IPv6
Evaluation of Vendors and Products

Silvia Hagen
Sunny Connection AG

www.sunny.ch

Sunny Connection

Topics

- Where to start
- IPv6 Basic requirements
- Requirements for specific device types
- Testing
- The Importance of Labs
- References

Full IPv6 Support

- When you purchase anything IT related, make sure it fully supports IPv6

- You heard this before – what does it mean?

- Sometimes „yes we support IPv6“ simply means that you can configure an IPv6 address on an interface – not really sufficient in most cases

Where to start

- High Level Plan
- Assessment

- Define your requirements carefully and aligned with your IPv6 design and integration plan
- Don‘t think your vendor knows what you need – he may just be waiting for you to tell him
- Don‘t base your designs on current issues (workarounds)

Node Requirements

- RFC 4294 defines minimum requirements for IPv6 nodes (hosts and routers). Common functionality.

- **What is a node?**
  - A node is a device that implements IPv6
  - A node that forwards IPv6 packets not explicitly addressed to itself is a router.
  - A node that is not a router is an IPv6 host.

Basic IPv6 Requirements

- **Must**
  - IPv6 - RFC 2460
  - ICMPv6 – RFC 4443
  - IPv6 Addressing – RFC 4291
  - SLAAC – RFC 4862
  - DHCPv6 client – RFC 3315, DNS – RFC 3596
  - Default Address Selection – RFC 3484 chk 4007
  - IPSec (ESP/AH), IKE, cryptographic algorithms

- **Should**
  - Neighbor Discovery - RFC 4861
  - Path MTU Discovery
  - Privacy Extensions – RFC 3041
  - MLD – RFC 2710

Optional

- **Options**
  - Link specific requirements
  - MLD and DHCP snooping, RA guard (layer 2 devices)
  - IPv6 Jumbograms
  - ULA‘s / CGA‘s
  - DHCPv6 – RFC 3315 – client, server or relay functionality
  - DNS – probably a good idea ;-) – resolver and/or server
  - Routing Protocol support?
  - Prefix Delegation
  - Transition Mechanisms?
  - Mobile IPv6, Nemo
  - QoS, DS field
  - Extended ICMP multi-part messages on roadmap (RFC 4884, 5095)
  - RFC4361 – DHCP identifiers for DHCPv4 and DHCPv6
  - Management Support (SNMP, MIBs)
  - ……

Be specific

- Specialized devices:
  - Layer 2 devices
  - Hosts (clients and servers)
  - Routers and layer 3 switches
  - Security devices (firewalls, IDS, IPS)

Requirements per device type

- For each type of device make two lists:
  - Mandatory features
  - Optional features

- What features you need depends on your designs and integration plan (for instance, if you don't plan to use CGA addresses because you have a PKI infrastructure, you don't need CGA support as a requirement in any of your lists)
- Some options that you may not need today should still be supported for future configurations

Require and test

- All the requirements you have on your list for each device need also to be tested in your lab.
- Don‘t believe brochures and fact sheets.
- And expect bugs and incompatibility issues. You need time to fix them with your vendors.

Reassess Vendor Portfolio

- Best vendor/provider for IPv4 product or service doesn't mean it is also best vendor/service for IPv6

- Test! Test what?
  - Verify and test features and functionality required
  - Test not only functionality, but performance and load behavior! (Hardware- vs. Software Implementation)
  - Test dual-stack, co-existence and transition mechanism performance specifically – for your integration design.

Criteria for vendors

- Analyze product line
- Assess functionality of products
- Assess performance of products
- Assess vendor's testing and Q&A procedures
- Assess vendor‘s support for IPv6
- Assess roadmap

The importance of labs

- Education
- Gather experience
- Test conformance, features and functionality of products
- Test performance and run load tests
- Find bugs and test bugfixes
- Test compatibility/interoperability
- Test Deployment Scenarios according to your integration plan
- Test management of new infrastructure
- Test deployment steps
- Train your support staff

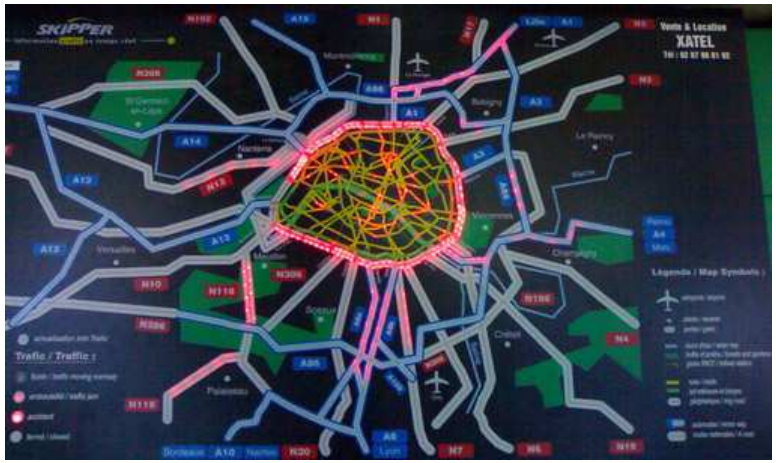
Outcome of testing

- Testing
  - Provides experience
  - Shows hidden features
  - Let's you refine your design and implementation plan
  - Reveals bugs
  - Minimizes risks

- Plan for enough time for bug fixing (early stacks)

Traffic flows

- Perform network performance tests and evaluate new traffic patterns
- Be aware that IPv6 does not double traffic, in most cases traffic will slowly shift from IPv4 to IPv6
- Be aware that in the beginning with most networks being dual-stacked, you not only have broadcast traffic on your segments, but Neighbor Discovery and Multicast traffic in addition to it.



Sunny Connection

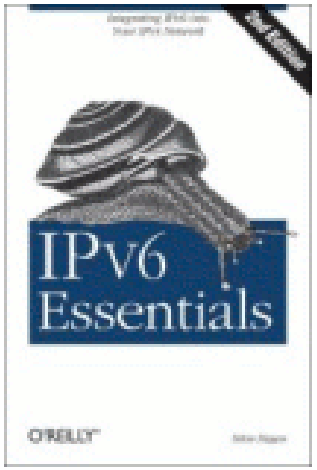
Futher information

- USGv6: A Technical Infrastructure to Assist IPv6 Adoption for the US Government
  Technical standards profile to assist acquisition of IPv6 capabilities in Hosts, Routers, and Network Protection Devices
  Refer to USGv6 at http://www.antd.nist.gov/usgv6
  (Test Labs, Tested Products, Buyers Guides etc)
- RIPE 501
  Best Common Practice (BCP) template that can be used by governments or large enterprises when developing tender documents.
  http://www.ripe.net/ripe/docs/ripe-501
- International IPv6 Forum – IPv6 Ready Logos
  www.ipv6forum.com

Thank you for your attention!

IPv6 Essentials

by Silvia Hagen, English
2nd Edition, O'Reilly, May 2006
ISBN 978-0-596-10058-2



Planning for IPv6

by Silvia Hagen, English
O'Reilly, September 2011
ISBN 978-1-4493-0539-0
eBook 978-1-4493-0538-3