IPv6 Deployment and Considerations

Anthony Chan anchan@ cisco.com
IPv6 Deployment and Considerations

Agenda

- IPv6 Market Trends
- IPv6 Planning Steps
- IPv6 Addressing
- IPv6 Deployment Options
- ASIAGOV Case Study
IPv6 Deployment and Considerations

Agenda

- IPv6 Market Trends
- IPv6 Planning Steps
- IPv6 Addressing
- IPv6 Deployment Options
- ASIAGOV Case Study
Market Factors Driving IPv6 Deployment

IPv4 Address Run-Out

2011

IPv6 OS, Content & Applications

Google
facebook
Microsoft

National IPv6 Strategies
US Federal/Civilian, US DoD, China NGI, EU

Infrastructure Evolution
SmartGrid, SmartCities
DOCSIS 3.0, 4G/LTE, IPSO

www.oecd.org: Measuring IPv6 Adoption
The Growing Internet Challenge …

The gap between supply and demand for IP addresses – the key Internet resource – is widening

The pool of IPv4 address blocks is dwindling rapidly

While the number of new Internet devices is exploding

1 – Geoff Huston, APNIC, www.potaroo.net, tracking /8 address-blocks managed by the Internet Assigned Numbers Authority
2 – Cisco Visual Networking Index / Intel Embedded Internet Projections
Say goodbye to this chart, and hello to...
This is accelerating! Consistently beating estimates.

Microsoft has just purchased 666,624 IP addresses for $7.5 million ($11.25/addr).

Source: Geoff Huston, APNIC
IPv6 Deployment and Considerations

Agenda
- IPv6 Market Trends
- IPv6 Planning Steps
- IPv6 Addressing
- IPv6 Deployment Options
- ASIAGOV Case Study
IPv6 Planning Steps

Business Case Identified/Justified

1. Evaluate effect on business model
2. Establish IPv6 project management team
3. Decide on IPv6 Architecture Strategy
4. Develop IPv6 exception strategy
5. Assess network including hardware and software, Applications and back end operations
6. Develop Adoption Timelines, Develop Cost Analysis, Develop Procurement Plan
7. Obtain IPv6 Prefix, Develop Addressing Plan, Develop Security Plan
8. Create Detailed Design for phase 1
10. Train Engineering and Operations on Technology and Solution in place
Readiness Assessment

- A key and mandatory step to evaluate the impact of IPv6 integration
- May be split in several phases
  - Infrastructure – networking devices and back end systems
  - Hosts, Servers and applications
- Must be as complete as possible to allow upgrade costs evaluation and planning
  - Hardware type, memory size, interfaces, CPU load,…
  - Software version, features enabled, license type,…, forwarding path, known limitations, best practices, etc
- Difficult to complete if a set of features is not defined per device’s category for a specific environment
  - IPv6-capable definition, knowledge of the environment and applications, design goals
- Break Network into Places in the network for a more accurate assessment
  - Should Map directly into your IPv6 Network Architecture strategy, Cost analysis and time lines
IPv6 Deployment and Considerations

Agenda
- IPv6 Market Trends
- IPv6 Planning Steps
- IPv6 Addressing
- IPv6 Deployment Options
- ASIAGOV Case Study
Building the IPv6 Address Plan

- Build on the lessons learned from how the IPv4 plan was developed and implemented
  - Does it make sense to follow the current IPv4 assignment model?

- Must be proportional to current usage and expected growth

- Check RIR policies on block sizing

- Hierarchy is key
  - Do you get a prefix for the entire company or do you get one prefix per site (what defines a site?)

- Cisco IPv6 Addressing White Paper
Getting IPv6 Space

- Each RIR has different requirements web site have specifics
  However anyone that has a PI IPv4 from a RIR qualifies for a PI IPv6

- For ARIN initial block size is site dependent
  1 to 12 sites $\rightarrow$ /44
  12 to 192 sites $\rightarrow$ /40
  192 to 3,072 sites $\rightarrow$ /36
  3,072 to 49,152 sites $\rightarrow$ /32
  Good source: https://www.arin.net/policy/nrpm.html

- Possible Options
  Get one large global block from local RIR and subnet out per region
  Get a separate block from each of the RIR you have presences in

- Which route to go?
  Depends on specific business case
  Enterprise with not much consumer interaction can stay with a single large block
  Enterprise that have a heavy consumer interaction using a block from each RIR will help avoid DNS and routing hacks to lead clients to regional Data Centers
PI and PA Allocation Process

Provider Assigned

Provider Independent

IANA

Registries

ISP

Org

Enterprise

/12

/32

/48

/12

/48

/32
Do I Get PI or PA?

- Mainly a Enterprise Issue
- Service Providers will get allocation direct from RIR
- PI space is great for organizations who want to multihome to different SPs
- PA is a great space if you plan to use the same SP for a very long time or you plan to NAT/Proxy everything with IPv6 (not likely)

Other things to consider

Do you get a prefix for the entire company or do you get one prefix per site (what defines a site?)

Do you get a prefix per regional registry (RIPE, APNIC, LACNIC, etc)
PI Space Concerns

- Concerns around prefix announcement from other regions
  Will providers accept prefixes from other regions?

- Concerns around prefix lengths
  What length prefix will providers accept?
  How do I do traffic engineering?
  What about providers upstream peers?

- Bottom line is to have a detailed conversation w/ your provider or peering partner about what their policies are
  [http://www.us.ntt.net/support/policy/routing.cfm#v6PeerFilter](http://www.us.ntt.net/support/policy/routing.cfm#v6PeerFilter)
Building the IPv6 Address Plan

- Template addressing
  Build information into the address
  Example 4 bit boundary 2001:0db8:1234:xyza::/48
  x = Region y = Site z = Building a = Floor

- Short numbers: less chance of transcription errors for loopbacks

- Split address block into two example of a /32
  /33 for internet Enabled devices /33 for Internal Restricted devices.
  Helps with Route Identification and makes filtering on edge easier.

- IPv6 Address Management – How are you going to manage these blocks?
What type of addressing should I deploy internal to my network? It depends:

ULA-only—Today, no IPv6 NAT is useable in production so using ULA-only will not work externally to your network.

ULA + Global allows for the best of both worlds but at a price—much more address management with DHCP, DNS, routing and security—SAS does not always work as it should.

Global-only—Recommended approach but the old-school security folks that believe topology hiding is essential in security will bark at this option.

Let’s explore these options…
ULA-Only Not Recommended

- Everything internal runs the ULA space
- A NAT supporting IPv6 or a proxy is required to access IPv6 hosts on the internet — must run filters to prevent any SA/DA in ULA range from being forwarded
- Works as it does today with IPv4 except that today, there are no scalable NAT/Proxies for IPv6
- Removes the advantages of not having a NAT (i.e. application interoperability, global multicast, end-to-end connectivity)
Both ULA and Global are used internally except for internal-only hosts

Source Address Selection (SAS) is used to determine which address to use when communicating with other nodes internally or externally

In theory, ULA talks to ULA and Global talks to Global—SAS ‘should’ work this out

ULA-only and Global-only hosts can talk to one another internal to the network

Define a filter/policy that ensures your ULA prefix does not ‘leak’ out onto the Internet and ensure that no traffic can come in or out that has a ULA prefix in the SA/DA fields

Management overhead for DHCP, DNS, routing, security, etc…

ULA + Global Not Recommended
Global-Only Recommended

- Global is used everywhere
- No issues with SAS
- No requirements to have NAT for ULA-to-Global translation—but, NAT may be used for other purposes
- Easier management of DHCP, DNS, security, etc.
- Only downside is breaking the habit of believing that topology hiding is a good security method 😊
Questions to Ask Your Service Provider

- **SP Deployment Type**
  - Dual Stack, Native or Overlay (if so what kind of overlay)?
  - What kind of SLA are provided for the services? Do you post metrics online?

- **What kind of services are offered**
  - Internet Services
  - Layer 2 or Layer 3 VPN’s
  - IPv6 Multicast support or plans?
  - DNS Services over v4 or V6?

- **Visibility and footprint to the IPv6 Internet.**
  - Peering arrangements

- **Service availability on nodes**
  - Available over 802.1Q or VLANs?
  - Separate or Same VRF’s?

- **Acceptance Policy**
  - Prefix length acceptance?
  - Provider Independent or Provider Assigned acceptance
  - Do your Peering partners have similar policy to yours?
  - What prefix length do your upstream providers accept?

- **Provisioning**
  - Is there a self service portal?
  - Routing add and deletes
  - When do you plan on providing v6 services as a default offering?

- **Charging model**
  - Do you charge for IPv6?

http://docwiki.cisco.com/wiki/What_To_Ask_From_Your_Service_Provider_About_IPv6
Production Quality IPv6 Improving

6to4 Is Trending Down, Native IPv6 Is Trending Up

Source: Google and Hurricane Electric
IPv6 Deployment and Considerations

Agenda

- IPv6 Market Trends
- IPv6 Planning Steps
- IPv6 Addressing
- IPv6 Deployment Options
- ASIAGOV Case Study
IPv6 Deployment Options

- IPv6 Only
  IPv6 is the only protocol operating in the network

- Dual Stack (in devices/hosts and networks)
  IPv4 and IPv6 operate in tandem over shared or dedicated links

- Tunnelling over IPv4 or MPLS (6in4, 6to4, 6PE, 6VPE, etc..)
  IPv6 confined to the edge of the IPv4 / MPLS core

- Protocol Translation (NAT64, NAT46, DNS64, etc..)
  Allow IPv6-only devices to communicate with IPv4-only devices
Dual Stack Backbone

- All P + PE routers are capable of IPv4+IPv6 support
- Two IGPs supporting IPv4 and IPv6
- Memory considerations for larger routing tables
- Native IPv6 multicast support
- All IPv6 traffic routed in global space
- Good for content distribution and global services (Internet)
Dual Stack Application Approach

- Dual stack in a device means
  - Both IPv4 and IPv6 stacks enabled
  - Applications can talk to both
  - Choice of the IP version is based on DNS and application preference
Dual Stack Approach & DNS

In a dual stack case an application that:

- Is IPv4 and IPv6-enabled
- Can query the DNS for IPv4 and/or IPv6 records (A) or (AAAA) records
- Chooses one address and, for example, connects to the IPv6 address
IPv6 Transit using MPLS 6PE (RFC 4798)

- 6PEs must support dual stack IPv4+IPv6 (acts as normal IPv4 PE)
- IPv6 packets transported from 6PE to 6PE over Label Switch Path
- IPv6 addresses exist in global table of PE routers only
  - IPv6 addresses exchanged between 6PE using MP-BGP session
- Core uses IPv4 control plane (LDPv4, TEv4, IGPv4, MP-BGP)
- Benefits from MPLS features such as FRR, TE
Services using MPLS 6PE

- Connects IPv6 islands over MPLS core (Transits edge to edge)
- Transition mechanism for providing **unicast** IPv6 access
- Coexistence mechanism for combining IPv4 and IPv6 services
- As other IPv6 “tunnel” technologies, enables services such as IPv6 Internet Access
- Peer-to-peer connectivity
- Access to IPv6 services supplied by the SP itself
Routing And Label Distribution Example

IPv6 Packet

IPv6 Network

CE3
IPv6

IPv6 Packet

MPLS IPv4 Backbone

IPv4 MPLS

P

IPv6 Packet

IPv6 Network

CE
IPv6

IPv6

2001:f00d::

IPv6

2001:db8::

IPv6

IPv6

IPv4

200.10.10.1

IPv6

IPv6

LDPv4 {Pop}

Binds label {Pop} to 200.10.10.1

2001:f00d::

Advertises 2001:f00d:: to 6PE1

MP-eBGP

MP-eBGP

IPv6 MP-iBGP

Advertises 2001:f00d:: to 6PE2

BGP Next Hop ::ffff:200.10.10.1

Label Binding {65}

IGPv4

200.10.10.1 reachable

IGPv4

200.10.10.1 reachable

IGPv4

200.10.10.1 reachable

LDPv4 {27}

Binds label {27} to 200.10.10.1

LDPv4 {48}

Binds label {48} to 200.10.10.1

MP-eBGP

IPv6 MP-iBGP

Advertises 2001:f00d:: to CE2
ipv6 cef

interface loopback0
  ip address 200.10.10.1 255.255.255.0

router bgp 100
  neighbor 2001:f00d:1::1 remote-as 65014
  neighbor 200.11.11.1 remote-as 100
  neighbor 200.11.11.1 update-source lo0

address-family ipv6
  neighbor 200.11.11.1 activate 6PE2
  neighbor 200.11.11.1 send-label
  neighbor 2001:f00d:1::1 activate CE1

ipv6 cef

interface loopback0
  ip address 200.11.11.1 255.255.255.0

router bgp 100
  neighbor 2001:db8:1::1 remote-as 65015
  neighbor 200.10.10.1 remote-as 100
  neighbor 200.10.10.1 update-source lo0

address-family ipv6
  neighbor 200.10.10.1 activate 6PE1
  neighbor 200.10.10.1 send-label
  neighbor 2001:db8:1::1 activate CE2
IPv6 VPN 6VPE (RFC 4659)

- 6VPE uses existing IPv4 MPLS infrastructure to provide IPv6 VPN
  Core uses IPv4 control plane (LDPv4, TEv4, IGPv4)
- PEs must support dual stack IPv4+IPv6
- Offers same architectural features as MPLS-VPN for IPv4
  RTs, VRFs, RDs are appended to IPv6 to form VPNv6 address
  MP-BGP distributed both VPN address families
  BGP NH uses IPv4 to IPv6 mapped address format ::ffff:A.B.C.D
- VRF can contain both VPNv4 and VPNv6 routes
- Solution suitable for IPv6 support to enterprises and government with VPN
For VPN customers, IPv6 VPN service is exactly as IPv4 VPN service
6PE is “like VPN” but prefixes are in global table, 6VPE is true VPN
6VPE enables services such as
IPv6 VPN Access
Carriers Supporting Carrier
Access to IPv6 services supplied by the SP itself
CE1 Configuration

ipv6 unicast-routing
ipv6 cef

interface Ethernet0/0
  description Link to PE1
  ip address 172.16.1.1 255.255.255.0
  ipv6 address 2001:db8:cafe:1::1/64

interface Ethernet1/0
  description to GREEN LAN
  ip address 10.1.1.1 255.255.255.0
  ipv6 address 2001:db8:beef:1::1/64
ipv6 rip GREEN enable

router bgp 500
  neighbor 2001:db8:cafe:1::2 remote-as 100
  neighbor 172.16.1.2 remote-as 100
  address-family ipv4
  redistribute eigrp 100
  neighbor 172.16.1.2 activate 6VPE1
  exit-address-family
  address-family ipv6
  neighbor 2001:db8:cafe:1::2 activate 6VPE1
  redistribute rip GREEN
  exit-address-family
New Multi-AF VRF Configuration

- **New VRF AF definition**
  - Allows address-families
  - Each with unique or common policies

- `vrf upgrade-cli multi-af-mode {common-policies | non-common-policies} [vrf <name>]`
  - This command can update existing VRF definitions
ipv6 unicast-routing
ipv6 cef
!
interface Loopback0
  ip address 200.10.10.1 255.255.255.255
!
interface Ethernet0/0
  Description Link to CE1
  vrf forwarding GREEN
  ip address 172.16.1.2 255.255.255.0
  ipv6 address 2001:db8:cafe:1::2/64
!
interface Ethernet2/0
  description Link to Core Network
  ip address 192.168.1.1 255.255.255.252
mpls ip
!
router ospf 1
  log-adjacency-changes
  redistribute connected subnets
  passive-interface Loopback0
  network 192.168.1.0 0.0.0.255 area 0
router bgp 100
neighbor 200.11.11.1 remote-as 100
neighbor 200.11.11.1 update-source lo0
!
address-family ipv4 ← Internet Routes
neighbor 200.11.11.1 activate
no auto-summary
no synchronization
exit-address-family
!
address-family vpv4 ← To 6VPE2
neighbor 200.11.11.1 activate
neighbor 200.11.11.1 send-community ext
exit-address-family
!
address-family ipv6 vrf GREEN ← To CE1
redistribute connected
neighbor 172.16.1.1 remote-as 500
neighbor 172.16.1.1 activate
exit-address-family
!
address-family ipv6 vrf GREEN ← To CE1
neighbor 2001:db8:cafe:1::1 remote-as 500
neighbor 2001:db8:cafe:1::1 activate
exit-address-family
6VPE2 IPv6 VRF Routes

6VPE2#show ipv6 route vrf GREEN
B 2001:db8:beef:1::/64 [200/0]
   via 200.10.10.1%Default-IP-Routing-Table, indirectly connected
B 2001:db8:beef:2::/64 [20/0]
   via FE80::A8BB:CCFF:FE01:FA00, Ethernet1/0
B 2001:db8:cafe:1::/64 [200/0]
   via 200.10.10.1%Default-IP-Routing-Table, indirectly connected
C 2001:db8:cafe:3::/64 [0/0]
   via Ethernet1/0, directly connected
L 2001:db8:cafe:3::2/128 [0/0]
   via Ethernet1/0, receive
L FF00::/8 [0/0]
   via Null0, receive
IPv6 Deployment and Considerations

Agenda

- IPv6 Market Trends
- IPv6 Planning Steps
- IPv6 Addressing
- IPv6 Deployment Options
- ASIAGOV Case Study
Customer Background

- APAC Governmental Agency: ASIAGOV
- Customer Drivers for IPv6
  - As per the national mandate, ensuring that country is viewed as a technology leader in the region.
  - To serve as a leading example for local ISPs and Enterprises to facilitate their eventual IPv6 protocol integration.
- Primary Goal is a public facing IPv6 rollout (Web + Mail Servers)
- Secondary Goal is an internal IPv6 rollout (IPv6 Internet Access, Web development)
IPv6 Assessment Engagement

- **Purpose of Cisco Engagement**
  
  To provide an IPv6 Architecture and Assessment for ASIAGOV that:
  - Reviews the *network infrastructure* and *application architecture*
  - Recommends best practices and appropriate implementation approach
  - Reviews and recommends improvements on security and network administration, operation and support design
  - Recommends an *implementation roadmap* of the IPv6 network protocols

- **Consultancy Scope**
  
  Core1: L3 MPLS VPN Network for connectivity to services
  Core2: L3 MPLS VPN Network for connectivity to Gov’t Bureaus
  ServicesNet: Central Services (Internet Proxy, Web Hosting, etc.)
ASIAGOV Network

ServicesNET: Service Blocks

Core2

EBGP

Core1

B/D

SVC1

SVC2

SVC3

SVC4

Internet
IPv6 Engagement Methodology

- Information Gathering & Data Consolidation
  - Initial Workshops (objective, c..)
  - Ongoing Interviews
  - Reviewed Objective and Identified Design Options
  - Consolidated Network Device and Server Application
  - Selected most applicable Network Design Approach
  - Assessed Devices against features
  - Feature Requirements List
  - Identified Support and Caveats
  - Identified Roadmap or Alternatives

- HLD Strategy

- Assessment
  - Documented High Level Architecture
  - Documented Assessment
  - Adjusted Device/Application
  - Documented Comment and Revisions
  - Six Week Nursing Period

- Documentation
  - Adjusted Device/Application
  - Documented Comment and Revisions
  - Six Week Nursing Period

- Optimization
  - Initial Workshops (objective, c..)
  - Ongoing Interviews
  - Reviewed Objective and Identified Design Options
  - Consolidated Network Device and Server Application
  - Selected most applicable Network Design Approach
  - Assessed Devices against features
  - Feature Requirements List
  - Identified Support and Caveats
  - Identified Roadmap or Alternatives

BRKSPM-2604_c1 © 2010 Cisco and/or its affiliates. All rights reserved. Cisco Confidential
IPv6 Consultancy Report Summary

- **Network Architecture Recommendations**
  - High Level IPv6 solution and recommended option
  - Combination of 6VPE and Dual Stack
  - IPv6 Best Practices

- **Assessment Report by Network Services Block**
  - Network Devices & Appliances: Cisco and/or 3rd Party
  - Servers & Applications: Server OS and specific Apps
  - Short and Long-term IPv6 solutions

- **Integration Report**
  - Recommended High Level Integration Approach
  - Suggested PDI and Testing
IPv6 High Level Architecture Design - Mail

- No change to current Mail IPv4 network architecture
- Dual Stack IPv6 protocol added by hardware and software upgrade

**Short Term Approach**
- Upgrade H/W and S/W for IM Switches
- Load Balancer S/W upgrade
- Add new MTA to support IPv6 email exchange
- No IPv6 support for POP, IMAP, SMTP auth and Webmail services
- Software / Appliance remain in IPv4 (e.g. Mail Scanner, Opensource DB server)

**Long Term Approach**
- Application Software/OS Upgrade (e.g. Webmail Scanner, PC OS, etc..)
- Application Software / Appliance Replacement (e.g. various Mail Scanning applications etc..)
Key Customer Benefits

- Assessment provided a holistic view in both architecture and assessment inclusion (software apps/OS).
- Device Assessment which identified SW and HW gaps so that ASIAGOV facilitated determining upcoming budget requirements.
- Provided ASIAGOV with long and short term solutions to certain application or architectural shortcomings.
Complete Your Session Evaluation

- Please give us your feedback!!
  Complete the evaluation form you were given when you entered the room
- This is session BRKxxx-xxxx

Don’t forget to complete the overall event evaluation form included in your registration kit

YOUR FEEDBACK IS VERY IMPORTANT FOR US!!! THANKS