IPv6 Security, Or... How Not to Deploy IPv6

Mark Ciecior

Me

Agenda

- Why is IPv6 a Thing?
- Deployment Metrics
- What's Different about IPv6?
- Security Failures
  - *(Opportunities for Improvement)*

Why is IPv6 a Thing?

List of assigned /8 blocks [edit]

Block	Organization	IANA date	RIR date	Notes
4.0.0.0/8	Level 3 Communications, Inc.	1992-12	1992-12-01	Originally Bolt Beranek and Newman Inc. (then GTE, then Genuity) 1992 Updated to Level 3 Communications, Inc. in 2007-04.
12.0.0.0/8	AT&T Services	1995-06	1983-08-23	Originally AT&T Bell Laboratories, retained by AT&T when Bell Labs was
17.0.0.0/8	Apple Inc.	1992-07	1990-04-16	
19.0.0.0/8	Ford Motor Company	1995-05	1988-06-15	
38.0.0.0/8	PSINet, Inc.	1994-09	1991-04-16	PSINet, then Cogent Communications.
44.0.0.0/8	Amateur Radio Digital Communications	1992-07	1992-07-01	
48.0.0.0/8	Prudential Securities Inc.	1995-05	1990-12-07	The Prudential Insurance Company of America.
56.0.0.0/8	US Postal Service	1994-06	1992-11-02	
73.0.0.0/8	Comcast Corporation	N/A	2005-04-19	Comcast Cable Communications LLC.

List of assigned /8 blocks to the United States Department of Defense [edit]

Block	Organization	IANA date	RIR date	Notes
6.0.0.0/8	Army Information Systems Center	1994-02	1994-02-01	Headquarters, USAISC.
7.0.0.0/8	DoD Network Information Center	1995-04	1997-11-24	Formerly IANA - Reserved 1995-04. Entirely assigned to DoD Network Information Center (DNIC) 1997-11-24 Updated to Administered by ARIN not before 2007.
11.0.0.0/8	DoD Intel Information Systems	1993-05	1984-01-19	
21.0.0.0/8	DDN-RVN	1991-07	1991-07-01	DoD Network Information Center (DNIC).
22.0.0.0/8	Defense Information Systems Agency	1993-05	1989-06-26	DoD Network Information Center (DNIC).
26.0.0.0/8	Defense Information Systems Agency	1995-05	1995-05-01	DoD Network Information Center (DNIC).
28.0.0.0/8	DSI-North	1992-07		DoD Network Information Center (DNIC).
29.0.0.0/8	Defense Information Systems Agency	1991-07	1991-07-01	DoD Network Information Center (DNIC).
30.0.0.0/8	Defense Information Systems Agency	1991-07	1991-07-01	DoD Network Information Center (DNIC).
33.0.0.0/8	DLA Systems Automation Center	1991-01	1991-01-01	DoD Network Information Center (DNIC).
55.0.0.0/8	DoD Network Information Center	1995-04	1996-10-26	Headquarters, USAISC. Formerly Boeing Computer Services 1995-04. Updated to DoD Network Information Center in 2007-02.
214.0.0.0/8	US-DOD	1998-03	1998-03-27	DoD Network Information Center (DNIC).
215.0.0.0/8	US-DOD	1998-03	1998-06-05	DoD Network Information Center (DNIC).

1. Introduction

IP version 6 (IPv6) is a new version of the Internet Protocol, designed as a successor to IP version 4 (IPv4) [RFC-791]. The changes from IPv4 to IPv6 fall primarily into the following categories:

- Expanded Addressing Capabilities

  IPv6 increases the IP address size from 32 bits to 128 bits, to support more levels of addressing hierarchy, a much greater number of addressable nodes, and simpler auto-configuration of addresses. The scalability of multicast routing is improved by adding a "scope" field to multicast addresses. And a new type of address called an "anycast address" is defined, used to send a packet to any one of a group of nodes.

- Header Format Simplification

  Some IPv4 header fields have been dropped or made optional, to reduce the common-case processing cost of packet handling and to limit the bandwidth cost of the IPv6 header.

- Improved Support for Extensions and Options

  Changes in the way IP header options are encoded allows for more efficient forwarding, less stringent limits on the length of options, and greater flexibility for introducing new options in the future.

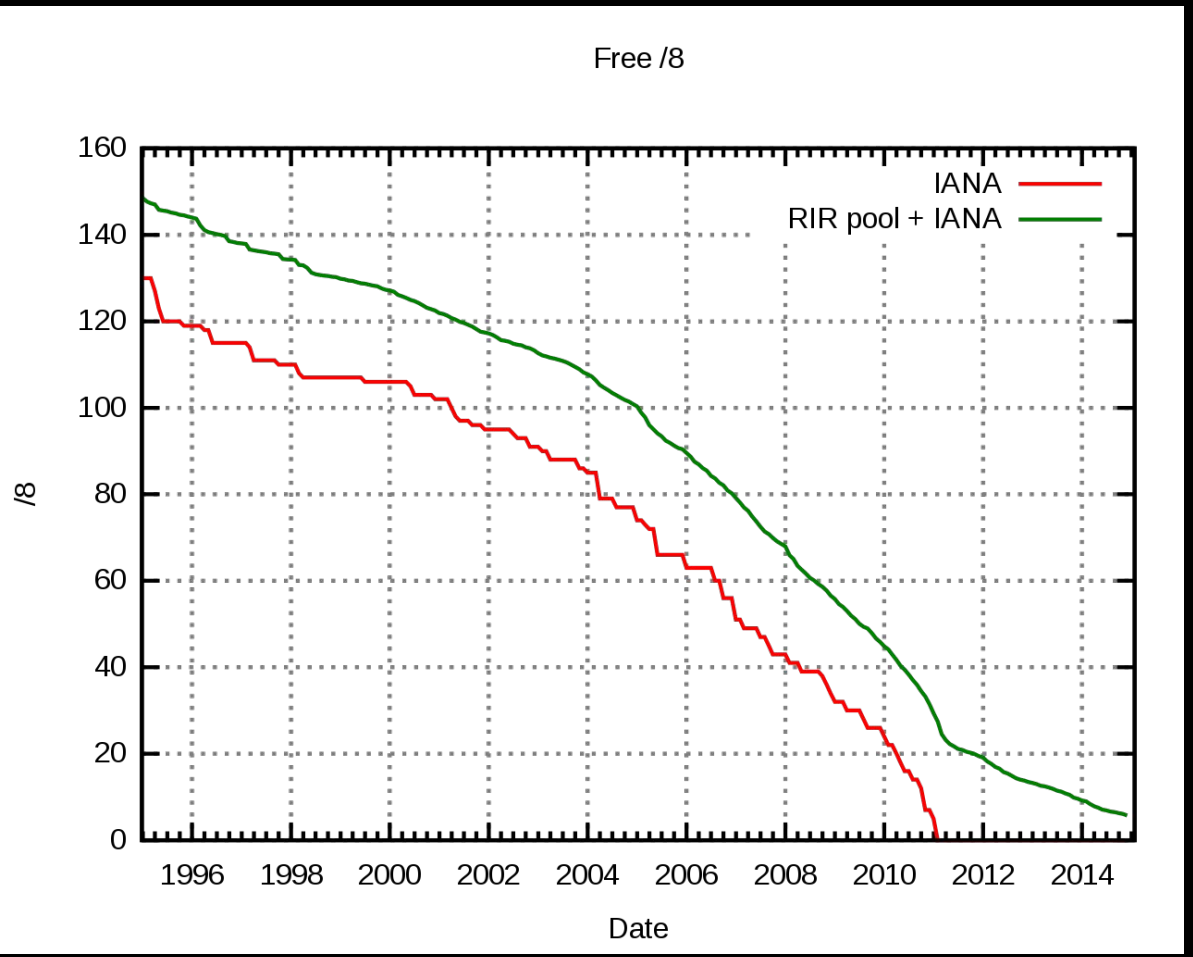
- Flow Labeling Capability

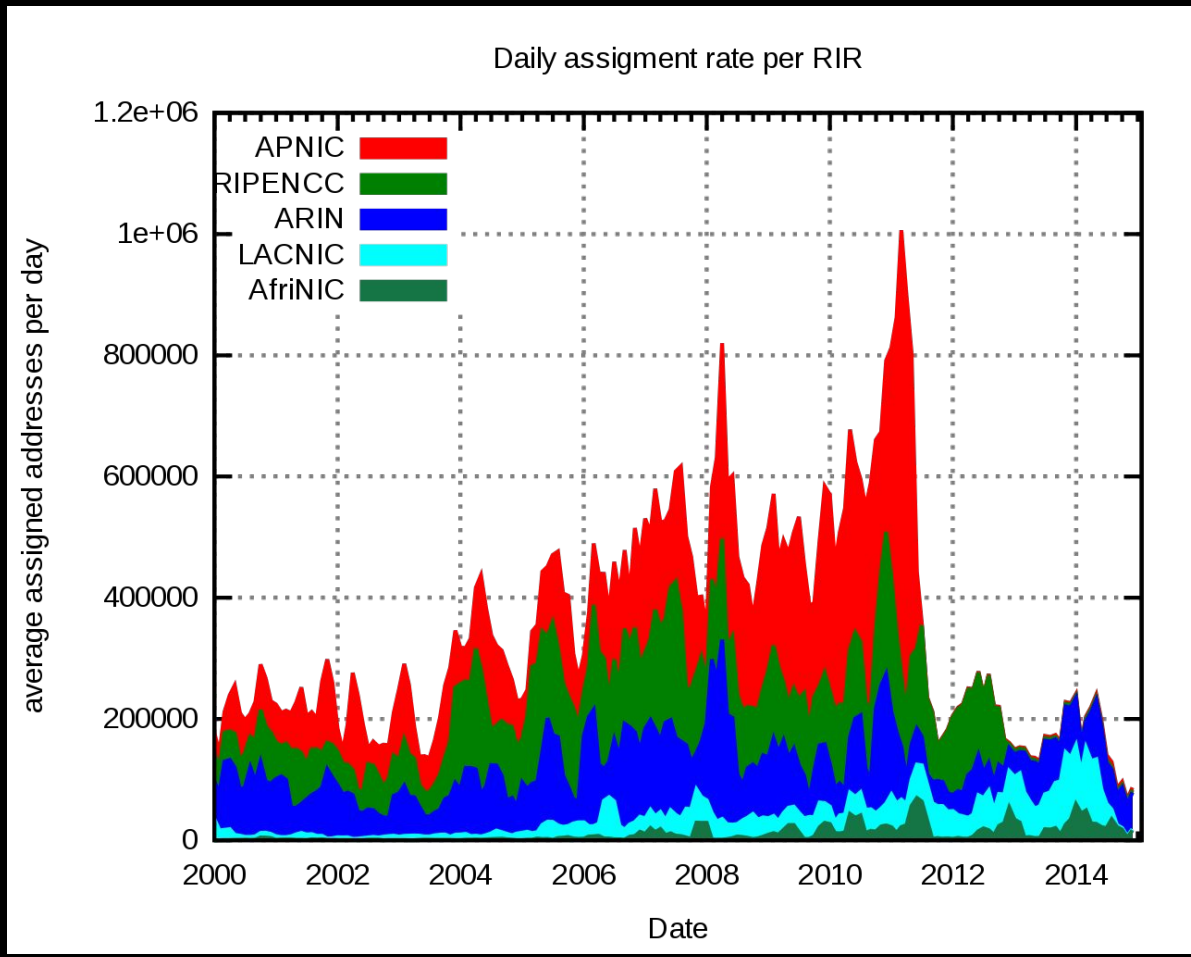
  A new capability is added to enable the labeling of packets belonging to particular traffic "flows" for which the sender requests special handling, such as non-default quality of service or "real-time" service.

- Authentication and Privacy Capabilities

  Extensions to support authentication, data integrity, and (optional) data confidentiality are specified for IPv6.

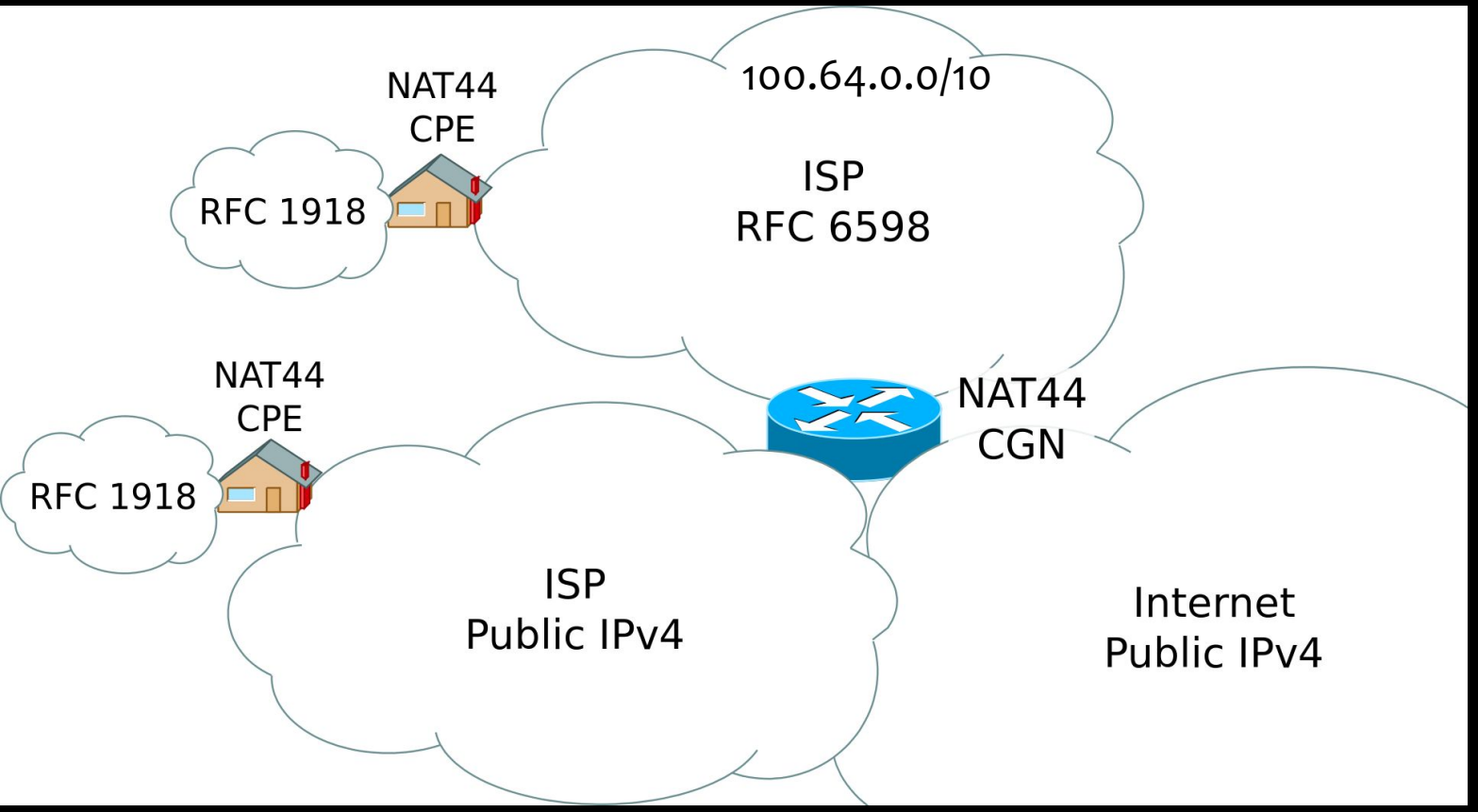
Why is IPv6 a Thing?

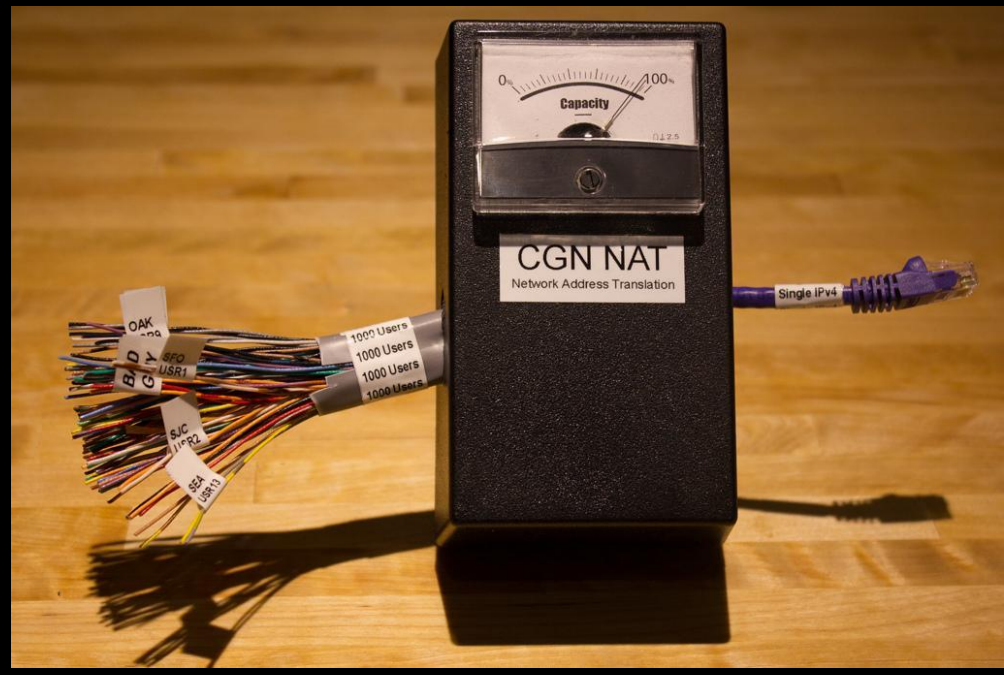




Source: IANA, RIPE

Why is IPv6 a Thing? – Carrier Grade NAT





Why is IPv6 a Thing? – Carrier Grade NAT

5. 2010 Summary of Results

The tables below summarize results from the 2010 NAT444 testing at CableLabs, Time Warner Cable, and Rogers Communications. They are included for comparison with 2011 results, documented above.

5.1. Case 1: Single Client, Single Home Network, Single Service Provider

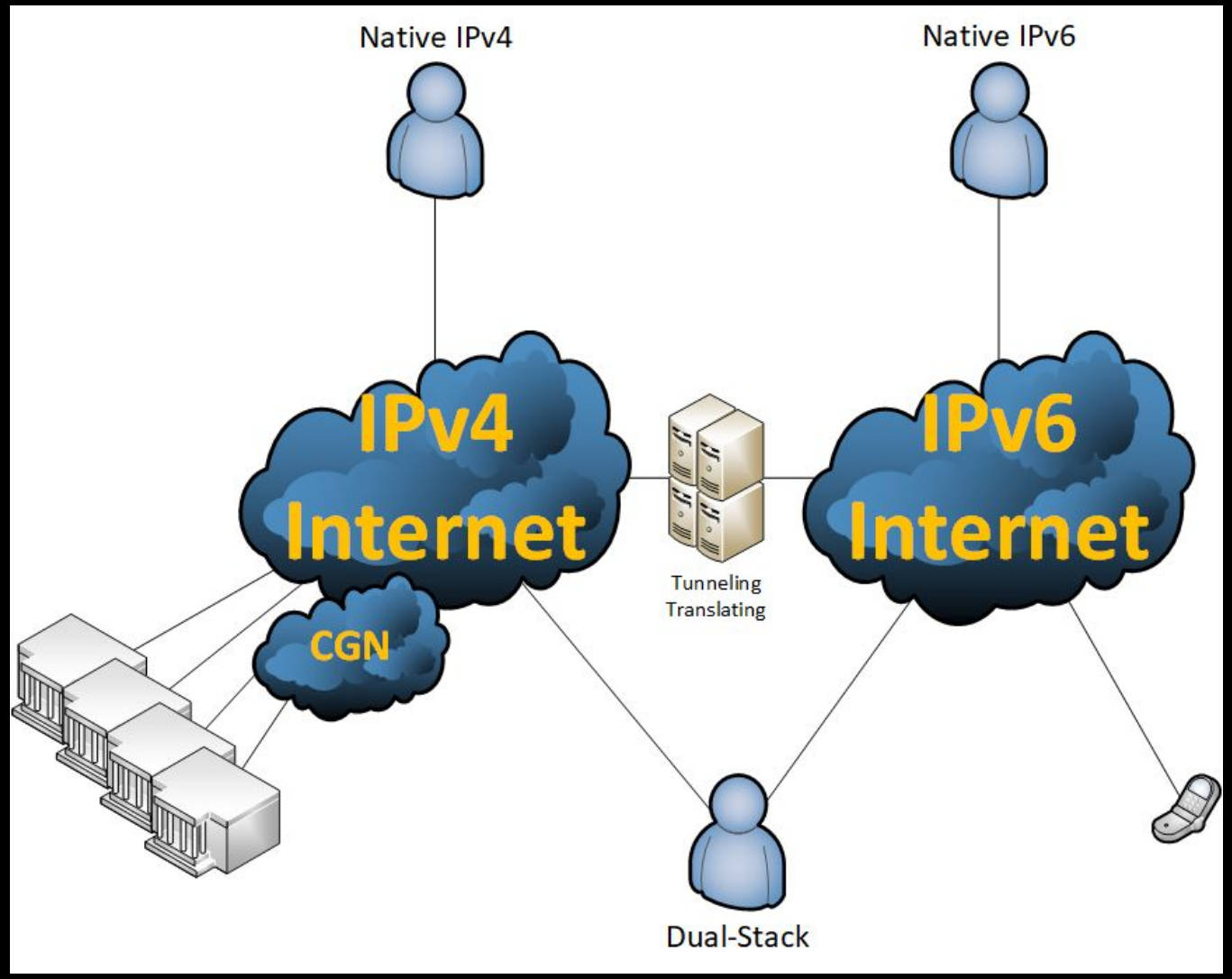
Test Case	Results	Notes
Web browsing	pass	
Email	pass	
FTP download	pass	performance degraded on very large downloads
BitTorrent leeching	pass	
BitTorrent seeding	fail	

(continued)

Xbox online	pass	Blocked by some LSNs.
Xbox network test	fail	Your NAT type is moderate. For best online experience you need an open NAT configuration. You should enable Universal Plug and Play (UPnP) on the router.
Nintendo Wii	pass behind one LSN, fail behind another	
PlayStation 3	pass	
Team Fortress 2	fail	pass behind one LSN, but performance degraded
StarCraft II	pass	
World of Warcraft	pass	
Call of Duty	pass	performance degraded behind one LSN
SlingCatcher	fail	
Netflix Party (Xbox)	fail	pass behind one LSN
Hulu	pass	performance degraded behind one LSN
AIM File Transfer	pass	performance degraded

Why is IPv6 a Thing? – Today's Internet

- LTE Phones
- Content Providers
- APNIC Users
- Most Users

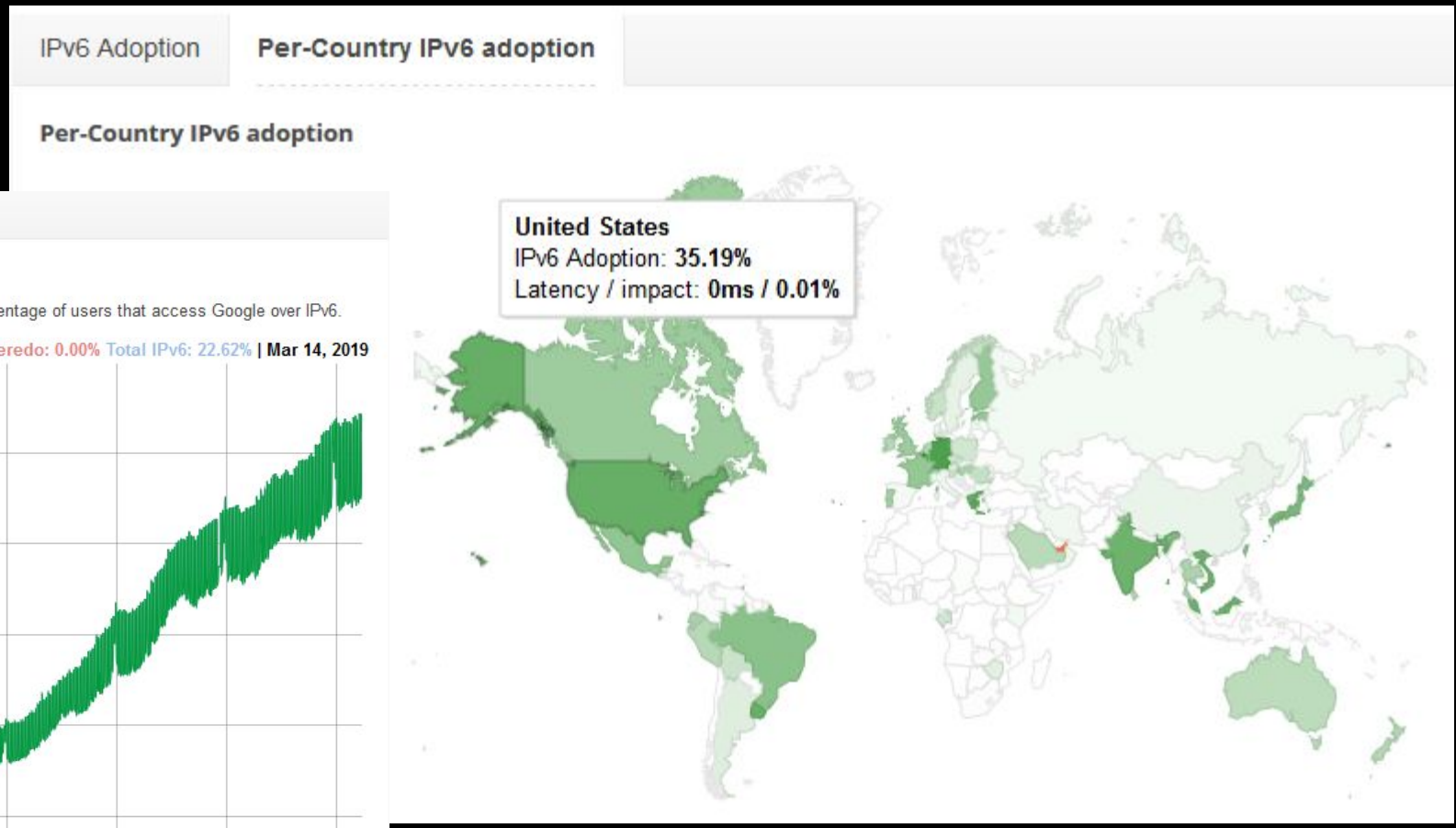


Why is IPv6 a Thing? – AAAA Records

- A Record -> IPv4
- AAAA Record -> IPv6
- Global IPv6 Address ==> AAAA request
- Happy Eyeballs Standard

```
ubuntu@ip-172-31-8-51:~$ dig facebook.com A +short
31.13.71.36
ubuntu@ip-172-31-8-51:~$ dig facebook.com AAAA +short
2a03:2880:f111:83:face:b00c:0:25de
ubuntu@ip-172-31-8-51:~$
```

Deployment Metrics

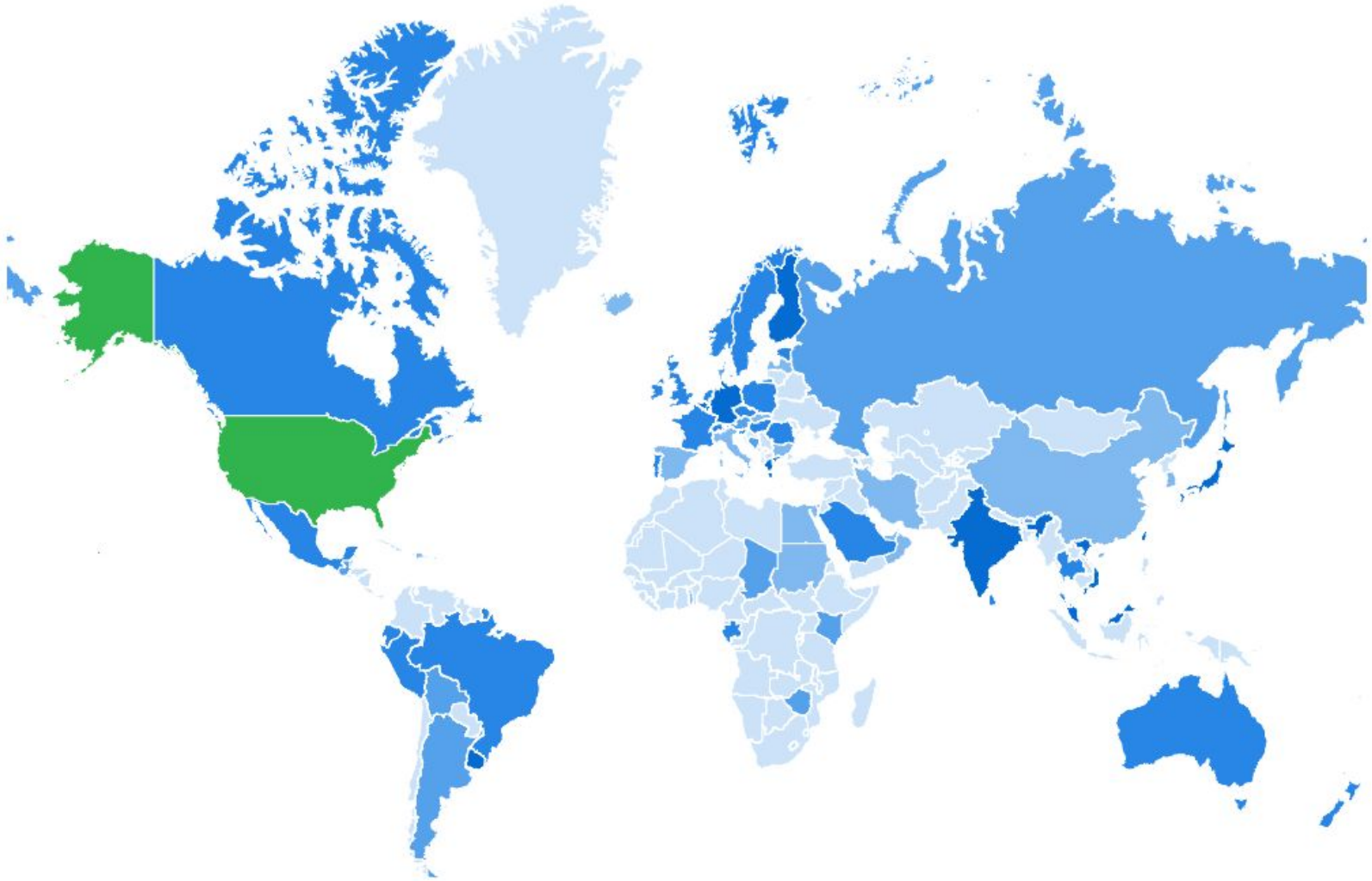


Deployment Metrics

United States 54.75% Adoption

Export All

PER-COUNTRY ADOPTION MAP



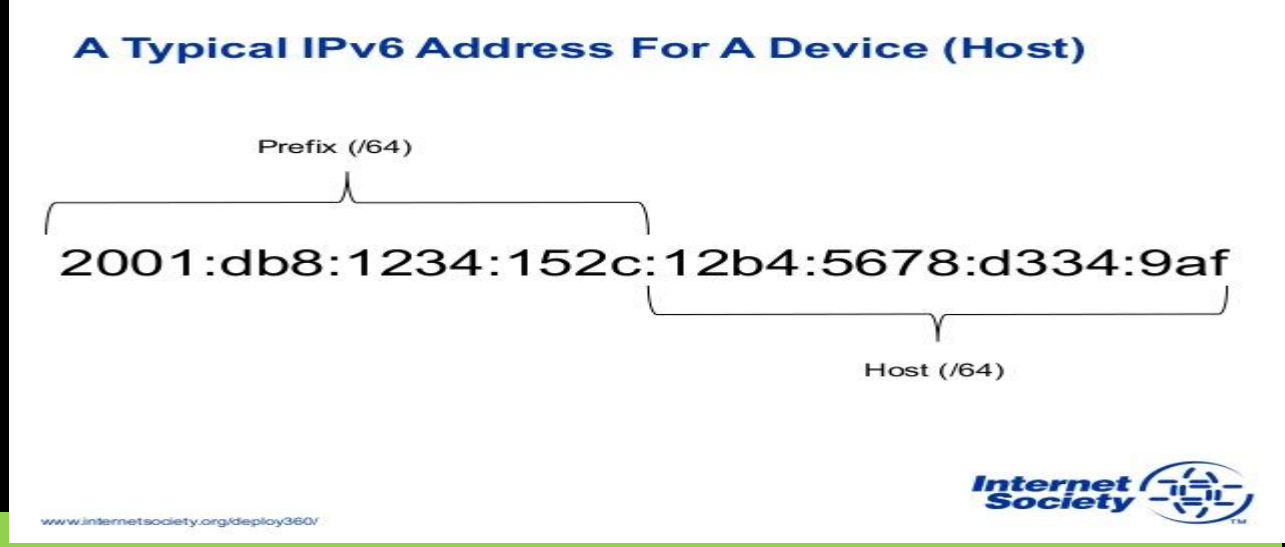
Akamai What We Do Products Resources

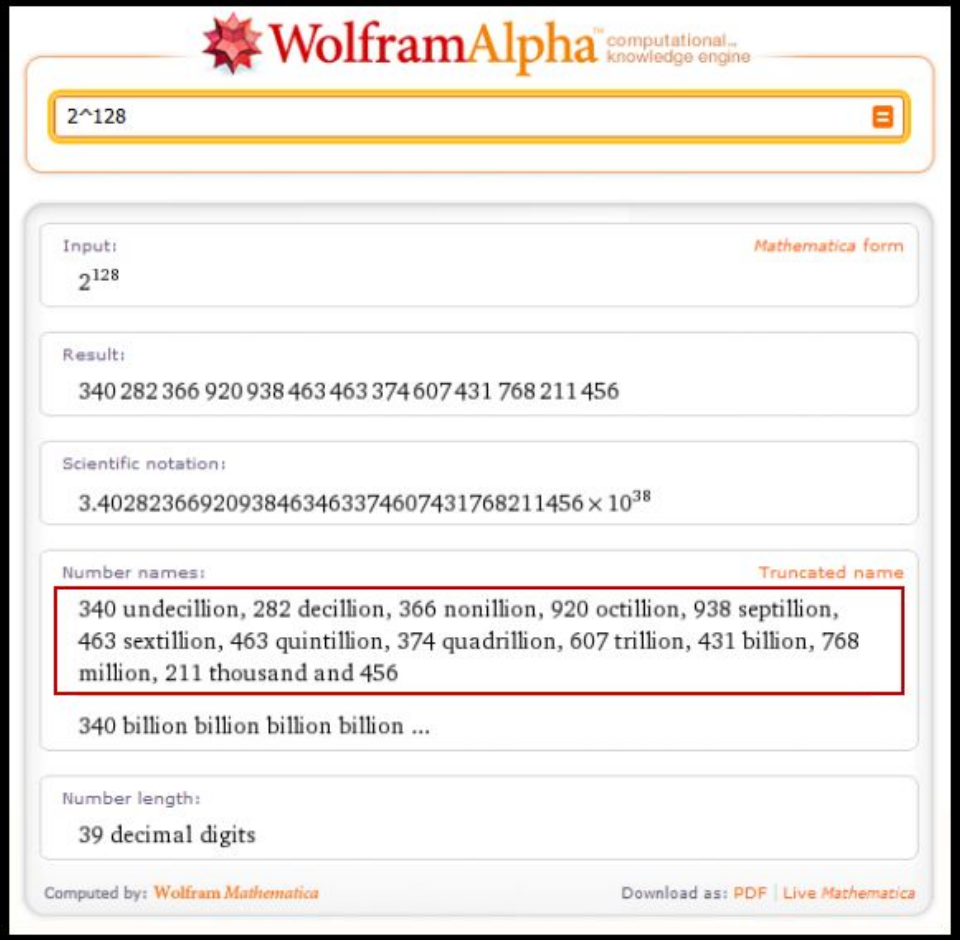
IPv6 Adoption By Networks

**Networks data is limited to the top 200 networks ranked by total IPv6 hits to platform.*

RANK	IPV6%	NETWORK
1	90.9%	Reliance Jio Infocomm Limited
2	68.4%	AT&T Communications Americas
3	66.2%	Comcast Cable
4	63.3%	Verizon Business
5	50%	Charter Communications Inc - TWC
6	95.9%	T-Mobile
7	75.7%	Sprint Communications
8	60.1%	Deutsche Telekom Germany
9	35.9%	Bharti Airtel Enterprise Ltd.
10	51.1%	Cox Communications Inc
11	80.1%	Sky Broadband
12	53%	KDDI Corporation

What's Different about IPv6?





An IPv6 address (in hexadecimal)

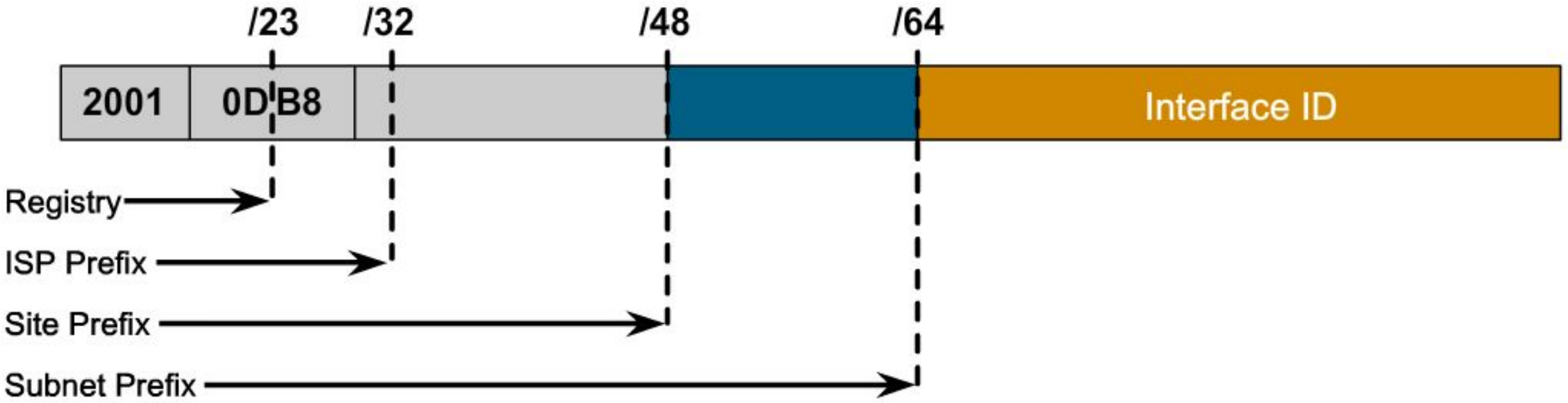
2001:0DB8:AC10:FE01:0000:0000:0000:0000

2001:0DB8:AC10:FE01:: Zeroes can be omitted

0010000000000001:0000110110111000:1010110000010000:1111111000000001:

0000000000000000:0000000000000000:0000000000000000:0000000000000000

What’s Different about IPv6?



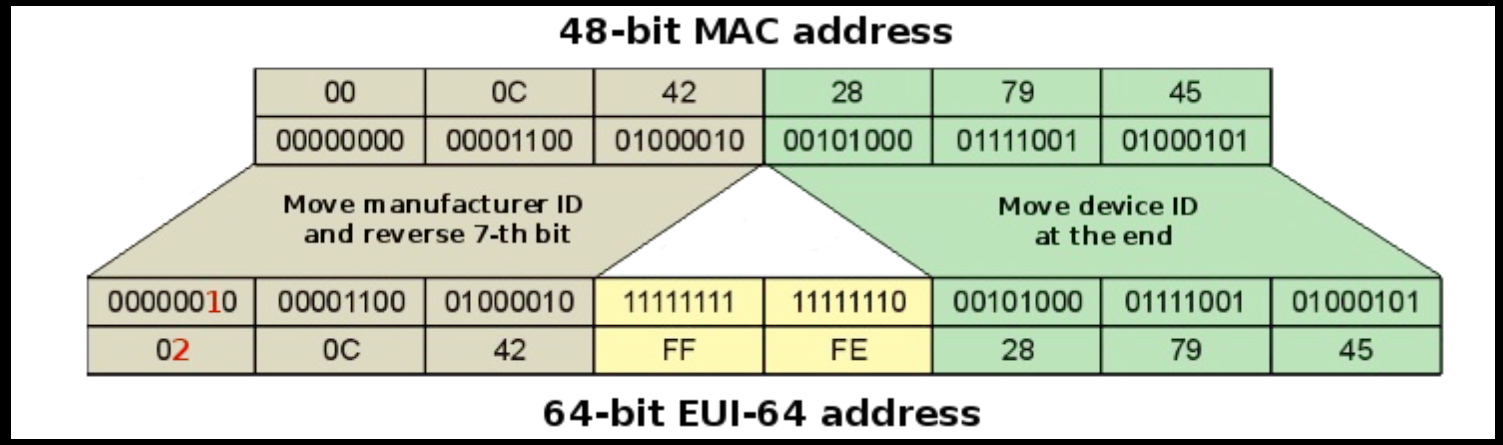
What's Different about IPv6?

Auto-address Configuration Method	ICMPv6 RA (Type 134)			Resulting IPv6 Addresses Configured	Additional Configuration Options *(DNS servers, domain search list, etc.)*
	A Flag	M Flag	O Flag		
SLAAC	1	0	0	Link-local, IPv6, Temporary IPv6	Manual (unless client supports RFC 6106/RDNSS)
Stateless DHCPv6	1	0	1	Link-local, IPv6, Temporary IPv6	DHCPv6
Stateful DHCPv6	0	1	N/R	Link-local, DHCPv6	DHCPv6

Source: Infoblox

What's So Insecure about IPv6? - Privacy

- EUI-64 Format



2001:470:dead:beef:20c:42ff:fe28:7945

What's So Insecure about IPv6? - Privacy

- RFC 4941 – Privacy Extensions for SLAAC
  - (new address every day/week)
- Disable SLAAC
  - (end-host can always override)

The random interface identifier generation algorithm, as described in this document, uses MD5 as the hash algorithm. The node MAY use another algorithm instead of MD5 to produce the random interface identifier.

3.2.1. When Stable Storage Is Present

The following algorithm assumes the presence of a 64-bit "history value" that is used as input in generating a randomized interface identifier. The very first time the system boots (i.e., out-of-the-box), a random value SHOULD be generated using techniques that help ensure the initial value is hard to guess [RANDOM]. Whenever a new interface identifier is generated, a value generated by the computation is saved in the history value for the next iteration of the algorithm.

A randomized interface identifier is created as follows:

1. Take the history value from the previous iteration of this algorithm (or a random value if there is no previous value) and append to it the interface identifier generated as described in [ADDRARCH].

2. Compute the MD5 message digest [MD5] over the quantity created in the previous step.

3. Take the leftmost 64-bits of the MD5 digest and set bit 6 (the leftmost bit is numbered 0) to zero. This creates an interface identifier with the universal/local bit indicating local significance only.

4. Compare the generated identifier against a list of reserved interface identifiers and to those already assigned to an address on the local device. In the event that an unacceptable identifier has been generated, the node MUST restart the process at step 1 above, using the rightmost 64 bits of the MD5 digest obtained in step 2 in place of the history value in step 1.

5. Save the generated identifier as the associated randomized interface identifier.

6. Take the rightmost 64-bits of the MD5 digest computed in step 2) and save them in stable storage as the history value to be used in the next iteration of the algorithm.

What's So Insecure about IPv6? - ICMP

- ICMP Requirements
  - Fragmentation only done by end hosts
  - All L2 devices must support MTU >=1280
  - End hosts must perform Path MTU Discovery
  - Network must tell end hosts if packet too big

4.3.1. Traffic That Must Not Be Dropped

Error messages that are essential to the establishment and maintenance of communications:

- Destination Unreachable (Type 1) - All codes
- Packet Too Big (Type 2)
- Time Exceeded (Type 3) - Code 0 only
- Parameter Problem (Type 4) - Codes 1 and 2 only

Appendix A.4 suggests some more specific checks that could be performed on Parameter Problem messages if a firewall has the necessary packet inspection capabilities.

Connectivity checking messages:

- Echo Request (Type 128)
- Echo Response (Type 129)

For Teredo tunneling [RFC4380] to IPv6 nodes on the site to be possible, it is essential that the connectivity checking messages are allowed through the firewall. It has been common practice in IPv4 networks to drop Echo Request messages in firewalls to minimize the risk of scanning attacks on the protected network. As discussed in Section 3.2, the risks from port scanning in an IPv6 network are much less severe, and it is not necessary to filter IPv6 Echo Request messages.

4.3.2. Traffic That Normally Should Not Be Dropped

Error messages other than those listed in Section 4.3.1:

- Time Exceeded (Type 3) - Code 1
- Parameter Problem (Type 4) - Code 0

Mobile IPv6 messages that are needed to assist mobility:

- Home Agent Address Discovery Request (Type 144)
- Home Agent Address Discovery Reply (Type 145)
- Mobile Prefix Solicitation (Type 146)
- Mobile Prefix Advertisement (Type 147)

What's So Insecure about IPv6? - ICMP

- Follow RFC
- SeND
  - PKI used to derive host address
  - Used to authenticate messages

4.3.1. Traffic That Must Not Be Dropped

Error messages that are essential to the establishment and maintenance of communications:

- Destination Unreachable (Type 1) - All codes
- Packet Too Big (Type 2)
- Time Exceeded (Type 3) - Code 0 only
- Parameter Problem (Type 4) - Codes 1 and 2 only

Appendix A.4 suggests some more specific checks that could be performed on Parameter Problem messages if a firewall has the necessary packet inspection capabilities.

Connectivity checking messages:

- Echo Request (Type 128)
- Echo Response (Type 129)

For Teredo tunneling [RFC4380] to IPv6 nodes on the site to be possible, it is essential that the connectivity checking messages are allowed through the firewall. It has been common practice in IPv4 networks to drop Echo Request messages in firewalls to minimize the risk of scanning attacks on the protected network. As discussed in Section 3.2, the risks from port scanning in an IPv6 network are much less severe, and it is not necessary to filter IPv6 Echo Request messages.

4.3.2. Traffic That Normally Should Not Be Dropped

Error messages other than those listed in Section 4.3.1:

- Time Exceeded (Type 3) - Code 1
- Parameter Problem (Type 4) - Code 0

Mobile IPv6 messages that are needed to assist mobility:

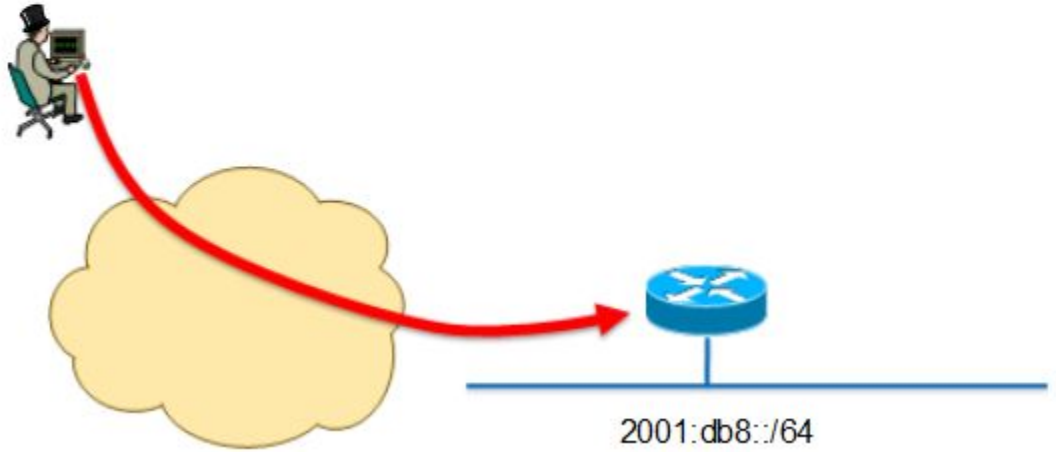
- Home Agent Address Discovery Request (Type 144)
- Home Agent Address Discovery Reply (Type 145)
- Mobile Prefix Solicitation (Type 146)
- Mobile Prefix Advertisement (Type 147)

What's So Insecure about IPv6? - Exhaustion

- (T)CAM Exhaustion
- NDP similar to ARP
- /64 allows for 7 gazillion addresses
- No switch can hold 7 gazillion entries

Scanning Made Bad for CPU
Remote Neighbor Cache Exhaustion RFC 6583

- Potential router CPU/memory attacks if aggressive scanning
  - Router will do Neighbor Discovery... And waste CPU and memory
- **Local router** DoS with NS/RS/…

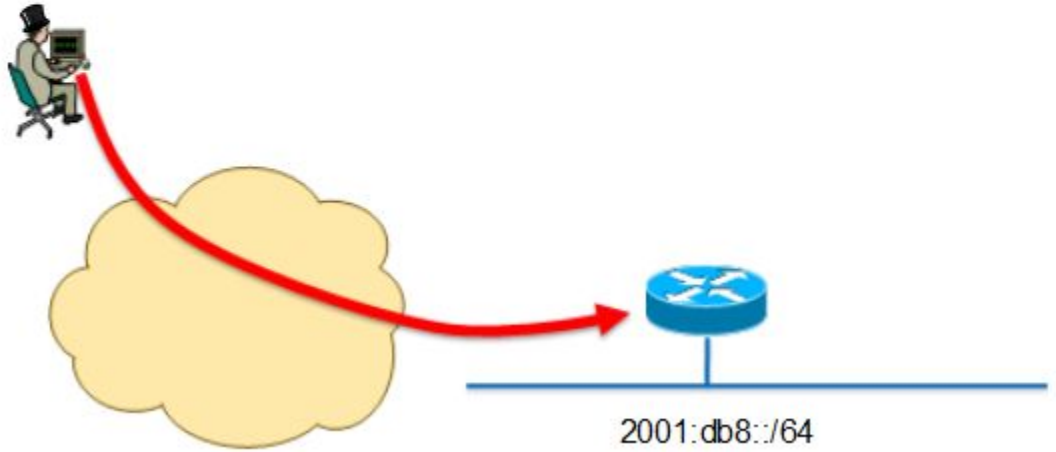


What's So Insecure about IPv6? - Exhaustion

- SeND
- /120 Prefix (same as IPv4 /24)

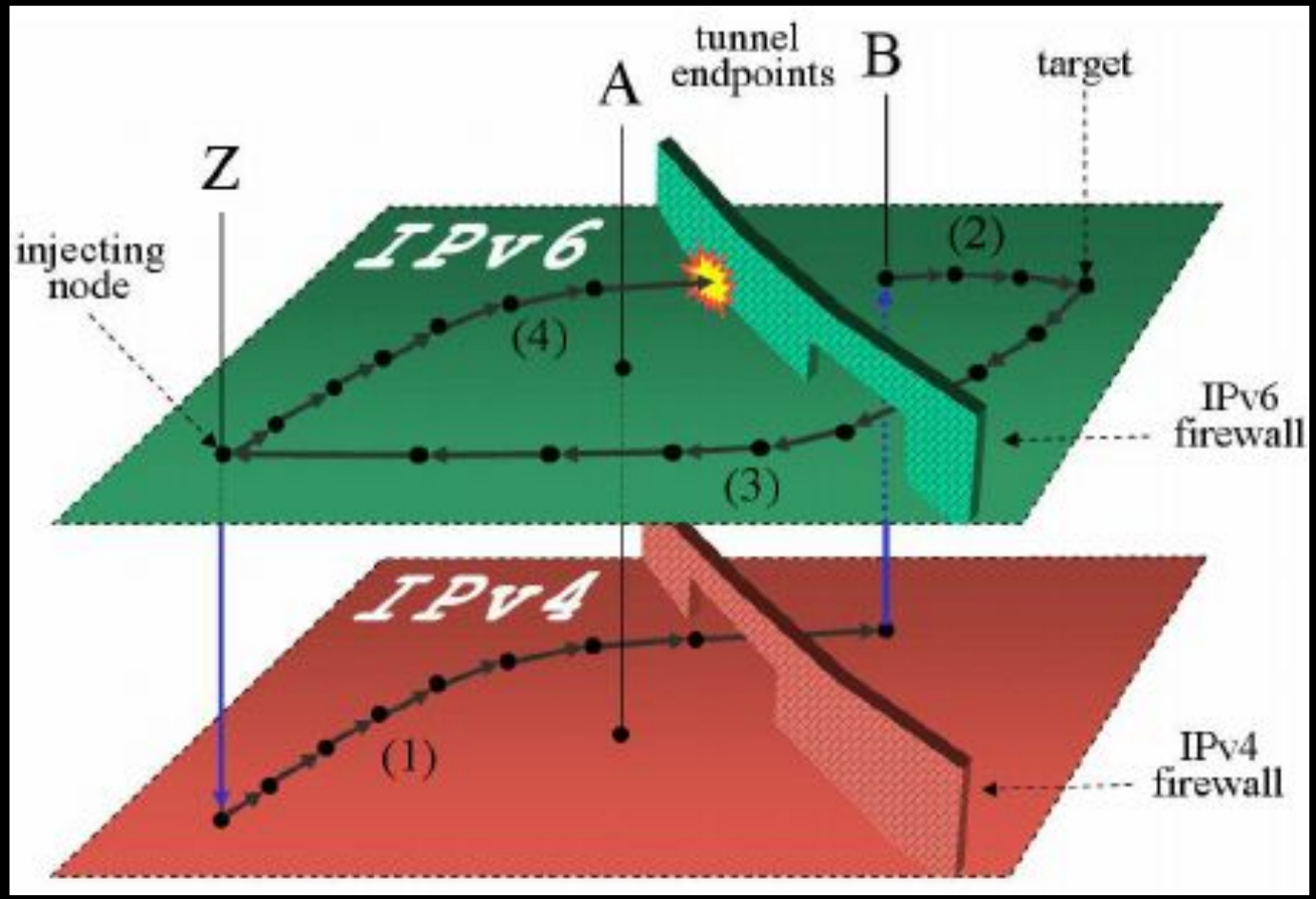
Scanning Made Bad for CPU
Remote Neighbor Cache Exhaustion RFC 6583

- Potential router CPU/memory attacks if aggressive scanning
  - Router will do Neighbor Discovery... And waste CPU and memory
- **Local router** DoS with NS/RS/…



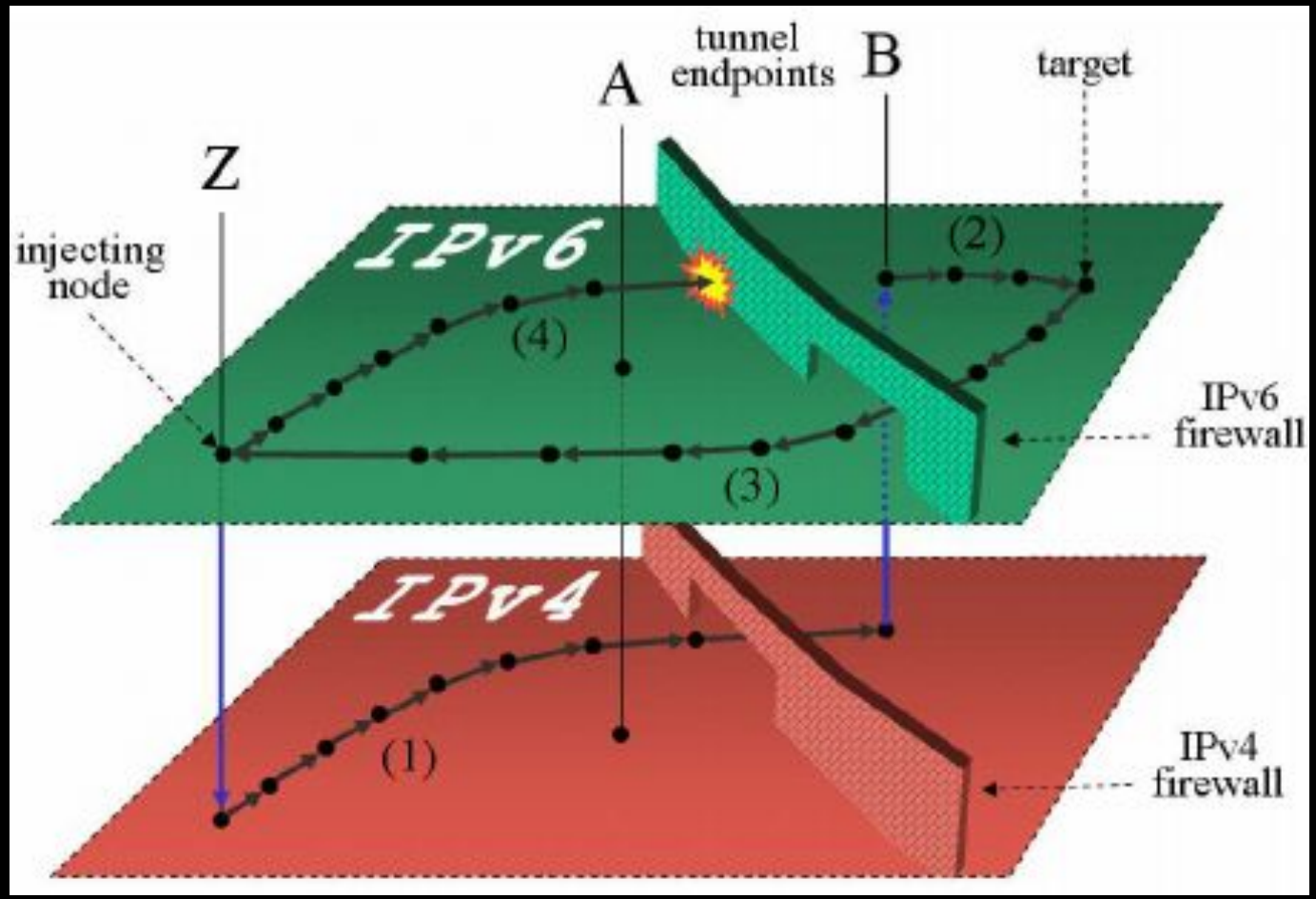
What's So Insecure about IPv6? - Tunneling

- 6in4
- Teredo (udp/3544)
- SSLVPN



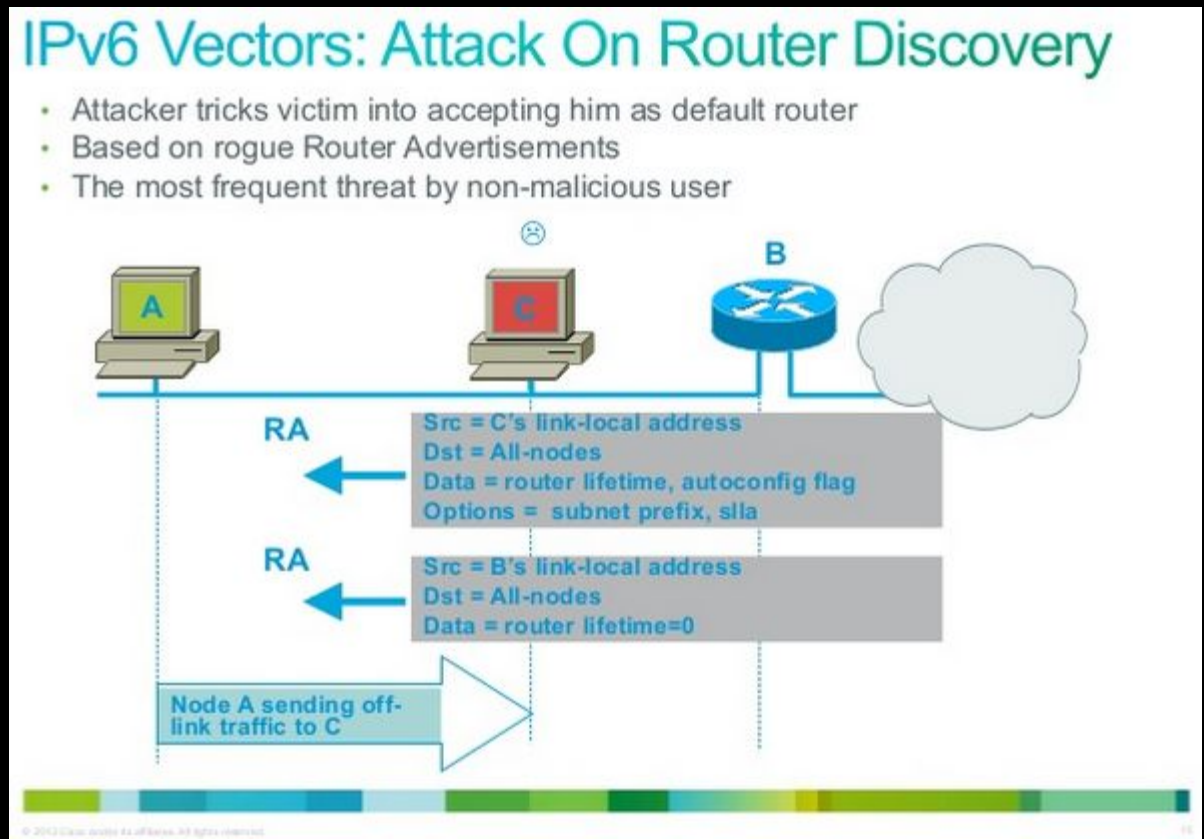
What's So Insecure about IPv6? - Tunneling

- Block Outbound
- Detection



What's So Insecure about IPv6? – False RA

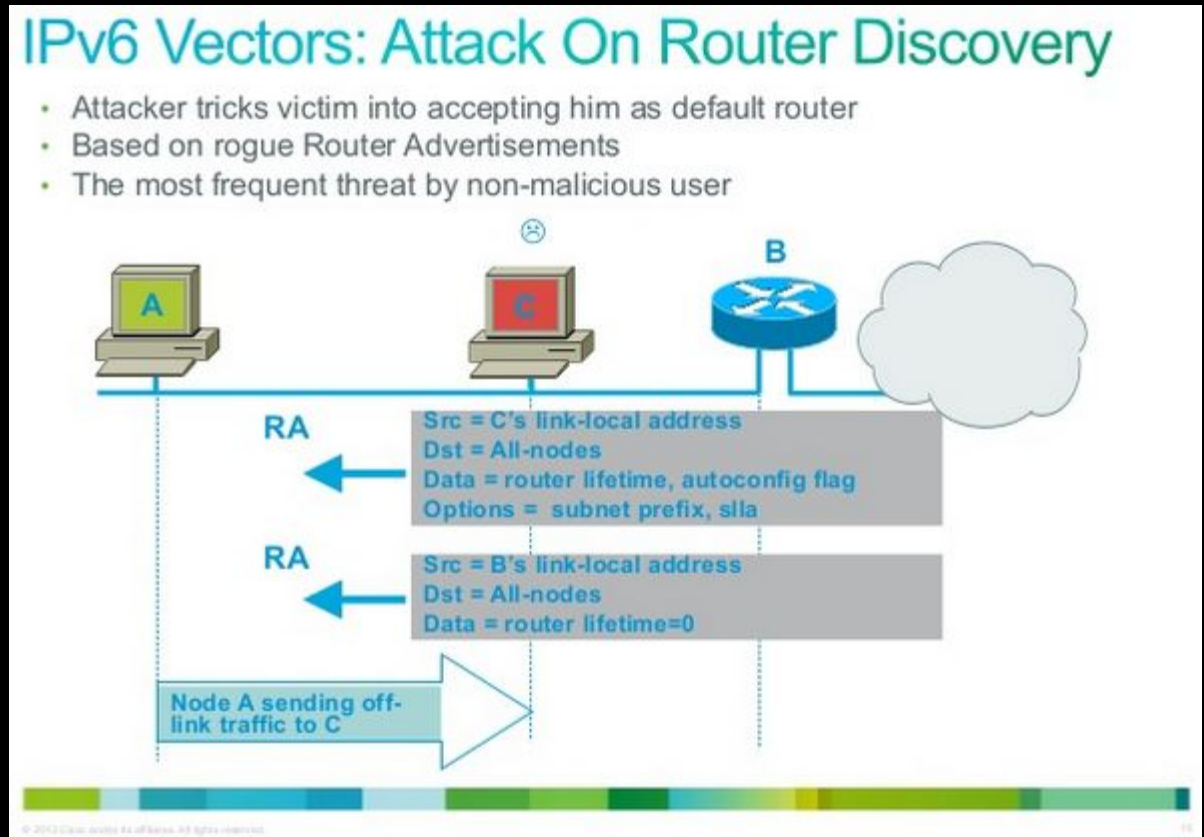
- Remember how prefixes are advertised?
- M/O/A Flags?



Source: Cisco

What's So Insecure about IPv6? – False RA

- RA Guard



Source: Cisco


Kernelcon

?