IP Address Lifecycle Management enabling v6 Transition & Cyber Security

DREN Networking and Security Conference 2011

Internet Associates, LLC
August 15-18, 2011
Briefing Agenda

- Introduction
- Mission
- Cyber Security
- IP Address Lifecycle Management (IPALM) Technology
- IP Address Planning & v6 Transition
- Questions
Introduction

- **IP Address Lifecycle Management**
  - Technology Foundations and its application to:
    - **Cyber Security**
    - **IP Address Planning and Design**
    - **Transition from IPv4 to hybrid v4/v6 networks**
Mission

- **Mission has not changed:**
  - Get the Accurate Information in the right form
    - to the right Decision Maker at the right location and
      at the right time inside the decision and execution cycle of the **Cyber** adversary
  - **Execution has changed radically**
    - From push to pull at the squad or individual Warfighter level
    - Technology from Telegraph, Telephone and Radio to Packet
Some Relevant 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
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

Interactive Analysis
- Packet Capture
- Protocol Analysis
- Deep Packet Inspection

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

Security Policy Generation & Management
- ACLs, SAML
- Event Correlation

Authentication & Policy Enforcement
- IPAM DNS DHCP

Network Traffic Generation & Analysis

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

IP & ASN Address, Interface & Network Topology

IP Address, Scope & DNS Resource Record With DNSSEC

IP Address, ACL & SAML

IP Address, Interface & Network Topology

© 2010 Internet Associates, LLC All Rights Reserved
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
Additional Requirements

- Maintain all Addresses under Management
  - Complete, Accurate Support for IPv4, IPv6 and ASNs Network Addresses
  - 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
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
## Number of v6 Addresses

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

- 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
IP Address Lifecycle

- **Network Structure and IP Address Plan**
- **Design & Engineering**
  - Collect addresses to reuse or remove IP space from the network.
- **Instantiation & Distribution**
  - Create and break up the IP space and distribute it to sub networks.
- **Allocation**
  - Assign blocks to network segments and addresses to network elements, including routers, switches & servers.
- **Aggregation**
  - Calculate larger blocks to improve network efficiency.
- **Deallocation**
  - Release addresses from decommissioned network blocks, interfaces & elements.
IP Address State Diagram

UNDEFINED
- define
- delete

FREE
- allocate
- deallocate
- request reclaim
- dispose
- create connection

CONNECTION
- patch address
- unpatch
- cancel reclaim
- request reclaim

CONNECTION (reclaim pending)
- patch address
- unpatch

RECLAIM
- deallocate
- complete reclaim to delete

ALLOCATED
- request reclaim
- cancel reclaim
- deallocate
- request reclaim

ALLOCATED (reclaim pending)
Simple Network Example

Hierarchical Networks

1. Branch
   - Accounting
   - Engineering
   - Lab
   - Headquarters
   - Sales
      - Sales East
      - Sales West
The Aggregate Tree

- **Branch**
  - **Accounting**
  - **Engineering**
    - **Lab**
  - **Headquarters**
  - **Sales**
    - **Sales East**
    - **Sales West**

- **A group of Networks (containers) that:**
  - Share one instance of address space either IPv4, IPv6 or ASN that defines a routing domain
  - Unique & Valid CIDR Addresses are maintained

- **Network Containers:**
  - Anchor Address, Connection Blocks, Equipment & Interfaces
  - Define Control Parameters including:
    - Address Allocation Methods & Order
    - Automatic Distribution of Address Blocks
    - DNS Suffix & FQDN, Zone & Update
    - IP Address block reuse interval
Network Tree

- Network Tree contain Aggregate Tree(s) of one or more types ASN, IPv4 or IPv6
- Duplicate Space is correctly managed
Instantiate & Distribute Space

Diagram showing network topology with IP addresses 192.168.0.0/26, 192.168.64.0/26, and 192.216.6.0/8.
Network Address Map Example

Plot Range: 192.168.120.0/24  Tile: /32
Zoom Base: 192.168.120.0

Address Shown
- 192.168.120.0/26
- 192.168.120.64/28
- 192.168.120.80/28
- 192.168.120.96/28
- 192.168.120.112/28
- 192.168.120.128/28
- 192.168.120.144/28
- 192.168.120.160/28
- 192.168.120.192/28

Address not Shown

- Interface
- ConnAvail
- Reserve
- Delegate
- DeAlloc
- Allocate
- Reclaim
- Free
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

Represented by a few large 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

192.168.1.0/25
192.168.1.128/26

Allows all Addresses Under Management

- Tightest Route Table Entries
De-allocation

Delete interfaces

Release a block

Coalesce blocks
Web Service Based System
IPv4, IPv6 & ASN Support

- ASN Based to support large Networks
- Multiple IPv4 & v6 Space
  - Operational, Planning or different organizations
- Multiple Private (RFC1918) or FEC0:: Space
IPALM Elements

- Validate, Organize & Control accurate IP addresses & associated information
- Equipment associates IP addresses with physical & virtual interfaces
- Connections – organize subnetworks
- Multiple Allocation & Assignment Methods for IPv4 & IPv6
- Automatic DNS Record Generation & RR Editor
- Custom Fields (multiple data types)
- Address, Network, Router & Switch Audit
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
Industry Standard Interfaces

- Network Management & OSS Interfaces
- Bi-directional XLS & XML with SOAP/XML API for Real Time Integration
- Multiple DNS/DHCP/IPAM/IDS/IPS Vendor Integration
DNS/DHCP/IPAM Server Interface
Distributed Virtualized DNS
IPALM MDD Architecture
Independent Enclaves

Enclave TS-SCI_1
- IPALM
- DNS/DHCP

Enclave TS-SCI_2
- IPALM
- DNS/DHCP

Enclave TS-SCI_N
- IPALM
- DNS/DHCP

Enclave S
- IPALM
- DNS/DHCP

Enclave SBU
- IPALM
- DNS/DHCP

Offensive & External
Aggressor Enclave
- IPALM
- DNS/DHCP
Distributed Sensor System
IPALM Netflow Integration
Network Discovery Issues
Defensive Cyber Operations

- Simultaneous dynamic offensive / defensive operations
- Increased Optemp with “Hackers”
- Use IPALM to renumber space as required
- Dynamic Layer 1 / 2 Defenses with rapid flow through provisioning
IP Address Planning & v6 Transition
Address Planning Methodology

1. Obtain Customer Requirements
2. Select a Network Architecture & Address Structure Base Plan Repository *.xml or *.xls
3. Add Sub-Network Elements Repository *.xls
4. Configure for Customer
5. Deliver *.xml or *.xls to Customer
6. Maintain database for Customer On-line
7. Continue to Maintain Customer database
8. Develop New Base Plan
9. Develop New Sub-Network Elements
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

- Which IPv6 Address Assignment & Transition techniques
  - Dual Stacking
  - Tunneling IPv6 over IPv4 then IPv4 over IPv6
  - SLAAC, Statefull, DHCPv6, etc.
Address Plan Inputs

- 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 in IPALM

- 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
Physical Network

Backbone

Aggregation Network

Network

Sub Network
Functional View

Department

Agencies

Regions

Sites

VLANS
Network Model in IPALM

- **Network Tree**
  - Overlay Functional Network on Physical Network
  - Maintain Unique IPv4 and IPv6 blocks and multiple Routing Domains

- **Connection Blocks**
  - Point to Point, VPN, LAN and VLAN circuits

- **Equipment**
  - Network Devices and their Interfaces
Conclusion

- Uncoordinated parochial control of addresses does not work in an integrated geographically dispersed IP network.
- Point system gaps will be exploited by persistent, focused threats.
Questions ?