Journey to a pure IPv6 Campus

Loghs Srinivasan
Director - SW Dev, Enterprise Network Solutions, Cisco
Oct. 2018
Agenda

- Business rationale to pursue IPv6
- Roadblocks to successful adoption
- Making it work
- IPv6 Readiness – Leap for IT
- Trouble shooting & Lesson Learn
- What Next?
Business rationale to pursue IPv6

- Migration from VM to containers
- Removing multi layer NAT
- Single stack (removal of dual stack)

Operational simplicity
Campus is the last frontier in this migration
## Roadblocks to a successful IPv6 adoption

- End user mindset (IPv4 literal to host name)
- Applications which are not v6 ready (Eg: TightVNC)
- Handling v4 only infrastructure (labs)
- Sites that are still v4 only enabled (Eg: bbc.com)
- Devices which do not support dhcpv6 (Android)
# Making it work
Pure IPv6 campus journey for IT

### IT Transition
- Examine access network

### Network Validation
- Building traffic analysis
- Access Network Dual stack
  - 100 V6 only devices/users

### End User Preparation
- Identify Primary applications in building
- Nat64/DNS64 for applications
  - SLAAC/ RDNSS for Android

### Step 1
- Prepare users for the transition
  - (Dual-stack is common but not 100%)
- Identify v4 literal hotspots (labs)
- Implement hostname

### Step 2
- Migrate Network
  - (data path to pure V6)
  - 100 V6 only devices
- War rooms to address any issues/questions

### Step 3
- IPv6 foundations determined healthy
- Migrate the entire building to V6

---

**One step for IPv6, a leap for IT readiness**
SJC23-IPv6 Only Network
IPv6 in Enterprise - Deployment details
San Jose building case study

- 500+ users
- 3 floors, 6 wiring closets
- 500+ switch ports, 120 APs
- 40~ applications
- 3 months phased approach
  - IT template
Supporting wide range of services for the building users

- **Applications** such as VNC, Remote Desktop, Google DOCS, Skype
- **Collab endpoints** on PCs/Laptops such as, Spark Client, Spark Web, Webex
- **Devices** such as: Mac, Windows, iPhone, Android OS
- **Enterprise services** such as CiscoTV, Anyconnect, Outlook, Telepresence, Proximity etc had to be carefully planned for operations
- **All mgmt configs** were done only using IPv6 - SNMP, Netflow, WaaS etc
- **Network protocols** used such as Nat64/DNS64, SLAAC
Building 23 IPv6 Transition: Users Experience

Understand what people use the network for
- Functional groups/Visitors
- Building Traffic analysis
- Identify Primary Applications:
  - Collaboration
    - Call/Telepresence
    - Spark (inc. Video Call)
    - Jabber
  - Business Apps
    - Exchange/email
    - http/intranet/wiki
    - Video/Cisco TV
    - VNC/Remote Desktop

Prepare Users for IPv6
- Build User Profiles
  - Engineering Dev/Test (lab dependent)
  - Business/Finance/Mgmt
  - Product Mgmt and Marketing
  - Engineering Release Mgmt
- Workshop and dry runs
  - Periodic dry runs to enable building users for transition
  - War rooms to address any issues/ questions
IPv6 - The journey

Where We Were  (July 2016)

- Enterprises Deployed
- Dual stack

IPv4
- Network Policy
- Mgmt Policy

IPv4
- Network Policy
- Mgmt Policy

Where We are now

- Enterprise products
- Few enterprises migrating to single stack

IPv6
- Network Policy
- Mgmt Policy
- IPv6 Solution Testing

San Jose building migrated to IPv6
One step for IPv6, a leap for IT readiness
The Building Network

- Keep it simple – L2, routing, DHCPv6, VSS, primarily wireless

```plaintext
interface Vlan22
  description v6WIRELESS-DATA
  no ip address
  ipv6 address FE80::DEF link-local
  ipv6 address X::1/64
  ipv6 nd prefix X::/64 0 0 no-autoconfig
  ipv6 nd managed-config-flag
  ipv6 nd other-config-flag
  ipv6 dhcp relay destination X::12
  ipv6 eigrp 233
```

- SLAAC for Android exception

```plaintext
interface Vlan27
  description ***SLAAC-VLAN***
  no ip address
  ipv6 address X::Y::Z::H::/64 eui-64
  ipv6 enable
  ipv6 nd ra dns-search-list domain cisco.com
  ipv6 nd ra dns server A::B::C::D::53
  ipv6 nd ra dns server A::B::C::F::53
```
How to deal with IPv6 islands

Islands aren’t always relaxing

- Despite dual-stack, v6 native internal apps/services are still not the norm
- DNS64/NAT64 is a critical enterprise service
DNS64/NAT64

NAT64/DNS64 holds it all together

- BIND9 as DNS64
  - can be added to existing
- ASR1002-X NAT64 with HA
  - Simple config and stable

```
nat64 prefix stateful 2001::/96
nat64 v4 pool NAT64-IPv4 10.x.y.z 10.x.y.zz
nat64 v6v4 list NAT64 pool NAT64-IPv4 overload redundancy 1 mapping-id 1
```
<table>
<thead>
<tr>
<th>Priority</th>
<th>Impact Level</th>
<th>Service</th>
<th>Application</th>
<th>Parity Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Medium</td>
<td>High</td>
<td>Client</td>
<td>File transfer FTP, TFTP, SSH, SCP</td>
<td>Yellow</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Client</td>
<td>Anyconnect</td>
<td>Yellow</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Client</td>
<td>Jabber</td>
<td>Green</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Client</td>
<td>Webex</td>
<td>Green</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Client</td>
<td>Outlook</td>
<td>Green</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
<td>Client</td>
<td>VNC</td>
<td>Green</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Client</td>
<td>Remote Desktop</td>
<td>Green</td>
</tr>
<tr>
<td>Medium</td>
<td>High</td>
<td>Client</td>
<td>Telepresence</td>
<td>Green</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Client</td>
<td>App Store</td>
<td>Green</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
<td>Client</td>
<td>IP Phone</td>
<td>Yellow</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Client</td>
<td>public web</td>
<td>Green</td>
</tr>
<tr>
<td>Medium</td>
<td>Medium</td>
<td>Client</td>
<td><a href="http://www.in.cisco.com">www.in.cisco.com</a></td>
<td>Green</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Client</td>
<td>Proximity</td>
<td>Red</td>
</tr>
<tr>
<td>Low</td>
<td>Low</td>
<td>Client</td>
<td>Google Docs</td>
<td>Yellow</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Client</td>
<td>dropbox</td>
<td>Yellow</td>
</tr>
<tr>
<td>High</td>
<td>Medium</td>
<td>Client</td>
<td>Cisco Print</td>
<td>Green</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Collab</td>
<td>Spark Client</td>
<td>Yellow</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Collab</td>
<td>Spark Web</td>
<td>Green</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Facilities</td>
<td>CCTV, Badge, Phys Security Infra</td>
<td>Yellow</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Mgmt</td>
<td>RCMD Mgmt</td>
<td>Yellow</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Mgmt</td>
<td>SNMP</td>
<td>Green</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Mgmt</td>
<td>Netflow</td>
<td>Yellow</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Mgmt</td>
<td>NTP</td>
<td>Green</td>
</tr>
<tr>
<td>High</td>
<td>High</td>
<td>Network</td>
<td>IPv6 Multicast</td>
<td>Red</td>
</tr>
<tr>
<td>High</td>
<td>Medium</td>
<td>Network</td>
<td>WaaS</td>
<td>Yellow</td>
</tr>
<tr>
<td>High</td>
<td>Medium</td>
<td>Network</td>
<td>ACS</td>
<td>Yellow</td>
</tr>
<tr>
<td>High</td>
<td>Medium</td>
<td>Network</td>
<td>ACS Radius</td>
<td>Yellow</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Network</td>
<td>dACLs/802.1x</td>
<td>Red</td>
</tr>
<tr>
<td>Medium</td>
<td>Low</td>
<td>Network</td>
<td>OSPFv3 routing, mult platforms</td>
<td>Green</td>
</tr>
<tr>
<td>Network</td>
<td>Low</td>
<td>Network</td>
<td>NAT64 on ASR/CSR</td>
<td>Green</td>
</tr>
<tr>
<td>Network</td>
<td>Low</td>
<td>Network</td>
<td>NAT64 on ASA</td>
<td>Green</td>
</tr>
<tr>
<td>Network</td>
<td>Low</td>
<td>Network</td>
<td>DNS64 on bind9</td>
<td>Green</td>
</tr>
<tr>
<td>Network</td>
<td>Low</td>
<td>Network</td>
<td>CAPWAP over v6</td>
<td>Green</td>
</tr>
</tbody>
</table>
Trouble shooting Case study & Lessons learn
Enterprise complexity

This is why the journey matters

• Real experience shows what matters to users
• Real data provides comparisons
• Real impact incentives app/services owners
Named based access - As much behavioral as technical

- IPv4 targets with host name, will be resolved by DNS64 – No problem
- But engineers are used to connecting to lab devices using IPv4 address, e.g. 172.16.32.1
- Facilitate easy naming using a script to convert IPv4 address to host name:
  e.g. 172.16.32.1 → 172-16-32-1.cisco.com
NAT64/DNS64 issues encountered

• Incorrect AAAA responses
  e.g. ::
    ::1
    fe80::x
    64:ff9b::x
    2001:DB8::x
  • Workaround is to set exclude rule for prefixes other than 2000::/3 in DNS64 server.

• AAAA query returns SERVFAIL causing DNS64 synthesis failure even though A query was successful
  • Workaround is to create zone for the offending service on DNS64 which returns a synthesized answer. Artificially forcing the client through NAT64.
Case Study – Hot topic for IPv6 War Room

- VMware Fusion
  - VMware fusion on Mac doesn't work on IPv6 Only Network with NAT66 between VM and host machine.
  - Workaround is to change network settings to bridge mode to make it work.

- Oracle Virtual Box on Mac doesn’t work
  - As per Oracle, Virtual box requires a SLAAC IPv6 Network

- Android doesn’t support DHCPv6
  - Used SLAAC+RDNSS+DNSSL for android clients
Case Study – Hot Topic for IPv6 War Room

• SoftPhone does not register
  • Details: SoftPhone requires port 8443. This is not enabled for IPv6.
  • Workaround: Development team is engaged to patch or upgrade their Call Manager as a verification mechanism in the short term.

• Outlook on mac
  • Outlook for Mac v15 and above supports IPv6
What Next?

• Working with leading enterprise partners to enable more IPv6 only deployments
• DC migration to IPv6-only to expand more buildings to IPv6
• Development process change for new features. Parity between v4 and v6 for new development
• Working with industry leaders to drive V6 readiness for apps