

IPv6 Enterprise Networks Scenarios

**Enterprise Design Team
draft-pouffary-v6ops-ent-v6net-03.txt**

IETF 57th - v6ops WG

July 2003 Vienna, Austria

Scope and goals

- Goal:
 - Define Enterprise Network Scenarios
- Non Goals:
 - Define all possible scenarios
- Each enterprise will need to select the transition to best suit their business requirements
 - One-size-fits-all transition scenario will simply not work
- Will provide possible solutions in the analysis document

Status update since IETF 55

- Some Team Members have left, new ones have joined the team
 - Design Team e-mail ent-v6net@viagenie.qc.ca
 - Send comments on the draft to v6ops@ops.ietf.org
 - Yanick Pouffary (HP), Jim Bound (HP), Marc Blanchet (Hexago), Tony Hain (Cisco), Paul Gilbert (Cisco), Margaret Wasserman (Wind River), Jason Goldschmidt (Sun), Aldrin Isaac (Bloomberg L.P.), Tim Chown (University of South Hampton), Jordi Palet Martinez (Consulintel), Fred Templin (Nokia)
- Extensive reworking of the document to represent WG input
- Ready for WG acceptance

Document Layout

- 3 base scenarios are defined to capture the essential abstraction set for the Enterprise
 - Each scenario has assumptions and requirements
 - Note Well:
 - There are definitively more scenarios
 - We cannot possibly cover all of them
 - We selected the most representative ones
- 4 Network Scenarios Characteristics Analysis defined
 - Network Operation Analysis
 - Enterprise Application Analysis
 - Enterprise IT Dept Operations Analysis
 - Enterprise Network Management System Analysis
- The upcoming slides cover what is in the document
 - Who has read the document?

Network Base Scenario 1

- Enterprise with an existing IPv4 network wants to deploy IPv6 in parallel with their IPv4 network
- Assumptions:
 - IPv4 characteristics have an equivalent in IPv6
- Requirements:
 - Don't break IPv4 network characteristics
 - IPv6 characteristics should be equivalent or "better" than the ones in IPv4
 - IPv6 is not required to solve every single problem

Network Base Scenario 2

- Enterprise with an existing IPv4 network wants to deploy a set of particular IPv6 “applications”
 - IPv6 deployment is limited to the minimum required to operate this set of IPv6 “applications”
- Assumptions:
 - IPv6 software/hardware components for the “application” set are available
- Requirements:
 - Don't break IPv4 network operations

Network Base 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

Example – Analysis of a network spread across a number of geographically separated campuses

- External connectivity required
- Multiple sites connected by leased lines
- Provider independent IPv4 addresses
- Applications run by the enterprise:
 - Internal Web/Mail
 - File servers
 - Java applications
 - Collaborative development tools
- DHCP (v4) is used for all desktops, servers use static address configuration. DHCP server to update naming records (dynamic DNS) and web based tool for static addresses
- Network management is done using SNMP
- Routers, switches, firewalls can be upgraded to support IPv6 rules
- Load balancers do not support IPv6, upgrade path unclear

Example – Analysis of a bank running a massive ATM network with some number of gazillions transactions

- 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 – Analysis of a Security Defense network

- External network required at secure specific points
- Network must be able absorb ad-hoc creation of subNetworks
- Entire parts of the Network are completely mobile (including routers)
- 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, analysis and Transfer
- All packets must be secured end-2-end with encryption
- Intrusion Detection exists on all network entry points
- VPNs can be used but NAT can never be used
- Nodes must be able to access IPv4 legacy applications over IPv6 network

Network Infrastructure Requirements Example

- DNS to Support both IPv4 and IPv6 DNS records
 - Need to determine how the DNS is to be managed and accessed
- Routing for Interior and Exterior routing will be required to support both IPv4 and IPv6 routing protocols
 - Need to define the routing topology, and any ingress and egress points to provider networks
 - Need to define points of transition mechanism to use within that routing topology
- Autoconfiguration - stateless / statefull autoconfiguration
 - Need to select best method of autoconfiguration
- Security same mechanisms for IPv4 and IPv6
- Applications - Need to be ported to support both IPv4 and IPv6
- Network Management – Need to manage IPv6 and points of transition
- Address Planning - Need to define and coordinated with the routing topology of the Enterprise network
- Etc.

Future work and goals

- Accept the document as a WG document
- Write a revision to scenarios document next IETF
 - Still have work to do on this scenarios doc but we need to hear from you on the mail list
 - Alain Durand (thanks) has given us input we need others
- Start on a new analysis document to map relevant transition mechanisms to the base scenarios