ISZT/HunCERT IPv6 Workshop

IPv6 for Dummies

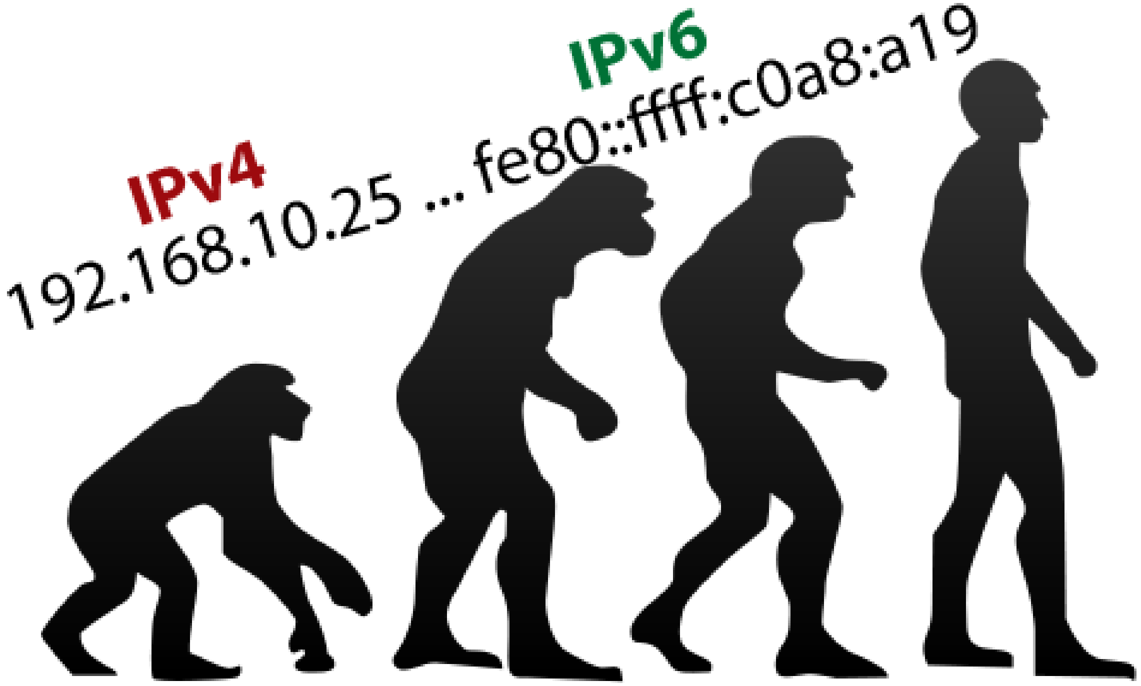
First Lecture

21st June 2022

10:00 - 12:00

Lecturer: Tibor K. Dravecz
INTEGRITY Ltd.

Authors: Tibor K. Dravecz, Tibor Dravecz, Zsolt Krüpl, Vencel Tátos


IPv4
192.168.10.25 ... fe80::ffff:c0a8:a19
IPv6

About ISZT/HunCERT IPv6 Workshop and Training

Main focus: CYBERSECURITY

First lecture	Summer holiday	Further lectures
21st June 2022	July-August 2022	September 2022 - 2023

1. IPv6 Primer (part of this is the series of lectures 'IPv6 for Dummies')
2. IPv6 Advanced and Special Studies
3. IPv6 Workshop: Best Practices, Case Studies, Consultation
4. IPv6 Training

Thematic of IPv6 for Dummies

First Lecture (21st June 2022)

- Introduction
- Historical background
- Internet Protocol, Version 6 (IPv6) Specification (RFCs)
- IPv6 data and statistics
- Basic concepts
- How IPv6 is different from IPv4
- Key security issues of IPv4

Second Lecture

- IPv6 header and header extensions
- IPv6 addressing and address spaces
- Global, local and special addresses
- Unicast, anycast and multicast

Third lecture

- ICMPv6
- Neighbor Discovery (ND) and Router Advertisement (RA)
- Autoconfiguration

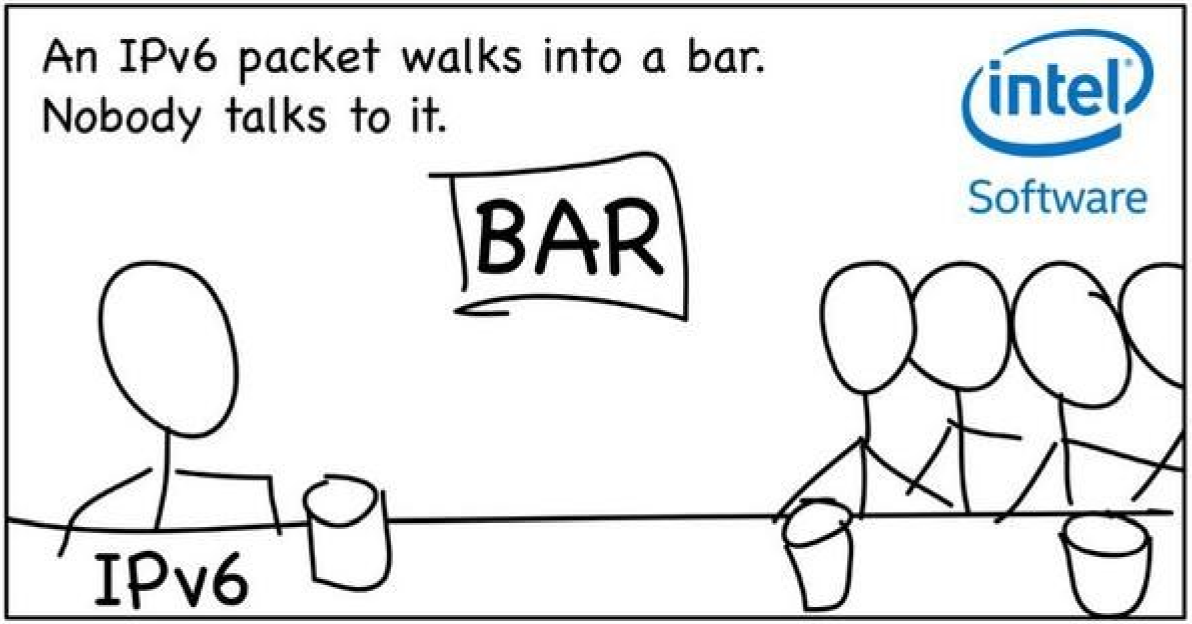
Fourth lecture

- DNS and IPv6

Further suggested topics

- RA guard
- IPsec
- Translating and tunneling
- NPT66 and NATs (NAT66, NAT64 etc.)
- Mobile IPv6
- IPv6 routing
- Enterprise security
- Distributed firewalls, directory services
- PKI for IPv6
- Zero trust model
- DDoS and IPv6
- IPv4/IPv6 legal and regulatory issues
- IPv6 privacy
- IoT and IPv6
- Some manufacturer specific presentations (e.g. Cisco, Arista, Mikrotik, Microsoft, VMware etc.)
- IPAM
- ...

Prologue


An IPv6 packet walks into a bar.
Nobody talks to it.
BAR
IPv6
intel
Software

Security checking-scanning

Open resolver checking on our IPv4 network

It works well.

Open resolver checking on an IPv6 network

Full verification is not possible,

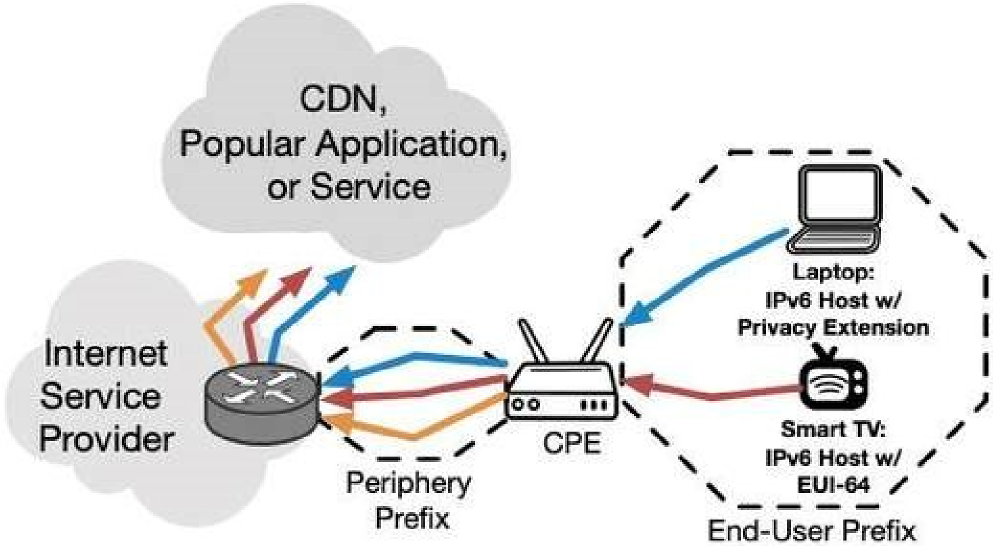
although partial inspection is possible (see *reconnaissance techniques*).

1 host, at least 1 piece of interfaces, but presumably more interfaces
2^64 IPv4 addresses/(virtual) interface
2^64 = 18 446 744 073 709 551 616 ≈ 1.8 * 10^{19}
~5 billion years/interface is needed

However, there exist solutions! - but not host testing.

IPv6 addresses can spoil your privacy

How legacy IPv6 addresses can spoil your network privacy – One bit of kit using EUI-64 screws up protections



Time	Host	IPv6 Address	Tracking ID
1	SmartTV	2001:db80:1111:b000:8e8f:90ff:fe12:3456	8e8f:90ff:fe12:3456
1	Laptop	2001:db80:1111:b000:ddde:abcd:1111:ff11	8e8f:90ff:fe12:3456
1	CPE	2001:db80:2222:b25d:aff0:abff:fe34:5679	aff0:abff:fe34:5679
...			
2	SmartTV	2001:db80:3333:fff1:8e8f:90ff:fe12:3456	8e8f:90ff:fe12:3456
2	Laptop	2001:db80:3333:fff1:1111:1123:ee11:2222	8e8f:90ff:fe12:3456
2	CPE	2001:db80:2222:b266:aff0:abff:fe34:5679	aff0:abff:fe34:5679

https://www.theregister.com/2022/03/22/legacy_ipv6_addressing_standard_enables/

Rate-limiting

Rate-Limiting: Traffic policy, Traffic shaping

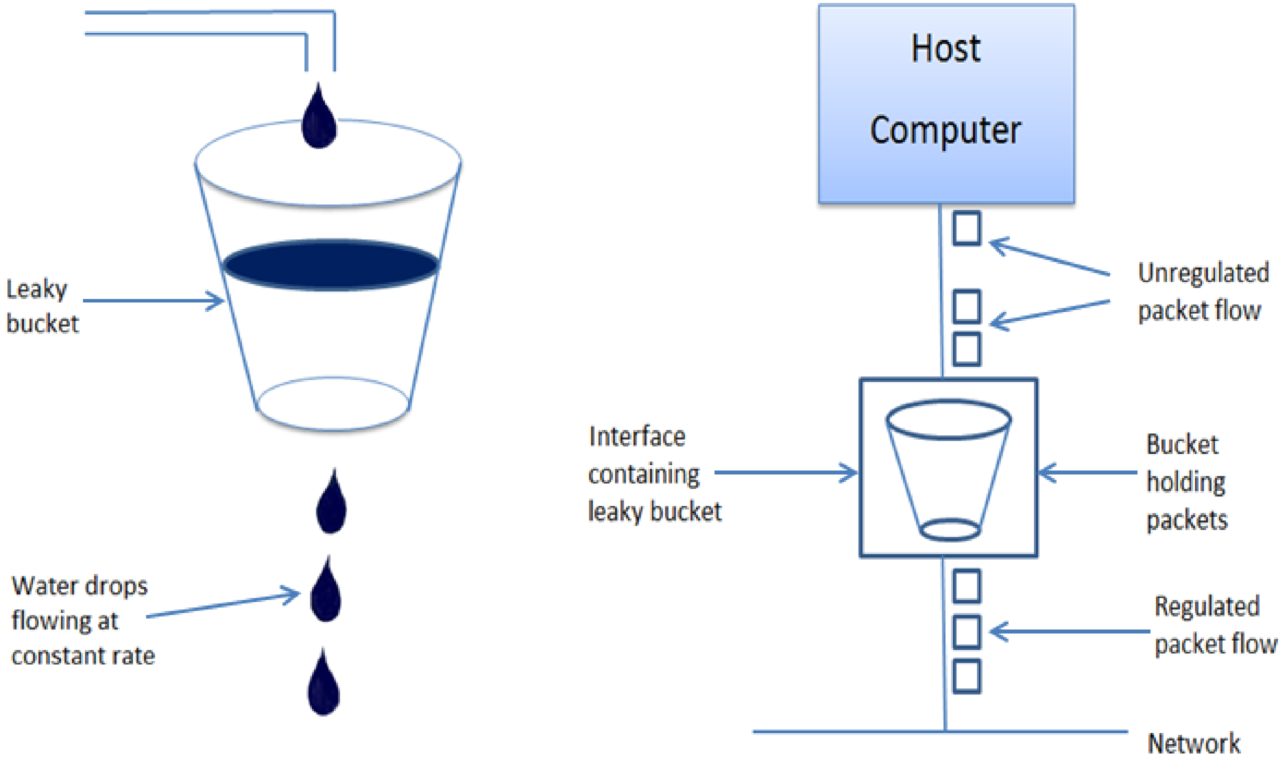


Fig: Leaky Bucket Algorithm

No effective IPv6 rate-limiting - apart from a few partial solutions

Preface

There are only this many IPv6 addresses left:

340,282,366,920,938,463,463,374,607,431,061,537,250

Projected IPv6 Exhaustion Date

5,395,000,000,000,000,000,000,000,000,000 AD

In Perspective

4,600,000,000 AD	Sun explodes; Earth destroyed
1,000,000,000,000,000 AD	Formation of new stars cease
100,000,000,000,000,000,000 AD	Solar systems no longer exist
5,395,000,000,000,000,000,000,000,000,000 AD	IPv6 Exhaustion
10,000,000,000,000,000,000,000,000,000,000,000,000,000 AD	Proton decay: no more atoms

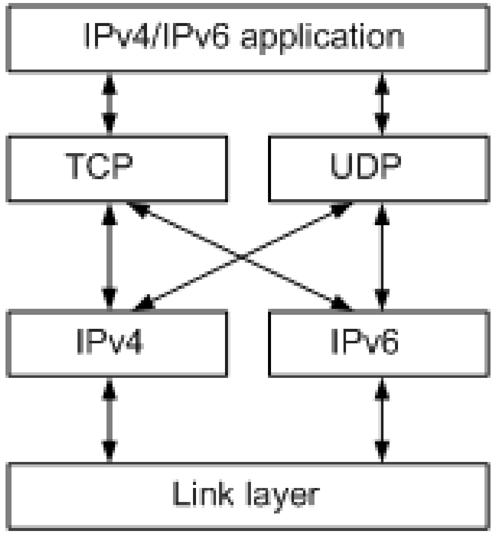
https://samsclass.info/ipv6/exhaustion.htm

IPv4 and IPv6

- **two different**
- **incompatible protocol.**

Internet Protocol vs. Internet Protocol Suite

TCP/IP model	Internet protocol suite		TCP/IP stack	
Four Layers of TCP/IP model			**IPv4 stack**	**IPv6 stack**
Application	Telnet, Ping, SMTP, BGP4 FTP, TFTP, SSH, NFS, NTP, DNS, HTTP, SNMP, RIP, TLS, DTLS *VPN		**IPv4 only** **IPv6 only** **Dual stack**	
Transport	QUIC TCP, UDP, UDP-Light, RUDP, SCTP *VPN			
Internet	ICMP, IGMP IP, IPsec, HIP …	OSPF, IS-IS		
Network Interface	*Data Link:* Ethernet - IEEEE 802.2, ARP *Physical Network:* Ethernet - IEEE 802.3, RS-232 *Tunnels, *VLAN, *FHRP			
TCP/IP Conceptual Layers				



Same protocols	Addition/Extension/ Complementation/Supplementation
HTTP SMTP, POP, IMAP TLS, DTLS NTP, PTP, DNS, LDAP EPP Ping	TCP, UDP, SCTP SNMP BGP4+ IPoAC

Not implemented in IPv6	Only IPv6	Completely different protocols
ARP IGMP	NDP, SLAAC IPHTTPS L2TPv3	IPv4 - IPv6 DHCPv4 - DHCPv6 ICMPv4 - ICMPv6

Myths

- **IPv6 is IPv4 with longer addresses.**
- ~~IPv6 is 'coming'.~~
- ~~IPv6 is not ready for production.~~
- **We don’t need IPv6.**
- **There is no rush.**
- **IPv6 replaces IPv4.**
- **IPv4 is going to disappear.**
- **IPv4 has run out of addresses.**
- **IPv6 is more/less secure than IPv4**
- **IPv6 will simplify the communication on the Internet.**

"I'm not using IPv6", "I'am not running it."

"We have enough IPv4 addresses, we don't need IPv6"

"It’s inherently secure." – "IPv6 Security enhancements (such as IPsec) makes it safer than IPv4."

1

"IPv6 Has Security Designed" – In Reality: IPv6 was Designed 20+ Years Ago

"Man-in-the-Middle (MITM) isn't possible with IPv6."

"IPv6 offers better QoS."

"Hackers aren't using IPv6."

"Address scanning is impossible in IPv6."

"Emergence a black market is likely/there is black market for IPv4 addresses."

---

[1] **“We know what’s happening”, We know what we’re doing”, “We will always have to run IPv4 protocols” …**

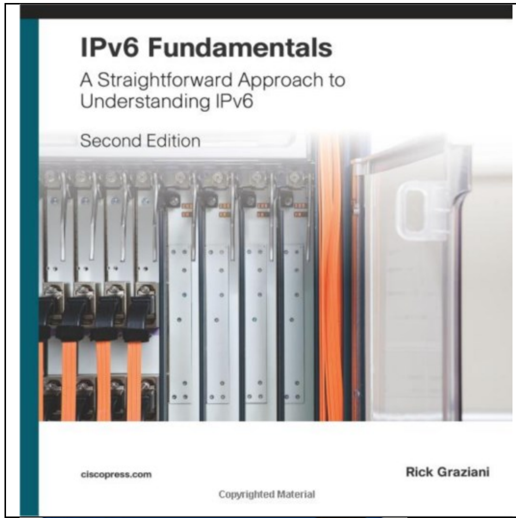
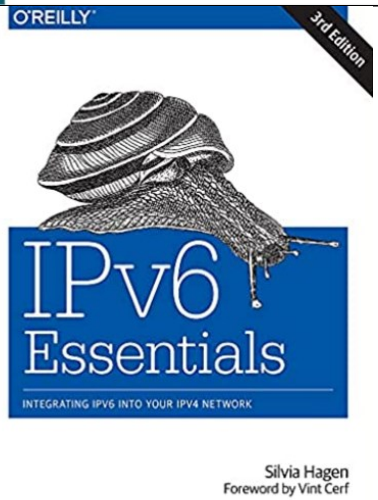
To Do

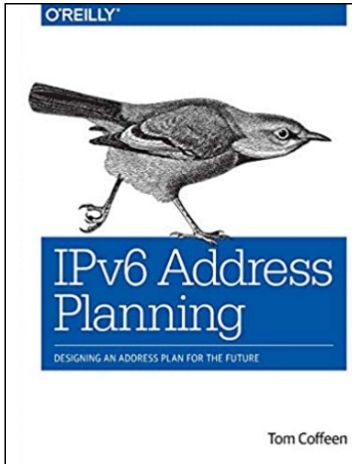
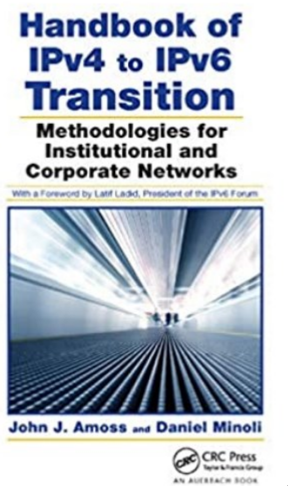
1. **Education, training – know-how and expertise**
2. **Inventory and assessment**
3. **Ensuring IPv6 compatibility**
4. **Checking/testing, testbeds, pilot projects**
5. **Congruency, uniformity**
6. **Control and audit**

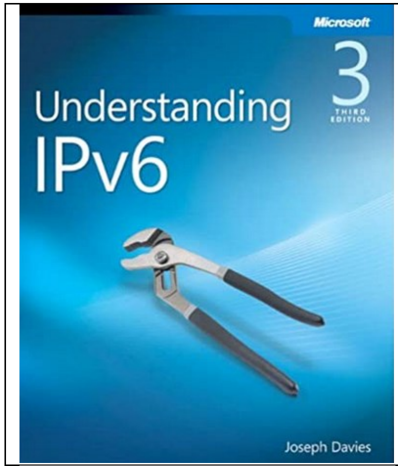
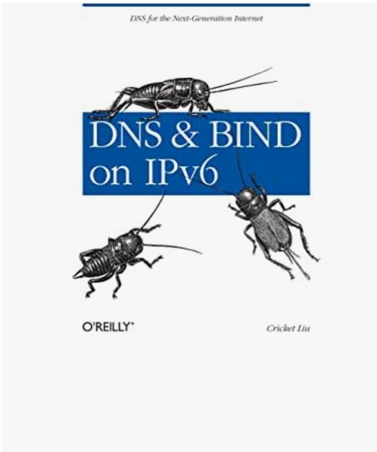
7. **First partially,**
   - 7.1. **then comprehensive deployment**
   - 7.2. **followed by maintenance and development**
   - 7.3. **checking/testing, control and audit**


CAUTION
Legacy IP Only
This product does not support the current generation of the Internet Protocol, IPv6.

Recommended literature

<table>
<tr>
<td>
</td>
<td>IPv6 Fundamentals: A Straightforward Approach to Understanding IPv6 2nd Edition
by Rick Graziani (author)
Cisco Press; 2nd edition (June 21, 2017)
English
Paperback, 688 pages
ISBN-13: 978-1587144776
ISBN-10: 1587144778</td>
</tr>
<tr>
<td>
</td>
<td>IPv6 Essentials: Integrating IPv6 into Your IPv4 Network 3rd Edition
by Silvia Hagen (Author)
O'Reilly Media; 3rd edition (June 29, 2014)
English
Paperback, 414 pages
ISBN-10 1449319211
ISBN-13 978-1449319212</td>
</tr>
</table>

	IPv6 Address Planning: Designing an Address Plan for the Future 1st Edition by Tom Coffeen (Author) O'Reilly Media; 1st edition (December 9, 2014) English Paperback, 286 pages ISBN-10 1491902760 ISBN-13 978-1491902769
	Handbook of IPv4 to IPv6 Transition: Methodologies for Institutional and Corporate Networks 1st Edition by John J. Amoss (Author), Daniel Minoli (Author) Auerbach Publications; 1st edition (September 19, 2019) English Paperback, 248 pages ISBN-10 0367388057 ISBN-13 978-0367388058
	Tutorials, e.g.: Tutorials Point: IPv6 Tutorial https://www.tutorialspoint.com/ipv6/index.htm

	Understanding IPv6: Your Essential Guide to IPv6 on Windows Networks Third Edition by Joseph Davies (Author) Microsoft Press; Third edition (June 30, 2012) English Paperback, 716 pages ISBN-10 0735659141 ISBN-13 978-0735659148
	DNS and BIND on IPv6: DNS for the Next-Generation Internet 1st Edition by Cricket Liu (Author) O'Reilly Media; 1st edition (June 14, 2011) English Paperback, 54 pages ISBN-10 9781449305192 ISBN-13 978-1449305192

"When Is It Time for IPv6? The answer in 2014 is now!"
– Silvia Hagen: IPv6 Essentials, 2014, O'Reilly

Today, the answer would be "yesterday",
but you shouldn't delay any longer, if not "yesterday", NOW!

Introduction

"Probably there will be no killer application either, so don't wait for one. Or as some people like to say, the killer application for IPv6 is the Internet."

"IPv6 will slowly and gradually grow into our network and Internet. Taking a step-by-step approach to IPv6 may be the most cost-efficeint way to integrate it, depending on your requirements."
– Silvia Hagen: IPv6 Essentials, 2014, O'Reilly

IPv6 addresses

Calculator.net – IP Subnet Calculator
https://www.cidr.eu/en/calculator
https://onlinebinarytools.com/convert-ipv6-to-binary

IPv6 Expanded Address	**2607:f8b0:4004:0c0b:0000:0000:0000:001b**
IPv6 Address (Shortened)	2607:f8b0:4004: c0b: 0: 0: 0: 1b
IPv6 Compressed Address	**2607:f8b0:4004:c0b :: 1b** (gmail-smtp-in.l.google.com)
Hexadecimal Representation	0x2607f8b040040c0b000000000000001b
Decimal Representation (Unsigned 128-bit integer)	50552053919386788291689459308644270107
Binary Representation (In Octets)	100110 00000111 11111000 10110000 01000000 00000100 00001100 00001011 00000000 00000000 00000000 00000000 00000000 00000000 00000000 00011011
Binary Representation (In Hexadectets /'Hextets'/)	0010011000000111 1111100010110000 0100000000000100 0000110000001011 0000000000000000 0000000000000000 0000000000000000 0000000000011011
PTR Label	b.1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.b.0.c.0.4.0.0.4.0.b.8.f.7.0.6.2.ip6.arpa.

How can one distinguish the host and the port in an IPv6 URL?

2607:f8b0:4004:0c0b:0000:0000:0000:001b~~:25~~

2607:f8b0:4004:c0b::1b~~:25~~

[2607:f8b0:4004:c0b::1b]:25

Is the "25" decimal, or hexadecimal?

https://[IPv6address]:port

valaki@[IPaddress]

A Compact Representation of IPv6 Addresses
RFC 1924 (R. Elz, University of Melbourne, 1996)

```
4. The New Encoding Format

   The new standard way of writing IPv6 addresses is to treat them as a
   128 bit integer, encode that in base 85 notation, then encode that
   using 85 ASCII characters.

4.1. Why 85?

   2^128 is 340282366920938463463374607431768211456.  85^20 is
   387595310845143558731231784820556640625, and thus in 20 digits of
   base 85 representation all possible 2^128 IPv6 addresses can clearly
   be encoded.

   84^20 is 305904398238499908683087849324518834176, clearly not
   sufficient, 21 characters would be needed to encode using base 84,
   this wastage of notational space cannot be tolerated.

   On the other hand, 94^19 is just
   30862366077815087592879016454695419904, also insufficient to encode
   all 2^128 different IPv6 addresses, so 20 characters would be needed
   even with base 94 encoding.  As there are just 94 ASCII characters
   (excluding control characters, space, and del) base 94 is the largest
   reasonable value that can be used.  Even if space were allowed, base
   95 would still require 20 characters.

   Thus, any value between 85 and 94 inclusive could reasonably be
   chosen.  Selecting 85 allows the use of the smallest possible subset
   of the ASCII characters, enabling more characters to be retained for
   other uses, eg, to delimit the address.
```

Converting an IPv6 address to Base85

For example
1080:0:0:0:8:800:200C:417A

Thus in base85 the address is:
4-68-70-46-66-12-63-31-61-19-
4-37-53-75-0-58-57-65-34-51.

Then, when encoded as specified above, this becomes:

4)+k&C#VzJ4br>0wv%Yp

IPv4 vs. IPv6 addresses

142.250.31.26
10001110.11111010.00011111.00011010

2607:f8b0:4004:c0b::1b
0010011000000111:1111100010110000:0100000000000100:0000110000001011:
0000000000000000:0000000000000000:0000000000000000:0000000000011011

2001:db8::/32 address space for documention

2001:db8:4004:0c0b:0000:0000:*192.168.0.123*
2001:db8:4004:c0b:0:0:*192.168.0.123*
2001:db8:4004:c0b::*192.168.0.123*

Reminiscence – Forms of IPv4 addresses

dotted decimal	127.0.0.1
dotted hexadecimal	0x7f:0x0:0x0:0x1
dotted octal	0177.0000.0000.0001 (017700000001_8)
dotted mixed	*see below*
decimal (DWORD)[2]	2130706433
octal	017700000001
hexadecimal	0x7f000001
PTR	1.0.0.127.in-addr.arpa.

Leading zeros are allowed, e.g.:

```
ping 0000000000000000000127.0.0.1
Pinging 87.0.0.1 with 32 bytes of data:
Reply from 87.0.0.1: bytes=32 time=51ms TTL=52
```

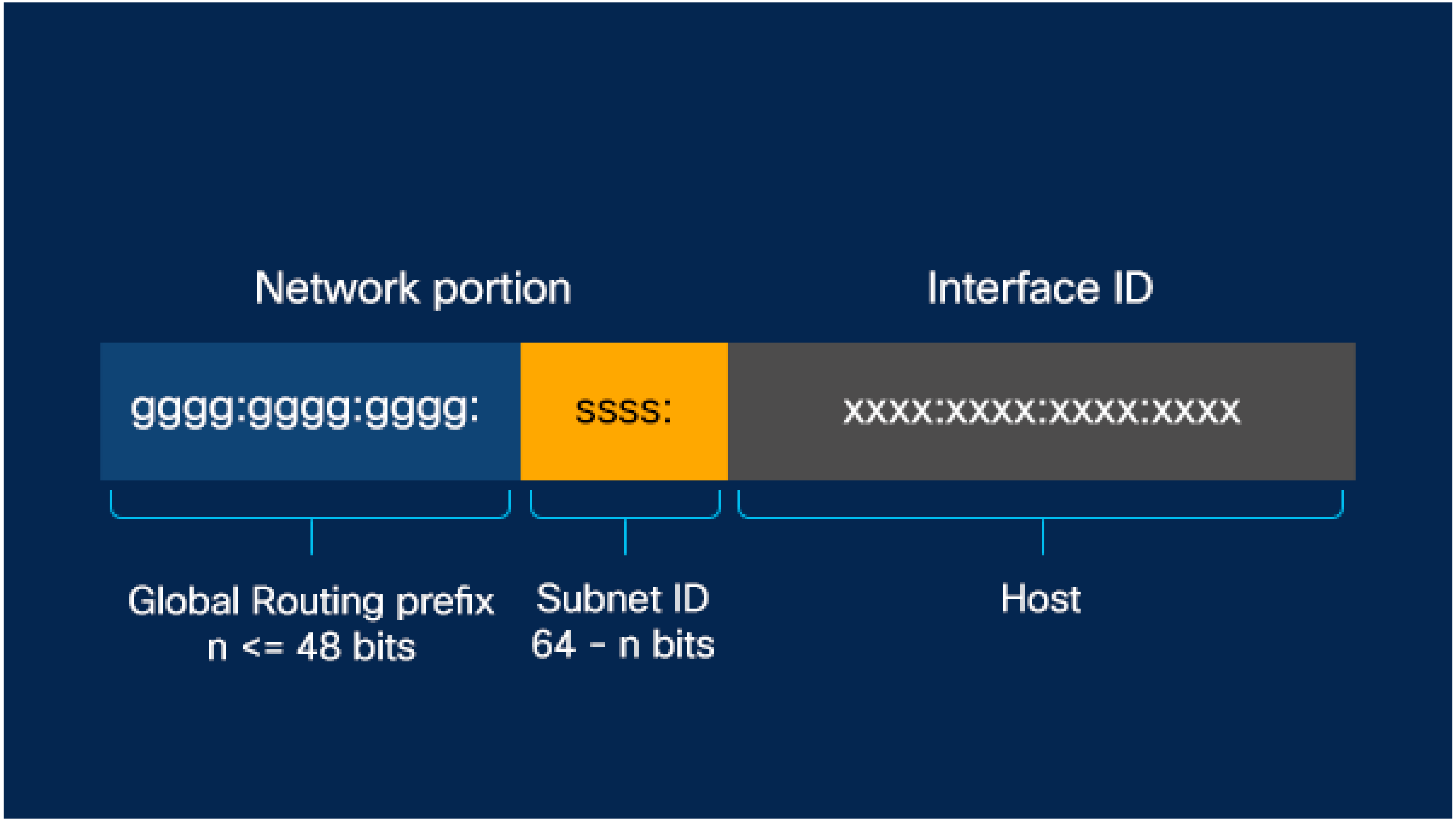
Example of mixed:

```
ping 0177.99.0xa.88
Pinging 127.99.10.88 with 32 bytes of data:
Reply from 127.99.10.88: bytes=32 time<1ms TTL=128
```

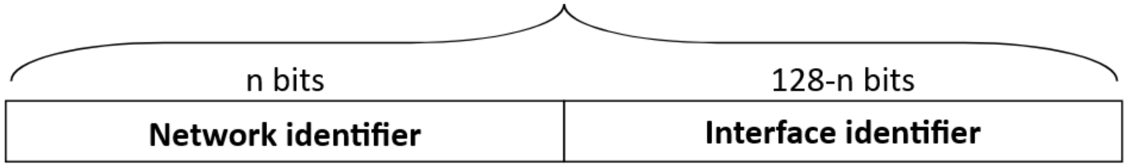
[2]
```
ping 2130706433
Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
```

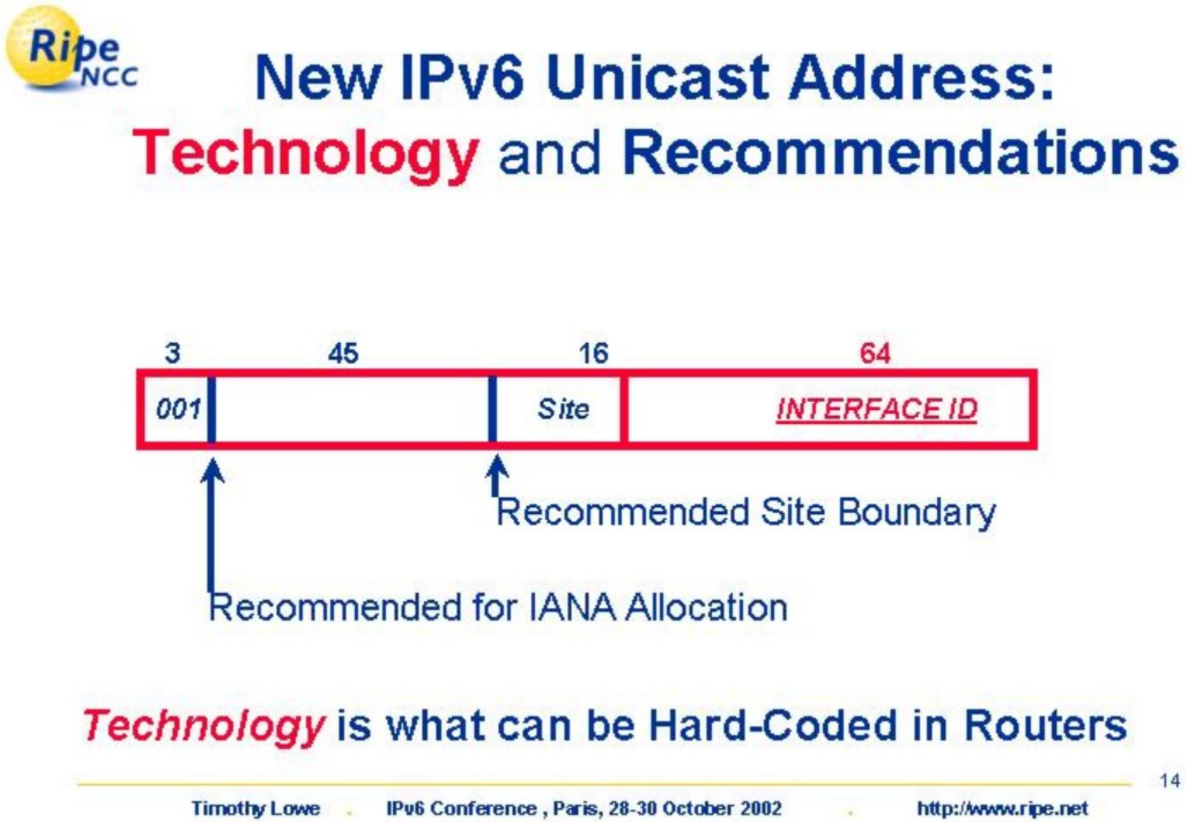
Parts of Address:

[128 - N network (prefix + subnet) bits | N interface bits]



IPv6 64-bit boundary





Scoping Concept, Zones, Indices[3]

IPv6 Scoped Address Architecture, RFC 4007 (March 2005)[4]

Every IPv6 address *other than the unspecified address* has a specific **scope**.

Unicast address	**Multicast address**
• Link-local • Global scope	• Interface-local • Link-local • Realm-Local (Subnet-local) • Admin-local • Site-local • Organization-local • Global scopes

A **scope zone** is an instance of a given scope. For instance, a link and all directly attached interfaces comprise a single link-local scope zone.

Zone_ID

[3] https://www.ibm.com/docs/en/zos/2.3.0?topic=addressing-scope-zones
[4] IPv6 Multicast Address Scopes, RFC 7346 (August 2014)

fe80::5909:b773:e140:bfa5**%7**
::1**%0**

ping fe80::5909:b773:e140:bfa5%7
Pinging fe80::5909:b773:e140:bfa5%7 with 32 bytes of data:
Reply from fe80::5909:b773:e140:bfa5%7: time<1ms

ping fe80::5909:b773:e140:bfa5%8
Pinging fe80::5909:b773:e140:bfa5%8 with 32 bytes of data:
PING: transmit failed. General failure

ping ::1%0
Pinging ::1 with 32 bytes of data:
Reply from ::1: time<1ms

ping ::1%1
Pinging ::1%1 with 32 bytes of data:
PING: transmit failed. General failure.

The percent sign ("%") and the URI syntax[5]

Character	ASCII decimal	UTF-8
%	37	%25

[fe80::5909:b773:e140:bfa5%**4b**]

↘"K"

[fe80::5909:b773:e140:bfa5%25**4b**]

↑zone_ID, hexadecimal

[fe80::5909:b773:e140:bfa5]:80

↑port number, decimal

[5] Uniform Resource Identifier (URI): Generic Syntax, RFC 3986
https://www.techtarget.com/whatis/definition/URI-Uniform-Resource-Identifier
https://www.w3schools.com/tags/ref_urlencode.asp

"The Prussian military theorist Carl von Clausewitz [Clausewitz] wrote, "Everything is very simple in war, but the simplest thing is difficult. These difficulties accumulate and produce a friction, which no man can imagine exactly who has not seen war.... So in war, through the influence of an 'infinity of petty circumstances' which cannot properly be described on paper, things disappoint us and we fall short of the mark". Operating a network is aptly compared to conducting a war. The difference is that the opponent has the futile expectation that homo ignoramus will behave intelligently."

Procedures for Renumbering an IPv6 Network without a Flag Day, RFC 4192 (Informal, September 2005)

IP renumbering and address plan; IPAM

"Renumbering of networks is generally a difficult and time-consuming project and should be avoided if at all possible." – https://www.internetsociety.org/resources/deploy360/2013/ipv6-address-planning-guidelines-for-ipv6-address-allocation/

"Using IPv4 and NAT a site can change providers and their external globally unique addresses while keeping the internal private addresses"
– https://meetings.ripe.net/ripe-50/presentations/ripe50-ipv6-renumbering.pdf (2005), https://www.ripe.net/participate/meetings/ripe-meetings/ripe-50

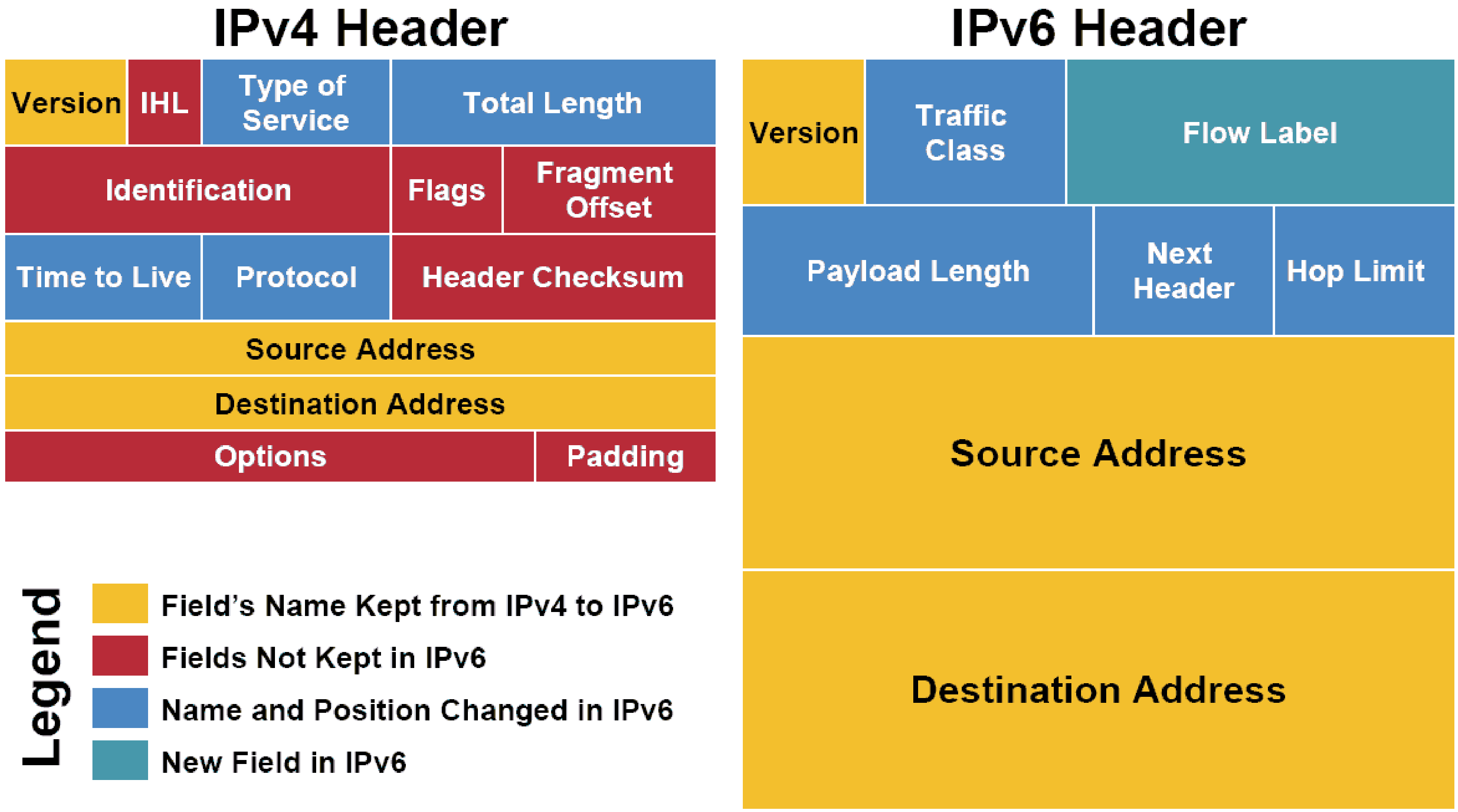
"Moving to another ISP required changing all IP addresses. Changing public IPv4 addresses was done in a few minutes. Changing public IPv6 addresses took me a couple of weeks. It was not only changing the interface IPv6 addresses but also lots of configuration details in almost all services/appliances where IPv6 GUAs were used as well."
– https://blog.apnic.net/2018/09/20/ipv6-renumbering-a-pain-in-the/

"The IETF recognizes renumbering to be a difficult problem to solve as indicated in the title of RFC 5887, Renumbering Still Needs Work." – https://www.internetsociety.org/resources/deploy360/2013/ipv6-address-planning-guidelines-for-ipv6-address-allocation/

There is a proposal to ARIN suggesting that anyone qualifying for an ASN can get PI addresses.
– https://meetings.ripe.net/ripe-50/presentations/ripe50-ipv6-renumbering.pdf

See also: RFC 1900, 2071, 2894, 4192, 5887, 6866, 6879

IPv4 versus IPv6 header

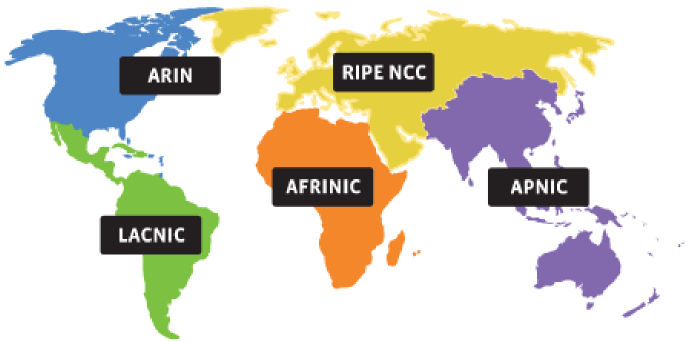


Organizations

IANA

- Number Resources (https://www.iana.org/numbers)
  - IPv4 Address Space
    - IPv4 Special Purpose Address Registry
  - IPv6 Address Space
    - IPv6 Global Unicast Allocations
    - IPv6 Multicast Address Allocations
    - IANA IPv6 Special Registry

Regional Internet Registries (RIRs)

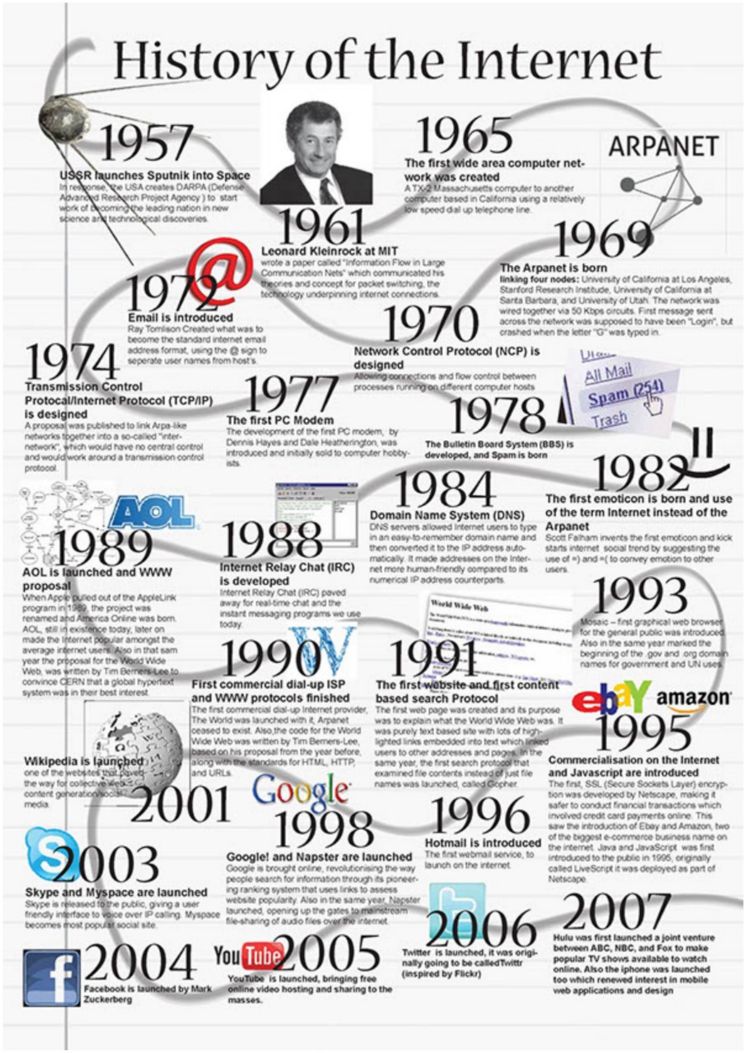


REGISTRY	AREA COVERED
AFRINIC	Africa Region
APNIC	Asia/Pacific Region
ARIN	Canada, USA, and some Caribbean Islands
LACNIC	Latin America and some Caribbean Islands
RIPE NCC	Europe, the Middle East, and Central Asia

https://www.iana.org/numbers

Once upon a time …

Historical background



A Summary of the IMP Software

Messages

Information is transmitted from HOST to HOST in bundles called messages. A message is any stream of not more than 8080 bits, together with its header. The header is 16 bits and contains the following information:

Destination	5 bits
Link	8 bits
Trace	1 bit
Spare	2 bits

The destination is the numerical code for the HOST to which the message should be sent. The trace bit signals the IMPs to record status information about the message and send the information back to the NMC (Network Measurement Center, i.e., UCLA). The spare bits are unused.

Network Working Group — Steve Crocker
Request for Comments: 1 — UCLA
7 April 1969

Title: Host Software
Author: Steve Crocker
Installation: UCLA
Date: 7 April 1969
Network Working Group Request for Comment: 1

"Be liberal in what you accept, and conservative in what you send." – Jon Postel

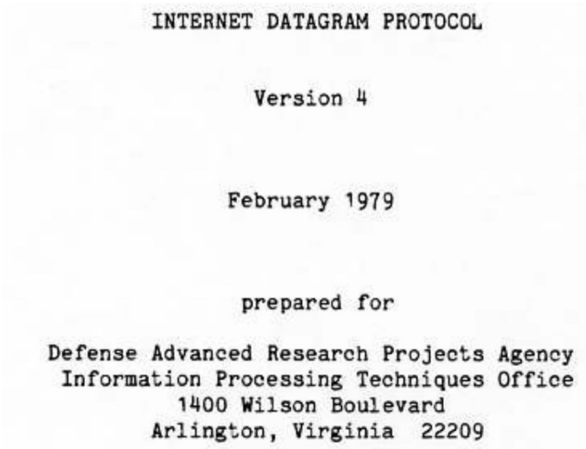
IPv4, RFC 791 (Sep 1981) (Updated by: 1349, 2474, 6864)

– in essence, this is the version 4 Internet protocol already in use today
"A datagram whose version number is not 4 MUST be silently discarded." – RFC 1122 (Internet Protocol Suite)

Internet Protocol, IEN[6] 128 (Jan 1980) [RFC 760]

– it is essentially the first version of the version 4 Internet protocol used today
RFC 760
Replaces: IENs 123, 111, 80, 54, 44, 41, 28, 26
"This document specifies the DoD Standard Internet Protocol. This document is based on five earlier editions of the ARPA Internet Protocol Specification, and the present text draws heavily from them. "
https://www.rfc-editor.org/ien/ien128.txt, https://datatracker.ietf.org/doc/html/rfc760

Internet Datagram Protocol (= Internet Protocol), Version 4, IEN 80 (Feb 1979)


INTERNET DATAGRAM PROTOCOL

Version 4

February 1979

prepared for

Defense Advanced Research Projects Agency
Information Processing Techniques Office
1400 Wilson Boulevard
Arlington, Virginia 22209

https://www.rfc-editor.org/ien/ien80.pdf

[6] Internet Experiment Note (IEN), Internet Experiment Note Index (http://www.postel.org/ien/txt/ien-index.txt, https://www.rfc-editor.org/ien/ien-index.html)

1976 United Kingdom
First networks in the world to use packet switching

"In 1976, 12 computers and 75 terminal devices were attached, and more were added until the network was replaced in 1986. NPL, followed by ARPANET, were the first two networks in the world to use packet switching, and were interconnected in the early 1970s. The NPL team also carried out simulation work on packet networks, including datagram networks."

Nov 11, 1977 USA
ARPANET

"With the role of the network reduced to a core of functionality, it became possible to exchange traffic with other network independently from their detailed characteristics, thereby solving Kahn's initial problem. DARPA agreed to fund development of prototype software, and after several years of work, the first demonstration of a gateway between the Packet Radio network in the SF Bay area and the **ARPANET** was conducted by the Stanford Research Institute. On November 22, 1977 a three network demonstration was conducted including the ARPANET, the SRI's Packet Radio Van on the Packet Radio Network and the Atlantic Packet Satellite network."

1978
International Packet Switched Service (IPSS)

"The British Post Office, Western Union International and Tymnet collaborated to create the first international packet switched network, referred to as the International Packet Switched Service (IPSS), in 1978. This network grew from Europe and the US to cover Canada, Hong Kong, and Australia by 1981. By the 1990s it provided a worldwide networking infrastructure."

https://historydraft.com/story/history-of-internet/three-network-demonstration-was-conducted/526/9289

" "The Prussian military theorist Carl von Clausewitz wrote, "Everything is very simple in war, but the simplest thing is difficult. These difficulties accumulate and produce a friction, which no man can imagine exactly who has not seen war.... So in war, through the influence of an 'infinity of petty circumstances' which cannot properly be described on paper, things disappoint us and we fall short of the mark". Operating a network is aptly compared to conducting a war. The difference is that the opponent has the futile expectation that homo ignoramus *[Homo sapiens ignoramus]* will behave intelligently." - https://datatracker.ietf.org/doc/html/rfc4192

Flag Day
Saturday January 1, 1983

Today known **TCP/IP protocol** was originally named as IP/TCP protocol – or we can say software – was redesigned as a modular protocol stack, using full-duplex channels. **Network Control Protocol (NCP)**, the predecessor of TCP, used two more simplex communications.

"ARPANET became the technical core of what would become the Internet, and a primary tool in developing the technologies used. The early ARPANET used the Network Control Program (NCP, sometimes Network Control Protocol) rather than TCP/IP. On January 1, 1983, known as flag day, NCP on the ARPANET was replaced by the more flexible and powerful family of TCP/IP protocols, marking the start of the modern Internet."
https://historydraft.com/story/history-of-internet/flag-day/526/9253

"the transition from the Network Control Program (NCP) to the Transmission Control Protocol/Internet Protocol (TCP/IP) stack, outlined in IETF RFC 801. After several years of coexistence of the two protocol stacks, on Jan. 1, 1983, system administrators across the very modest network that would eventually become today's internet switched off NCP. Only TCP/IP was supported from that time on, and it is still the core Internet protocol stack nearly 30 years later. "
https://blog.verisign.com/domain-names/do-we-need-an-ipv6-flag-day/

No flag day needs for IPv6 adoption!

IETF IPng Time Line

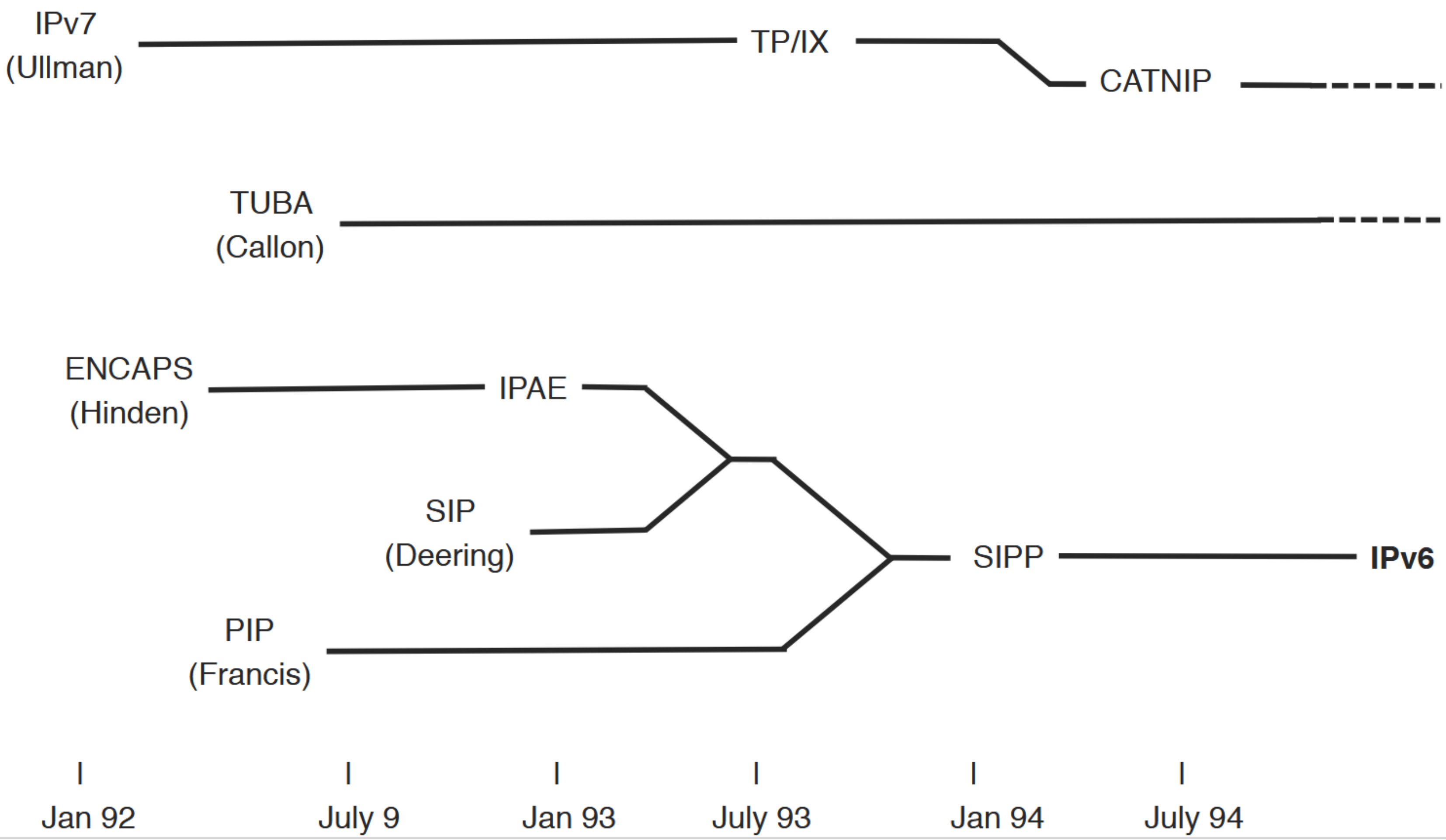
Check Point
SOFTWARE TECHNOLOGIES LTD

- ~1990
  - Internet growing exponentially and started looking like running out of IP addresses
  - Projected exhaustion of Class B Address space
- 1991
  - Routing and Addressing (ROAD) group formed
    - Recommended implementing CIDR and develop IP Next Generation (IPng)
- 1992
  - IAB issues "IP Version 7"
    - This came to be known as the "Kobe Incident"
- 1992 (cont)
  - IETF issues call for IPng proposals
- 1993
  - IESG took on IPng responsibility
  - IPng Area formed
    - Scott Bradner & Allison Mankin area directors
  - RFC1550 Call for IPng Solicitation published
- 1994
  - IPng Recommendation

1994
Classless Inter-Domain Routing (CIDR)

"Finally, routing technologies were developed for the Internet to remove the remaining centralized routing aspects. The Exterior Gateway Protocol (EGP) was replaced by a new protocol, the Border Gateway Protocol (BGP). This provided a meshed topology for the Internet and reduced the centric architecture which ARPANET had emphasized. In 1994, **Classless Inter-Domain Routing (CIDR)** was introduced to support better conservation of address space which allowed use of route aggregation to decrease the size of routing tables."
https://historydraft.com/story/history-of-internet/classless-inter-domain-routing/526/9304

IPng Candidates



IP Version Numbers

Version	Name
0-3	Unassigned
4	Internet Protocol (current IPv4)
5	Stream Protocol (ST) (not an IPng)
6	SIP – SIPP – IPv6
7	IPv7 – TP/IX – CATNIP
8	Pip
9	TUBA
10-15	unassigned

Internet (ARPANET) 1977 → IPv4 1981 → IPv6 1995

IP: Next Generation (IPng) White Paper Solicitation
RFC 1550
December 1993

The Recommendation for the IP Next Generation Protocol
RFC 1752
January 1995

Internet Protocol, Version 6 (IPv6) Specification
RFC 1883 Proposed Standard
December 1995

Internet Protocol, Version 6 (IPv6) Specification
RFC 2460 Draft Standard

- Errata exist; Updated by: 5095, 5722, 5871, 6437, 6564, 6935, 7045, 7112
- Obsoleted by: 8200

Internet Protocol, Version 6 (IPv6) Specification
RFC 8200 Internet Standard
July 2017

IP Next Generation (IPng) – Solicitation

IP: Next Generation (IPng) White Paper Solicitation, RFC 1550, December 1993

5. Engineering considerations

See on next slide

6. Security Considerations

"This RFC **raises no security issues**, but does invite comment on the security requirements of IPng."

5.1 **Scaling** - What is a reasonable estimate for the scale of the future data networking environment? The current common wisdom is that IPng should be able to deal with 10 to the 12th nodes.

5.2 **Timescale** - What are reasonable time estimates for the IPng selection, development and deployment process or what should the timeframe requirements be? ...

5.3 **Transition and deployment** - Transition from the current version to IPng will be a complex and difficult process. ...

5.4 **Security** - What level and type of security will be required in the future network environment? What features should be in an IPng to facilitate security?

5.5 **Configuration, administration and operation**

5.6 **Mobile hosts** - How important is the proliferation of mobile hosts to the IPng selection process? ...

5.7 **Flows and resource reservation**

5.8 **Policy based routing**

5.9 **Topological flexibility**

5.10 Applicability - What environment / marketplace do you see for the application of IPng? How much wider is it than the existing IP market?

5.11 **Datagram service** - Existing IP service is "**best effort**" and based on hop-by-hop routed datagrams. What requirements for this paradigm influence the IPng selection?

5.12 **Accounting**

5.13 **Support of communication media**

5.14 **Robustness and fault tolerance**

5.15 **Technology pull** - Are there technologies that will pull the Internet in a way that should influence IPng? Can specific strategies be developed to encompass these?

5.16 **Action items** - suggested charges to the directorate, working groups or others to support the concerns or gather more information needed for a decision

https://datatracker.ietf.org/doc/html/rfc1550

IP Next Generation (IPng) – Recommendation

The Recommendation for the IP Next Generation Protocol, RFC 1752, January 1995

12.1 IPv6 Header Format

The IPv6 header, although longer than the IPv4 header, is considerably simplified. A number of functions that were in the IPv4 header have been relocated in extension headers or dropped. [Deering94b]

```
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Version|                      Flow Label                       |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Payload Length        |  Next Header  |   Hop Limit   |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                         Source Address                        +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                                                               |
+                                                               +
|                                                               |
+                      Destination Address                      +
|                                                               |
+                                                               +
|                                                               |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

* Version - Internet Protocol version number. IPng has been assigned version number 6. (4-bit field)

6.1 The IPng Technical Criteria document

"**security** - IPng must provide a secure network layer"

11.1 IPng Criteria Document and IPng

"security - IPng includes specific mechanisms for **authentication and encryption** at the internetwork layer; the security features do rely on the presence of a yet to be defined key management system"

12. IPv6 Overview

"support for authentication and privacy - IPv6 includes the definition of an extension which provides support for **authentication and data integrity**. This extension is included as a basic element of IPv6 and support for it will be required in all implementations.

IPv6 also includes the definition of an extension to support **confidentiality by means of encryption**. Support for this extension will be strongly encouraged in all implementations."

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

12.2.5 Authentication Header
12.2.6 Privacy Header

22. Security Considerations

"The security of the Internet has long been questioned. … Almost all of this attention has been negative, pointing out the many places where the level of possible security is far less than that deemed necessary for the current and future uses of the Internet."

"The **use of firewalls** is increasing on the Internet. We hope that the presence of the authentication and privacy features in IPv6 will **reduce the need for firewalls**, but we do understand that they will continue to be used for the foreseeable future." …
"**We recommend that an "IPv6 framework for firewalls**" be developed. This framework should explore the ways in which the Authentication Header can be used to strengthen firewall technology and detail how the IPv6 packet should be analyzed by a firewall."

"We believe that IPv6 with its inherent security features will provide the foundation upon which the Internet can continue to expand its functionality and user base."

Internet Protocol, Version 6 (IPv6) Specification

RFC 1883 Proposed Standard, December 1995

```
Security Considerations

   This document specifies that the IP Authentication Header [RFC-1826]
   and the IP Encapsulating Security Payload [RFC-1827] be used with
   IPv6, in conformance with the Security Architecture for the Internet
   Protocol [RFC-1825].
```

Terminology

- **node** - a device that implements IPv6.
- **router** - a node that forwards IPv6 packets not explicitly addressed to itself. [See Note below].
- **host** - any node that is not a router. [See Note below].
- **upper layer** - a protocol layer immediately above IPv6. Examples are transport protocols such as TCP and UDP, control protocols such as ICMP, routing protocols such as OSPF, and internet or lower-layer protocols being "tunneled" over (i.e., encapsulated in) IPv6 such as IPX, AppleTalk, or IPv6 itself.
- **link** - a communication facility or medium over which nodes can communicate at the link layer, i.e., the layer immediately below IPv6. Examples are Ethernets (simple or bridged); PPP links; X.25, Frame Relay, or ATM networks; and internet (or higher) layer "tunnels", such as tunnels over IPv4 or IPv6 itself.
- **neighbors** - nodes attached to the same link.
- **interface** - a node's attachment to a link.
- **address** - an IPv6-layer identifier for an interface or a set of interfaces.
- **packet** - an IPv6 header plus payload.
- **link MTU** - the maximum transmission unit, i.e., maximum packet size in octets, that can be conveyed in one piece over a link.
- **path MTU** - the minimum link MTU of all the links in a path between a source node and a destination node.

Internet Protocol from specification to Internet Standard

Internet Protocol, Version 6 (IPv6) Specification **RFC 1883 Proposed Standard, December 1995** **Internet Protocol, Version 6 (IPv6) Specification** **RFC 2460 Draft Standard, December 1998** **Internet Protocol, Version 6 (IPv6) Specification** **RFC 8200 Internet Standard (STD: 86), July 2017**	**Security Architecture for the Internet Protocol** **RFC 1825, Proposed Standard, August 1995** "This memo describes the security mechanisms for IP version 4 (IPv4) and IP version 6 (IPv6) and the services that they provide. Each security mechanism is specified in a separate document. This document also describes key management requirements for systems implementing those security mechanisms. This document is not an overall Security Architecture for the Internet and is instead focused on IP-layer security." **Security Architecture for the Internet Protocol** **RFC 2401, Proposed Standard, November 1998** "This memo specifies the base architecture for IPsec compliant systems. The goal of the architecture is to provide various security services for traffic at the IP layer, in both the IPv4 and IPv6 environments. This document describes the goals of such systems, their components and how they fit together with each other and into the IP environment. It also describes the security services offered by the IPsec protocols, and how these services can be employed in the IP environment. This document does not address all aspects of IPsec architecture. Subsequent documents will address ..." **Security Architecture for the Internet Protocol** **RFC 4301, Proposed Standard, December 2005** "This document specifies the base architecture for IPsec-compliant systems. ..."

Are you using IPv6?

???

In fact, you are using IPv6!

Internet Protocol version 10 (IPv10)

Internet Protocol version 10 (IPv10) Specification, September 17, 2020
https://datatracker.ietf.org/doc/html/draft-omar-ipv10-12.html

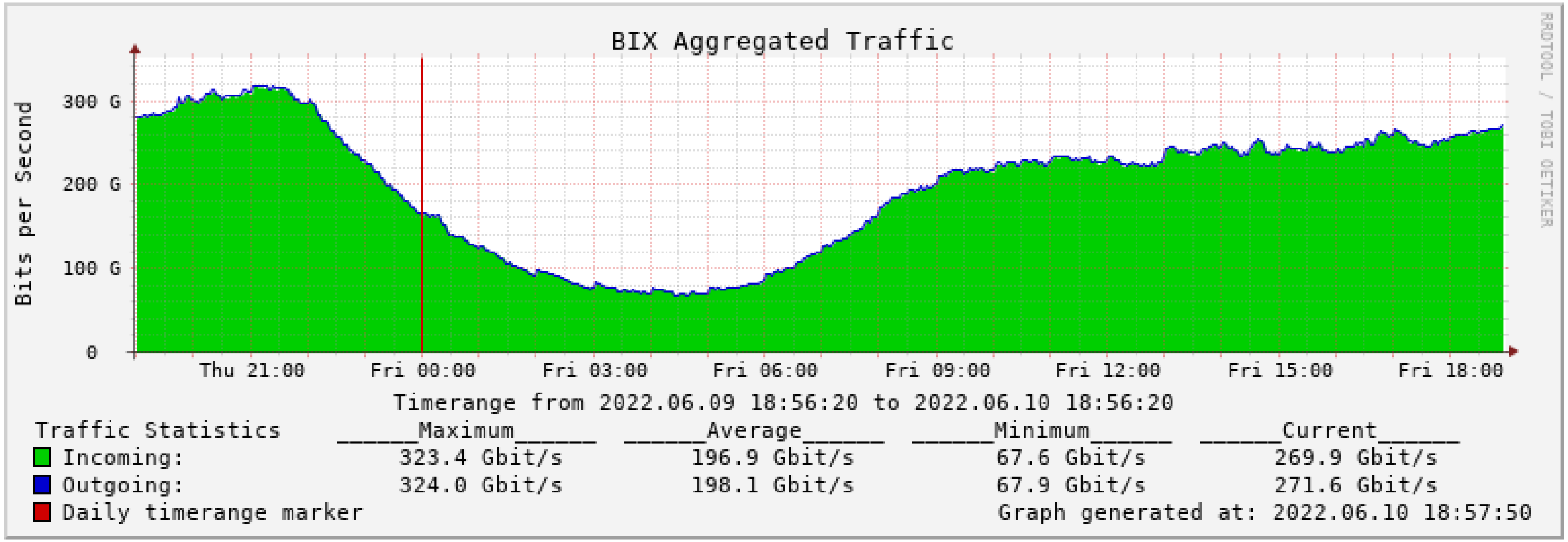
• IPv10 is the solution presented in this Internet draft. • It solves the issue of allowing IPv6 only hosts to communicate to IPv4 only hosts and vice versa in a simple and very efficient way, especially when the communication is done using both direct IP addresses and when using hostnames between IPv10 hosts, as there is no need for protocol translations or getting the DNS involved in the communication process more than its normal address resolution function. • IPv10 allows hosts from two IP versions (IPv4 and IPv6) to be able to communicate, and this can be accomplished by having an IPv10 header containing a mixture of IPv4 and IPv6 addresses added to the original IP packet header regardless the IP packet version. • The new IPv10 header contains a source and destination IP addresses from two different versions. From here the name of IPv10 arises, as the new added header can contain (IPv6 + IPv4 / IPv4 + IPv6) addresses.	Advantages of IPv10. 1) Introduces an efficient way of communication between IPv6 hosts and IPv4 hosts. 2) Allows IPv4 only hosts to exist and communicate with IPv6 only hosts even after the depletion of the IPv4 address space. 3) Adds flexibility when making a query sent to the DNS for hostname resolution as IPv4 and IPv6 hosts can communicate with IPv4 or IPv6 DNS servers and the DNS can reply with any record it has (either an IPv6 record Host AAAA record or an IPv4 record Host A record). 4) There is no need to think about migration as both IPv4 and IPv6 hosts can coexist and communicate to each other which will allow the usage of the address space of both IPv4 and IPv6 making the available number of connected hosts be bigger. 5) IPv10 support on "all" Internet connected hosts can be deployed in a very short time by technology companies developing OSs (for hosts and networking devices, and there will be no dependence on enterprise users and it is just a software development process in the NIC cards of all hosts to allow encapsulating both IPv4 and IPv6 in the same IP packet header. 6) Offers the four types of communication between hosts: - IPv6 hosts to IPv4 hosts (6 to 4). - IPv4 hosts to IPv6 hosts (4 to 6). - IPv6 hosts to IPv6 hosts (6 to 6). - IPv4 hosts to IPv4 hosts (4 to 4).

The previous slide was only a joke.

Maybe it wasn't really a complete joke:-)

"The pandemic has of course changed a great many things, including network traffic patterns, such as a shift away from corporate network traffic towards more domestic traffic during weekdays."
- https://labs.ripe.net/author/stephen_strowes/ipv6-adoption-in-2021/

IPv6 adoption today



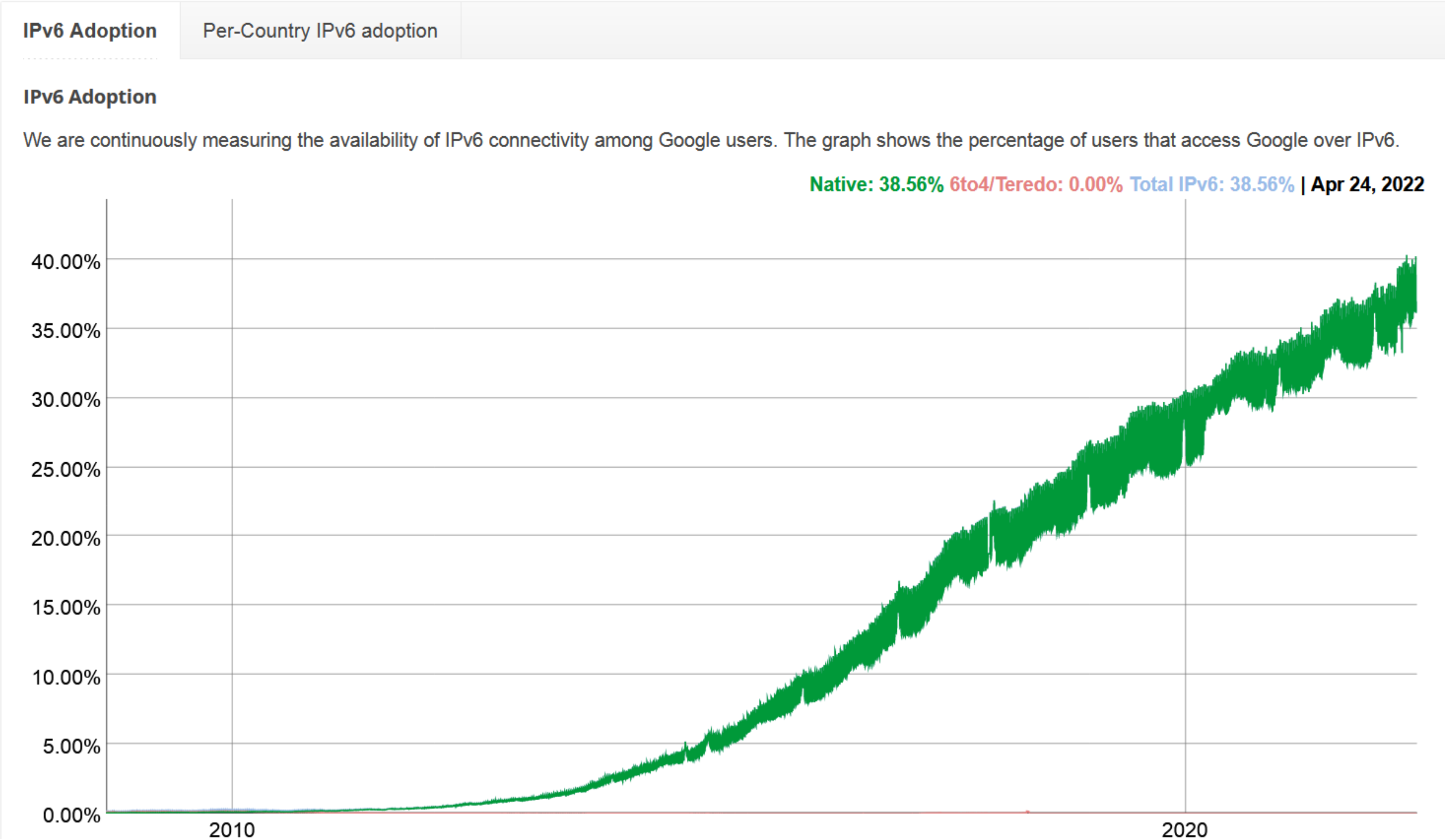
https://www.bix.hu/en/statistics/aggregated, June 10, 2022

How much of this is IPv6?

	IPv6 Traffic (vs Usage/Users)			
	Internet Exchanges	Corporate public|internal	Home	Mobile
World	<3-5%	<10% | <5%	10-30%	30+%
USA	<3%			70++%
South America	5%>			
EU	<5%			
Asia	*little IX traffic*			
Africa	*little IX traffic*			
Hungary	*unknown*			

	IPv6 Traffic				
	YouTube	Facebook	Akamai	CloudFlare	Internet DNS
World	**Why is it difficult to answer clearly?**				
Hungary					

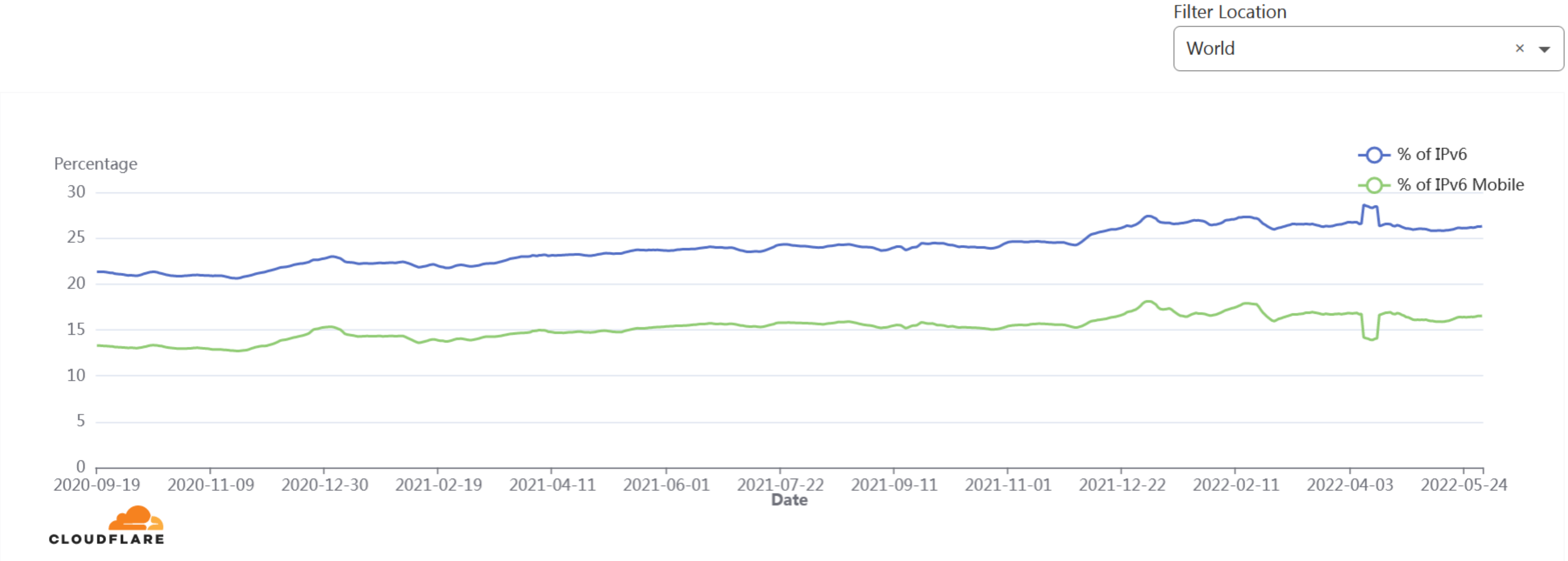
June 2022



"Google collects statistics about IPv6 adoption in the Internet on an ongoing basis. We hope that publishing this information will help Internet providers, website owners, and policy makers as the industry rolls out IPv6."

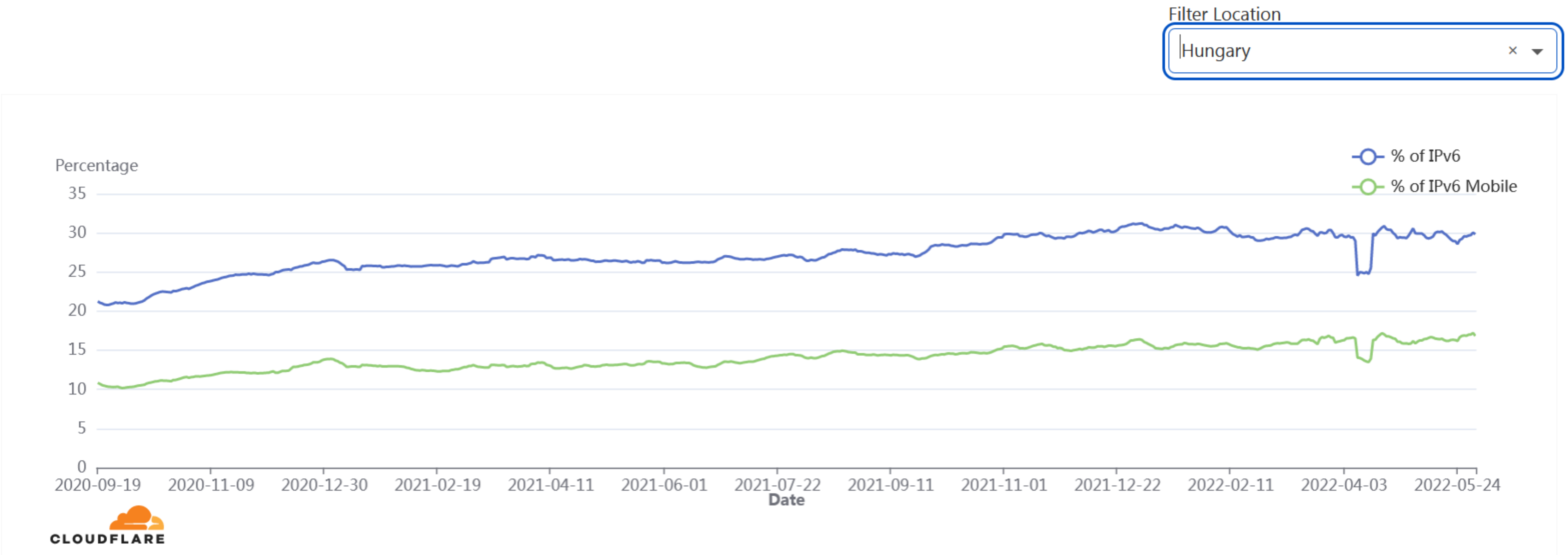
https://www.google.com/intl/en/ipv6/statistics.html

IPv6 adoption trends by location



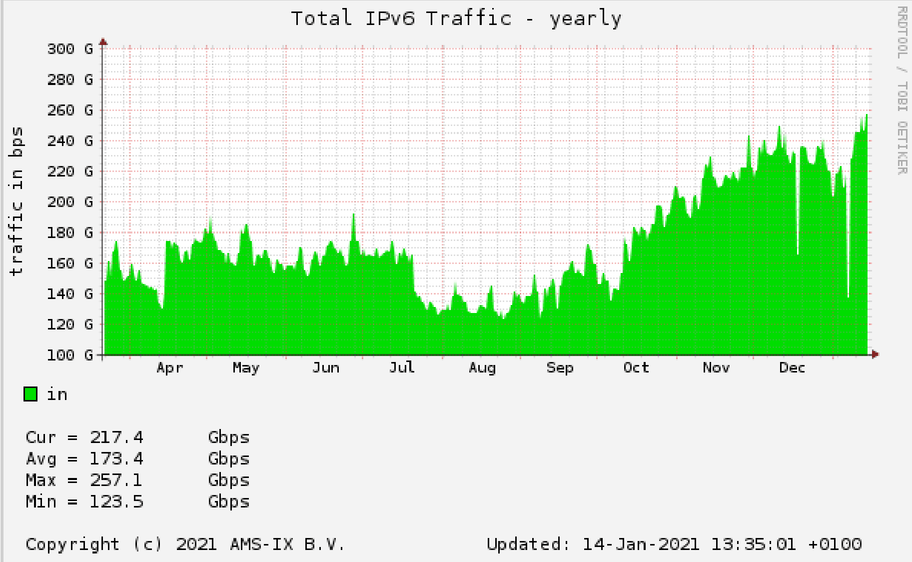
https://radar.cloudflare.com/notebooks/ipv6-adoption-2022

IPv6 adoption trends by location

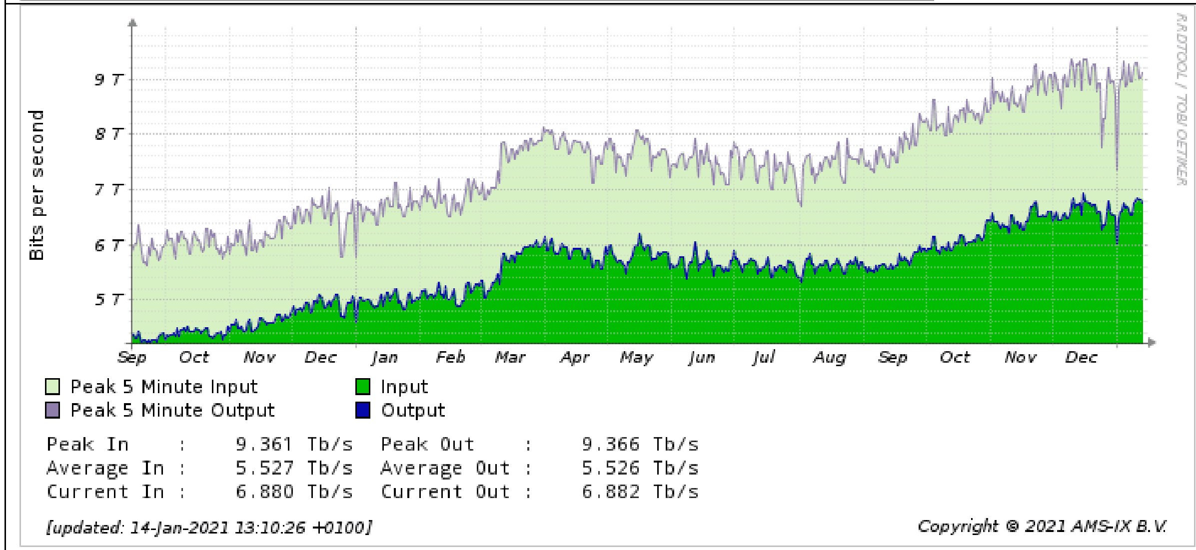


https://radar.cloudflare.com/notebooks/ipv6-adoption-2022

AMS-IX: Amsterdam Internet Exchange Point

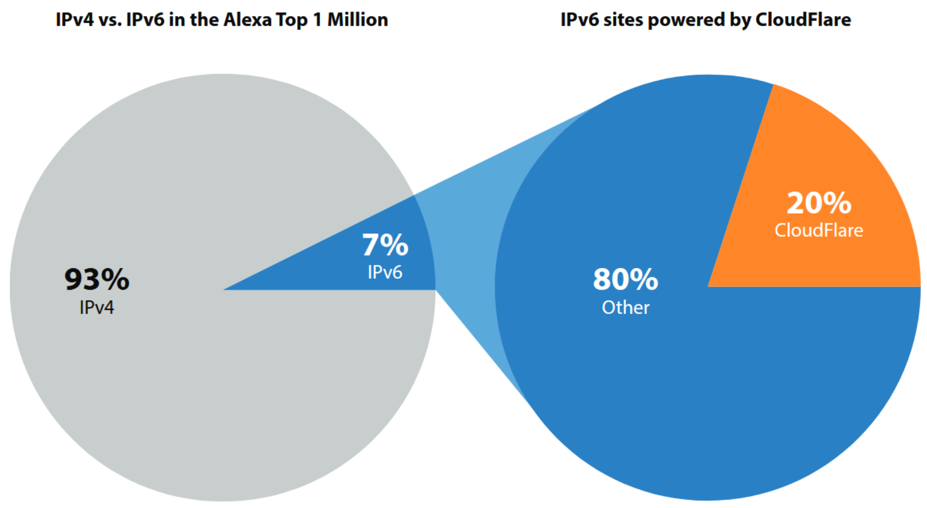


Regarding the adoption of the IPv6 protocol, the following graph shows AMS-IX **IPv6 traffic** from April 2020 to December 2020.

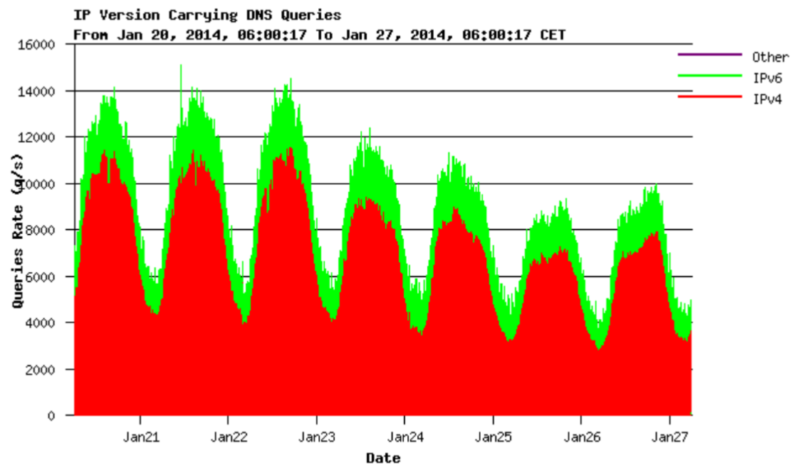


The following graph from AMS-IX stats website shows aggregated traffic statistics from September 2019 to mid-January 2021.

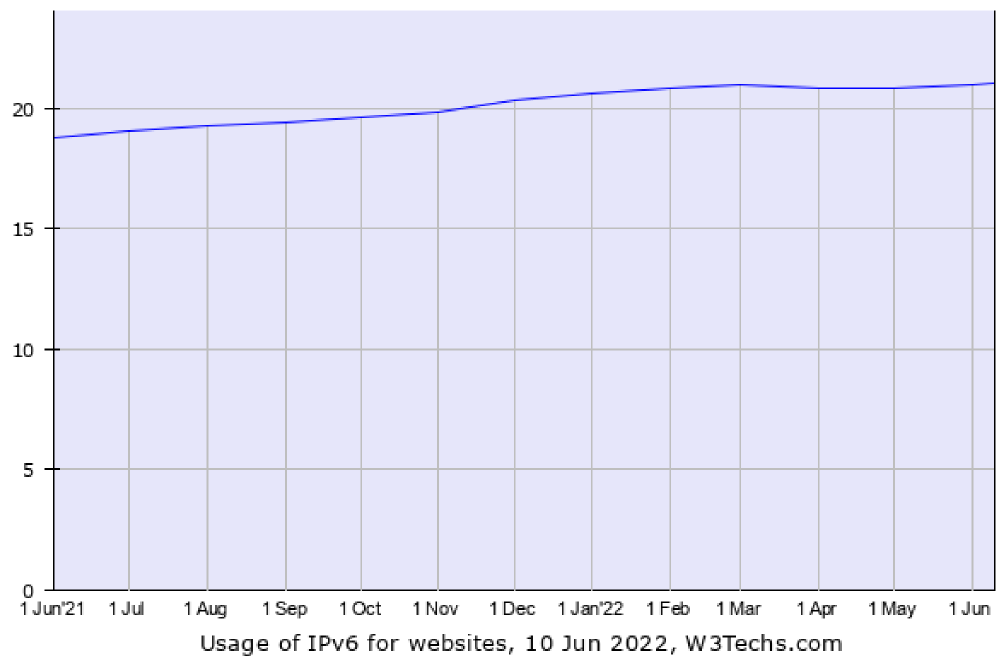
https://www.stackscale.com/blog/ixp-ams-ix/#Traffic



CloudFlare, 2014
https://www.cloudflare.com/static/media/pdf/cloudflare-whitepaper-ipv6.pdf



Statistiky DNS pro doménu .CZ, January 2022



Usage statistics of IPv6 for websites, 2022

This diagram shows the historical trend in the percentage of websites using IPv6.

Popular sites using IPv6:

Google.com Youtube.com Qq.com Facebook.com
360.cn Wikipedia.org Yahoo.com Sina.com.cn
Live.com Zoom.us

https://w3techs.com/technologies/details/ce-ipv6

Well-known providers that do not support IPv6: Slack, Discord, etc.

IPv6 deployment in Hungary by Cisco

IPv6 Deployment : 56.51%

- **Prefixes: 33.15%**
- **Transit AS: 75.5%**
- **Content: 64.57%**
- **Users: 39%**

https://6lab.cisco.com/stats/search.php, June 10, 2022

(https://6lab.cisco.com/stats/information.php#all, https://6lab.cisco.com/stats/information.php#content)

Akamai Report - June 2022[7]

	World IPv6 Launch (2012)	10 years later (2022)
Peak IPv6 traffic	~1 Gbps	41 Tbps *(> 41,000 Gbps)*
Daily IPv6 requests	3.9 billion per day *(and 8 million in 2011)*	> 4,000 billion per day
IPv6 addresses observed per day	19 million	7.5 billion *(across 2.2 billion "/64" prefixes)*

Fig. 1: How IPv6 traffic on the Akamai CDN has grown in the decade since World IPv6 Launch

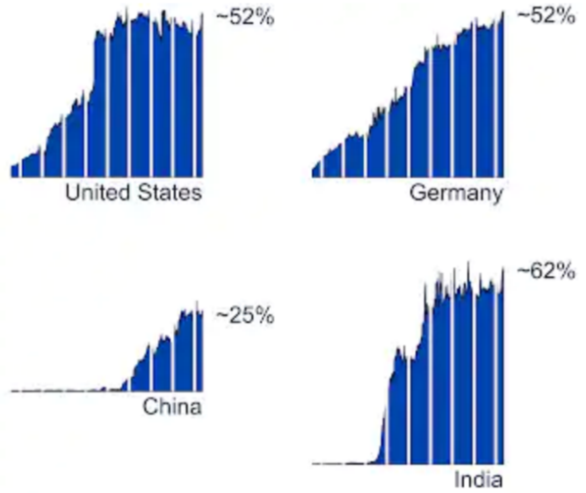


Fig. 2: Percentage of requests over IPv6 to a subset of dual-stack sites on Akamai from July 2013 to May 2022 for top 10 global economies (by GDP in 2022, per IMF).

In this pictures:
USA, Germany, China and India of this ten economies.

- **IPv6 Mobile**

"Many of the world's largest mobile ISPs have migrated their networks to be IPv6-centric, and more than 90% of handsets on those networks have IPv6-only connectivity."

- **IPv6-only clients on closed systems**

"A number of closed-system client device platforms have been deploying with a single-stack IPv6-only model."

- **IPv6-enabled relay services[8]**
- **IPv4+IPv6 dual-stack content (on CDNs)**
- **IPv6 enables better performance, perhaps enchanced security**
- **IPv6-only for cloud hosting and server deployments**
- **Enable dual-stack delivery with the CDN**
- **New opportunities, broader deployment, more content and services, IoT, consumer devices and services, gaming, VR, IPv6 only providers, services, data centers and (open) software**

[7] https://www.akamai.com/blog/trends/10-years-since-world-ipv6-launch

[8] e.g. Apple's iCloud Private Relay (https://www.akamai.com/blog/cloud/powering-and-protecting-online-privacy-icloud-private-relay)

China

"A few days ago, the Central Cyberspace Administration of China, the National Development and Reform Commission, and the Ministry of Industry and Information Technology jointly issued the "2022 Work Arrangement for Further Promoting the Large-scale Deployment and Application of IPv6" (hereinafter referred to as the "Work Arrangement").

...

"Notice on Accelerating the Large-scale Deployment and Application of the Internet Protocol Version 6 (IPv6)" shall be implemented in depth. ... comprehensively improve the level of IPv6 development, and take practical actions to welcome the victory of the 20th Party Congress.

...

The "Work Arrangement" clarifies the work goals for 2022 : by the end of 2022,

- **the number of active IPv6 users will reach 700 million,**
- **the number of IPv6 connections in the Internet of Things will reach 180 million,**
- **the proportion of IPv6 traffic on fixed networks will reach 13%,**
- **and the proportion of IPv6 traffic on mobile networks will reach 45%."**

– http://www.cac.gov.cn/2022-04/25/c_1652510306015791.htm, April 25, 2022

India

2-8/IPV6-Review/2015-NT
Government of India
Ministry of Communications
Department of Telecommunications
(Networks and Technology Wing)

Date: 02/11/2021

Subject: Revision of IPv6 Transition Timelines– reg.

In continuation to the DoT's letter of even number dated 11 Feb 2020 regarding revision of IPv6 Transition timelines, approval of the competent authority is hereby conveyed for further extension of timelines for IPv6 Transition as under:

a) All Government organizations should complete IPv6 transition and migration of their websites on IPv6 latest by 30th June,2022.

b) All new retail wireline customer connections provided by Service Providers after 31st December, 2022 shall be capable of carrying IPv6 traffic either on dual stack or on native IPV6.

c) The Service Providers shall endeavour to progressively replace/upgrade the CPEs which are not IPv6 ready and are owned by Service Providers latest by 31st December,2022.

This is for kind information and necessary action please.

(Sachin Rathore)
ADG(NT-I)

https://dot.gov.in/ipv6-transition

"NEW DELHI: The department of telecom (DoT) has fixed **December 2022 as the deadline for internet service providers to customise their network as well as change modem and routers at customer premise for the services as per the internet protocol address, IPv6**.

The DoT has set June 30, 2022, as the last date for government organisation for complete transition to IPv6, according to an official note issued on November 2.

All new retail wireline customer connections provided by service providers after December 31, 2022, shall be capable of carrying IPv6 traffic either on dual stack on native IPv6," the note said.

The IP addresses help in identifying and connecting various devices and servers onto the internet."

http://timesofindia.indiatimes.com/articleshow/87541813.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst, November 5, 2021

"The Occam's razor principle of "if it's not necessary, don't add entities", from the perspective of IT professionals is "as long as it works, don't change it."
https://coinyuppie.com/will-metaverse-become-an-inflection-point-for-ipv6/

Metaverse

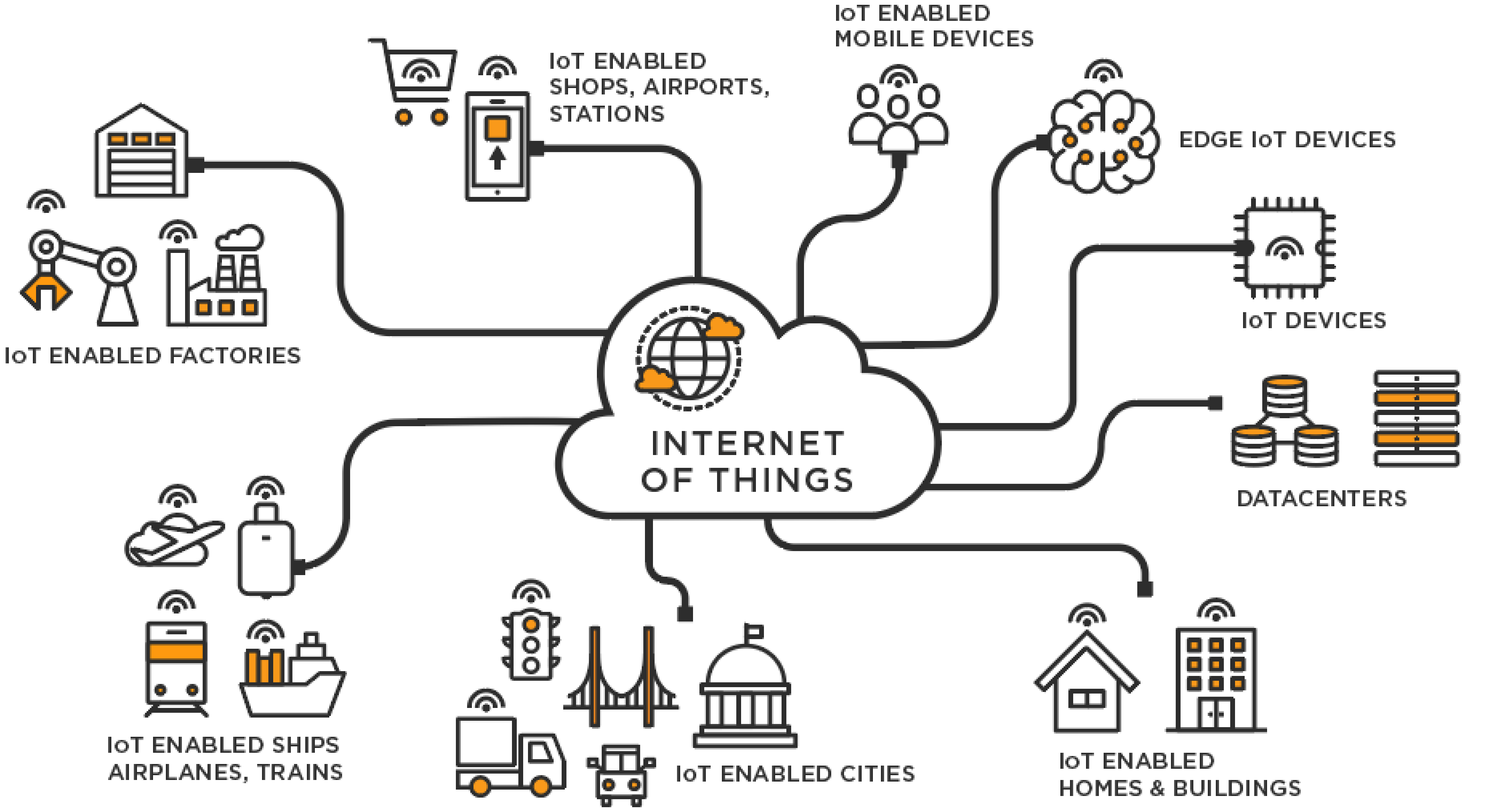
Will Metaverse become an inflection point for IPv6?
— https://coinyuppie.com/will-metaverse-become-an-inflection-point-for-ipv6/

Without IPv6 there may be no Metaverse - The Metaverse will be possible thanks to IPv6
— https://prensa.lacnic.net/news/en/ipv6/why-is-ipv6-so-important-for-the-development-of-the-metaverse

Metaverses or metauniverses are environments where humans interact socially and economically through their avatars in cyberspace, which is an amplified metaphor for the real world, except that there are no physical or economic limitations.
"You can think about the Metaverse as an embodied Internet, where instead of just viewing content — you are in it. And you feel present with other people as if you were in other places, having different experiences that you couldn't necessarily have on a 2D app or webpage."
— Mark Zuckerberg, Facebook CEO

"Key elements:
IPv6 is the only protocol that can guarantee enough IP resources to support the Metaverse. IPv6 avoids the use of NAT mechanisms that would create technological difficulties for the deployment of the Metaverse. **IPv6 links have lower RTT delay than IPv4 links**, and this allows avatar representations, including holograms, to be displayed synchronously. Considering the huge amount of data involved in the deployment of the Metaverse, it is necessary to ensure the least possible data loss. This is why **IPv6 is the best option**, as evidence shows that **data loss is 20% lower when** using IPv6 than when using IPv4"
— https://prensa.lacnic.net/news/en/ipv6/why-is-ipv6-so-important-for-the-development-of-the-metaverse
— https://medium.com/@alantraceywootton/proposing-a-transport-layer-for-the-metaverse-e4f52bdf4241

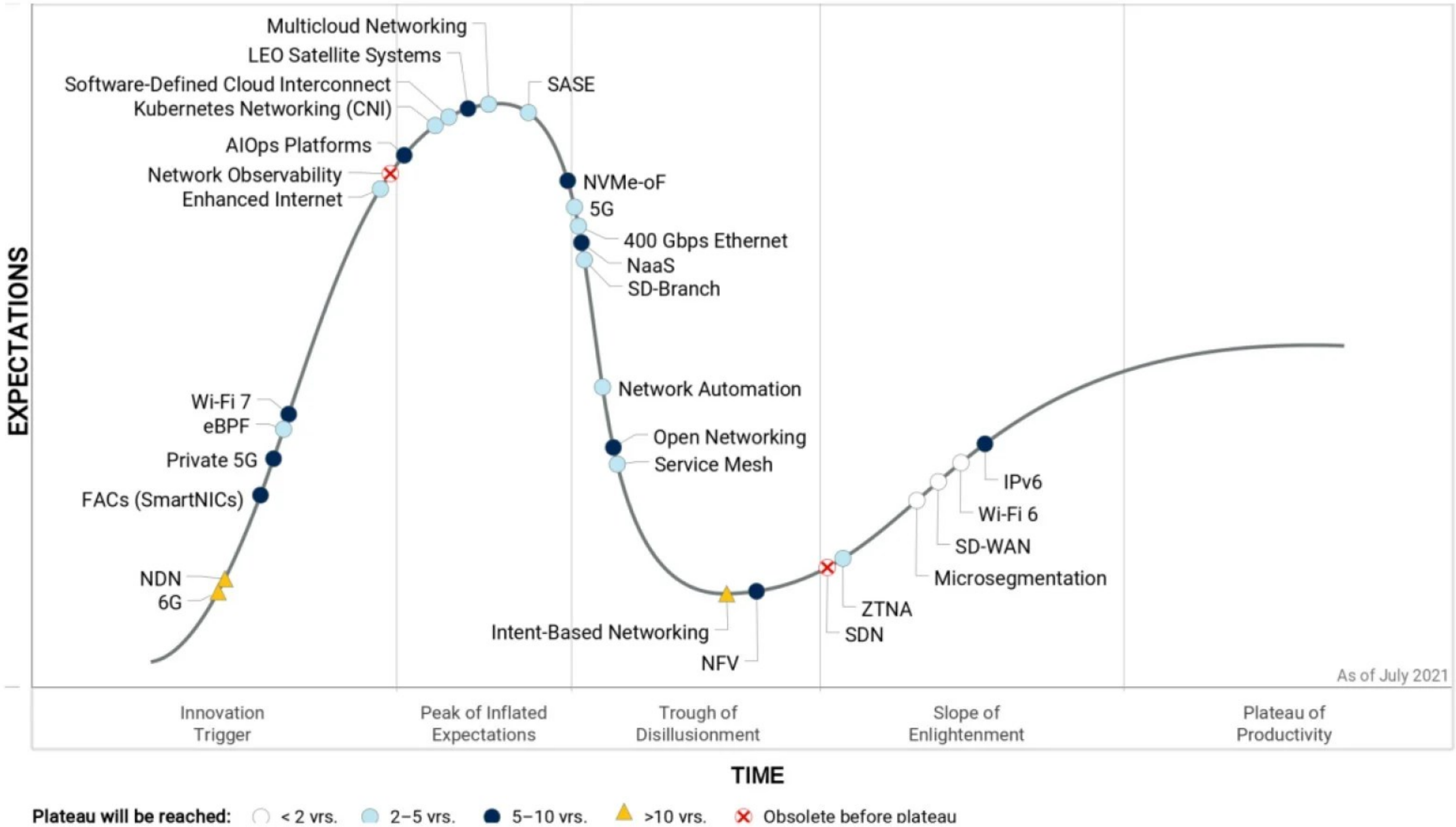
IoT



https://threws.com/future-of-iot-using-machine-learning/

Gartner's latest Hype Cycle for Enterprise Networking, 2021

"**IPv6 is still five to ten years away from ascending** to analyst firm Gartner's **plateau of productivity**, and remains a technology **employed by only "early mainstream" users**."
– https://www.theregister.com/2021/07/15/ipv6_istilli_510_years_away/



Attack surface

IPv4 attack surface < IPv4 attack surface + IPv6 attack surface

https://en.wikipedia.org/wiki/Attack_surface

Vulnerability of networks < Vulnerability of applications

IPv6 terminology

Node
Host
Router
Interface

Neighbor
Link

Link-local address
Unique-local address (ULA)
Global unicast address (GUA)
IPv4 embedded address

Scope, Zone, Zone_ID

Extension header
Packet flow identification

Link MTU, Path MTU

Dual host

Translation

IP autoconfiguration

Neighbor Discovery
Neighbor Solicitation and Advertisement
Router Solicitation and Advertisement

Stateless address autoconfiguration (SLAAC)

RA Guard
RA throttling

AAAA record

IPv6 address space

2^{128} addresses
typical 2^{64} subnet and 2^{64} interface address

Address categories:

- Unicast
- Anycast
- Multicast (no broadcast)

Scoping concepts (scopes, zones)

Address configuration

Why a new Internet protocol?

Why was it created?

What are the constraints?

What are the driving forces?

What are our benefits?

Why now? (Why yesterday? Why tomorrow?)

What is fundamentally different?

- 128-bit address space
  - New header format
  - Routing operations
  - Fragmentation, MTU(s)
  - Network configuration (autoconfiguration etc.)
  - …

Further improvements:

- Jumbogram
- Address scopes
- …

Consequences:

- Exile of NAT
- …

(See also: IPsec, QoS, Flow Labels, …)

Deficiencies and imperfections

- Support
- Faulty codes and implementations
- Knowledge and practice
- IPv6 reputation
- Renumbering difficulties
- …

- Security
- DDoS protection
- Privacy
- Rate-limiting
- IPsec …
- QoS
- Flow

NAT sentenced to death

"One of the primary goals of humanity is not to repeat the same mistakes made in the past. The desire is to “fail forward” frequently in different ways on the path to continual improvement. When it comes to IPv6, the protocol designers wanted to avoid repeating the mistakes of IPv4; specifically, its limited address space that necessitates Network Address Translation (NAT)."

"**IPv6 advocates** have extolled the benefits of **restoring the end-to-end model** of communication originally conceived of by the early IPv4 protocol designers. IPv6 **evangelists have also cautioned against using NAT with IPv6**. However, **many network and security architects are comfortable with the concept of NAT and may wonder why NAT doesn’t exist for IPv6**."

"For decades, IPv6 purists have fought against establishing a standard for IPv6 NAT (e.g., IPv6 to IPv6 Network Address Translation or NAT66).

Today, **there isn’t even a pending draft of NAT66**, much less a published IETF RFC. In addition, there is an IETF RFC titled “Local Network Protection for IPv6” (RFC 4864) that lists all the reasons why NAT is not needed for IPv6."

Statfull NAT versus stateless NPT66 – see next slide

“IPv6-to-IPv6 Network Prefix Translation” (RFC 6296). Note the subtlety in the RFC title where the word “Prefix” takes the place of the word “Address”.

- https://blogs.infoblox.com/ipv6-coe/you-thought-there-was-no-nat-for-ipv6-but-nat-still-exists/ (December 28, 2021)

NPT66

IPv6-to-IPv6 Network Prefix Translation (NPT66)
RFC 6296 (Experimental, June 2011)

Features:
- **stateless, transport-agnostic**
- it allows direct inbound connections to internal nodes
- function that provides the address-independence
- 1:1 relationship between addresses in the inside" and "outside" prefixes, preserving end-to-end reachability at the network layer

Uses:
- Hiding hosts
- Avoid renumbering
- Between Peer Networks
- Redundancy and Load Sharing
- Multihoming

Security:
- It is RECOMMENDED that NPTv6 Translators also implement firewall functionality randomizing the subnet identifier, the idea is to make it harder for worms to guess a valid subnet identifier at an advertised network prefix;
- Due to the potential interactions with IKEv2/IPsec NAT traversal, it would be valuable to test interactions of NPTv6 with various aspects of current-day IKEv2/IPsec NAT traversal.

Mike O'Dell: GSE - An Alternate Addressing Architecture for IPv6 (GSE for IPv6, Internet-Draft v3.7, February 1997)

Central Concepts of the Architecture:
- **A strong distinction between Public and Private Topology**
- A strong distinction between system identity and location
- **GSE - Global, Site, and End-system address elements**
- The deep similarity of Re-homing and Multi-homing
- Rewriting address prefixes at Site boundaries
- Very aggressive hierarchical network topology aggregation
- Optimizing actual forwarding paths by limited-scope cut-throughs

```
External Network:  Prefix = 2001:0DB8:0001:/48
   --------------------------------------
                 |
                 |
           +-------------+
           |    NPTv6    |
           |  Translator |
           +-------------+
                 |
                 |
   --------------------------------------
Internal Network:  Prefix = FD01:0203:0405:/48
```

Figure 1: A Simple Translator (The Simplest Case)

```
   Internal Prefix = FD01:4444:5555:/48
   --------------------------------------
     V           |      External Prefix
     V           |      2001:0DB8:6666:/48
     V       +---------+     ^
     V       | NPTv6   |     ^
     V       | Device  |     ^
     V       +---------+     ^
External Prefix      |           ^
2001:0DB8:0001:/48   |           ^
   --------------------------------------
   Internal Prefix = FD01:0203:0405:/48
```

Figure 2: Flow of Information in Translation (NPTv6 between Peer Networks)

```
External Network:  Prefix = 2001:0DB8:0001:/48
   --------------------------------------
       |                 |
       |                 |
   +-------------+   +-------------+
   | NPTv6       |   | NPTv6       |
   | Translator  |   | Translator  |
   |  #1         |   |  #2         |
   +-------------+   +-------------+
       |                 |
       |                 |
   --------------------------------------
Internal Network:  Prefix = FD01:0203:0405:/48
```

Figure 3: Parallel Translators (Redundancy and Load Sharing)

```
  External Network #1:         External Network #2:
Prefix = 2001:0DB8:0001:/48    Prefix = 2001:0DB8:5555:/48
---------------------------    ---------------------------
       |                 |
       |                 |
   +-------------+   +-------------+
   | NPTv6       |   | NPTv6       |
   | Translator  |   | Translator  |
   |  #1         |   |  #2         |
   +-------------+   +-------------+
       |                 |
       |                 |
   --------------------------------------
Internal Network:  Prefix = FD01:0203:0405:/48
```

Figure 4: Parallel Translators with Different Upstream Networks (Multihoming)

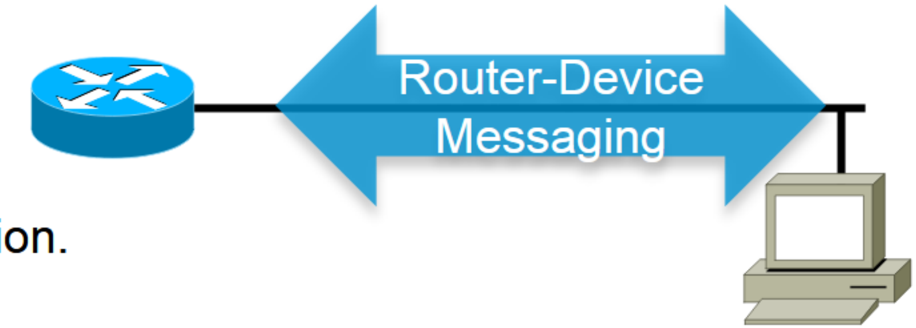
https://datatracker.ietf.org/doc/html/rfc6296

Neighbor Discovery and Router Advertisement

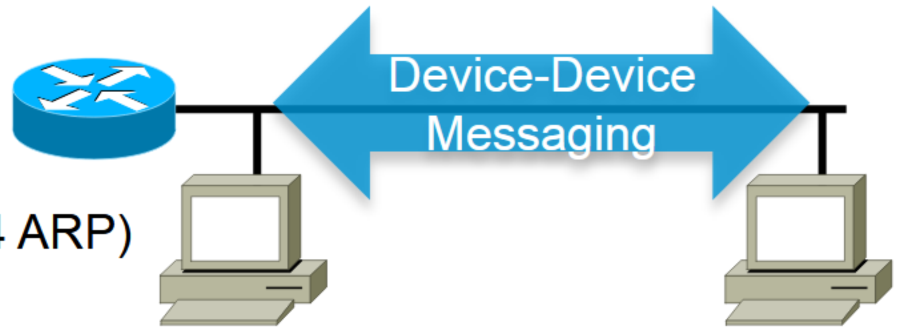
“Introducing” ICMPv6 Neighbor Discovery

ICMPv6 informational messages used by Neighbor Discovery (RFC 4861):

- **Router Solicitation Message**
- **Router Advertisement Message**
  - Used for dynamic address allocation.



- **Neighbor Solicitation Message**
- **Neighbor Advertisement Message**
  - Used with address resolution (IPv4 ARP) and with DAD

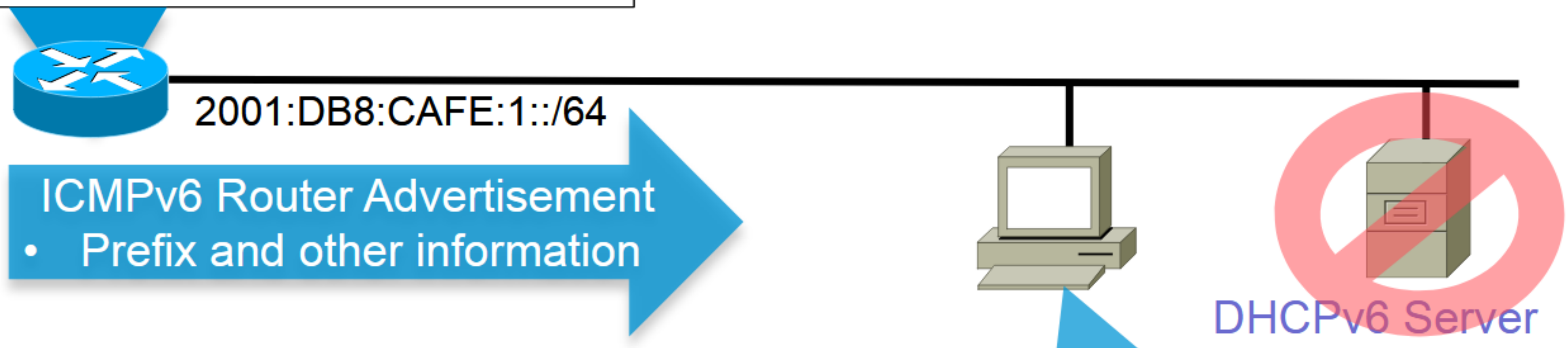


- **Redirect Message (Similar to ICMPv4)**

SLAAC and DHCPv6

SLAAC: Stateless Address Autoconfiguration

```
Router(config)# ipv6 unicast-routing
```



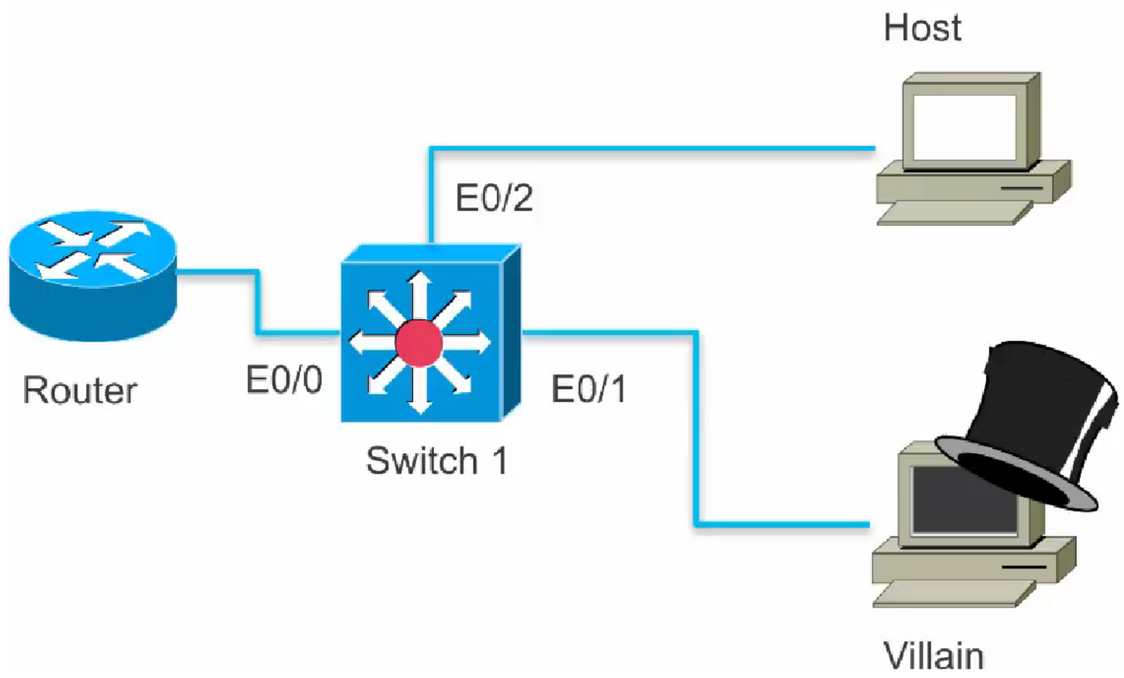
I know the network prefix from the RA.
I just need to come up with my own Interface ID for my GUA!

SLAAC (Stateless Address Autoconfiguration)

- Allows a device to create its own IPv6 global unicast address without the services of a DHCPv6 server.
- **Prefix:** From the Router Advertisement (RA).
- **Interface ID:**
  - EUI-64
  - Random 64-bit value

First Hop Security (e.g. RA Guard)

"IPv6 FHS (First Hop Security) are different features that secure IPv6 on L2 links. First “hop” might make you think about the first router but that's not the case. These are all switch features, in particular, the switch that sits between your end devices and the first router."
– https://networklessons.com/cisco/ccie-routing-switching-written/ipv6-first-hop-security-features



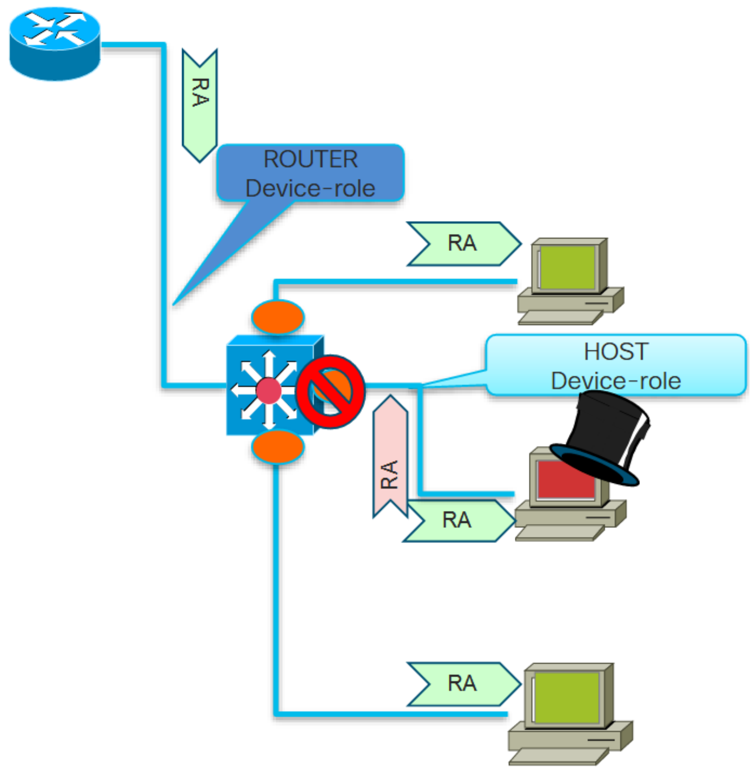
First Hop Security: RAguard since 2010 (RFC 6105)

- Port ACL
  blocks all ICMPv6 RA from hosts

```
interface FastEthernet0/2
  ipv6 traffic-filter ACCESS_PORT in
  access-group mode prefer port
```

- RAguard

```
ipv6 nd raguard policy HOST
 device-role host
ipv6 nd raguard policy ROUTER
 device-role router
vlan configuration 1
 ipv6 nd raguard attach-policy HOST
interface Ethernet0/0
 ipv6 nd raguard attach-policy ROUTER
```



cisco Live!

https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKSEC-3200.pdf

FHS implementation shortcomings

Switches and routers	**Virtualization**
• RA Guard impelemted: e.g. Cisco, HPE, Broadcom, Juniper • Arista EOS – it is an alternative solution? • RA Guard not implemented: e.g. Mikrotik	• Hyper-V - full implementation from Windows 2012 R2, Hyper-V 3.0 • VMware (with or without NSX) - the situation is disgraceful • KVM - it depends …

ICMPv6 types and filtering

Internet Control Message Protocol (ICMPv6) for the Internet Protocol Version 6 (IPv6) Specification, RFC 4443 (Internet Standard, 2006, Updated by: 4884)

Neighbor Discovery for IP version 6 (IPv6) RFC 4861 (Draft Standard, September 2007):

133 Router Solicitation
134 Router Advertisement
135 Neighbor Solicitation
136 Neighbor Advertisement
137 Redirect Message

https://www.iana.org/assignments/icmpv6-parameters/icmpv6-parameters.xhtml

From: draft-ietf-v6ops-icmpv6-filtering-recs-03 Informational
Errata exist

Network Working Group E. Davies
Request for Comments: 4890 Consultant
Category: Informational J. Mohacsi
NIIF/HUNGARNET
May 2007

Recommendations for Filtering ICMPv6 Messages in Firewalls

```
# from RFC 4890
chain icmpv6-nontransit {
   jump icmpv6-both

   # MUST NOT BE DROPPED
   # configuring the node and maintaining unicast and
multicast communications through the interfaces of a
node
   icmpv6 type nd-router-solicit accept
   icmpv6 type nd-router-advert accept
   icmpv6 type nd-neighbor-solicit accept
   icmpv6 type nd-neighbor-advert accept
   icmpv6 type ind-neighbor-solicit accept
   icmpv6 type ind-neighbor-advert accept

   # Link-Local Multicast Receiver Notification
   icmpv6 type mld-listener-query accept
   icmpv6 type mld-listener-report accept
   icmpv6 type mld-listener-done accept
   icmpv6 type mld2-listener-report accept

   # SEND Certificate Path Notification
   icmpv6 type 148 accept
   icmpv6 type 149 accept

   # Multicast Router Discovery
   icmpv6 type 151 accept
   icmpv6 type 152 accept
   icmpv6 type 153 accept
}

# from RFC 4890
chain icmpv6-transit {
   jump icmpv6-both
}

# from RFC 4890
chain icmpv6-both {
   # MUST NOT BE DROPPED
   # establishment and maintenance of communications
   icmpv6 type destination-unreachable accept
   icmpv6 type packet-too-big accept
   icmpv6 type time-exceeded icmpv6 code 0 accept
   icmpv6 type parameter-problem icmpv6 code { 1, 2 }
accept

   # connectivity checking
   icmpv6 type echo-request accept
   icmpv6 type echo-reply accept

   # SHOULD NOT BE DROPPED
   icmpv6 type time-exceeded icmpv6 code 1 accept
   icmpv6 type parameter-problem icmpv6 code 0 accept
}
```

 # Vencel Tátos, 2022

Neighbor Discovery and Router Advertisement security hardening

IPsec – Why not?

SeND

– unfortunately, this is not yet applicable always or everywhere

```
"IPv6 has the same stupid shit as IPv4"
"IPv6 Security is distinct from IPv4 Security"
```

Major IPv6 security issues

- **Network Security vs Application Security**

- **The Internet lacks effective privacy and effective authentication mechanisms beneath the application layer.**
- **IPv6 as a protocol suite isn't inherently more or less secure than its predecessor.**

- **Larger attack surface**
- **Two protocols that live together and are used together**
- **Vulnerable translation mechanisms and implementations**

Same	**IPv4 only**	**New in IPv6 era**
• Reconnaissance Attacks • Denial of Service Attacks • Man-in-the-middle Attacks • Address Spoofing Attacks • Malware Attacks	• ARP poisoning Attacks • We have been forced to use NAT and CGN	• Gigantic address space ○ sparse allocation of addresses • ND and RA, autoconfiguration • No more NAT

Major IPv6 security issues:

- Inadequate IPv6 Security Training and Education
- Ineffective Rate Limiting
- Lack of IPv6 Support at ISPs and Vendors
- Logging Systems and SIEM Systems May Not Work Properly
- Bugs in (New) Code
- IPv6 (May) Run By Default
- Absence of Network Address Translation (NAT)

DoS/DDoS and IPv6

"**There is not any mechanism to protect against DoS attacks.** Defending against these type of attacks is outside the scope of this specification."
Internet Protocol, Version 6 (IPv6) Specification
RFC 8200 (Internet Standard, July 2017)

See also Operational Security Considerations for IPv6 Networks (RFC 9099, August 2021)

- There are special vulnerabilities in IPv6 (e.g. ND, RA, autoconfiguration etc.).
- There are weaknesses in IPv6 design and implementation (e.g. rate limiting).
- There are, can be and will be immaturity, unrecognized flaws or imperfections in design, implementation and codes.

"IPv6 has several vulnerabilities

- First, due to their relatively immature nature as network structures, most IPv6 networks are ill-equipped to identify DDoS attacks when they occur.
- Next, many network administrators apparently have no intention of creating plans to mitigate future cyber-attacks, leaving their networks open and exposed, although this situation will undoubtedly change should DDoS attacks increase significantly.

…

The first recorded incidence of a significant IPv6 DDoS attack was recorded in March 2018 where a DNS dictionary attack originated from over 1,900 native IPv6 hosts. The attack occurred on more than 650 networks and targeted the DNS service Neustar."

https://www.allot.com/blog/ipv6_ddos_attack_vulnerability/#
https://www.siliconrepublic.com/machines/ipv6-iot-ddos-mobile-world-congress

IPv6 security incidents and DDos attacks

Very few reported incidents and attacks,

- none have been reported to HunCERT yet,
- only a few major attacks are known in the world, but they are also orders of magnitude smaller (even the largest involved only 1,900 hosts, which was an attack in 2018[9]) than the largest IPv4 attacks.

It is not yet worthwhile for hackers to focus on IPv6.

Unfortunately, this will inevitably change.

---

[9] https://www.siliconrepublic.com/machines/ipv6-iot-ddos-mobile-world-congress

Benefits

Increased address space – from 32 bits to 128 bits

Room for many levels of structured hierarchy and routing aggregation
The ability to deploy new services and expand networks without battling constraints of address exhaustion
Easier and better address management and delegation than IPv4 (stateless auto-configuration)

NAT – we can get rid of NAT and CGN

New opportunities

Speed[10]

Meet/fulfill customer[11] expectations

Potential benefits:

Security QoS Flow ...

[10] latency, bandwidth, packet loss
[11] and other

Legal and regulatory issues

There are websites, services **that are only available on IPv6**, and there are Internet features that are only available on IPv6, and for which translation solutions are unsuitable, inadequate, or unsatisfactory.

1. **Is an IPv4 only service a full-featured Internet access service?**
2. **Should consumers and buyers be made aware of this?**
3. **How much should be highlighted and emphasize?**

And what would we get if we asked these questions with IPv6 as well?

Privacy

?

Best Practices

Scenario 1 What should I do if I don't want to use IPv6 at all?

Scenario 2 All I need is to make my website available on IPv6 as well.

Scenario 3 I want to use an isolated internal IPv6 network.

Scenario 4 I provide co-lococation hosting services, my client needs IPv6 in addition to IPv4.

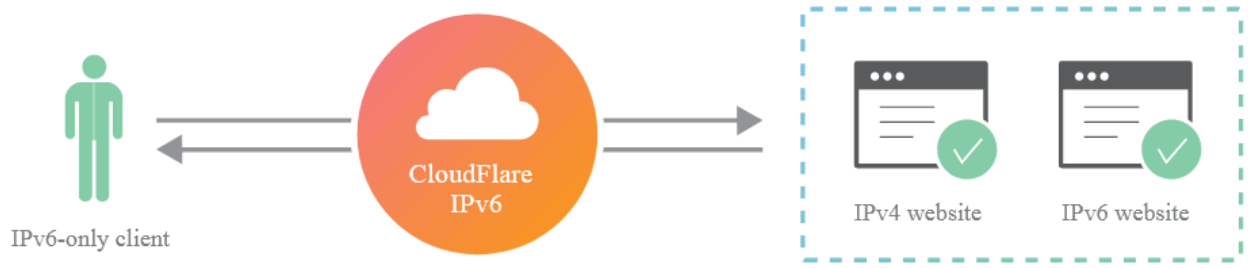
More sophisticated cases:

Scenario …
…

Solutions and cases

CloudFlare

IPv4-to-IPv6 Translation Gateway



Cloudflare's Automatic IPv6 Gateway allows IPv4-only websites to support IPv6-only clients with no additional configuration. No hardware. No software. No code changes. And no need to change your hosting provider.

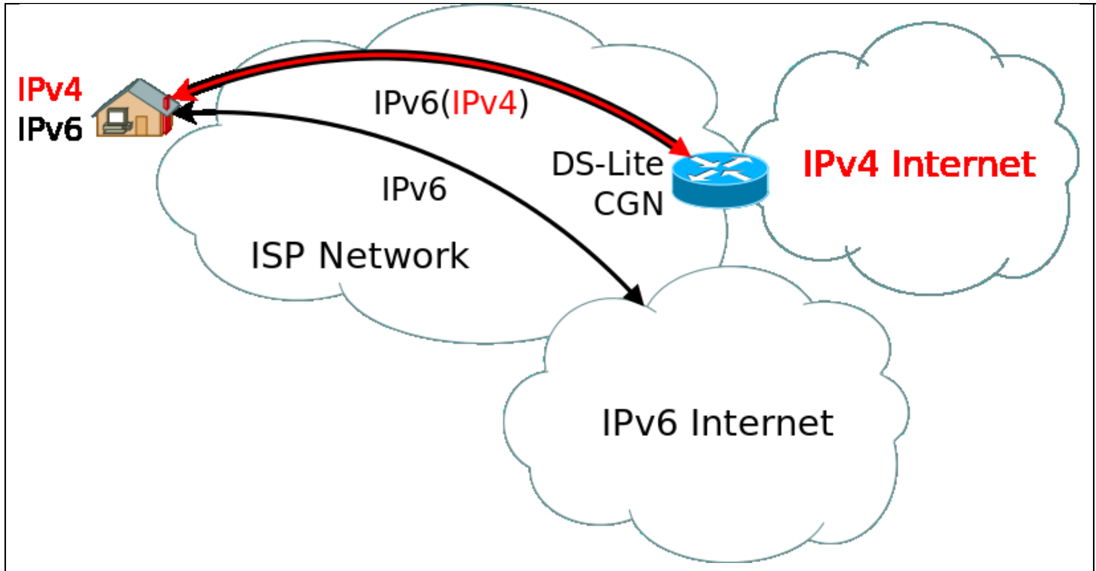
"**Pseudo IPv4**

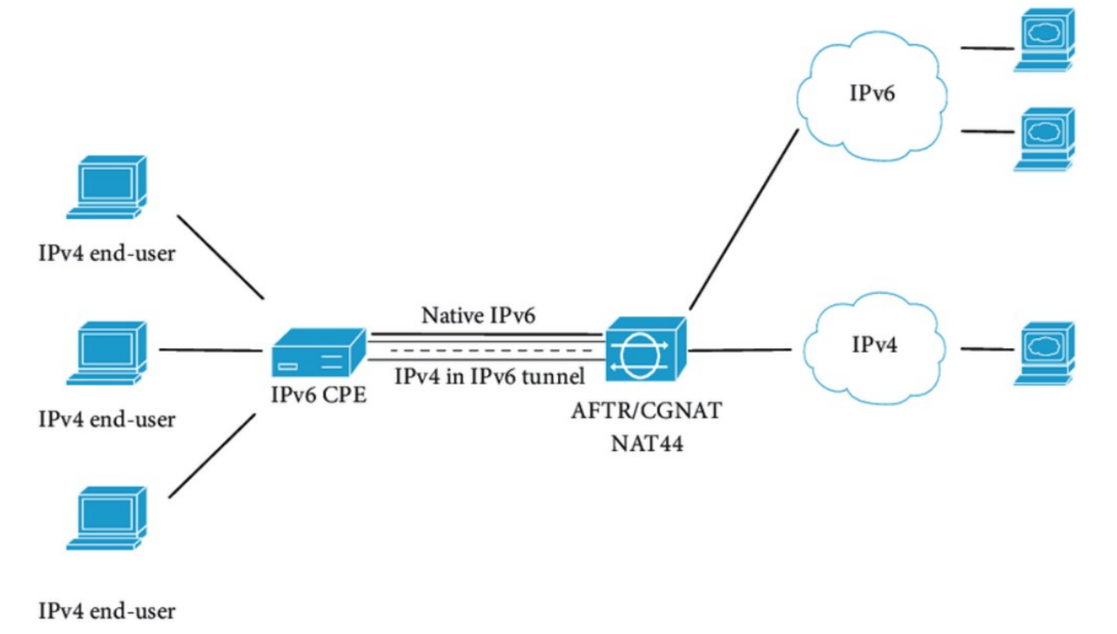
Legacy services that require IPv4 support can take advantage of our Pseudo IPv4 service. Pseudo IPv4 works by adding an HTTP header to requests established over IPv6 with a "pseudo" IPv4 address. Using a hashing algorithm, Pseudo IPv4 will create a Class E IPv4 address which will always produce the same output for the same input; the same IPv6 address will always result in the same Pseudo IPv4 address."

https://www.cloudflare.com/ipv6/

https://www.cloudflare.com/static/media/pdf/cloudflare-whitepaper-ipv6.pdf

DS-Lite



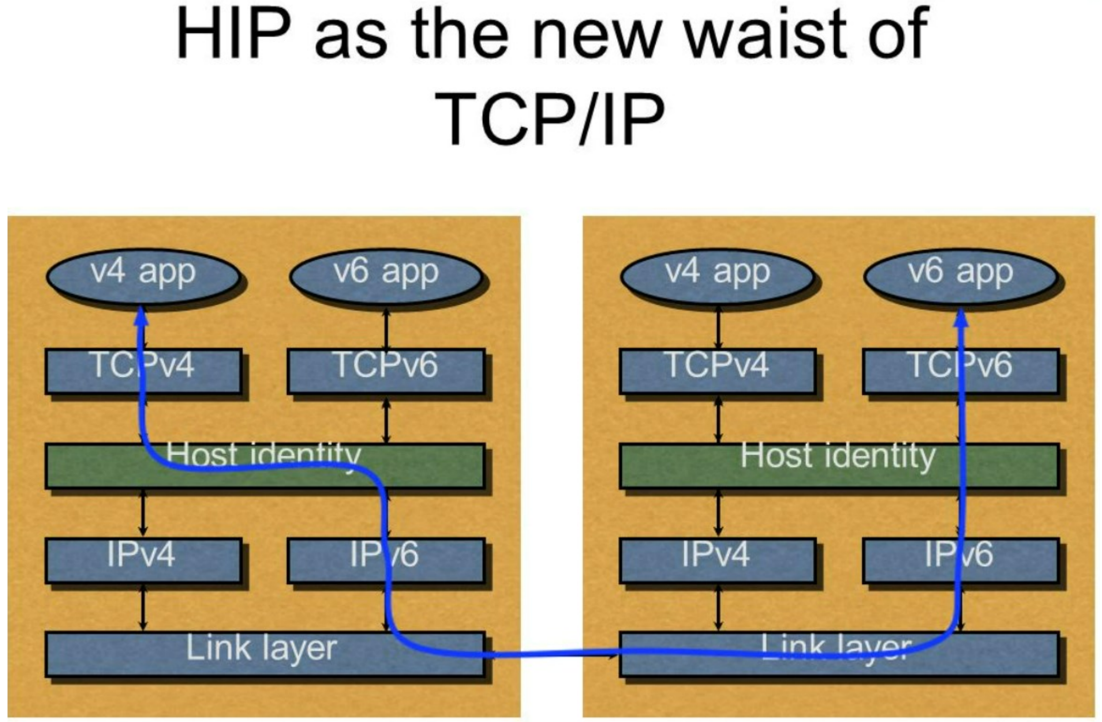


DS-Lite: IPv4 traffic is tunneled from a customer's network to a carried grade NAT in the provider network sharing an IPv4 address with potentially many customers

DS-Lite: IPv4 traffic is tunneled from a customer's network to a carried grade NAT in the provider network sharing an IPv4 address with potentially many customers

Internet protocol extensions

Host Indentity Protocol



https://slideplayer.com/slide/6639918/
https://www.slideserve.com/wayde/host-identity-protocol-m2nm-sydney-17-october-2007-powerpoint-ppt-presentation

Host Identity Protocol
https://en.wikipedia.org/wiki/Host_Identity_Protocol

Host Identity Protocol (HIP) Architecture, RFC 4423
https://datatracker.ietf.org/doc/html/rfc4423

More extensions:

- **Identifier/Locator Network Protocol**
- **Locator/Identifier Separation Protocol**
- **Mobile IP (MIP)**
- …

... see further cases in further lectures.

```
1st rule of informatics:
            If it works, don't touch it!
```

Why not adopt iPv6?

Blockers to IPv6 Adoption:

- **Blocker 1: Why should we fix something that is not broken?**
- **Blocker 2: We have no budget for IPv6**
- **Blocker 3: We lose the benefits of NAT44**

- **Overcoming Blockers: Why should we fix something that is not broken?**

https://labs.ripe.net/author/david_holder/blockers-to-ipv6-adoption/

Future

?

Complex Addressing in IPv6
RFC 8135 (M. Danielson, M. Nilsson 2017)

Complex Addressing in IPv6

Abstract

The 128-bit length of IPv6 addresses (RFC 4291) allows for new and innovative address schemes that can adapt to the challenges of today's complex network world. It also allows for new and improved security measures and supports advanced cloud computing challenges.

Table of Contents

Recommended literature

Erik Nygren, Akamai: 10 Years Since World IPv6 Launch, June 06, 2022
https://www.akamai.com/blog/trends/10-years-since-world-ipv6-launch

IPv6 will be the faster option
Dani Grant | dani@cloudflare.com | @thedanigrant
https://www.ripe.net/participate/meetings/regional-meetings/cloudflare-and-ipv6-dani-grant.pdf

Legacy support on IPv6-only infra
https://engineering.fb.com/2017/01/17/production-engineering/legacy-support-on-ipv6-only-infra/

Spamhaus IPv6 Blocklists Strategy Statement
https://www.spamhaus.org/organization/statement/012/spamhaus-ipv6-blocklists-strategy-statement

ICANN's IPv6 Initiative
https://www.icann.org/resources/pages/ipv6-initiative-2017-02-28-en

Operational Security Considerations for IPv6 Networks
RFC 9099, Informational (Aug 2021)
https://datatracker.ietf.org/doc/rfc9099/

RFC Index
https://www.rfc-editor.org/rfc-index.html

IETF Datatracker - Document Search
https://datatracker.ietf.org/doc/search?

Tutorials

Khan Academy: Computing – Computers and the Internet
https://www.khanacademy.org/computing/computers-and-internet

Tutorials Point:
Introduction to Internet, WWW and Web Browsers
https://www.tutorialspoint.com/computer_concepts/computer_concepts_introduction_to_internet_www_web_browsers.htm
Computer - Networking
https://www.tutorialspoint.com/computer_fundamentals/computer_networking.htm
Computer - Internet and Intranet
https://www.tutorialspoint.com/computer_fundamentals/computer_internet_intranet.htm
Internet Technologies Tutorial
https://www.tutorialspoint.com/internet_technologies/index.htm
IPv6 Tutorial
https://www.tutorialspoint.com/ipv6/index.htm

6DEPLOY-2 Tutorials
http://www.6deploy.eu/index.php?page=tutorials2

Eric Vyncke: Advanced IPv6 Security Threats and Mitigation
https://www.ciscolive.com/c/dam/r/ciscolive/emea/docs/2020/pdf/BRKSEC-3200.pdf

Presentations

Rick Graziani:
Help! I need to learn IPv6 - Rick Graziani
https://studylib.net/doc/10184625/help--i-need-to-learn-ipv6---rick-graziani
7: SLAAC (SLAAC Presentation)
https://studylib.net/doc/15481907/slaac-presentation
Intermediate IPv6 SLAAC and DHCPv6
https://studylib.net/doc/9400570/intermediate-ipv6-slaac-and-dhcpv6
8: DHCPv6 (Dynamic Host Configuration Protocol for IPv6)
https://studylib.net/doc/9264174/slide-1---cabrillo-college
IPv6, Wireless, and Security
https://studylib.net/doc/15481767/ipv6--wireless--and-security-cs-1-rick-graziani-cabrillo-...
…
https://studylib.net/search/Graziani/8

Cisco: IPv6 Addressing and Basic Connectivity Configuration Guide, Cisco IOS XE Release 3S

https://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipv6_basic/configuration/xe-3s/ip6b-xe-3s-book/ip6-add-basic-conn-xe.html

IBM: z/OS Communications Server –Internet Protocol Version 6
https://www.ibm.com/docs/en/zos/2.3.0?topic=guide-internet-protocol-version-6

Hurricane Electric Internet Services: IPv6 Certifications
Free IPv6 Certifications
https://ipv6.he.net/certification/

Data and Statistics

https://www.internetworldstats.com

https://radar.cloudflare.com/

https://www.akamai.com/internet-station/traffic-map

https://www.vyncke.org/ipv6status/
https://www.vyncke.org/ipv6status/project.php

https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/index.html#rirdelegs
https://www-public.imtbs-tsp.eu/~maigron/RIR_Stats/RIR_Delegations/Delegations/IPv6/HU.html

https://engineering.fb.com/2018/06/06/connectivity/how-ipv6-deployment-is-growing-in-u-s-and-other-countries/#:~:text=IPv6%20has%20become%20the%20dominant,deployment%20and%20some%20much%20more.
https://www.facebook.com/ipv6/?tab=ipv6_country
https://engineering.fb.com/2017/01/17/production-engineering/legacy-support-on-ipv6-only-infra/

IPv6 Security

https://www.cs.columbia.edu/~smb/papers/v6worms.pdf

https://www.internetsociety.org/deploy360/ipv6/security/

https://www.allot.com/blog/ipv6_ddos_attack_vulnerability/#

https://www.siliconrepublic.com/machines/ipv6-iot-ddos-mobile-world-congress

IPv6 Privacy

https://www.theregister.com/2022/03/22/legacy_ipv6_addressing_standard_enables/

https://www.sidn.nl/en/news-and-blogs/privacy-aspects-of-ipv6

IPv6 history

https://www.ripe.net/support/training/ripe-ncc-educa/presentations/bob-hinden-ipv6-pastpresentfuture.pdf

Quizes

https://quizizz.com/admin/quiz/5e173a2ed7e627001b129301/cisco-ip-addressing-ipv4-vs-ipv6

https://ipcisco.com/ipv6-quiz-1-n2685ss/
https://ipcisco.com/ipv6-quiz-2-n584eds/
https://ipcisco.com/ipv6-quiz-3-nsdf745/
https://ipcisco.com/ipv6-quiz-4-ndfg475/
https://ipcisco.com/ipv6-quiz-5-n475dfe/

Useful websites

IANA
https://www.iana.org/
Number Resources
https://www.iana.org/numbers
Internet Protocol Version 6 Address Space
https://www.iana.org/assignments/ipv6-address-space/ipv6-address-space.xhtml
IANA IPv6 Special-Purpose Address Registry
https://www.iana.org/assignments/iana-ipv6-special-registry/iana-ipv6-special-registry.xhtml

RFC Index
https://www.rfc-editor.org/rfc-index.html

Contents

Quiz sample

Which is not an IPv6 address?

A. add:cafe:bad:code:be:dead::beef
B. ::
C. ed:bed:be:bad::192.168.0.123
D. fc80:0002:ec01:ed02:fg03::0001

What is the default route address of IPv6?

A. 0:0:0:0:0:0:0:1/128
B. ::/0
C. ::/128
D. 0:0:0:0:0:0:0:1/0

Which is a loopback address of these?

A. 127.0.0.1
B. 127.1.2.8
C. ::0
D. ::1

Which is true?

A. IPv6 header has a fixed size and not extensible.
B. IPv6 header is simpler than IPv4 Header.
C. An IPv6 header may be shorter than an IPv4 header.
D. An IPv4 header may be shorter than an IPv6 header.

Which is false?

A. IPv4 and IPv6 is the two halves of the same protocol.
B. IPv6 stack should be compatible with IPv4 protocol.
C. NAT is not possible with IPv6.
D. NPT66 is stateless.

Which is false?

A. A carrier-grade NAT user is not on the Internet.
B. P2P applications typically do not work with NAT.
C. IPsec tunnel can be established via NAT.
D. There is not any unused and unallocated /24 range.

Which is false?

1. It is possible to assign one unicast address to multiple intrefaces.
2. It is possible to assign one unicast address to the multiple interfaces of multiple hosts.
3. An anycast address must not have assigned multiple interfaces of the same host.
4. To a single interface can be assigned several global and local unicast, anycast and multicast addresses.

Which is IPv6/IPv4 'almost' agnostic protocol? [See also https://www.ibm.com/docs/en/zos/2.4.0?topic=tutorials-how-does-ipv6-affect-tls]

A. TLS
B. HTTP
C. ICMP
D. DHCP

Command with correct IP-address syntax:

E. ping 0000000177.000.0.00001
F. ping 0000::1
G. ping 00000::1
H. ping 1234567890

Command with incorrect IP-address syntax:

I. ping 0000000177.000.0.00001
J. ping 0000::1
K. ping 00000::1
L. ping 1234567890

Which is false?

A. Every IPv6 address has a specific scope.
B. The IPv6 unicast loopback address, ::1, is treated as having link-local scope within an imaginary link to which a virtual "loopback interface" is attached.
C. Link-local is a smaller scope than global.
D. Two scopes of different size may cover the exact same region of topology.

What is the acronym of IP?

A. Internet Protocol
B. Initial Point
C. Intellectual Property
D. Internal Protocol

Which country's ISO-3166 country code is IP?

A. Islamic Parastate
B. Isle of Patagonia
C. Iguana
D. None of the above ones.

Comments

Interface ID configuration

- Static and manual configuration
- Autoconfiguration
  - SLAAC
    - Based on EUI-64 (Extended Interface Identifier)
    - Pseudorandom (privacy) address
      - according to RFC 4941
      - according to RFC 7217
      - proprietary/unique or draft status protocol
  - SLAAC + DHCPv6
- Dynamically assigned
  - by DHCP server (DHCPv6)
    - DHCPv6 according to RFC 3315 (obsoleted by RFC 8415)
    - DHCPv6 according to RFC 4941 (pseudorandom /'privacy'/)
    - proprietary/unique or draft status protocol
  - other solutions

Textual representation of scoped addresses

```
Ethernet adapter VMware Network Adapter VMnet1:
  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . :  fe80::5909:b773:e140:bfa5%7
  IPv4 Address. . . . . . . . . . . :  192.168.249.1
  Subnet Mask . . . . . . . . . . . :  255.255.255.0
  Default Gateway . . . . . . . . . :
  DNS Servers . . . . . . . . . . . :  fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1

Ethernet adapter VMware Network Adapter VMnet8:
  Connection-specific DNS Suffix  . :
  Link-local IPv6 Address . . . . . :  fe80::169:43b6:ea21:e578%10
  IPv4 Address. . . . . . . . . . . :  192.168.198.1
  Subnet Mask . . . . . . . . . . . :  255.255.255.0
```

"RFC 4007 (IPv6 Scoped Address Architecture) introduces the percent sign ("%") as a separator between an IPv6 address literal and a zone_id . It describes that a zone identifier can be numeric or a string."
https://labs.ripe.net/author/philip_homburg/whats-the-deal-with-ipv6-link-local-addresses/

DHCPv4 versus DHCPv6

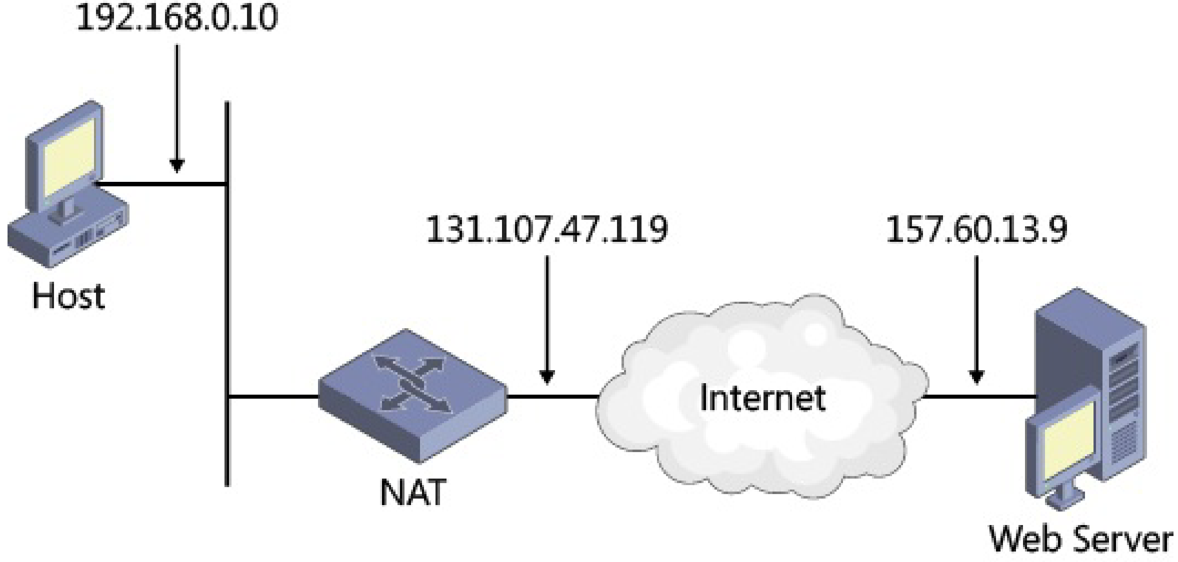
DHCPv6 IAID . . . . : 100683862
DHCPv6 Client DUID. . . . . : 00-01-00-01-21-D3-5C-13-74-46-A0-90-D2-A4

IAID = Identity Association Identifier
DUID = DHCP Unique Identifier

Definition of the UUID-Based DHCPv6 Unique Identifier (DUID-UUID)
RFC 6355 (Aug 2011)
"DUID-UUIDs are derived from the already-standardized Universally Unique IDentifier (UUID) format. DUID-UUID makes it possible for devices to use UUIDs to identify themselves to DHC servers and vice versa. UUIDs are globally unique and readily available on many systems, making them convenient identifiers to leverage within DHCP."
https://datatracker.ietf.org/doc/html/rfc6355

- "DHCPv4 uses the MAC address and an optional Client ID to identify the client for purposes of assigning an address. Each time the same client arrives on the network, it gets the same address, if possible."
- "DHCPv6 uses basically the same scheme, but makes the Client ID mandatory and imposes structure on it. The Client ID in DHCPv6 consists of two parts: a DHCP Unique Identifier (DUID) and an Identity Association Identifier (IAID). The DUID identifies the client system (rather than just an interface, as in DHCPv4), and the IAID identifies the interface on that system."
  – https://docs.oracle.com/cd/E19253-01/816-4554/clientid/index.html

NAT(44)



1.)
Destination address: 157.60.13.9
Source address: 192.168.0.10
Destination TCP port: 80
Source TCP port: 1025

2.)
Destination address: 157.60.13.9
Source address: 131.107.47.119
Destination TCP port: 80
Source TCP port: 5000

3.)
Destination address: 131.107.47.119
Source address: 157.60.13.9
Destination TCP port: 5000
Source TCP port: 80

4.)
Destination address: 192.168.0.10
Source address: 157.60.13.9
Destination TCP port: 1025
Source TCP port: 80

Understanding IPv6: Your Essential Guide to IPv6 on Windows Networks Third Edition by Joseph Davies (Author)

Thank you for your attention and we look forward to seeing you on further lectures!

Tibor K. Dravecz

Copyright