Deploying IPv6 Securely

Robert M. Hinden
Check Point Software

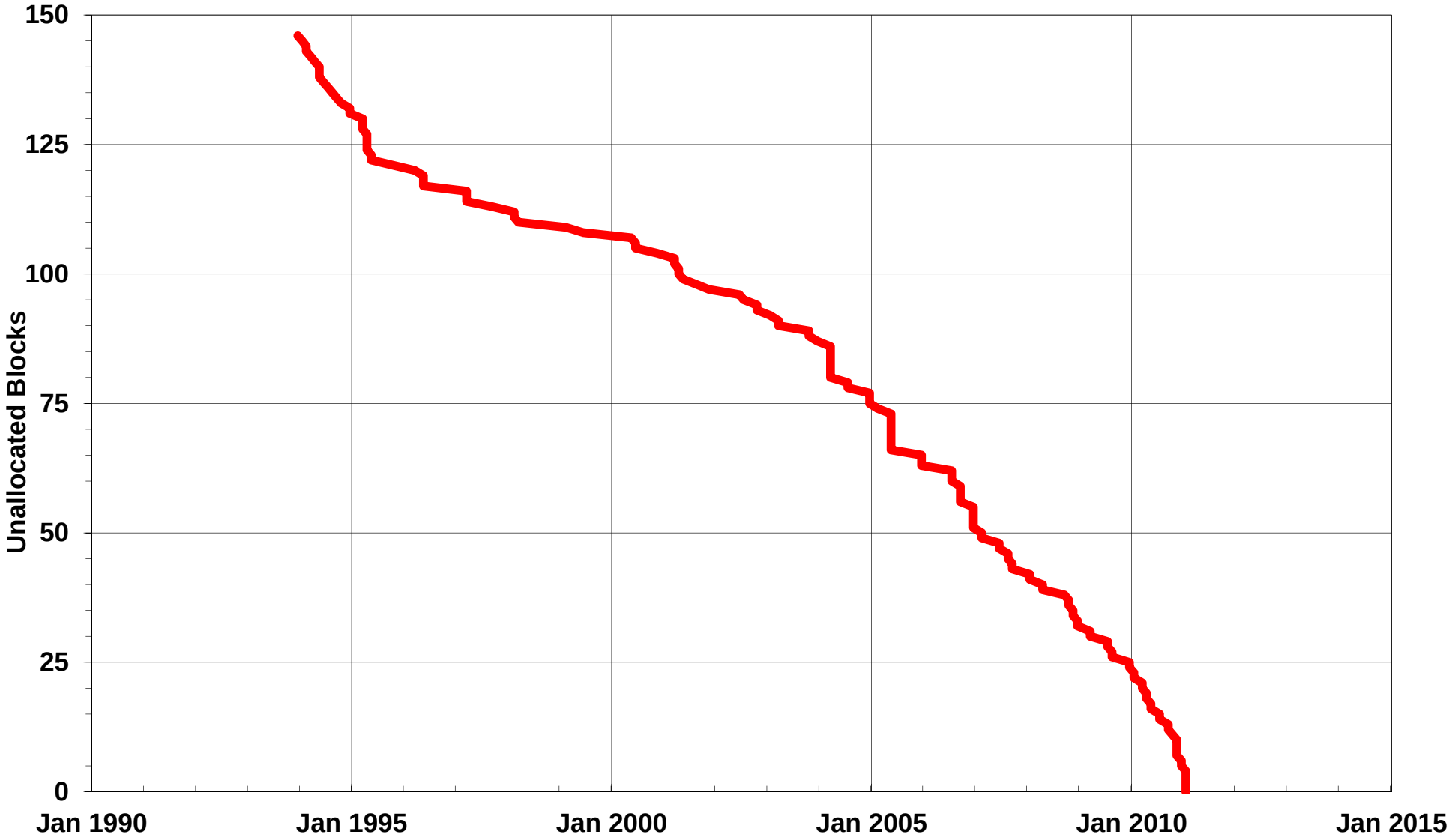
Danny McPherson
VeriSign

Session ID: TECH-202
Session Classification: Intermediate

Agenda

1. IPv6 Is Being Deployed Now
2. Overview of IPv6 Security
3. What Are the Issues?
4. How to Deploy IPv6 Securely
5. Q & A

IPv4 Addresses Have Run Out



(Last allocation to RIRs from the IANA free pool 31 Jan 2011)

Address Exhaustion Driving IPv6 Deployment

IPv4 Addresses Have Run Out	▪ Final IANA allocation to Regional Internet Registries was on 1/31/2011 ▪ Major RIRs will exhaust their remaining addresses this year
Effects	▪ IPv4 addresses are now a scarce resource ▪ Small blocks of IPv4 address are available at rising cost ▪ Large ISP size blocks are not available

The Internet will continue to grow

IPv6 Status

ISP's	Products	Content Providers

▪ Backbone ISP's support IPv6 today
▪ Broadband ISPs are adding IPv6 support
▪ Wireless ISPs support underway
	▪ Routers, Switches
	▪ Firewalls, IPS
	▪ Load Balancers
	  ▪ Win 7 / Vista
	  ▪ MacOS X
	  ▪ Linux / BSD
	  ▪ IOS
		▪ Google
		▪ Yahoo
		▪ Facebook
		▪ YouTube
		▪ ….

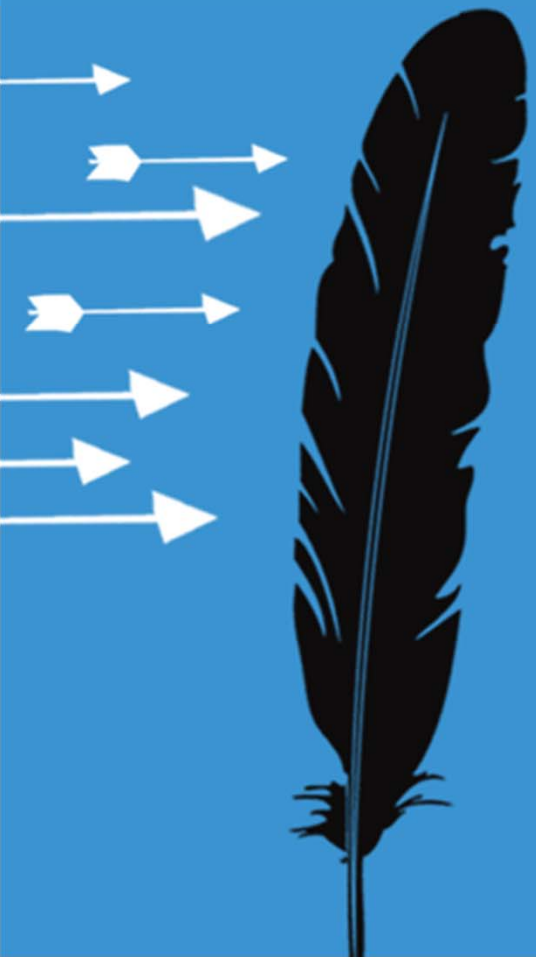
World IPv6 Launch

THE FUTURE IS FOREVER
6 JUNE 2012

Major Internet service providers (ISPs), home networking equipment manufacturers, and web companies around the world are coming together to permanently enable IPv6 for their products and services by 6 June 2012.

Organized by the Internet Society

http://www.worldipv6launch.org/



Overview of IPv6 Security

What Is IPv6?

IPv6 = IPv4 with Bigger Addresses

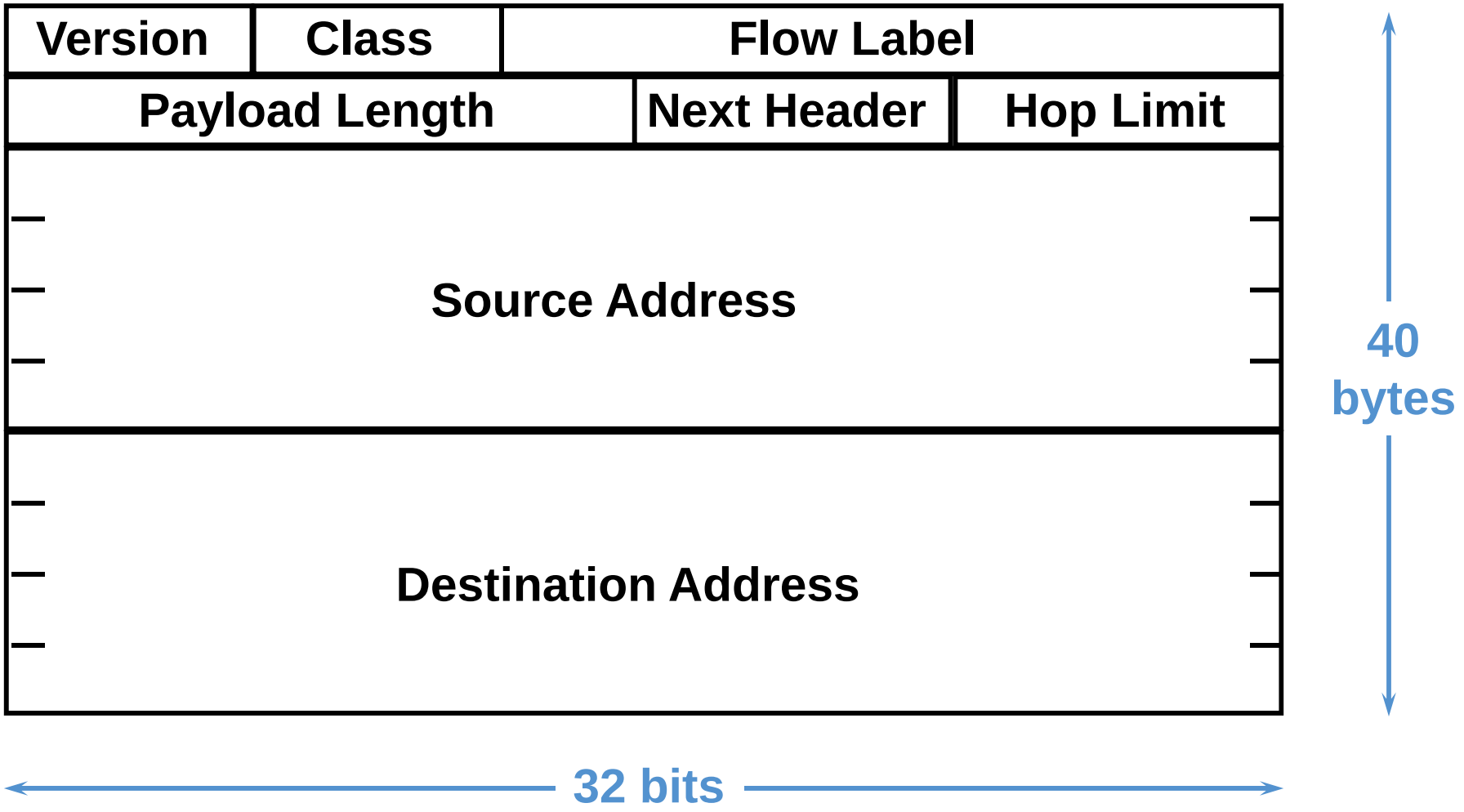
Other Differences

- 40 byte fixed header
- No header checksum
- Address Auto-configuration
- Extension Headers

Transition Mechanisms

- Tunneling
  IPv6 in IPv4, IPv4 in IPv6, IPv6 over IPv4, ….
- Translation
  NAT46, NAT64, NAT66

IPv6 Header Format



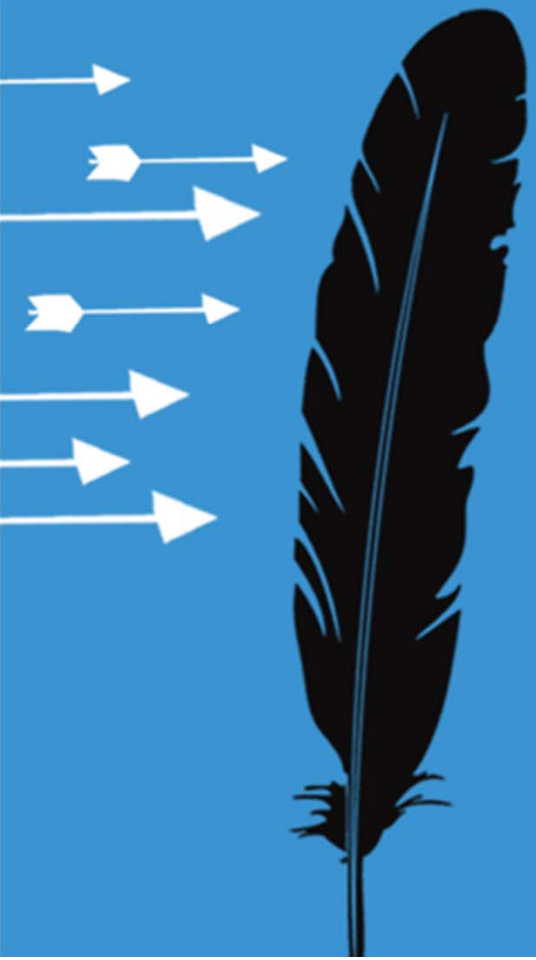
IPv6 Security

IPv6 Security Features

- Sparse Address Space
- Improved design as compared with IPv4
- IPSec required
- Secure Neighbor Discovery
- Unique Local Addresses
- Privacy addresses

Issues

- Rogue Router Advertisements
- Transition tunneling solutions
- Extension header architecture



IPv6 Security Challenges

IPv6 Security Challenges

IPv6 as a Covert Channel for Malware

Vulnerabilities in Basic IPv6 Mechanisms

Transition and Tunneling Mechanisms

IPv6 as Covert Channel for Malware

IPv6 Enabled by Default

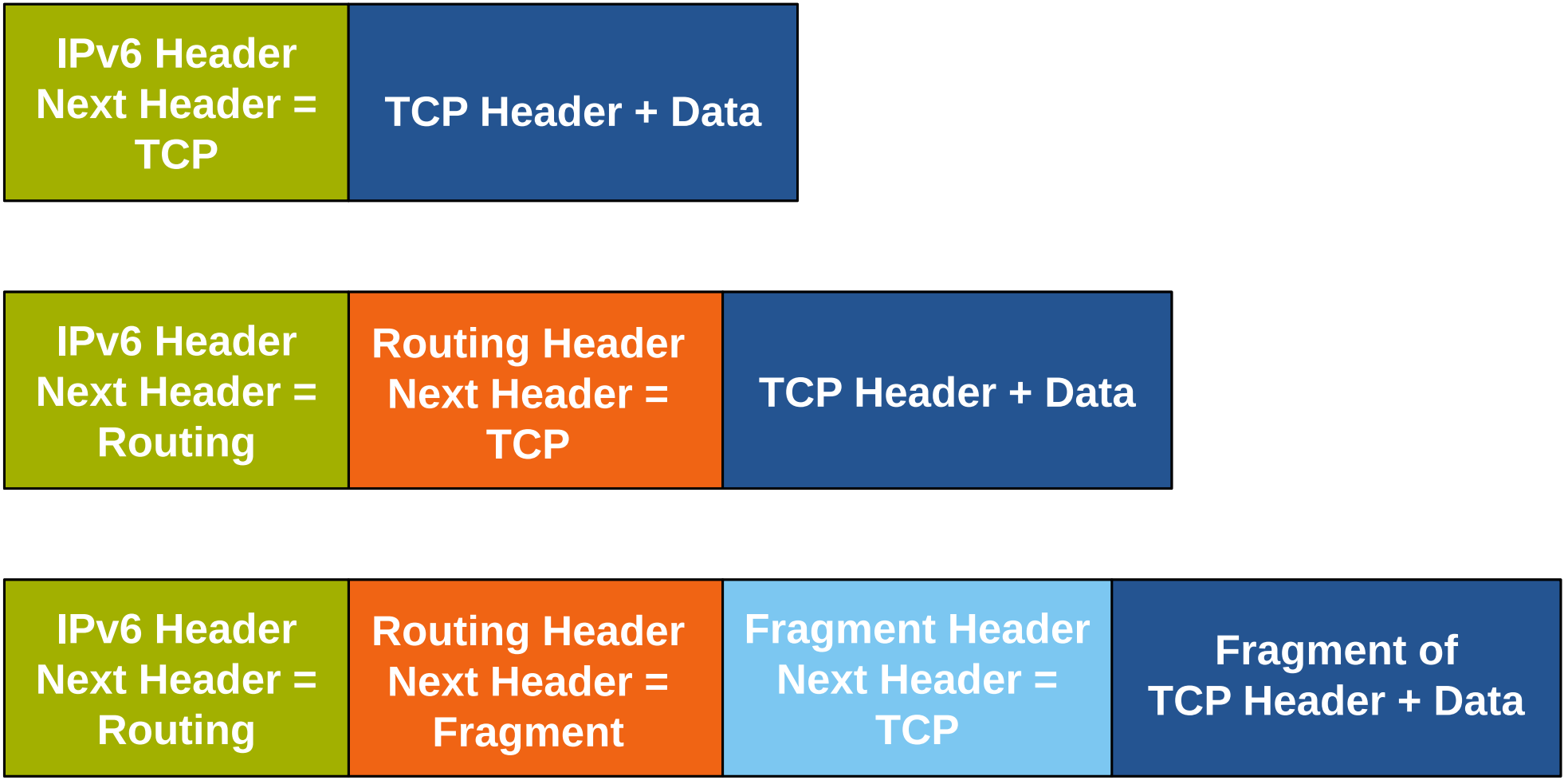
- Most host Operating systems enable IPv6 by default
- It's easy to create IPv6 / IPv4 tunnels to carry traffic outside of an enterprise
- Windows Vista/7 can do this automatically

IPv6 Running Now

- Set up by users who want to try IPv6
- Could be used as covert channel by botnets and malware

You can't stop what you can't see

IPv6 Extension Headers

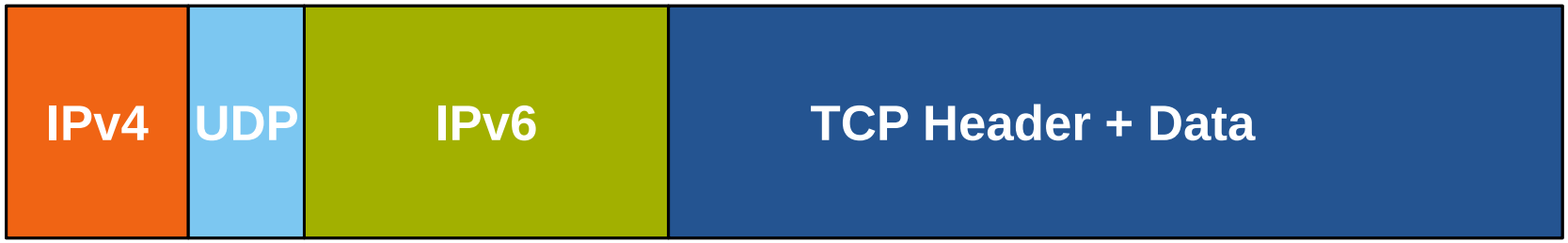


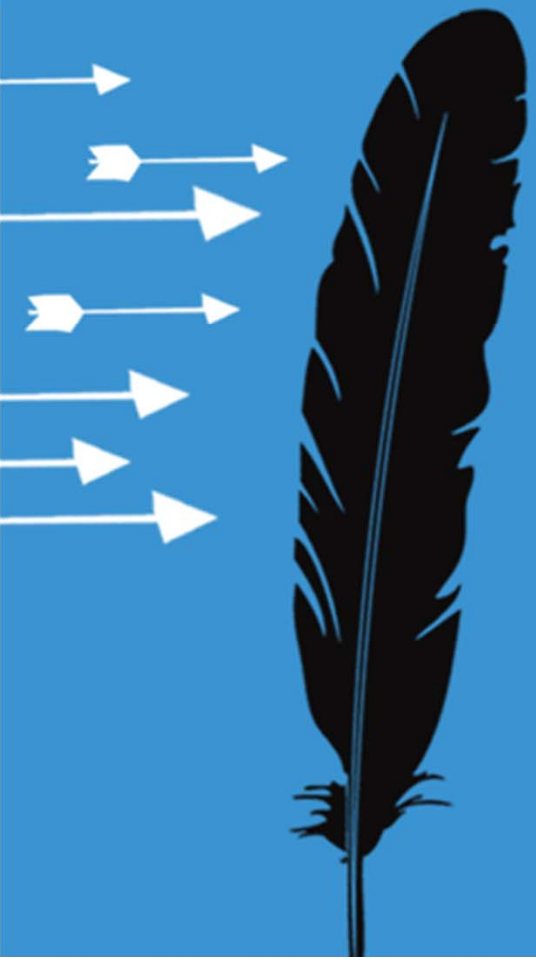
IPv6 Transition Mechanisms

IPv6 in IPv4 Tunnel RFC4213

IPv4 in IPv6 Tunnel RFC2473

Tunneling IPv6 over UDP through NAT RFC4380





How to Deploy IPv6 Securely

IPv6 Deployment Recommendations

Create IPv6 Security Policy that Parallels IPv4 Security Policy

Protect Against Rogue Router Advertisements and DHCPv6 Servers

Set Up Default Firewall Rules that Block All Types of Transition Tunnels

IPv6 Security Policy

Parallel IPv4 Policy

- All objects should have IPv6 information
- Basic rules should be implemented for IPv4 and IPv6
- Specific rules for IPv6 where necessary

Verify

- Rules are implemented in extensions headers
- Rules are implemented in tunneled traffic

Rogue Router Advertisements and DHCPv6 Servers

Rogue RA & DHCPv6

- Easy to turn host into Router via Connection Sharing
- Unauthorized Access Points & Routers (plugged in backwards)
- Similar problems with DHCPv4

Solutions

- Identify host and port using IPS
- Disable port at L2 switch (or physically)

Default Rules to Block Transition Tunnels

Block Tunnels by Default

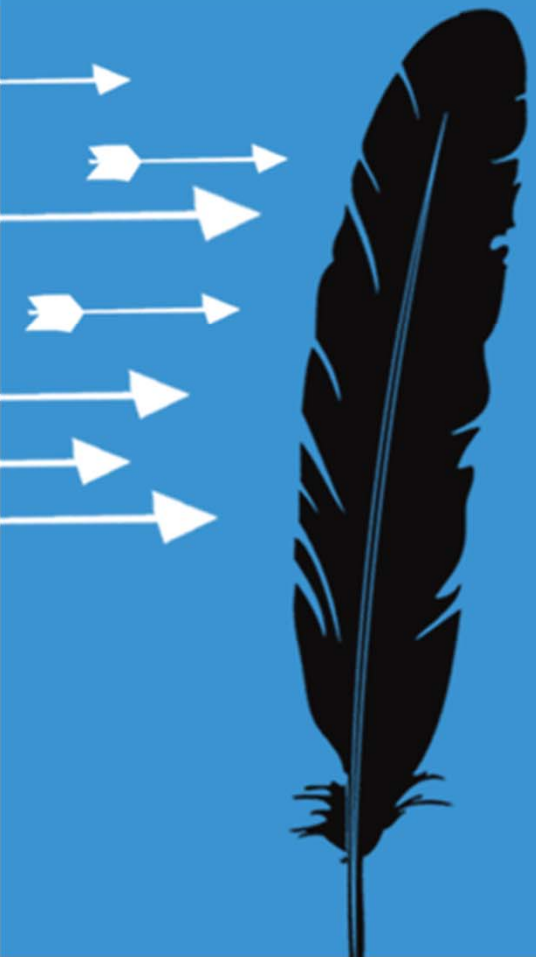
- Turn off host based tunnels by default
- Only authorized tunnels should be allowed
- Configured and Automatic tunnels

Examples

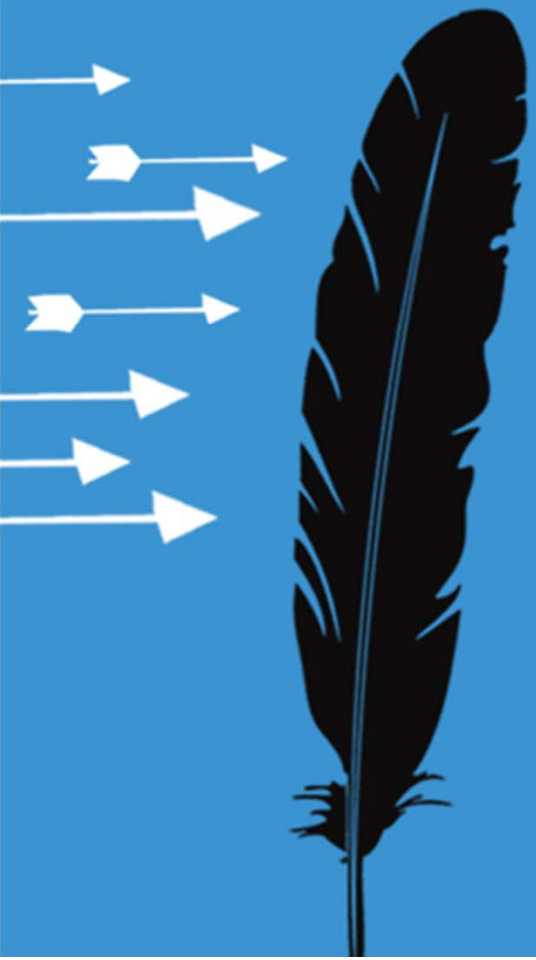
- Block IPv6 in IPv4 from any SRC to any DST
- Allow IPv6 in IPv4 from <Router A> to <Tunnel Broker B>
- Block IPv4 in IPv6 from any SRC to any DST
- Block IPv6 over IPv4 from any SRC to any DST
- ……

Summary Recommendations

- Create IPv6 security policy that parallels current IPv4 security policy
- Protect against rogue Router Advertisements and DHCPv6 servers
- Create default Firewall rules that block all types of transition tunnels



Questions and Answers



Thank You!