Secure64
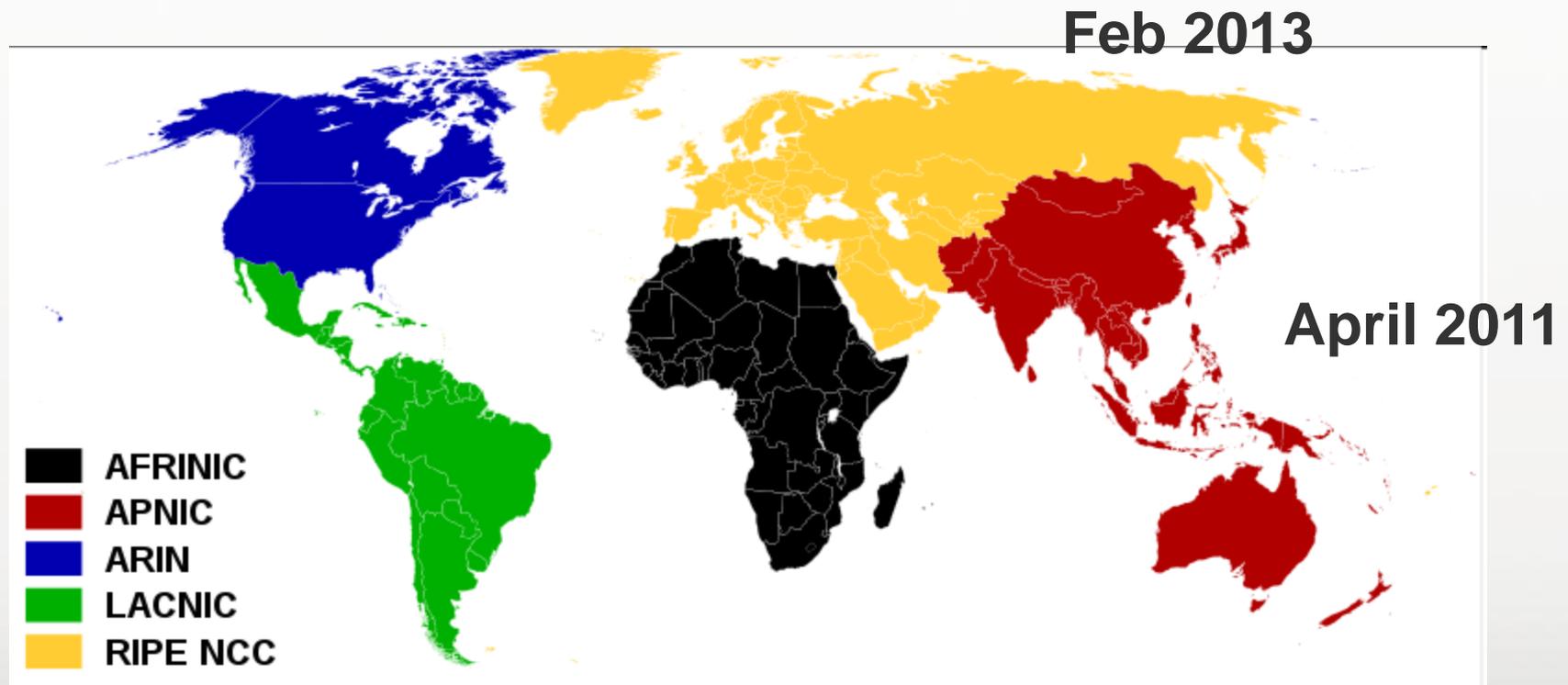
Use cases for DNS64/NAT64

SECURE64

Agenda / About Me

- VP of Sales and Customer Solutions at Secure64 Software Corp.

- Director and founder of the TXv6TF

- Personal blog at IPv4depletion.com

IPv4 Depletion

- Global IANA pool depleted in Feb-2011

Feb 2013

April 2011

- AFRINIC
- APNIC
- ARIN
- LACNIC
- RIPE NCC

IPv6 Deployment

- Deployment is minimal,
  - Texas Universities: 1/107
    - www.tamu.edu 2606:aa00:3:202::6
  - Texas Corporations: 0/30
    - softlayer.com 2607:f0d0:1000:11:1::4
  - Texas Counties: 2/233
    - www.angelinacounty.net. 2620:0:50e0:3::31
    - www.co.kerr.tx.us 2001:470:1f11:bcd:21e:c9ff:feaf:68c8

- But on the other hand,
  - Large content providers (Google, Yahoo!, etc) are committed to the world IPv6 launch day.
  - 25% of all DNS lookups have the potential to go over IPv6, mainly because of Godaddy
  - IPv6 compliant organizations reported peaks of 68% IPv6 traffic during the world IPv6 day in 2011.

About Secure64

Supporting IPv6 in DNS

Transition Mechanisms

Native/Dual Stack

Translate

Dual Stack

NAT64/DNS64

DOCSIS 3.0

IVI

3GPP

DNS

6to4

A+P

Teredo

6RD

LISP

DS-LITE

ISATAP

Tunnel v4 in v6
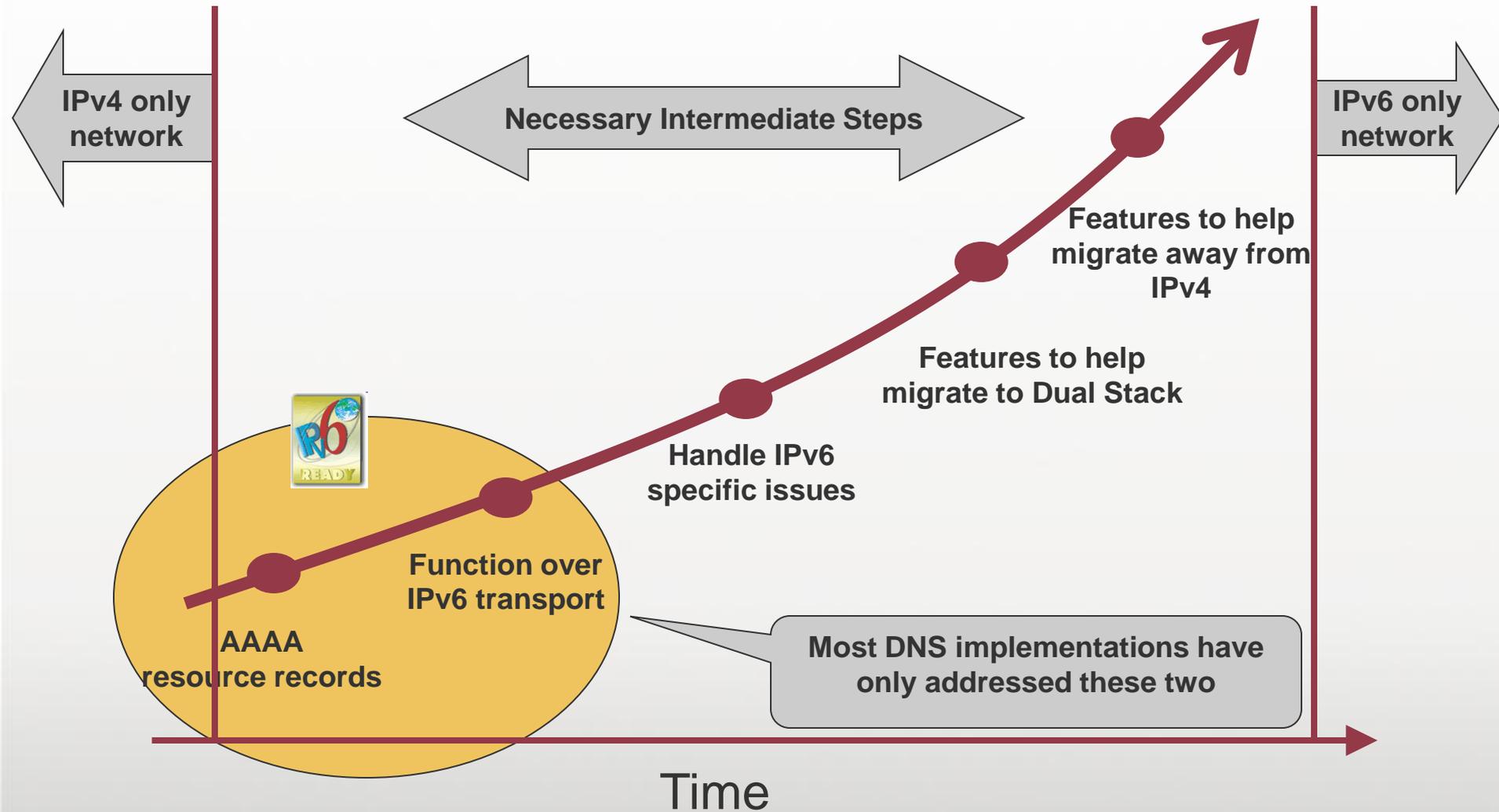
Tunnel v6 in v4
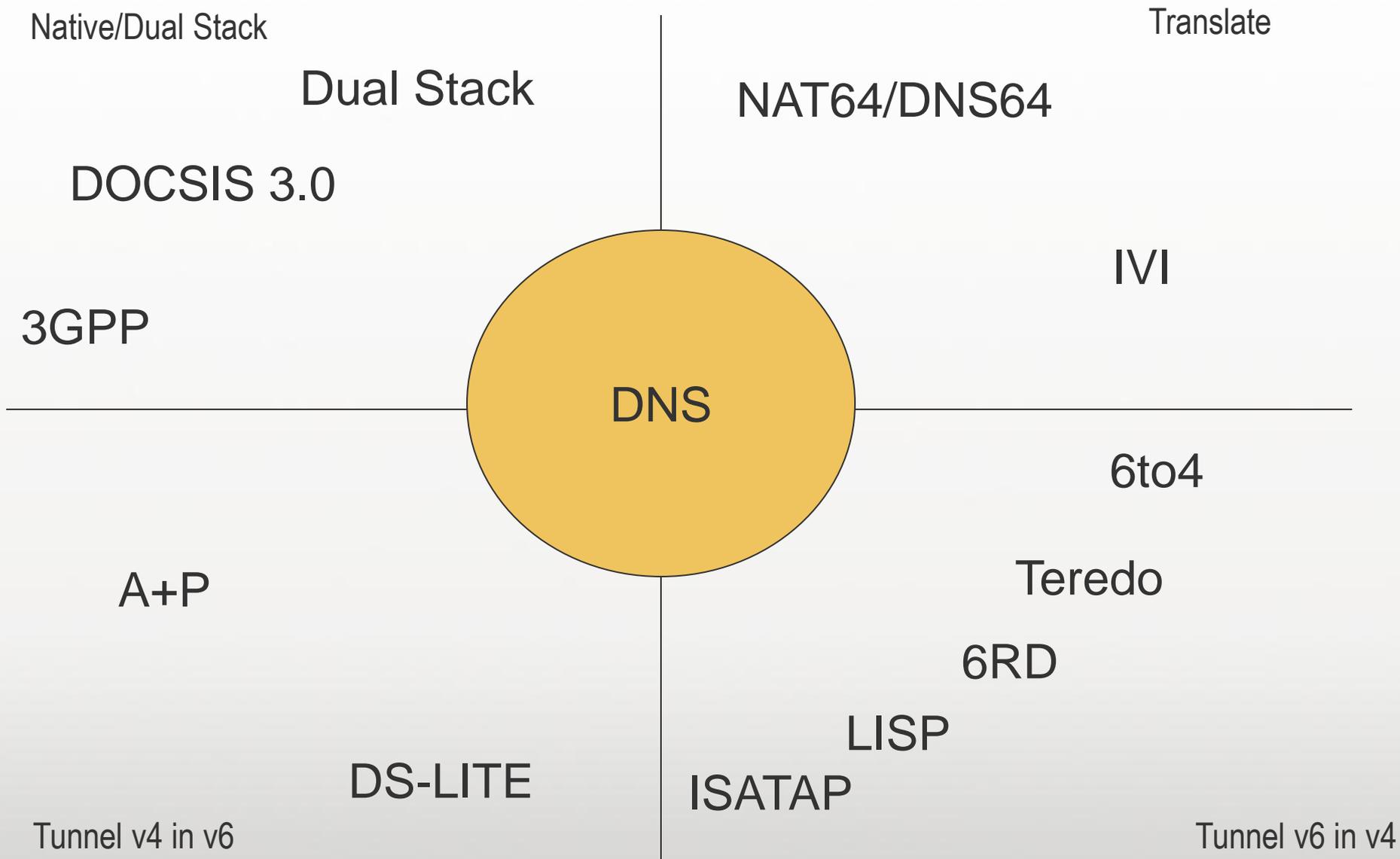
What is NAT64/DNS64

- Transition mechanism to IPv6
- Defined in RFC 6146 and RFC 6147

- Two components, DNS server and NAT gateway.
- Utilizes DNS to "lie" to the client, saying that everything has an AAAA record.
- Multiple use cases.

- Use Case I (Service Providers)
  - Allow IPv6 only clients to communicate with IPv4 only servers

- Use Case II (Content providers)
  - Enable IPv6 for IPv4 only servers without dual stacking each server.

- The reason we can do NAT64 is that the IPv6 address space is larger than the IPv4 address space.

IPv6 and DNS

- Some common misunderstandings and pitfalls about v6 and DNS:

- The network protocol (v4 or v6) is not linked to the record type (A or AAAA) that can be looked up.

- The network protocol (v4 or v6) used between the client and the recursive DNS is not related to the network protocol used between the recursive DNS and the authoritative DNS.

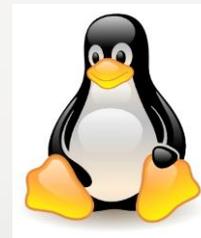- If there is an outgoing v6 interface, then the DNS system will start to use it.

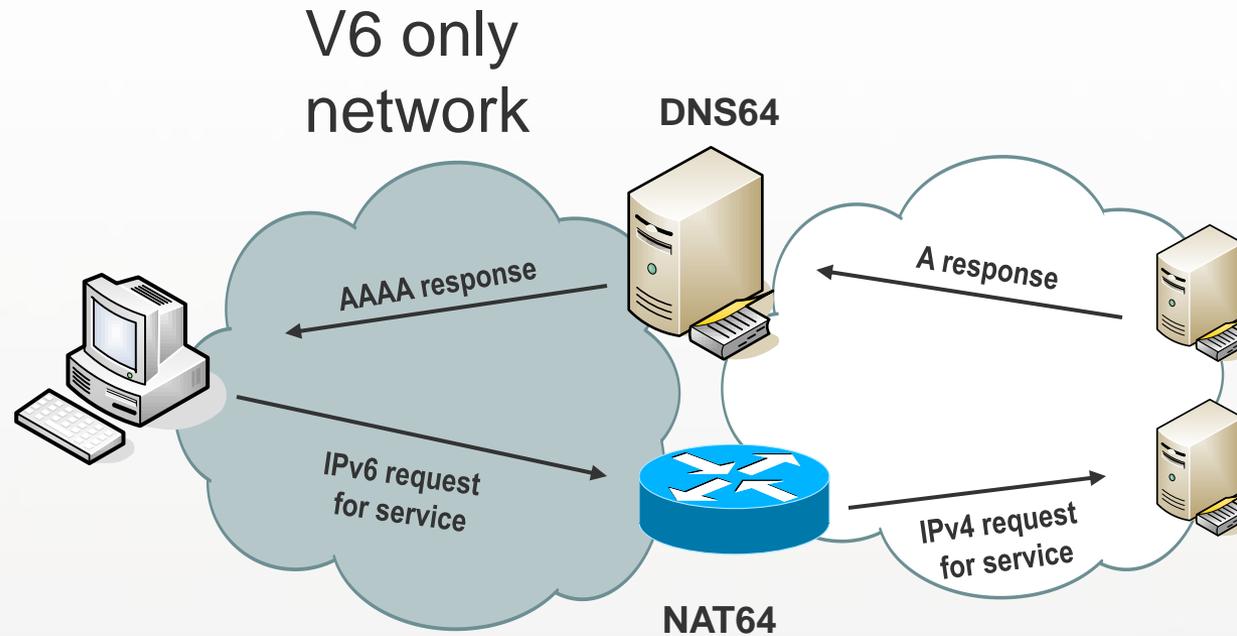# x2 load on DNS
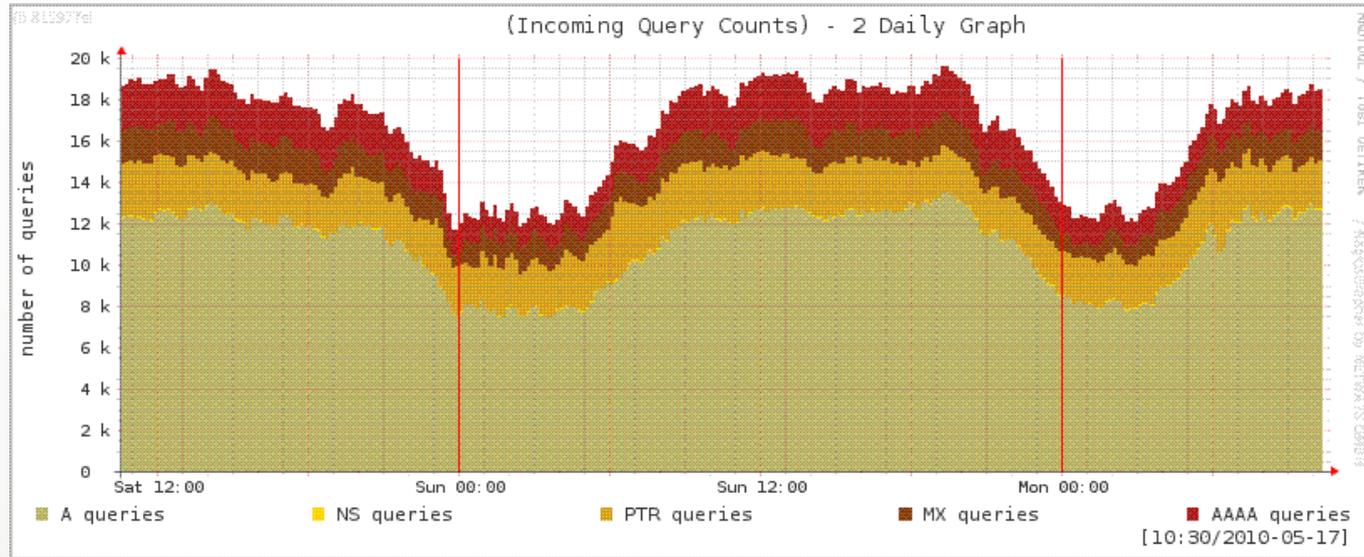
getaddrinfo()

A

AAAA

Dual Stack Issues

- Brokenness – A painful long timeout before the user reverts back to IPv4
  - Happy eyeballs implemented in Firefox and Chrome
  - Filter-AAAA implemented in some DNS servers
  - Does not appear to be a large problem. No complaints during world IPv6 day reported.

NAT64 / DNS64 Solution

V6 only
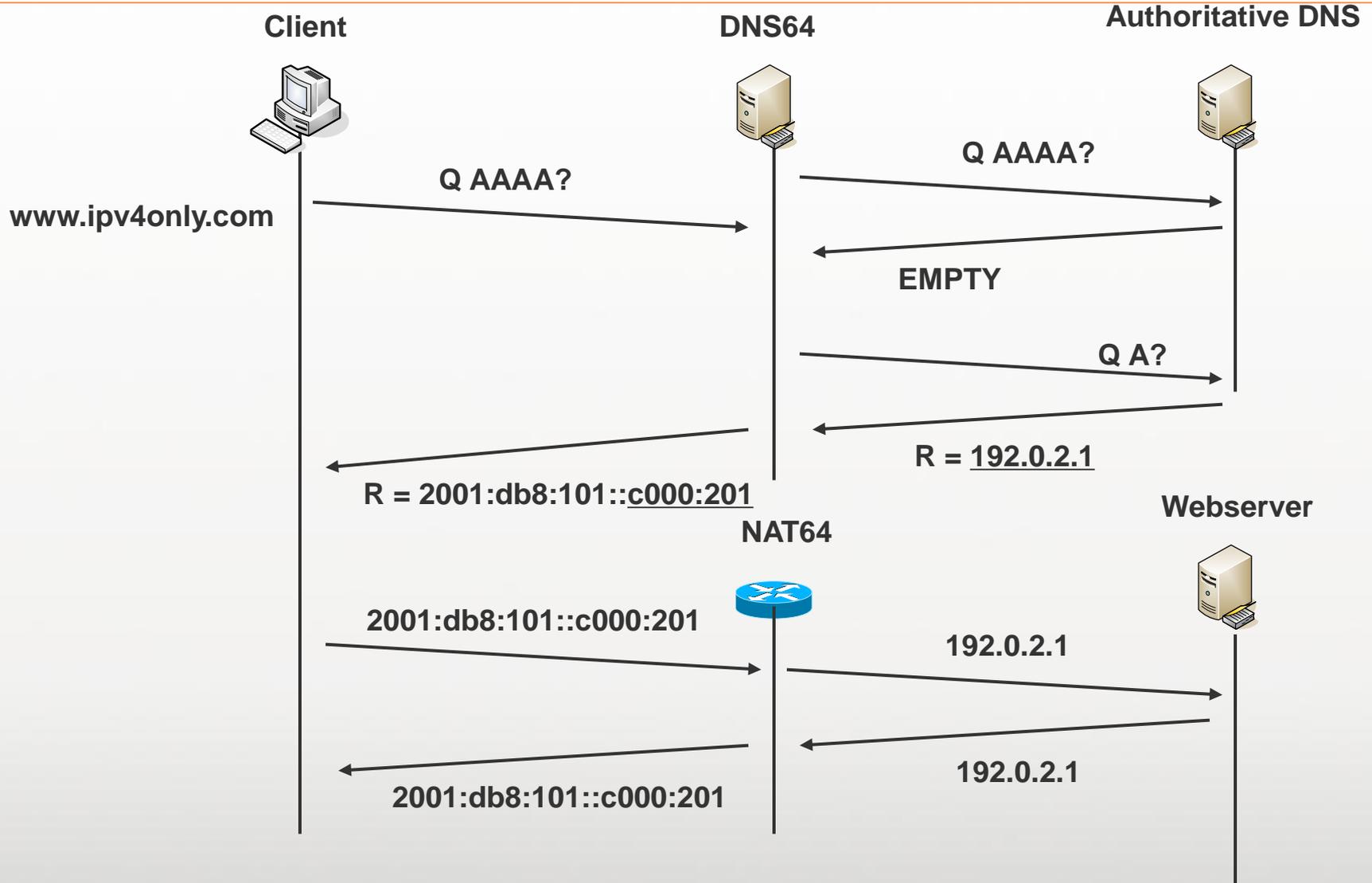network

DNS64

AAAA response

IPv6 request
for service

A response

IPv4 request
for service

NAT64

- Secure64 DNS cache:

```
dns64-prefix list:
     2001:db8:1::/96
     2001:db8:2::/96
     2001:db8:3::/96
```

NAT64 / DNS64 Under The Hood

Client   **DNS64**   **Authoritative DNS**

Q AAAA?

www.ipv4only.com   Q AAAA?

EMPTY

Q A?

R = 192.0.2.1

R = 2001:db8:101::c000:201

Webserver

NAT64

2001:db8:101::c000:201

192.0.2.1

2001:db8:101::c000:201

192.0.2.1

- Only viable approach if you don't have enough IPv4 addresses for dual stack

- DNS64/NAT64 does not break anything. But badly programmed applications/websites might not work.

- User experience with NAT64 is (almost) the same as NAT44 and better than NAT444

  - We had some issues with NAT44 back in the days too. But we managed to work around those
    - ▶ Passive FTP
    - ▶ IPSEC over UDP
    - ▶ Peer to Peer

NAT64/CGN and Logging

To the v4 internet

To the v6 internet

NAT64

v6

v4
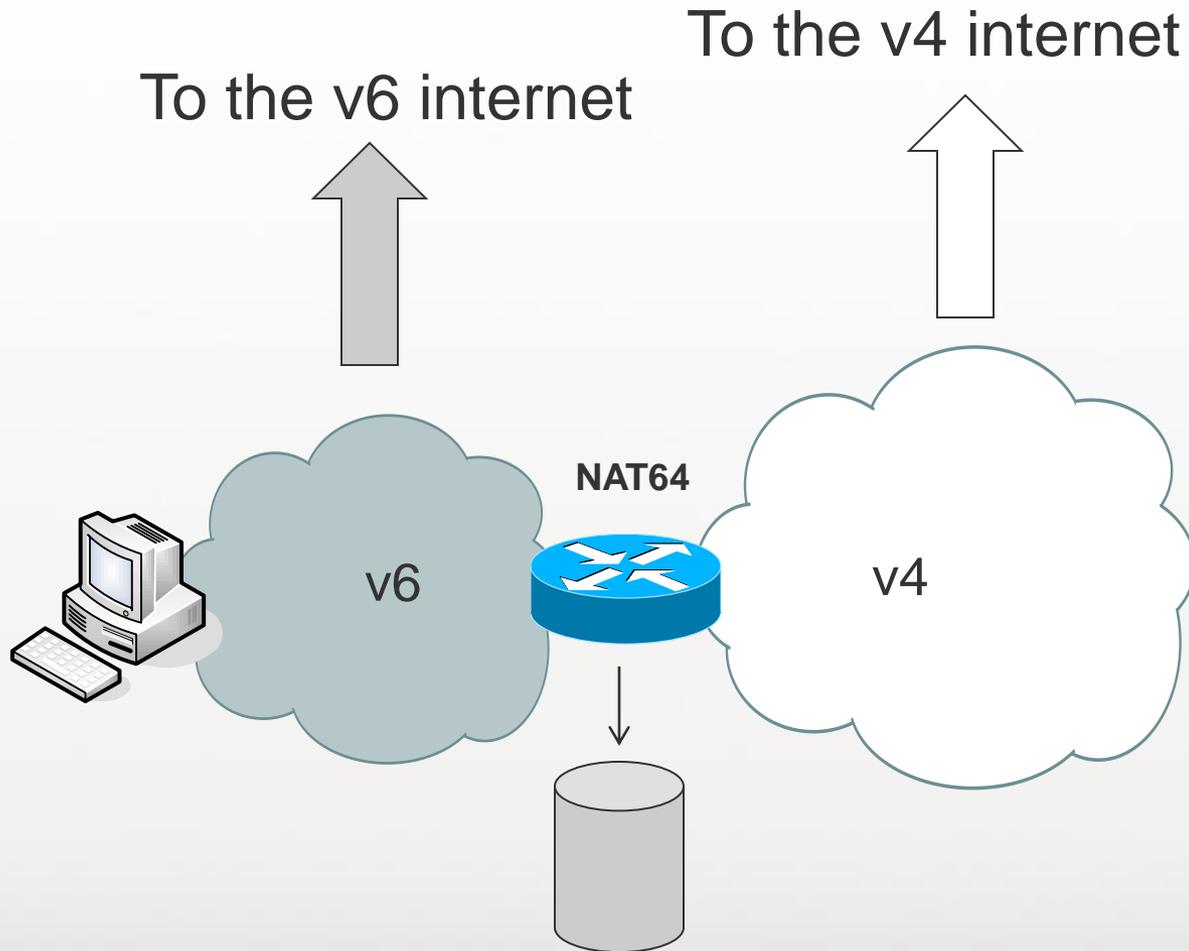
- Each user will create gigabytes of logs
- Only packets to the v4 internet have to be logged
- Maximizing the native v6 traffic minimizes the logs
- Make sure your DNS64 server returns all native domains without using PREF64 translation.

Logging - As a content provider, make sure to turn on v6 so that your visitors don't have get all their sessions logged.
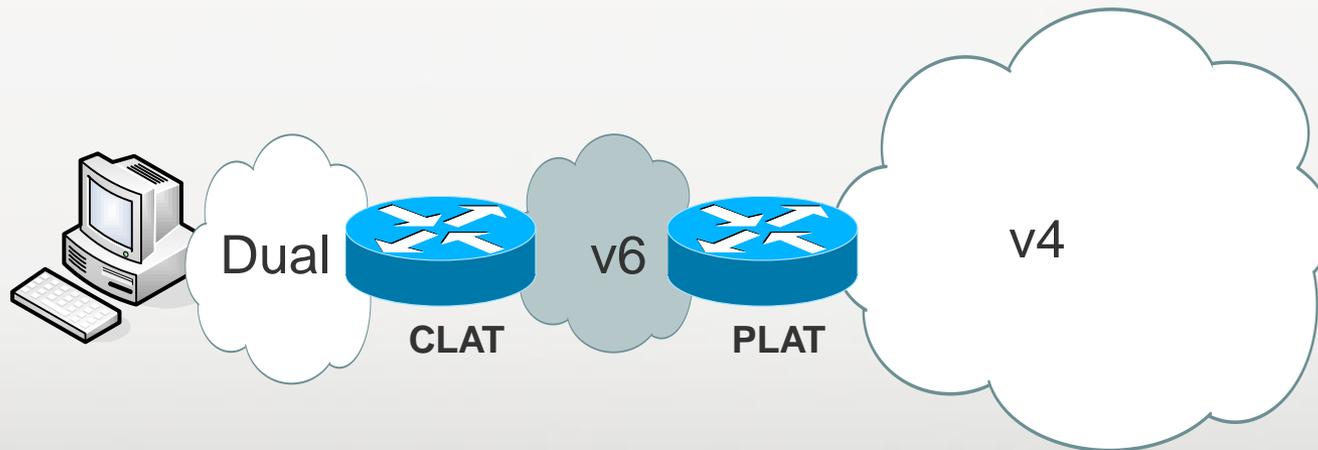
Use case 1.5
The Future of NAT64/DNS64

- How do we handle broken applications and websites?
- draft-ietf-behave-nat64-discovery-heuristic-07.txt
- draft-ietf-v6ops-464xlat-01

DNS64 Functionality Options

- Sticky clients
  - Make sure a client goes to the same IPv4 server during the session.

- Mixed deployments using views
  - The same DNS server must be able to handle different types of networks and different NAT64 gateways.

- Load balancing via DNS
  - Coarse load balancing of NAT64 gateways

- High availability
  - Take one NAT64 gateway out of rotation if it becomes unavailable.

Configuring for DNS64/NAT64

DNS is now a network technology:

- Who manages the DNS64?
- Do we need to teach our network operators Unix?
- How do we monitor the solution?

So let's manage it like we manage our other network devices:

```
[view@Secure64]#> enable sysadmin
[sysadmin@Secure64]#> route default 10.10.5.1
[sysadmin@Secure64]#> route default 2001:DB8:1:5::1
[sysadmin@Secure64]#> route sym
[sysadmin@Secure64]#> ifconfig eth1 10.10.5.2 255.255.255.0
[sysadmin@Secure64]#> ifconfig eth2 2001:DB8:1:5::2/64
[sysadmin@Secure64]#> activate
[sysadmin@Secure64]#> save
[sysadmin@Secure64]#> show config

[view@Secure64]#> enable cachednsadmin
[cachednsadmin@Secure64]# edit cache.conf
  interface: 10.10.5.2
    interface: 2001:DB8:1:5::2
    outgoing-interface: 10.10.5.2
    outgoing-interface: 2001:DB8:1:5::2
    access-control: 0.0.0.0/0 allow
    access-control: ::0/0 allow
  dns64-prefix: 64:ff9b::/96
<CTRL-X to save and exit>

[cachednsadmin@Secure64]# stop cachedns
[cachednsadmin@Secure64]# start cachedns
```
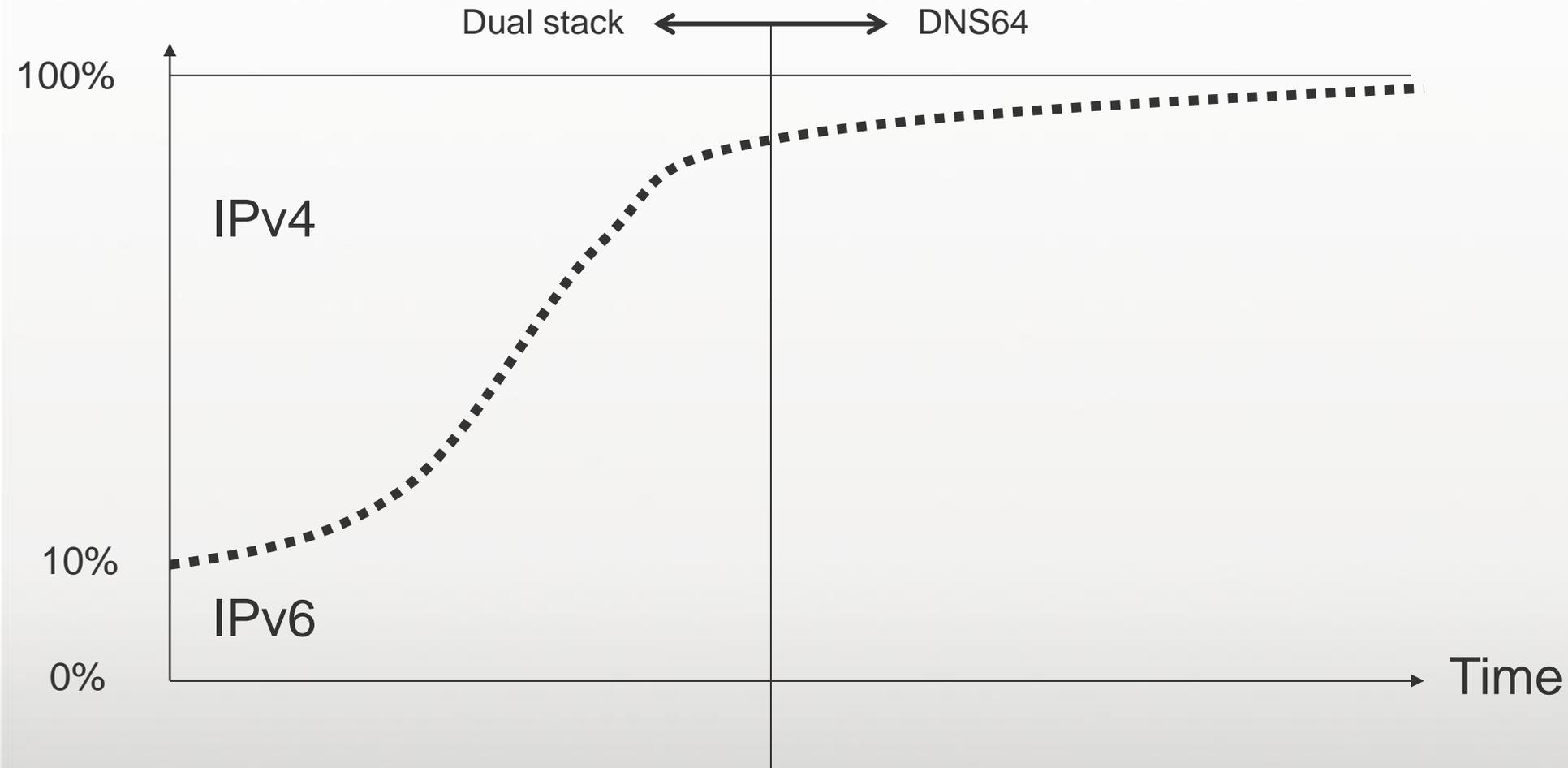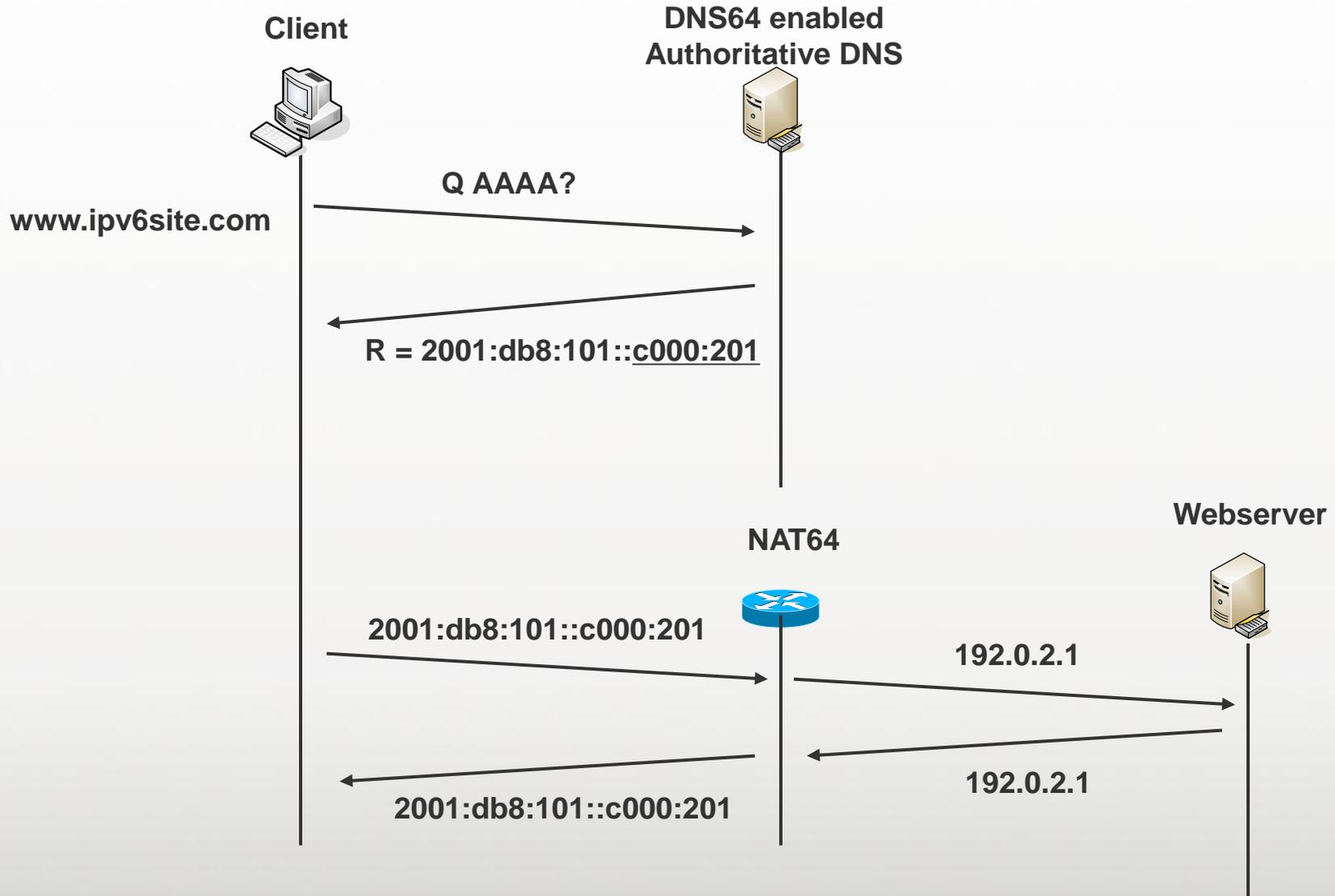
DNS64 Everybody Will Need It

Client

DNS64 enabled Authoritative DNS

Q AAAA?

www.ipv6site.com

R = 2001:db8:101::c000:201

NAT64

Webserver

2001:db8:101::c000:201

192.0.2.1

2001:db8:101::c000:201

192.0.2.1

Use case II,
NAT64 / DNS64 for Hosting Providers

SECURE 64

- Simple way of providing a large number of externally reachable servers with IPv6 connectivity

- Just add DNS records point to the NAT64 device
  - www.example.com A 192.0.2.1
  - www.example.com AAAA 2001:db8:101::c000:201

- Does not prevent IPv4 depletion

Conclusions

- The migration to IPv6 will increase the load on DNS servers
- Dual stack is the IETF recommended transition mechanism but not the only one. Consider alternatives such as DNS64/NAT64
- Some applications are broken and can't work over NAT64/DNS64
- There are many small pitfalls with DNS64/NAT64

- Additional resources
  - http://www.secure64.com/transition-to-ipv6
  - Stephan.lagerholm@secure64.com
  - Visit our booth here at the summit

Questions?