

**Rocky Mountain IPv6 Task Force** 

2012 North American IPv6 Summit



### 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



# 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 address 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



Data Center Consolidation and Virtualization Customer Connection and Experience

Mobile Devices Lack of Address Space



### It started with Howard in '99

Macmillan Network Architecture and Development Series

M

### DESIGNING ADDRESSING ARCHITECTURES

for Routing and Switching

Howml C. Berkowitz



### 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

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

## 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
  - 4,294,967,296

/96



## 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**



\*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 Technologies**

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



### **INTELLIGENT TECHNOLOGIES**





### **IP Address State Diagram**



### **Physical Network**





### **Functional View**





### ASNs are used in Routing



### **Organization and Visibility**













### **Accurate Allocation**

#### Manually or automatically select a free block

#### Create a network segment





### **IP address Aggregation**

### Many small blocks

## Represented by a few large blocks



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





### **Utilization Fit**

Free Block List

<del></del>

Low

High

Low

High

Free Block List

Free Block List





Selected Larger Free Block



Residue Free Block







### **Rated Fit**





### Automatic Block Loan







## Connections

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



## Named Connection Blocks



#### Named Connection Block IPv4 /29



#### Named Connection Block IPv6 /64 Subnet



2001.0	C: 4382: 7E4 :: /	64	
2001:B	C1430217E4:F	***:****:****	FF
299118	C1438217E4 F	FFF FFFF:FFF;FF	FE
2001: B	(1430217E4:F	FFF:FFFF:FFF:FF	FD
2001:0	C:4382:7E4:F	FFF:FFFF:FFF;FF	ŧς
-		:	
			-
5001:0	14302170410	000:0000:0000:00	<u>94</u>
2001:8	C:4302:7E4:0	000:0000:0000:000	63
2001:9	C14302:7E4:0	000:0000:0000:00	62
2001-0	C:4302:7E4:0	001 0000 0000 000	01



### 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?



## **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

		Zoom Out In Up Down		
		Plot Range: 3600:ab::/32		
		Address Shown		
		<u>3600:ab:1000::/36</u>		
		<u>3600:ab:2000::/48</u> <u>3600:ab:2001:200::/55</u>		
		<u>3600:ab:2001:400::/54</u> <u>3600:ab:2001:800::/53</u>		
		3600:ab:2001:1100::/56 3600:ab:2001:1200::/55		
		3600:ab:2001:1400::/54 3600:ab:2001:1800::/53		
MobileNetwork	Infrastructure	3600:ab:2001:2200::/56 3600:ab:2001:2500::/56		
	NDC001	3600:ab:2001:2600::/55 3600:ab:2001:2800::/53		
CE01-02	COR01-02	3600:ab:2001:3000::/52 3600:ab:2001:4000::/50		
PE01-02	SupportZone	3600:ab:2001:8000::/49 3600:ab:2002::/47		
	NDC003	3600:ab:2004::/46 3600:ab:2008::/45		
OAMReserved		3600:ab:2010::/44 3600:ab:2020::/44		





### Virtualized DNS







## 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





### **QUESTIONS?**