IPal* in the Cyber Security Eco-System

Internet Associates, LLC

A Certified VOSB

www.internetassociatesllc.com

August 4, 2010

Briefing Agenda

- Introduction
- Consensus Audit Guidelines
- IP*al* Technology Foundations
- IP*al* Demonstration
- Questions

… IPal, Patented US Developed Technology

Most extensive Intellectual Property coverage for Automated IPAM in the Industry

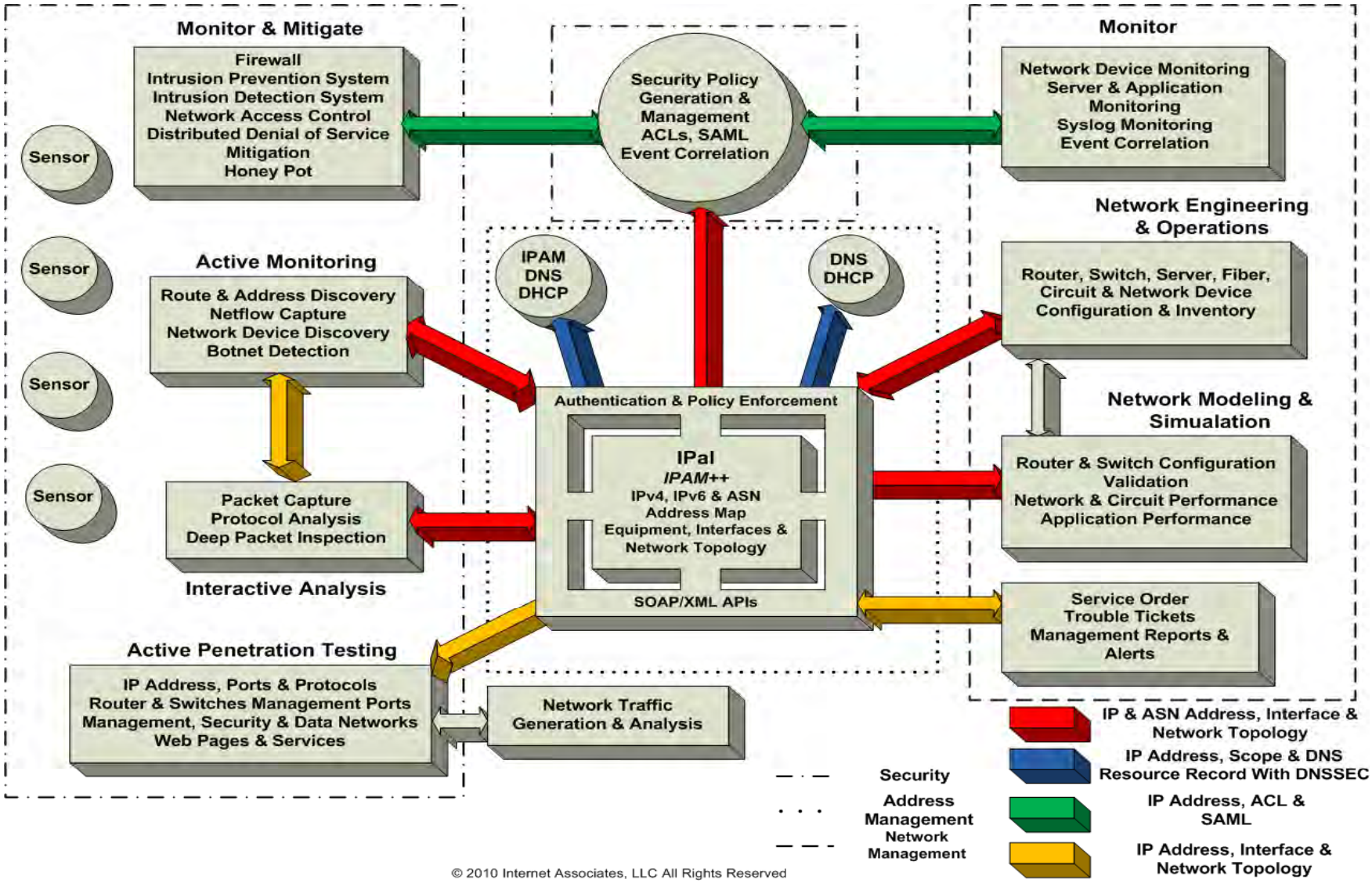
20 Critical Controls – Consensus Audit Guidelines

- 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)

IP*al* in Cyber Security Eco-System



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

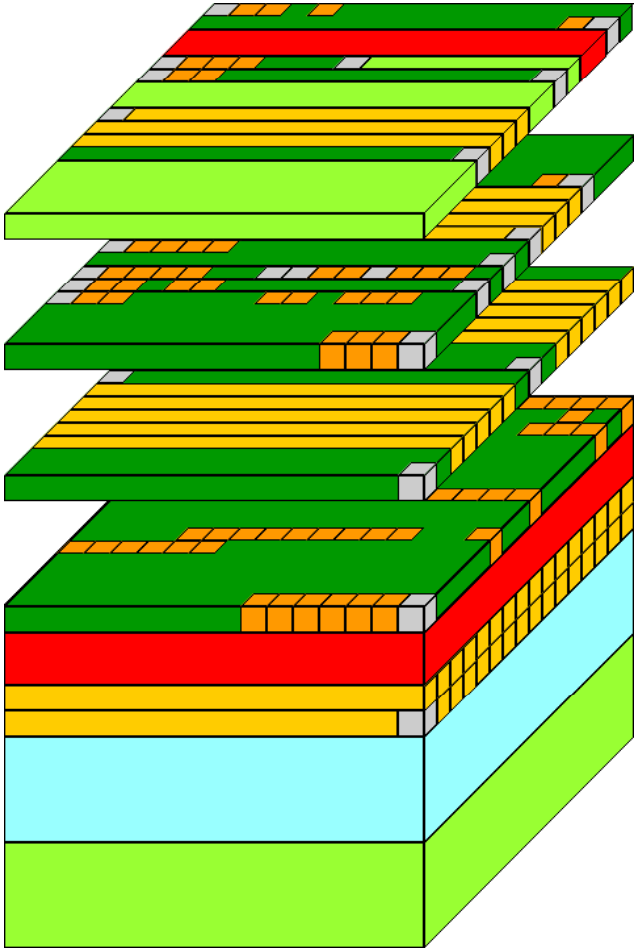
Number of v6 Addresses

- /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

IP Address Lifecycle Management (IPALM)

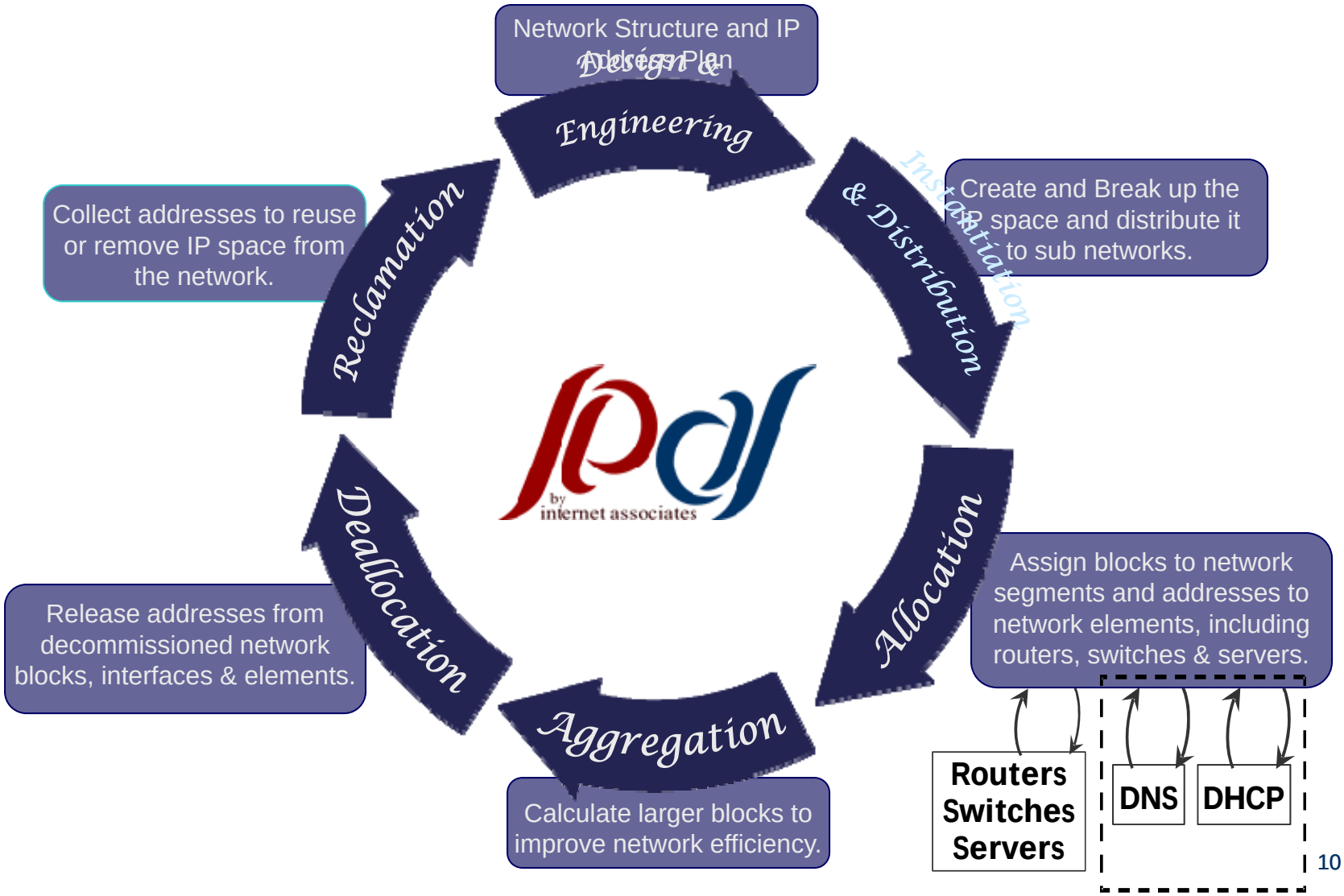
- Manage addresses from definition to decommissioning through a lifecycle process
- Engineered IP Address Blocks (EIPAB)
  - Efficient block allocations and layout
  - Input Validation on all addresses with accurate assignments
  - Guaranteed unique within a routing domain
- Single Department/Enterprise-wide 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

IPALM

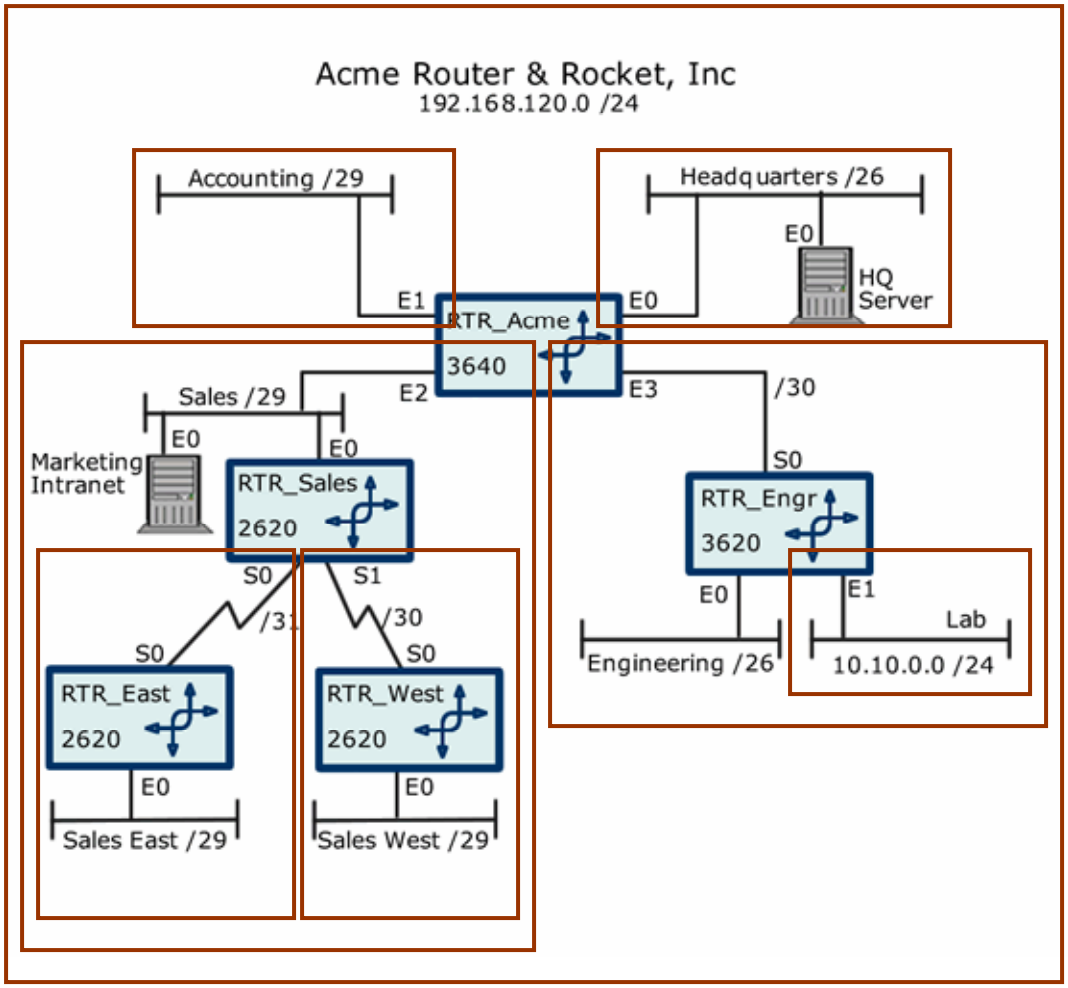


- IP Address Space is a binary data structure containing engineered IP address blocks of any size
  - Manage any size of block from /0 to /128 IPv6 & /0 to /32 IPv4
  - Split, Combine, Move, Coalesce, & Loan Blocks
  - All IP Addresses in the block are under Management
  - Multiple Unique Routing Domains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

IP Address Lifecycle



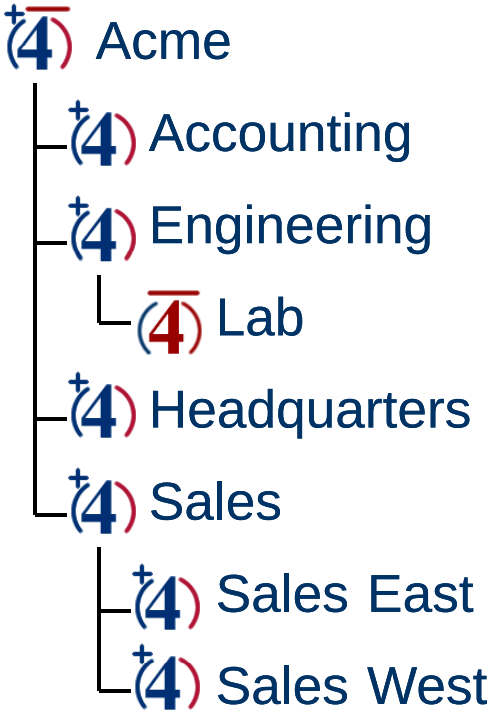
IPal Network



Hierarchical Networks

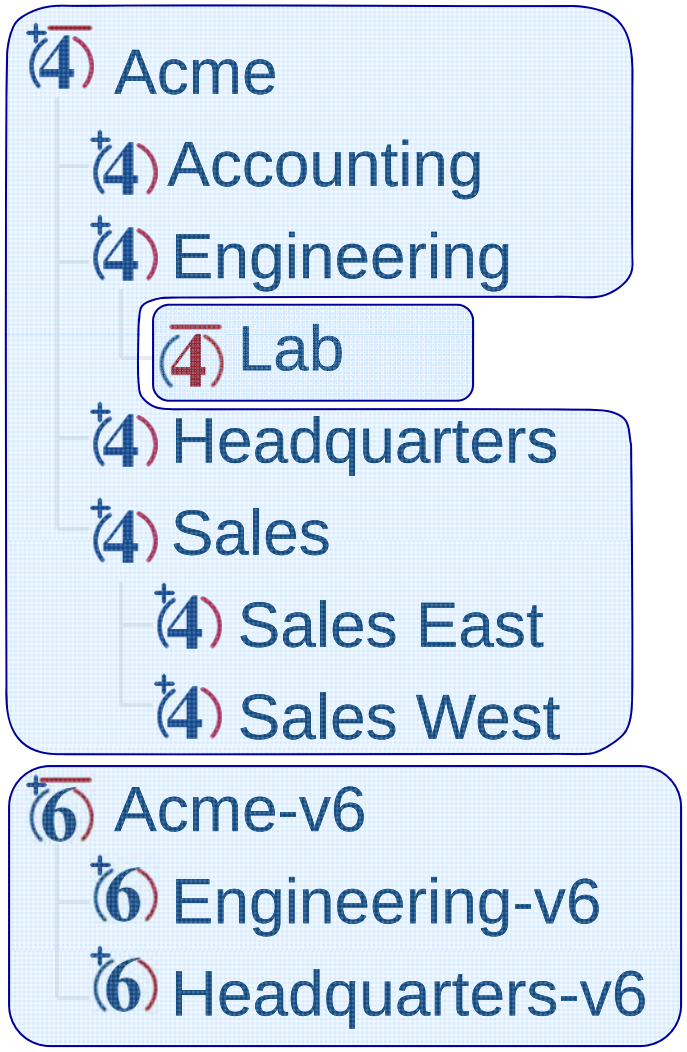
- Acme
  - Accounting
  - Engineering
    - Lab
  - Headquarters
  - Sales
    - Sales East
    - Sales West

The Aggregate Tree



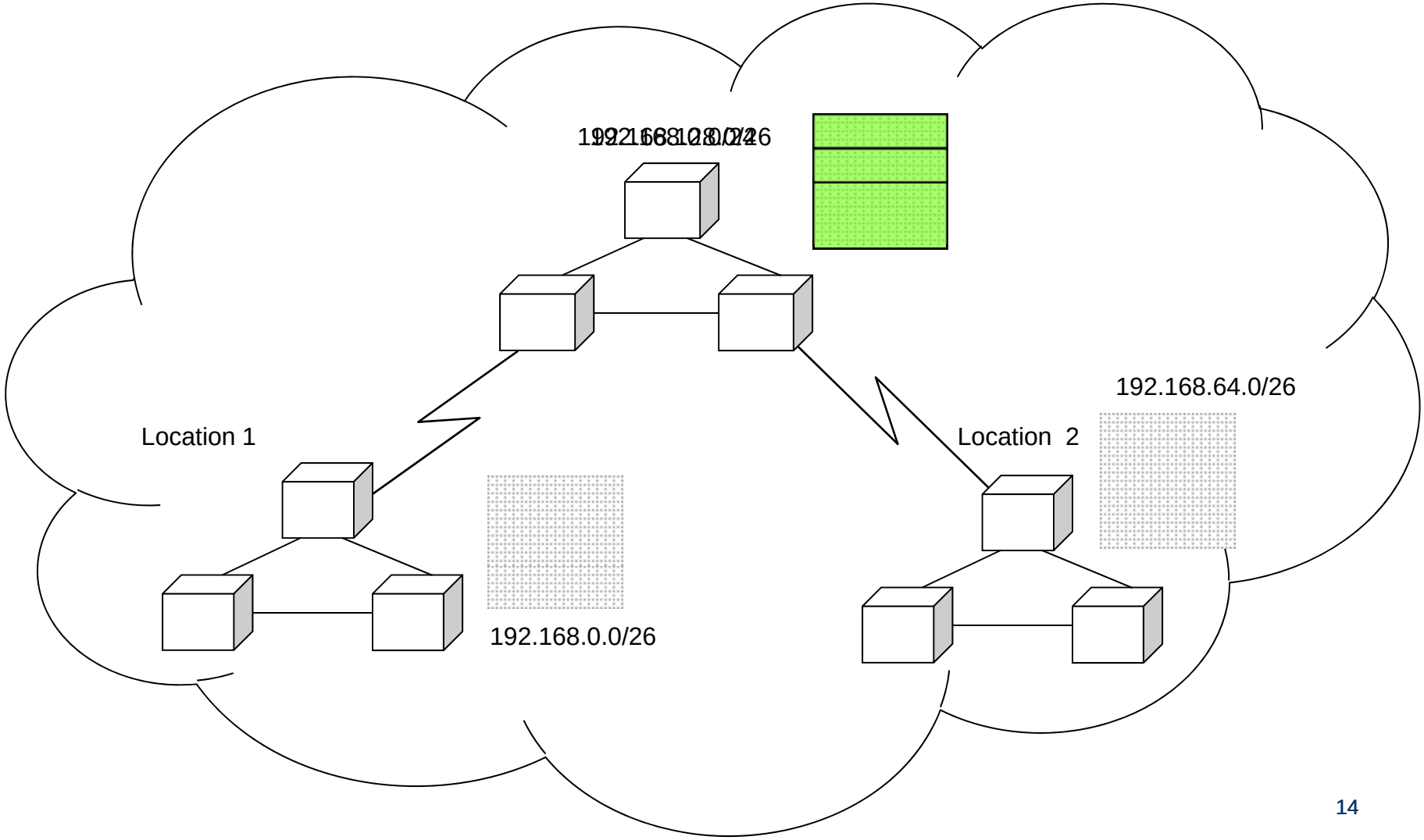
- A group of Networks (containers) that:
  - Share one instance of address space either IPv4, IPv6 or ASN that defines a routing domain
  - Unique & Valid CIDR Addresses are maintained
- Network Containers:
  - Anchor Address, Connection Blocks, Equipment & Interfaces
  - Define Control Parameters including:
    - 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

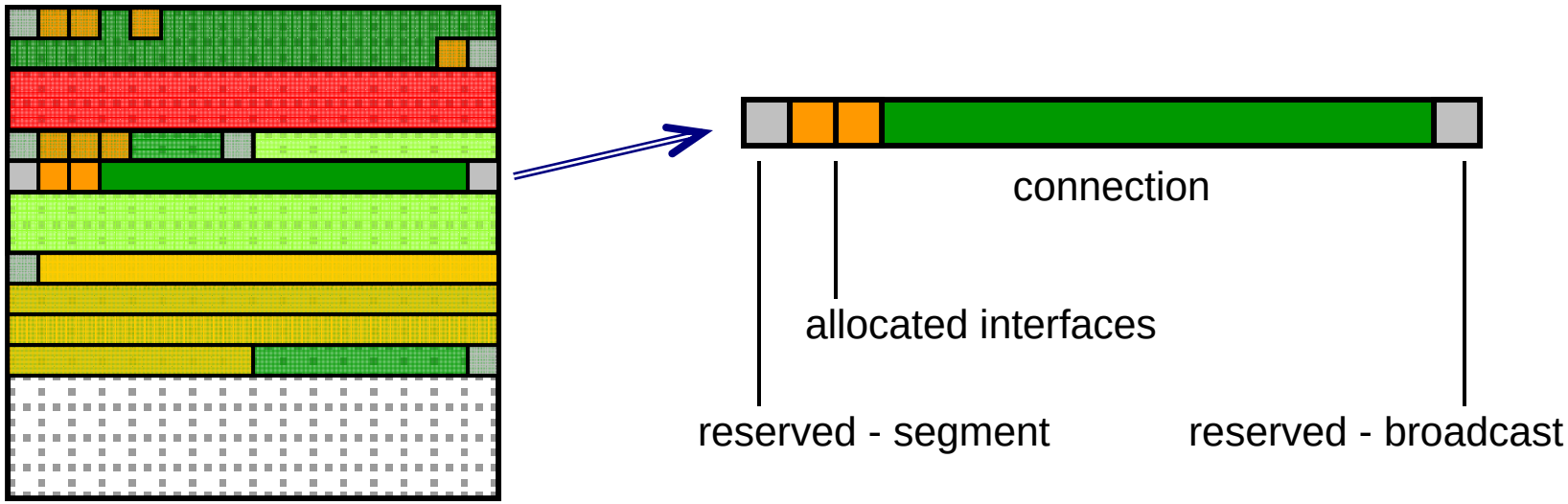
Instantiate & Distribute Space



Accurate Allocation

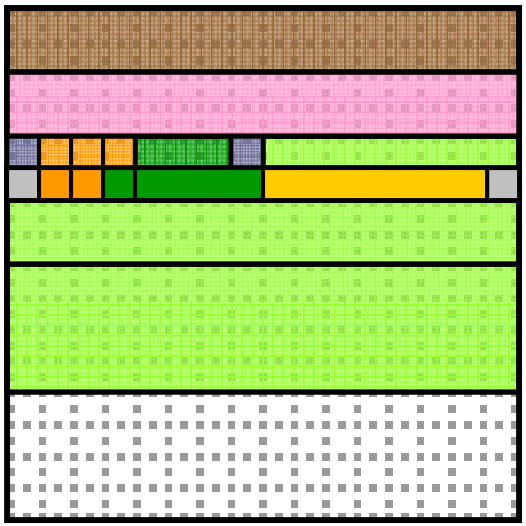
Manually or automatically select a free block

Create a network segment



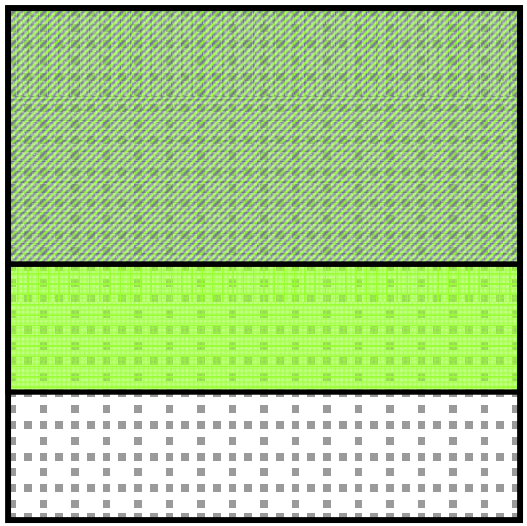
IP address Aggregation

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

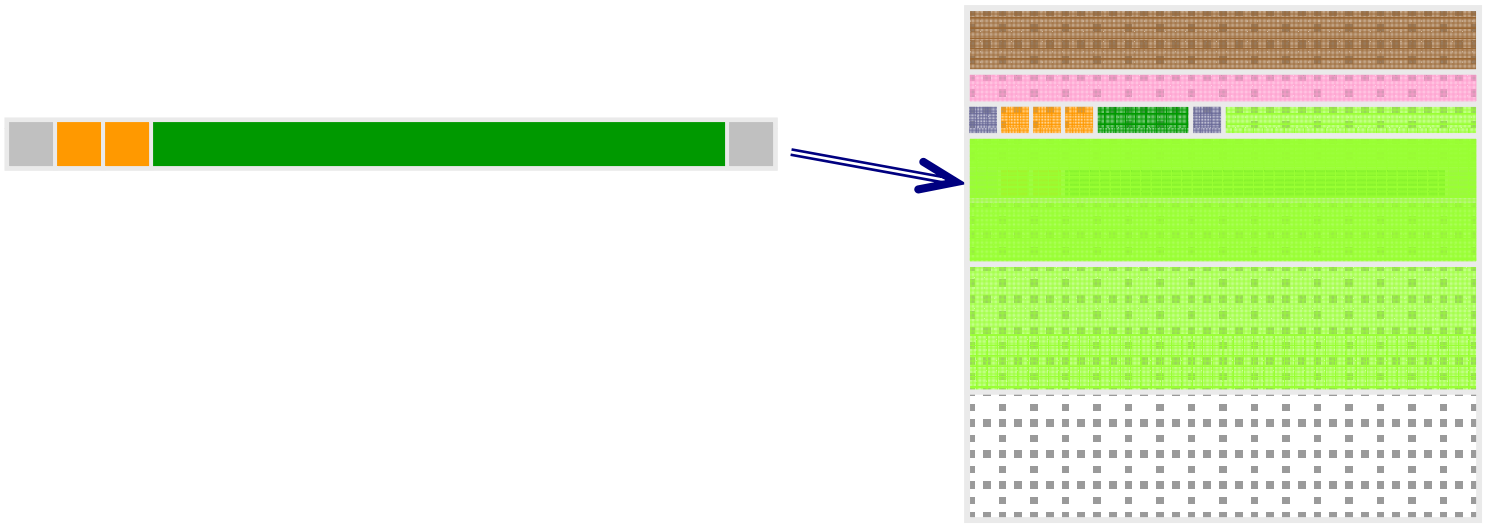
Allows all Addresses Under Management

- Tightest Route Table Entries

Deallocation

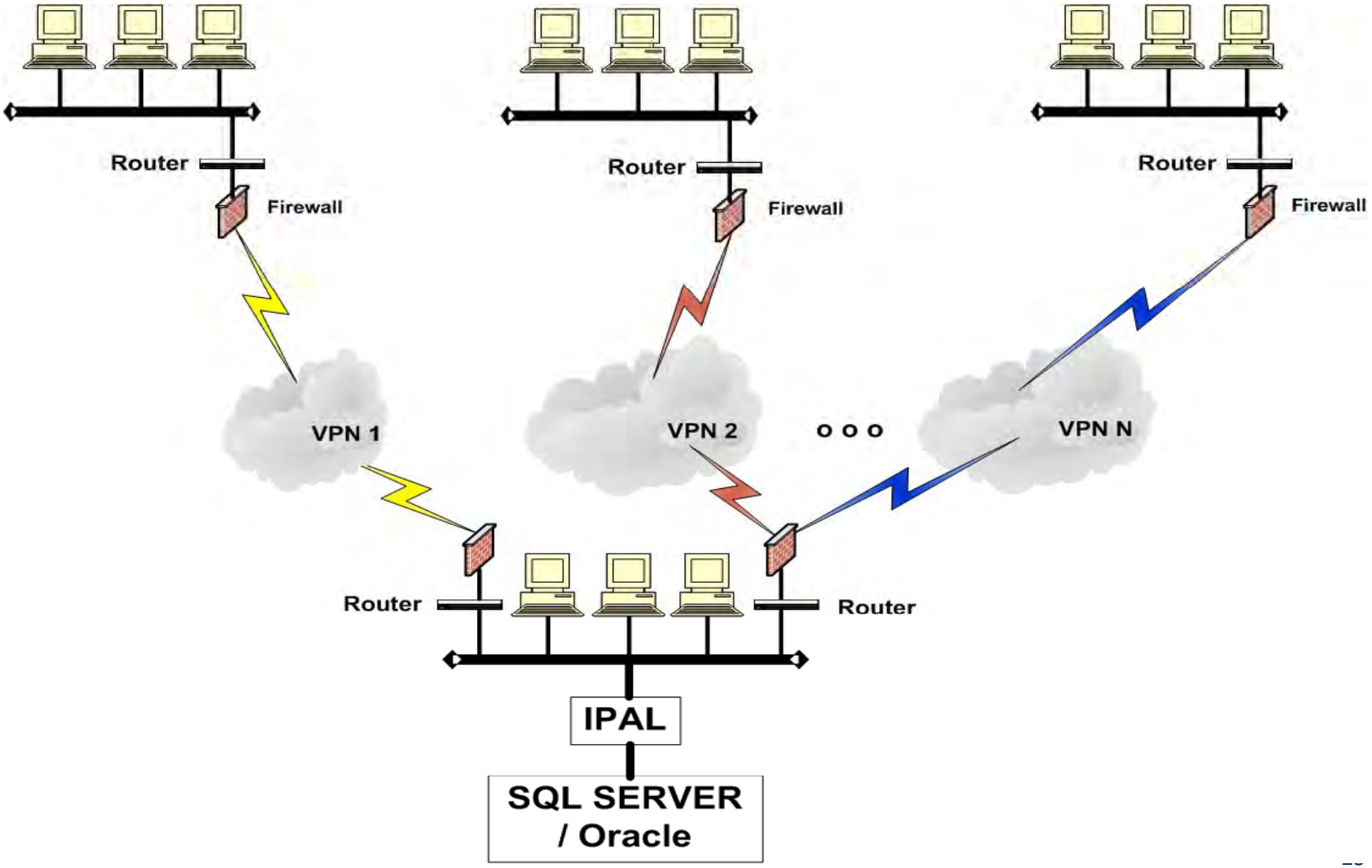
Delete interfaces

Release a block

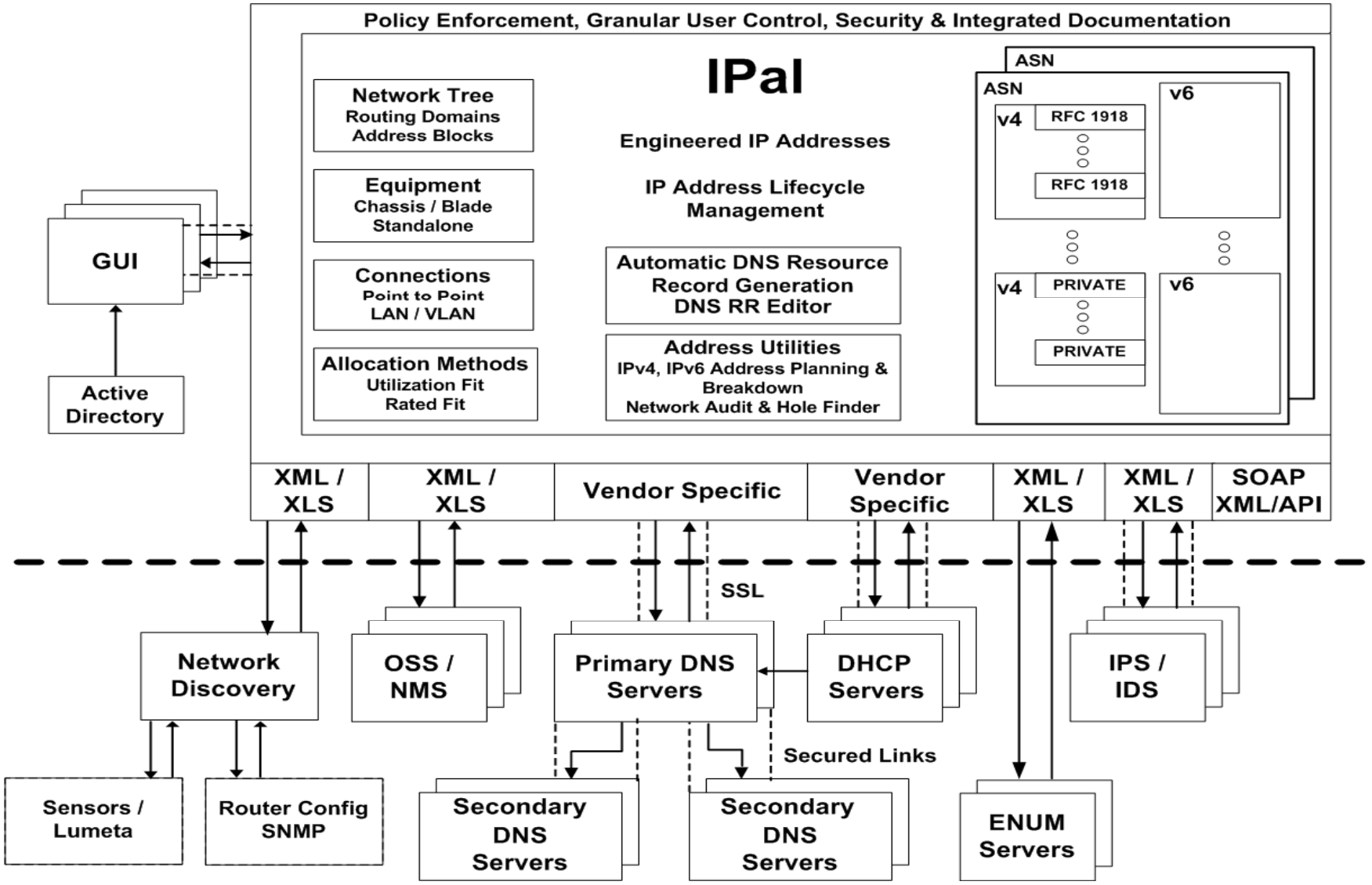


Coalesce blocks

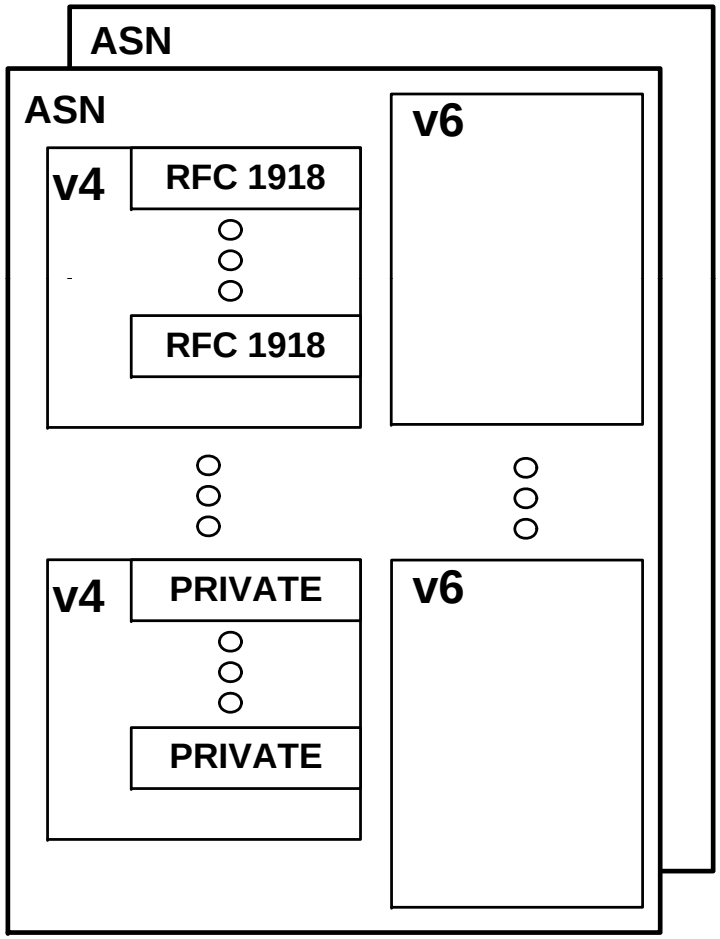
Web Service Based System



IP*al* Architecture

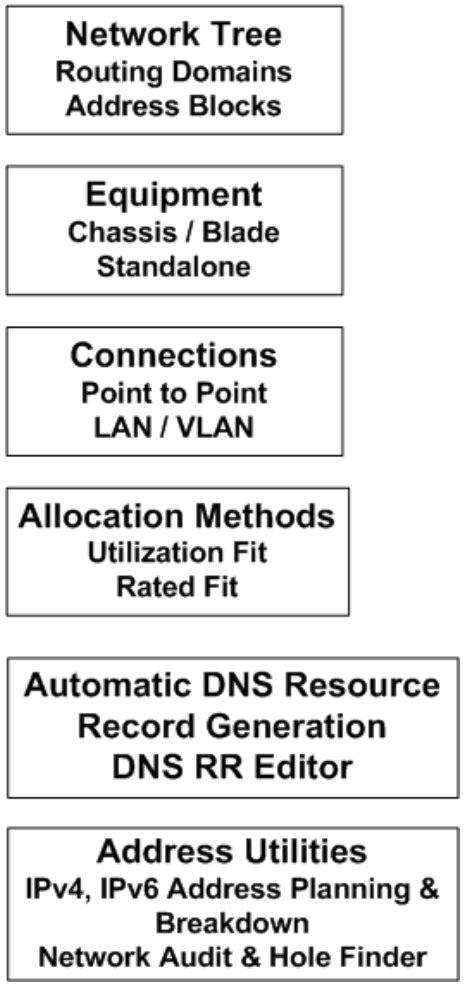


IPv4, IPv6 & ASN Support



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

IPal Elements



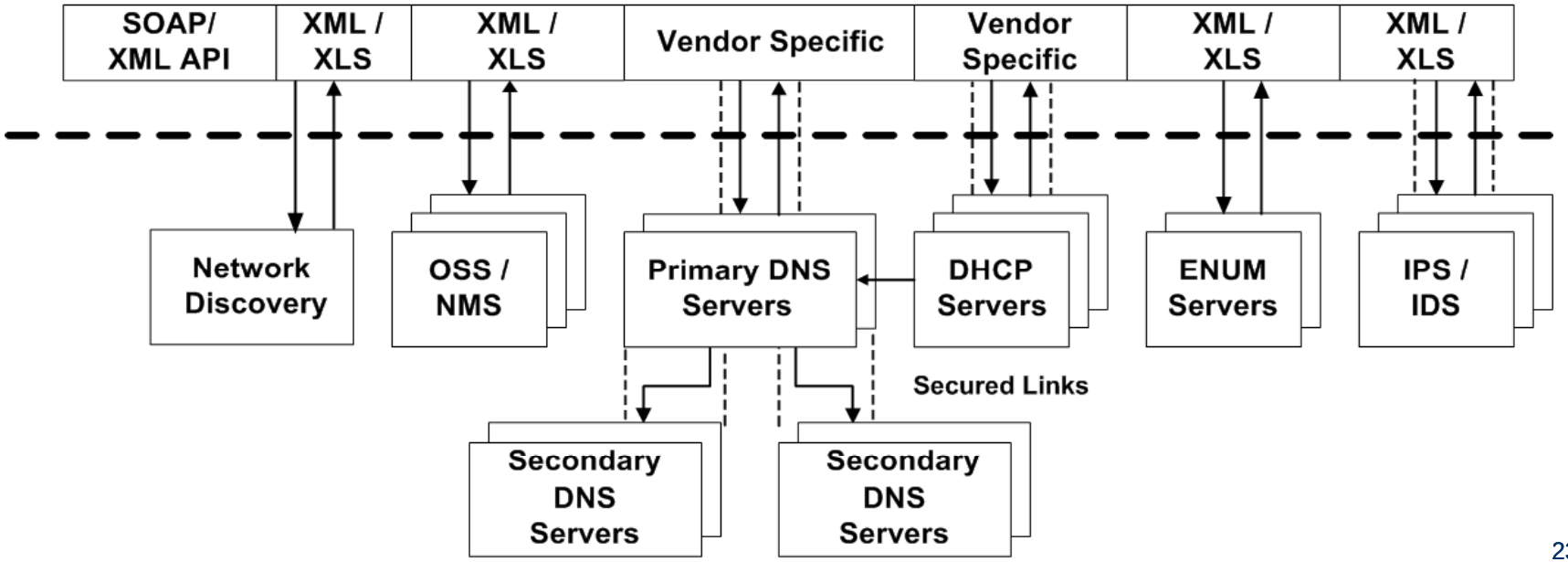
- Validate, Organize & Control accurate IP addresses & associated information
- Equipment associates IP addresses with physical & virtual interfaces
- Connections – organize subnetworks
- Multiple Allocation & Assignment Methods for IPv4 & IPv6
- Automatic DNS Record Generation & RR Editor
- Custom Fields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

IPv6 Support

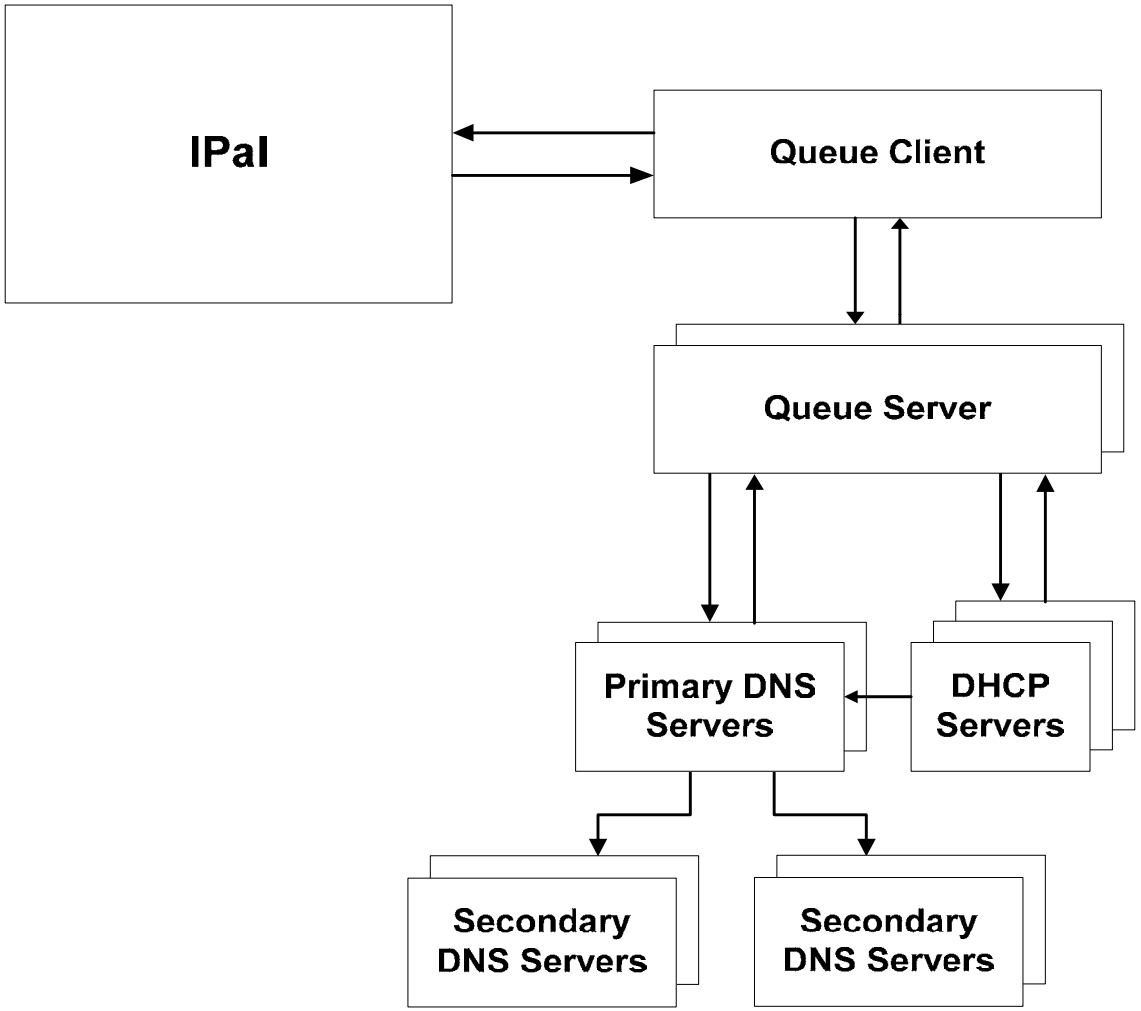
- Address Planning & Design
- Dual Stack – Physical and virtual interfaces support multiple IPv4 and IPv6 addresses
- Interfaces addresses
  - EUI-64, Random, or user-defined
- IPv4 – IPv6 Transition
  - Architect network tree
  - Load existing v4 devices using network discovery
  - Optimize & enhance network structure
  - Add dual stack network structure & v6 address blocks

Industry Standard Interfaces

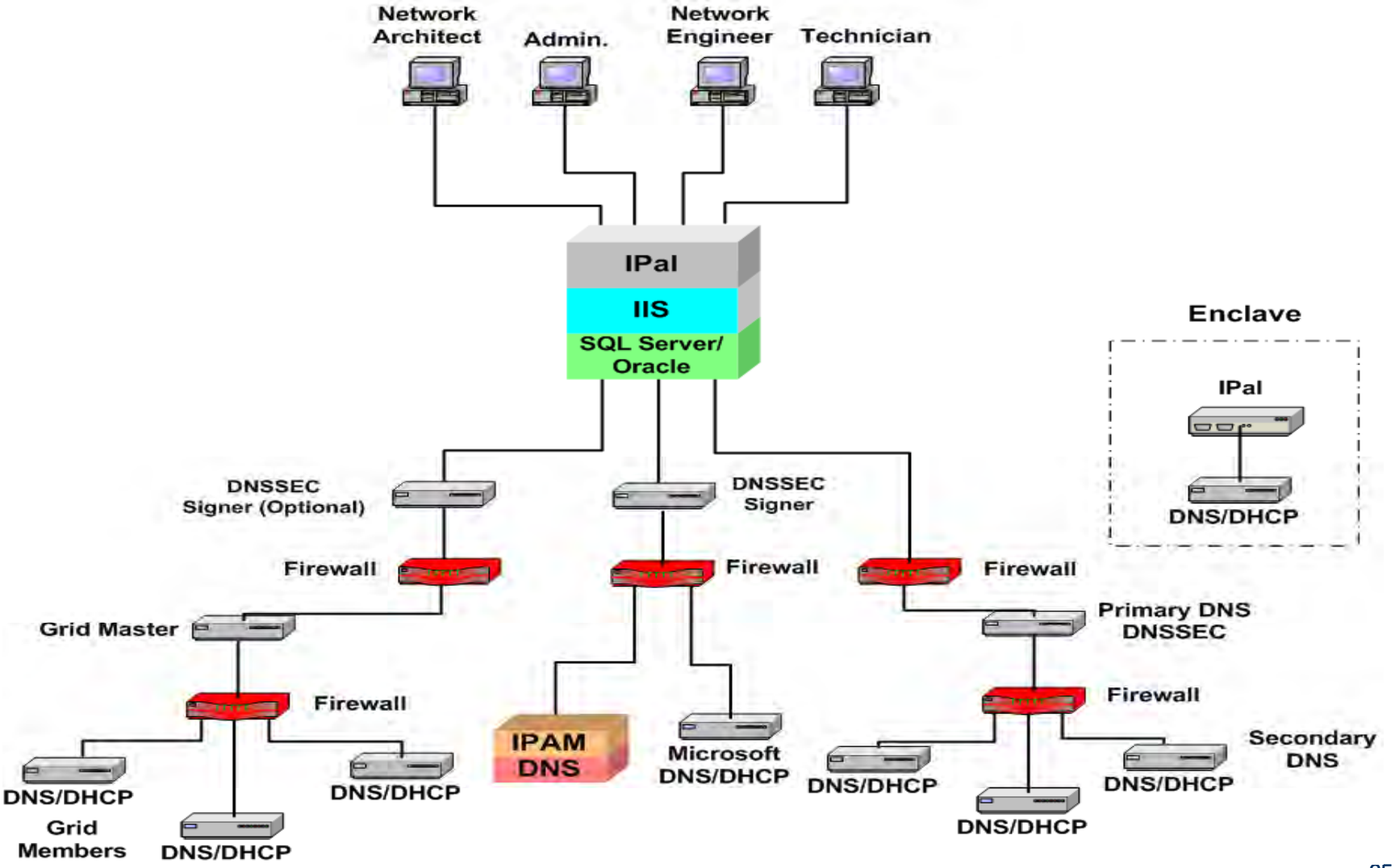
- DNS/DHCP vendor specific interfaces: Cisco, Microsoft, ISC's BIND, Infoblox, InfoWeapons, Secure64
- Lumeta, SolarWinds, What's Up Gold
- Bi-directional XLS & XML with SOAP/XML API



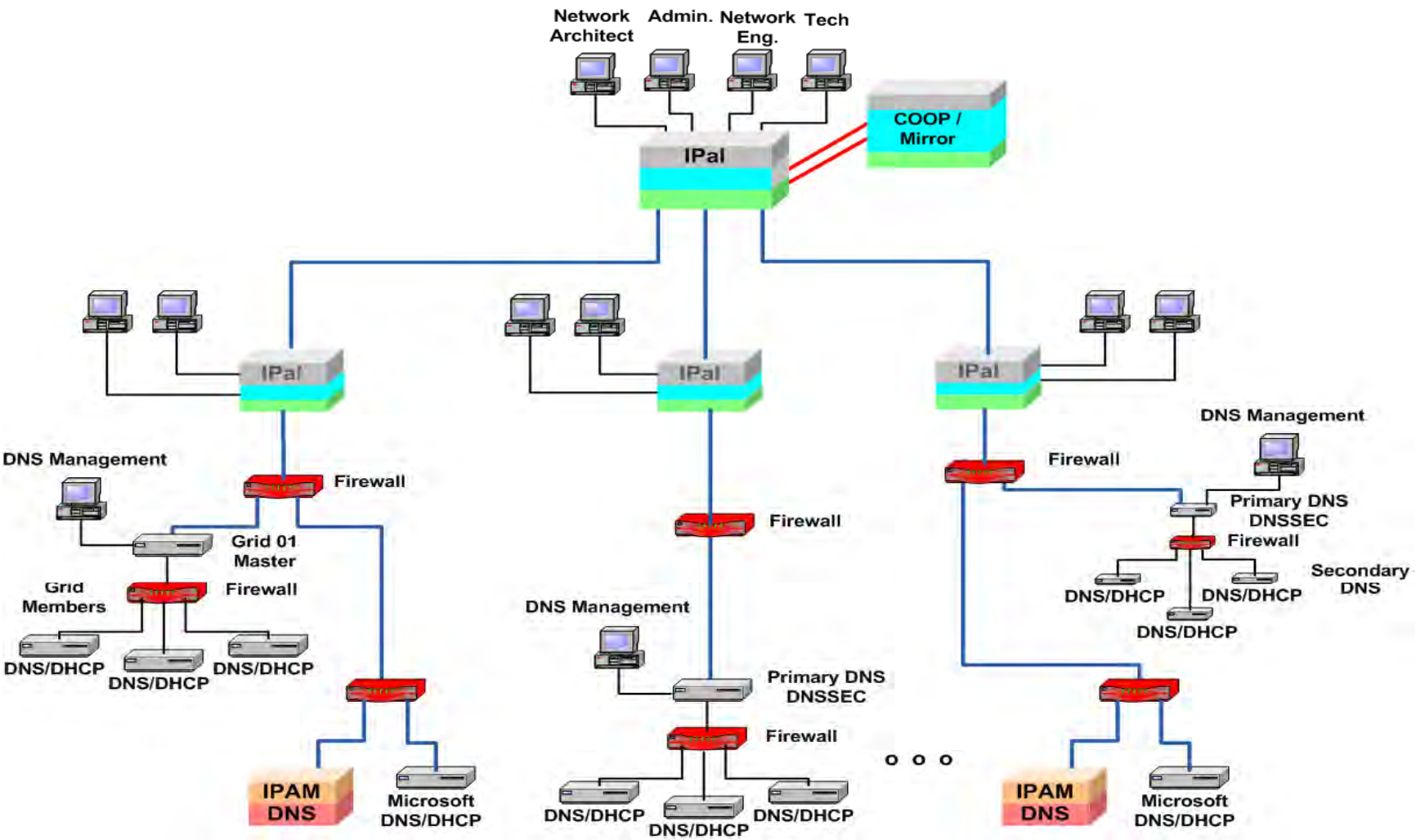
DNS / DHCP Server Interface



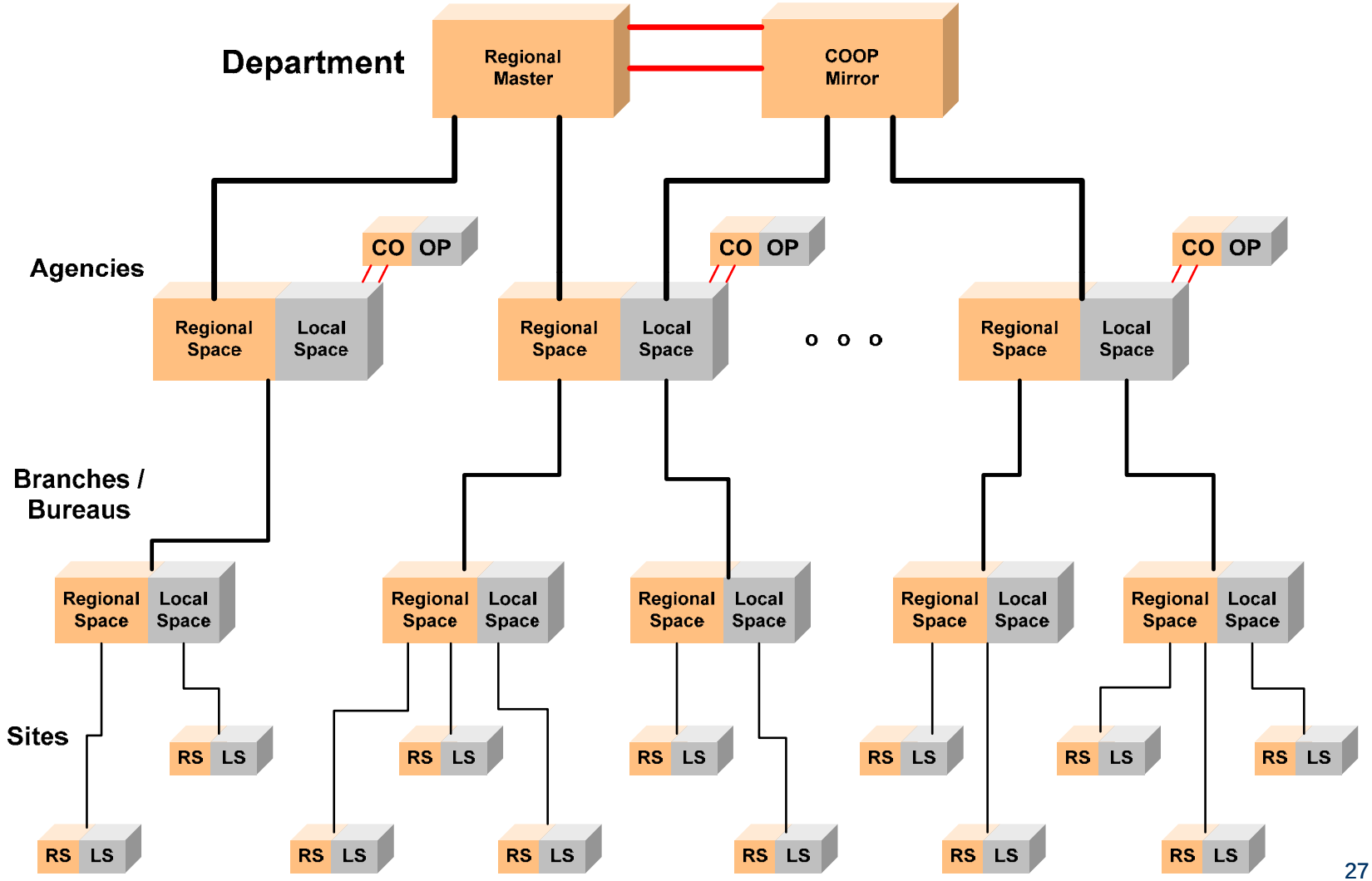
Virtualized DNS



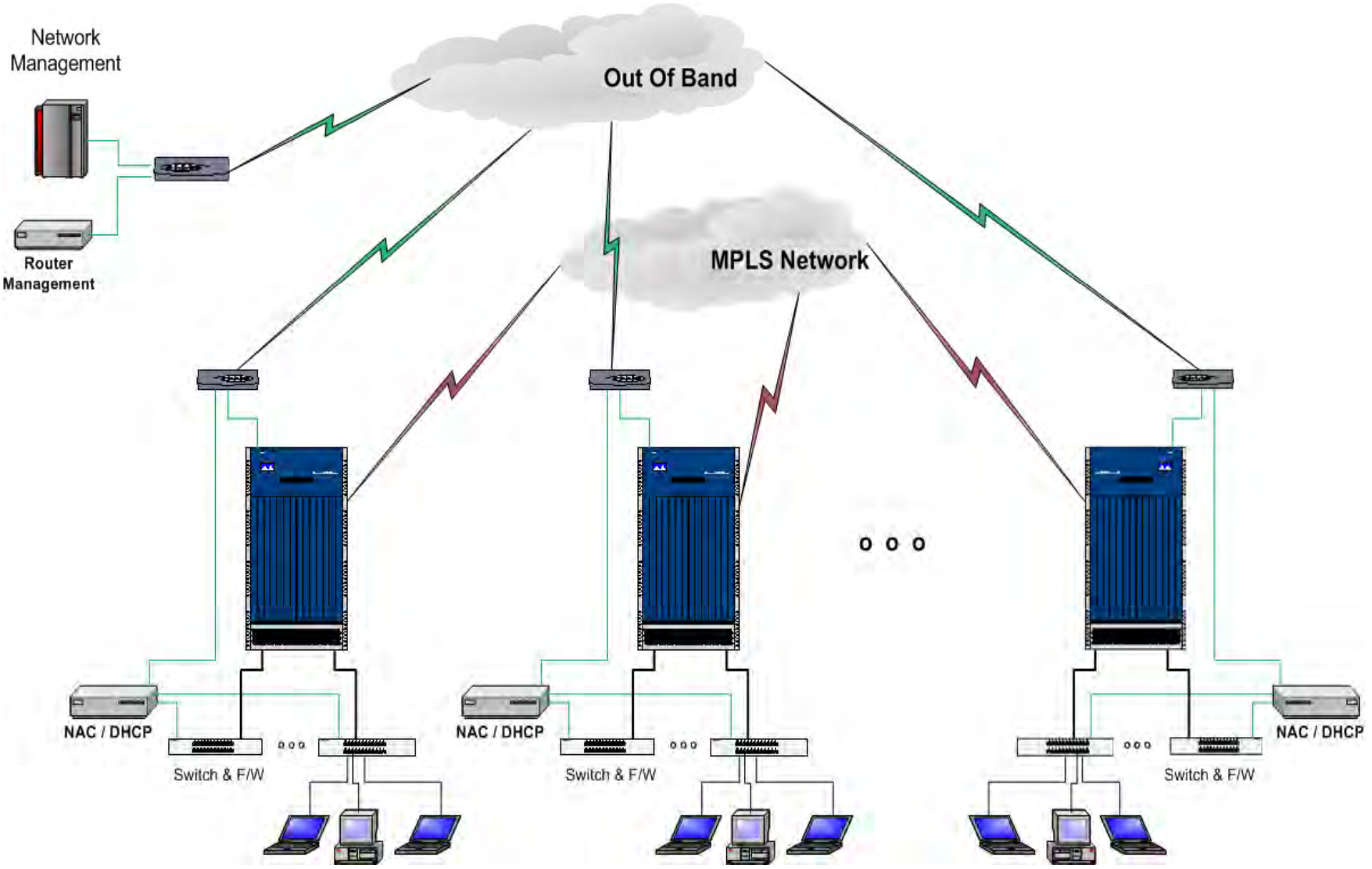
Distributed Virtualized DNS



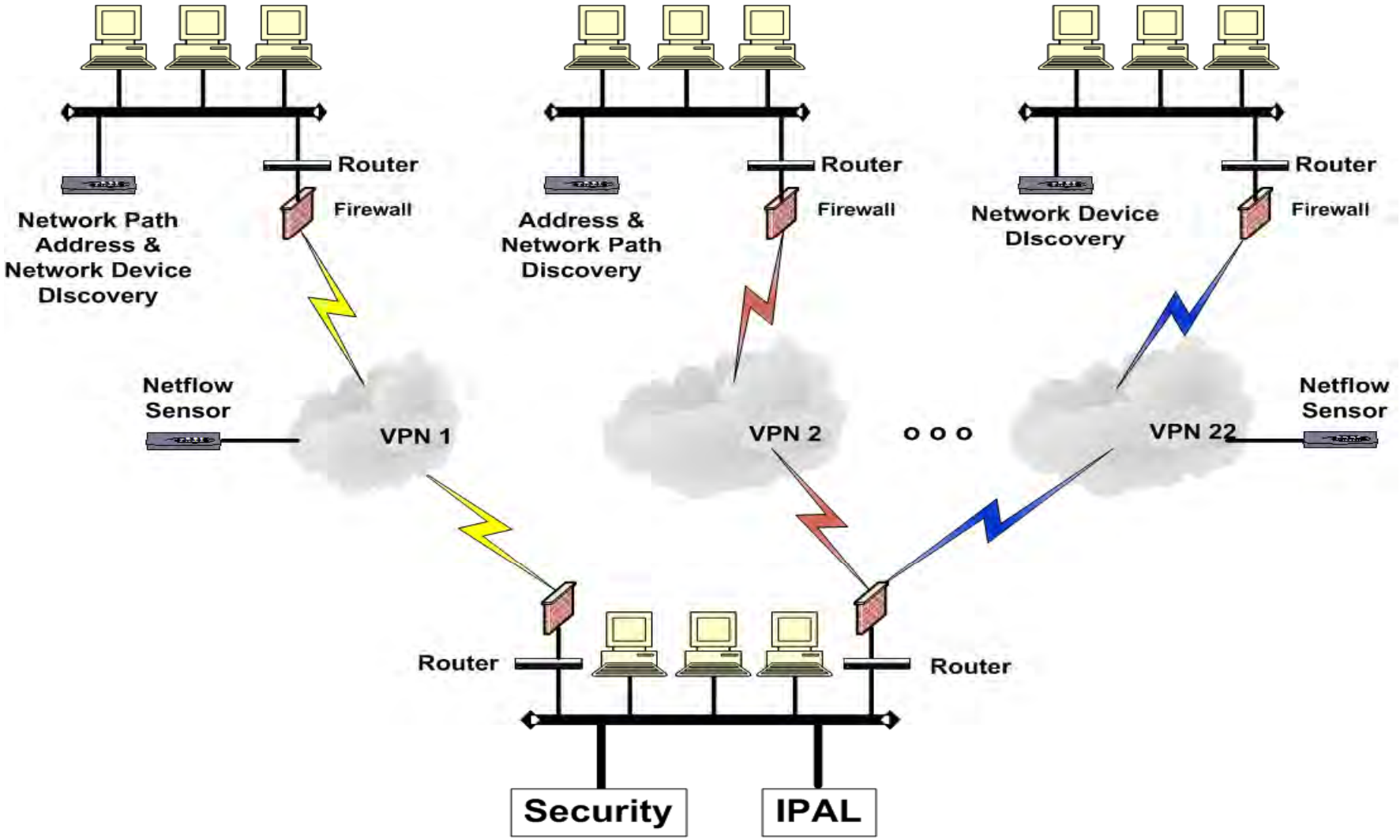
IP*al* MDD Architecture



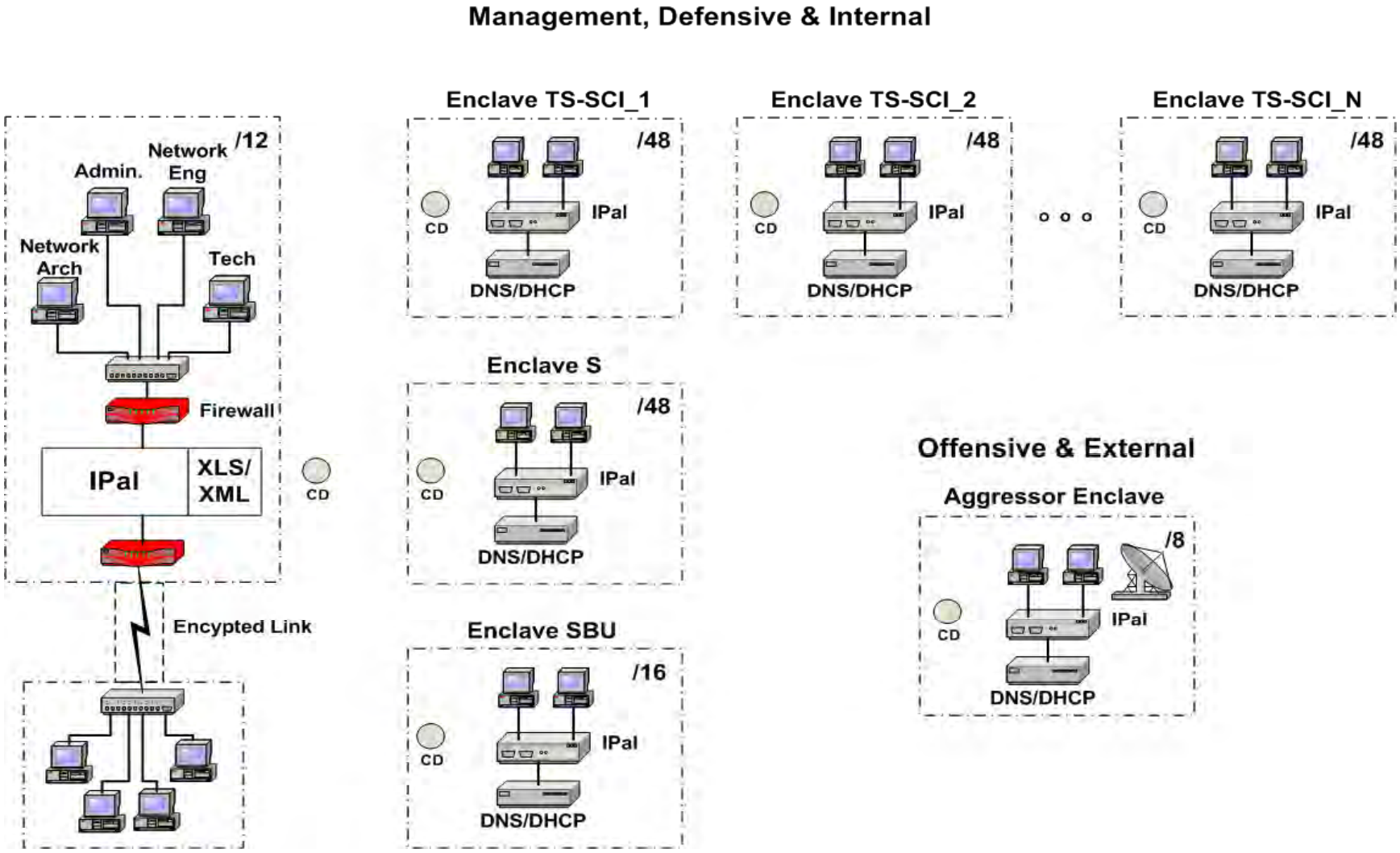
Network Discovery Issues



Distributed Sensor System



Independent Enclaves



Partial List, Authorized Resellers

- Various Contract Vehicles
  - GTSI
  - Iron Bow Technologies (formally Apptis)
- SDVOSB
  - Fedstore
  - Innovative Management Concepts (TS/SCI)
- 8(a)
  - Intellispring (GSA Holder)
- Small Business
  - Auspex Technologies, LLC

… The Extended Internet Associates Family