colles, BP027,
06901 Sophia Antipolis CEDEX
FRANCE

Phone: + 33492956285
EMail: Yanick.pouffary@hp.com

Jim Bound (Editor)
Hewlett Packard
110 Spitbrook Road
Nashua, NH 03062
USA

Phone: (603) 884-0062
EMail: jim.bound@hp.com

Marc Blanchet
Viagenie inc.
2875 boul. Laurier, bur. 300
Ste-Foy, Quebec, G1V 2M2
Canada

EMail: Marc.Blanchet@viagenie.qc.ca

Tony Hain
Cisco Systems
500 108th Ave. N.E. Suite 400
Bellevue, WA 98004
USA

EMail: alh-ietf@tndh.net

Paul Gilbert
Cisco Systems
1 Penn Plaza, 5th floor,
NY, NY 10119
USA

Phone: (212) 714-4334
EMail: pgilbert@cisco.com

Margaret Wasserman
ThingMagic
One Broadway
Cambridge, MA 02142
USA

Phone: (617) 758-4177
EMail: margaret@thingmagic.com

Jason Goldschmidt
Sun Microsystems
M/S UMPK17-103
17 Network Circle
Menlo Park, CA 94025
USA

Phone: (650) 786-3502
Fax: (650) 786-8250
EMail: jason.goldschmidt@sun.com

Aldrin Isaac
Bloomberg L.P.
499 Park Avenue
New York, NY 10022
USA

Phone: (212) 940-1812
EMail: aisaac@bloomberg.com

Tim Chown
School of Electronics and Computer Science
University of Southampton
Southampton SO17 1BJ
United Kingdom

EMail: tjc@ecs.soton.ac.uk

Jordi Palet Martinez
Consulintel
San Jose Artesano, 1
Madrid, SPAIN

Phone: +34 91 151 81 99
Fax: +34 91 151 81 98
EMail: jordi.palet@consulintel.es

Fred Templin
Nokia
313 Fairchild Drive
Mountain View, CA 94043
USA

Phone: (650) 625-2331
EMail: ftemplin@iprg.nokia.com

Roy Brabson
IBM
PO BOX 12195
3039 Cornwallis Road
Research Triangle Park, NC 27709
USA

Phone: (919) 254-7332
EMail: rbrabson@us.ibm.com

Full Copyright Statement

Copyright (C) The Internet Society (2005).

This document is subject to the rights, licenses and restrictions contained in BCP 78, and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in BCP 78 and BCP 79.

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgement

Funding for the RFC Editor function is currently provided by the Internet Society.

