Enterprise IPv6 Deployment Summary

Shannon McFarland
CCIE# 5245
Corporate Consulting Engineer
CE/CTO
shmcfarl@cisco.com
Reference Materials


Recommended Reading


“IPv6 Enterprise Deployment” Cisco Press Coming later this year!
Agenda

- Enterprise Adoption
- Planning and Deployment Summary
- Infrastructure Deployment
- Communicating with the Service Providers
Enterprise Adoption
Enterprise Adoption Spectrum

Kicking the tires
- Is it real?
- Do I need to deploy everywhere?
- Equipment status?
- SP support?
- Addressing
- What does it cost?

Pilot/Early Deployment

Production/Looking for parity and beyond
- Mostly or completely past the “why?” phase
- Assessment (e2e)
- Weeding out vendors (features and $)
- Focus on training and filling gaps

- Still fighting vendors
- Content and wide-scale app deployment
- Review operational cost of 2 stacks
- Competitive/Strategic advantages of new environment
Monitoring Market Drivers

Address Space
- Emerging Markets
- Public IPv4 Address Space
- RFC1918 Exhaustion
- RFC1918 Collisions (M&A)

Operating Systems – Applications
- All major OSes support IPv6
- Microsoft W7/Server 2008
- Microsoft DirectAccess

National IT Strategy
- US Federal Mandate
- CNGI
- European Commission

Infrastructure Evolution
- DOCSIS 3, FTTH, Cloud, Mobile SP, Sensor Networks
Planning and Deployment Summary
### IPv6 Integration Outline

#### Pre-Deployment Phases
- Establish the network starting point
- Importance of a network assessment and available tools
- Defining early IPv6 security guidelines and requirements
- Additional IPv6 “pre-deployment” tasks needing consideration

#### Deployment Phases
- Transport considerations for integration
- Campus IPv6 integration options
- WAN IPv6 integration options
- Advanced IPv6 services options
Integration/Coexistence Starting Points
Example: Integration Demarc/Start Points in Campus/WAN

1. Start dual-stack on hosts/OS
2. Start dual-stack in campus distribution layer (details follow)
3. Start dual-stack on the WAN/campus core/edge routers
4. NAT-PT for servers/apps only capable of IPv4 (temporary only)
Pre-Deployment Checklist

Other Critical Network Planning Requirements

✓ Establish starting point, network assessment, security guidelines
✓ Acquire IPv6 address block and create IPv6 addressing scheme
✓ Create and budget for an IPv6 lab that closely emulates all network elements (routers, switches, hosts, OS)
✓ Upgrade DNS server to support IPv6
✓ Establish network management considerations (hardware, MIBs required for v6, etc.)
✓ Routing and multicast protocol and selection/evaluation process (align with IPv4 choice is possible)
✓ Consider options for centralized ISATAP router (see campus example)
✓ Evaluate IPv6-capable transport services available from current Service Provider (SP)
Infrastructure Deployment

Start Here: Cisco IOS Software Release Specifics for IPv6 Features
http://www.cisco.com/univercd/cc/td/doc/product/software/ios123/123cgcr/ipv6_c/ftipv6s.htm
IPv6 Coexistence

- IPv6 Network
- IPv6 Host
- Configured Tunnel/MPLS (6PE/6VPE)
- Dual Stack
  - IPv4: 192.168.99.1
  - IPv6: 2001:db8:1::1/64
- IPv6/IPv4
- MPLS/IPv4
- Configured Tunnel/MPLS (6PE/6VPE)
- IPv6 Network
- IPv6 Host

IPv6/IPv4

- ISATAP Tunneling
  - (Intra-Site Automatic Tunnel Addressing Protocol)
  - 6to4
  - 6rd
  - Manual Tunnels
Campus IPv6 Deployment Options
Dual-Stack IPv4/IPv6

- #1 requirement—switching/routing platforms **must** support **hardware** based forwarding for IPv6
- IPv6 is transparent on L2 switches but—
  - L2 multicast—MLD snooping
  - IPv6 management—Telnet/SSH/HTTP/SNMP
  - Intelligent IP services on WLAN
- Expect to run the same IGPs as with IPv4
- VSS supports IPv6
Campus IPv6 Deployment Options

Hybrid Model

- Offers IPv6 connectivity via multiple options
  - Dual-stack
    - Configured tunnels—L3-to-L3
    - ISATAP—Host-to-L3
- Leverages existing network
- Offers natural progression to full dual-stack design
- May require tunneling to less-than-optimal layers (i.e. core layer)
- ISATAP creates a flat network (all hosts on same tunnel are peers)
  - Create tunnels per VLAN/subnet to keep same segregation as existing design (not clean today)
- Provides basic HA of ISATAP tunnels via old Anycast-RP idea
Campus IPv6 Deployment Options
IPv6 Service Block—an Interim Approach

- Provides ability to **rapidly deploy IPv6 services without touching existing network**
- Provides **tight control of where IPv6 is deployed** and where the traffic flows (maintain separation of groups/locations)
- Offers the same advantages as Hybrid Model without the alteration to existing code/configurations
- Configurations are very similar to the Hybrid Model
  - ISATAP tunnels from PCs in access layer to service block switches (instead of core layer—Hybrid)
- 1) Leverage existing ISP block for both IPv4 and IPv6 access
- 2) Use dedicated ISP connection just for IPv6—Can use IOS FW or PIX/ASA appliance

![Diagram showing IPv6 service block deployment options with ISATAP tunnels and VLANs]

Primary ISATAP Tunnel
Secondary ISATAP Tunnel

---

2

IPv4-only Campus Block

Internet

Dedicated FW

WAN/ISP Block

Data Center Block

VLAN 2

VLAN 3

1

ISATAP

IPv6 Service Block

Agg Layer

Access Layer

Core Layer

Dist. Layer

Access Layer

Agg Layer

Core Layer

Dist. Layer

Core Layer

Dist. Layer

Primary ISATAP Tunnel
Secondary ISATAP Tunnel

---

Presentation_ID © 2006 Cisco Systems, Inc. All rights reserved. Cisco Public 16
IPv6 Data Center Integration

- The single most overlooked and potentially complicated area of IPv6 deployment
- Front-end design will be similar to campus based on feature, platform and connectivity similarities – Nexus, 6500 4900M
- IPv6 for SAN is supported in SAN-OS 3.0
- Major issue in DC with IPv6 today- NIC Teaming
- Watch status of IPv6 support from App, Grid, DB vendors, DC management
  - Get granular – e.g. iLO
  - Impact on clusters – Microsoft Server 2008 Failover clusters full support IPv6 (and L3)
- Build an IPv6-only server farm?
IPv6 in the Data Center
Biggest Challenges Today

- Network services above L3
  SLB, SSL-Offload, application monitoring (probes)
  Application Optimization (WAAS)
  High-speed security inspection/perimeter protection

- Application support for IPv6
  If an application is protocol centric (IPv4):
    Needs to be rewritten
    Needs to be translated until it is replaced
    Wait and pressure vendors to move to protocol agnostic framework

- Growing DC complexity
  Virtualization should make large DCs simpler and more flexible
  Lack of robust DC/Application management is often the root cause of all evil
  Ensure management systems support IPv6 as well as the devices being managed
WAN/Branch Deployment

- Cisco routers have supported IPv6 for a long time
- Dual-stack should be the focus of your implementation—but, some situations still call for tunneling
- Support for every media/WAN type you want to use (Frame Relay, leased-line, broadband, MPLS, etc.)
- Don’t assume all features for every technology are IPv6-enabled
- Better feature support in WAN/branch than in campus/DC
IPv6 Enabled Branch
Take Your Pick—Mix-and-Match

- **Branch Single Tier**
  - Internet
  - Dual-Stack IPSec VPN (IPv4/IPv6)
  - IOS Firewall (IPv4/IPv6)
  - Integrated Switch (MLD-snooping)

- **Branch Dual Tier**
  - Internet
  - Dual-Stack IPSec VPN or Frame Relay
  - IOS Firewall (IPv4/IPv6)
  - Switches (MLD-snooping)

- **Branch Multi-Tier**
  - MPLS
  - Dual-Stack IPSec VPN or MPLS (6PE/6VPE)
  - Firewall (IPv4/IPv6)
  - Switches (MLD-snooping)
Remote VPN – IPv6

- Cisco VPN Client 4.x
  - IPv4 IPSec Termination (PIX/ASA/IOS VPN/Concentrator)
  - IPv6 Tunnel Termination (IOS ISATAP or Configured Tunnels)

- AnyConnect Client 2.x
  - SSL/TLS or DTLS (datagram TLS = TLS over UDP)
  - Tunnel transports both IPv4 and IPv6 and the packets exit the tunnel at the hub ASA as native IPv4 and IPv6

- Microsoft DirectAccess
Communicating with the Service Provider
Top SP Concerns for Enterprise Accounts

- Port to Port Access
- Multi-Homing
- IPv6
- Content
- Provisioning
Port-to-Port Access

- **Basic Internet**
  - Dual-stack or native IPv6 at each POP
  - SLA driven just like IPv4 to support VPN, content access

- **MPLS**
  - 6VPE
  - IPv6 Multicast

- **Hosted (see content)**
  - IPv6 access to hosted content
  - Cloud migration (move data from Ent DC to Hosted DC)
Multi-Homing

Port to Port Access  Multi-Homing

Content  Provisioning

IPv6

PI/PA Policy Concerns

- PA is no good for customers with multiple providers or change them at any pace
- PI is new, constantly changing expectations and no “guarantee” an SP won’t do something stupid like not route PI space
- Customers fear that RIR will review existing IPv4 space and want it back if they get IPv6 PI

NAT

- Religious debate about the security exposure – not a multi-homing issue
- If customer uses NAT like they do today to prevent address/policy exposure, where do they get the technology from – no scalable IPv6 NAT exists today

Routing

- Is it really different from what we do today with IPv4? Is this policy stuff?
- Guidance on prefixes per peering point, per theater, per ISP, ingress/egress rules, etc.. – this is largely missing today
Hosted/Cloud Apps today
- IPv6 provisioning and access to hosted or cloud-based services today (existing agreements)
- Salesforce.com, Microsoft BPOS (Business Productivity Online Services), Amazon, Google Apps

Move to Hosted/Cloud
- Movement from internal-only DC services to hosted/cloud-based DC
- Provisioning, data/network migration services, DR/HA

Contract/Managed Marketing/Portals
- Third-party marketing, business development, outsourcing
- Existing contracts – how to offer to connect over IPv6
Provisioning

SP Self-Service Portals

- Not a lot of information from accounts on this but it does concern them
- How can they provision their own services (i.e. cloud) to include IPv6 services and do it over IPv6

SLA

- More of a management topic but the point here is that customers want the ability to alter their services based on violations, expiration or restrictions on the SLA
- Again, how can they do this over IPv6 AND for IPv6 services
The Scope of IPv6 Deployment

Web Content Management

Applications & Application Suites

Networked Device Support

Networked Infrastructure Services

Deployment Scenario

IPv6 over IPv4 Tunnels
(Seeded, 6to4, ISATAP, GRE)

Dual-Stack

IPv6 over MPLS
(6PE/6VPE)

IP Services (QoS, Multicast, Mobility, Translation)

Hardware Support

Connectivity

IP Addressing

Routing Protocols

Instrumentation

Basic Network Infrastructure

Roll-out Releases & Planning

Staff Training and Operations
Conclusion

- Create a virtual team of IT representatives from every area of IT to ensure coverage for OS, Apps, Network and Operations/Management

- Microsoft Windows Vista, 7 and Server 2008 will have IPv6 enabled by default—understand what impact any OS has on the network

- Deploy it – at least in a lab – IPv6 won’t bite

- Things to consider:
  - Focus on what you must have in the near-term (lower your expectations) but pound your vendors and others to support your long-term goals
  - Don’t be too late to the party – anything done in a panic is likely going to go badly