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

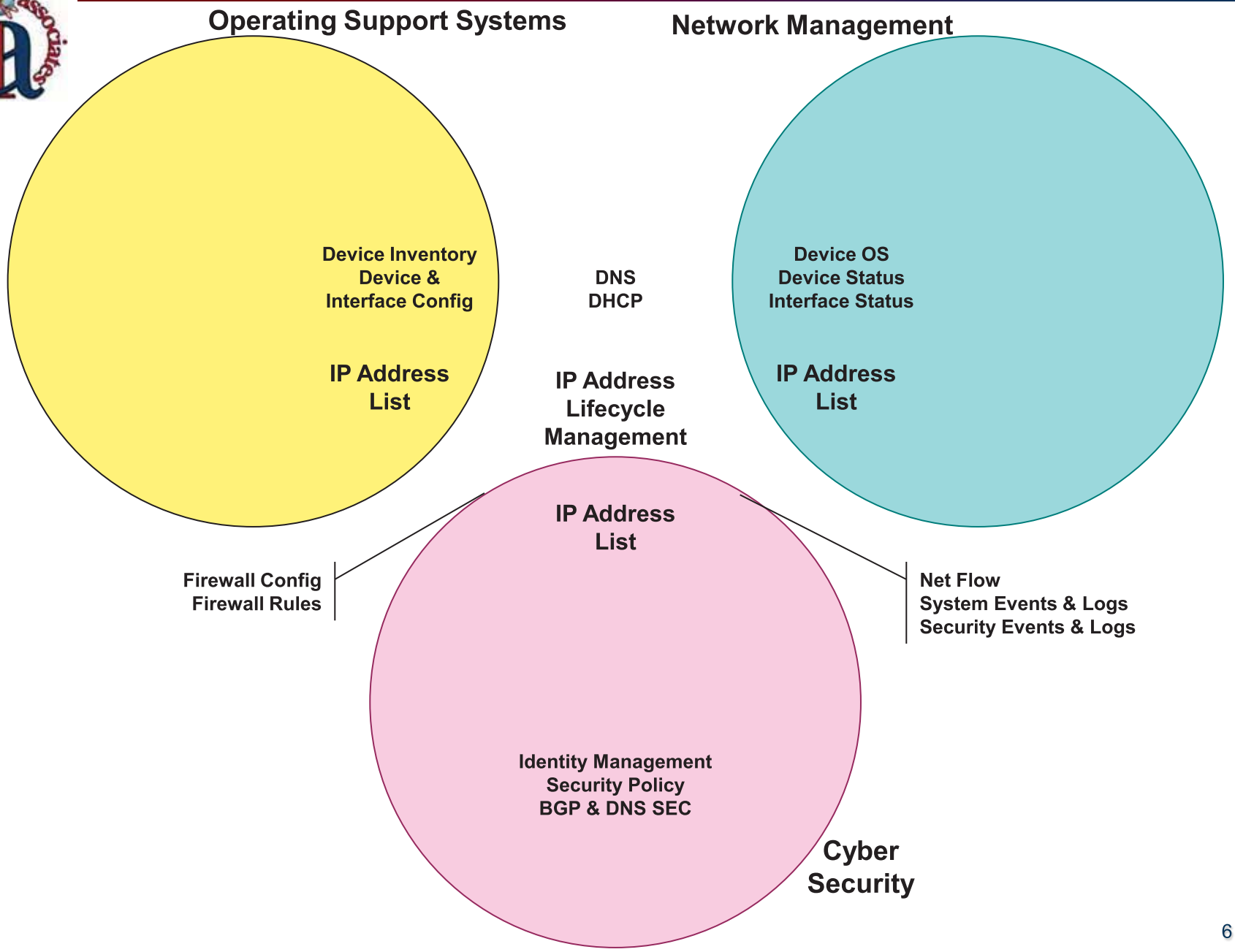
- IP Address Lifecycle Management
  - Technology Foundations and its application to:
    - Cyber Security
    - IP Address Planning and Design
    - Transition from IPv4 to hybrid v4/v6 networks

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


Operating Support Systems
Network Management
Device Inventory
Device &
Interface Config
IP Address
List
DNS
DHCP
Device OS
Device Status
Interface Status
IP Address
List
IP Address
Lifecycle
Management
IP Address
List
Firewall Config
Firewall Rules
Net Flow
System Events & Logs
Security Events & Logs
Identity Management
Security Policy
BGP & DNS SEC
Cyber
Security

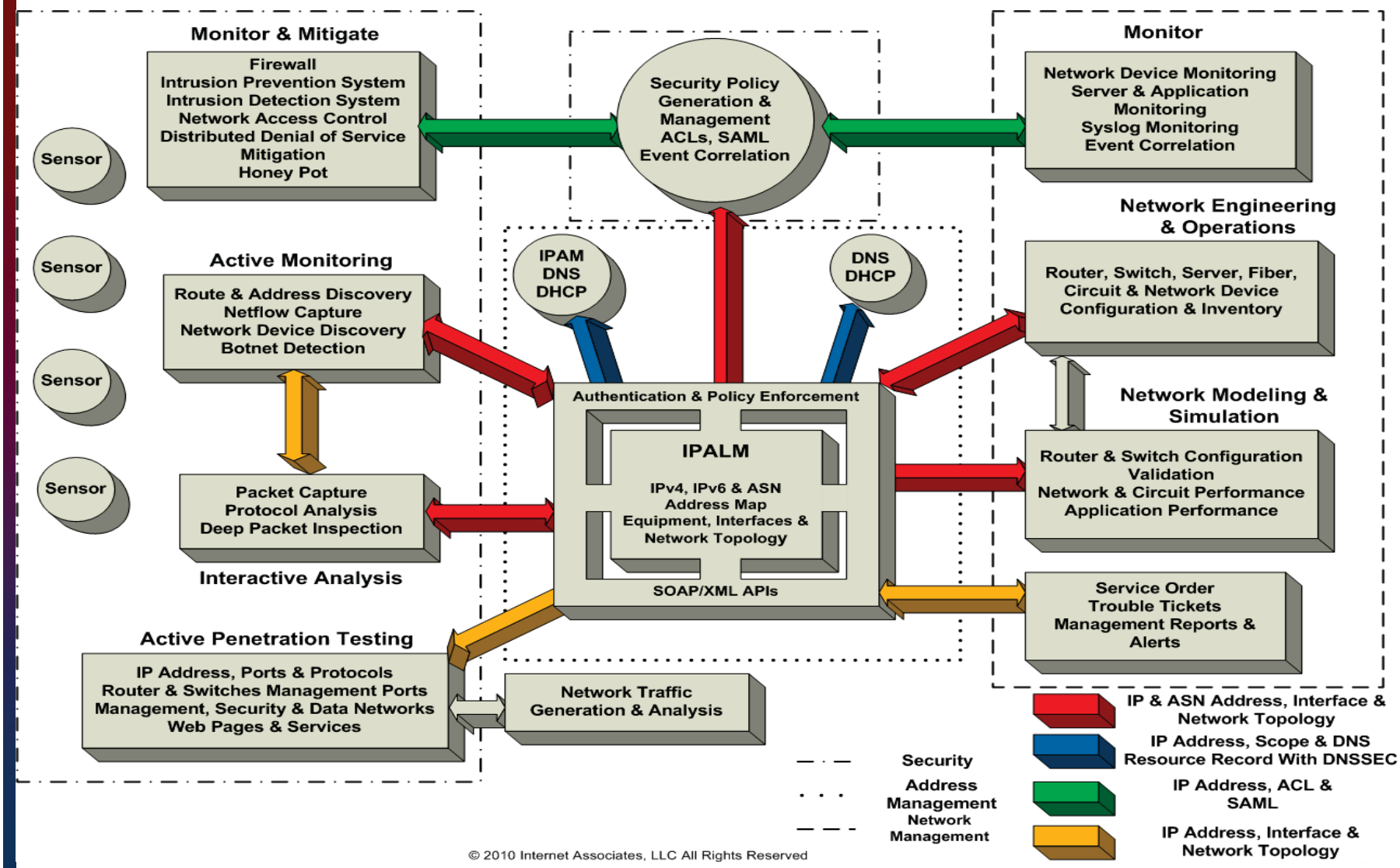
20 Critical Controls – Consensus Audit Guidelines

- 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



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

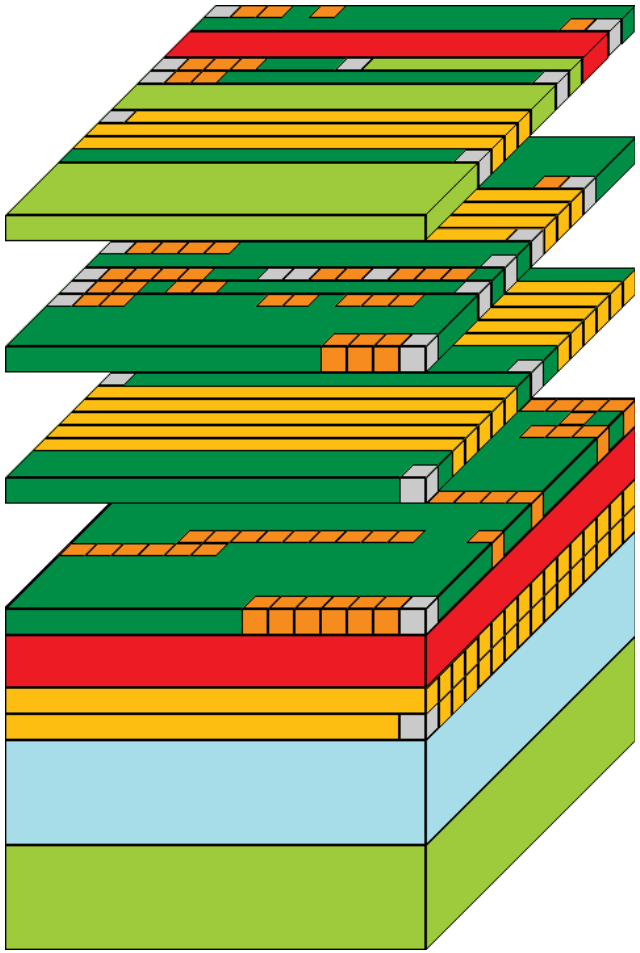
Detailed IPALM Methods

- 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

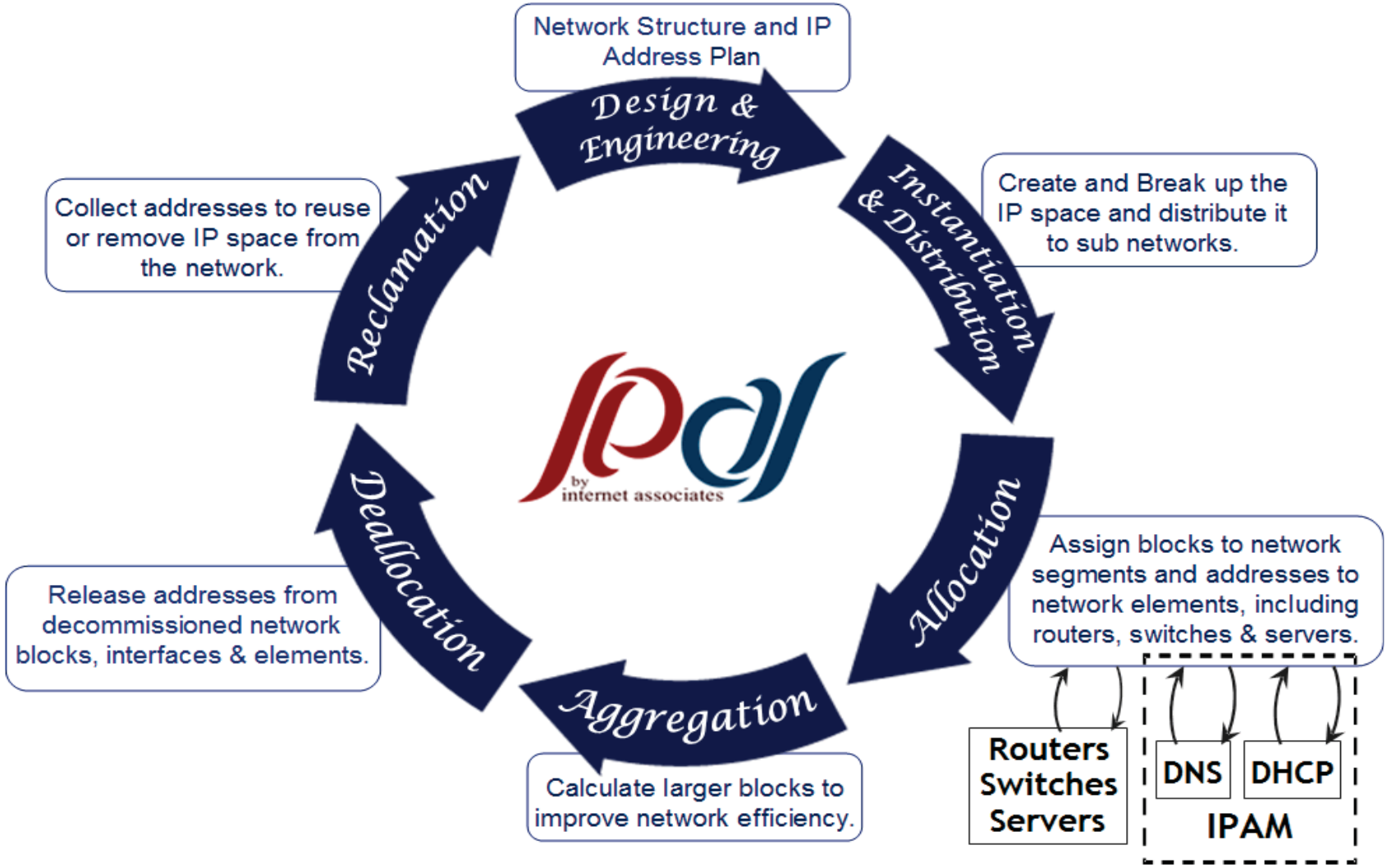
- /0 340,282,366,920,938,463,463,374,607,431,768,211,456
- /16 519,229,685,853,482,762,853,049,632,922,010
- /24 20,282,409,603,651,670,423,947,251,286,016
- /32 79,228,162,514,264,337,593,543,950,336
- /48 1,208,925,819,614,629,174,706,176
- /64 18,446,744,073,709,551,616
- /96 4,294,967,296

IPALM Foundation Concepts

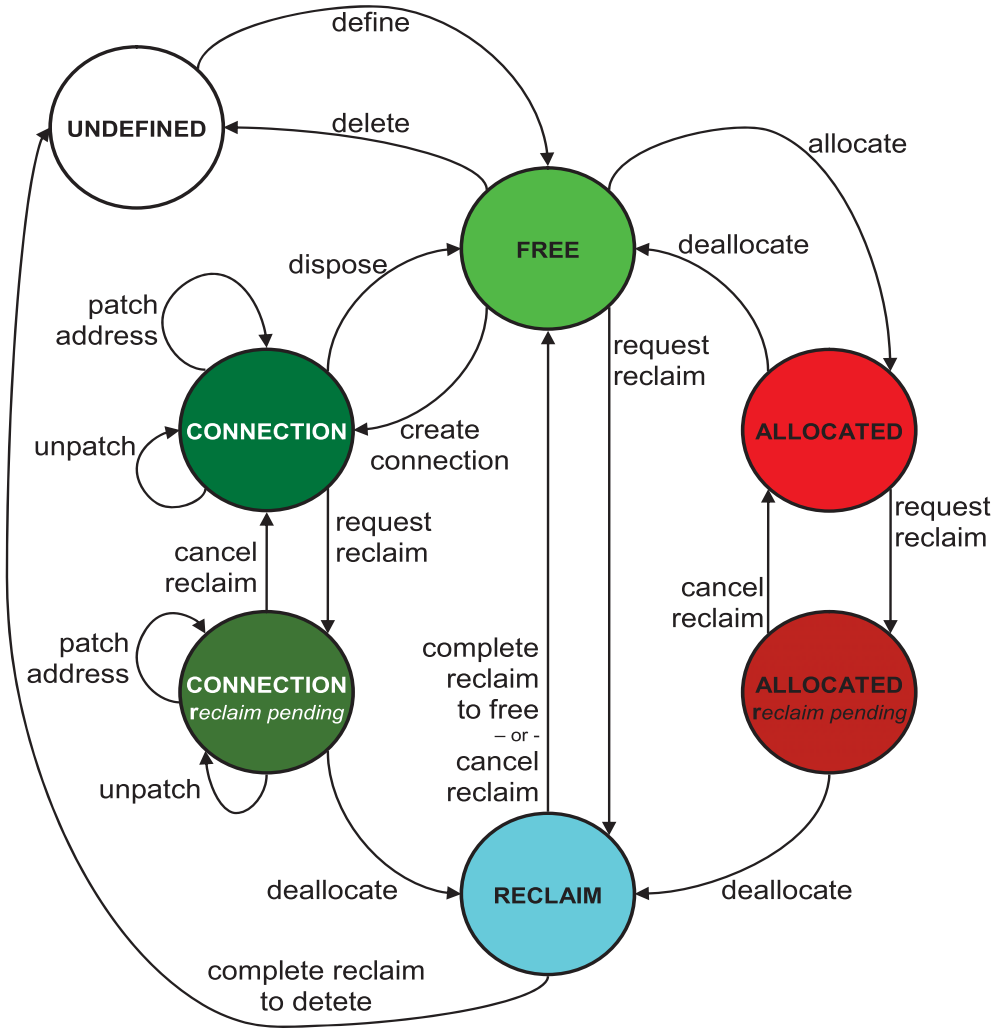


- IP Address Space is a binary data structure containing engineered IP address blocks of any size
  - Manage any size of block from /0 to /128 IPv6 & /0 to /32 IPv4
  - Split, Combine, Move, Coalesce, & Loan Blocks
  - All IP Addresses in the block are under Management
  - Multiple Unique Routing Domains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

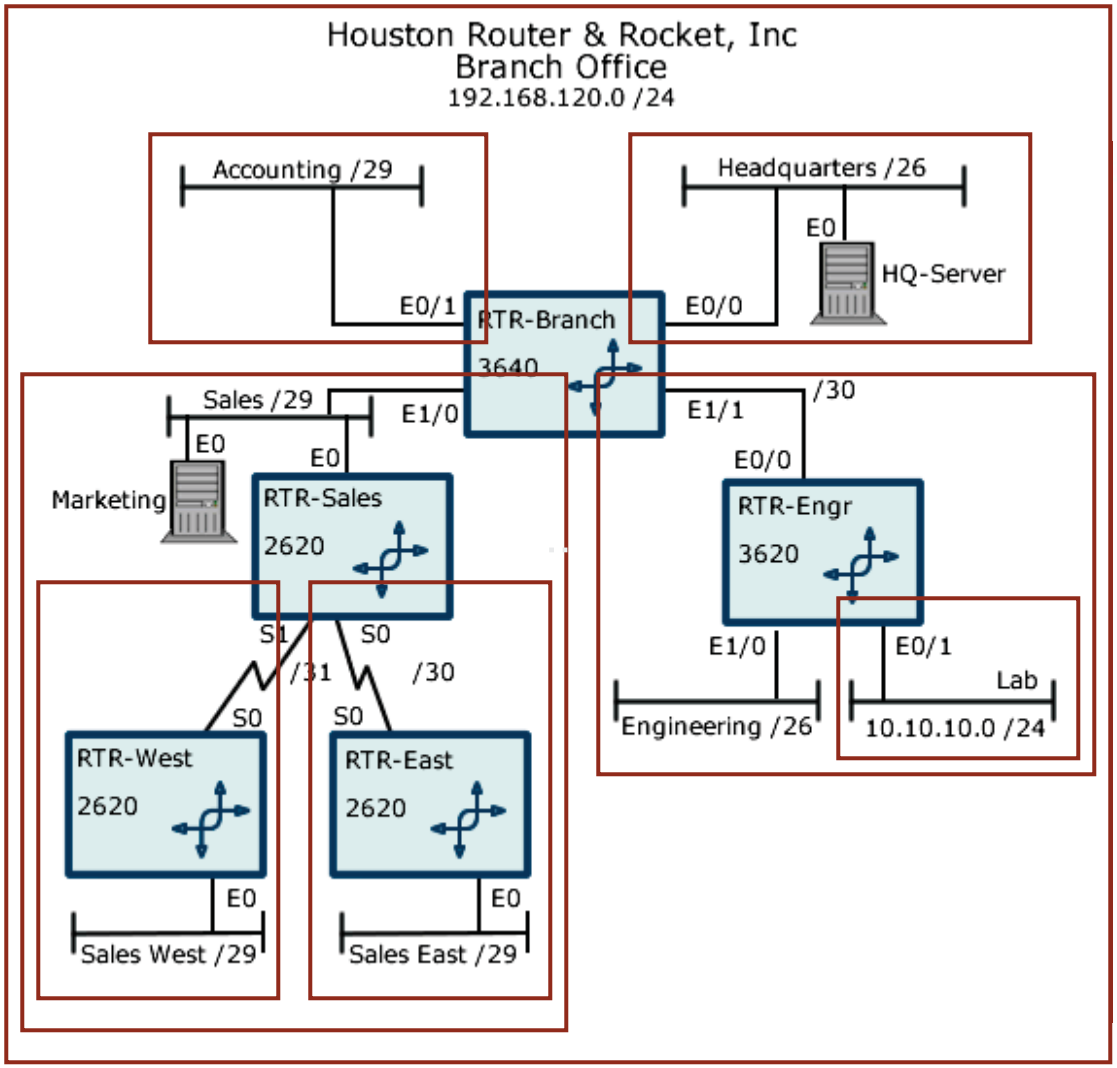
IP Address Lifecycle



IP Address State Diagram



Simple Network Example



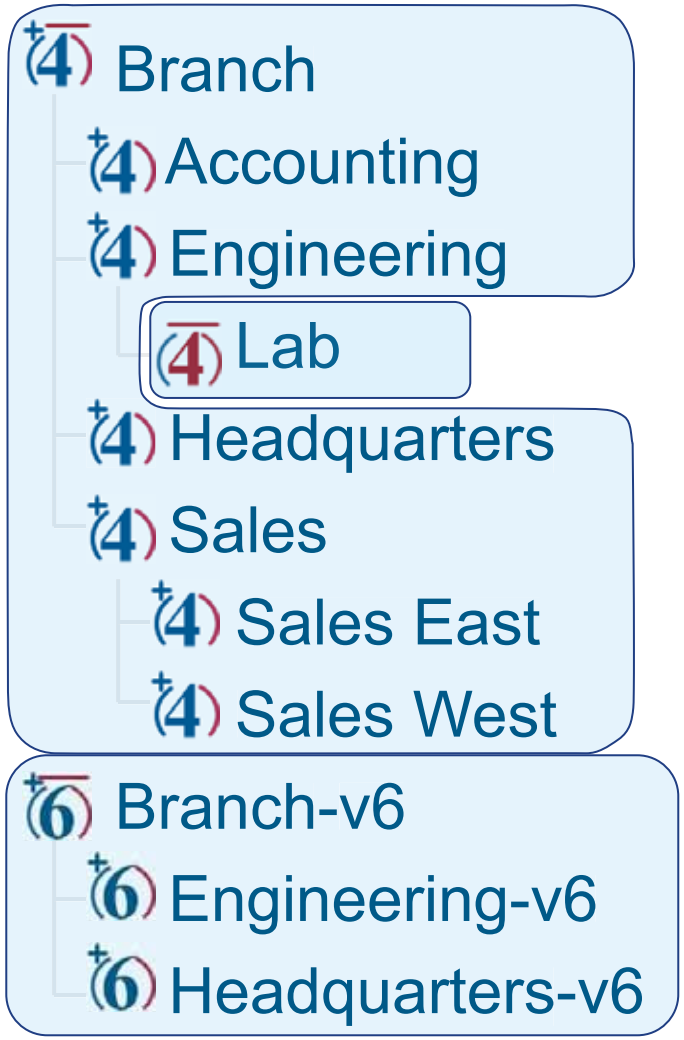
Hierarchical Networks

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

The Aggregate Tree

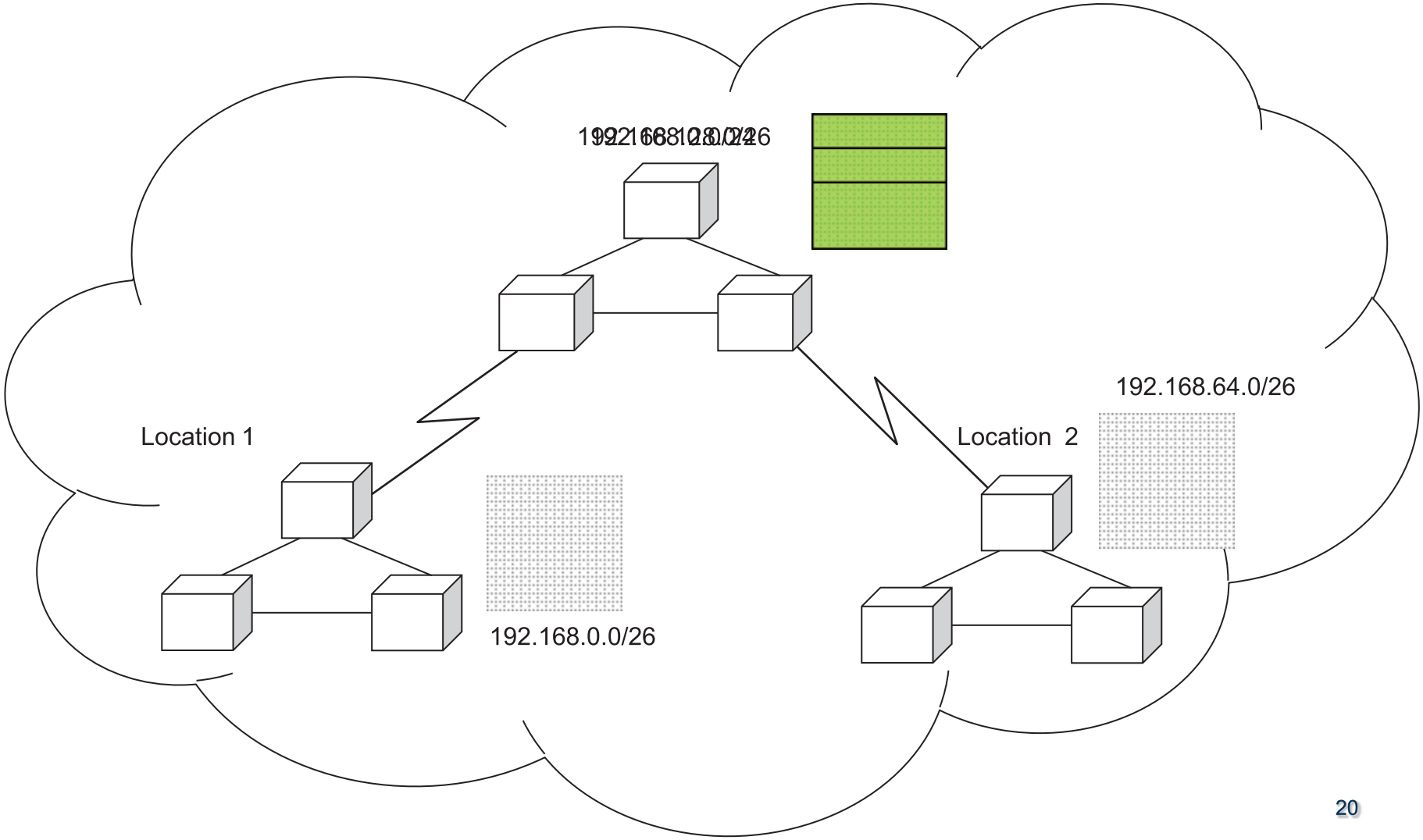
- A group of Networks (containers) that:
  - Share one instance of address space either IPv4, IPv6 or ASN that defines a routing domain
  - Unique & Valid CIDR Addresses are maintained
- Network Containers:
  - Anchor Address, Connection Blocks, Equipment & Interfaces
  - Define Control Parameters including:
    - Address Allocation Methods & Order
    - Automatic Distribution of Address Blocks
    - DNS Suffix & FQDN, Zone & Update
    - IP Address block reuse interval

Network Tree

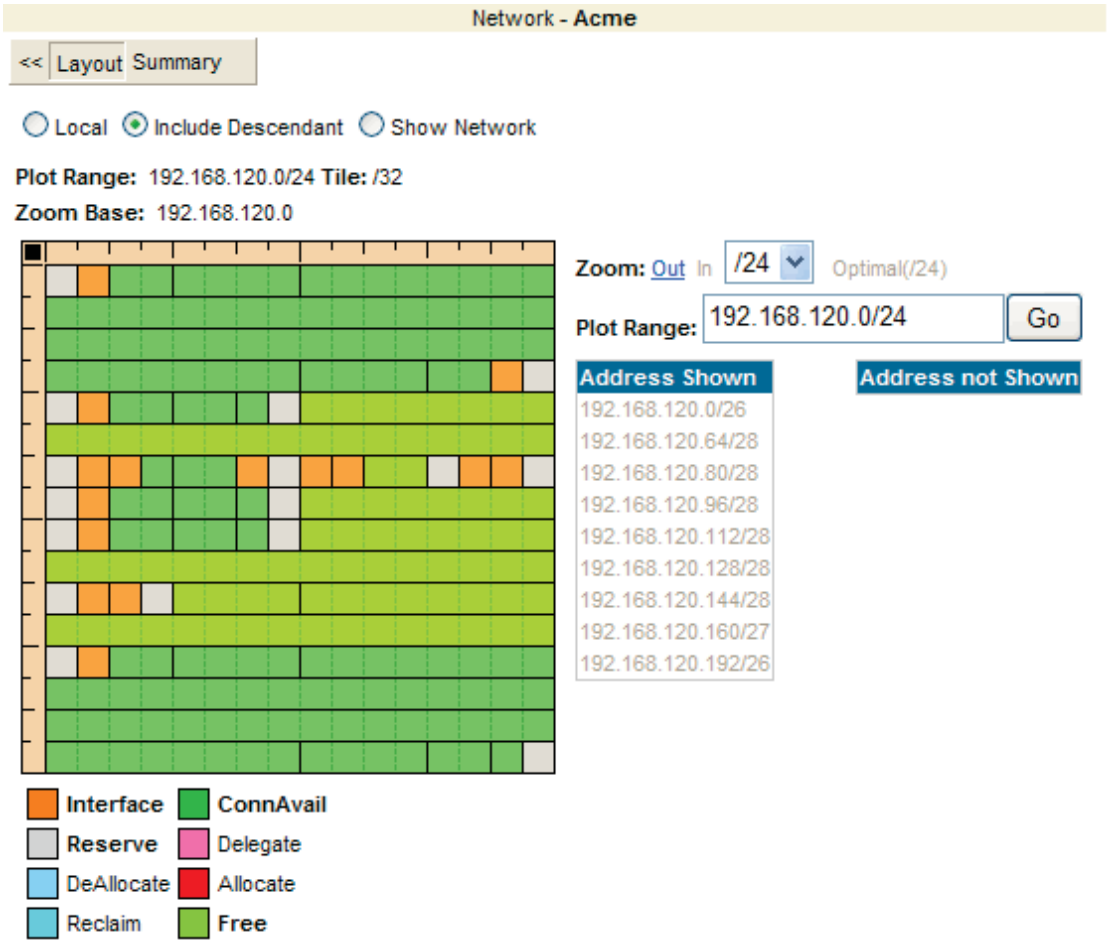


- Network Tree contain Aggregate Tree(s) of one or more types ASN, IPv4 or IPv6
- Duplicate Space is correctly managed

Instantiate & Distribute Space



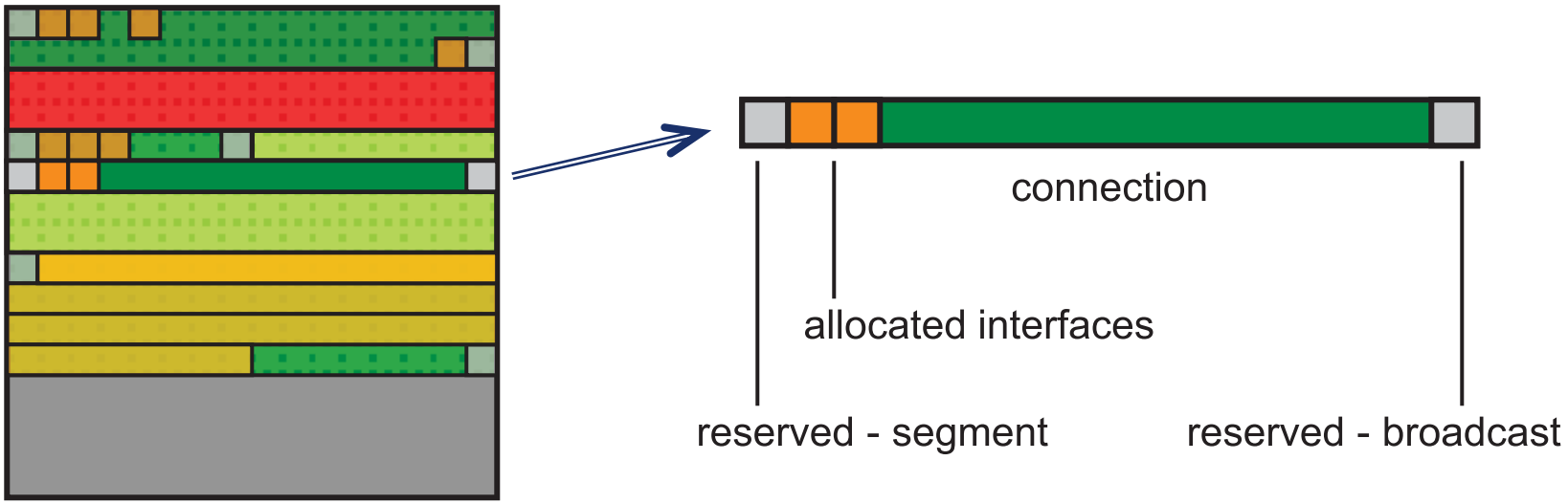
Network Address Map Example



Accurate Allocation

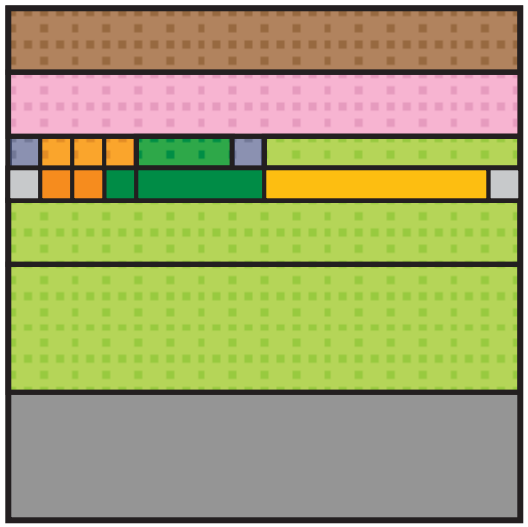
Manually or automatically select a free block

Create a network segment



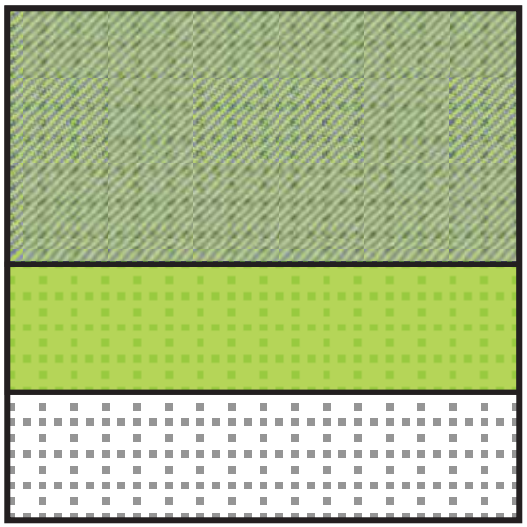
IP address Aggregation

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

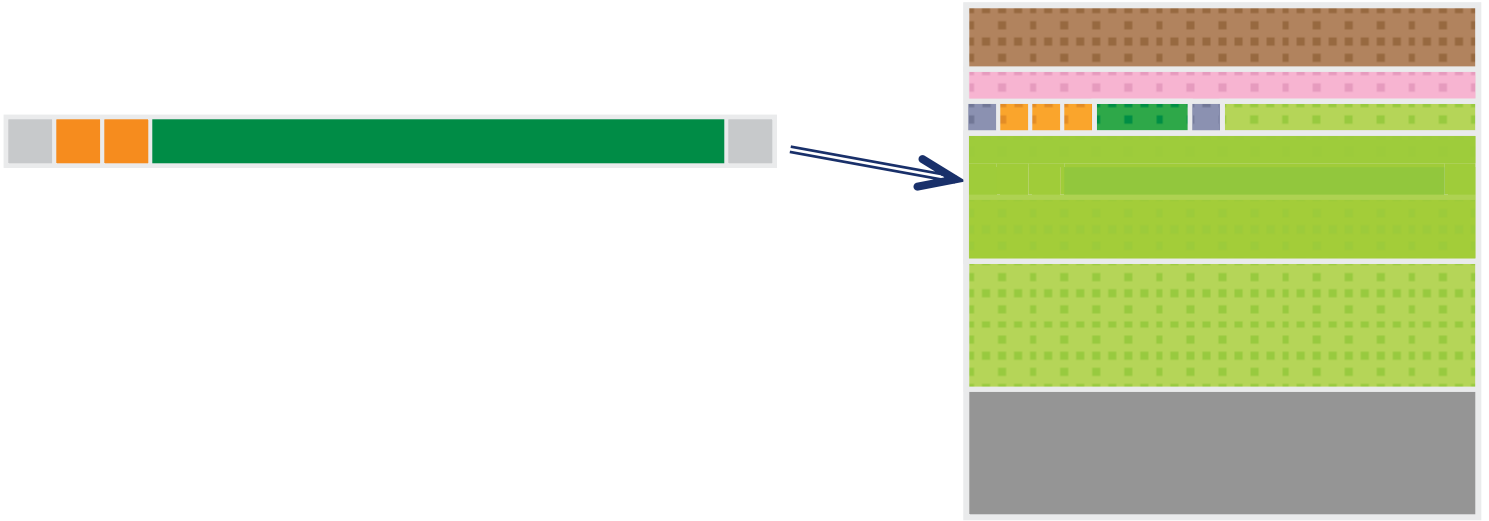
Allows all Addresses Under Management

- Tightest Route Table Entries

De-allocation

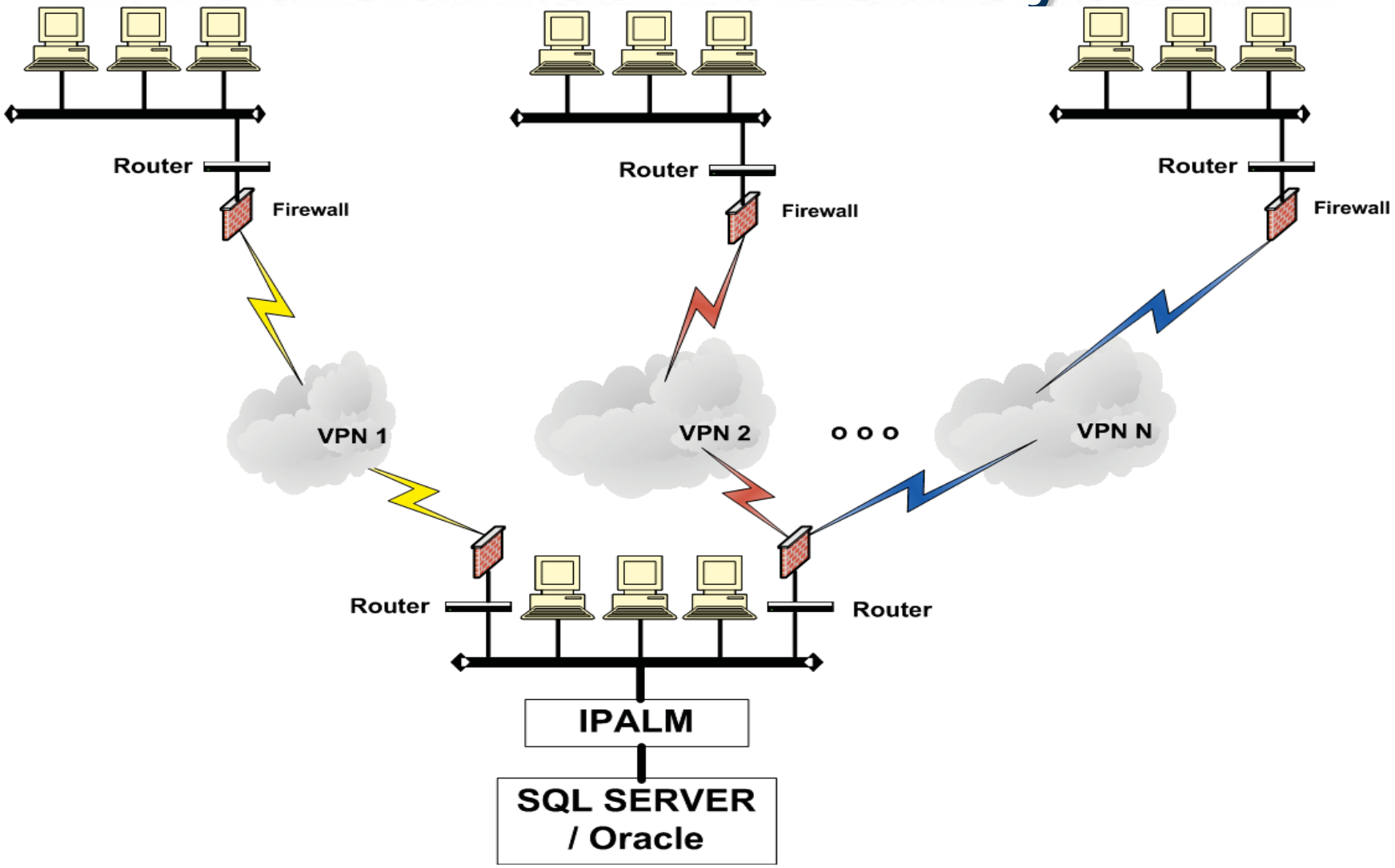
Delete interfaces

Release a block

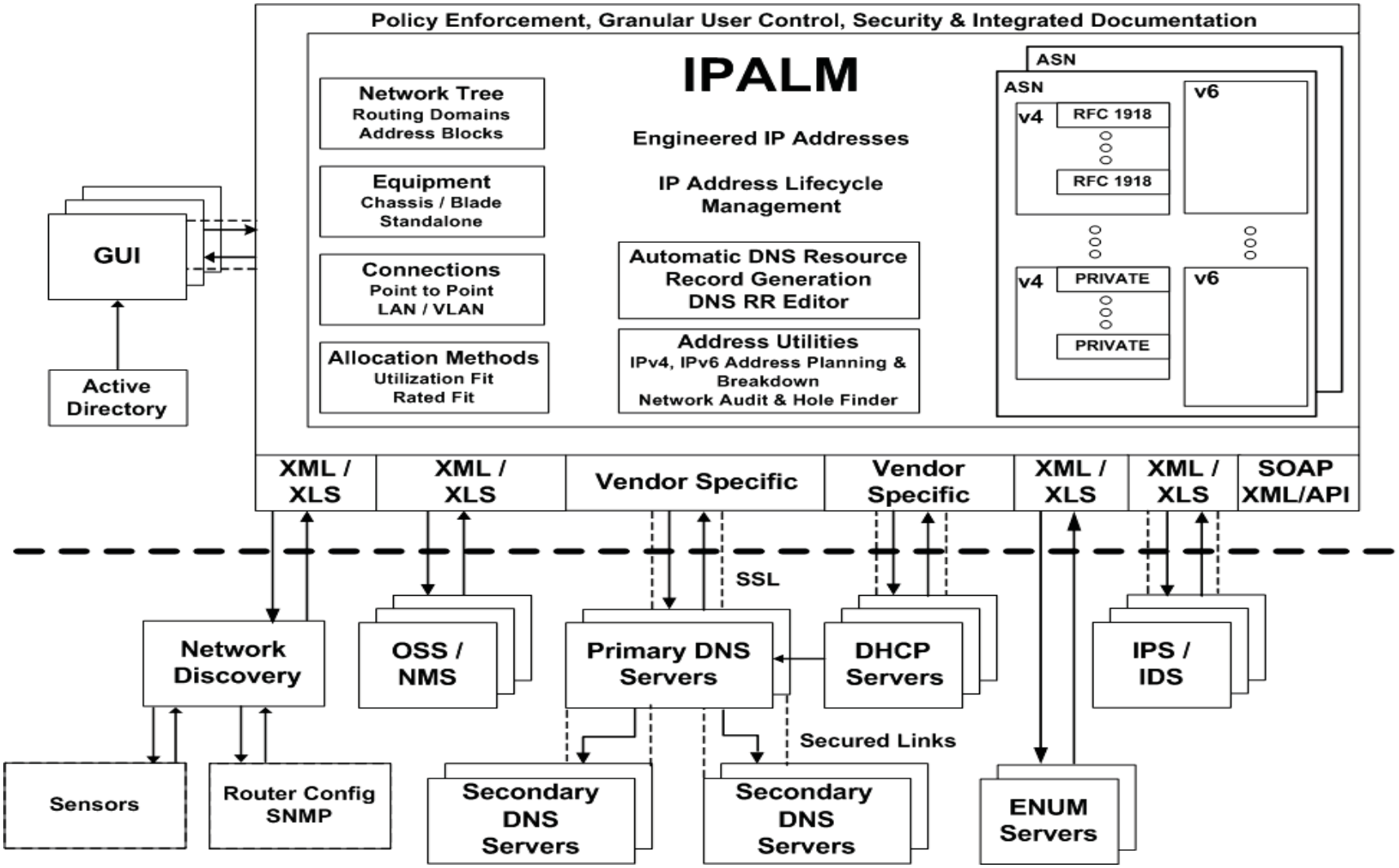


Coalesce blocks

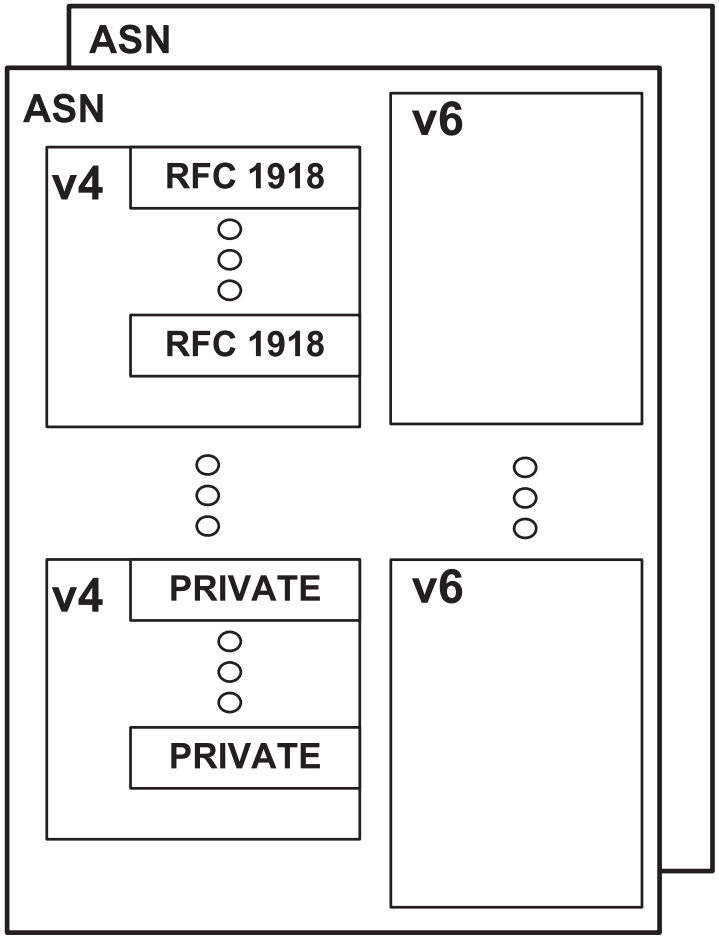
Web Service Based System



IPALM Architecture

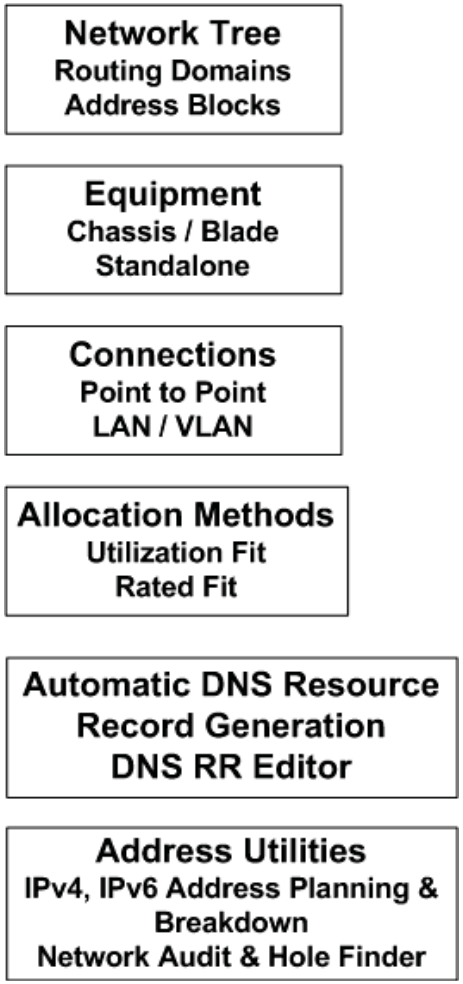


IPv4, IPv6 & ASN Support



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

IPALM Elements



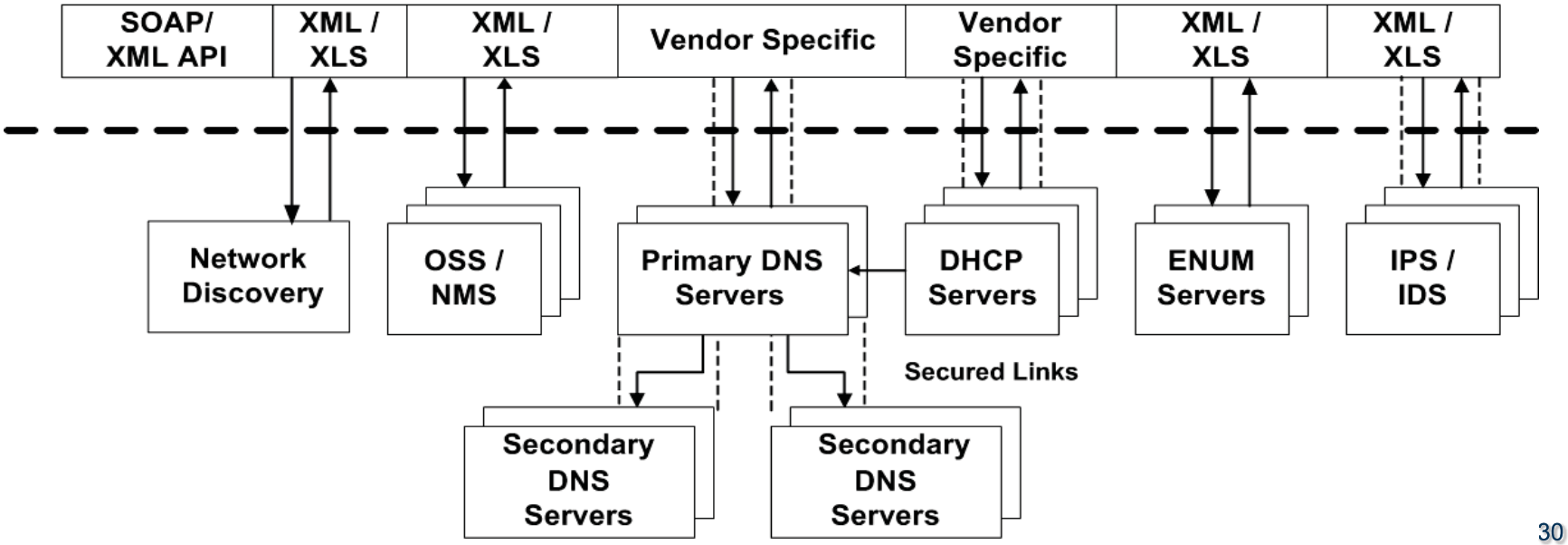
- Validate, Organize & Control accurate IP addresses & associated information
- Equipment associates IP addresses with physical & virtual interfaces
- Connections – organize subnetworks
- Multiple Allocation & Assignment Methods for IPv4 & IPv6
- Automatic DNS Record Generation & RR Editor
- Custom Fields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

IPv6 Support

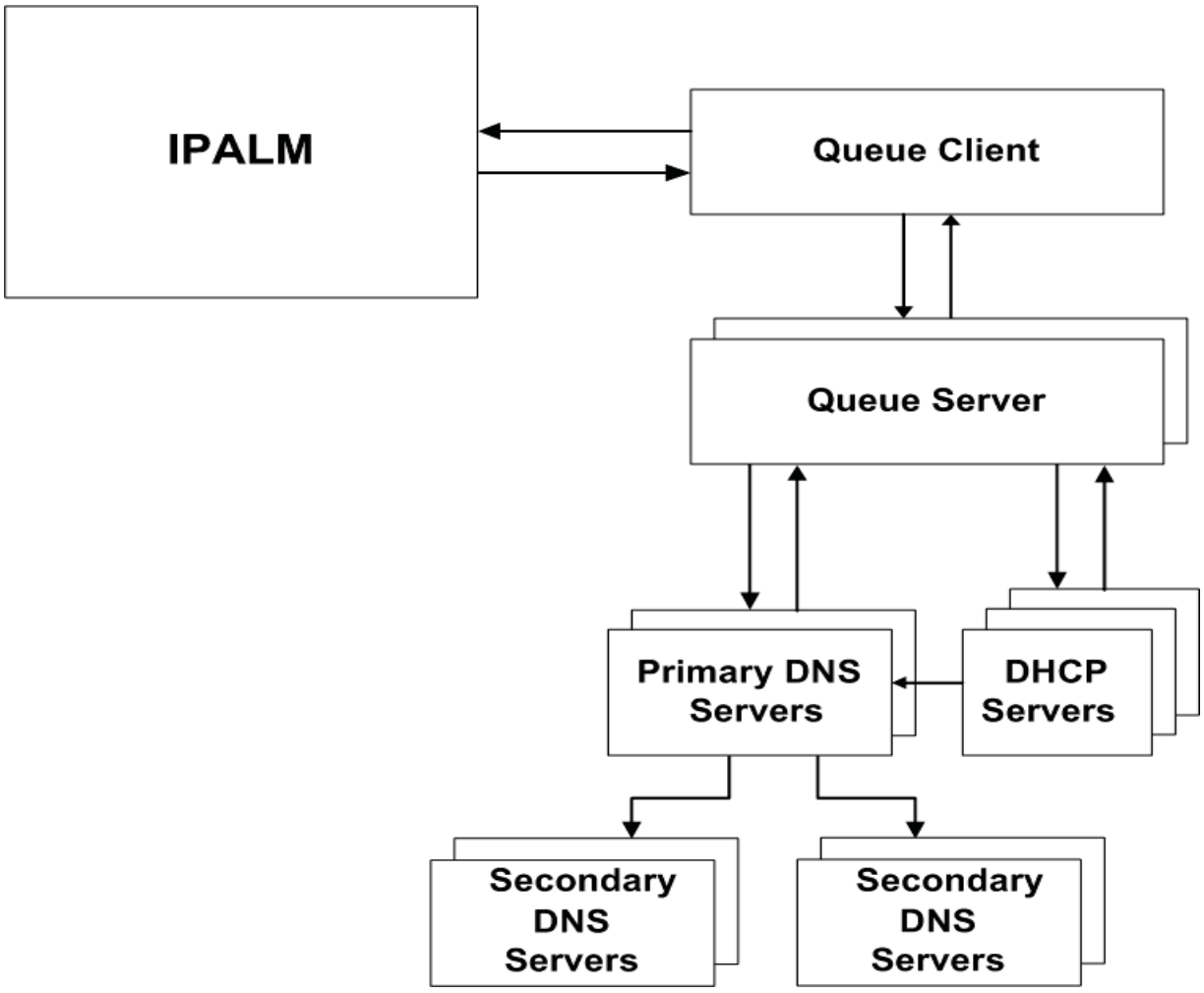
- Address Planning & Design
- Dual Stack – Physical and virtual interfaces support multiple IPv4 and IPv6 addresses
- Interfaces addresses
  - /64 EUI-64 or Random, user-defined
- IPv4 – IPv6 Transition

Industry Standard Interfaces

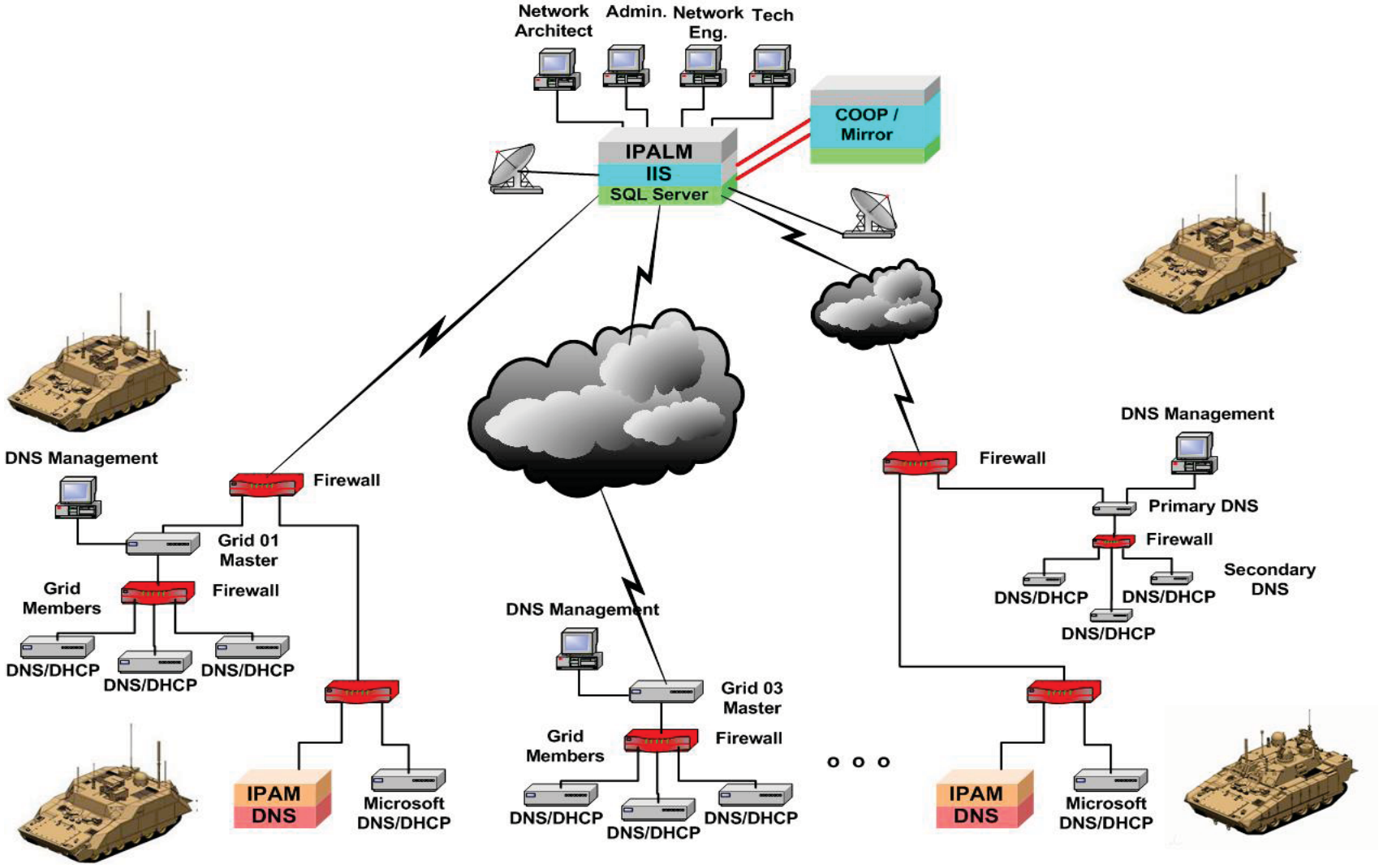
- Network Management & OSS Interfaces
- Bi-directional XLS & XML with SOAP/XML API for Real Time Integration
- Multiple DNS/DHCP/IPAM/IDS/IPS Vendor Integration



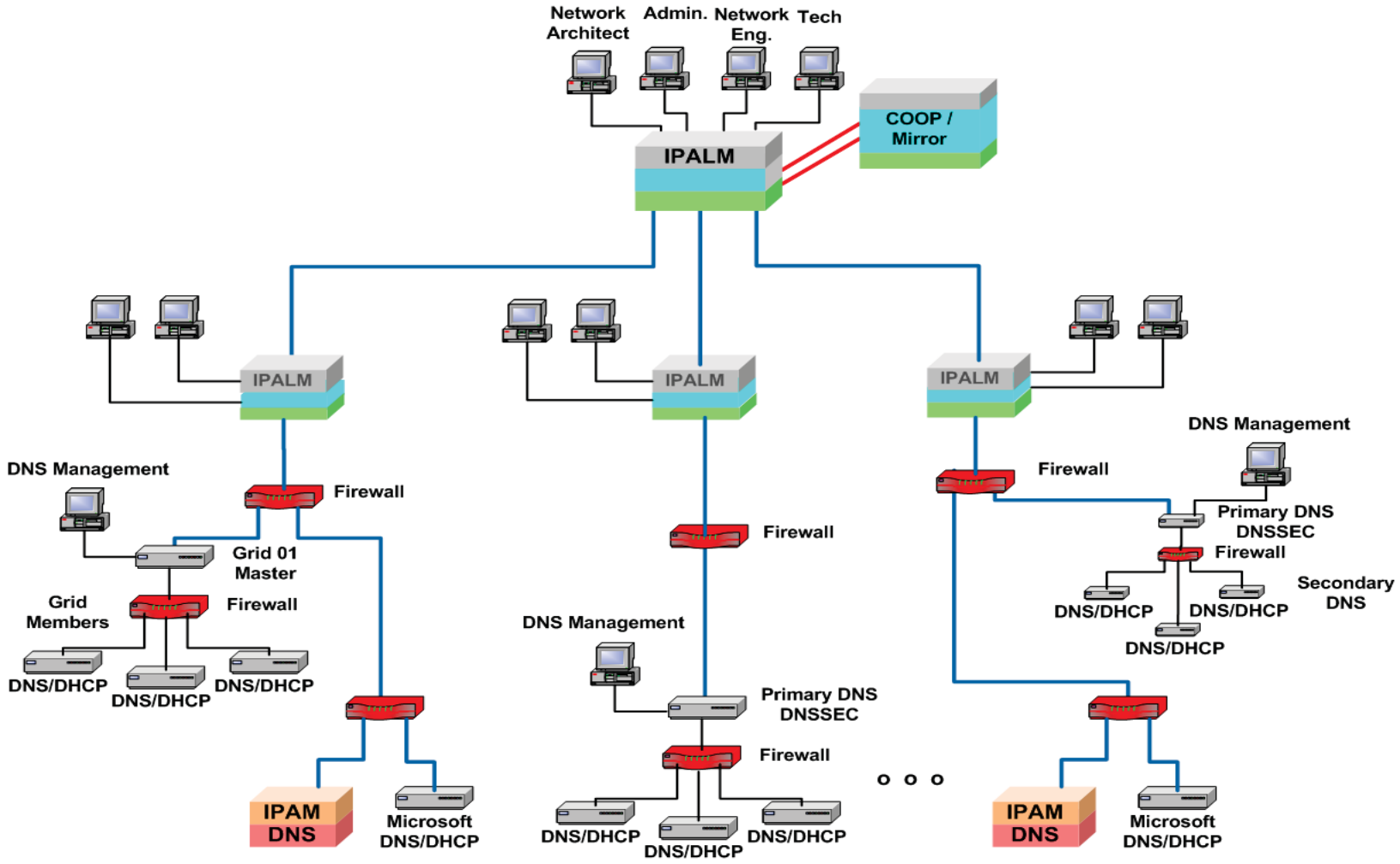
DNS/DHCP/IPAM Server Interface



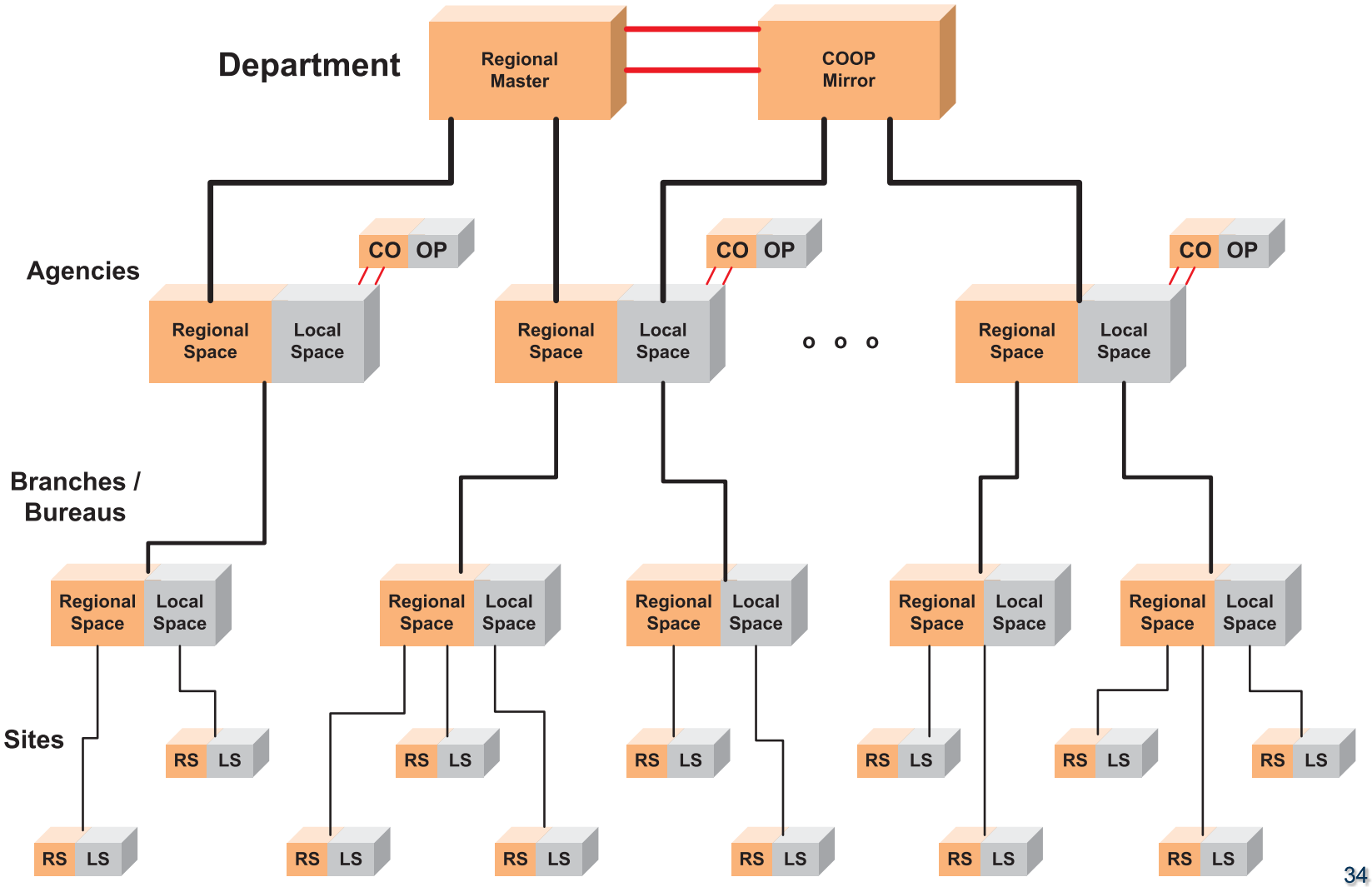
Centralized IPALM



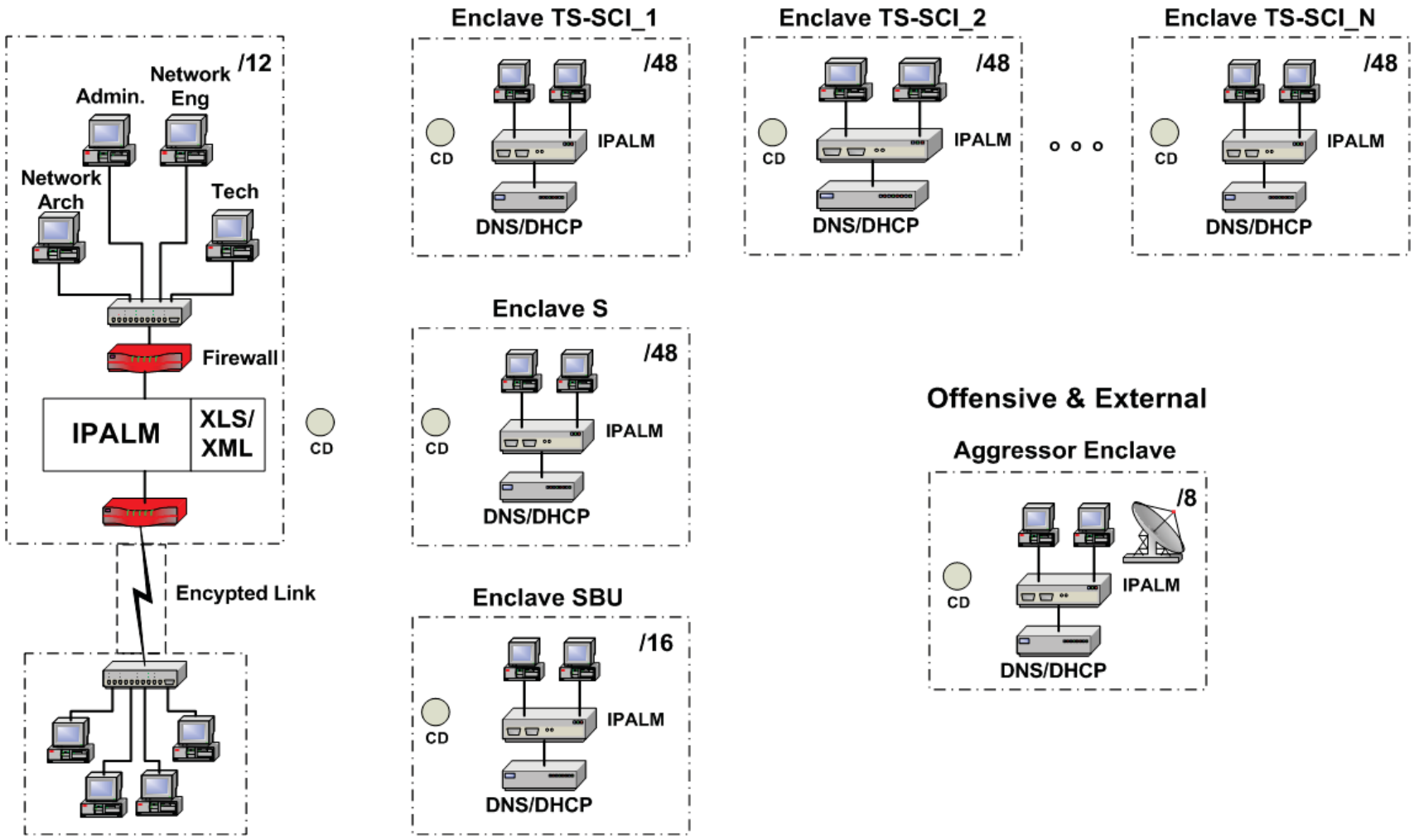
Distributed Virtualized DNS



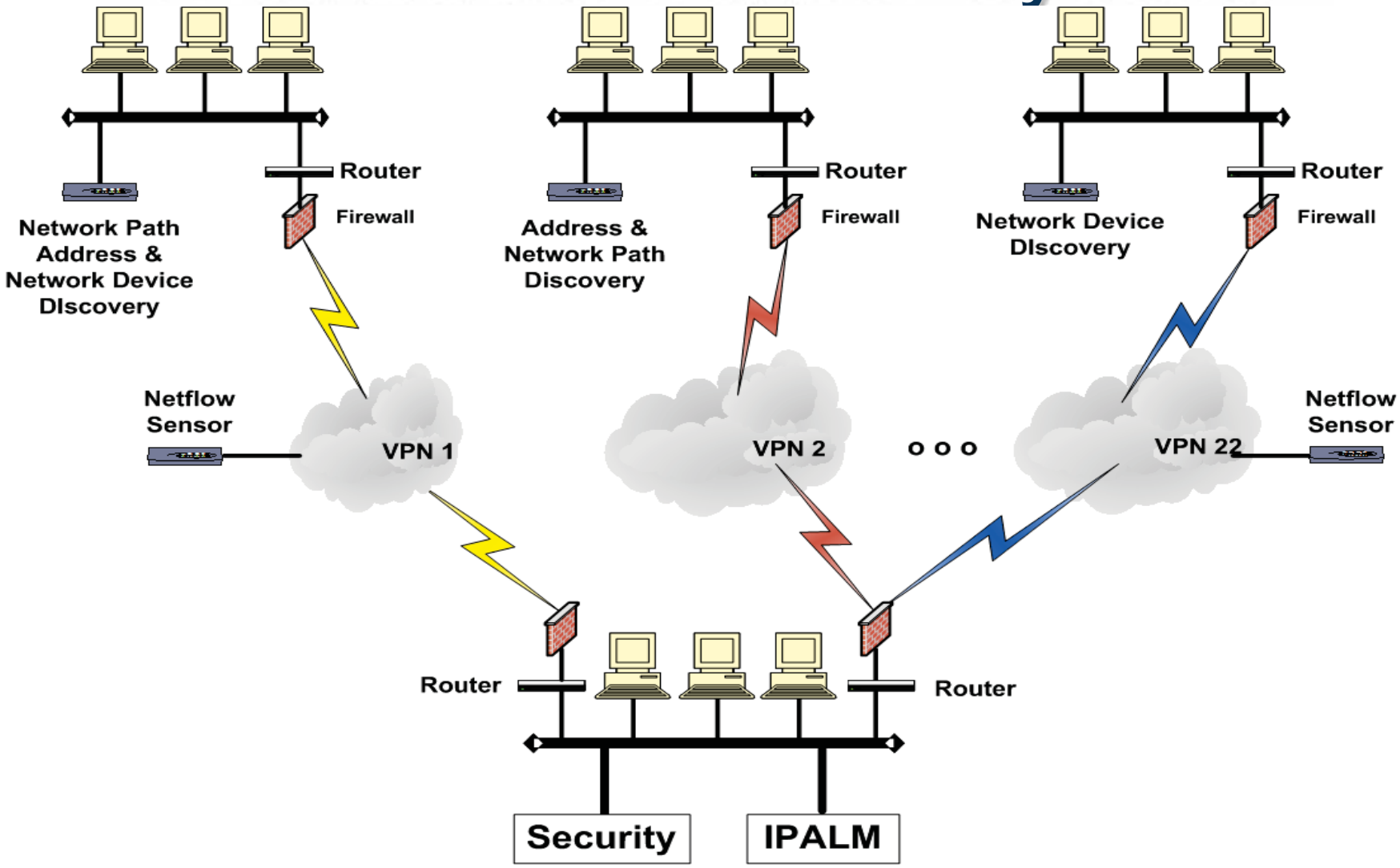
IPALM MDD Architecture



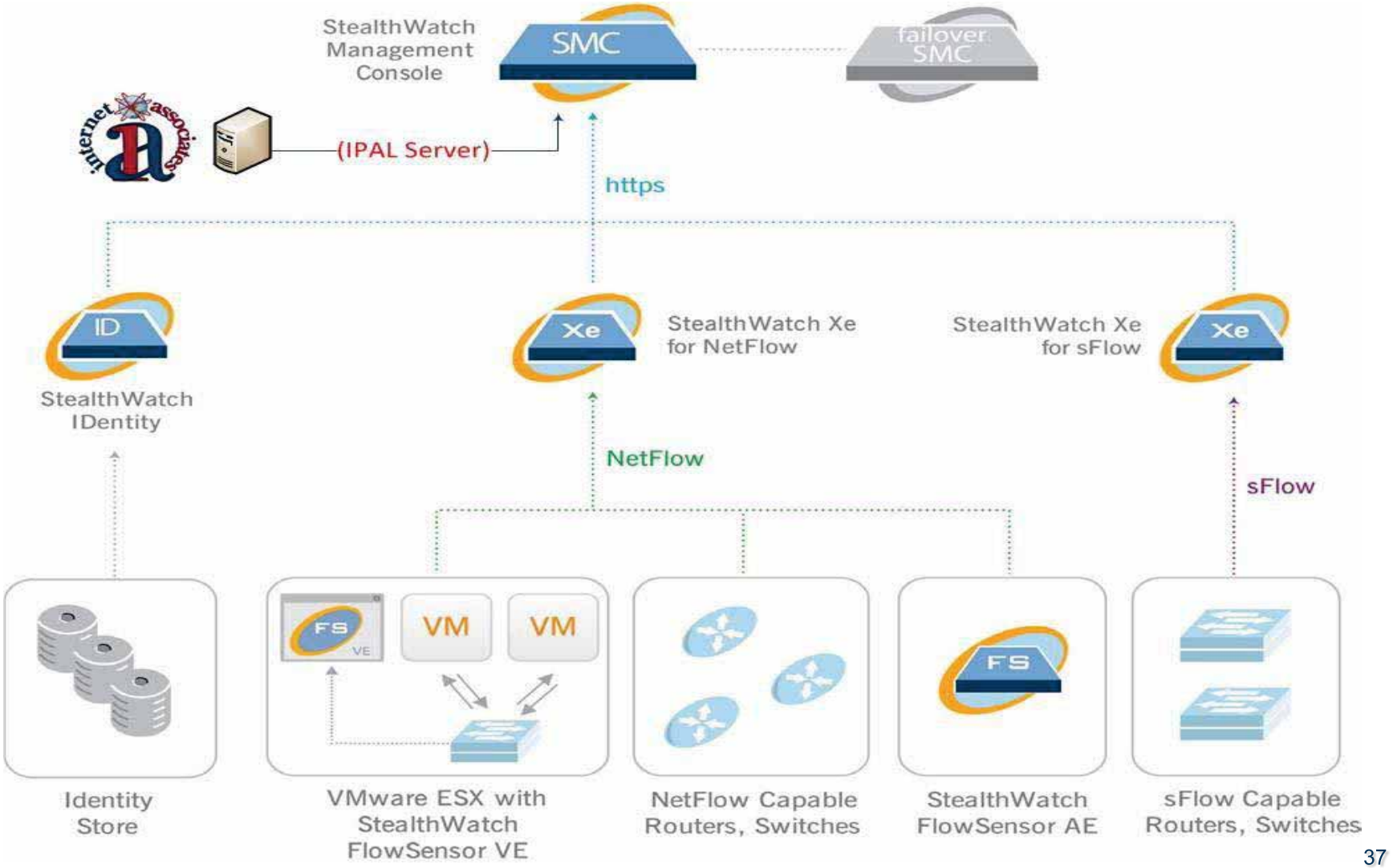
Independent Enclaves



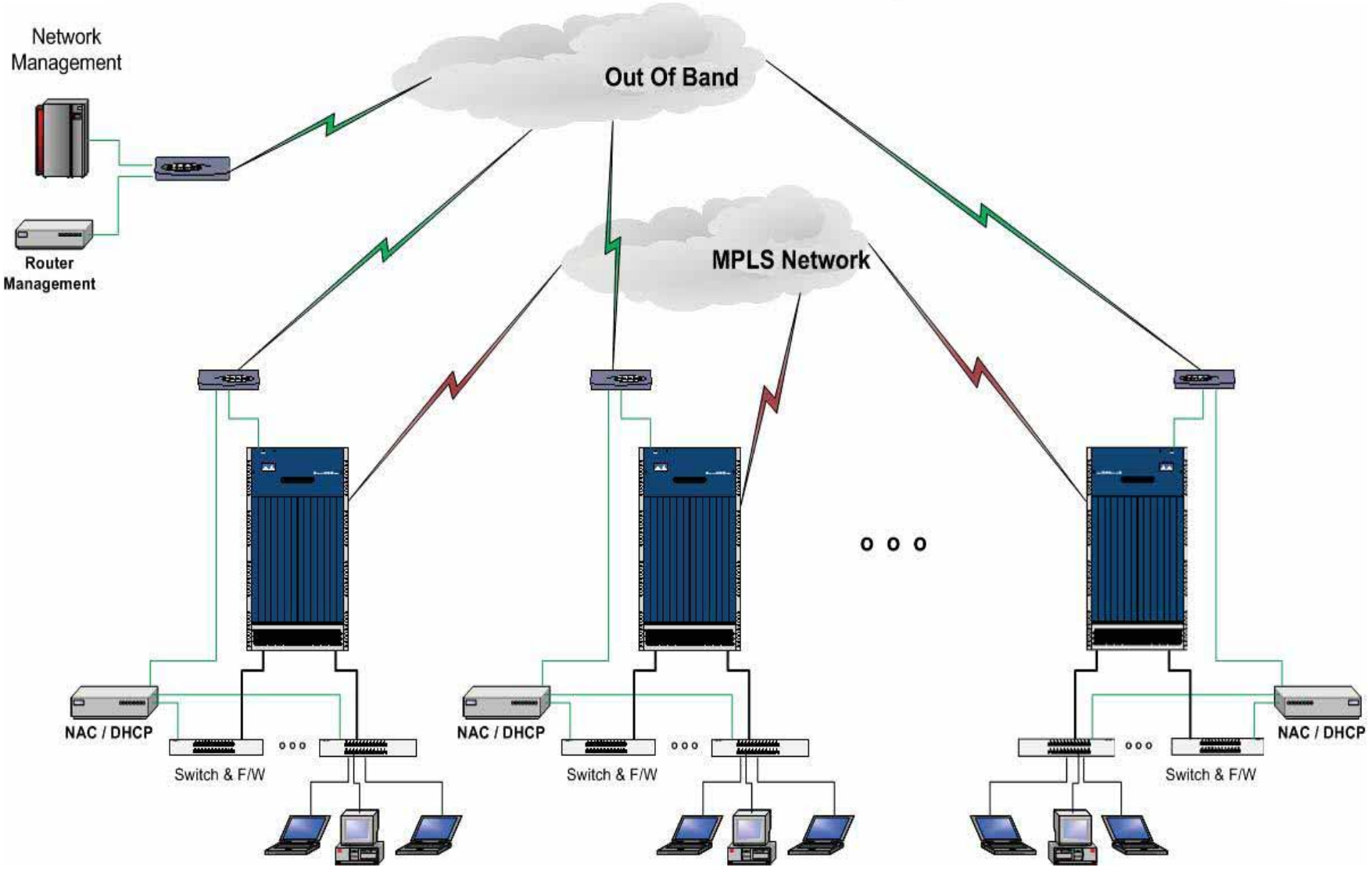
Distributed Sensor System



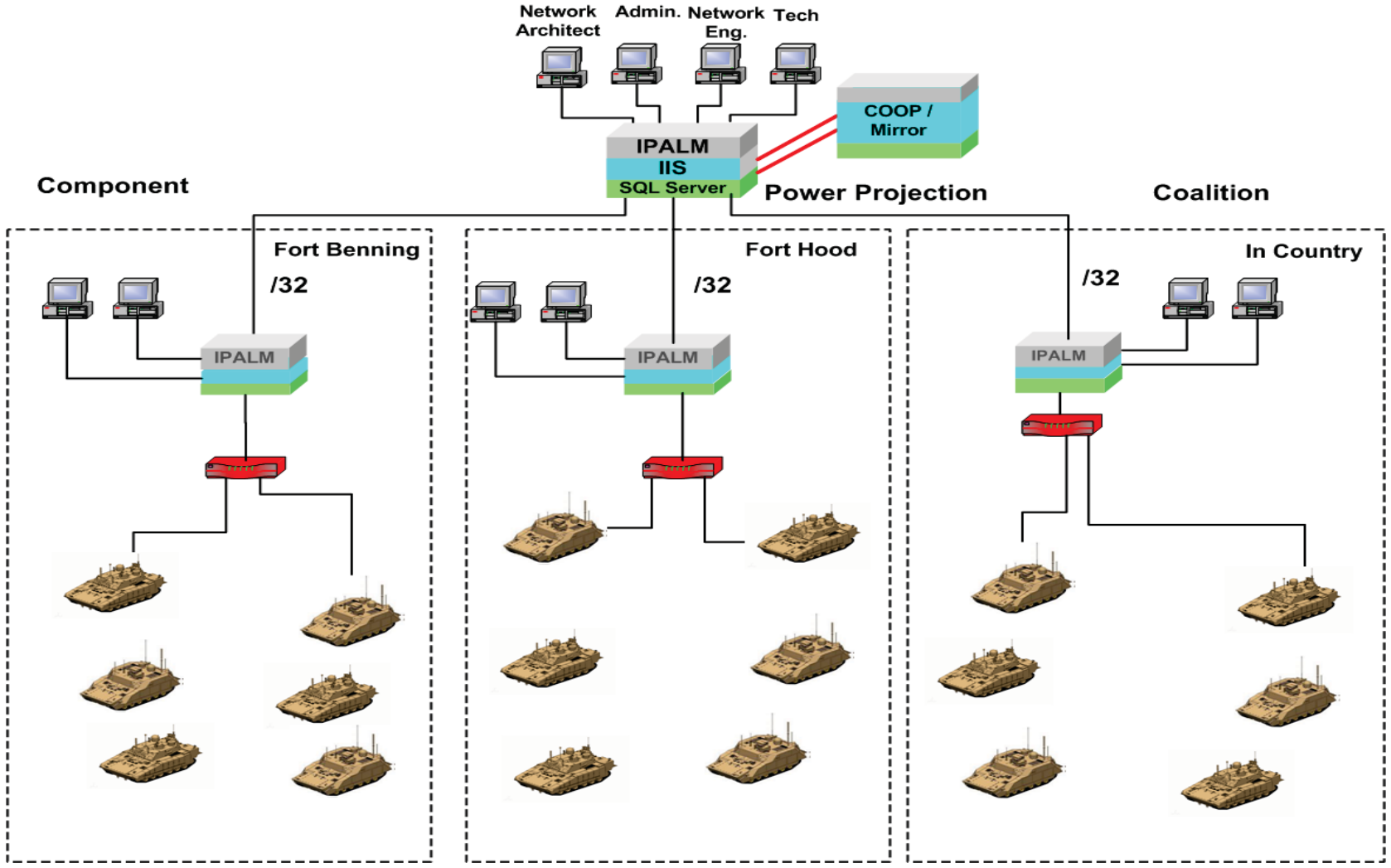
IPALM Netflow Integration



Network Discovery Issues



Rapid Deployment

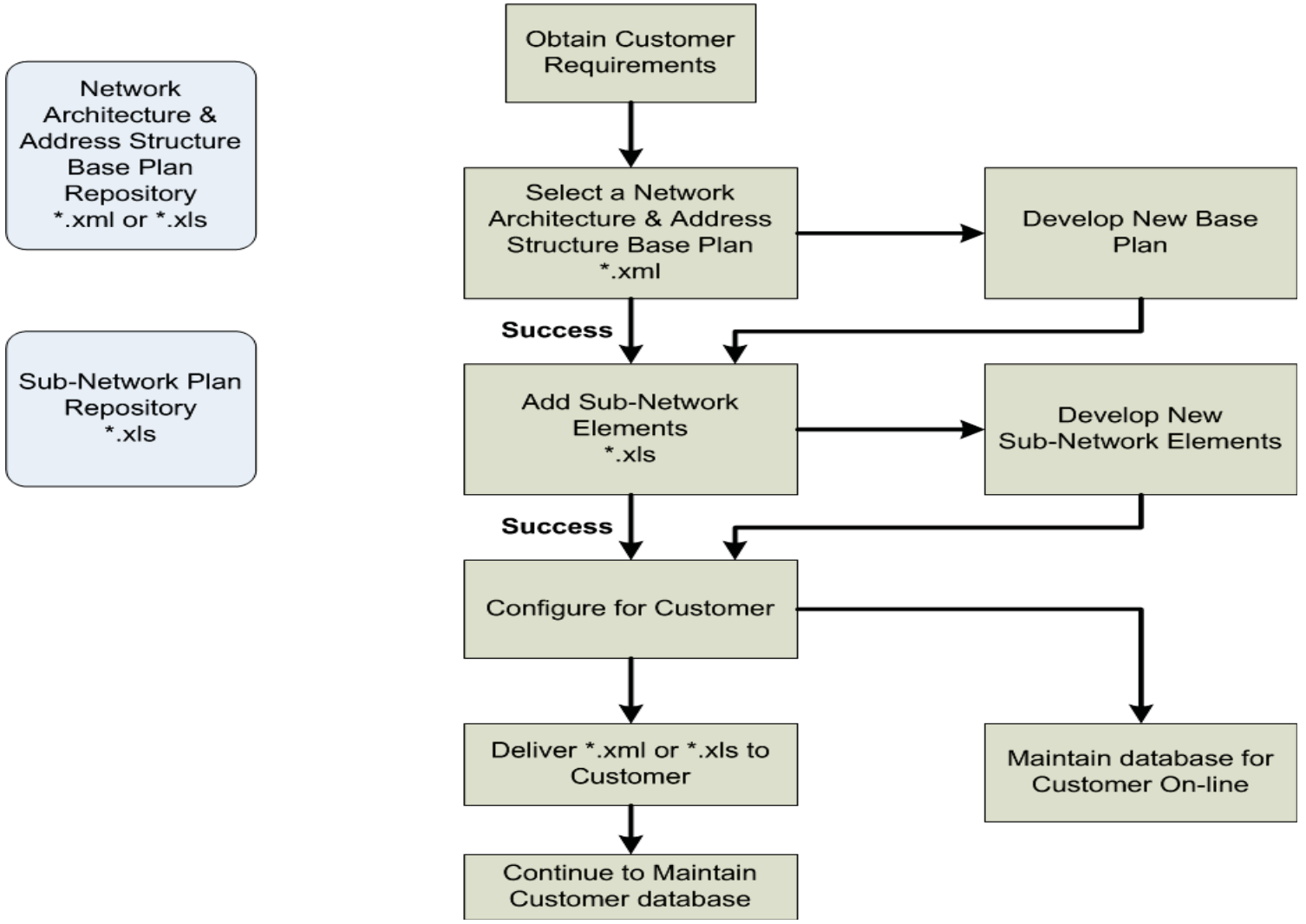


Defensive Cyber Operations

- 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



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.

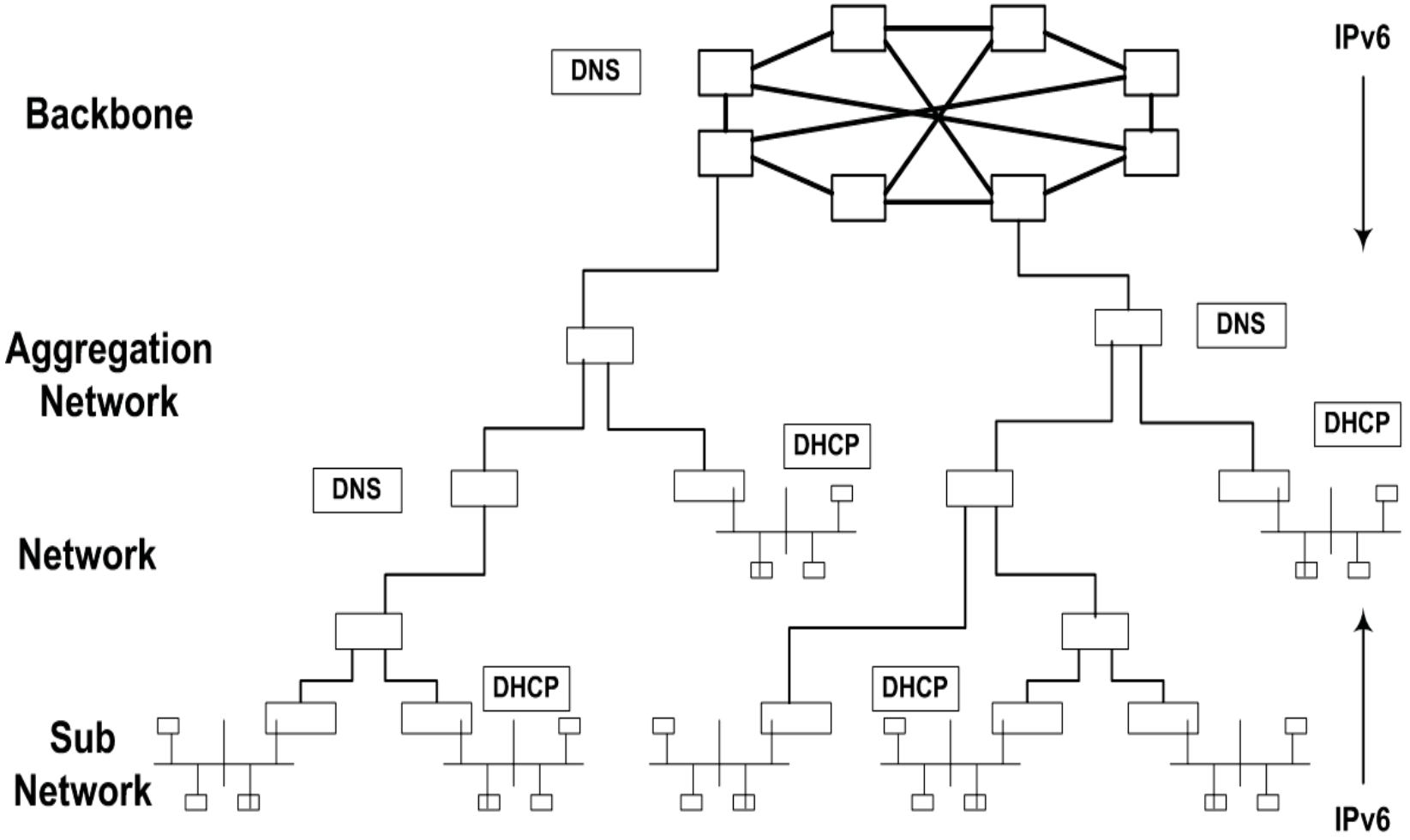
Address Plan Inputs

- 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

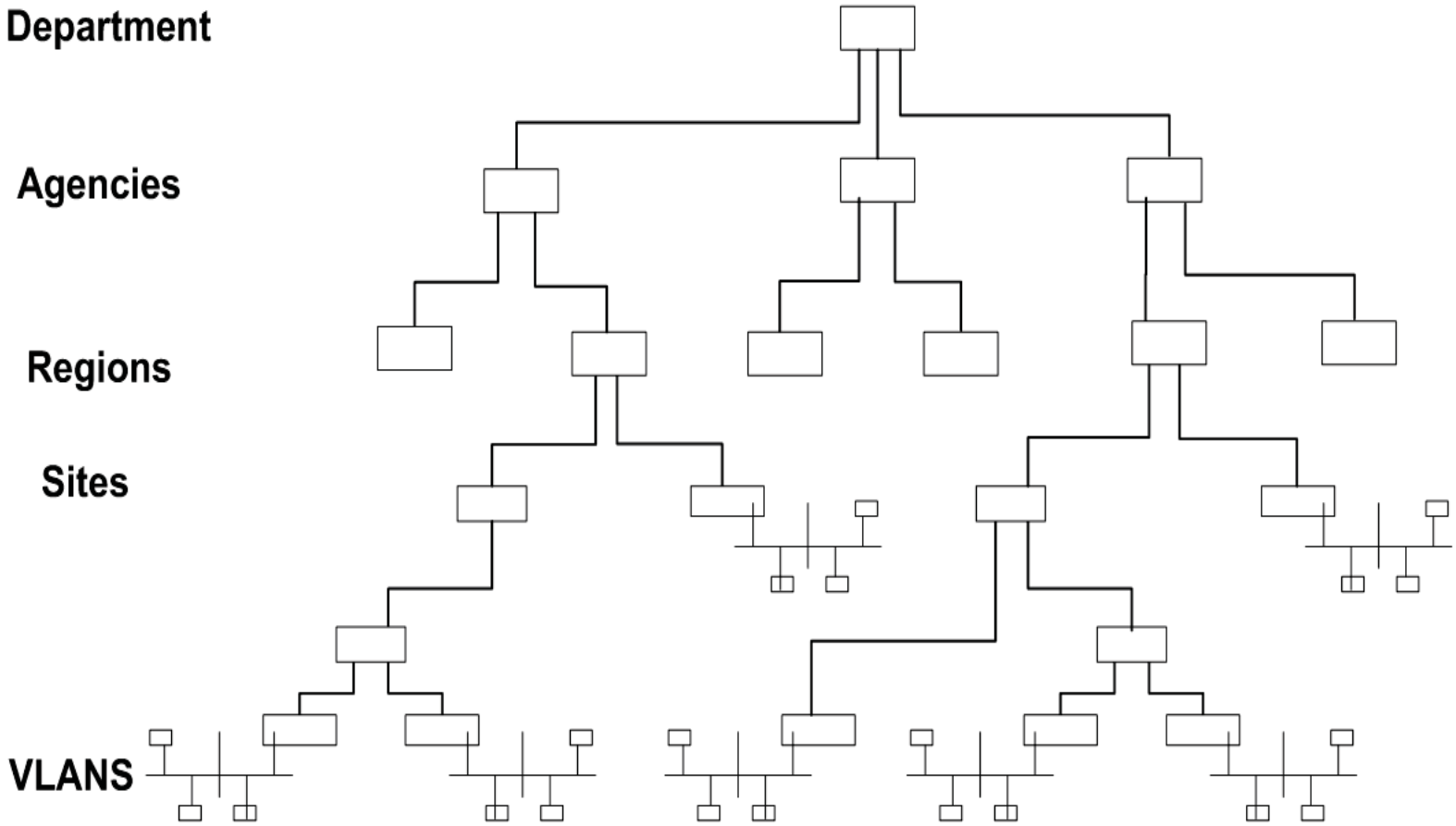
Address Plan Process in IPALM

- 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



Functional View



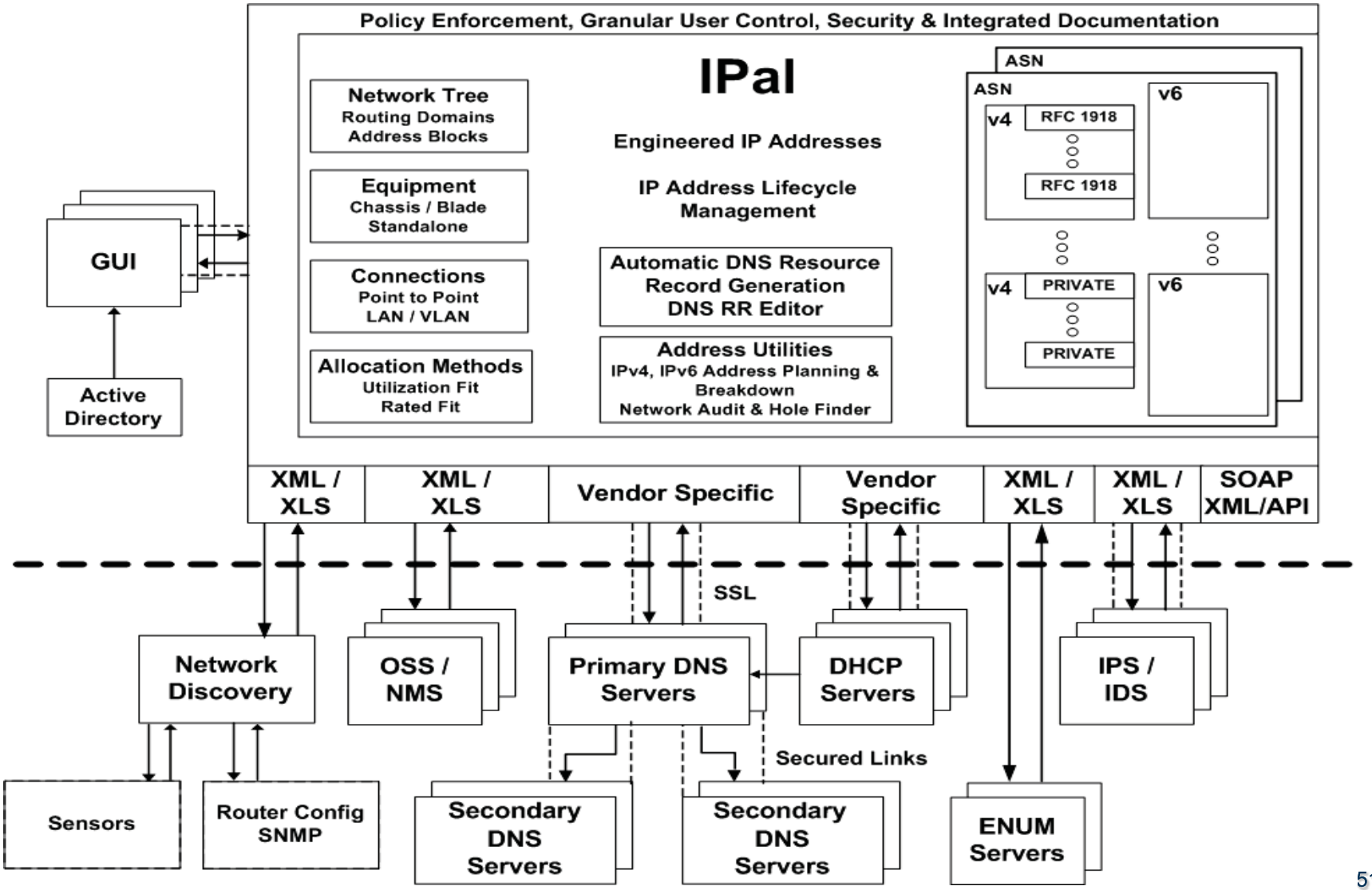
Network Model in IPALM

- 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
- Manual Network Provisioning & Management with layers of required approvals allows adversary success

IP*al* Solution Architecture



Questions ?