IPv6 Operations (v6ops)
Internet Draft
Document: draft-pouffary-v6ops-ent-v6net-03.txt
Obsoletes: draft-pouffary-v6ops-ent-v6net-02.txt
Obsoletes: draft-ietf-v6ops-entnet-scenarios-00.txt
Expires: December 2003

J. Bound (Editor)
See Author Section

June 2003

IPv6 Enterprise Networks Scenarios

draft-pouffary-v6ops-ent-v6net-03.txt

Status of this Memo

Abstract

This document describes the scenarios for IPv6 deployment within Enterprise networks. It will focus upon an Enterprise set of network base scenarios with assumptions, coexistence with legacy IPv4 nodes, networks, and applications, and network infrastructure requirements. These requirements will be used to provide analysis to determine a set of Enterprise solutions in a later document.

Table of Contents

1. Introduction

This document describes the scenarios for IPv6 deployment within Enterprise networks. It will focus upon an Enterprise set of network base scenarios with assumptions, coexistence with legacy IPv4 nodes, networks, and applications, and network infrastructure requirements. These requirements will be used to provide analysis to determine a set of Enterprise solutions in a later document.

The audience for this document is the enterprise network team considering deployment of IPv6.

To frame the discussion the document will describe a set of scenarios and characteristics for each scenario and then follow those sets with example scenario use, and points of transition.

Each enterprise will need to select the transition to best suit their business requirements. Any attempt to define a default or one-size-fits-all transition scenario will simply not work.

While it is difficult to quantify all the potential motivations for enterprise network teams to move to IPv6, there are some cases where an abstract description is possible.

2. Terminology

Enterprise Network	- An Enterprise Network is a network that has multiple links, a router connection to a Provider, and is actively managed by a network operations entity.
Provider	- A Provider is an entity that provides services and connectivity to the Internet or other private external networks for the Enterprise Network.
IPv6/IPv4	- 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.

3. Network Base Scenarios

Three base scenarios are defined to capture the essential abstraction set for the Enterprise. Each scenario has assumptions and requirements.

These scenarios will drive the network characteristics and then examples for use by this document.

3.1 Network Base Scenarios Defined

Scenario 1: Enterprise with an existing IPv4 network wants to deploy IPv6 in parallel with their IPv4 network.

- Assumptions: The IPv4 characteristics have an equivalent in IPv6.
- Requirements: Don't break IPv4 network characteristics assumptions with IPv6. IPv6 should be equivalent or "better" than the ones in IPv4, however, it is understood that IPv6 is not required to solve every single problem.

Scenario 2: 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 set are available.
- Requirements: Don't break IPv4 network operations

Scenario 3: Enterprise deploying a new network or re-structuring an existing network, decides IPv6 is the basis for network communication.

- Assumptions: Required IPv6 network components are available, or available over some defined timeline.
- Requirements: Interoperation and Coexistence with IPv4 network operations and applications are required for communications.

3.2 Network Scenarios Characteristics

Characteristic 1 - Providers for External Network Operation
- Is external connectivity required?
- One site vs. multiple sites?
- Leased lines or VPN?
- IPv4 existing address ownership (Provider based addresses vs. Provider independent addresses)?
- Multi-homing?
- Do ISPs offer IPv6 service?
- Is there an external data-center?

Characteristic 2 - Enterprise Application Analysis
- List of applications in use?
- Can the application be upgraded to IPv6?
- Can the application support both IPv4 and IPv6?

Characteristic 3 - Enterprise IT Department Operations Analysis
- Who "owns"/"operate" the network: in house, outsourced?
- Is a Tele-commuter work force supported?
- Is inter-site communications required?
- Is network mobility used?
- IPv4 addressing plan?
- IPv4 addressing assignment procedure (DHCP vs. manual)?
- Internal IPv4 routing protocols used?
- External IPv4 routing protocols used?
- IPv4 Network Management policy/procedure?
- IPv4 QoS policy/procedure?
- IPv4 Security policy/procedure?
- List of "network operation" software that may be impacted by IPv6?
  - DNS
  - Management (SNMP & ad-hoc tools)
  - File servers
  - Backup
- Are all these software functions upgradeable to IPv6?
- If not upgradeable, then what are the workarounds?
- Do any of the software functions store IP addresses?
- List of "network operation" hardware that may be impacted by IPv6
  - Routers/switches
  - Firewalls
  - Load balancers
  - VPN terminators
  - Security Servers
- Are all these hardware functions upgradeable to IPv6?
- If not, what are the workarounds?
- Do any of the hardware functions store IP addresses?

Characteristics 4 û Enterprise Network Management System
- Considerations for Network Management System
- What behavior to expect from NMS for each transition vehicle
- Translators for IPv6 Operations
- Tunnels for IPv6 operations.
- Does transition vehicle fit any existing supported management models? example: dual-stack: v6/v4 <=> ipx/v4
- Which protocol to use for NM transport in dual stack? v6/v4?
- Protocol single vs. multi-protocol.
- Discovery of protocol used in-band or out-of-band.
- Receiving Events in-band and out-of-band
- Status Monitoring of software state and node state.
- Effects of Autoconfiguration Model selected.
- Effects of Dynamic Updates to DNS
- Performance Management
- Effects of multiple addresses per non-routing node
- Configuration Management in mixed v4/v6 environment
- Policy Management and enforcement for the Enterprise
- Security Management tools for the Enterprise

3.3 Network Scenarios Examples

Example Network A:

A network spread 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.

Applications run by the enterprise:
- Internal Web/Mail.
- File servers.
- Java applications.
- Collaborative development tools.

Internal network operation:
- In house operation of the network.
- DHCP (v4) is used for all desktops, servers use static address configuration.
- The DHCP server to update 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.

Example Network B:

A bank running a massive ATM network with some number of gazillions of transactions per second against central databases external network operation:
- External connectivity not required.
- Multiple sites connected by VPN.

Applications run by the enterprise:
- ATM transaction application.
- ATM management application.

Internal Network Operation:
- IPsec must protect all traffic.
- QoS policy for guaranteed delivery and urgent transactions.
- Network is managed through in-house developed tools.

Example Network C:

A Security Defense network:
- External network required at secure specific points.
- Network is its own Internet.
- Network must be able 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)
- Networking infrastructure mostly does not exist today with IPv4.
- Network True 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 create 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 Internet points 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.

4. Support for Legacy IPv4 Nodes and Applications

The Enterprise network will have to support the coexistence of IPv6 and IPv4, to support legacy IPv4 applications and nodes. The Enterprise user has the following choices for that coexistence to consider today.

4.1 IPv4 Tunnels to Encapsulate IPv6

IPv6/IPv4 nodes want to communicate using IPv6, but an IPv4 Internal router is between them. These nodes could also be Mobile nodes on a visited network

4.2 IPv6 Tunnels to Encapsulate IPv4

An IPv4/IPv6 node wants to communicate with a legacy IPv4 node and is on an IPv6 only link and routing domain.

4.3 IPv6 NAT to Communicate with IPv4

An IPv6/IPv4 node wants to communicate with a legacy IPv4 only node.

Using NAT for this point of transition will preclude end-2-end security, applications, and remove some benefits from the IPv6 protocol.

5. Network Infrastructure Requirements

The Enterprise will need to determine what network infrastructure they require for their deployment of IPv6. This infrastructure will need to be analyzed and understood as a critical resource to manage.

5.1 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.

5.2 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 routing topology, and any ingress and egress points to provider networks. The enterprise will also need to define points of transition mechanism to use within that routing topology.

5.3 Autoconfiguration

IPv6 introduces the concept of stateless autoconfiguration in addition to statefull autoconfiguration. The enterprise will have to determine the best method of autoconfiguration, for their network.

5.4 Security

Current existing mechanisms used for IPv4 to provide security need to be supported for IPv6 within the Enterprise.

5.5 Applications

Existing applications will need to be ported to support both IPv4 and IPv6.

5.6 Network Management

The addition of IPv6 and points of transition will need to be managed by the Enterprise network operations center. This will affect many components of the network and software required on nodes.

5.7 Address Planning

The address space within the Enterprise will need to be defined and coordinated with the routing topology of the Enterprise network.

6. 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 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.

References

None at this time

Acknowledgments

The Authors would like to acknowledge input from the following: IETF v6ops Working Group, Brian Carpenter, Alain Durand, and Bob Hinden.

Authors/Design Team

Send email to ent-v6net@viagenie.qc.ca to contact the design team and send comments on the draft to v6ops@ops.ietf.org.

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
Phone: 603.884.0062
Email: jim.bound@hp.com

Marc Blanchet

Tony Hain

Paul Gilbert
Cisco Systems
1 Penn Plaza, 5th floor,
NY, NY 10119
Phone: 212.714.4334
Email: pgilbert@cisco.com

Margaret Wasserman
Wind River
10 Tara Blvd, Suite 330
Nashua, NH 03062 USA
Phone: 603.897.2067
Email: mrw@windriver.com

Jason Goldschmidt
Sun Microsystems
M/S UMPK17-103
17 Network Circle
Menlo Park, CA 94025
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
Phone: 212.940.1812
Email: aisaac@bloomberg.com

Tim Chown

Jordi Palet Martinez
Consulintel
San Jose Artesano, 1
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
Phone: 650.625.2331
Email: ftemplin@iprg.nokia.com