Enterprise IPv6 Deployment Strategies

BRKRST-2301

Tim Martin
CCIE #2020
Solutions Architect

@bckcntryskr
Agenda

• Planning & Deployment Strategies
• Design Considerations
• Host Configuration & Behavior
• IPv6 in the Campus
• IPv6 in the Data Center
• IPv6 Translation Techniques
• IPv6 on the Internet Edge
• Conclusion
IPv6 Sessions at Cisco Live

- BRKRST-2301 - Enterprise IPv6 Deployment
- BRKCRT-2000 – Hard Core IPv6 Routing - No Fear
- BRKRST-2304 - Hitchhiker's Guide to Troubleshooting IPv6
- BRKRST-2667 - How to write an IPv6 Addressing Plan
- COCRST-2355 - Inside Cisco IT: Making The Leap To IPv6
- BRKSPG-2602 - IPv4 Exhaustion: NAT and Transition to IPv6 for Service Providers
- BRKSPG-2607 - IPv6 Deployment Best Practices for the Cable Access Network
- BRKRST-2116 - IPv6 from Intro to Intermediate
- BRKRST-2311 - IPv6 Planning, Deployment and Troubleshooting
- BRKSEC-2003 - IPv6 Security Threats and Mitigations
- BRKSPV-2951 - Lessons learned from the first deployment of an IPv6 IPTV system
- BRKSPG-3300 - Service Provider IPv6 Deployment
- TECRST-3614 - Practical Knowledge for Enterprise IPv6 Deployments
- LTRRRST-1301 - IPv6 Hands-on Lab
Reference Materials


Recommended Reading
Planning and coordination is required from many across the organization, including …

✓ Network engineers & operators
✓ Security engineers
✓ Application developers
✓ Desktop / Server engineers
✓ Web hosting / content developers
✓ Business development managers
✓ …

Moreover, **training will be required** for all involved in supporting the various IPv6 based network services

- **Build your IPv6 Transition Team**
Where do I start?

- Core-to-Access – Gain experience with v6
- Turn up your servers – Enable the experience
- Access-to-Core – Securing and monitoring
- Internet Edge – Business continuity
IPv6 Deployment Options

Encapsulation Services

- IPv4 over IPv6
- IPv6 over IPv4

Translation Services

Dual Stack

Recommended Enterprise Co-existence Strategy
Design Considerations
Hybrid Mode

- Leverages existing IPv4 infrastructure
- Allows “slower” roll into IPv6 deployment
- Poor scalability and overall performance, no Multicast support
- Tunneling everywhere, “flattens” the network you have built
Service Block Mode

- Provides tighter control of where IPv6 is deployed
- Allows for reduced time to deliver IPv6 services
- Cost of SB equipment and it’s reuse in the network
- Eventually hits scalability and overall performance, no Multicast support
Dual Stack Mode

- Preferred Method, Versatile, Scalable and Highest Performance
- No Dependency on IPv4, runs in parallel on dedicated HW
- No tunneling, NAT or other performance degrading technologies
- Does require IPv6 support on all devices
IPv4 & IPv6 Combined

- Should we use both on the same link at Layer 3?
- Separate links, possibly to collect protocol specific statistics
- Routing protocols OSPFv3, EIGRP combined or separate?
- Fate sharing between the data and control planes per protocol
Infrastructure with Link Local on Links

- Topology hiding, Interfaces cannot be seen by off link devices
- Reduces routing table prefix count, Less configuration
- Need to use ULA or GUA for management and troubleshooting
- What about DNS?, WAN connections and more
Unique Local Address (ULA) & Global

- Both ULA and Global are used except for Internal only hosts
- Semi random generator requires non sequential /48’s, avoid M&A challenges
- Need to use Global for troubleshooting beyond the internal network
- Multiple policies to maintain (ACL, QoS, Routing, etc..)
To NAT or NOT

• Today, NAT44 & RFC1918
• All PA or all PI and peering in multiple regions
  – PI from one region and run it everywhere?
  – ISP in one region reject PI block from another?
  – What about translation?
• IETF does NOT recommend the use of NAT66 w/IPv6
• NAT ≠ Firewall – RFC 4864 (Local Network Protection)
• NAT ≠ Firewall – RFC 7021 (Impact of CGN on Applications)

Some enterprises are getting a prefix per RIR and only deploying one. Building backup plans with the others.
Prefix Length Considerations

- /64 everywhere a host
- /127 Point to Point
  - Allocate the full /64
  - Don’t use all 0’s or 1’s
  - Nodes 1&2 not in subnet
- /128 Loopback
  - out of a single /64 as a option
- /64 on every access port..
Host Configuration & Behavior
IPv6 Host Portion Address Assignment

<table>
<thead>
<tr>
<th>Similar to IPv4</th>
<th>New in IPv6</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Manually configured</strong></td>
<td><strong>State Less Address Auto Configuration</strong></td>
</tr>
<tr>
<td>Assigned via DHCPv6</td>
<td>SLAAC EUI64</td>
</tr>
</tbody>
</table>

* Secure Neighbor Discovery (SeND)
RA Message

• M-Flag – Stateful DHCPv6 to acquire IPv6 address
• O-Flag – Stateless DHCPv6 in addition to SLAAC
• H-Flag – Mobile IP home agent
• Preference Bits – Low, Med, High
• Router Lifetime – Must be >0 for Default
• Options - Prefix Information, Length, Flags
• L bit – Only way a host get a On Link Prefix
• A bit – Set to 0 for DHCP to work properly

Type: 134 (RA)
Code: 0
Checksum: 0xff78 [correct]
Cur hop limit: 64
∞ Flags: 0x84
  1… .... = Managed (M flag)
  .0.. .... = Not other (O flag)
  ..0. .... = Not Home (H flag)
  ...0 1... = Router pref: High
Router lifetime: (s)1800
Reachable time: (ms) 3600000
Retrans timer: 1000
ICMPv6 Option 3 (Prefix Info)
Prefix length: 64
∞ Flags: 0x80
  1… .... = On link (L Bit)
  .1... .... = No Auto (A Bit)
Prefix: 2001:0db8:4646:1234::/64
IPv6 on SLAAC

C:\Documents and Settings\> netsh
netsh> interface ipv6
netsh interface ipv6> show address
Querying active state...
Interface 5: Local Area Connection

<table>
<thead>
<tr>
<th>Addr Type</th>
<th>DAD State</th>
<th>Valid Life</th>
<th>Pref. Life</th>
<th>Address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Public</td>
<td>Preferred</td>
<td>29d23h58m25s</td>
<td>6d23h58m25s</td>
<td>2001:0db8:2301:1:202:8a49:41ad:a136</td>
</tr>
<tr>
<td>Temporary</td>
<td>Preferred</td>
<td>6d21h48m47s</td>
<td>21h46m</td>
<td>2001:0db8:2301:1:bd86:eac2:f5f1:39c1</td>
</tr>
<tr>
<td>Link</td>
<td>Preferred</td>
<td></td>
<td></td>
<td>fe80::202:8a49:41ad:a136</td>
</tr>
</tbody>
</table>

netsh interface ipv6> show route
Querying active state...

<table>
<thead>
<tr>
<th>Publish</th>
<th>Type</th>
<th>Met</th>
<th>Prefix</th>
<th>Idx</th>
<th>Gateway/Interface Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>no</td>
<td>Autoconf</td>
<td>8</td>
<td>2001:0db8:2301:1::/64</td>
<td>5</td>
<td>Local Area Connection</td>
</tr>
<tr>
<td>no</td>
<td>Autoconf</td>
<td>256</td>
<td>::/0</td>
<td>5</td>
<td>fe80::20d:bdff:fe87:f6f9</td>
</tr>
</tbody>
</table>
IPv6 on DHCP

mymac:# ifconfig -a
en1: 8863<UP,BROADCAST,SMART,RUNNING,SIMPLEX,MULTICAST> mtu 1500
    options=10b<RXCSUM,TXCSUM,VLAN_HWTAGGING,AV>
    ether 68:5b:35:88:53:74
inet6 fe80::6a5b:35ff:fe88:5374%en1 prefixlen 64 scopeid 0x6
inet 10.130.31.112 netmask 0xffffff00 broadcast 10.130.31.255
nd6 options=1<PERFORMNUD>

mymac:# netstat –r
Destination          Gateway              Flags  Netif
default              fe80::5:73ff:fe0a0:d523  UGc     en1

Windows 7, Mac OSX use pseudo random by default.
MSFT Transitional Adapters

C:\> ipconfig

Tunnel adapter **ISATAP** Adapter
Media State : Media disconnected
Connection DNS Suffix : foo.com

Tunnel adapter **Teredo** Adapter
Media State : Media disconnected
Connection-specific DNS Suffix :

Tunnel adapter **6TO4** Adapter:
Media State : Media disconnected
Connection-specific DNS Suffix :

← Used within administrative domain (IP41)
::0:5efe:w.x.y.z/96 – Private v4
::200:5efe:w.x.y.z/96 – Global v4

← Used with RFC 1918 address’s (UDP3544)
2001:0:{srvr v4}:{flags}:{udp}:{nat v4}

← Used with global IPv4 address’s (IP41)
2002:xw.x.y.z::

Can be disabled via Registry, GPO, Powershell, etc.
RFC 6724 – Default Address Selection

- Scope, Preferred over Deprecated, Native over Transitional, Temporary over Public
- Must support application override API, Choice of v6 over v4 is application dependent
- Give IPv6 300ms Head Start Pv6/IPv4 Lookup & Connect Retrieve and Display

| Temporary | Preferred | 2001:0db8:2301:1:bd86:eac2:f5f1:39c1 |
| Public    | Preferred  | 2001:0db8:2301:1:202:8a34:bead:a136 |
| Link      | Preferred  | fe80::202:8a34:bead:a136 |

NCSI – Network Connection Status Indicator

Application Layer
TCP/UDP
IPv6
IPv4
Disabling Ephemeral Addressing

- Enable DHCPv6 via the M flag
- Disable auto configuration via the A bit in option 3
- Enable Router preference to high
- Enable DHCPv6 relay

```plaintext
ipv6 unicast-routing
!
interface fastEthernet 0/0
  ipv6 address 2001:db8:1122:acc1::/64 eui-64
  ipv6 nd managed-config-flag
  ipv6 nd prefix default no-autoconfig
  ipv6 nd router-preference high
  ipv6 dhcp relay destination 2001:db8:add:cafe::1
```
Campus
HSRP for IPv6

- Many similarities with HSRP for IPv4 from design perspective (odd/even prefix)
- Virtual MAC derived from HSRP group number and virtual IPv6 link-local address
- Layer 2 - 0005.73a0.0001 → 3333.0000.0066
- Layer 3 – FE80::5:73ff:fea0:1 → FF02::66
- Layer 4 – UDP port 2029 (HSRPv6)

Unix Host with GW of VIP

unixhost# route -A inet6 | grep ::/0 | grep eth2
::/0 fe80::5:73ff:fea0:1

interface FastEthernet0/1
ipv6 address 2001:DB8:66:67::2/64
standby version 2
standby 2 ipv6 autoconfig
standby 2 timers msec 250 msec 800
standby 2 preempt
standby 2 preempt delay minimum 180
standby 2 authentication cisco
GLBP for IPv6

- Modification to NA, default GW is announced via RA using vmac
- AVG assigns Vmac’s and responds to NDP, directing hosts to the AVF’s
- R1 - Layer 2 – 0007.B400.0101 → 3333.0000.0066
- R2 - Layer 2 – 0007.B400.0102 → 3333.0000.0066
- R1&2 - Layer 3 – FE80::1001 → FF02::0100:5E00:66
- Layer 4 – UDP port 3222 (GLBPv6)

```conf
interface fastethernet0/0
ipv6 address 2001:db8::/64 eui-64
glbp 6 ipv6 fe80::1001
glbp 6 priority 110
glbp 6 preempt
glbp 6 load-balancing weighted
glbp 6 weighting 110 lower 95 upper 105
glbp 6 authentication md5 key-string 7 cisco
```
IPv6 QoS Policy & Syntax

- IPv4 syntax has used “ip” following match/set statements
  - Example: match ip dscp, set ip dscp
- Modification in QoS syntax to support IPv6 and IPv4
- New match criteria
  - match dscp
  - match precedence
- New set criteria
  - set dscp
  - set precedence
- No change for IPv6 WRED, WRR, Policing
**IPv6 Multicast Listener Discovery (MLD)**

- MLD uses LL source addresses
- 3 msg types: Query, Report, Done
- MLD packets use “Router Alert” in HBH
- MLDv1 = (*,G) shared, MLDv2 = (S,G) source

---

**MLD Snooping**

<table>
<thead>
<tr>
<th>MLD</th>
<th>IGMP</th>
<th>Message Type</th>
<th>ICMPv6 Type</th>
<th>Function</th>
</tr>
</thead>
<tbody>
<tr>
<td>MLDv1 (RFC 2710)</td>
<td>IGMPv2 (RFC 2236)</td>
<td>Listener Query</td>
<td>130</td>
<td>Used to find out if there are any multicast listeners</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Listener Report</td>
<td>131</td>
<td>Response to a query, joins a group</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Listener Done</td>
<td>132</td>
<td>Sent by node to report it has stopped listening</td>
</tr>
<tr>
<td>MLDv2 (RFC 3810)</td>
<td>IGMPv3 (RFC 3376)</td>
<td>Listener Query</td>
<td>130</td>
<td>Used to find out if there are any multicast listeners</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Listener Report</td>
<td>143</td>
<td>Enhanced reporting, multiple groups and sources</td>
</tr>
</tbody>
</table>
Zeroconf over IPv6

- Apple (Bonjour) has a light weight approach, adopted quicker
- FF02::FB – Multicast DNS – mDNS
- Microsoft (Rally) has a more robust, heavier implementation, has moved slower
- FF02::C – Simple Service Discovery Protocol – SSDP, UPnP
- FF02::1:3 – Link Local Multicast Name Resolution – LLMNR (File Sharing enabled)
IPv6 First Hop Security (FHS)

IPv6 FHS

Core Features
- RA Guard
- DHCPv6 Guard
- Source/Prefix Guard
- Destination Guard

Advance Features
- RA Throttler
- ND Multicast

Protection:
- • Rouge or malicious RA
- • MiM attacks
- • Invalid DHCP Offers
- • DoS attacks
- • MiM attacks
- • Invalid source address
- • Invalid prefix
- • Source address spoofing
- • DoS attacks
- • Scanning
- • Invalid destination address
- • Scale converting multicast traffic to unicast
- • Control traffic necessary for proper link operations to improve performance

IPv6 Snooping
First Hop Security for IPv6 Clients

- RA Guard - enabled at AP by default, always on at the controller
- DHCPv6 Guard – blocks client side DHCPv6 Advertise packets
- Source Guard – prevents client spoofing, enabled at controller by default
- Address Accounting – RADIUS “Framed-IP-Address” attribute
FHS Configurations

- Three Iterations of FHS, Platform Specifics Will Vary
- Port Access Control List (PACL), Lot’s of Flexibility
- Individual Guard Components, Prior to Binding Table
- Feature Aggregation Bundled Under Policy, Gleaning

**PACL**

```plaintext
ipv6 access-list FHS
deny icmp any any router-adver
permit ipv6 any any!
interface gigabitethernet1/0/1
ipv6 traffic-filter FHS in
```

**Guards**

```plaintext
interface ethernet1/0/1
ipv6 nd raguard
ipv6 dhcp guard policy Host
device-role client!
vlan configuration 46
ipv6 dhcp guard attach-policy
```

**Policy**

```plaintext
ipv6 snooping logging packet drop
ipv6 snooping policy HOST!
interface gigabitethernet1/0/1
switchport port-security maximum 2
ipv6 snooping attach-policy HOST
```
RA Throttle & ND Multicast Suppression

- Scaling the 802.11 multicast reliability issues
- NDP process is multicast “chatty”, consumes airtime
- Controller rate limits the period RA’s, while allowing RS to flow
- Caching allows the Controller to “proxy” the NA, based on gleaning
Distribution Layer: General Prefix Feature

```
ipv6 general-prefix foo-core 2001::0db8:4646:6000::/52
ipv6 general-prefix foo-acc 2001::0db8:4646:6acc::/56
ipv6 unicast-routing

interface GigabitEthernet1/0/1
description To 6k-core-right
ipv6 address foo-core ::3:0:0:0:d63/64
ipv6 eigrp 10
ipv6 hello-interval eigrp 10 1
ipv6 hold-time eigrp 10 3
ipv6 authentication mode eigrp 10 md5
ipv6 authentication key-chain eigrp 10 eigrp
ipv6 summary-address eigrp 10 2001::0db8:4646:6000::/52

interface GigabitEthernet1/0/2
description To 6k-core-left
ipv6 address foo-core ::C:0:0:0:d63/64
ipv6 eigrp 10
ipv6 summary-address eigrp 10 2001::0db8:4646:6000::/52

interface Vlan4
description Data VLAN for Access
ipv6 address foo-acc ::4:d63/64
ipv6 eigrp 10

interface Vlan6
description Data VLAN for Access
ipv6 address foo-acc ::6:d63/64
ipv6 eigrp 10
ipv6 router eigrp 10
no shutdown
router-id 10.122.10.10
passive-interface Vlan4
passive-interface Vlan6
passive-interface Loopback0
```

RIPng

RIPng – UDP 521, 15 hops
FE80::/64 Source → FF02::9 Destination

Distance Vector, Hop Count (1-15)

Split Horizon, Poison Reverse

Beuller, Bueller, anyone?

IPv6 unicast-routing

Interface loopback 0
IPv6 address 2001:db8:1000::1/128
IPv6 rip CISCO enable

Interface ethernet 0/0
IPv6 address 2001:db8:5000:31::1/64
IPv6 rip CISCO enable

IPv6 router rip CISCO
**ISIS**

**IS-IS – (RFC5308) CLNS**
IPv4 & IPv6

Link State
2 New TLV’s Added

Topology Support
- Single Topology
- Multi Topology
- Multi Instance

---

**IPv6 unicast-routing**

**Interface ethernet 0/0**

**IPv6 address 2001:db8:5000:31::1/64**

**IPv6 router isis CISCO**

**Isis circuit-type level-1**

**Isis ipv6 metric 10000**

**Router isis CISCO**

**Net 49.0001.2222.2222.222.00**

**Metric style wide**

**Address-family ipv6**

**Multi-topology**
**EIGRP**

**EIGRP – IP 88**
FE80::/64 Source → FF02::A Destination
2 New TLV’s – internal-type & external-type
No Split Horizon, Auto Summary Disabled

Stub reduces the topology table and the number of queries being sent into the infrastructure..

EIGRP can perform better in large scale hub and spoke environments

---

Ipv6 unicast-routing!
Interface loopback0
Ipv6 address 2001:db8:1000::1/128
Ipv6 eigrp 11!
Interface ethernet 0/0
Ipv6 address 2001:db8:5000:31::1/64
Ipv6 eigrp 11!
Ipv6 router eigrp 11
Passive-interface loopback0
Eigrp router-id 10.10.10.10
OSPFv3

OSPFv3 – IP 89
FE80::/64 Source → FF02::5 (all), FF02::6 (DR’s)
Link-LSA (8) – Local Scope, NH
Intra-Area-LSA (9) – Routers Prefix’s
Use Inter-Area-Prefix (3) – Between ABR’s

Can converge quickly to a point of scale, initial database build and discovery takes some time

Link state protocols perform better in full mesh environments, if tuned correctly

Iov6 unicast-routing
!
Interface loopback0
Iov6 address 2001:db8:1000::1/128
Iov6 ospf 3 area 0 instance 13
!
Interface ethernet 0/0
Iov6 address 2001:db8:5000:31::1/64
Iov6 ospf 3 area 0 instance 13
!
Iov6 router ospf 3
router-id 10.10.10.10
passive-interface loopback0
MPLS 6PE

- RFC 4798
  - Utilizes Existing IPv4 Core
  - Dual Stack on the PE
- MP-BGP Next Hop ::ffff:192.0.2.210
- LDP Next Hop 192.0.2.210
- Control Plane uses IPv4, for now

IPv6  MP-BGP  LDPv4

router bgp 192
no bgp default ipv4-unicast
bgp log-neighbor-changes
neighbor 192.0.2.3 remote-as 192
neighbor 129.0.2.3 update-source Loopback0

address-family ipv6
redistribute connected
redistribute static
no synchronization
neighbor 192.0.2.3 activate
neighbor 192.0.2.3 send-label
exit-address-family

ipv6 route 2001:db8:babe::/48 2001:db8:1:1::2

IPv4 core, LDP, IGP, TE, etc.
MPLS 6VPE

- RFC 4659
  - Utilizes Address Family (AF) in VRF Context
  - Allows for VPN Functionality
- Subsequent Address Family Identifiers (SAFI)
  - MP-BGP Address-family SAFI = 2 (IPv6)
  - VRF Address-family SAFI = 128 (VPN)

IPv4 core, LDP, IGP, TE, etc.

vrf definition 6vpe
rd 192:1
route-target export 192:1
route-target import 192:3

address-family ipv6
exit-address-family

router bgp 192
address-family vpnv6
neighbor 192.0.2.3 activate
neighbor 192.0.2.3 send-community both
exit-address-family

address-family ipv6 vrf 6vpe
redistribute connected
redistribute static
no synchronization
exit-address-family
Data Center
IPv6 Transition Stages in the Data Center

- IPv4 Only Data Center
  - IPv6 Translation on the Front End
- Dual Stack
  - Both IPv4 & IPv6 Into the Data Center
- IPv6 Only Data Center
  - IPv4 Translation on the Front End
- What is the Cost of Each Stage?
Traditional IPv4 Only

- IPv4
- Load Balancer inline
- No translation in this design
- Services are Firewalled
IPv4 Only Data Center

- Dual Stack Front End
- Translation via NAT/Proxy/SLB
- Easy to Turn Up
- Hard to Move Forward
- False Sense of Accomplishment
Dual Stacked

- IPv4 & IPv6 Addressing on All Devices
- Incremental Operational Cost (~20%)
- Double Everything (ACL’s, SLA’s, etc.)
- Two Data Planes, Two Control Planes
- Recommended Approach
IPv6 Only Data Center

- Dual Stack Front End
- Translation via NAT/Proxy/SLB
- Forces Developers to use IPv6
- Reduces Operational Costs
- Eliminates Complexity within the DC
IPv6 Only

- IPv4 Sailed Toward Sunset
- Not Likely for a Very Long Time
- Someday, Maybe Someday
Data Center Interconnect (DCI)

- Replication Services, Disaster Recovery
- Shared Assets and Resources
- Overlay Transport Virtualization (OTV)
  - L2 Technologies Encapsulated in L3
  - IPv6 Within OTV over IPv4
  - Disable Optimized Multicast Forwarding (OMF) in IGMP snooping on OTV edge devices for IPv6 Solicited Node Multicast traffic to flow.
IPv6 Readiness: Servers

• Hosts are ready
  – Windows enabled by default, disabling it = no more support from Microsoft
  – Mac OS X, iOS, Android, Linux, */BSD: enabled by default

• File & Print
  – No WINS or NetBios over IPv6
  – SMB on TCP 445

• SQL Server
  – IPv6 preferred
  – Watch for v4 socket calls

• Server 2008/R2
  – Needs Unified Access Server

• Server 2012
  – Includes UAS, NAT64/DNS64
Migrating Applications to IPv6

- Inconsistent API’s use of IPv6 Addresses
  - Some functions expect a URL (must enclose with brackets for IPv6)
  - Some functions expect just an IP (no bracket)
- Know whether your app displays or accept an IPv6 address
- 198.51.100.44:8080 → [2001:db8:café:64::26]:8080

- Home grown App’s may only support IPv4
- Pressure vendors to move to protocol agnostic framework
- RFC 3493 – Open Socket Call, 64 bit structure align to HW
- RFC 3542 – Raw Socket, ping, Traceroute, r commands
Provisioning & Network Management

- SNMPv3 over IPv6 and managing IPv6 MIB’s
- Protocol Version Independent (PVI) manage the same OID’s (RFC’s 4292, 4293)
- NetFlow, Deep Packet Inspection, IPSLA, all work with IPv6
- IPv6 support for Wireshark, Packet analysis, MRTG, Netflow collectors, etc..

DHCP
- Server supports IPv4 and IPv6
- Internal & external

DNS
- Server supports IPv4 & IPv6
- DNSSEC

IPAM
- Integrated DNS and DHCP
- Configuration and reporting
Resilient DDI Design

- Anycast Address for Client Access to DHCP/DNS
- Uses the same address in multiple locations
- Simple, Scalable and Reliable Solution
- Global Unicast Address (GUA) for Service Uptime
- DNS server injects /128 via OSPF
Translation Techniques
Translation Techniques

**Proxy**
- IPv6 Internet
- IPv6
- IPv4
- Makes State. SW @ L7 performance

**Server Load Balancer**
- IPv6 Internet
- IPv6
- IPv4
- Client Visibility Access to L7

**Stateful NAT64**
- IPv4 Internet
- IPv4
- IPv6
- Transparent @ L4 MTU Issues
NAT64 Translation Techniques

• Translation Algorithms
  – RFC 6052 (Implementation Details)

• Framework for Translation
  – RFC 6144 (Implementation Scenarios)

• Stateless NAT64
  – RFC 6145 (IP/ICMP Translation Algorithm)
  – Maps the Entire IPv4 Internet into IPv6 Prefix

• Stateful NAT64
  – RFC 6146 (State Table for IPv4/IPv6 Translation)
  – Used mainly where IPv6-only clients need to access IPv4 servers

• DNS64
  – RFC 6147 (IPv6 Client to IPv4 Server)
Framework for Translation

Scenarios Defined

• RFC 6144
  – 8 Total Scenarios (4, 7, 8 are NA)
  – 1, 2, 3 Involve Internet Connectivity
  – 5 & 6 Are Focused on Intranet Connectivity

• Stateless Translation
  – Algorithmic Mapping
  – Address Information & Translator Configuration
  – Initiation from IPv4 or IPv6

• Stateful Translation
  – Uses a State Table for Translation
  – Based on L3/L4 Tuples
  – Generally Initiation is from IPv6
Stateless IP/ICMP Translation

Ideal for IPv6 Only Data Center

- RFC 6145
  - Algorithmic Binding
  - 1:1 Address Mapping

- IP Header Fields
  - Copy ToS to/from Traffic Class
  - Id, Flags & Offset to/from EH 44
  - TTL to/from Hop Limit and Decrement
  - Protocol to/from Next Header
  - Checksum Computed IPv6 to IPv4

- ICMP Header Fields
  - Type Translated (IPv4 8, 0 to IPv6 128, 129)
Stateful NAT64

Ideal for IPv6 Only Networks Accessing IPv4

• RFC 6146
  – State Table is Maintained
  – Overload Address Mapping

• TCP/UDP/ICMP Headers
  – Form L4 Portion of State Tuple
  – Pseudo Checksum for IPv6 Portion
  – No Multicast, IPSec, etc.

• MUST use DNS64 RFC 6147
  – Synthesis DNS Records AAAA to A

• ALG’s May be Required

• MTU Issues Possible

*Use Static IPv6 to IPv4 Mappings
**DNS64**

- Step 1 ➔ IPv6 PC queries **AAAA Record** for v4 Server
- Step 2 ➔ DNS responds “empty” **AAAA Record**
- Step 3 ➔ Translator Sends **A Record** for v4Server
- Step 4 ➔ DNS Server responds **A Record** for IPv4Server
- Step 5 ➔ translates it to a **AAAA Record**

**Network-Specific Prefix**

- 2001:db8:122:344::6
- 2001:db8:122:344::/64
- 192.0.2.0/24
- 3001::/96
- 3001::3001:c000:221

**IPv6 PC**

- 2001:db8:122:344::6

**DNS Server**

- 192.0.2.0/24
NAT64

← Source IPv6 3001::3001:c000:221 Dest. IPv6 2001:db8:122:344::6

← Source IPv4 192.0.2.33 Dest. IPv4 192.0.2.1

→ Source IPv6 2001:db8:122:344::6 Dest. IPv6 3001::3001:c000:221

→ Source IPv4 192.0.2.1 Dest. IPv4 192.0.2.33
SLB64 Translation Technique
Citrix NetScaler

- Virtual IP (VIP), SNAT Pool
- Publish Appropriate AAAA Record
- IPv6 to IPv4, Similar to NAT64
- Translation & SLB are done on same platform

- OS/App dictate design parameters
- Rapid Time to Deploy
X-Forwarded-For (XFF)

- Web Server Logging for **Geo Location, Analytics, Security**, etc..
- Source IP of client requests will be logged as the SNAT or other NAT’d address
- Packet may go through multiple proxies

**Example:**

```
GET / HTTP/1.1
Host: www.foo.org
User-Agent: Mozilla Firefox/3.0.3
Accept: text/html,application/xhtml+xml,application/xml
Accept-Language: en-us,en
Keep-Alive: 300
x-forward-for: 2001:db8:ea5e:1:49fa:b11a:aaf8:91a5
Connection: keep-alive
```
Internet Edge to ISP

- Do you support dual stack peering?
- Do you have a separate (SLA) for IPv6?
- Do you support BGP peering over IPv6?
- Do you have a FULL IPV6 route table?
- What is the maximum prefix length?

- What about DNS…

Hosted Cloud Service

- Maximum prefix length offered by the cloud provider?
- Access to provisioning and billing portal over IPv6?
- Global IPv6 addressing for VM’s in your environment?
Internet Edge to ISP

Single Link
Single Prefix

ISP 1

Enterprise

Default Route

Dual Links
Single Prefix

ISP 1
POP1
POP2

Enterprise

Multi-Homed
Multi-Prefix

USA
ISP 1
ISP2

Enterprise

BGP

ISP3
ISP4

Europe
Multi Homing

- **Challenges Arise**
  - Upstream Address Filters
  - Asymmetric Routing
  - Default GW & NH Selection

- **Small to Medium Enterprise**
  - Provider Allocated
  - NPTv6, LISP

- **Medium to Large Enterprise**
  - Provider Independent
  - BGP
Multi Homed (NPTv6)

- Small to Medium Enterprise
  - Provider Allocated
  - Not Topology Hiding
- Swaps Left Most Bits of Address
  - Just the Prefix
  - Length Must be Equal
- Public on Outside (2001:db8::/48)
- Private on Inside (FD00::/8)
- No Protocol “fixups”, Unless ALG’s are Supported
Multi Homed (LISP)

- Small to Medium Enterprise
- Tunneling the PA IPv6 over LISP
  - Provider Allocated /48
  - Hosted by PxTR Provider
- Avoids Multi Prefix PA Issues
- Possibly an ISP that is IPv4 Only
- SHIM6, HIP, ILNP etc.
  - OS Mods, Code Change
Multi Homed, Multi Prefix (BGP)

- Medium to Large Enterprise
- Use a /127 on pt-2-pt, /64 on multipoint
- **MD5 shared secret’s**, IPSec could be used
- **Controlling TTL**, accepting >254 only (allow -1)
- Prefix Size Filtering, /32 - /48

```
router bgp 200
bgp router-id 4.6.4.6
neighbor 2001:db8:cafe:102::2 remote-as 2014
neighbor 2001:db8:cafe:102::2 ttl-security hops 1
neighbor 2001:db8:cafe:102::2 password cisco4646
```
IPv6 Bogon and Anti-Spoofing Filtering

- Anti-spoofing (RFC2827, BCP38), Multi homed filtering (RFC3704, BCP 84)
- uRPF – Unicast Reverse Path Forwarding
Securing the Edge, FW and/or Perimeter Router

• Address Range
  – Source of 2000::/3 at minimum vs. “any”, permit assigned space

• ICMPv6
  – Error types thru, NDP to, RFC 4890

• Extension Headers
  – Allow Fragmentation, others as needed. Block HBH & RH type 0

• IPv6 ACL’s
  – IPv6 traffic-filter – to apply ACL to an interface

  ```
  permit icmp any any nd-na
  permit icmp any any nd-ns
  deny ipv6 any any
  ```
Conclusion
Key Take Away

• Gain **Operational Experience** now
• Security enforcement is possible
• Control IPv6 traffic as you would IPv4
• “Poke” your Provider’s
• IPv6 is here now are you?
Complete Your Online Session Evaluation

• Give us your feedback and you could win fabulous prizes. Winners announced daily.

• Complete your session evaluation through the Cisco Live mobile app or visit one of the interactive kiosks located throughout the convention center.

Don’t forget: Cisco Live sessions will be available for viewing on-demand after the event at CiscoLive.com/Online
Continue Your Education

• Demos in the Cisco Campus
• Walk-in Self-Paced Labs
• Table Topics
• Meet the Engineer 1:1 meetings
Registration Open for the 2014 North American IPv6 Summit

Register HERE for the 2014 North American IPv6 Summit, September 24-25, 2014!

Organized by the Rocky Mountain IPv6 Task Force (RMv6TF), and supported by the North America Regional IPv6 Task Forces, this is the largest IPv6 event in North America.
Thank you.