Migration to IPv6 using DNS64/NAT64

Stephan Lagerholm

SECURE64

Agenda / About me

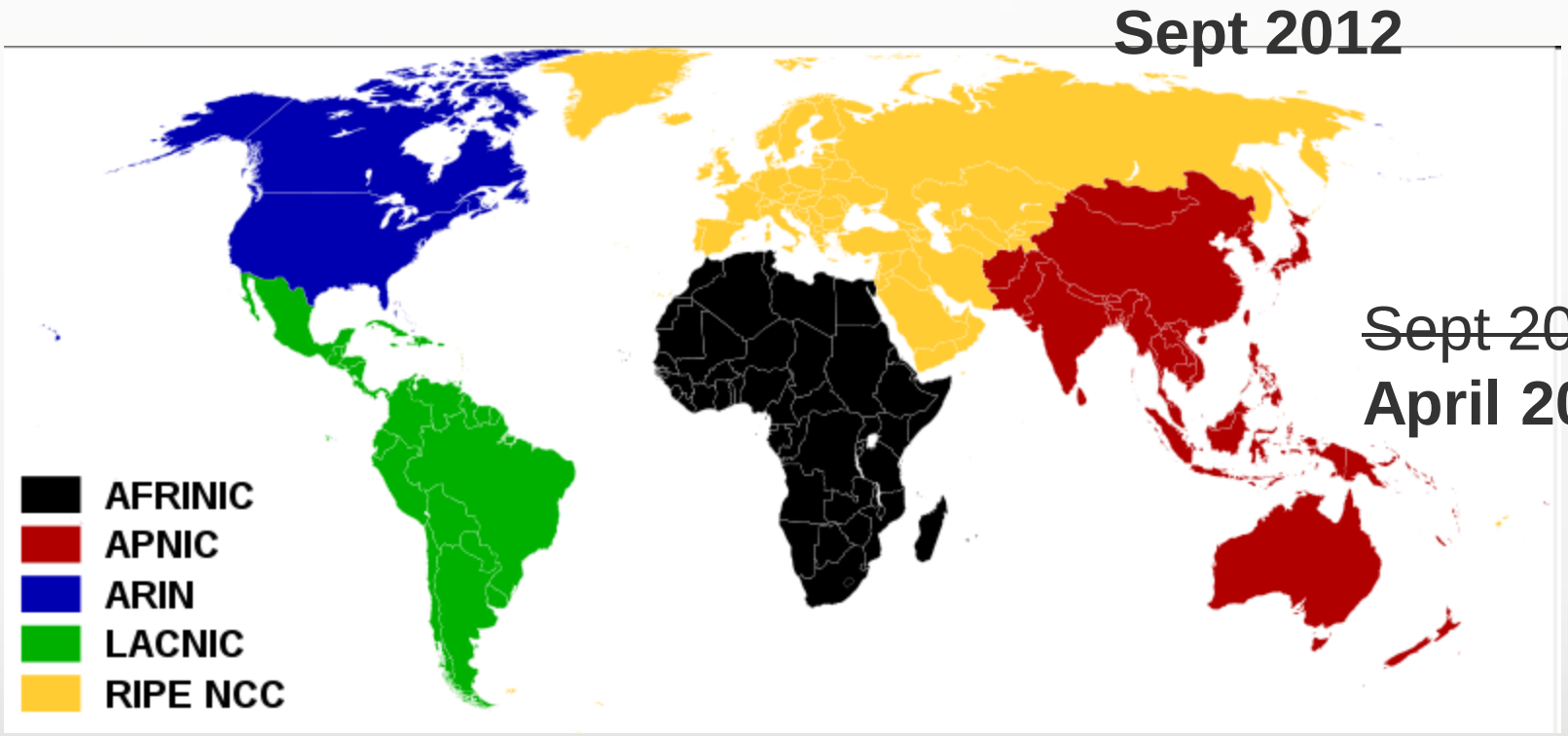
SECURE64

- DNS Architect at Secure64 Software Corp.
- Director and founder of the TXv6TF
- Personal blog at IPv4depletion.com

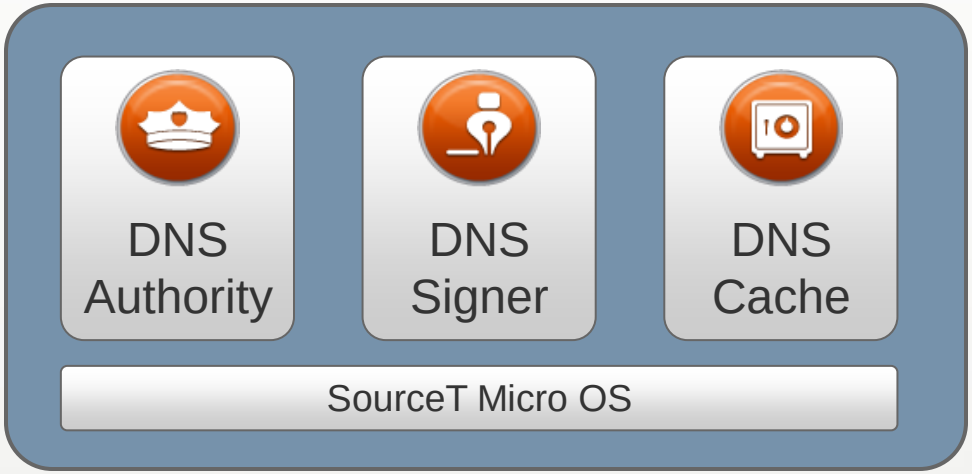
IPv4 depletion

SECURE64

- Global IANA pool depleted in Feb-2011

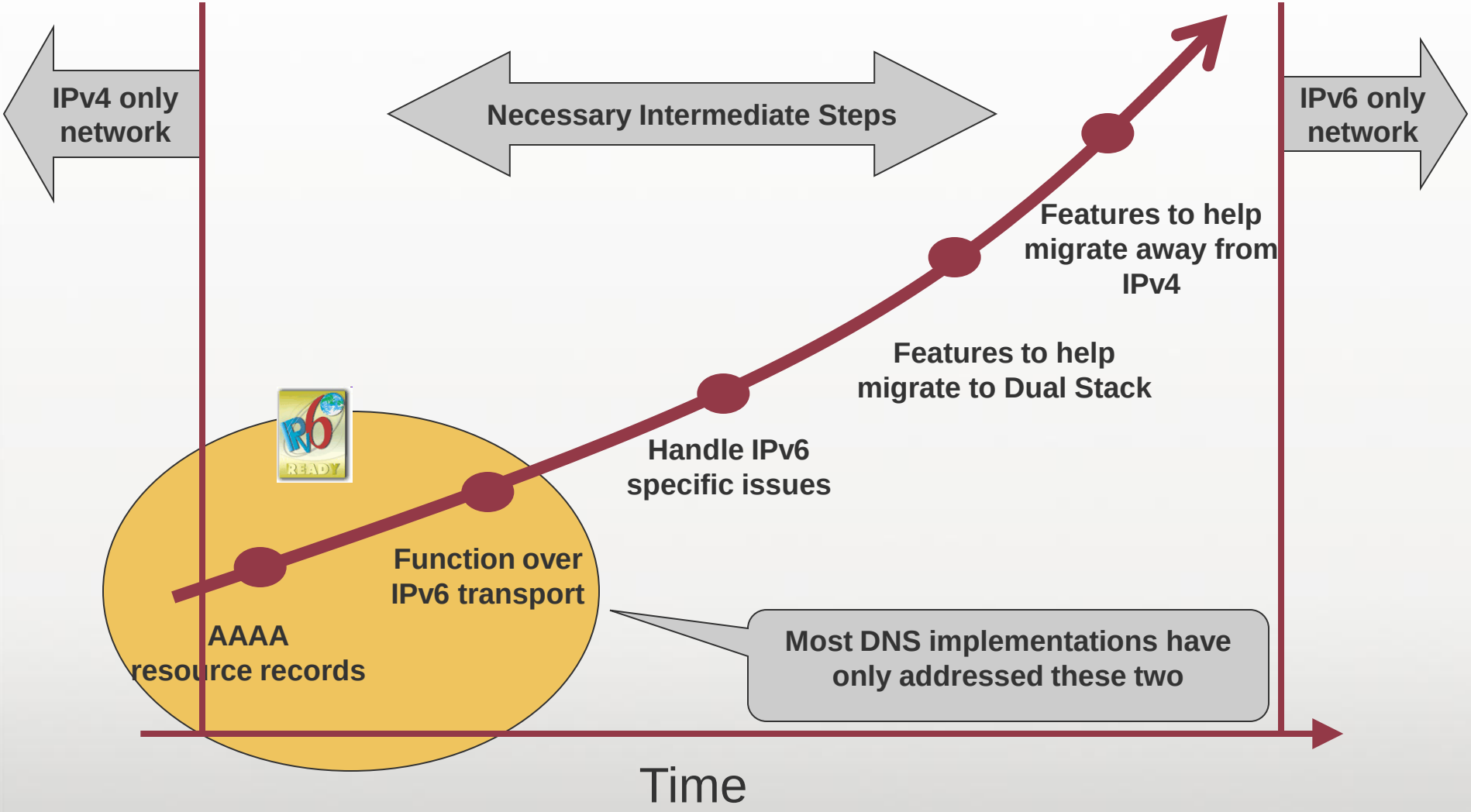


SECURE64



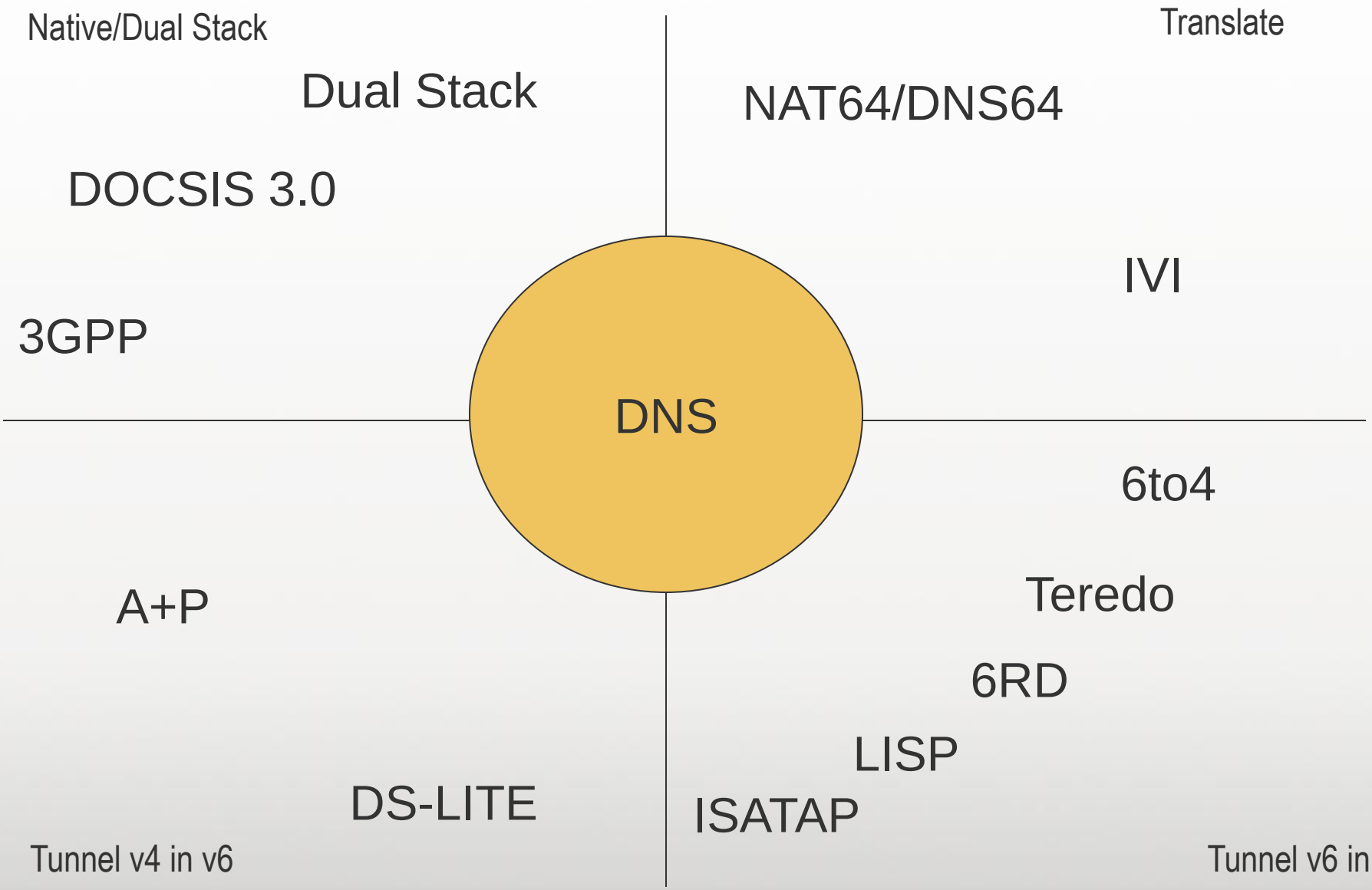
Supporting IPv6 in DNS

SECURE64



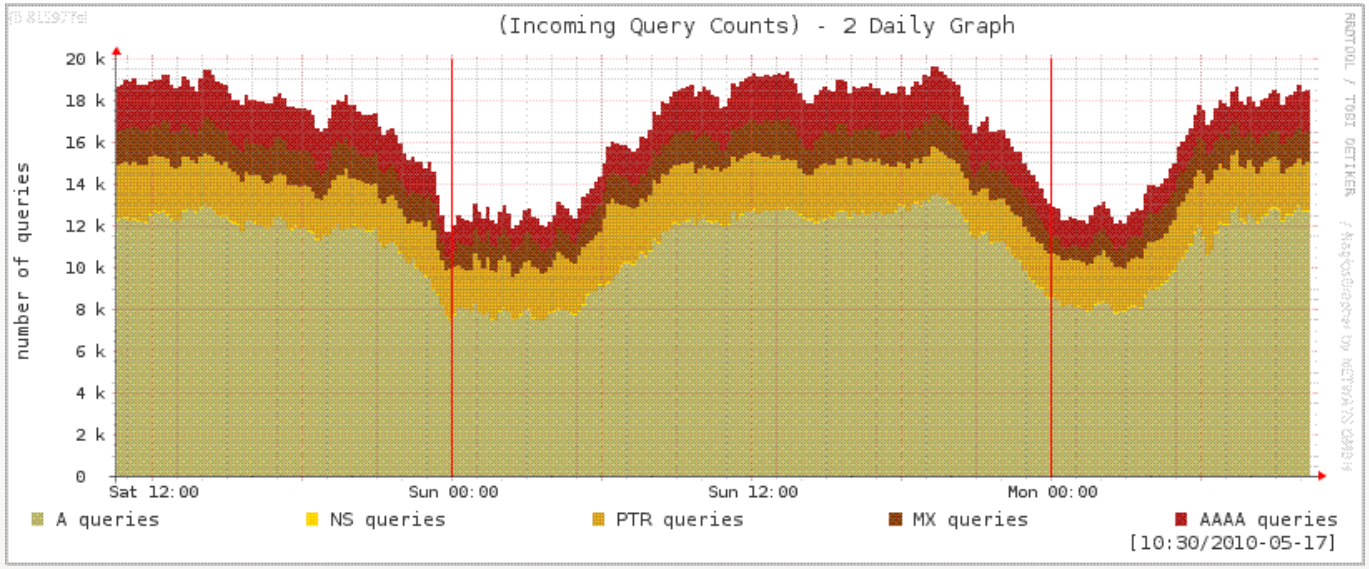
Transition Mechanisms

SECURE64



x2 load on DNS

SECURE64



getaddrinfo()

A

AAAA

IPv6 and DNS

SECURE64

- 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.

Secure64 IPv6 features

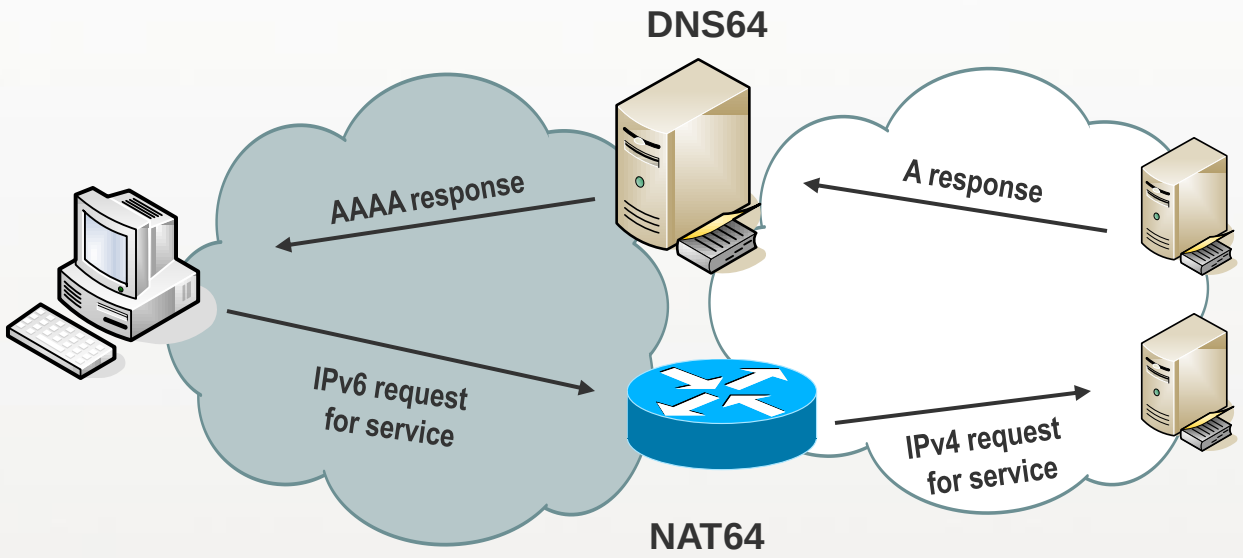
SECURE64

- Basic features:
  - IPv6 interfaces (autoconfig and statically configured)
  - Syslog, Ping6, NTP, dig, SNMP
  - Routing protocols with IPv6 support
  - Denial of Service protection over IPv6
- Advanced features:
  - DNS64
  - Disable AAAA on IPv4 transport (the Yahoo! hack)

NAT64 / DNS64 Solution

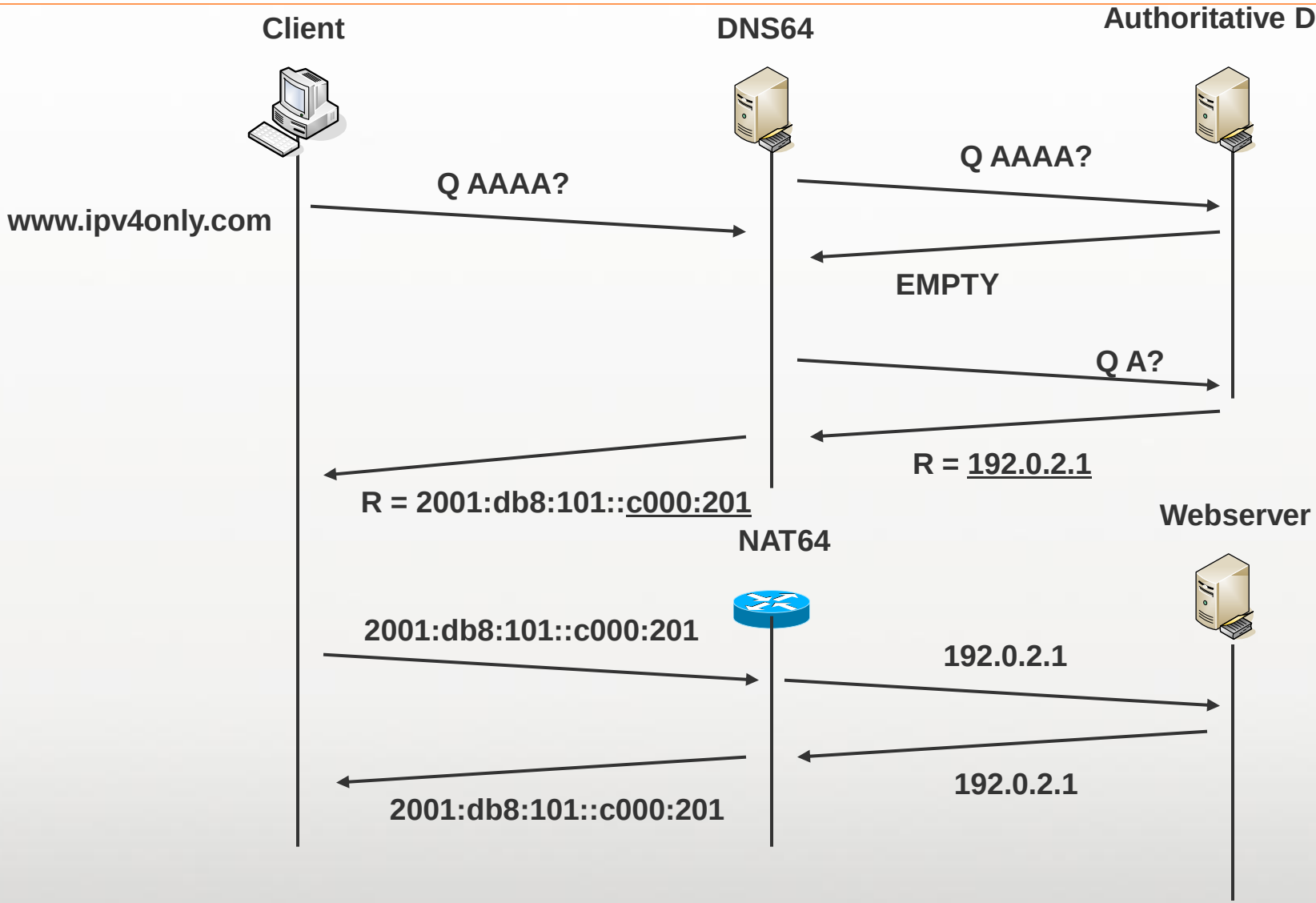
SECURE64

- RFC 6146/6147



NAT64 / DNS64 Under The Hood

SECURE64



Secure64 DNS configuraton

SECURE64

```
[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
```

Transition using translators (DNS64)

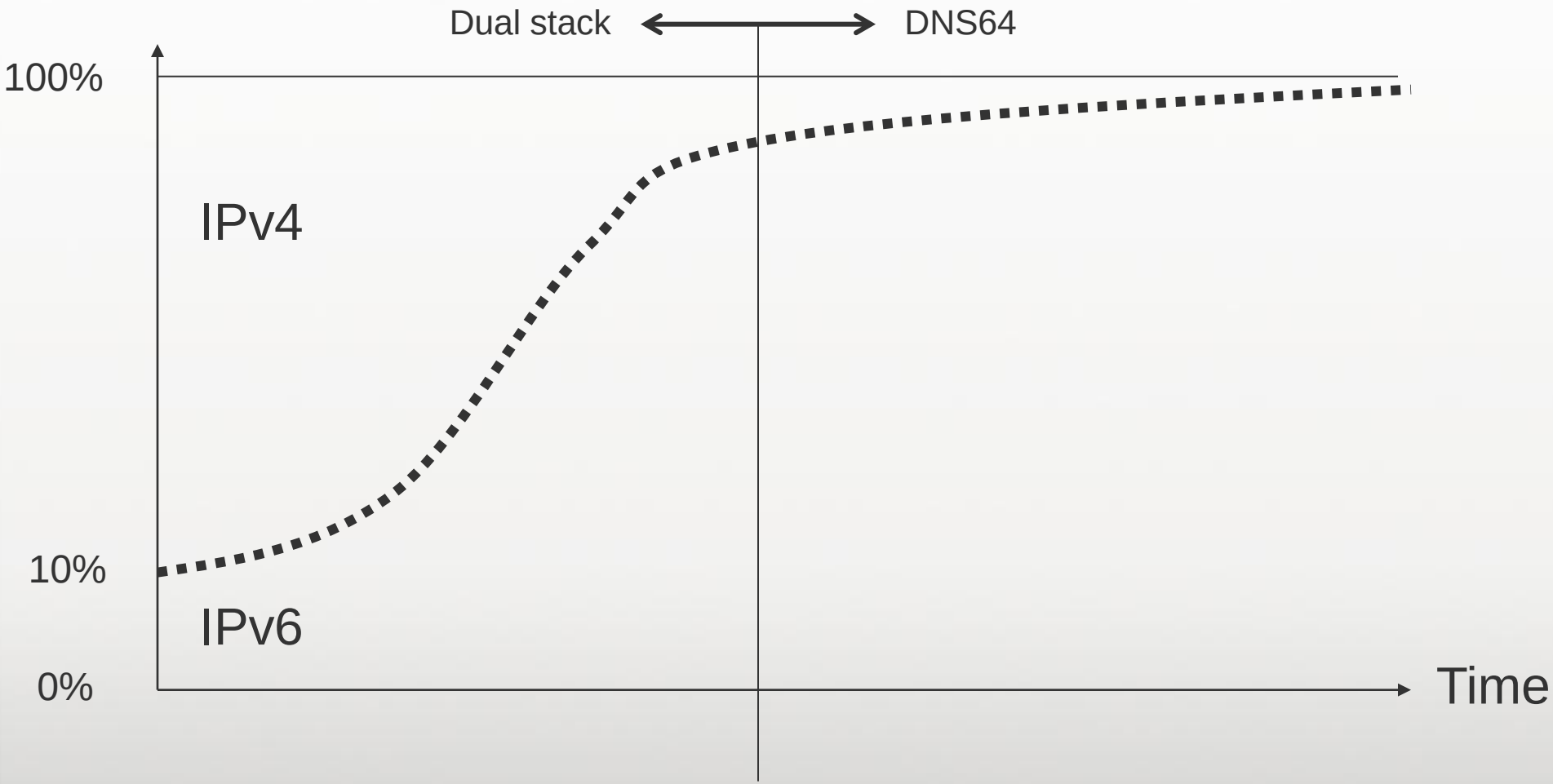
SECURE64

- Good approach if you don’t have enough IPv4 addresses for dual stack.
- IPv6-only network on the client side!
- User experience with NAT64 is (almost) the same as NAT44

- Stuff that’s broken doesn’t work.
- Only one network to maintain.

DNS64 everybody will need it

SECURE64



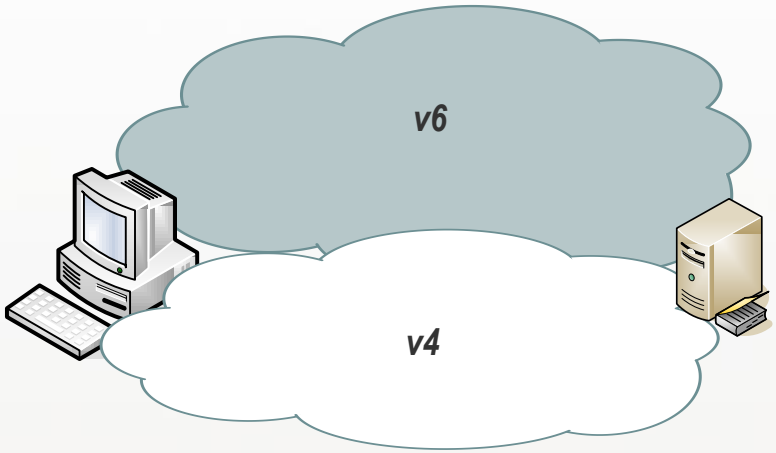
Additional DNS64 functionality

SECURE64

- *Sticky clients*
  - *You don't want a client to change from one NAT64 gateway to another during a session*
- *Mixed deployments using views*
  - *Any combination of Dual stack, IPv4 only, IPv6 only*
- *Load balancing via DNS*
  - *Multiple DNS64 prefixes*
- *High availability*
  - *Provision multiple DNS servers to the clients*
  - *How can we take a NAT64 out of rotation?*

HTTP problem in details

SECURE64



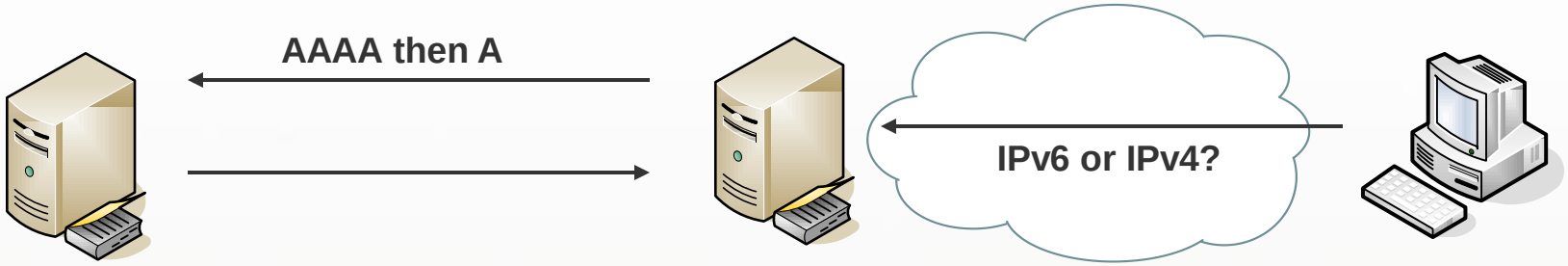
Today some content providers are not giving out AAAA unless you are on their white list because it might break 0.078% of IPv4 clients = could be millions of users and millions in revenue

Content providers DNS decides if A or AAAA or both

- There are problems when client IPv6 connection is broken
  - Extreme slowdown as client retries AAAA and then A lookups
- Estimated 0.078% of clients have this problem
  - Some older Opera browsers, some older Apple OSes, etc.
  - Amounts to millions of users for some large content providers like Google, Yahoo, etc.
- This is a HTTP problem, not applicable for other protocols such as DNS and SMTP.

One Proposed Solution Using DNS

SECURE64



- Caching side (ISP, consumer of content)
  - If query came in over IPv4, respond negatively to the AAAA request and wait for the A request
- Side effects:
  - Breaks DNSSEC
  - Turns off IPv6 for clients that can only do DNS queries over IPv4 (ie Windows XP)
- Future feature? Filter A over IPv6

Testing IPv6

SECURE64

- Useful Open Source Tools
  - ISIC6
    - Stack Integrity Checker
    - http://isic.sourceforge.net/
  - Resperf/dnsperf/dig
    - All work over Ipv6
  - Scapy
    - Packet Manipulation
    - http://www.secdev.org/projects/scapy/
  - THC
    - “The Hackers Choice” attack tools.
    - http://thc.org/thc-ipv6/

Questions?