HKNOG 1.0
Hong Kong
1 September 2014

Security in an IPv6 World
Myth & Reality

What is the Internet Society?

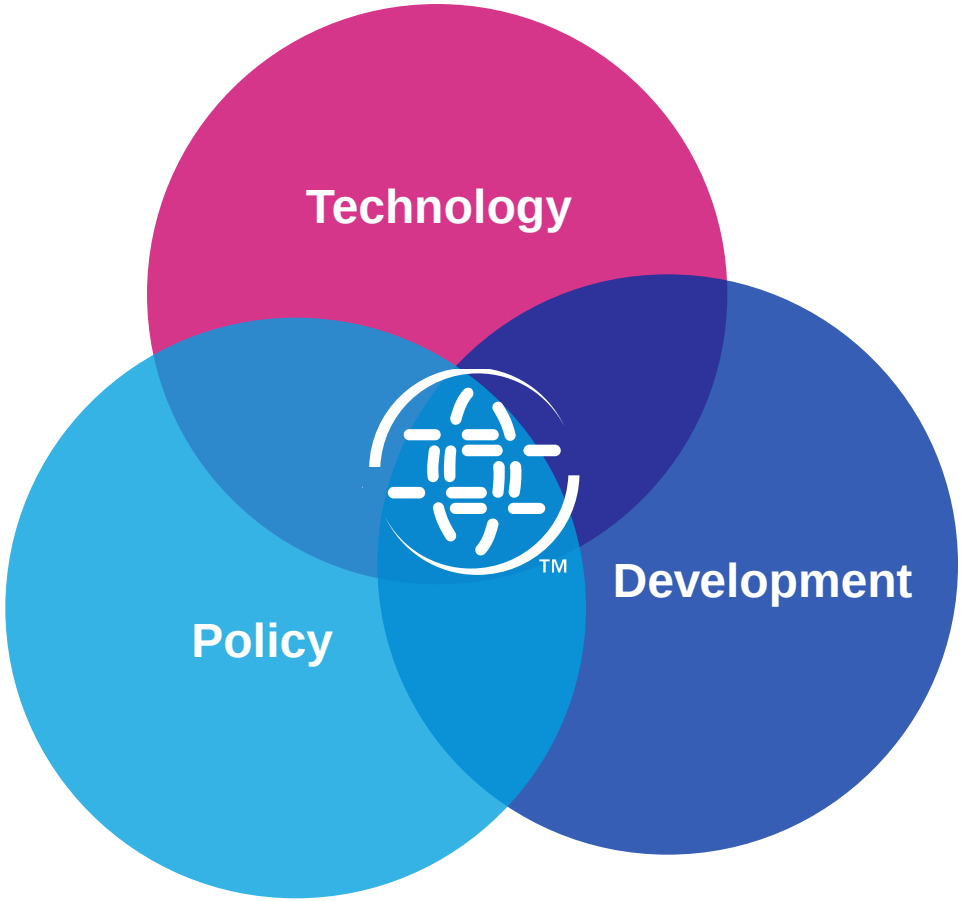
The Internet Society (ISOC) is a cause-based organization that works with governments, industries, and others to ensure the technologies and policies that helped develop and evolve the Internet will continue into the future.

Our programs cultivate an Internet that is open to everyone, everywhere and aim to ensure that it will continue to be a tool for creativity, innovation, and economic growth.

MISSION: To promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world.

Internet Society™

How We Work To Protect Our Internet



Operating at the intersection of **policy**, **technology**, and **development** allows the Internet Society to be a thought leader on issues key to the Internet's continued growth and evolution.

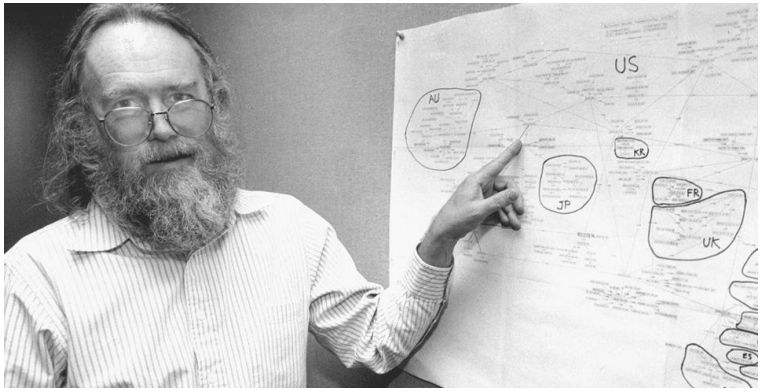
Internet Society

History

Founded in 1992 by Internet pioneers Vint Cerf and Bob Kahn as an international nonprofit organization.

The Internet Society is the organizational home of the Internet Engineering Task Force (IETF), the primary entity responsible for establishing the Internet's open standards and best practices.

For more details, visit
www.internetsociety.org/history



Internet Society™

Global Presence

100+
Chapters Worldwide

65,000+
Members and Supporters

145+
Organization Members

6
Regional Bureaus

18
Countries with ISOC Offices

The Deployment & Operationalization Team

- **Chris Grundemann,** Director, Deployment & Operationalization
- **Dan York,** Senior Content Strategist
- **Megan Kruse,** Technology Outreach Manager
- **Jan Žorž,** Operational Engagement Programme Manager

Internet Society™

Deployment & Operationalization Projects

Internet Society™

The Deploy360 Programme

About Deploy360

The Challenge:

- The IETF creates protocols based on open standards, but some are not widely known or deployed
- People seeking to implement these protocols are confused by a lack of clear, concise deployment information

The Deploy360 Solution:

- Provide hands-on information on IPv6, DNSSEC, TLS for applications, and Securing BGP to advance real-world deployment
- Work with first adopters to collect and create technical resources and distribute these resources to fast following networks

Internet Society™

Deploy360 Components

Web Portal
(Online Knowledge Repository)

- Technical documents
- Audience-specific information
- Blogs & social media

Social Media
(Constant Audience Engagement)

- Twitter
- Facebook
- Google+
- YouTube
- RSS Feeds

Speaking Engagements
(Come Meet Us or Invite Us to Speak)

- IPv6 Summits
- Interop Events
- Network Operators' Groups

ION Conferences
(Hands-on Educational Events)

- Ireland
- Djibouti
- Canada
- Singapore
- India

Web Portal – www.internetsociety.org/deploy360

IPv6, DNSSEC, Securing BGP, TLS for Applications knowledge base including tutorials, case studies, training resources, etc.

Content specific to:

- Network Operators
- Developers
- Content Providers
- Consumer Electronics Manufacturers
- Enterprise Customers

Blog posts

Social media integration

Internet Society™

Social Media Channels

https://twitter.com/deploy360

https://www.facebook.com/Deploy360

http://gplus.to/deploy360

http://www.youtube.com/user/Deploy360

http://www.internetsociety.org/deploy360/feed/

http://soundcloud.com/deploy360/

Internet Society™

Speaking Engagements (External Events)

Consumer Electronics Show

North American IPv6 Task Force

Eurasian Network Operators' Group (ENOG)

Large Installation Systems Administration (LISA) Conference

Interop

Broadband World Forum

IPv6 Webinars

ION Conferences

3-4 events per year, co-located with a diverse set of events in varying locations

Next Event: ION Belfast, 8-9 September 2014

Recent Events:

- ION Djibouti – 2 June 2014
- ION Toronto – 11 November 2013
- ION Krakow – 30 September 2013

Past events in Singapore, Brazil, Slovenia, India, Argentina, and the US

Future events information announced at http://www.internetsociety.org/deploy360/ion/

Internet Society™

Next Steps

Adding more content

- Clearly defined content growth using published roadmaps for IPv6, DNSSEC, Securing BGP, and TLS for applications
- Actively engaged with industry professionals to curate or create deployment content

Adding features based on audience feedback (including yours!)

Adding information in multiple languages

Increasing blogging and social media efforts

Internet Society™

Your Participation

Visit and explore
http://www.internetsociety.org/deploy360

Create Content

- Help us develop materials based on your experiences
- We will credit your work

Define New Features

- Tell us what you need to get started on your own deployment
- We have the flexibility to make changes/additions

Contact us: deploy360@isoc.org

Internet Society™

Best Current Operational Practices (BCOP)

What's a BCOP?

Best Current Operational Practice

- A living document describing the best operational practices currently agreed on by subject matter experts

- Vetted and periodically reviewed by the global network engineering community (GNEC)

The Problem

- Operational knowledge tends to be “tribal”
- Presentations, hallway conversations, internal documents, in someone’s head…
- Technology, tools, and practices change over time…
- There are hundreds of operational forums globally
- Archives stored in different formats, some searchable, rarely have speech text or video, no vetting, and state unknown.
- **How do I find up-to-date, relevant information when I need it?**

Internet Society™

The BCOP Solution

Open, Transparent, Bottom-up, and Community led

- **Community driven, community written, community vetted Best Current Operational Practices from an open forum, list, and publicly searchable site.**
- **Community written and approved Development Process for BCOPs**
- **Everyone is welcome to participate**

80/20 model

BCOP efforts around the world:

http://www.internetsociety.org/deploy360/about/bcop/

•Africa region: A BCOP group was started under AfNOG, lead by Douglas Onyango

•Asia: BCOP Task Force started at JANOG, co-chaired by Seiichi Kawamura and Yoshinobu Matsuzaki, NZNOG BCOP starting up, lead by Dean Pemberton

- No whole-region effort started yet

•Europe: RIPE BCOP Task Force created, co-chaired by Benno Overeider and Jan Žorž

•Latin America: A BCOP Task Force was started under LACNOG, lead by Luis Balbinot and Pedro R Torres Jr.

•North America: NANOG BCOP Committee established, lead by Aaron Hughes and Chris Grundemann

Internet Society™

BCOP documents currently in progress:

- *IPv6 troubleshooting for residential helpdesks (RIPE)*
- *DNSSEC for authoritative name servers (RIPE)*
- *(e)BGP configuration (RIPE & NANOG)*
- *IPv6 Peering (NANOG)*
- Public Peering Exchange Participant (NANOG)
- Ethernet OAM (NANOG)
- Anti-DDoS (NANOG)
- BCP 38 (NANOG)
- Africa specific IPv6 FAQ (AfNOG)

Internet Society™

Potential Topics for Additional BCOPs

http://www.internetsociety.org/deploy360/about/bcop/topics/

- How to test your network performance
- How to check your visibility from global Internet
- De-Aggregation: strict filtering /48s out of /32
- How are operators using IRR?
- IPv6 enterprise network renumbering scenarios, considerations, and methods
- DNS Policies
- Email Policies
- ICMP Filtering
- … (we need more suggestions)

Internet Society™

Next Steps

Where are we going from here?

- Continue to bootstrap new efforts as needed
- Develop new BCOP documents
  - Lots of low-hanging fruit
- Review and update existing BCOP documents
- Start thinking & talking about Global coordination

Internet Society™

Get Involved Today!

Join this grass-roots effort at the ground floor!

- Contribute to an existing draft
- Offer ideas for new drafts
- Kick off a new document
- Start a local or regional BCOP effort
- Email deploy360@isoc.org for more information

Internet Society™

Operators & the IETF

Project Rationale

In a perfect world:

- Operators participate in the IETF standards process
- New standards work perfectly once deployed
- Deployment and operationalization concerns are addressed
- Operators know when to participate, and do so in a timely manner

In reality:

- Network operators are not engaged enough in the IETF process
- Many operators do not join IETF mailing lists or attend meetings
- Operators do not know standards are even under development
- Standards deemed ready by recent IETF attendees sometimes turn out to be problematic in operational networks

Internet Society™

ISOC's Role

The discussion about operator input (or lack thereof) into the IETF process is not new, but there was very little hard data to back up anecdotal evidence

DO created and marketed an online survey in 2014 to understand the operators' issues so that we can address the concerns and ultimately help make better standards

We are working to facilitate communications between operators and the IETF to help ensure operational realities inform standards development

Internet Society™

Initial Survey Results (Part 1)

Most survey participants were Operators/Engineers/Architects; more than 90% hold primarily technical roles

Many have heard of the IETF and know what it does, but do not know how to participate

A strong majority claim they are interested in IETF mailing lists, find the content relevant, believe it's important to their jobs, but don't have enough time to participate in mailing lists

Internet Society™

Initial Results (Part 2)

~50% do not participate in the IETF in any form; ~30% participate only on mailing lists

+50% believe operator input is welcome; 64% say they do NOT rely on vendors to represent them

50% of respondents claim to have a managerial role

82% say that they do not have a travel budget for IETF meetings

Internet Society™

Next Steps

Analyze and synthesize survey results and feedback

Collect data into an IETF Internet-Draft, including a report on the challenges to greater operator engagement and a summary of potential solutions, including:

- Things operators and operator groups can do to help provide more input
- Things the IETF can do to help operators participate
- Things ISOC can do to help facilitate greater operator engagement

Internet Society™

Security in an IPv6 World
Myth & Reality

Time to get Technical

Internet Society™

This talk…

Aims to debunk the most common IPv6 security myths

Is NOT a comprehensive look at IPv6 security practices

Internet Society™

Let’s get to busting

Some Myths…

Myth:
I’m Not Running IPv6, I Don’t Have to Worry

Myth:
I’m Not Running IPv6, I Don’t Have To Worry

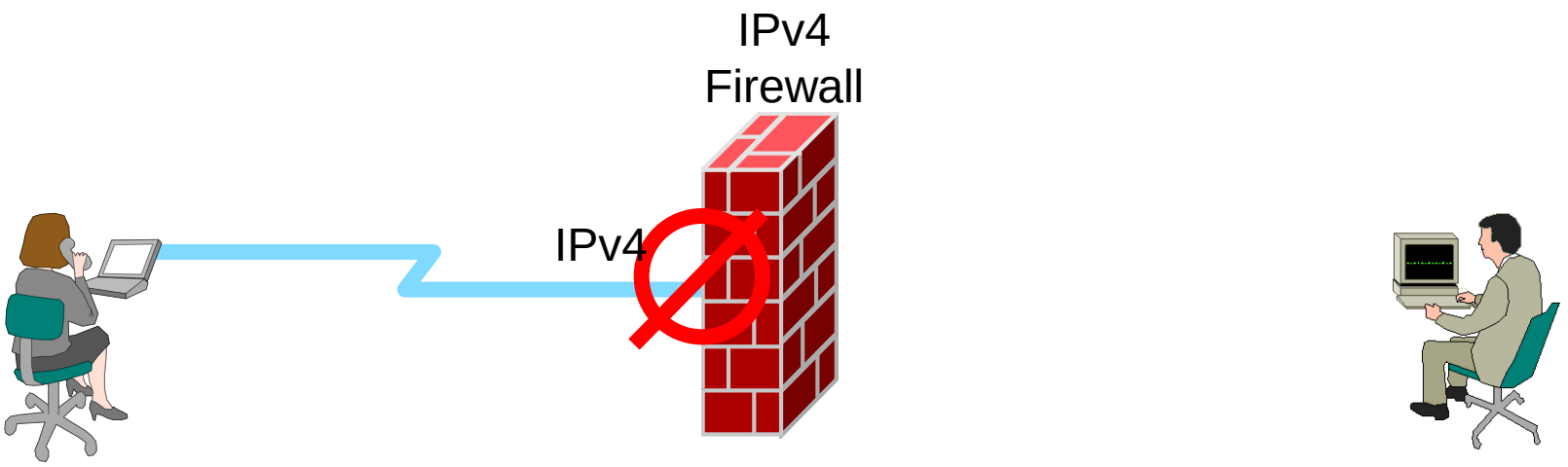
Reality:
Your Applications are Using IPv6 Already

- Linux, Mac OS X, BSD, and Microsoft Vista/Windows 7 systems all come with IPv6 capability, some even have IPv6 enabled by default (IPv6 preferred)
  - They may try to use IPv6 first and then fall-back to IPv4
- If you are not protecting your IPv6 nodes then you have just allowed a huge back-door to exist!

Internet Society™

Myth:
I’m Not Running IPv6, I Don’t Have To Worry

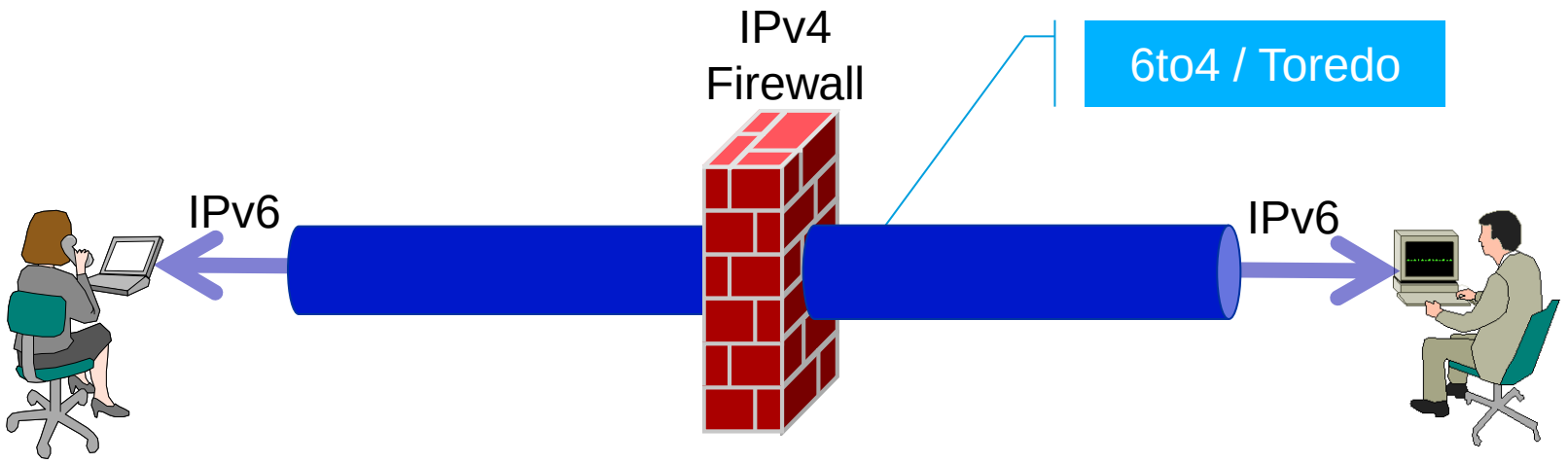
Reality:
Your Users are Using IPv6 Already



Internet Society™

Myth:
I’m Not Running IPv6, I Don’t Have To Worry

Reality:
Your Users are Using IPv6 Already



Internet Society™

MYTH:
IPv6 Has Security Designed In

MYTH:
IPv6 Has Security Designed In

Reality:
IPsec Is Not New

IPsec exists for IPv4

IPsec mandates in IPv6 are no guarantee of security

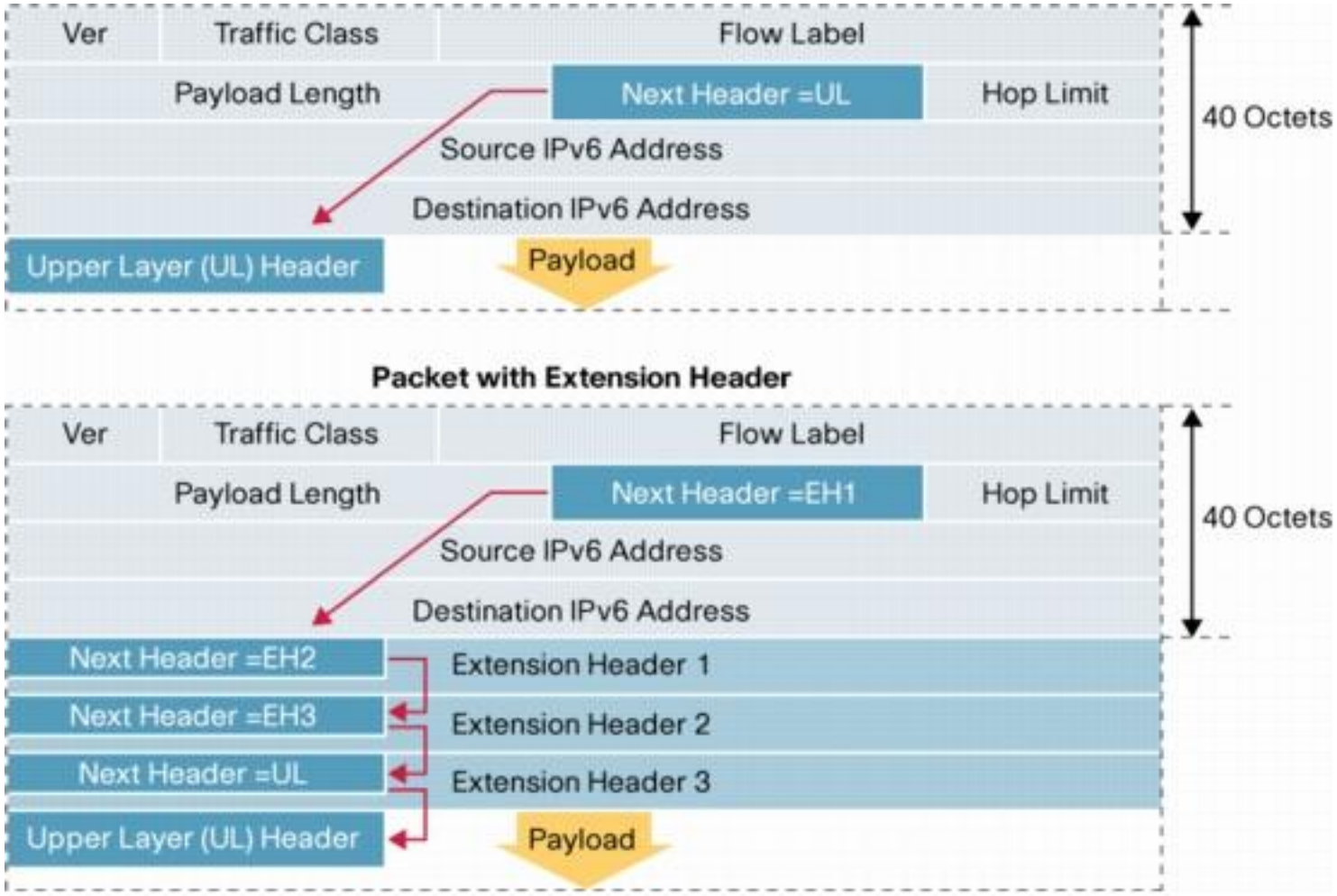
Internet Society™

MYTH:
IPv6 Has Security Designed In

Reality:
IPv6 Was Designed 15-20 Years Ago

Internet Society™

Reality:
Extension Headers



http://www.cisco.com/en/US/technologies/tk648/tk872/technologies_white_paper0900aecd8054d37d.html

Internet Society™

MYTH:
IPv6 Has Security Designed In

Reality:

Routing Header Type 0 (RH0) – Source Routing

- **Deprecated in RFC 5095:**

The functionality provided by IPv6's Type 0 Routing Header can be exploited in order to achieve traffic amplification over a remote path for the purposes of generating denial-of-service traffic.

Internet Society™

MYTH:
IPv6 Has Security Designed In

Reality:

Hop-by-Hop Options Header

- **Vulnerable to low bandwidth DOS attacks**
- **Threat detailed in draft-krishnan-ipv6-hopbyhop**

Internet Society™

MYTH:
IPv6 Has Security Designed In

Reality:

Extension Headers are vulnerable in general

- **Large extension headers**
- **Lots of extension headers**
- **Invalid extension headers**

Internet Society™

MYTH:
IPv6 Has Security Designed In

Reality:

Rogue Router Advertisements (RAs)

- **Can renumber hosts**
- **Can launch a Man In The Middle attack**
- **Problem documented in RFC 6104**

In this document, we summarise the scenarios in which rogue RAs may be observed and present a list of possible solutions to the problem.

Internet Society™

MYTH:
IPv6 Has Security Designed In

Reality:

Forged Neighbor Discovery messages

ICMP Redirects – just like IPv4 redirects

MYTH:
IPv6 Has Security Designed In

Reality:
Many Attacks Are Above Or Below IP

- Buffer overflows
- SQL Injection
- Cross-site scripting
- E-mail/SPAM (open relays)

Internet Society™

Myth:
NO IPv6 NAT Means Less Security

Myth:
NO IPv6 NAT Means Less Security

Reality:
Stateful Firewalls Provide Security

- NAT can actually reduce security

Internet Society™

Myth:
IPv6 Networks are too Big to Scan

Myth:
IPv6 Networks are too Big to Scan

Reality:

SLAAC - EUI-64 addresses (well known OUIs)

- **Tracking!**

DHCPv6 sequential addressing (scan low numbers)

6to4, ISATAP, Teredo (well known addresses)

Manual configured addresses (scan low numbers, vanity addresses)

Exploiting a local node

- **ff02::1 - all nodes on the local network segment**
- **IPv6 Node Information Queries (RFC 4620)**
- **Neighbor discovery**
  - Leveraging IPv4 (Metasploit Framework "ipv6_neighbor")

IPv6 addresses leaked out by application-layer protocols (email)

Internet Society™

Myth:
IPv6 Networks are too Big to Scan

Reality:
Privacy Addresses (RFC 4941)

Privacy addresses use MD5 hash on EUI-64 and random number

Often temporary – rotate addresses

- **Frequency varies**
- **Often paired with dynamic DNS (firewall state updates?)**

Makes filtering, troubleshooting, and forensics difficult

Alternative: Randomized DHCPv6

- **Host: Randomized IIDs**
- **Server: Short leases, randomized assignments**

Internet Society™

Myth:
IPv6 is too New to be Attacked

Myth:
IPv6 is too New to be Attacked

Reality:
Tools Are Already Available

- THC IPv6 Attack Toolkit
- IPv6 port scan tools
- IPv6 packet forgery tools
- IPv6 DoS tools

Internet Society™

Myth:
IPv6 is too New to be Attacked

Reality:
Bugs And Vulnerabilities Published

- Vendors
- Open source software

Internet Society™

Myth:
IPv6 is too New to be Attacked

Reality:

Search For “*securityfocus.Com Inurl:bid IPv6*”

Myth:
96 more bits, no magic (It’s just like IPv4)

Myth:
96 more bits, no magic (It's just like IPv4)

Reality:
IPv6 Address Format Is Drastically New

- 128 bits vs. 32 bits
- Hex vs. Decimal
- Colon vs. Period
- Multiple possible formats (zero suppression, zero compression)
- Logging, grep, filters, etc.

Internet Society™

Myth:
96 more bits, no magic (It's just like IPv4)

Reality:
Multiple Addresses On Each Host

- Same host appears in logs with different addresses

Myth:
96 more bits, no magic (It's just like IPv4)

Reality:
Syntax Changes

- Training!

Myth:
Configure IPv6 Filters Same AS IPv4

Myth:
Configure IPv6 Filters Same As IPv4

Reality:
DHCPv6 && ND Introduce Nuance

- Neighbor Discovery uses ICMP
- DHCPv6 message exchange:
  - Solicit: [your link local]:546 -> [ff02::1:2]:547
  - Advertise: [upstream link local]:547 -> [your link local]:546
  - and two more packets, both between your link locals.

Internet Society™

Reality: Example Firewall Filter (mikrotik)

Flags: X - disabled, I - invalid, D - dynamic

0 ;;; Not just ping - ND runs over icmp6.

chain=input action=accept protocol=icmpv6 in-interface=ether1-gateway

1 chain=input action=accept connection-state=established in-interface=ether1-gateway

2 ;;; related means stuff like FTP-DATA

chain=input action=accept connection-state=related in-interface=ether1-gateway

3 ;;; for DHCP6 advertisement (second packet, first server response)

chain=input action=accept protocol=udp src-address=fe80::/16 dst-address=fe80::/16 in-interface=ether1-gateway dst-port=546

4 ;;; ssh to this box for management (note non standard port)

chain=input action=accept protocol=tcp dst-address=[myaddr]/128 dst-port=2222

5 chain=input action=drop in-interface=ether1-gateway

Internet Society™

Myth:
It supports IPv6

Myth:
It supports IPv6

Reality:
It Probably Doesn't

At least not in all the ways you need it too…

- Detailed requirements (RFP)
  - RIPE-554
- Lab testing
- Independent/outside verification

Internet Society™

Myth:
There are no IPv6 Security BCPs yet

Myth:
There are no IPv6 Security BCPs yet

Reality:
There Are!

Perform IPv6 filtering at the perimeter

Use RFC2827 filtering and Unicast RPF checks throughout the network

Use manual tunnels (with IPsec whenever possible) instead of dynamic tunnels and deny packets for transition techniques not used

Use common access-network security measures (NAC/802.1X, disable unused switch ports, Ethernet port security, MACSec/TrustSec) because SeND won't be available any time soon

Strive to achieve equal protections for IPv6 as with IPv4

Continue to let vendors know what you expect in terms of IPv6 security features

Internet Society™

Myth:
There are no IPv6 Security Resources

Myth:
There are no IPv6 Security Resources

Reality:
There Are!

***IPv6 Security*, By Scott Hogg and Eric Vyncke, Cisco Press, 2009**

Guidelines for the Secure Deployment of IPv6 Recommendations of the National Institute of Standards and Technology

Deploy360 has a section specifically on IPv6 Security

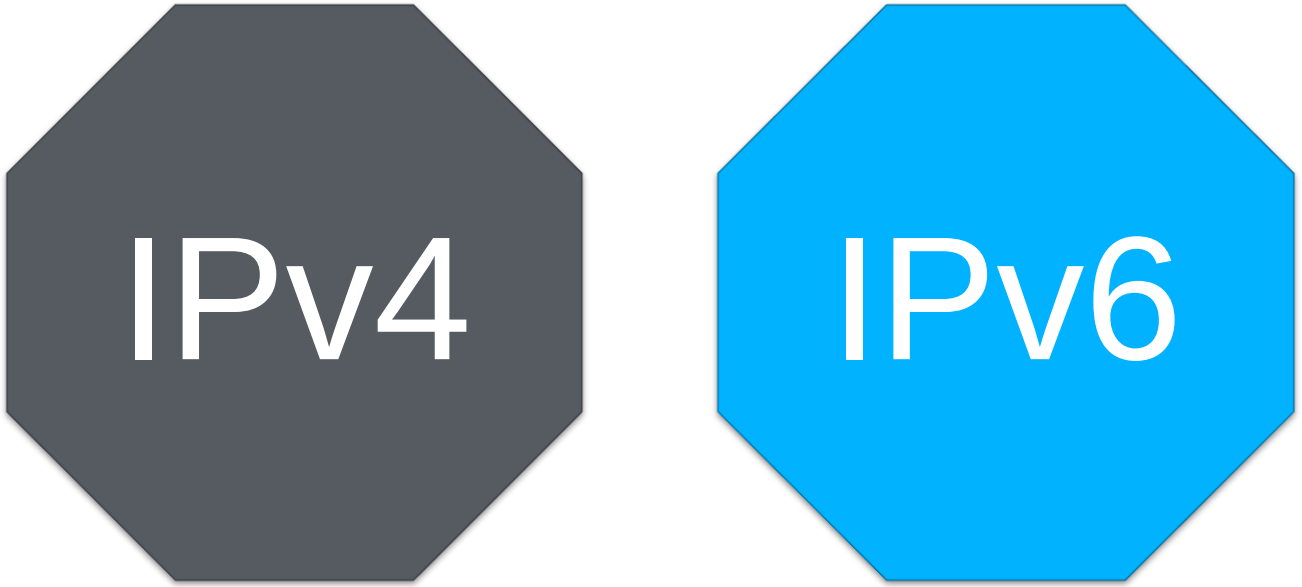
Search engines are your friend!

Internet Society™

The Reality of Dual-Stack

Two sets of filters

Two sets of bugs



Internet Society™

Thank you!

Gratitude and Credit:

- Scott Hogg – My IPv6 Security Guru
- Rob Seastrom – For the Mikrotik example
- The Internet – Lots of searching
- You – Thanks for listening!

@ChrisGrundemann
http://chrisgrundemann.com
http://www.internetsociety.org/deploy360/

Internet Society™