Putting
IPv6
to work

North American IPv6 Summit

Grand Hyatt, Denver, Colorado
September 23-25, 2014

Rocky Mountain IPv6 Task Force
RMv6TF

IPv6 Security and Unicorns

Staying with IPv4 or moving to IPv6 in the Security Operations Centers (SOC)

Joe Klein, CISSP…

Joe.Klein@Disrupt6.com

#JoeKlein +1.703.594.1419

DISRUPT6

"Next Generation Security for the Next Generation Internet"

Rocky Mountain IPv6 Task Force

RMv6TF

IPv6 Deployment Delay

“With IPv6, security products are the long pole in the tent”

- *Kris Strance, DoD CIO IPv6 Lead (2005)*

“USG IPv6 transition is being delayed due to a lack of IPv6 security products.”

- *Bob Gourley, CTO of Crucial Point (2014)*

“We added IPv6 to our product by upgrading the IP data field to 128 bits, now we can claim IPv6 support”

- Business Executive, Security Product Company (2014)

The Question…

Should your

Security Operations Center (SOC) ---

1. Do nothing,

2. Move to Dual Stack, or Native IPv6?

Definitions

Unicorn

- A mythical animal typically represented as a horse with a single straight horn projecting from its forehead

Rainbows and Unicorns (RU)

- A sarcastic expression of well-being used when confronted by a s**tstorm or a clusterf*** of magnificent and awe inspiring proportions. A series of painful incidents or unfortunate experiences.

Rainbows, Butterflies and Unicorns (RBUs)

- When a situation or expectations are unrealistic and one has to put on a ☺ regardless.

Definition

Security

- The state of being free from danger or threat
- The state of feeling safe, stable, and free from fear or anxiety

Cybersecurity RBU

- Measures taken to protect a computer or computer systems against unauthorized access or attack

Definition

Cyber Security Operations Center (C-SOC)

- Measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack
- Can be managed in-house or outsourced to Managed Security Service Providers (MSSP)
- Should be 24x7

Why your SOC needs IPv6!

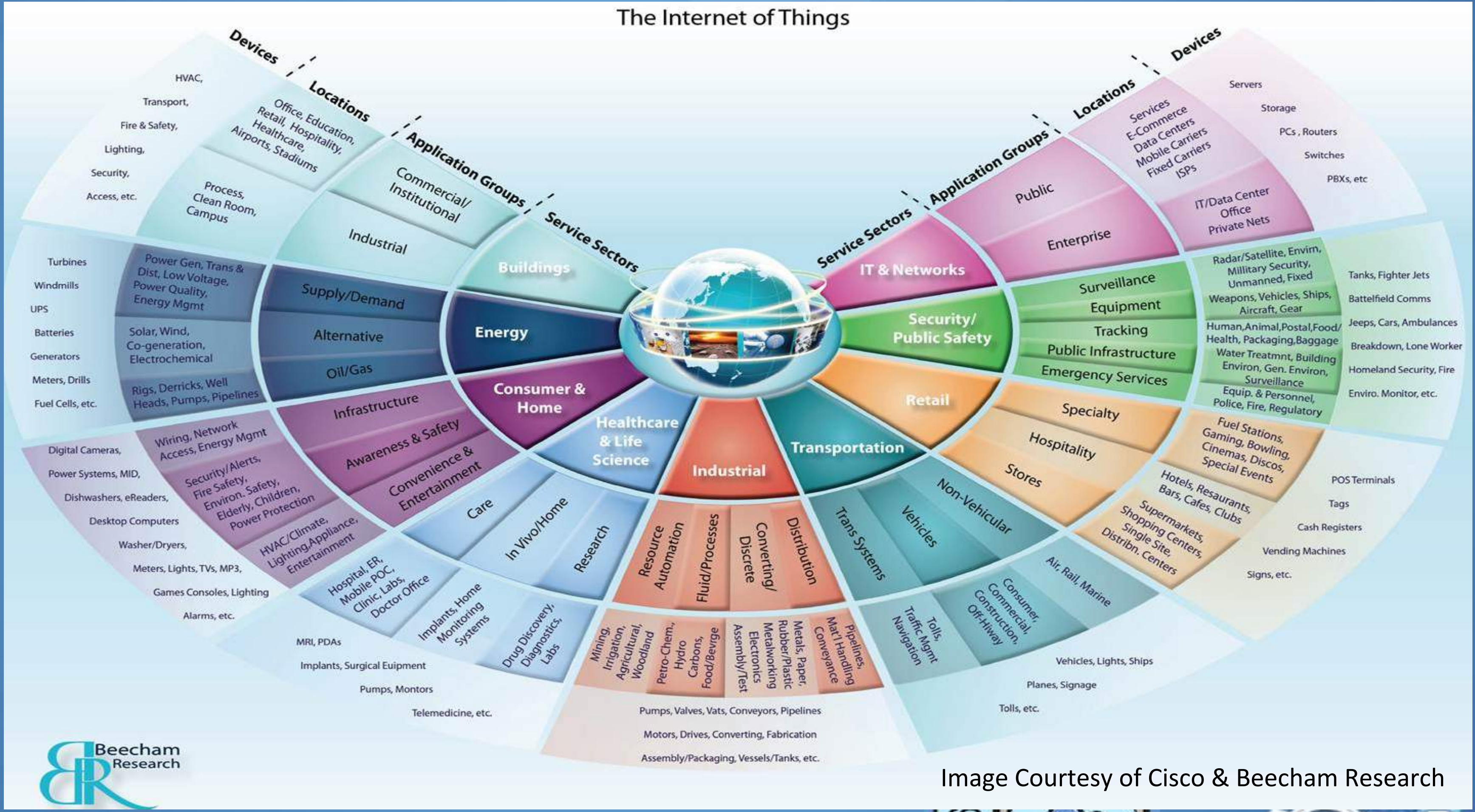

The Internet of Things
Devices
Locations
Application Groups
Service Sectors
HVAC,
Transport,
Fire & Safety,
Lighting,
Security,
Access, etc.
Office, Education, Retail, Hospitality, Healthcare, Airports, Stadiums
Process, Clean Room, Campus
Commercial/ Institutional
Industrial
Buildings
Turbines
Windmills
UPS
Batteries
Generators
Meters, Drills
Fuel Cells, etc.
Power Gen, Trans & Dist, Low Voltage, Power Quality, Energy Mgmt
Solar, Wind, Co-generation, Electrochemical
Rigs, Derricks, Well Heads, Pumps, Pipelines
Supply/Demand
Alternative
Oil/Gas
Energy
Digital Cameras,
Power Systems, MID,
Dishwashers, eReaders,
Desktop Computers
Washer/Dryers,
Meters, Lights, TVs, MP3,
Games Consoles, Lighting
Alarms, etc.
Wiring, Network Access, Energy Mgmt
Security/Alerts, Fire Safety, Environ. Safety, Elderly, Children, Power Protection
HVAC/Climate, Lighting,Appliance, Entertainment
Infrastructure
Awareness & Safety
Convenience & Entertainment
Consumer & Home
MRI, PDAs
Implants, Surgical Euipment
Pumps, Montors
Telemedicine, etc.
Hospital, ER, Mobile POC, Clinic, Labs, Doctor Office
Implants, Home Monitoring Systems
Drug Discovery, Diagnostics, Labs
Care
In Vivo/Home
Research
Healthcare & Life Science
Resource Automation
Fluid/Processes
Converting/ Discrete
Distribution
Mining, Irrigation, Agricultural, Woodland
Petro-Chem., Hydro Carbons, Food/Bevrge
Metals, Paper, Rubber/Plastic Metalworking Electronics Assembly/Test
Pipelines, Mat'l Handling Conveyance
Pumps, Valves, Vats, Conveyors, Pipelines
Motors, Drives, Converting, Fabrication
Assembly/Packaging, Vessels/Tanks, etc.
Industrial
Trans Systems
Vehicles
Non-Vehicular
Tolls, Traffic Mgmt Navigation
Consumer, Commercial, Construction, Off-Hiway
Air, Rail, Marine
Vehicles, Lights, Ships
Planes, Signage
Tolls, etc.
Transportation
Specialty
Hospitality
Stores
Fuel Stations, Gaming, Bowling, Cinemas, Discos, Special Events
Hotels, Resaurants, Bars, Cafes, Clubs
Supermarkets, Shopping Centers, Single Site, Distribn. Centers
POS Terminals
Tags
Cash Registers
Vending Machines
Signs, etc.
Retail
Surveillance
Equipment
Tracking
Public Infrastructure
Emergency Services
Radar/Satellite, Envim, Millitary Security, Unmanned, Fixed
Weapons, Vehicles, Ships, Aircraft, Gear
Human,Animal,Postal,Food/ Health, Packaging,Baggage
Water Treatmnt, Building Environ, Gen. Environ, Surveillance
Equip. & Personnel, Police, Fire, Regulatory
Tanks, Fighter Jets
Battelfield Comms
Jeeps, Cars, Ambulances
Breakdown, Lone Worker
Homeland Security, Fire
Enviro. Monitor, etc.
Security/ Public Safety
Public
Enterprise
Services E-Commerce Data Centers Mobile Carriers Fixed Carriers ISPs
IT/Data Center Office Private Nets
Servers
Storage
PCs , Routers
Switches
PBXs, etc
IT & Networks
Beecham Research

Image Courtesy of Cisco & Beecham Research

CAUTION
Legacy IP Only
This product does not support the current generation of the Internet Protocol, IPv6.

Impact on SOC operations, staying on IPv4

CAUTION
Legacy IP Only
This product does not support the current generation of the Internet Protocol, IPv6.

- IPv4 BGP Routing and Internal/IGP routing; Packet Filtering
- Security Products, Tools & Services
- CGN & Tunnels
  - Loss of threat intel
  - Loss of geo-location
  - Broken Applications
  - Legal discovery
  - New 'state' challenges
- Outsourced Services

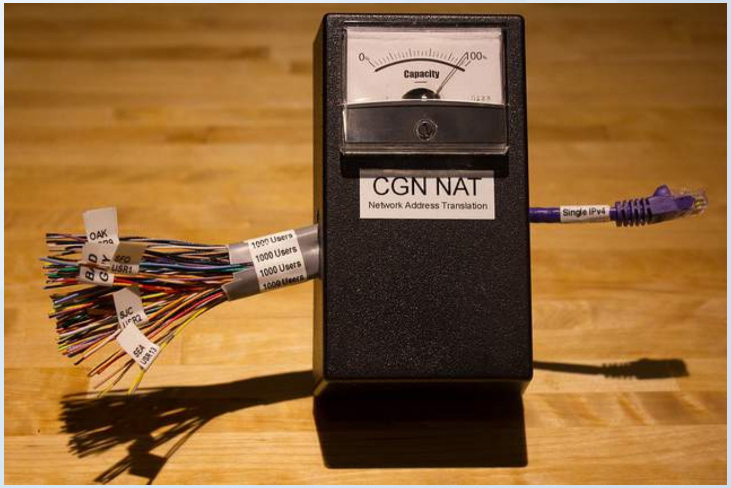
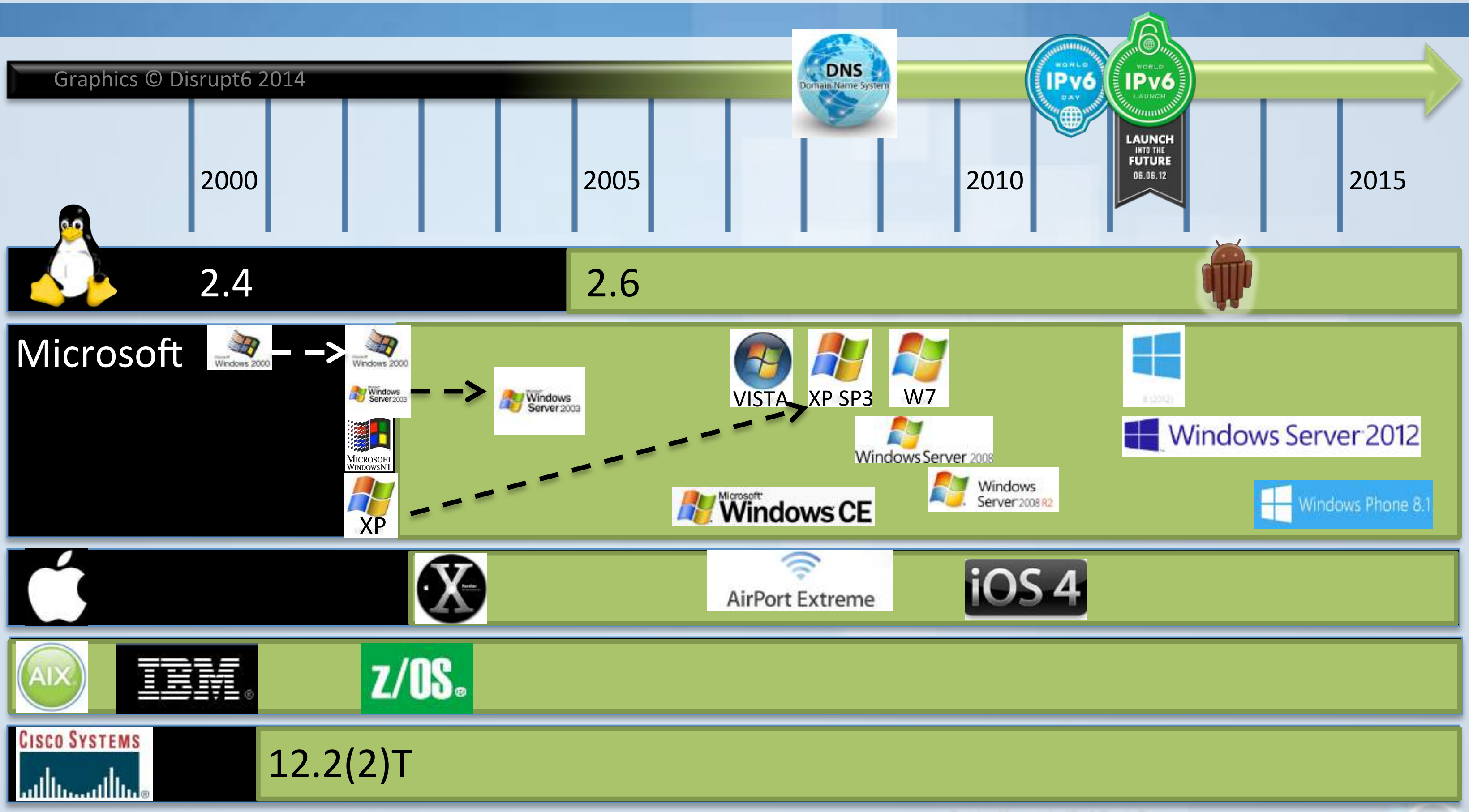


Photo by Jason Fesler - http://flic.kr/p/bhDoxg

Why your SOC needs IPv6: Operating System Rollout



Graphics © Disrupt6 2014

2000 | 2005 | 2010 | 2015

DNS Domain Name System

World IPv6 Day

World IPv6 Launch — LAUNCH INTO THE FUTURE 06.06.12

2.4 | 2.6

Microsoft: Windows 2000 → Windows 2000; Windows Server 2003 → Windows Server 2003; Microsoft Windows NT; XP → XP SP3; VISTA; W7; Windows Server 2008; Windows Server 2008 R2; Microsoft Windows CE; 8 (2012); Windows Server 2012; Windows Phone 8.1

AirPort Extreme | iOS 4

AIX | IBM | z/OS

Cisco Systems | 12.2(2)T

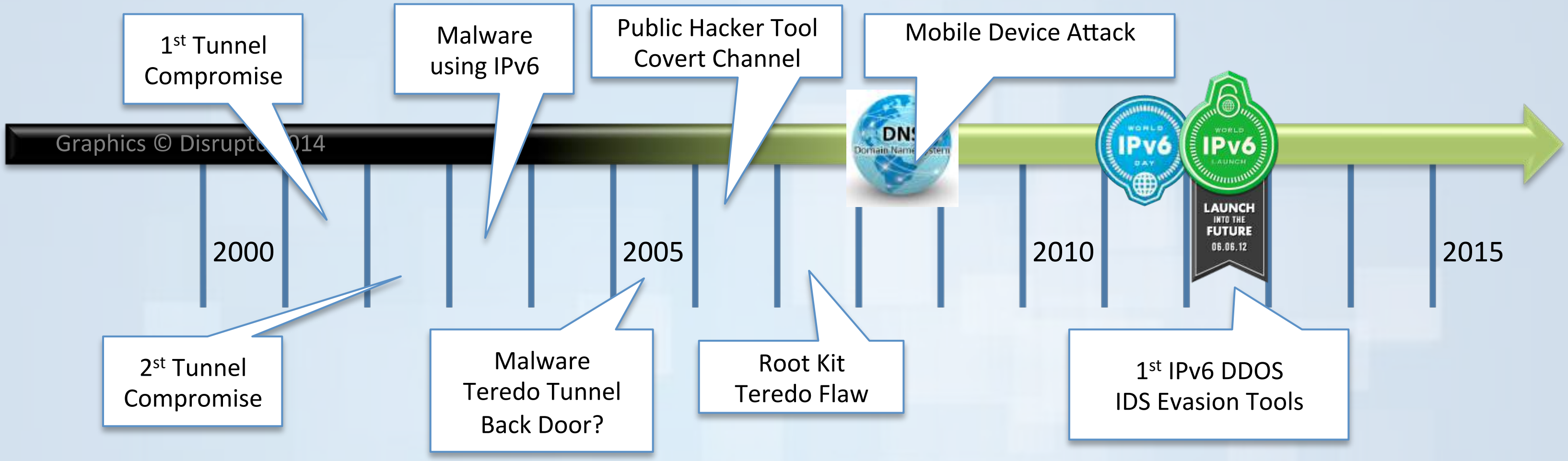
■ IPv6 Capable | 🟩 IPv6 Enabled

Rocky Mountain IPv6 Task Force

RMv6TF

DISRUPT6

Why your SOC needs IPv6:
IPv6 Attacks & Vulnerabilities



Graphics © Disrupt6 2014

1st Tunnel Compromise

2st Tunnel Compromise

Malware using IPv6

Malware Teredo Tunnel Back Door?

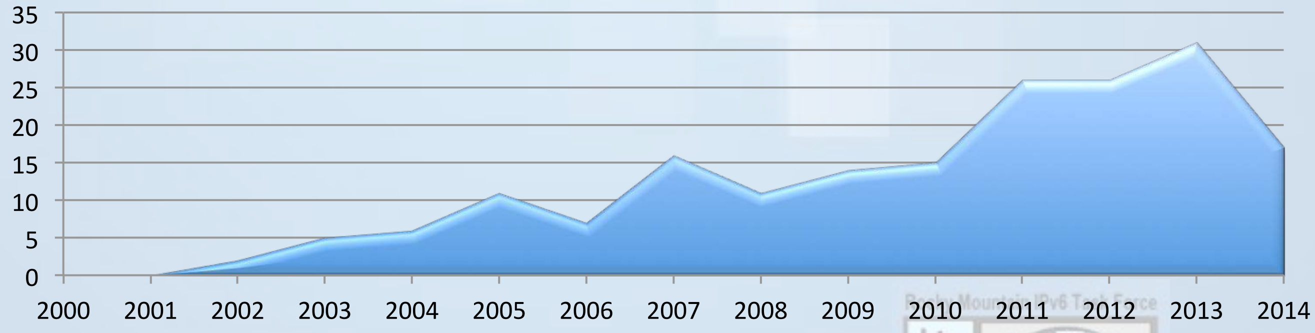
Public Hacker Tool Covert Channel

Root Kit Teredo Flaw

Mobile Device Attack

1st IPv6 DDOS IDS Evasion Tools

Published IPv6 Vulnerabilities



Answer

Should your

Security Operations Center (SOC) ---

1. Do nothing,

2. Move to Dual Stack, or Native IPv6?

Pick #2, move to dual stack today!

Question

Will a dual-stack environment help us to close tickets faster?

Closing Tickets Faster - External

The problem with IPv4, since RFC 1918:

- Addresses: 212.23.16.4 & 17.126.66.253
  - Is this address on the Bogon List?
  - Which RIR allocated the address?
  - Is this a NAT device or an endpoint?
  - Can you identify the subnet for the last hop router?
  - Can you identify the number of addresses on that segment?

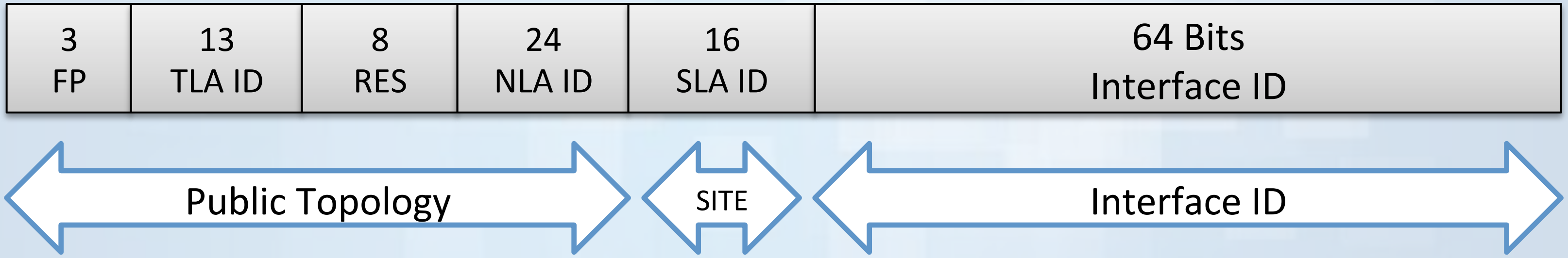
Rocky Mountain IPv6 Task Force

RMv6TF

DISRUPT6

Closing Tickets Faster - External

The benefit of IPv6 end-to-end & hierarchical sparse address allocation:



3	13	8	24	16	64 Bits
FP	TLA ID	RES	NLA ID	SLA ID	Interface ID

Public Topology

SITE

Interface ID

FP	Format Prefix (001)
TLA ID	Top-Level Aggregation Identifier
RES	Reserved for future use
NLA ID	Next-Level Aggregation Identifier
SLA ID	Site-Level Aggregation Identifier
INTERFACE ID	Interface Identifier

Closing Tickets Faster - Internal

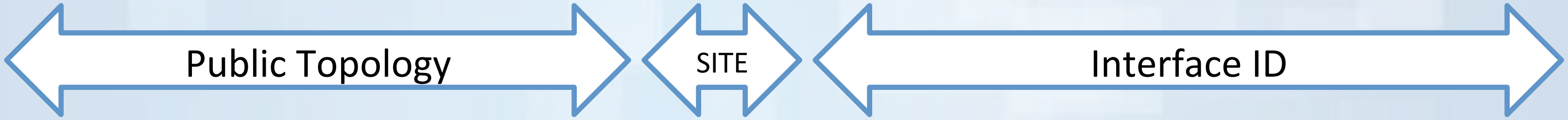
Problem with IPv4, since RFC 1918

- Addresses: 10.23.16.4 & 10.126.66.253
  - Is this a NAT device or an endpoint?
  - Can you identify the subnet for the last hop router?
  - Can you identify the number of addresses on that segment?
  - What is the MAC address of this device?

Closing Tickets Faster - Internal

- The benefit an address plan, IPv6 end-to-end connections & EUI-64:

3 FP	13 TLA ID	8 RES	24 NLA ID	16 SLA ID	64 Bits Interface ID



Public Topology:

- Same Unicast address for all devices

SLA ID:

- Address Planning via IPAM tool

INTERFACE ID

- Interface Identifier

::1610:9fff:fe3a:a812

Step 1: 16:10:9f:3a:a8:12

Step 2: 14:10:9f:3a:a8:12

Apple Device

Question

What are four things I can do to begin moving to a dual stack environment?

Rocky Mountain IPv6 Task Force

RMv6TF

DISRUPT6

Decide on how to upgrade?

1. ***Add IPv6 features to existing systems and processes***
    - **Advantage:**
        - Less costly, requires minimal changes in processes, only upgrade products that must be upgraded
2. ***Upgrade to dominant IPv6 features, and map IPv4 features and addresses:***
    - **Advantage:**
        - Opportunity to redesign from an IPv6 viewpoint, and stream line and simplify integration and processes
        - Better long term results and lower costs

IPv6 Training for Key People

- **People that require training:**
  - SOC Manager
  - Security Architect
  - SOC Analyst – multiple levels
  - Firewall/Router/Proxy admin
  - HIDS/AV Admin
  - Database Administrator
  - Developers
  - Red, Blue and Scan Teams
  - Email filter manager
  - Threat Intelligence Analysis
  - Forensics analysts and reverse engineers
  - Help Desk
- **Reference:** National Cybersecurity Workforce Framework, http://niccs.us-cert.gov/training/tc/framework

IPv6 SOC Technology Inventory

Standard Security Coverage

- Routers & Switches
- Firewall
- Proxy Servers
- NIDS / NIPS
- HIDS/Host AV + Firewalls
- Endpoint Security
- NAC/NAP
- DLP
- VPN
- Encryption
- UTM (unified threat mgmt)

Unified Visibility Portal

Security Event Analysis Framework

Log Management

Other Devices to Cover

- Unix/Linux/Wintel Systems
- Web Server Apps
- Database/Big Data servers
- IAM Server
- AAA Servers & Services
- Anti Virus monitoring
- Vulnerability Scanners
- Mainframe/BYOD
- Content Filters
- E-Mail Security
- Patch Management
- 'Unmanaged" Mobile/BYOD
- External/Outsources services

IPv6 SOC Virtual Lab

Justification:

- Test and validate security devices, applications and scripts, otherwise you have to trust the vendor

Platform:

- Virtual Box, VMWare, GNS3, Ubuntu, Kali Linux

Tools:

- Scapy, THC-IPv6, SI6 Networks' IPv6 Toolkit, Security Onion, Microsoft OS licenses

Environment:

- Add ‘dev/test’ environment which replicates your production services and management platforms/tools

Final Thought

“We manage [cyber] security through
either leadership or crisis.
In the absence of leadership,
we are left with crisis.”

- *Matthew Rosenquist*

*“Don’t allow IPv6 to become
your cybersecurity crisis”*

- Joe Klein

Thank you

Joe Klein

Joe.Klein@Disrupt6.com

#JoeKlein +1.703.594.1419

Rocky Mountain IPv6 Task Force

RMv6TF

DISRUPT6