IPv6 and DNS

Secure64

SECURE64

About me

SECURE64

- Stephan Lagerholm
- Director and Founder of TXv6TF.
- Secure64 Software Corp. Sponsor of the event.

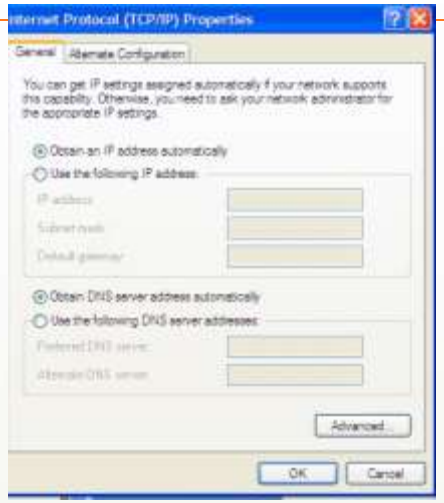
- Agenda:
- DNS and IPv6 basics
- DNS64 (RFC 6147)
- 464XLAT (RFC 6877)
- Heuristic discovery of DNS64 prefix (RFC 7050)
- Reverse Delegation and IPv6 (draft-howard-isp-ip6rdns-06)
- IPv6 and small packets
- Denial of Service attacks over IPv6 (a future look into what will come)

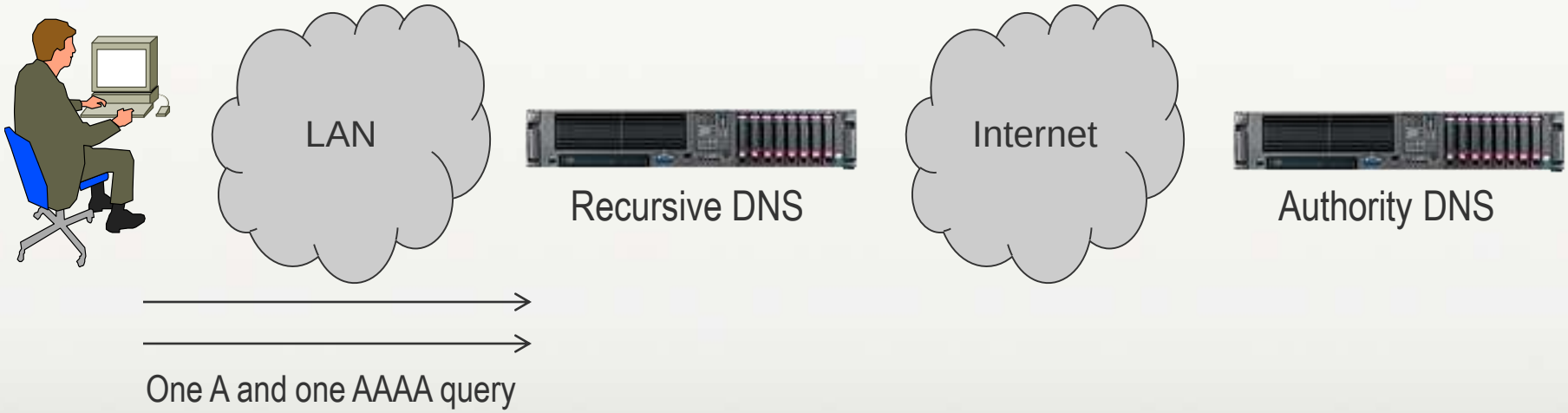
Before we begin as always…

SECURE64

- Deployment is minimal,
  - Texas Universities: 4/107 (4/107 , 1/107)
    - Texas AM
    - Sam Houston State University
    - University of Houston
    - University of Texas of the Permian Basin
  - Texas Corporations: 3/30 (2/30, 0/30)
    - AT&T
    - Texas Instrument
    - Baker Hughes
  - Texas Counties: 3/233 (1/233, 2/233)
    - Brewster, Kerr and Angelina county.

DNS and IPv6





- Client prefers IPv6 over IPv4
- Twice the load on the DNS

History of DNS and IPv6

- Some attempts did not work that very well:
- A6 records (use AAAA instead)
- Ip6.int (use ip6.arpa instead)
- NAT-PT (use NAT64 instead)

Independent queries (default config)

- A recursive DNS server will typically favor the fastest responding server based on RTT

Filter-AAAA-on-v4-transport

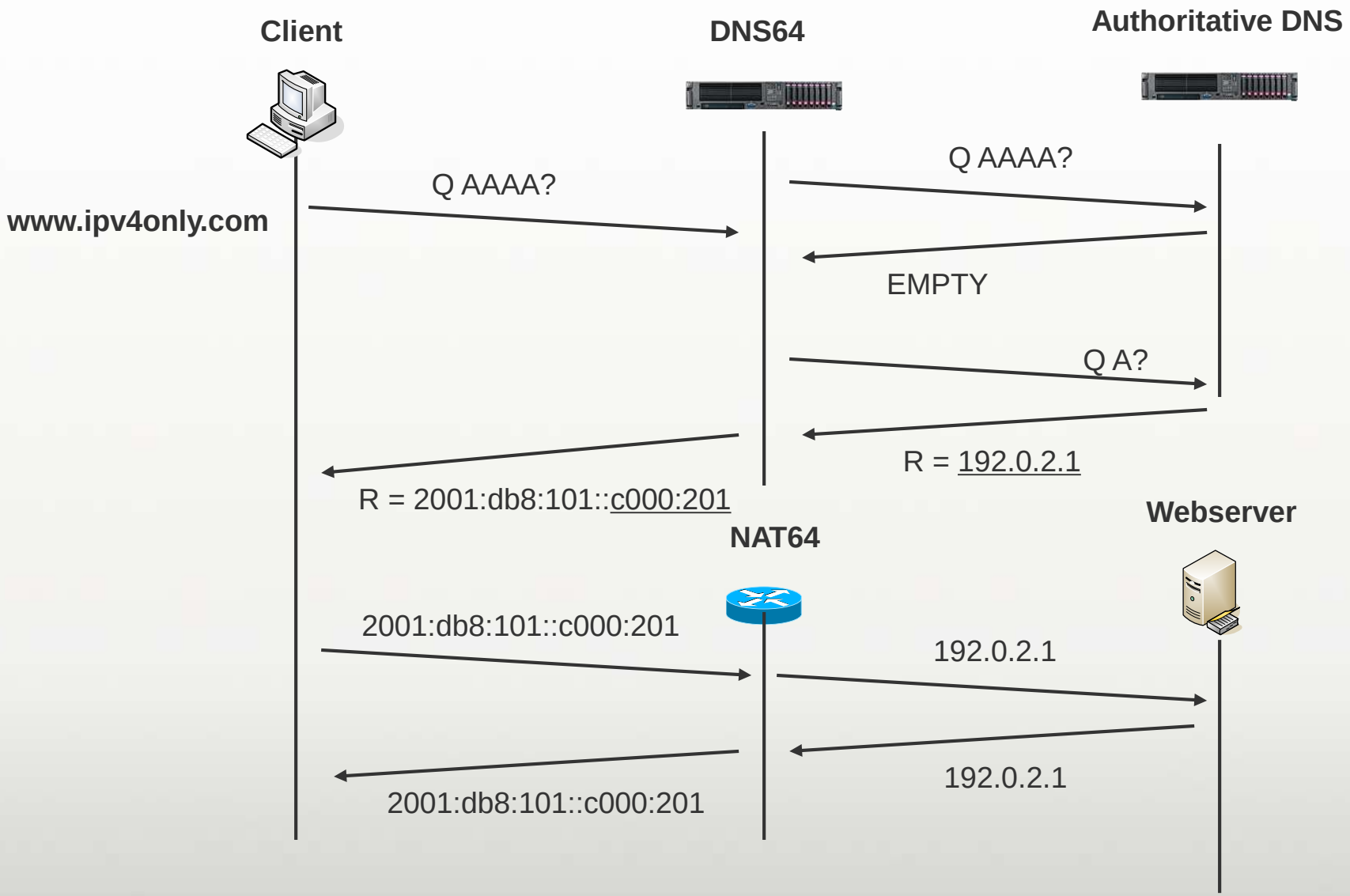
- Unless the client can prove that he speaks IPv6 we are not going to send him to IPv6 sites.
- This setup is becoming increasingly rare.

DNS64

SECURE64

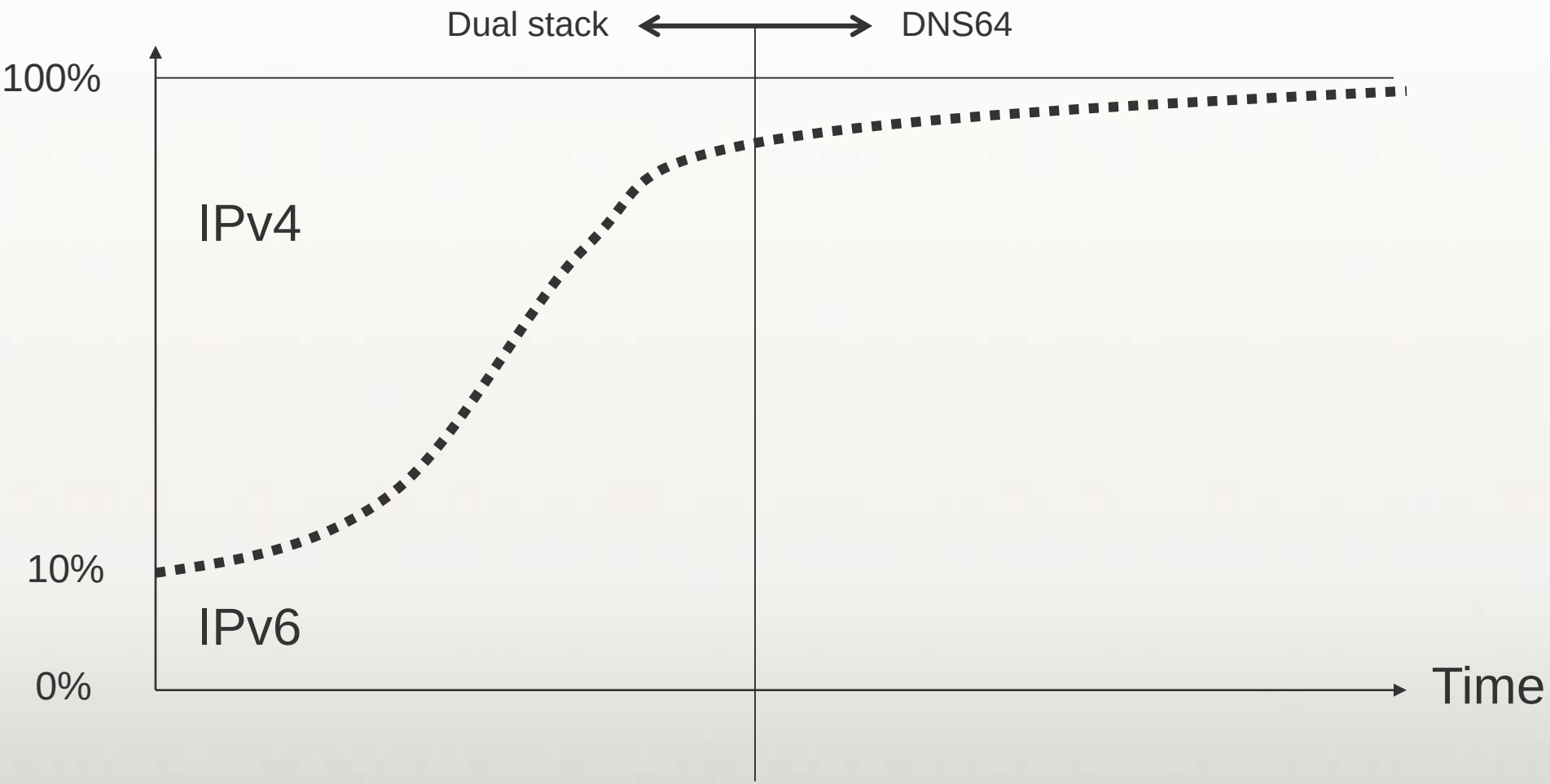
- Moves a network directly to IPv6 without having to deploy dual stack
- Is one of many transition technologies to IPv6
- Allow IPv6 only clients to access IPv4 only content
- Defined in RFC
- Requires both DNS64 and NAT64 devices deloyed in the network to work
- There are issues with IPv4 literals
- Can be combined with Dual Stack or other standards.

NAT64 / DNS64 Under The Hood



DNS64 (RFC 6147)

DNS64 Everybody Will Need It



DNS64 Design and functionality options

SECURE64

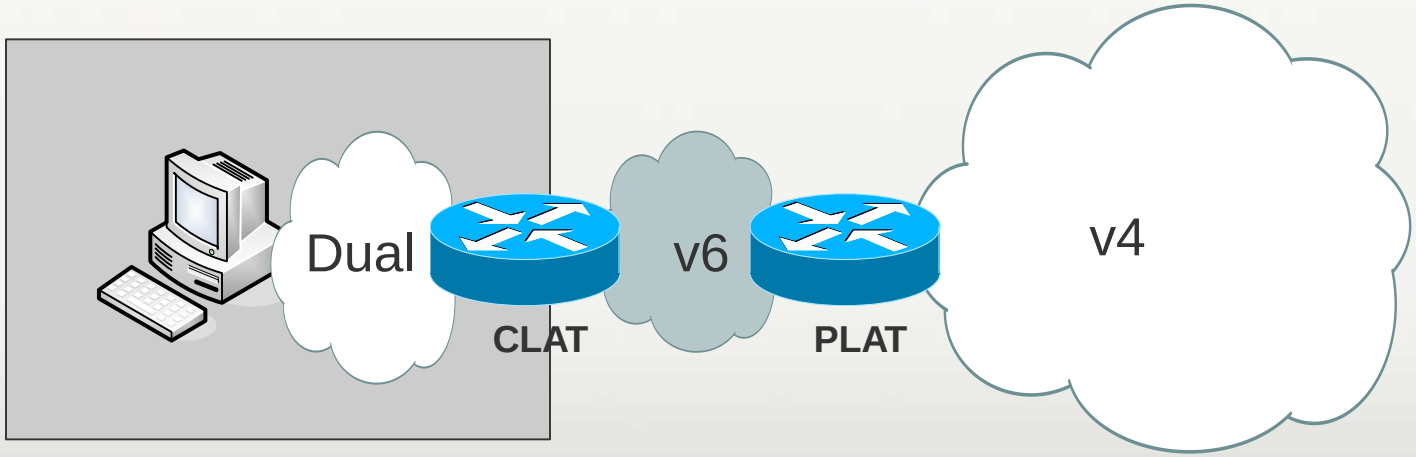
- Sticky clients
  - Make sure a client goes to the same IPv4 server during the session.
- Mixed deployments using views
  - The same DNS server must be able to handle different types of networks and different NAT64 gateways.
- Load balancing via DNS
  - Coarse load balancing of NAT64 gateways
- High availability
  - Take one NAT64 gateway out of rotation if it becomes unavailable.

- How to handle broken applications?
  1. Stop using the broken applications. Works for Enterprise but not for Service Providers.
  2. Continue using IPv6 but dual stack the entire network. Bad because you don't get the benefit of IPv6 only
  3. 464XLAT

464XLAT (RFC 6877)

- 464XLAT is a way to handle broken websites.
- Can be used standalone or with DNS64.
- CLAT is a stateful translation v4-v6, PLAT is stateless v6-v4
- Supported by Android, configured with

```
plat_subnet 2001:db8:1:2:3:4::
```



Could be one device

Heuristic discovery (RFC 7050)

SECURE64

- Heuristic discovery of DNS64 prefix (RFC 7050)
- Instead of having to configure the plat subnet manually, the handset can figure it out with some intelligent queries.
- Works in Andriod 4.3 using the `plat_from_dns64_hostname`
- ipv4only.arpa. domain is created, if you get a AAAA response back you know you are behind a DNS64 and can figure out the prefix.

Reverse IPv6 Delegation (draft-howard)

SECURE64

- Reverse delegation of just a single /64 would require 4 billion disks with 400 G of storage
- Feature (Service) parity between IPv4 and IPv6
- Feature parity is hard for IPv6 reverse delegation. Traditionally they have been pre-generated in IPv4:

```
1.2.3.4.in-addr.arpa  PTR  client1.houston.provider.net.
2.2.3.4.in-addr.arpa  PTR  client2.houston.provider.net.
3.2.3.4.in-addr.arpa  PTR  client3.houston.provider.net.
4.2.3.4.in-addr.arpa  PTR  client4.houston.provider.net.
```

- Alternatives for IPv6 (draft-howard-isp-ip6rdns-06):
  - Delegate DNS – Not all customers can/will run DNS
  - Dynamic DNS – Scaling issues
  - Wildcard – not a perfect solution
  - Synthetic IPv6 – not widely implemented

Comparison of IETF draft options (draft-howard)

SECURE64

	Do Nothing	Wildcards	Dynamic DNS	Synthesize
# new servers	0	0	Many	**0**
Reverse record exists		✓	✓	✓
Reverse record matches forward record			✓	✓
Works with DNSSEC		✓	Difficult	**Difficult**

DNS solutions need to evolve to simplify reverse IPv6 DNS

Synth

SECURE64

Traditional method

No service parity between v4 and v6
Spam filters, ssh, etc does not work

Gigabytes of zone transfers, long startup time, large memory requirements

1.2.3.4.in-addr.arpa
d.b.8.1.0.0.2.ip6.arpa →

client-1-2-3-4.example.com
NXDOMAIN ←

← $GENERATE

New method

Service parity between v4 and v6

Minimal zone transfer, quick startup, low memory requirements

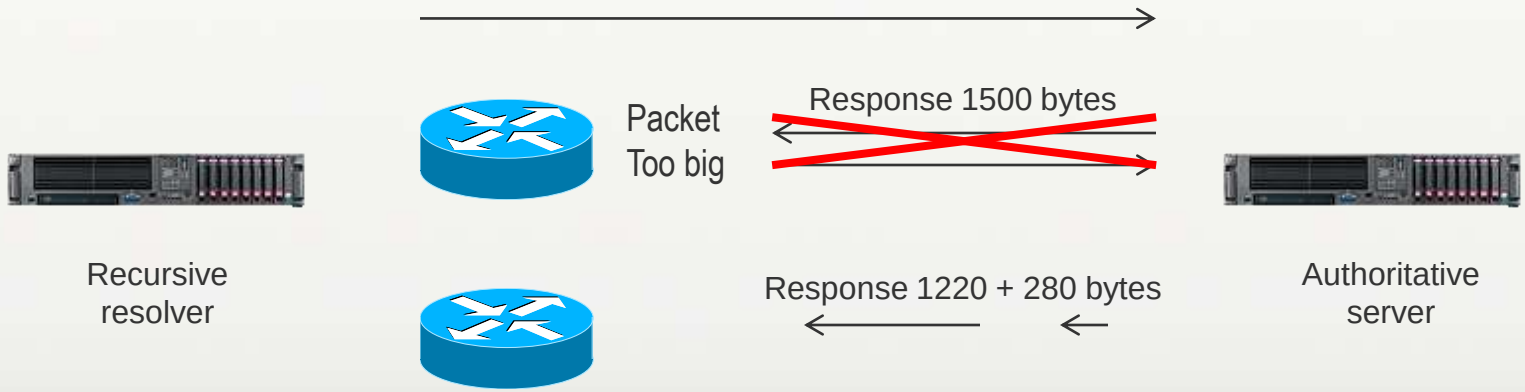
1.2.3.4.in-addr.arpa
d.b.8.1.0.0.2.ip6.arpa →

client-1-2-3-4.example.com
Client-d-b-8-1-v6.example.com ←

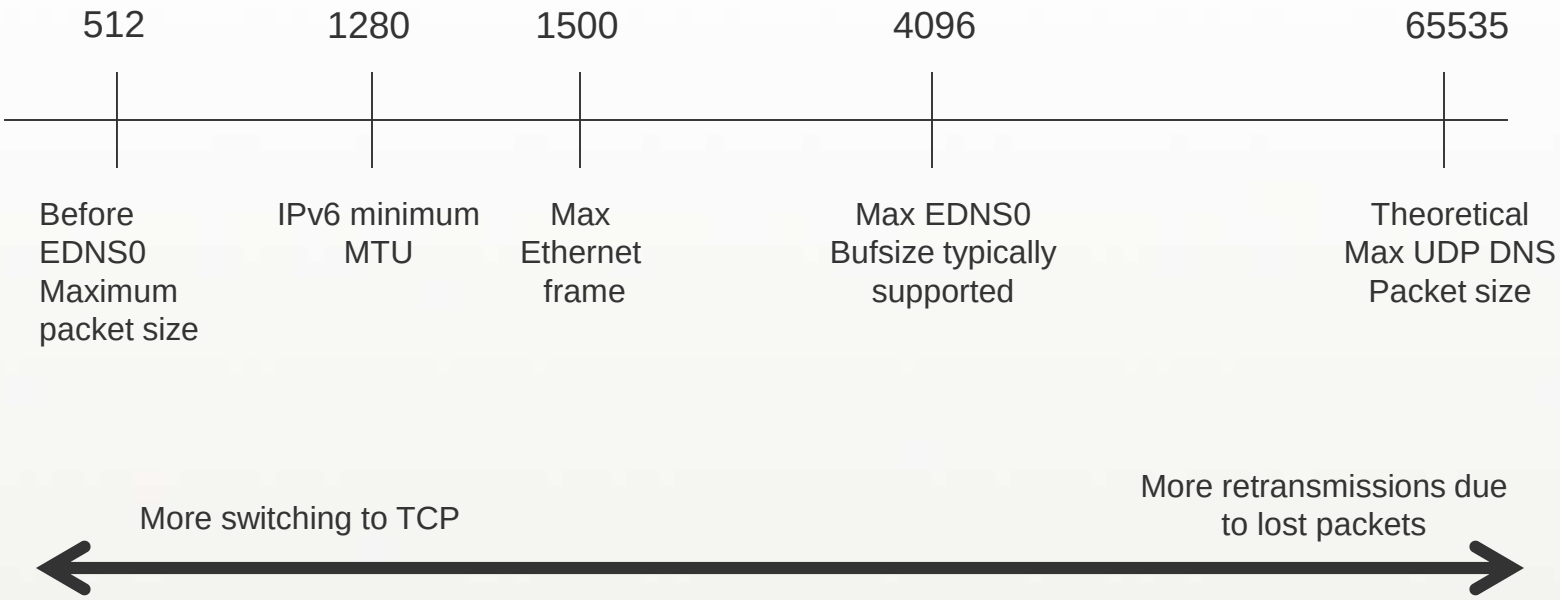
← S64-SYNTH

Packet Too Big issue in IPv6

- Lack of intermediate fragmentation in IPv6 cause issues
- Correct processing of PTB packets is complex



DNS network packets



- DNS are small packets.
- A fancy algorithm does not pay off.
- Initial advertized bufsize=1440 for IPv4 and 1220 for IPv6

DOS attacks over IPv6

SECURE64

- IPv4 defense against DOS attacks is to blacklist (block/drop/rate limit) the offending IPv4 address.
- With IPv6 each client will be given a very large set of IPv6 addresses.
- A sneaky attacker or Botnet controlled computer could traverse the large address space to avoid getting blacklisted without using the same source in 100+ years.

- Conclusion:
  - Defenses against DOS attacks must be re-architectured in IPv6 to work on prefixes.

- DNS Response Rate Limiting defaults to IPv6 Prefix Length /56