IPv6 is Here. Is Your Network Secure?

August 9, 2011

Jeremy Duncan

Senior Director & IPv6 Network Architect

Salient Federal Solutions

2610:f8:ffff:2011:06:08::1

SALIENT FEDERAL SOLUTIONS

Capabilities

Information technology and engineering services in intelligence, defense, homeland security and cyber security domains

Headquartered in Fairfax, Virginia

16 offices and 141 locations across the U.S. and overseas.

Over 800 employees

300+ Employees with TS/SCI or higher clearances

Acquired SGIS and Command Information

SALIENT FEDERAL SOLUTIONS

Cyber Attacks: Frequent and Costly

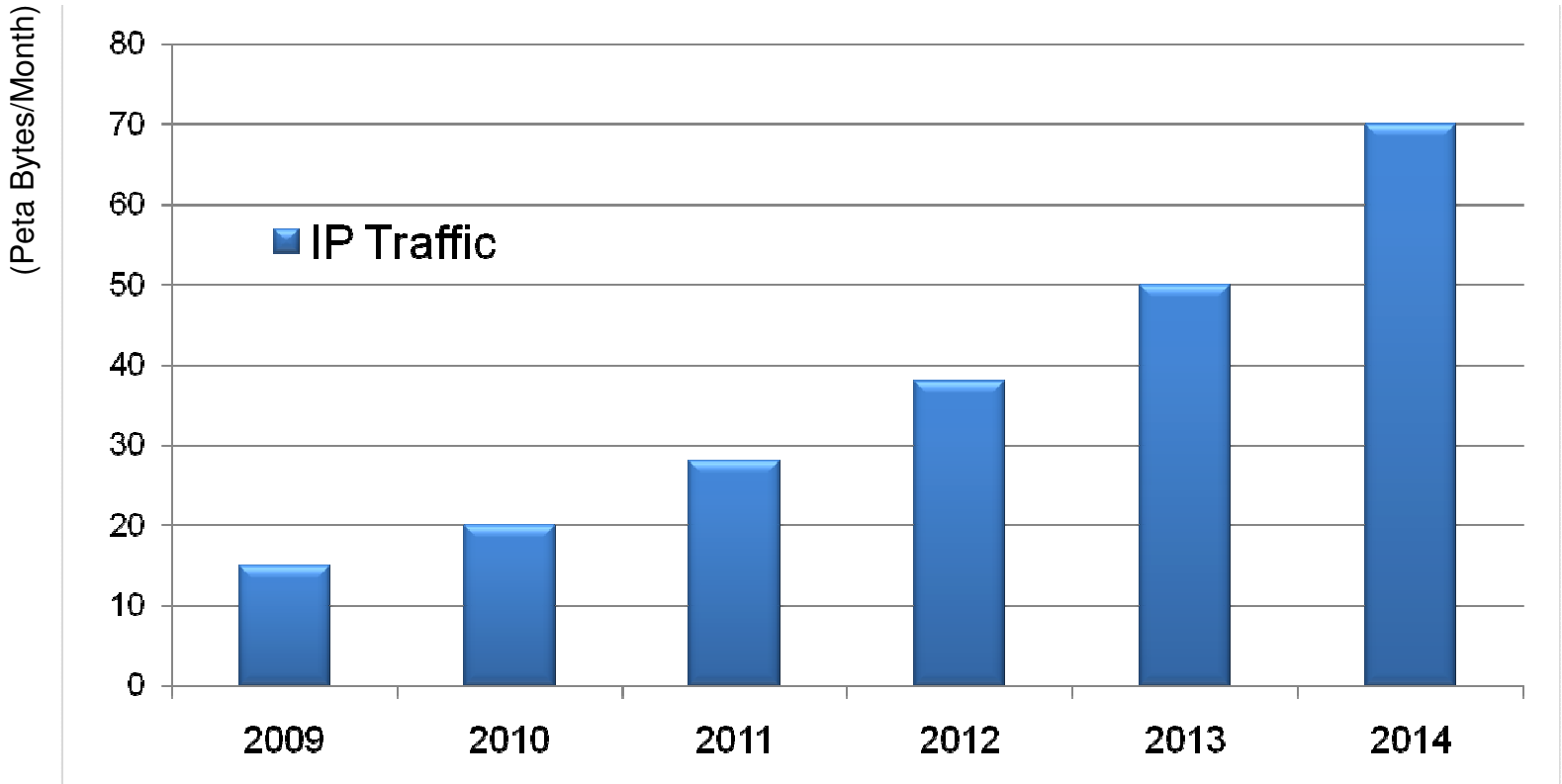
"The number of probes Defense experiences a day almost matches the number of military computers. [That's] 250,000 attacks an hour, 6 million a day, or 2.19 billion a year."

–General Keith Alexander
U.S. Cyber Command

"The cost of the downtime caused by cyber attacks is high, according to the study. For corporations, the average cost is $6.3 million a day."

–World Economic Forum

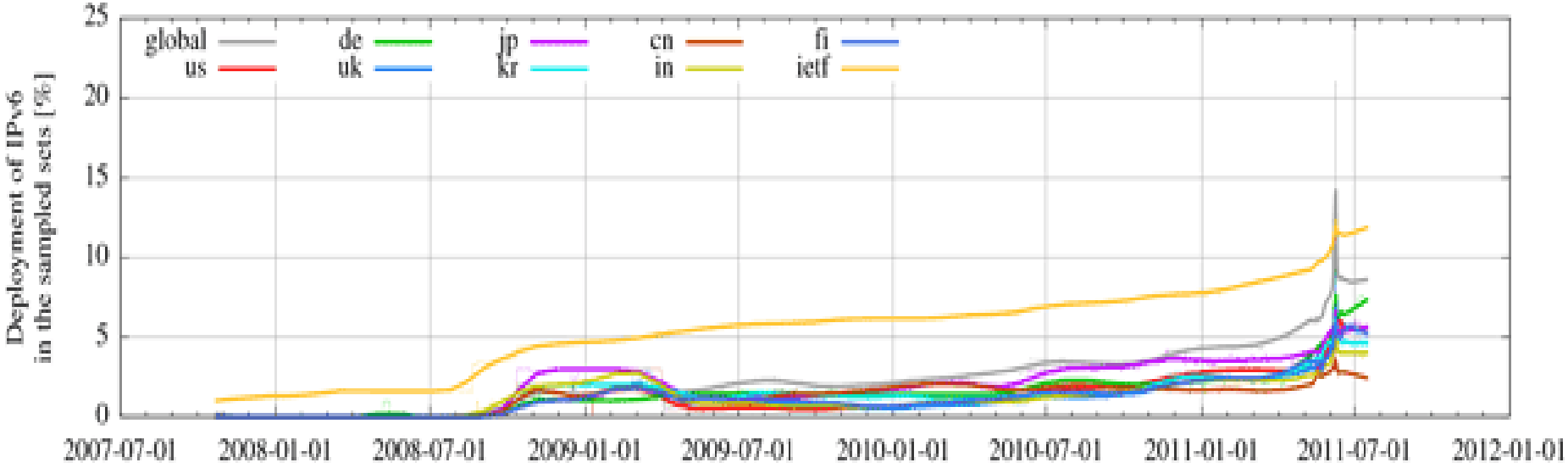
Every Year, There's More to Defend



Source: Ovum, IDC, Gartner

And IPv6 Traffic Grew 1,400% in the Last 12 Months…

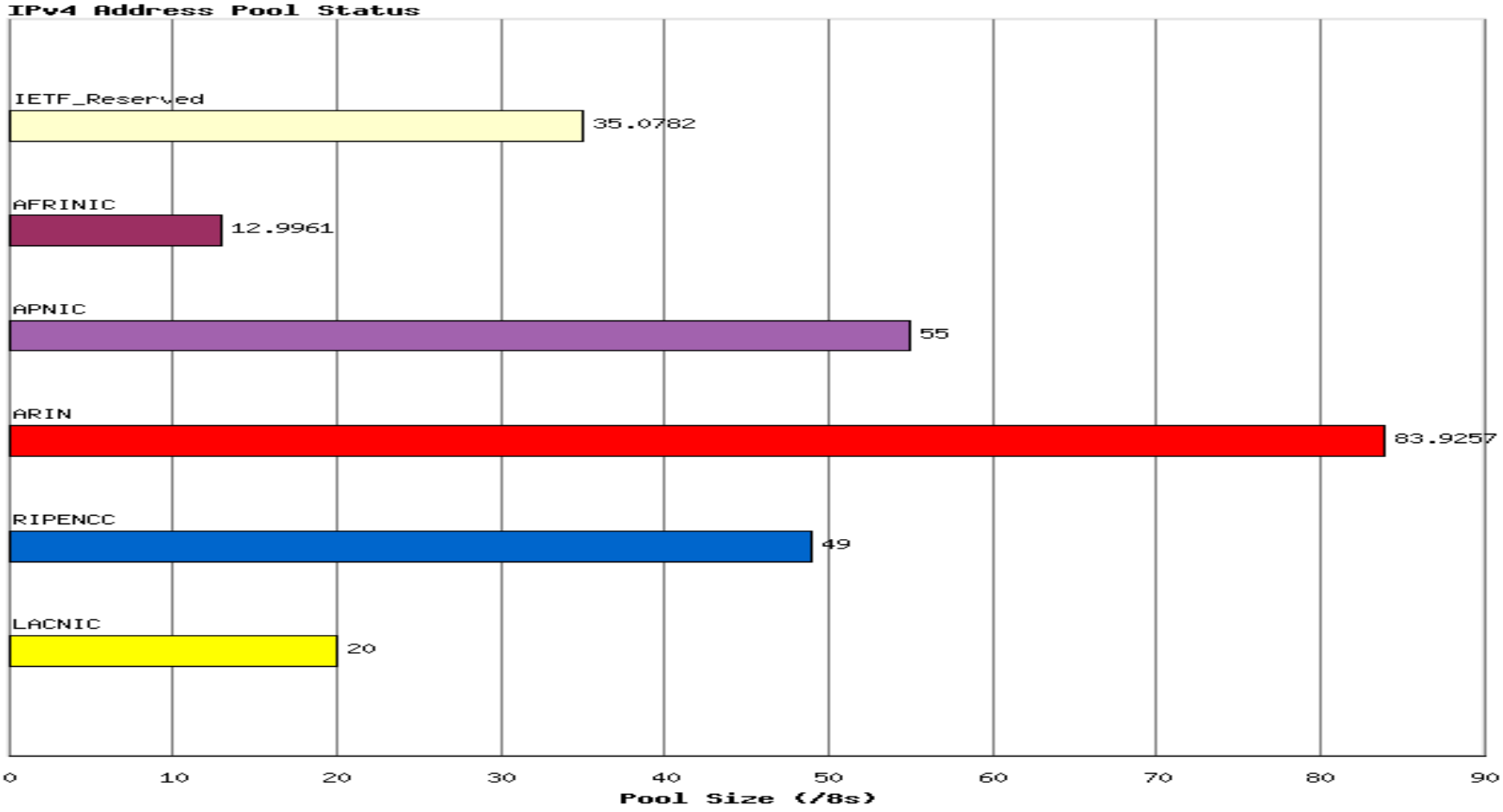
Every Year, There's More to Defend (cont.)



Source: https://fit.nokia.com/lars/meter/data/ipv6.pdf

The amount of registered AAAA grew 100% in one year

How much IPv4 is left?



Source:http://www.potaroo.net/tools/ipv4/

IPv4 RIR Projected Exhaustion

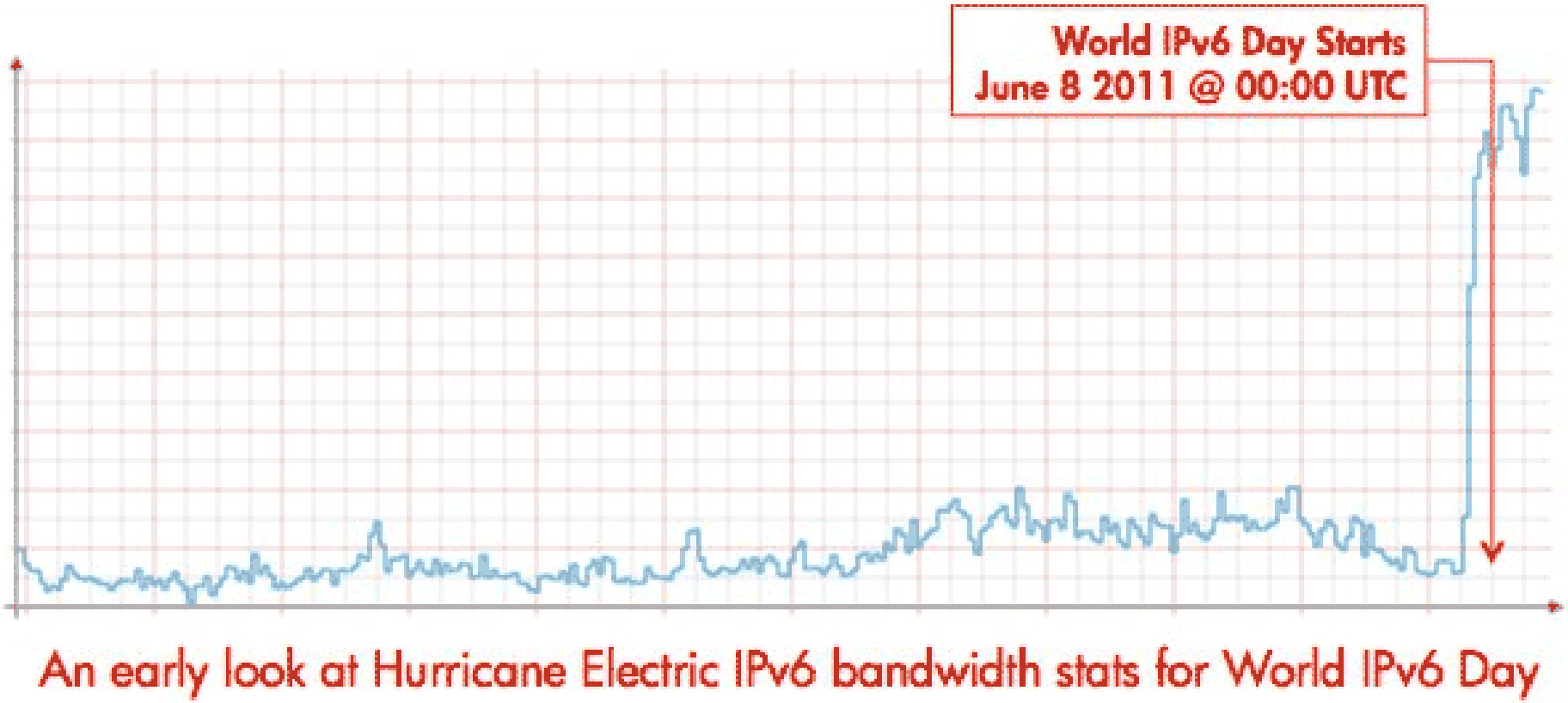
- APNIC (Asia Pacific NIC) → **NOW (last /8)**
- RIPENCC (Europe NIC) → **1 March 2012**
- AFRINIC (Africa NIC) → **4 August 2012**
- ARIN (North America NIC) → **23 Nov 2012**
- LACNIC (Latin America NIC) → **30 Apr 2014**

Source:http://www.potaroo.net/tools/ipv4/

June 8th, 2011 – World IPv6 Day

- Led by the Internet Society, 24 hour period where all the big content providers enabled IPv6 on their publically facing website:
  - Google
  - Facebook
  - Yahoo
  - Verizon
  - Bing
  - CNN
  - Salient Federal Solutions

June 8th, 2011 – World IPv6 Day



IPv6 utilization shot up to sustained 1Gbps globally

World IPv6 Day: What did we learn?

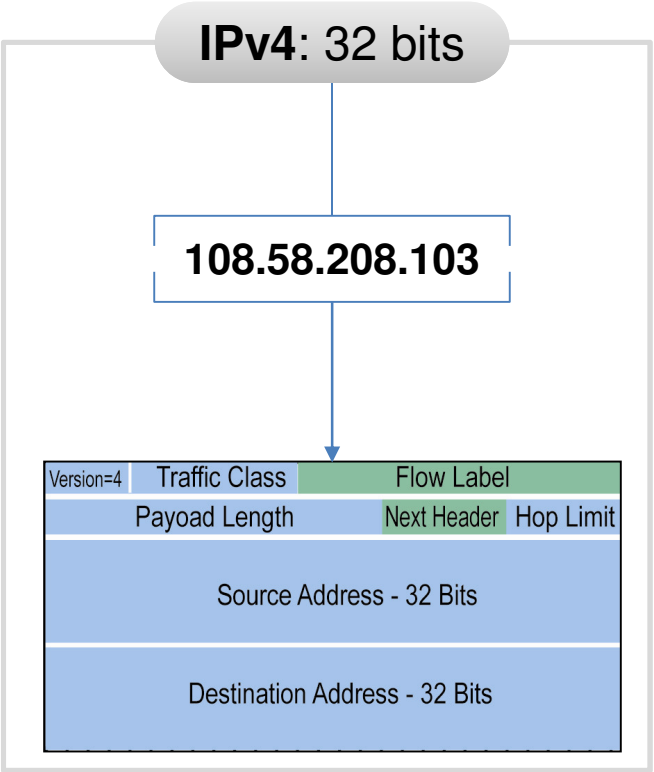
- IPv6 didn’t kill the Internet
- Some IPv6 Path MTU issues
- Native IPv6 penetration still low (30-35%)
- IPv6 tunneling represented 65-70% of all IPv6 traffic during the 24 hour test

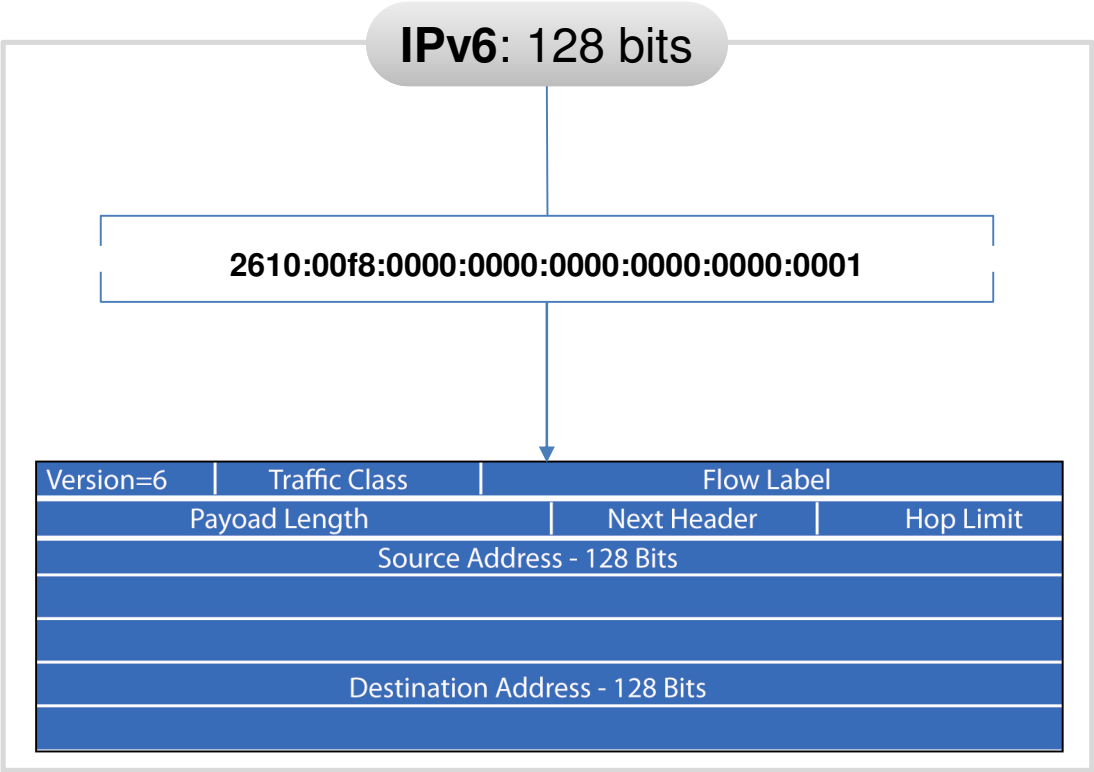
The US Government Path Forward

OMB memo (9/28/2010) requires agencies to:

- Upgrade public/external facing servers and services (e.g. web, email, DNS, ISP services, etc) to operationally use native IPv6 by the end of FY 2012;
- Upgrade internal client applications that communicate with public Internet servers and supporting enterprise networks to operationally use native IPv6 by the end of FY 2014;
- Designate an IPv6 Transition Manager to lead the agency's IPv6 transition activities, and liaison with the wider Federal IPv6 effort as necessary; and,
- Ensure agency procurements comply with FAR requirements for use of the USGv6 Profile and Test Program for the completeness and quality of their IPv6 capabilities.

IPv6 Adds Functionality
But Also Vulnerabilities





Attack Surfaces

IP-HTTPS Tunnels

IPv4 + IPv6

IPv4 over IPv6 tunnels

IPv4

IPv6

UDP/TCP tunnels

IPv6 over IPv4 tunnels

NAT64

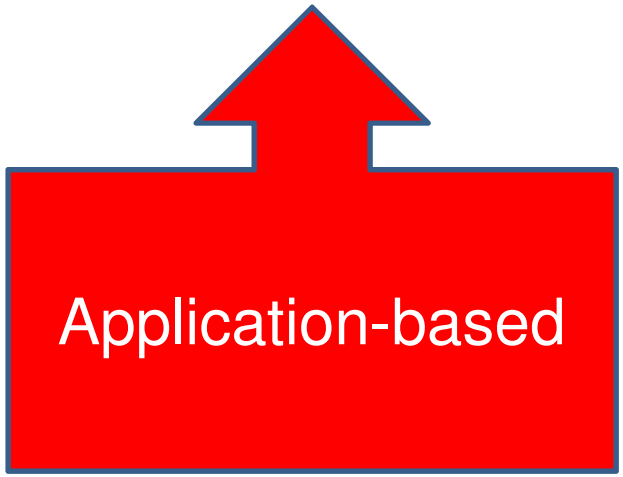
Tunnels (GRE, etc)

Encryption tunnels

DS-Lite

Known IPv4 Vulnerabilities

- PHP & SQL injection
- Distributed Denial of Service (DDoS)
- Bot Nets
- Spyware/Adware



Known IPv6 Vulnerabilities

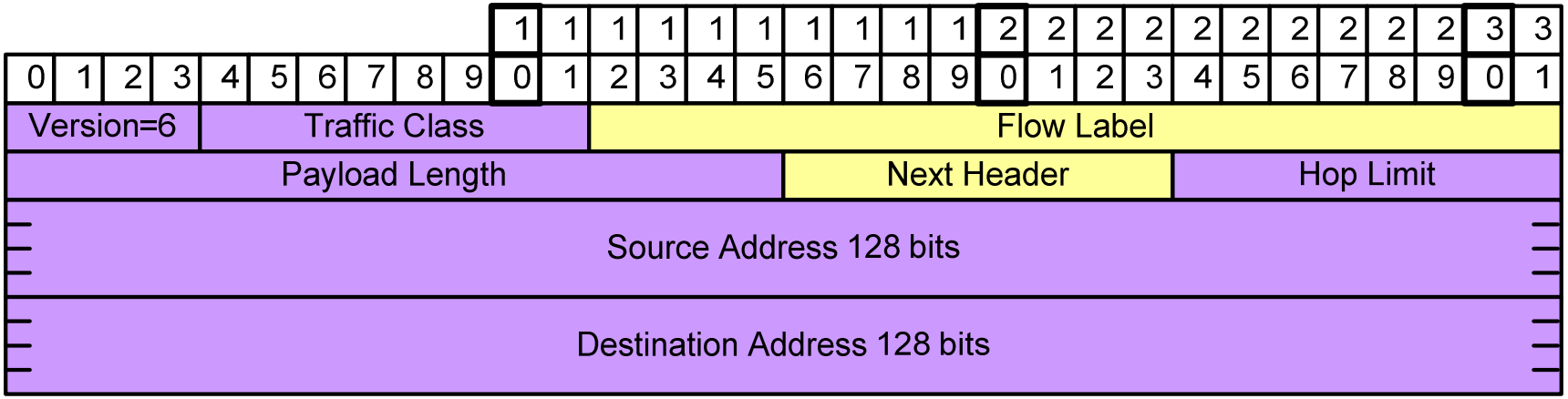
- IPv6 header vulnerabilities
- IPv6 extension header vulnerabilities
- Rouge RA attacks
- IPv4 in IPv6 tunnels (many types)
- All the other IPv4 application vulnerabilities

Network & Application based!

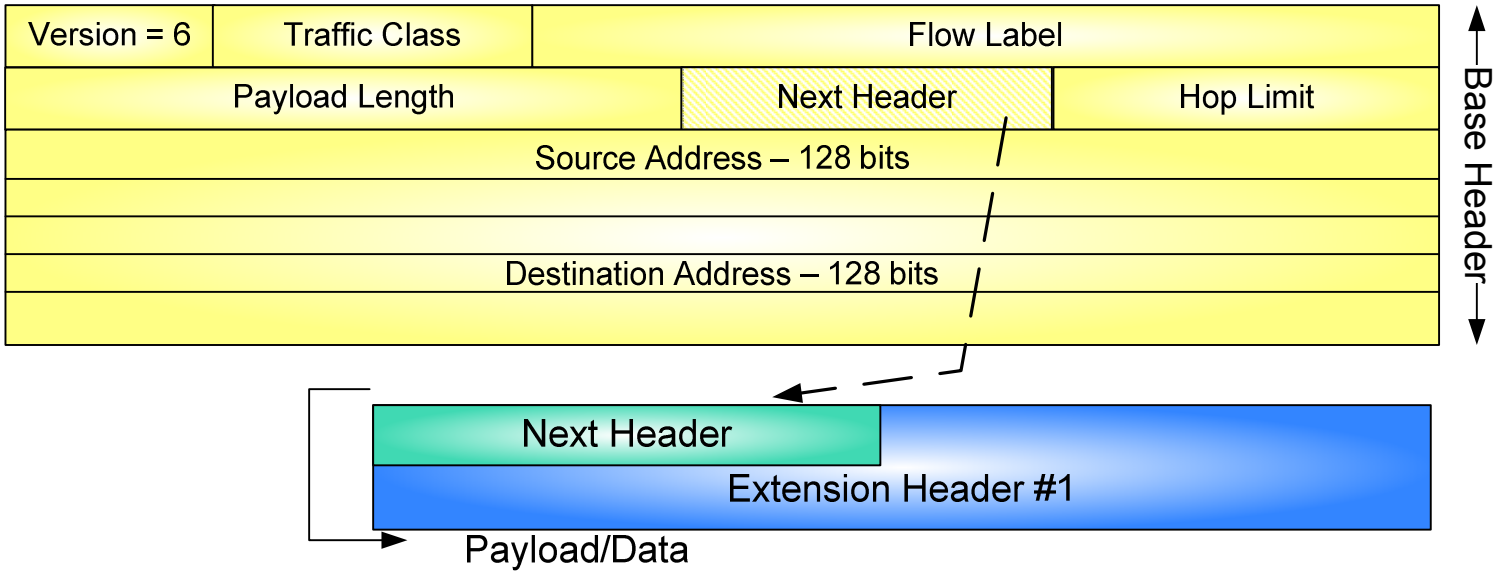
The IPv6 Header is *completely* different

IPv4 Header

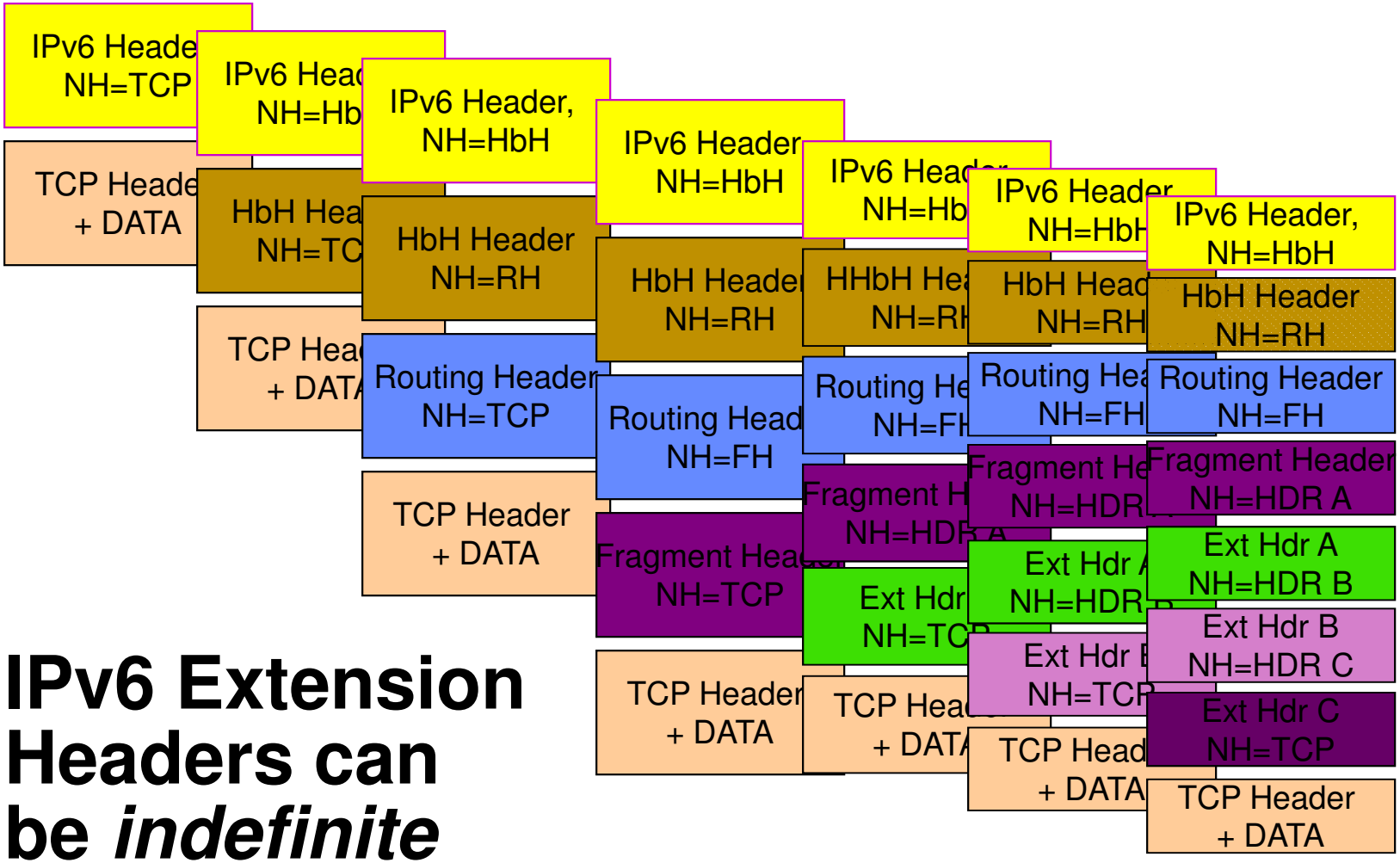
IPv6 Header



IPv6 Extension Headers



- IPv6 uses Extension headers to replace the functionality of the "options" field from IPv4
- All extension header information is within the payload, and not the IPv6 base header
- The "Next Header" field in the IPv6 base header identifies the Extension header to follow

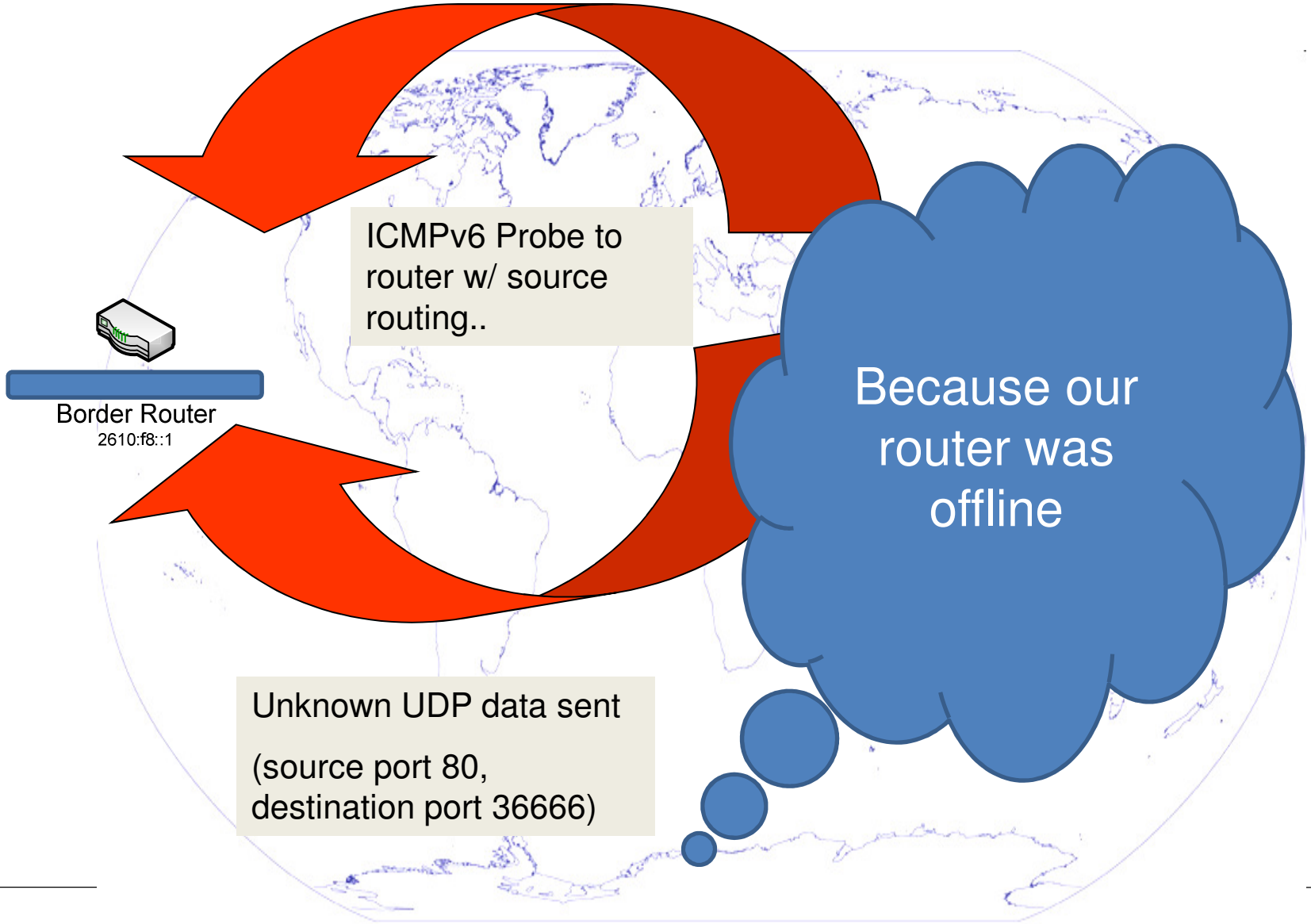


IPv6 Extension Headers can be *indefinite*

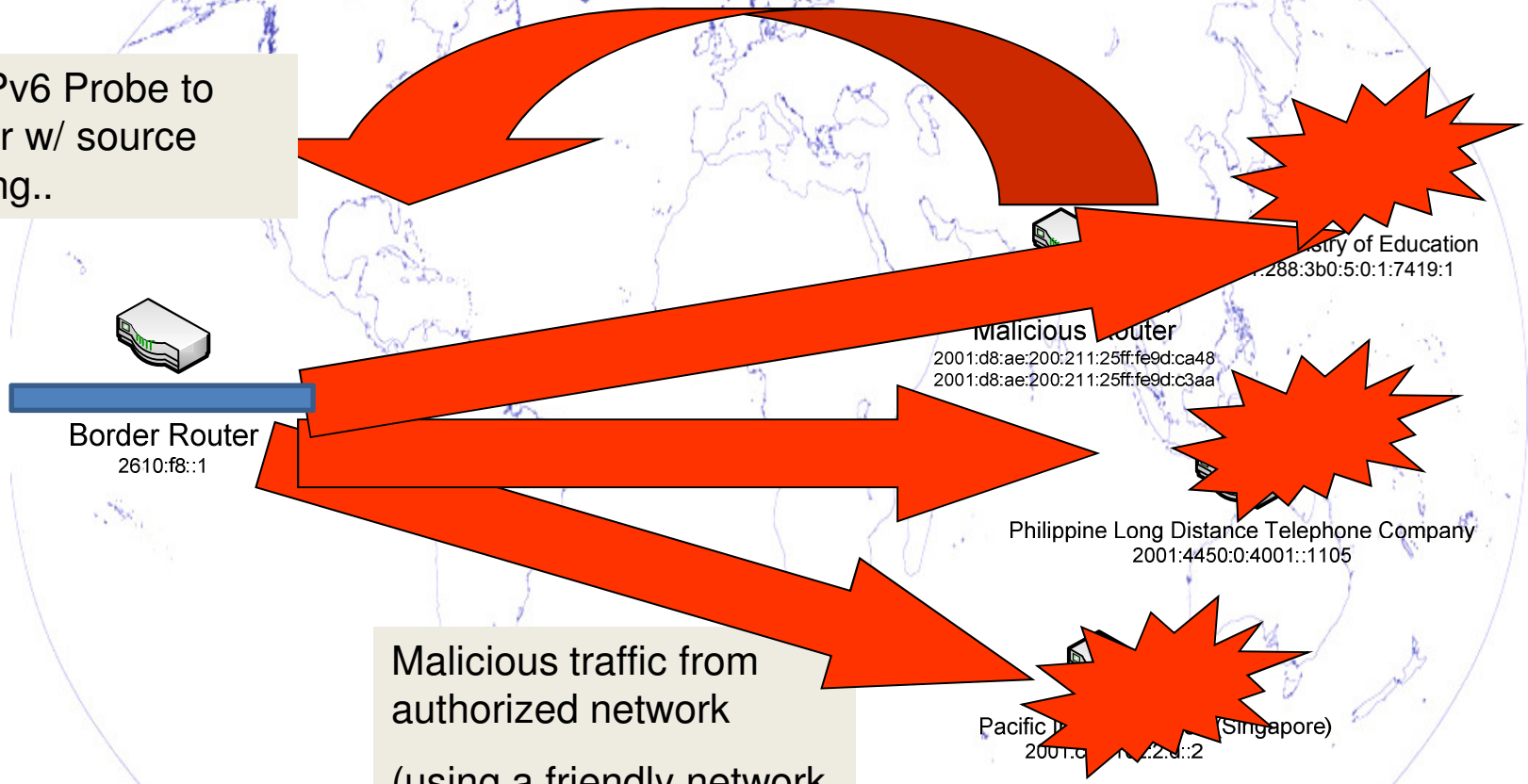
Real-World IPv6 Attack Vectors

- Example # 1: Router Header Type 0
- Example # 2 : IPv6 tunnels & what can be done
- Example # 3: IPv4 AAAA DNS queries
- Example # 4: Rouge Router Advertisements

Example #1: Routing Header Type 0



If the router had been online…

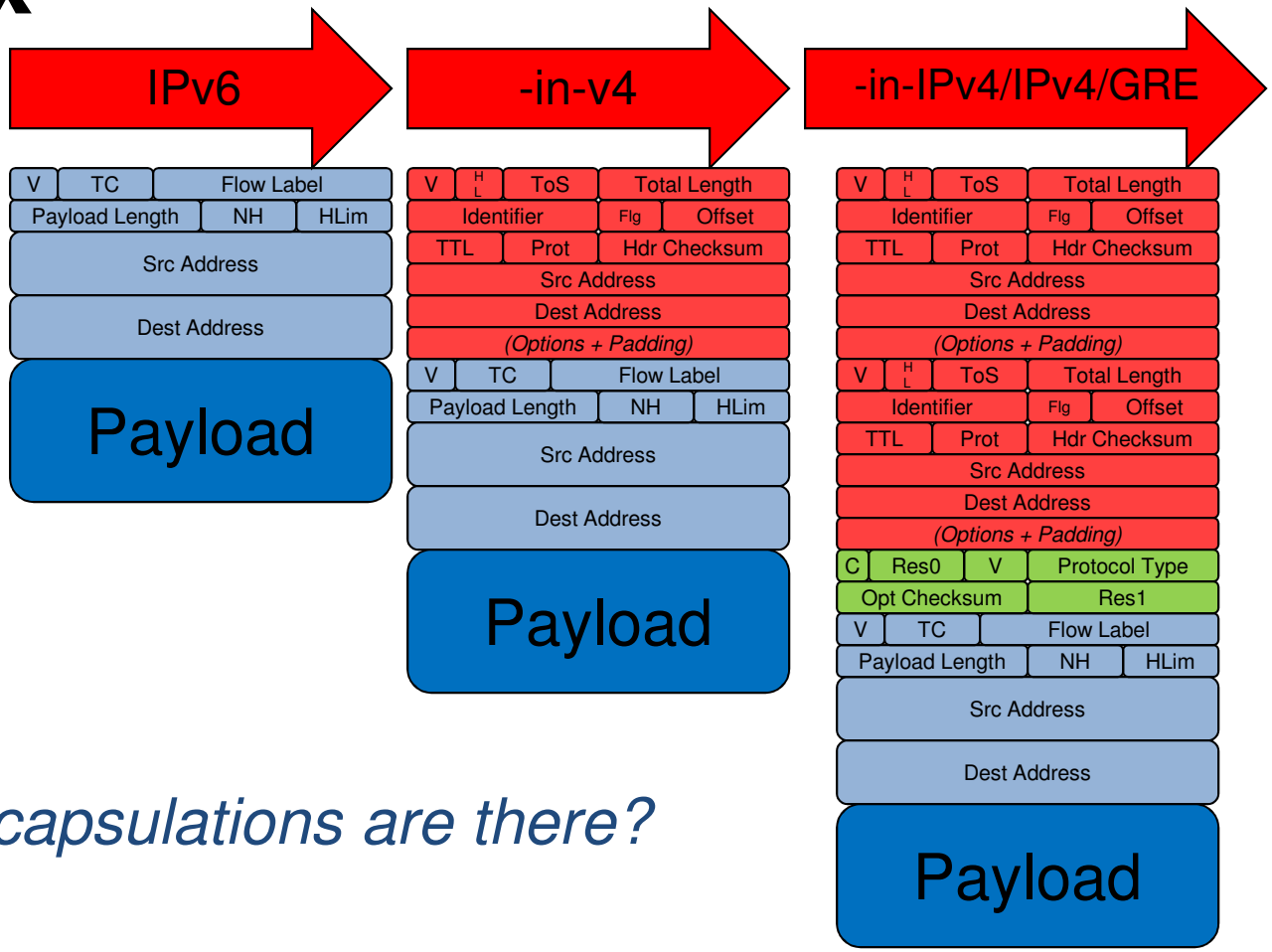


Example #2: IPv6 Tunnels

IPv6 Tunnels are a Transition Mechanism

- Protocol 41 and 47 Tunnels
  - 6in4
  - 6to4
  - 6RD
  - IPv6 in GRE
  - Dual-Stack Lite
- UDP Based Tunnels
  - Teredo (Port 3544)
  - AYIYA (Port 5072)
  - TIC (Port 3874)
  - TSP (Port 3653)
- TCP Based Tunnels
  - IP-HTTPS (Microsoft Direct Access)

Tunneled Packet Processing is Complex



How many encapsulations are there?

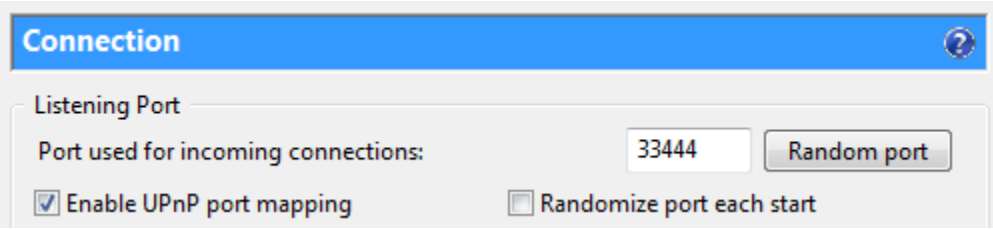
Tunnels Need to be Protected

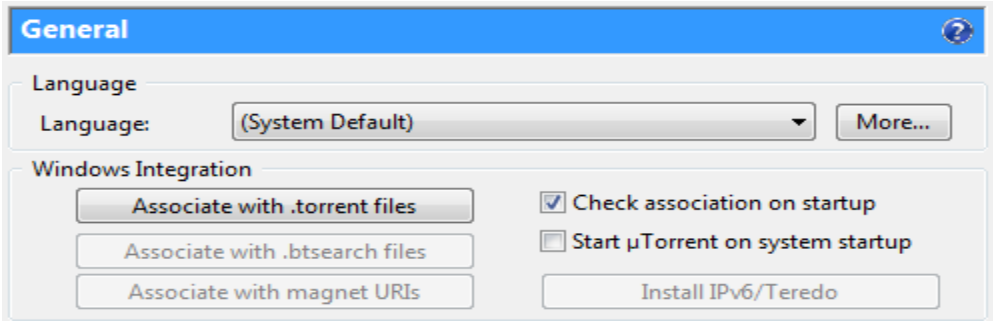
- ACLs can protect against Protocol 41, 47, IPSec and port specific UDP traffic
- What if you don't know the Port?
  - Miredo: Teredo can be configured to run on any port
  - GoGoNet6: TSP can listen on any UDP port (ie 53, 80, 443, etc)
  - Microsoft Direct Access will use all of them (6to4, Teredo, IP-HTTPS)

uTorrent – Teredo and IPv6-Capable

- Uses ephemeral port for connections
- User may randomly choose port
- Port may be randomly chosen on restart
- IPv6 support “on by default”

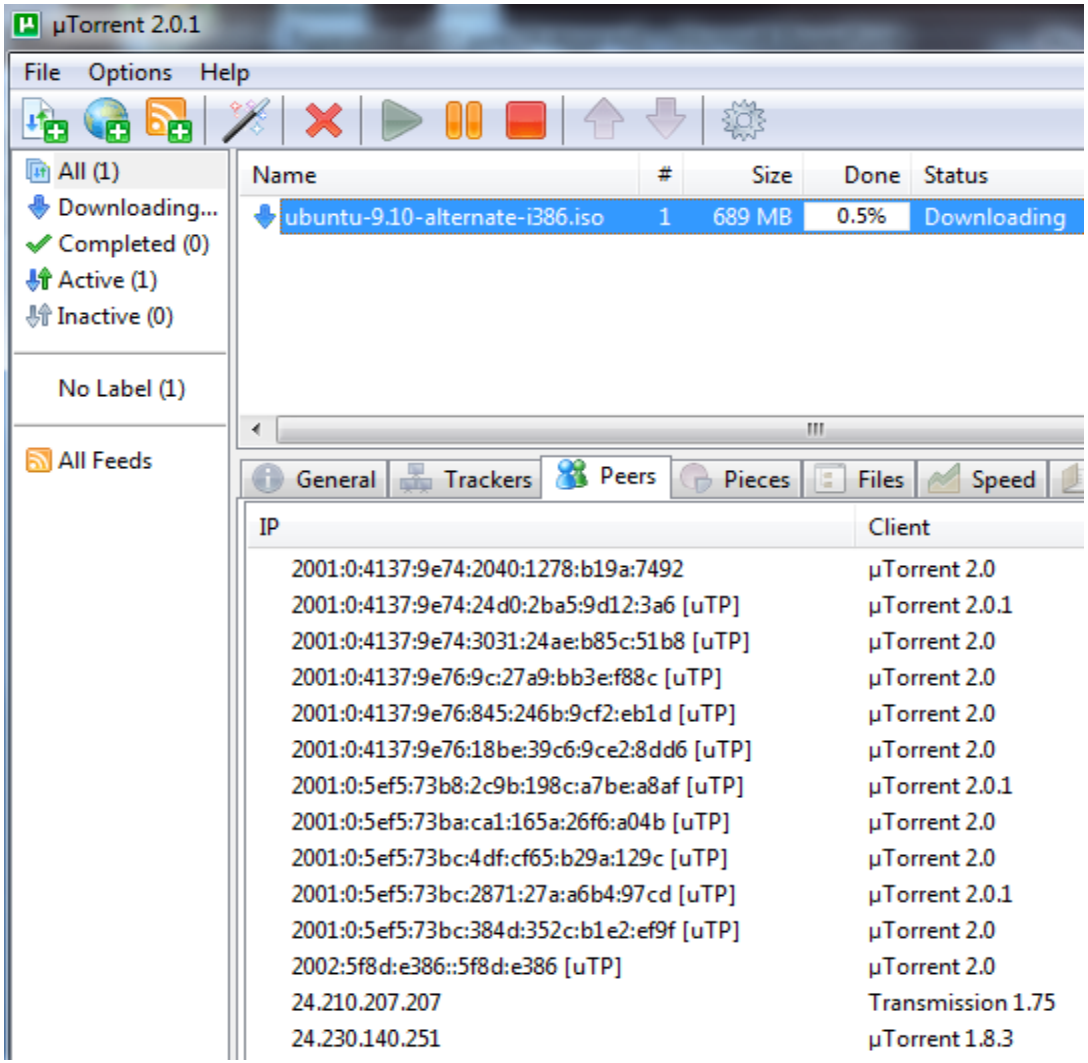
How it’s being used **NOW**



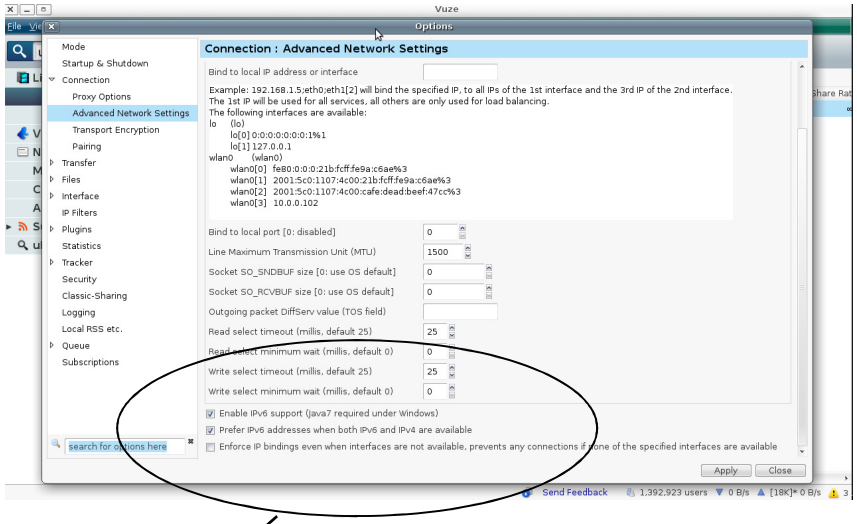


uTorrent – Teredo Peers

- uTorrent runs very well over Teredo
- BitTorrent community is discovering IPv6

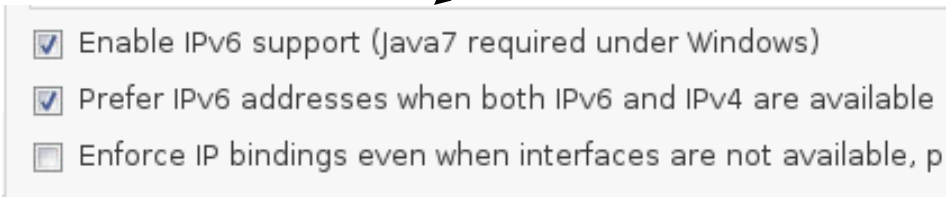


Vuze– IPv6 Peers



- Vuze (formerly Azureus) is another fully IPv6-enabled bit torrent client

- See how easy it is to "prefer" IPv6!



ubuntu-10.04-desktop...	89.133.83.39	µTorrent 1.8.3	L		100.0%	146 B/s
ubuntu-10.04-desktop...	62.83.35.208	Azureus 4.4.0.4	R		99.2%	0 B/s
ubuntu-10.04-desktop...	2607:f2c0:f00e:5b00:217:f2ff:fee7:6a4c	µTorrent Mac 1.0	R		100.0%	6.8 kB/s

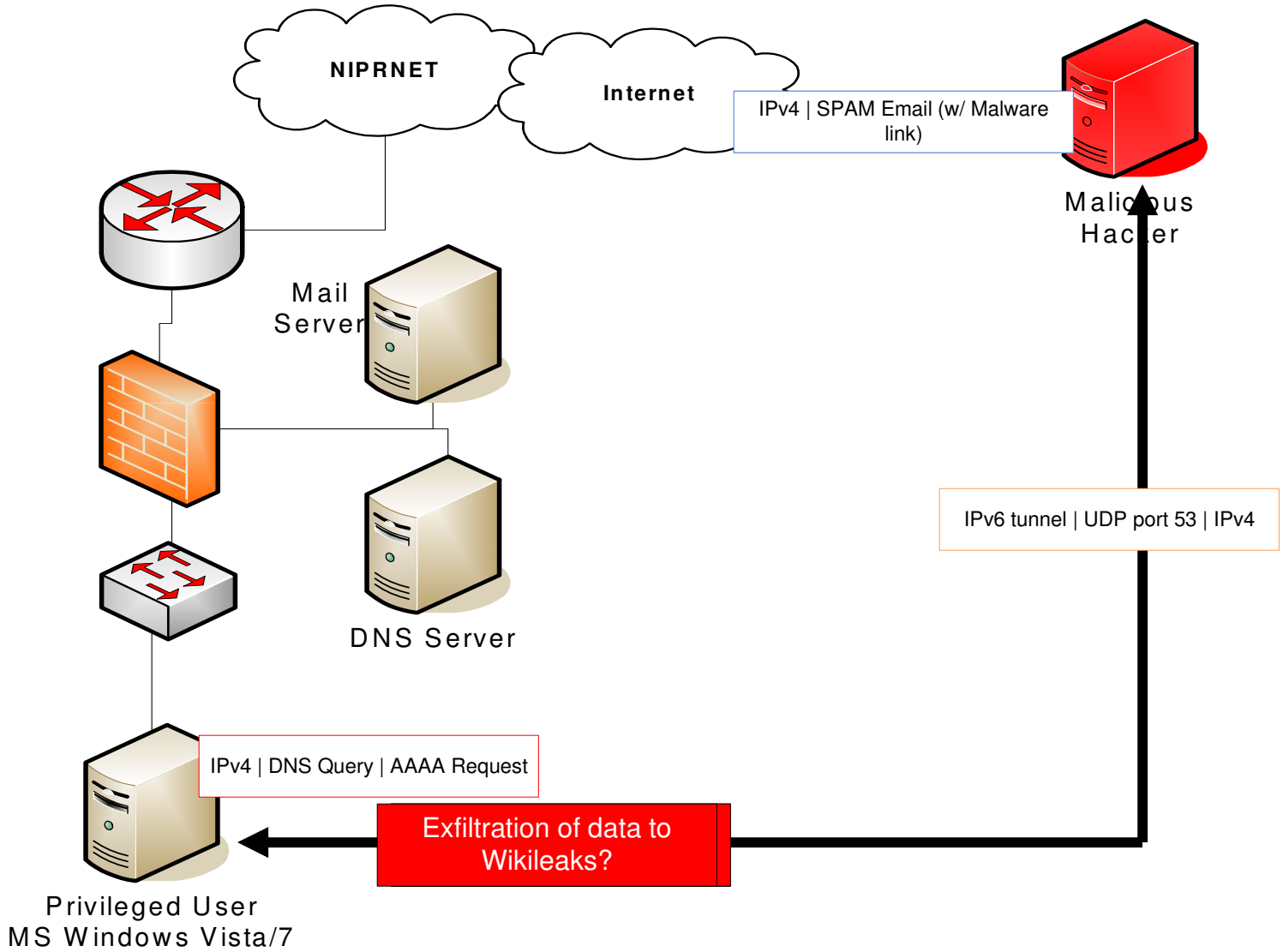
Example# 3: IPv4 AAAA DNS Queries broadcast IPv6 enabled hosts!

- Microsoft Dual Stack enabled on ALL MS Vista/Windows 7/Server 2008, MAC OSX, & Linux systems
- AAAA Queries present on ***every*** network we monitored.
- Considered 'harmless' by many mainstream security and network engineers
- Must be disabled by DoD MO2 guidelines (section 3.3.6.1)
  - "AAAA records may not transit beyond the intra-enclave security zone"

IPv4 AAAA DNS – The Loaded Gun

- Remote Hacker sees an organization sending 100,000+ AAAA queries a day
- Hacker Floods an organization's mail servers with SPAM
  - It only takes one user with elevated privileges to open one SPAM message to execute the encapsulated malware
  - Consider MS 10-009, MS 10-029 & CVE-2010-1892 as examples
- Malware establishes an IPv6 in UDP tunnel through an organization's firewall to Remote Hacker on UDP port 53
  - Such as Miredo or GoGoNet6
- Remote Hacker exfiltrates sensitive data from an organization's enterprise network

The Loaded Gun Scenario



Example #4: Rogue Router Advertisements (RA)

- IPv6-enabled workstations (untouched Vista, 7, Linux, Mac, etc) always listen for Router Advertisements
- User X downloads that same pesky malware
  - Sets up tunnel like the non-standard UDP port example (or port 53)
  - Installs basic router advertisement daemon & IPv6 forwarding
- User X sends RAs out to those IPv6-enabled machines with User X as its default gateway for IPv6
- Now there are active IPv6 malware on an enterprise that can't be detected
- Read RFC 6104 for more details

Example #4: Rogue Router Advertisements, cont.

- Microsoft won't fix it
- Only mitigations currently:
  - Cisco RA Guard (Must have IPv6 enabled on your core)
  - Use of DPI inspection in your core

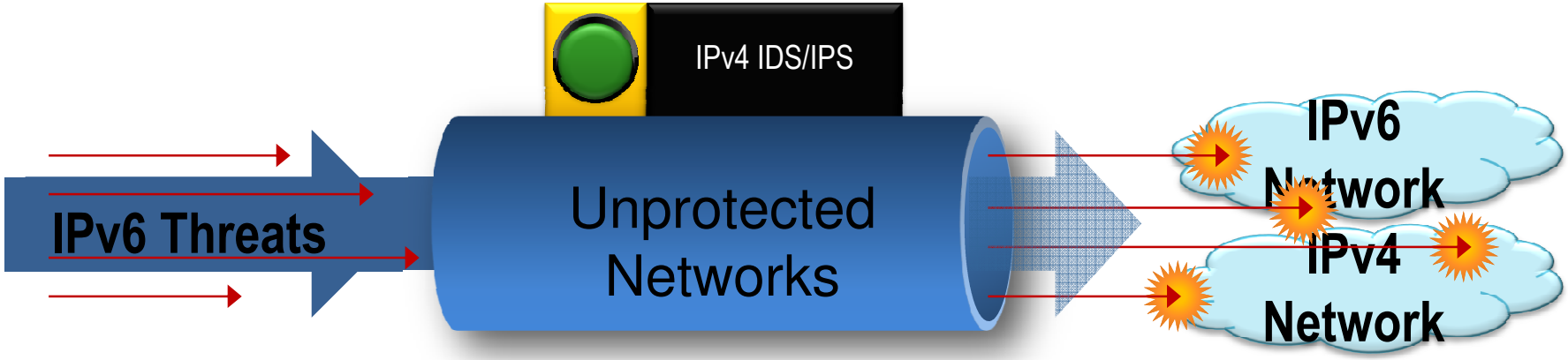
Government's Specific Vulnerabilities from Supporting Contractor Networks

- Accidental IPv6 deployment
  - Windows 7 and Server 2008
- Mis-configured Windows Server 2008 w/ IPv6 enabled causes DNS to break in an IPv4-only environment
  - Link-Local Name Resolution (DNS of last resort). If a host answers on IPv6 it will use it.
- IPv4 AAAA queries
- IPv6 tunneling w/ Teredo and 6to4

How Can You Fix This?

- Implement IPv6 on your enterprise ***now***
  - After you plan, design, test and design!
- Hold your security vendors accountable ***now***
- Get your Systems and Network Engineers trained ***now***
- Use Deep Packet Inspection (DPI) to have better awareness
- Have an IPv6 Cyber Security Plan ***now***
  - Tools (monitoring, prevention, detection)
  - Architecture
  - Engineering

IPv6 Tunneling Gives Attackers a Green Light to Penetrate Networks



Assure6 Protects IPv4 and IPv6 Networks from IPv6 Tunneling

Your Information is Protected

Functional Component
Information Assurance
Intrusion Detection & Analysis
Threat Assessment

SALIENT ASSURE6

"Helps Air Force Drive **Enterprise Policy Management** Security Across its Gateways…"

Summary

- IPv6 Threats are Real – both native and tunneled
- Hackers are using IPv6 to tunnel into networks undetected by current security tools - ***Now***
- Companies must develop a security policy to address IPv6.

Questions?

Jeremy Duncan

Salient Federal Solutions

Email: Jeremy.Duncan@salientfed.com

Google Voice: 540.440.1193