Critical Infrastructure: The IPv6 Transition Challenge

Danny McPherson

Verisign, Inc.

Robert M. Hinden

Check Point Software

Session ID: TECH-302

Session Classification: Intermediate

RSACONFERENCE2012

Agenda

1 The Internet Architecture

2 Why the need for IPv6

3 Transition, Dual-Stack and Coexistence

4 Protocol Issues

5 Happy Eyeballs

The Internet Architecture

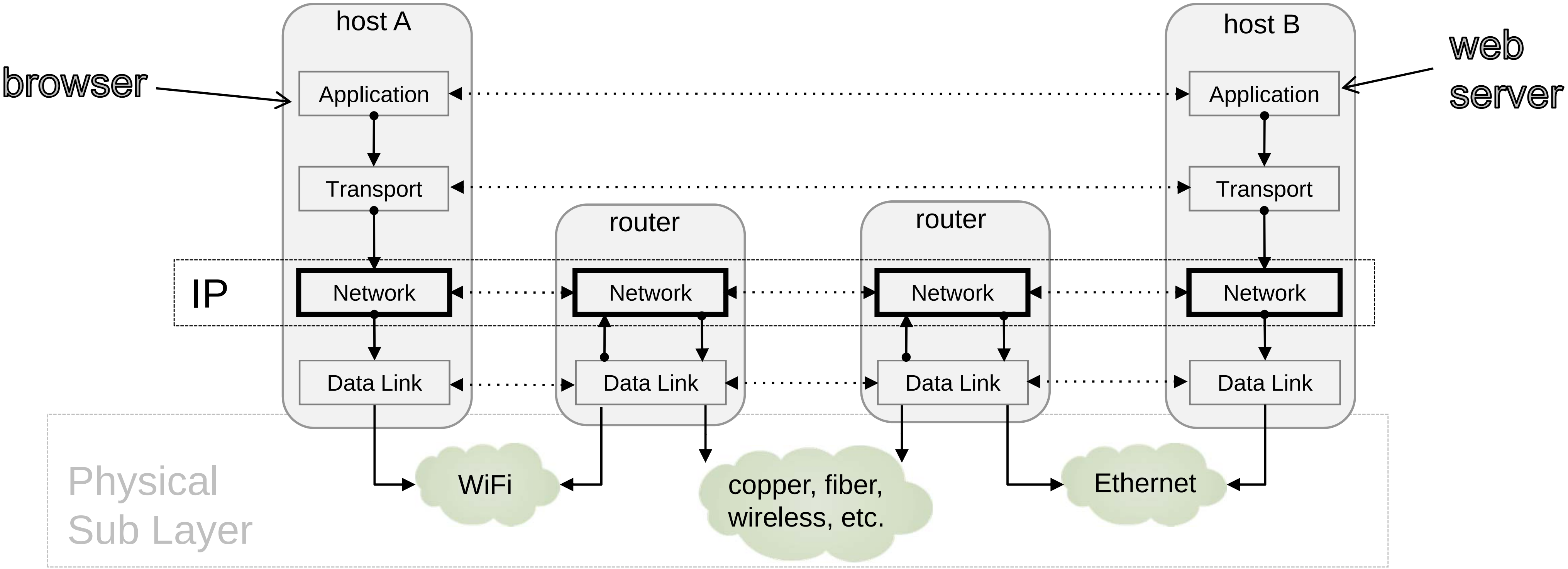
- Ubiquitous data communications platform; no single authority
  - Global collection of loosely interconnected networks
  - Datagram / packet-based connectionless network service
  - Ultimate goal is **any-to-any** connectivity **end-to-end**

- Primary Internet Infrastructure Elements
  - Name: What we seek (DNS)
  - Address: Where it is (IP)
  - Route: How to get there (BGP)

IP

- IPv4 originally deployed in 1981

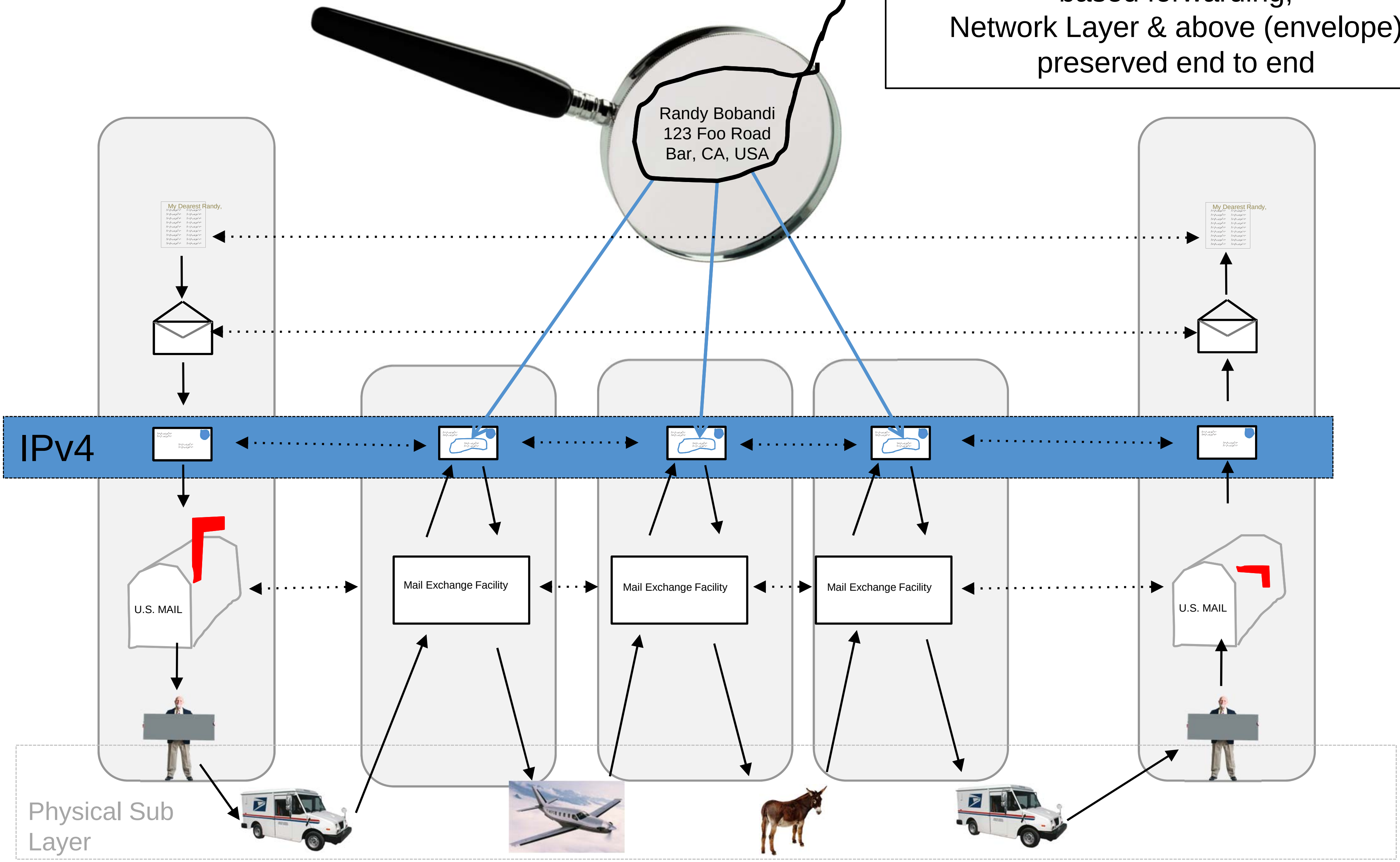
The Internet Protocol Model



- The IP model employs an **end-to-end** layered architecture
  - Transactions split into functional layers – IP @ “Network” Layer
  - Only IP and higher layers operate end-to-end – simplifies network devices
- Packets switched hop-by-hop based on destination IP address
  - Each device connected to the Internet requires a unique IP address
  - There are 2^{32} (4,294,967,296) unique IP addresses in IPv4

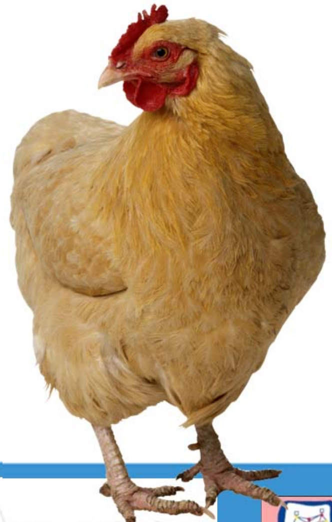
IP Model & Postal System Analogy

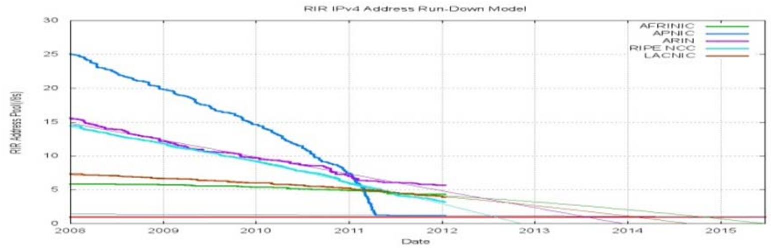
IP Employs Hop-by-hop Destination-based forwarding;
Network Layer & above (envelope) preserved end to end



An Induction Problem? Worse?

- Responses to IPv4 depletion minimized rate
  - People adapt, they innovate – duh!
  - People become immune to IPv4 doomsday – duh!
- Recurring “*you need IPv6*” with no driving externalities has been problematic, particularly now that *you need IPv6 preparedness* ☺





Source: Geoff Huston, http://www.potaroo.net/tools/ipv4/plotend.png

IPv4, IPv6 & Induction..

- Internet growth has exceeded all expectations
  - IPv4 address depletion discussed in ~1990
  - Initial estimates projected IPv4 depletion ~2000

- The Internet community responded, developing several solutions
  1. Removed “fixed size” classes/boundaries in IP architecture (CIDR)
  2. Address sharing at the edge via network address translators (NATs)
  3. Developed responsible IPv4 allocation policies and conservation efforts (RIRs)
  4. **Next generation IP design began early ‘90s, IPv6 high-level design finalized in 1999**

IPv6 Architectural Components

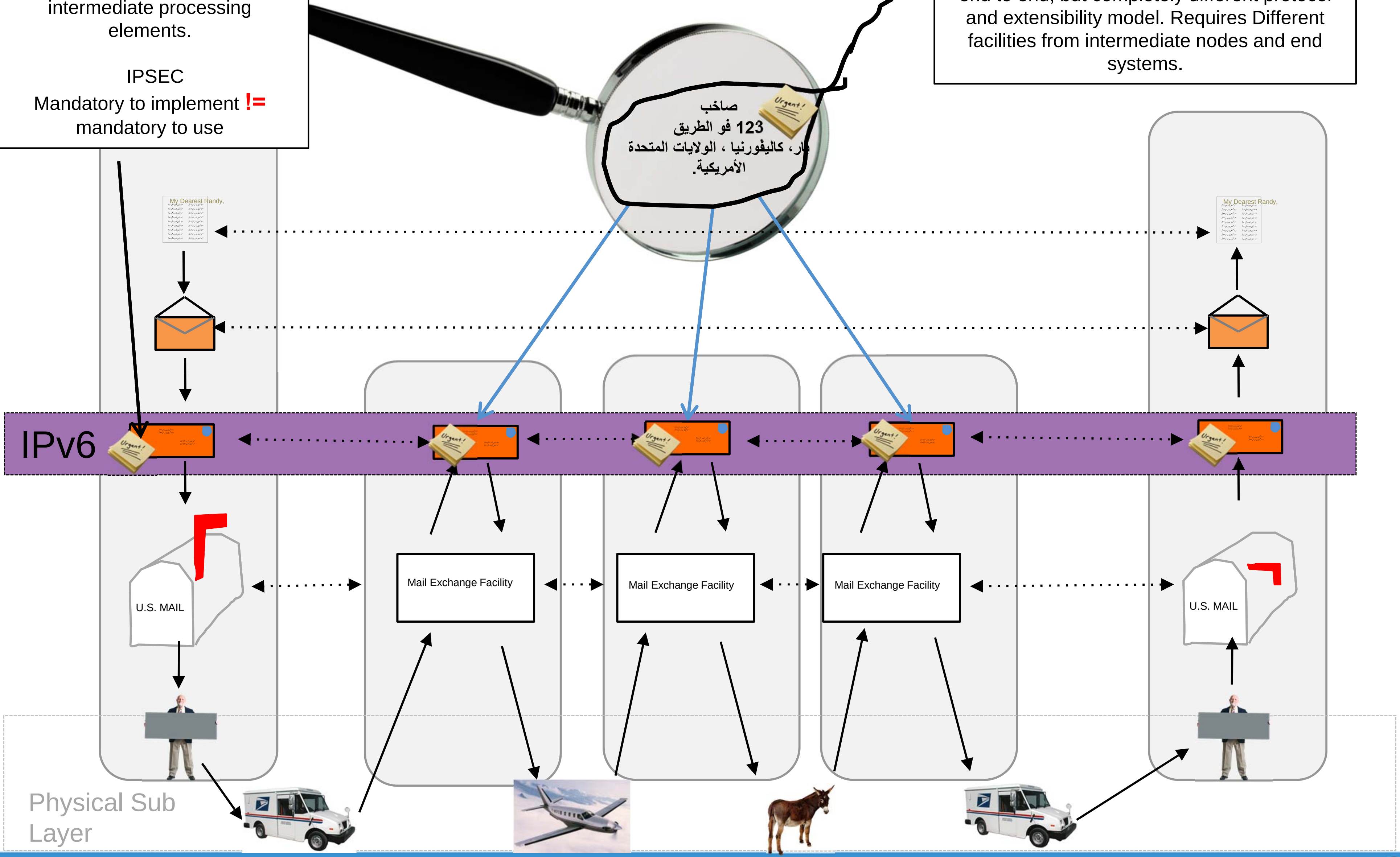
- IPv6 provides 3.4x10^{38} addresses (340,282,366,920,938,463,463,374,607,431,768,211,456)
  - Not intended to be radical solution – considered conservative engineering
- Used and managed similar to IPv4
  - IPv6 colon-separated hexadecimal address: **2001:1890:1112:1::20**
  - As opposed to IPv4s dotted-quad: **64.170.98.32**
- IPSEC Mandatory to implement
  - **not** mandatory to use
- Employs extension headers rather than principle IP header options
  - Extension headers are chained and serve many different purposes

IPv6 Model & Postal System Analogy

IPv6 introduces an array of extension headers targeted to either end systems or intermediate processing elements.

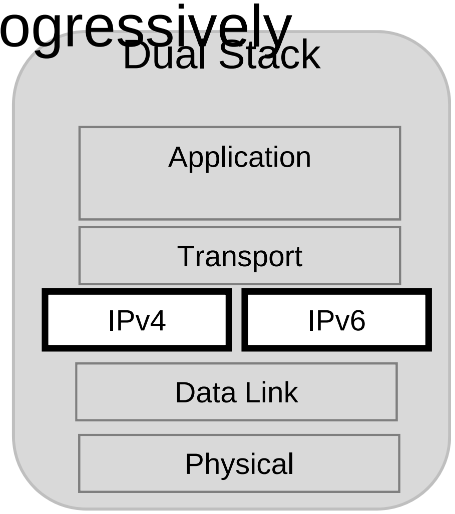
IPSEC
Mandatory to implement != mandatory to use

IPv6 also employs hop-by-hop destination-based forwarding;
Network Layer & above (envelope) preserved end to end, but completely different protocol and extensibility model. Requires Different facilities from intermediate nodes and end systems.



IPv6 and Transitional Coexistence

- IPv4 -> IPv6 transition plan was ‘**dual stack**’
  - Both protocols operate at Network layer
  - Are **not** ‘**bits on the wire**’ compatible
  - Transition plan best when plentiful quantities of IPv4 and IPv6 exist
  - IPv4 depletion will impair dual stack transition plan, introducing expense and potential disruption to Internet as service platform
  - Following depletion dual stack transition problems progressively worse
- Interoperability and Coexistence
  - **Everything** in the IP stack has to handle either – or both
  - IPv4 devices may never be upgraded to IPv6
  - IPv6-only devices may communicate with IPv4 devices
- Greenfield now with Large-scale/Carrier-grade NATS



Dual Stack

Application

Transport

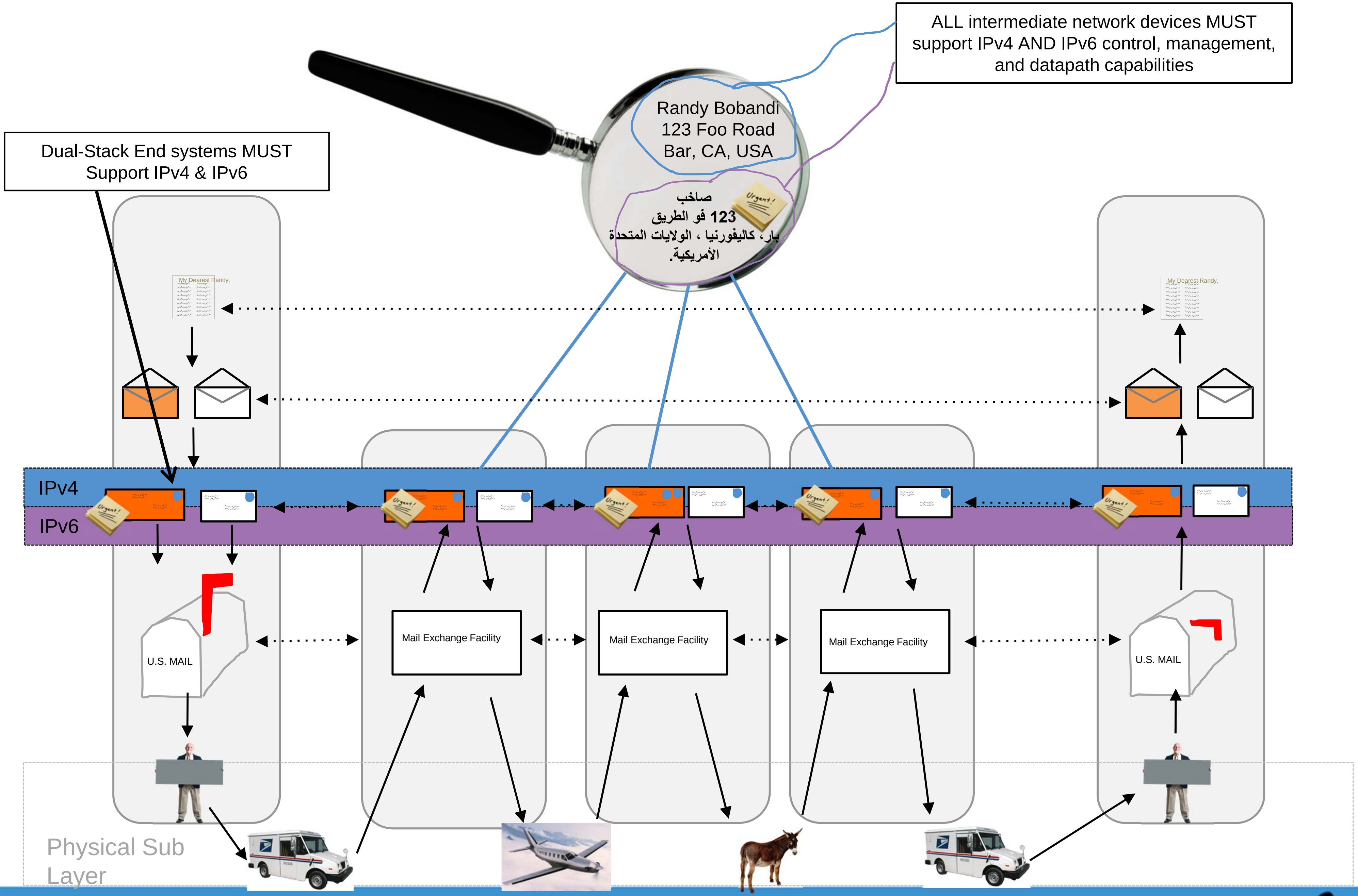
IPv4

IPv6

Data Link

Physical

Dual Stack



ALL intermediate network devices MUST support IPv4 AND IPv6 control, management, and datapath capabilities

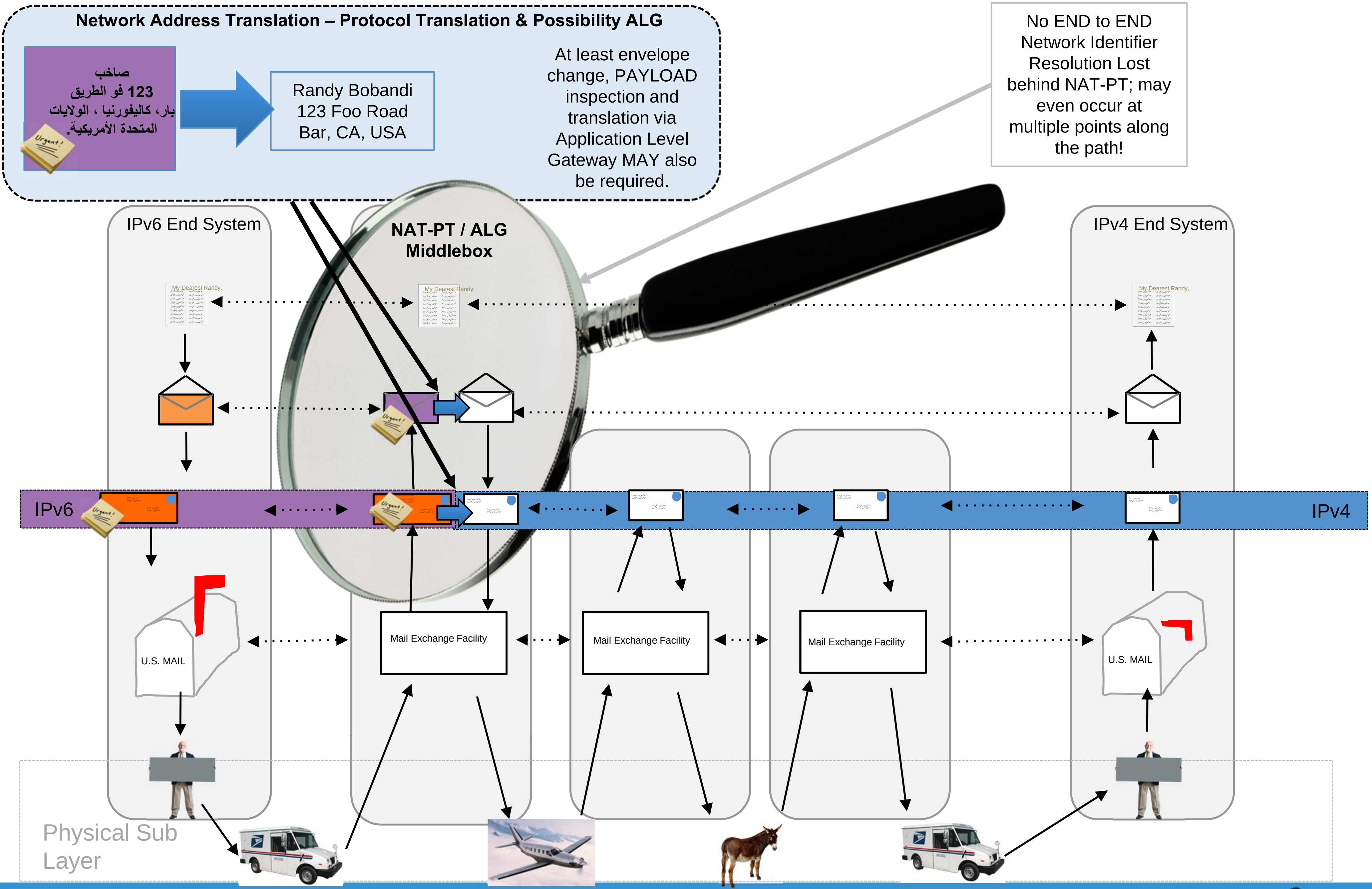
Dual-Stack End systems MUST Support IPv4 & IPv6

Middleboxes

- Middle boxes such as Carrier Grade NATs (CGNs) / NAT-PTs are going to bridge the IPv6 world to the IPv4 world for many moons
  - Middleboxes manipulate packets in the network, compromise the end-to-end principle
  - Require transaction state in the network
  - Utilize address and/or port sharing
  - Also may need to employ application level gateway (ALG) functions

- NAT-PTs can even appear at multiple points along a single transaction datapath!

Reality: A Long Period of Transitional Co-Existence



Network Address Translation – Protocol Translation & Possibility ALG

صاحب
123 فو الطريق
بار، كاليفورنيا ، الولايات
المتحدة الأمريكية.

Randy Bobandi
123 Foo Road
Bar, CA, USA

At least envelope change, PAYLOAD inspection and translation via Application Level Gateway MAY also be required.

No END to END Network Identifier Resolution Lost behind NAT-PT; may even occur at multiple points along the path!

Network Externalities

- There’s been no ‘killer app’ to drive both end systems and network operators to adopt IPv6
  - The *IPv4 depletion stick* is as good as it gets

- The result has been little market demand for equipment and applications that support IPv6, result in little implementation and GA support
  - Recall that IPv6 has to be supported in end stacks, routers, applications, security tools, etc..
  - Chicken and egg problem….

Functional Parity

- Network and security operators need to obtain functional parity between IPv4 and IPv6 capabilities for ALL functions immediately…
  - Every device and application in your environment needs to be checked for IPv6 functional preparedness
  - All regression testing, vulnerability tools, etc.. need to be adapted to support IPv6
- IPv6 enabled by default on many devices today, if you’re not using it you should turn it off!
- Function and feature parity are still sorely lacking, particularly at scale and in middleboxes

EXT Headers, IPSEC, Security, et al..

- **No security magic in IPv6 –** largely just 96 more bits
  - IPSEC SHOULD be there
- Large address space and subset size makes vulnerability scanning and node discovery more challenging
  - Augment with passive monitoring and telemetry data tie-ins from flow data and address assignment functions
  - Utilize link layer access controls
- Explicitly scope those extension headers, disable all but what you use
- Ensure your security devices sufficiently scale and process / filter IPv6 packets

IPv6 and Covert Channels

- Operators need full visibility into both native IPv6 and transition technologies (6to4, 6RD, Teredo, etc):
  - allow IPv6 packets to *jump the IPv4 moat* without configuring dedicated tunnels
  - fly under the radar where IPv4 tools would have prevented or detected problems
- IPv6 proxies may introduce problems, including
  - discovery attacks
  - spoofing & reflection attacks
- Obtaining visibility and functional parity with IPv4 key
  - If parity isn't there then IPv6 may well be providing a covert data exfiltration or bot C&C channel in your network today!

Be Wary Middleboxes

- NAT-PT devices can be problematic
  - Lawful intercept compliant (bindings need to be maintained and timestamps)
  - Number space reputation services (e.g., IP blacklists)
  - User tracking such as advertising or IP geolocation
  - Collateral damage in network layer controls (e.g., ACLs)
  - NAT-PT devices itself is problematic because of state-based devices

- State in middleboxes and ALGs can introduce significant new attack surface

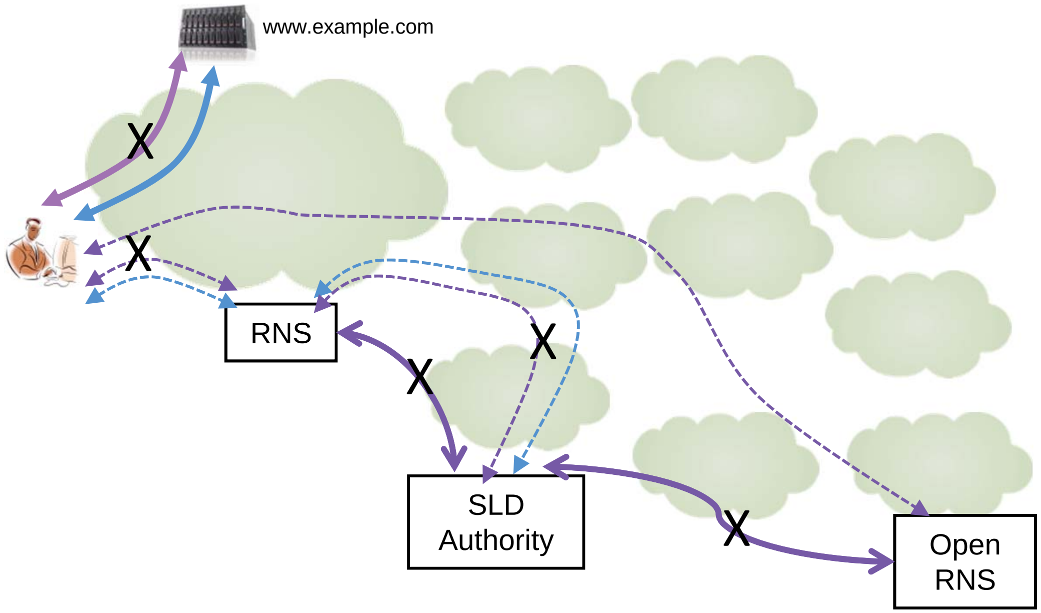
IPv6 Neighbor Discovery (ND) & Solicitation

- Five different types of ICMPv6 for several purposes, e.g.:
  - determining the link layer addresses of neighbors on attached links
  - purging cached values that become invalid
  - to discover neighbors willing to forward packets on their behalf
  - Duplicate Address Detection (DAD)
  - Neighbor Unreachability Detection (NUD)

- Attacks here likely to replace their IPv4 counterparts such as ARP spoofing. In general, it's a good idea:
  - to keep ports disabled unless explicitly provisioned
  - implement link layer access control and security mechanisms
  - be sure to disable IPv6 completely where it's not in use

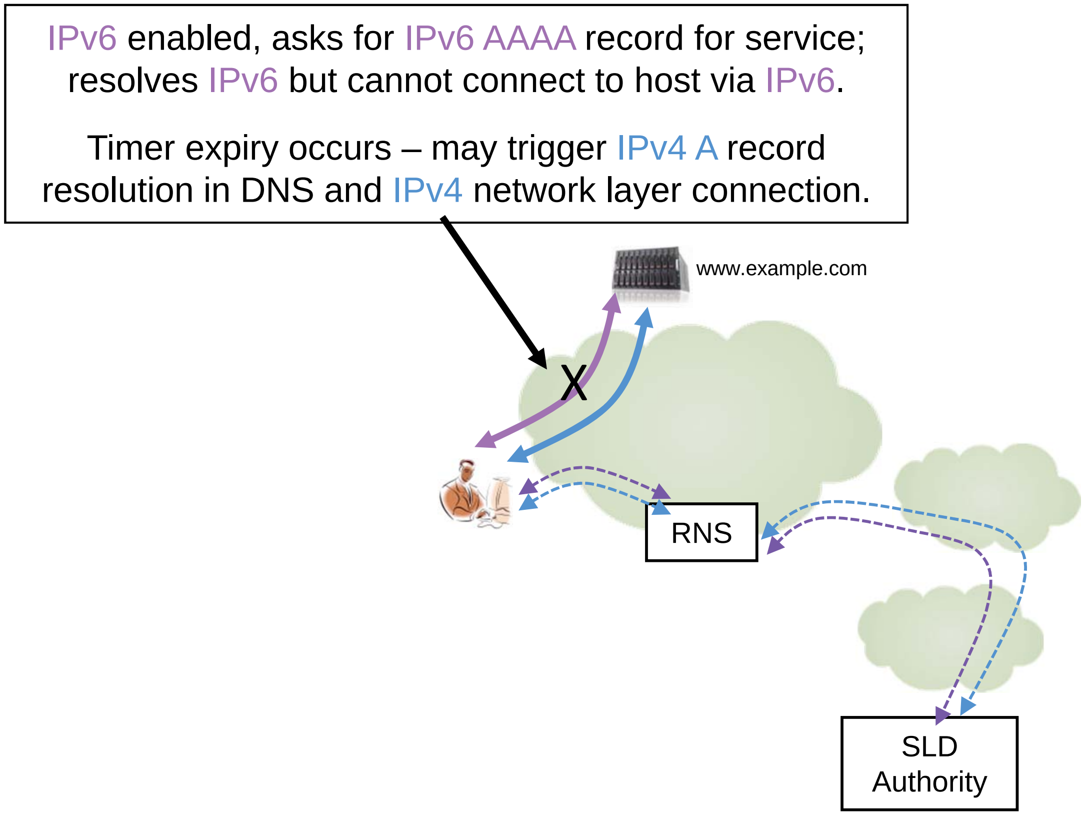
AAAA Whitelisting Challenges Incremental Deployability

If DNS authority (or web server) have not measured workable IPv6 connectivity to recursive name server then don't respond with AAAA to that recursive name server.



Extremely conservative, breaks incrementally deployability and makes some broad assumptions!

Systemic Interactions & Unhappy Eyeballs



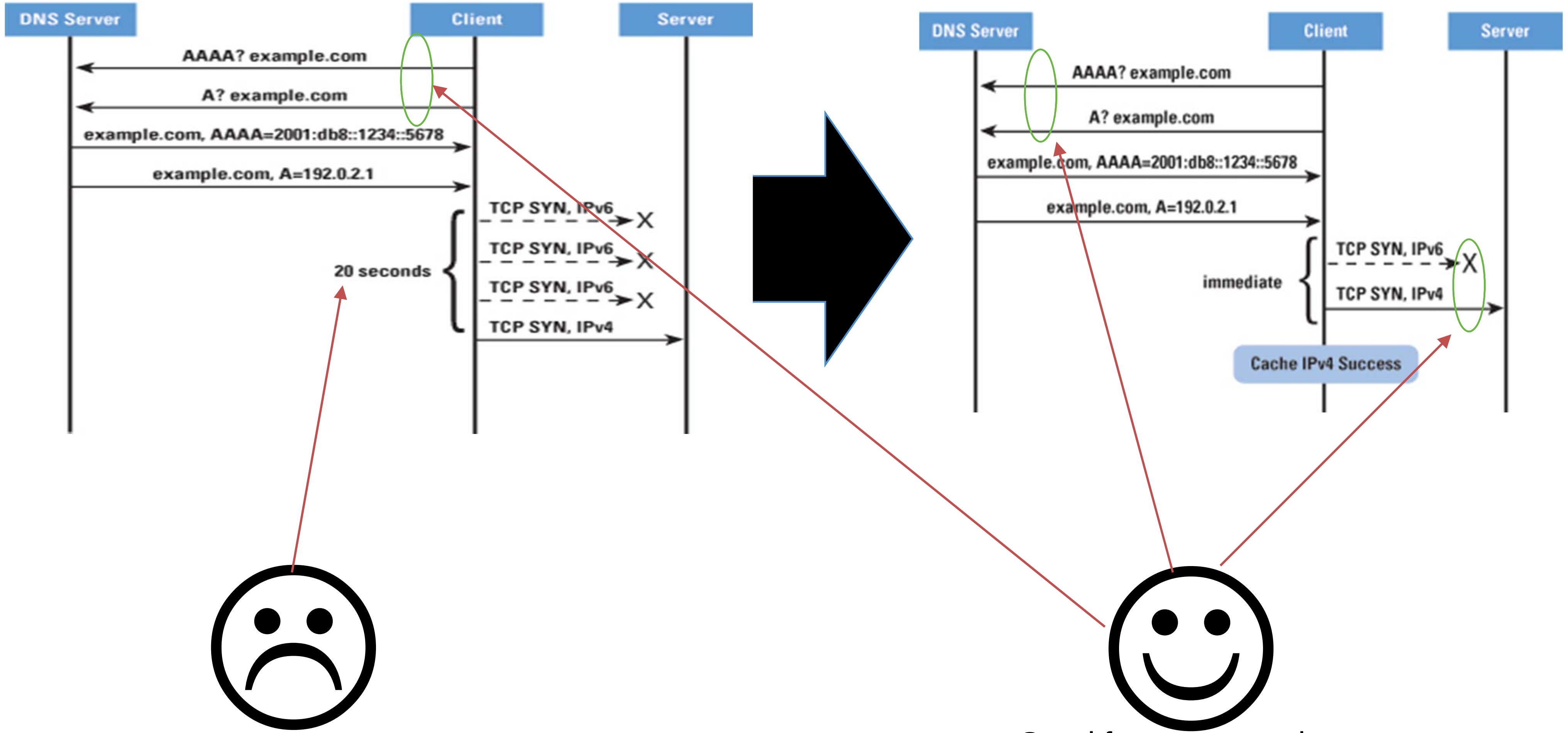
IPv6 enabled, asks for IPv6 AAAA record for service; resolves IPv6 but cannot connect to host via IPv6.

Timer expiry occurs – may trigger IPv4 A record resolution in DNS and IPv4 network layer connection.

User can’t access site over IPv6, or experiences considerable delay because returned network layer identifier address doesn’t match datapath connection capability to remote node

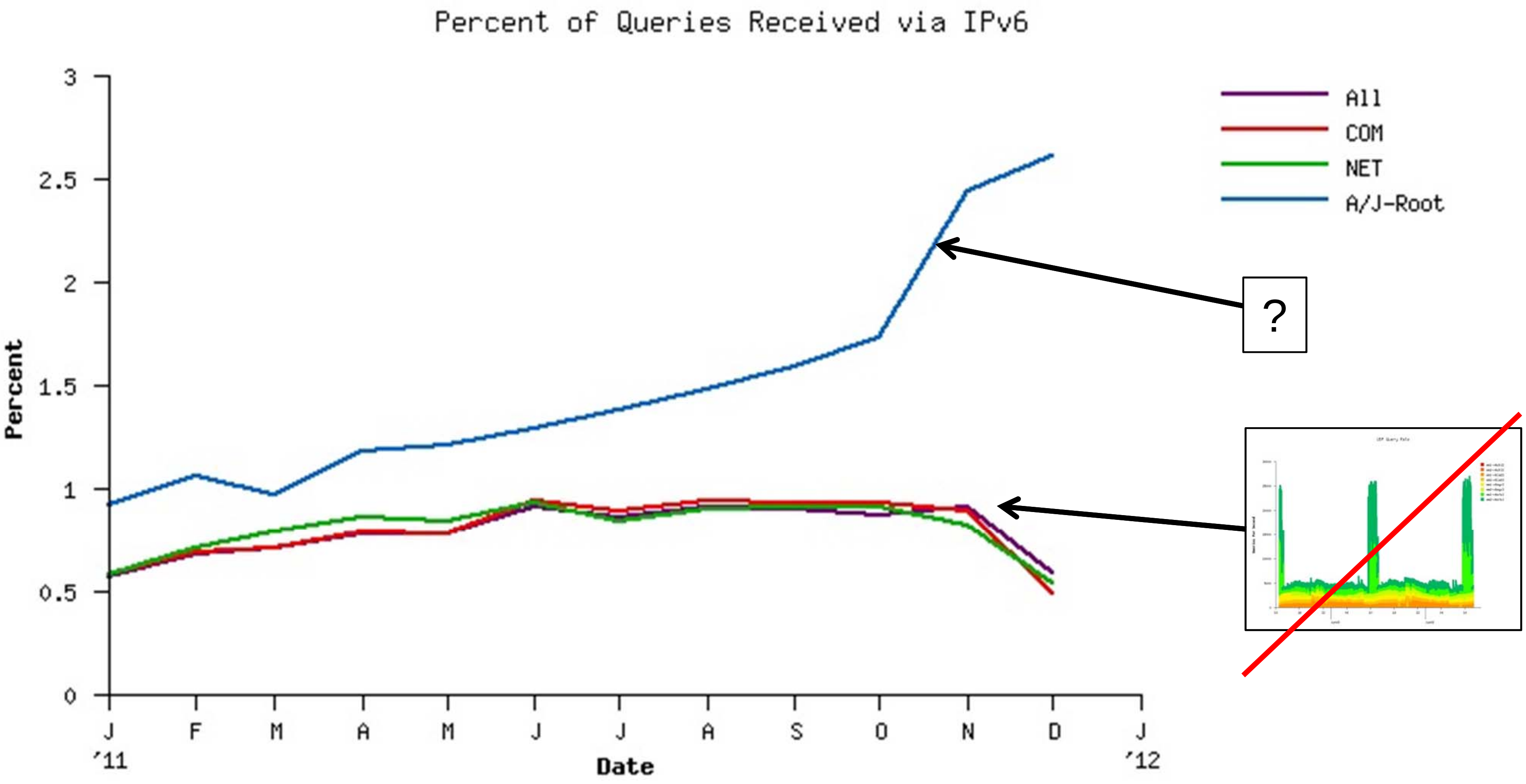
Transitional Co-Existence and Happy Eyeballs

Source: Internet Protocol Journal



Good for user experience,
bad for systemic state!

IPv6 Traffic Query Percentages :: A Verisign Perspective

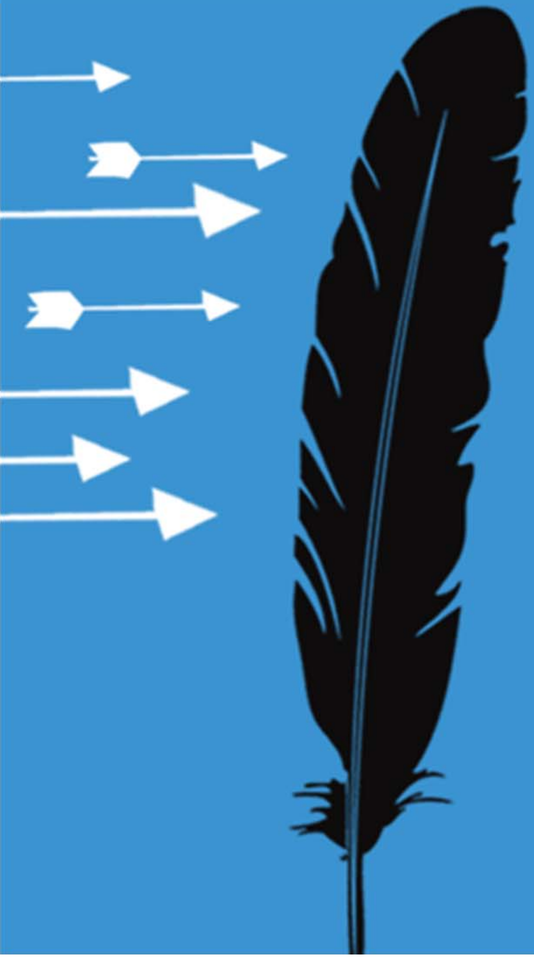


?

Apply Slide

- The time is now to consider IPv6 in your environment
  - If for nothing more than to determine what new security vulnerabilities you have – it’s enabled by default in many systems today
- Focus on visibility and functional parity!
- IPv6 impacts you and your environment whether you act or not!

Questions and Answers



Thank You!