Connect with Addressing Intelligence to Automate IPv6 Planning, Transition & Cyber Security

John L Lee, CTO
Co-Chair, IPv6 Address Planning Team, ACT-IAC, Federal IPv6 Working Group
Co-Editor, Planning Guide/Roadmap Toward IPv6 Adoption within the U.S. Government
SME Address Management Tools, NAv6TF

Internet Associates, LLC A Certified VOSB

April 11, 2012
IPv6 is moving

Planning Guide/Roadmap Toward
IPv6 Adoption within the US Government

Version 1.0
May 2000

Architecture and Infrastructure Committee,
Federal Chief Information Officers Council
Why Manage Addresses?

- If the Internet is a multi-billion dollar engine
  - IP addresses are the ball bearings …
- If the Internet is a castle (skyscraper)
  - IP addresses are the keys …
- If the Internet is a collection of networks and computers
  - IP addresses are how your route and switch traffic across it…
Agenda

- Business Drivers
- Address Management Issues
- Cyber Security
- Intelligence, Automation and its Technology Underpinnings
- Dynamic Address Planning
Business Drivers

- Data Center Consolidation and Virtualization
- Customer Connection and Experience
- Mobile Devices
- Lack of Address Space
It started with Howard in ‘99
This is not your fathers v4 network ...

Do not apply v4 thinking and design constraints to v6 networks

Ron Broersma, DREN Chief Engineer
Management Issues

- Large Geographically Dispersed Networks
- Multiple Political / Functional Boundaries
- Components not fully coordinated & Integrated
  - Operating & Support Systems
    - Network Planning, Design, Modeling & Provisioning
  - Network & Operations Management
  - Cyber Security Elements
Address Management 101

- Address uniqueness
  - Large number of new devices
  - Every device requires an address
  - Unique within a routing domain
- Proper engineering
  - Valid addresses
  - Efficient routing
  - Effective use of address space
- Critical for network operation
  - Errors cause disruption of network service
Partial List of Requirements

- Maintain all Addresses under Management
  - Complete, Accurate IP Address Lifecycle Support for IPv4, IPv6 and ASNs
  - Multiple Routing Domains
- Design & Engineer Address Architectures
- Model Equipment, Circuits, LANs & VLANs
- Coordination of Address and related information with Interfaces to:
  - Address, Device, Netflow & Network Discovery
  - Network Management & Security Applications
One Address per row

- **Text File**
  - Host.txt each line is an IP Address

- **Spread Sheet**
  - Each Row is one IP Address

  192.168.10.1 /32

- **DNS & DHCP**
  - Dynamic Host Configuration Protocol
  - Dynamic Name System

---

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Name</th>
<th>Office Number</th>
<th>Telephone</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.0.0</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.1</td>
<td>Core Router</td>
<td>Telco Closet 010</td>
<td>x2000</td>
</tr>
<tr>
<td>192.168.0.2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.3</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.4</td>
<td>Printer01</td>
<td>A100</td>
<td>x101</td>
</tr>
<tr>
<td>192.168.0.5</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.6</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.7</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.8</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.9</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.10</td>
<td>John</td>
<td>A140</td>
<td>x140</td>
</tr>
<tr>
<td>192.168.0.11</td>
<td>Sally</td>
<td>B200</td>
<td>x200</td>
</tr>
<tr>
<td>192.168.0.12</td>
<td>Alice</td>
<td>A050</td>
<td>x150</td>
</tr>
<tr>
<td>192.168.0.13</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.14</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.15</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.16</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.17</td>
<td>Jane</td>
<td>B120</td>
<td>x252</td>
</tr>
<tr>
<td>192.168.0.18</td>
<td>Joe</td>
<td>C120</td>
<td>x300</td>
</tr>
<tr>
<td>192.168.0.19</td>
<td>Cindy</td>
<td>Reception</td>
<td>x010</td>
</tr>
<tr>
<td>192.168.0.20</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.21</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.22</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.23</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.24</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>192.168.0.25</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Number of v6 Addresses

- /0: 340,282,366,920,938,463,463,374,607,431,768,211,456
- /16: 519,229,685,853,482,762,853,049,632,922,010
- /24: 20,282,409,603,651,670,423,947,251,286,016
- /32: 79,228,162,514,264,337,593,543,950,336
- /48: 1,208,925,819,614,629,174,706,176
- /64: 18,446,744,073,709,551,616
- /96: 4,294,967,296
IPALM

- IP Address Space is a binary data structure containing engineered IP address blocks of any size
  - Manage any size of block from /0 to /128 IPv6 & /0 to /32 IPv4
  - Split, Combine, Move, Coalesce, & Loan Blocks
  - All IP Addresses in the block are under Management
  - Multiple Unique Routing Domains supported
What is IP Address Lifecycle Management (IPALM)

- Enterprise/Component wide address authority and repository with distributed capability
- Automated methods to allocate, assign, un-assign & reclaim addresses
- Policy enforcement and rules to increase accuracy & integrity of addresses and network structure in the repository
- Equal functionality support for v4 and v6
Detailed IPALM Methods

- Manage addresses from definition to decommissioning through a lifecycle process
- Engineered IP Address Blocks (EIPAB)
  - Efficient block allocations and layout
  - Input Validation on all addresses with accurate assignments
  - Guaranteed unique within a routing domain
- Single Department/Enterprise-wide repository
  - High availability, mirrored transaction processing with geographically dispersed systems for COOP
  - Multiple simultaneous web based access
  - Policy Enforcement System wide
  - Active Directory Integration with PIV/CAC Card Multi-factor authentication support
IPv6 Support

- Address Planning & Design
- Dual Stack – Physical and virtual interfaces support multiple IPv4 and IPv6 addresses
- Interfaces addresses
  - /64 EUI-64 or Random, user-defined
- IPv4 – IPv6 Transition
20 Critical Controls – Consensus Audit Guidelines

- Inventory for Authorized & Unauthorized Devices & Software (1&2)
- Secure Configurations for Hardware & Software on Laptops, Workstations & Servers (3)
- Secure Configurations for Network Devices such as Firewalls, Routers & Switches (4)
- Boundary Defense (5)
- Maintenance, Monitoring, and Analysis of Security Audit Logs (6)
20 Critical Controls – Consensus Audit Guidelines …

- Continuous Vulnerability Assessment & Remediation (10)
- Account Monitoring & Control (11)
- Malware Defenses (12)
- Limitation & Control of Network Ports, Protocols & Services (13)
- Wireless Device Control (14)
- Secure Network Engineering (16)
- Penetration Tests and Red Team Exercises (17)
Cyber Security Eco-System

Monitor & Mitigate
- Firewall
- Intrusion Prevention System
- Intrusion Detection System
- Network Access Control
- Distributed Denial of Service Mitigation
- Honey Pot

Active Monitoring
- Route & Address Discovery
- Netflow Capture
- Network Device Discovery
- Botnet Detection

Active Penetration Testing
- IP Address, Ports & Protocols
- Router & Switches Management
- Ports Management, Security & Data Networks
- Web Pages & Services

Monitor
- Network Device Monitoring
- Server & Application Monitoring
- Syslog Monitoring
- Event Correlation

Network Engineering & Operations
- Router, Switch, Server, Fiber, Circuit & Network Device Configuration & Inventory

Network Modeling & Simulation
- Router & Switch Configuration Validation
- Network & Circuit Performance Application Performance
- Service Order Trouble Tickets
- Management Reports & Alerts

Authentication & Policy Enforcement
- IPAM
- DNS DHCP
- IP Address, IPv4, IPv6 & ASN Address Map
- Equipment, Interfaces & Network Topology
- SOAP/XML APIs

Network Traffic Generation & Analysis
- Security Policy Generation & Management
- ACLs, SAML Event Correlation

Sensor

IPal Technology is covered under U.S. Patents 7,127,505, 7,330,907, 7,523,189, 7,558,881, 7,739,406 and other US and International Patents Pending.
Automated IPAM (IPALM)
Automated Technologies

- Address Lifecycle Model
- Control, Organization and Trees
- Allocation and Assignment Methods
- Equipment Templates, Connections
- Interactive Address Map
- Planning Engine
INTELLIGENT TECHNOLOGIES
IP Address Lifecycle

Network Structure and IP Address Plan
Create and Break up the IP space and distribute it to sub networks.

Design & Engineering

Reclamation
Collect addresses to reuse or remove IP space from the network.

Deallocation
Release addresses from decommissioned network blocks, interfaces & elements.

Aggregation
Calculate larger blocks to improve network efficiency.

Allocation
Assign blocks to network segments and addresses to network elements, including routers, switches & servers.

Instantiation & Distribution

DNS DHCP IPAM

Routers Switches Servers
Note: Undefined state is before addresses are entered into or after they are removed from the system.
Functional View

Company

Departments

Regions

Sites

VLANS
ASNs are used in Routing
Organization and Visibility

Control Information

- Address Type: {IPv4 | IPv6 | ASN}
- Aggregated: {Yes | No}
- Block Allocation: Utilization Fit {High | Low}
- Algorithm: Rated Fit {High | Low}
- Block Loan: Min. Block Size, Max Block Size
- Re-use Interval: Interval in days
- Suffix Label
- Complete Suffix
- DNS Zone
- DNS Update: {Yes | No}

Free Block List

Allocated Connection Block List

Network Container Structure

- Parent
- Children

Equipment List
Multiple Routing Domains

[Diagram showing a tree structure with NCS nodes and aggregate trees for ASN, IPv4, and IPv6.]
Instantiate & Distribute Space

Location 1

192.168.0.0/24
192.168.0.0/26

Location 2

192.168.64.0/26
192.168.64.0/26
Accurate Allocation

Manually or automatically select a free block

Create a network segment

connection

allocated interfaces

reserved - segment

reserved - broadcast
IP address Aggregation

Many small blocks

- 192.168.1.0/27
- 192.168.1.32/27
- 192.168.1.64/29
- 192.168.1.72/29
- 192.168.1.80/28
- 192.168.1.96/27
- 192.168.1.128/26

Represented by a few large blocks

- 192.168.1.0/25
- 192.168.1.128/26

Allows all Addresses Under Management

- Tightest Route Table Entries
Deallocation

- Delete interfaces
- Release a block
- Coalesce blocks
Packet and Protocol Monitoring

Multi-protocol and xFlow Monitoring

OptiviewXG

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

NCS

OptiviewXG
Utilization Fit

Free Block List

Block Request Size

High

Low

Free Block List

Selected Larger Free Block

High

Low

Free Block List

Allocated Connection Block

High

Low

Residue Free Block
Automatic Block Loan

Network Tree with Loan

First Level Block Loans

Deeper Block Loans
Efficient Planning & Layout

Layout Command allows both horizontal and vertical allocations.

Template Layout
Connections

- Models a network segment
- CIDR block
- Within a connection:
  - interfaces
  - reserved segment and broadcast
  - DHCP
  - restricted
  - available
Named Connection Blocks

Dual Stacked LAN Segment

Named Connection Block IPv4 /29
- connection
- allocated interfaces
- reserved - segment
- reserved - broadcast

Named Connection Block IPv6 /64 Subnet

IPv4 Address
IPv6 Address
IPv6 Link Local Address
Equipment

- Models network devices: routers, switches, servers, etc.
- Defined in an Anchor network
- Addresses are assigned to interfaces
- Virtual interfaces may be added for additional addresses

```
RTR_A
  E0  192.168.120.162 /29
  S0  192.168.120.168 /31
  S1  192.168.120.173 /30

RTR_B
  S0  192.168.120.169 /31
  E0  192.168.120.177 /29

RTR_C
  S0  192.168.120.174 /30
  E0  192.168.120.193 /29
```
What is Equipment?

Equipment Templates

Equipment

Attribute Information

Port 0
Port 1

Blade 0
Port 0
Port 1
Port 2
Virtual 0 IPv6
Virtual 1 IPv6
Virtual 2 IPv6
Virtual 3 IPv4

Blade 1
Port 0
Port 1
Port 2
Port 3

Allocated Connection Block List v6 and v4

Equipment and Connection Blocks distributed across the network
Address Map Detail

- **/26 block**
  - Reserved addresses
  - Allocated to interfaces
  - Restricted
  - DHCP
  - Available

- **Allocated /29 block**

- **Delegated /29 block**

- **Free /29 and /30 blocks**

- **Full /30 connection**
  - Reserved
  - Interfaces
Interactive Address Display

Plot Range: 3600:ab::/32
Tile: /40

Address Shown
- 3600:ab::/36
- 3600:ab:1000::/36
- 3600:ab:2000::/48
- 3600:ab:2001:200::/55
- 3600:ab:2001:400::/54
- 3600:ab:2001:800::/53
- 3600:ab:2001:1100::/56
- 3600:ab:2001:1200::/55
- 3600:ab:2001:1400::/54
- 3600:ab:2001:1800::/53
- 3600:ab:2001:2200::/56
- 3600:ab:2001:2500::/56
- 3600:ab:2001:2600::/55
- 3600:ab:2001:2800::/53
- 3600:ab:2001:3000::/52
- 3600:ab:2001:4000::/50
- 3600:ab:2001:8000::/49
- 3600:ab:2002::/47
- 3600:ab:2004::/46
- 3600:ab:2008::/45
- 3600:ab:2010::/44
- 3600:ab:2020::/44
Web Service Based System
Automated Interfaces

Network Interconnections and Address blocks both Free and Allocated / Assigned

Library of Complete Plans and Designs
Xml Format
Library of Sub-Plans and Designs
Xls Format

Bi-directional Interface

SOAP/XML API

Firewalls
IPS/IDS/NAC
Network Provisioning, Management, Operations And Cyber Security
Virtualized DNS
Multiple Simultaneous Databases

IPALM (IPal)

Database Management System

Database 1

Contents of Database 1

Database 2

Contents of Database 4

Database 3

Database 4
IPv4 to IPv6 Transition

- Architect network tree
- Load existing v4 address blocks and devices
- Optimize & enhance network structure
- Add IPv6 blocks and distribute
- Enable dual stack on Equipment Interfaces
- Add Tunnels as required
Address Plan Decisions

- Utilizing Current IPv4 Network Structure
  - What part of the network will be transitioned and when

- What IPv6 Transition techniques
  - Dual Stacking
  - Tunneling IPv6 over IPv4 then IPv4 over IPv6
  - Some legacy IPv4 systems will remain
  - In the future a pure IPv6 network
Inputs to the Address Plan

- How many locations and how are they interconnected
- What is the hierarchy? Functional, Geographic, Political or combination
- At each location how many
  - Network Devices – Routers, Switches, Security, Transmission, etc…
  - End User Devices – PCs, Laptops, Printers, PDAs, Cellphones, etc…
  - LANs, VLANs, Point to Point Circuits
Address Plan Process

- Create network architecture
- Define master address block
- Distribute address space
  - Break up Master Block
  - Multiple levels
- Allocate blocks and connections
- Initial Address Plan is complete
- Refine Network Model as needed
Address Plan Engine

Network Architecture & Address Structure Base Plan Repository
*.xml or *.xls

Sub-Network Plan Repository
*.xls

Obtain Customer Requirements

Select a Network Architecture & Address Structure Base Plan
*.xml

Develop New Base Plan

Success

Add Sub-Network Elements
*.xls

Develop New Sub-Network Elements

Success

Configure for Customer

Deliver *.xml or *.xls to Customer

Maintain database for Customer On-line

Continue to Maintain Customer database
QUESTIONS?