Configuring DNS for Clients

Betty DuBois

PACKET DETECTIVE

@PacketDetective www.bettydubois.com

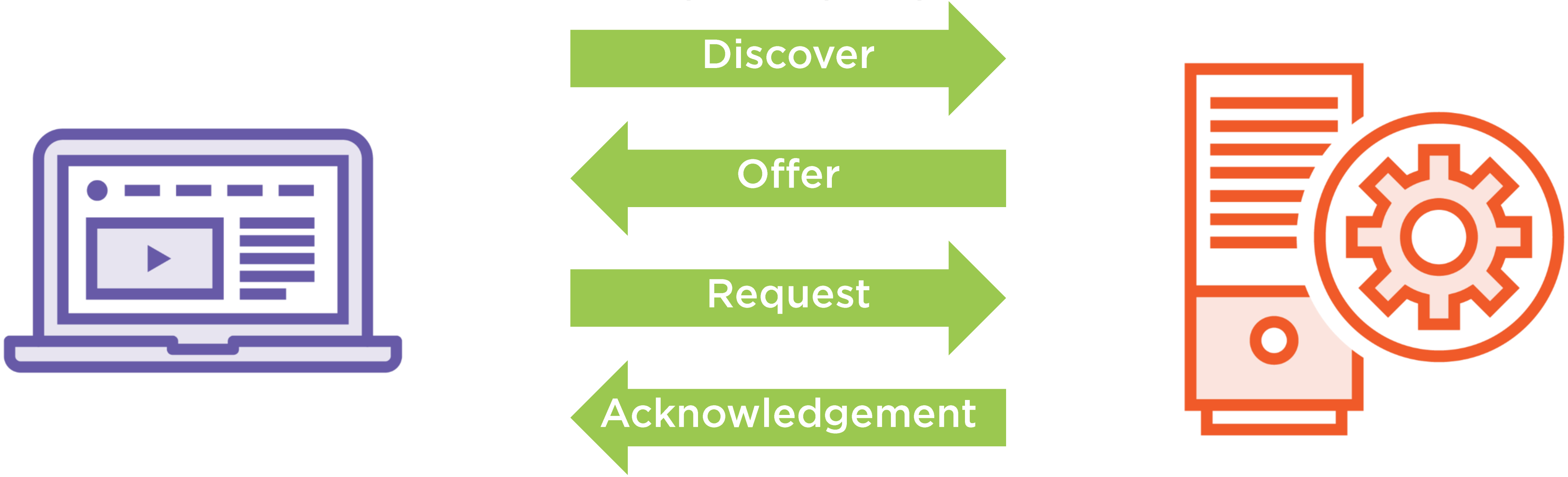
Module Goals

Examine how clients obtain DNS server information

Clear DNS cache

Implement DNS over HTTPs (DoH) and DNS over TLS (DoT)

How Clients Obtain DNS Configuration Information



Discover

Offer

Request

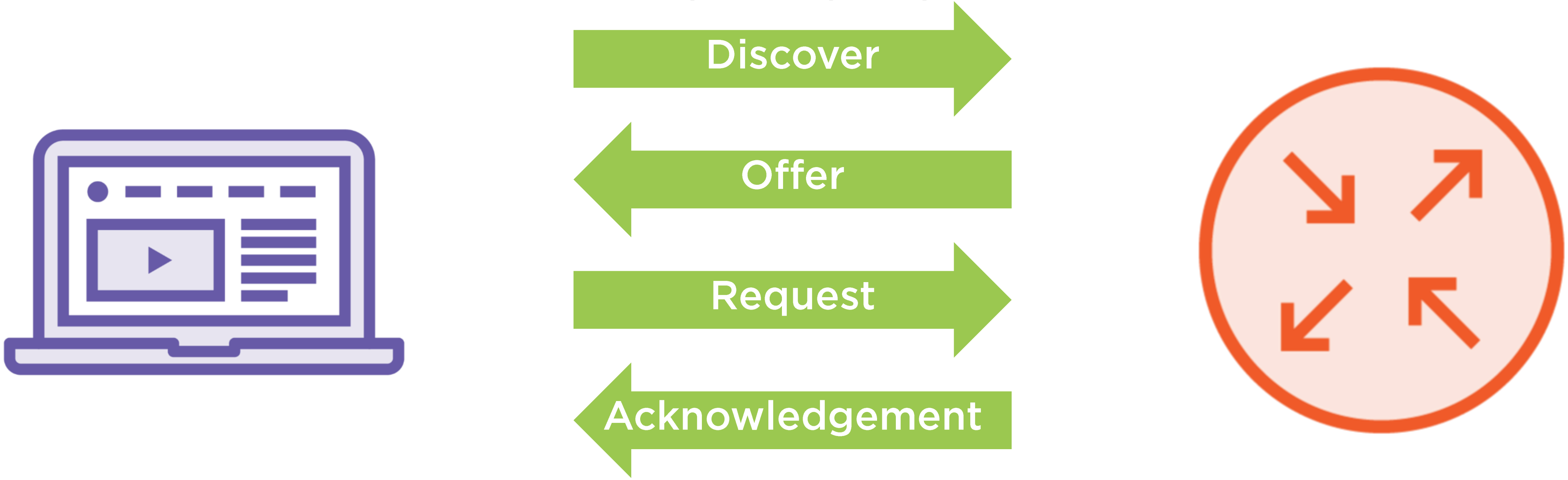
Acknowledgement

Help! I need an address and some other stuff.

DORA to the rescue

Here is an IP address, subnet mask, default gateway and DNS server IP address. Have fun!

How Clients Obtain DNS Configuration Information



Help! I need an address and some other stuff.

DORA to the rescue

Here is an IP address, subnet mask, default gateway and DNS server IP address. Have fun!

Multiple DNS Servers

Why have multiple DNS servers?

- Load balancing
- Fail over/redundancy
- Multiple Locations

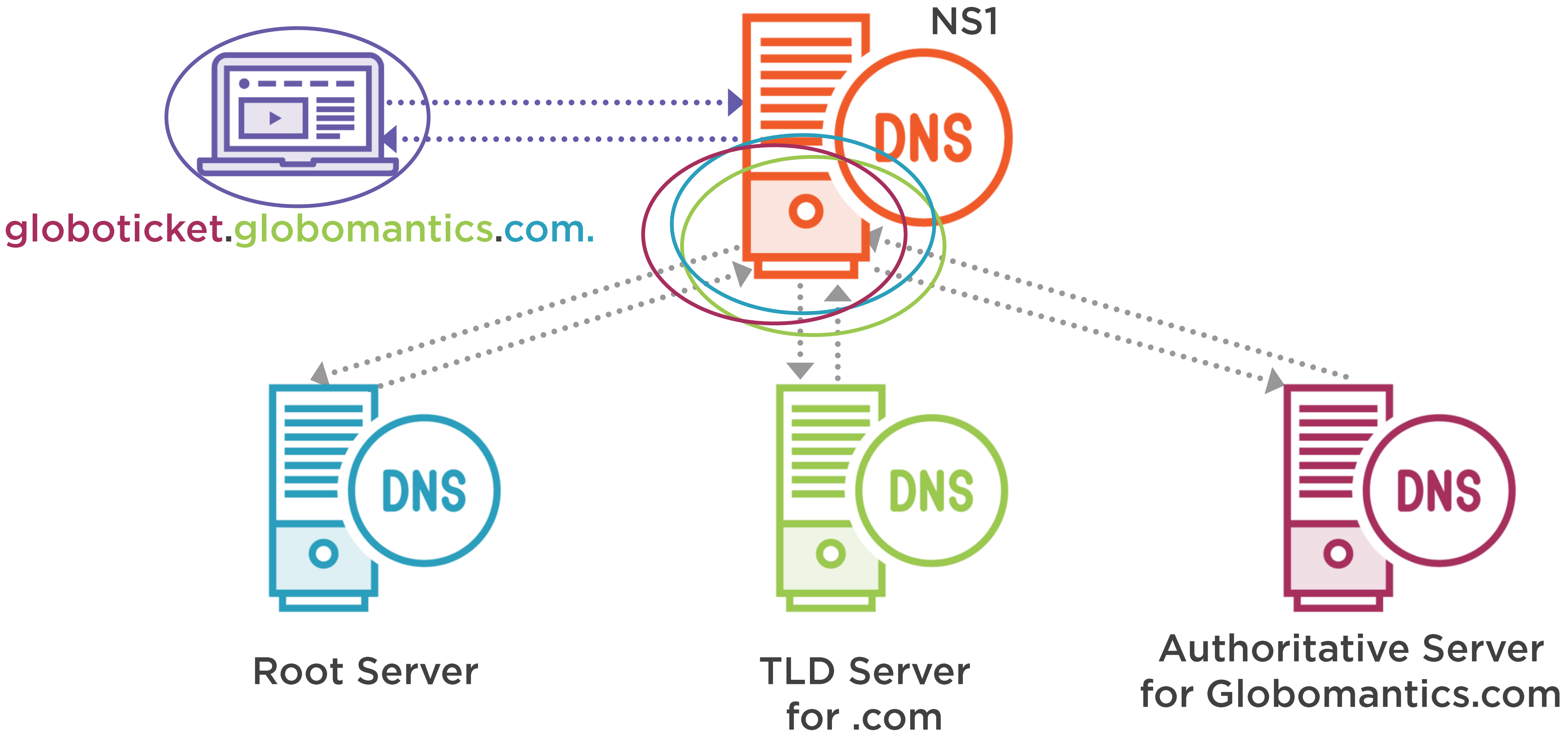
Demo

Determine how many DNS servers a client is using

Find the DNS IP addresses in the DHCP header using Wireshark

DNS Cache

Where are Records Cached?



Common TTL Times for DNS Records

1 second

60 seconds - 1 minute

300 seconds - 5 minutes

3600 seconds - 1 hour

86400 seconds - 24 hours

604800 seconds - 7 days

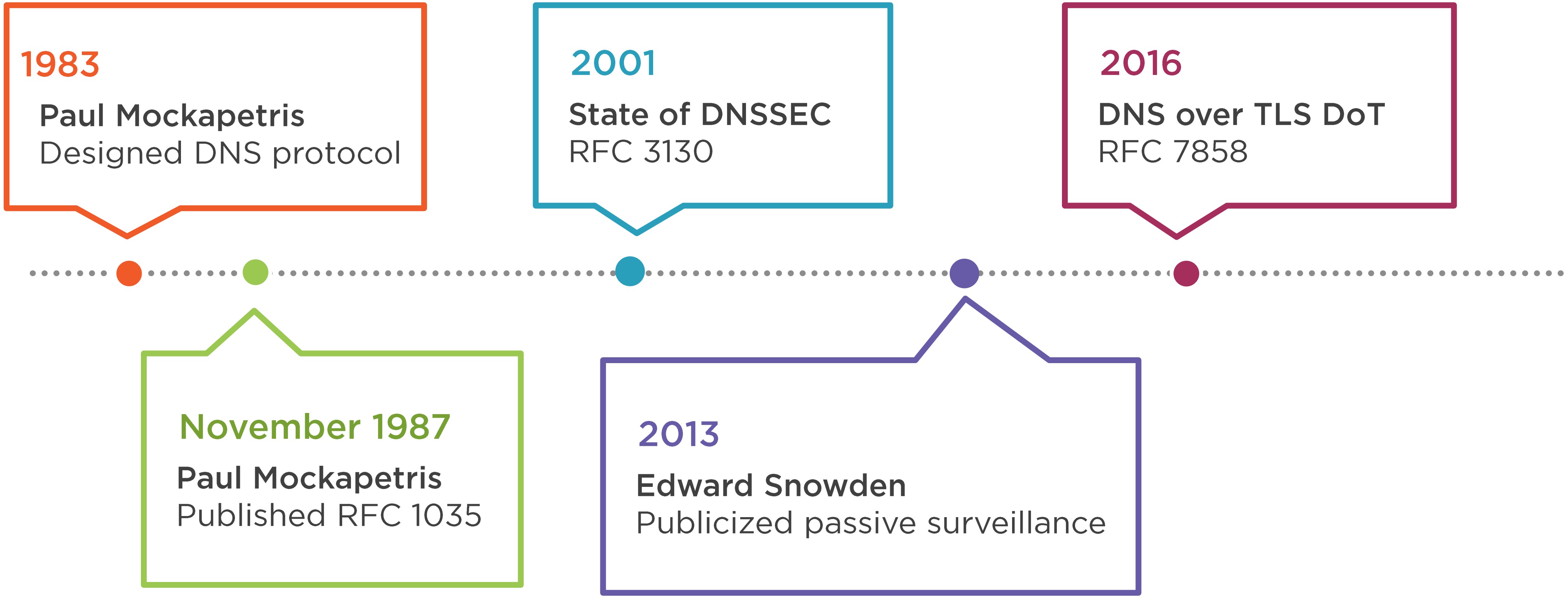
Demo

Clear DNS cache at client and server

Capture with Wireshark

DNS Privacy

DNS Privacy Timeline



1983

Paul Mockapetris
Designed DNS protocol

November 1987

Paul Mockapetris
Published RFC 1035

2001

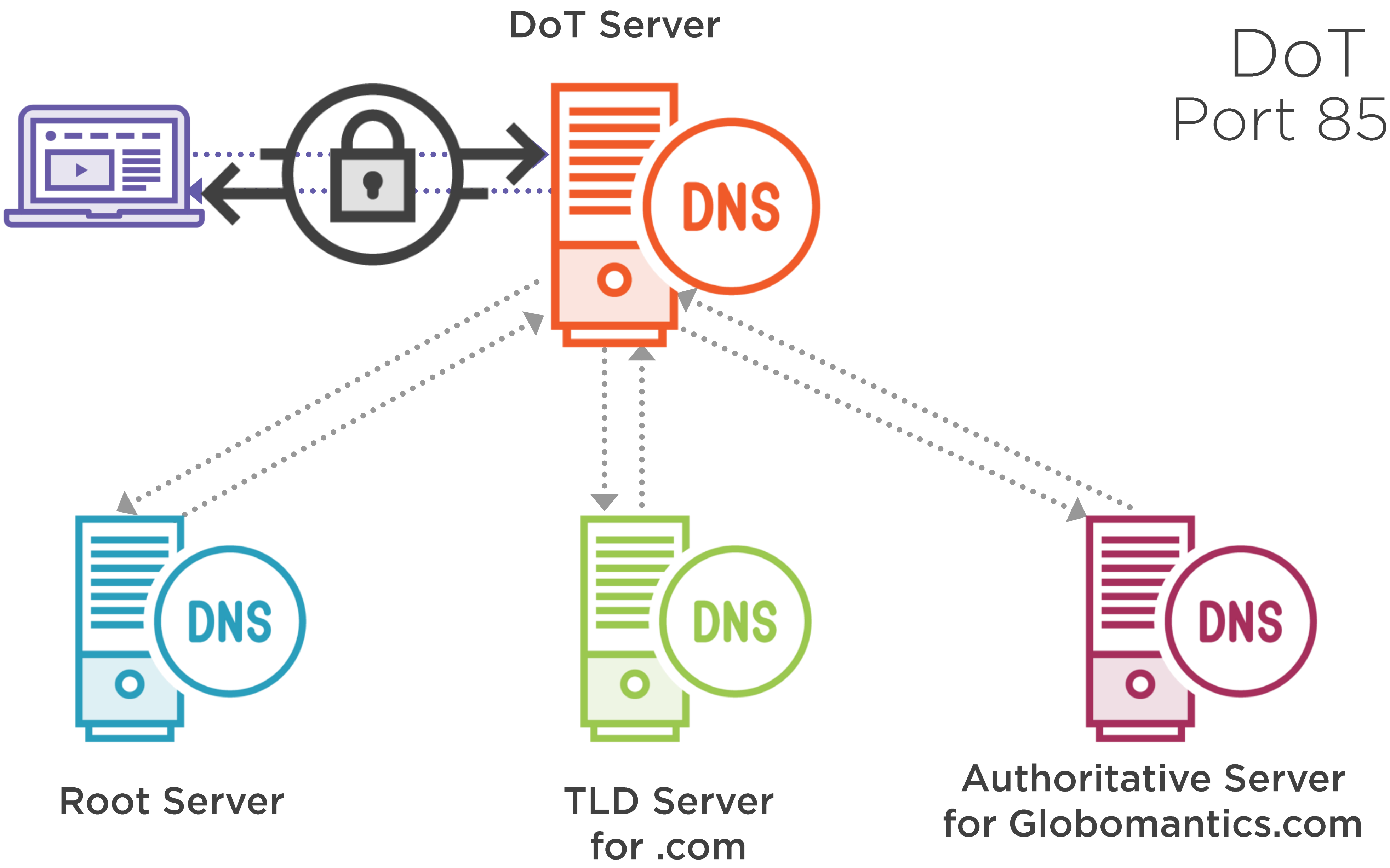
State of DNSSEC
RFC 3130

2013

Edward Snowden
Publicized passive surveillance

2016

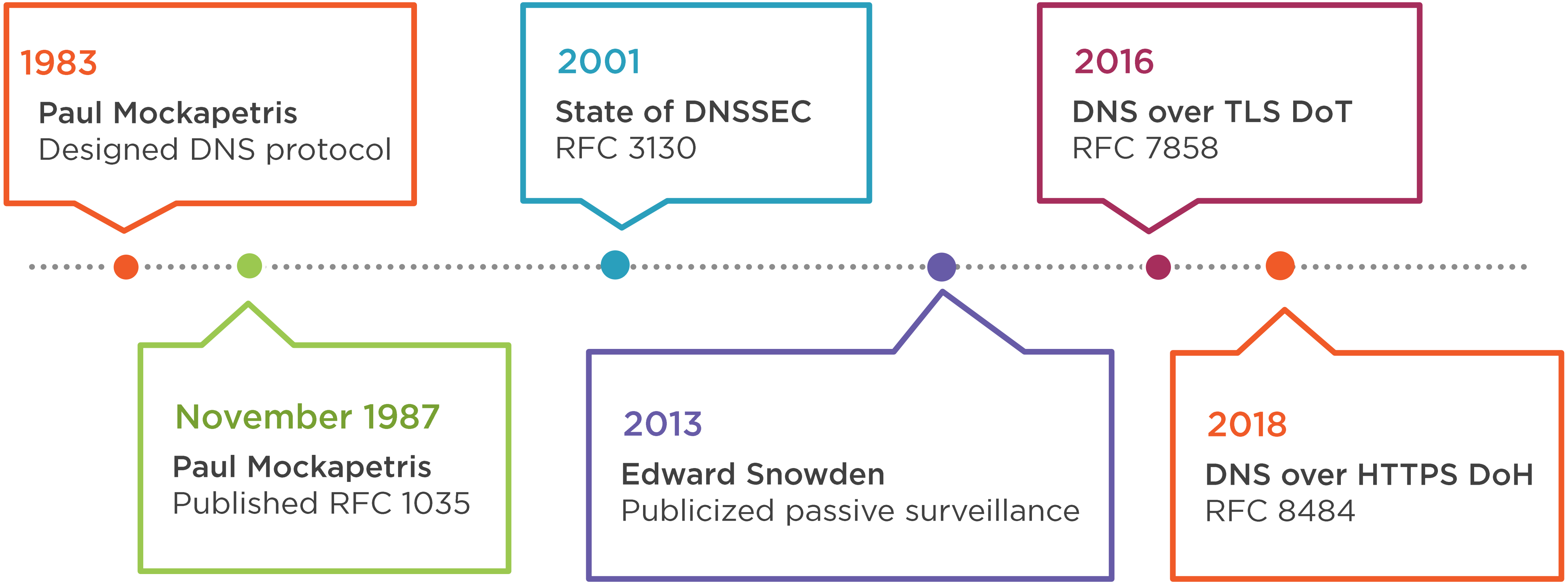
DNS over TLS DoT
RFC 7858


DoT Server
DNS
DNS
DNS
DNS
Root Server
TLD Server for .com
Authoritative Server for Globomantics.com

DoT

Port 853

DNS Privacy Timeline



1983

Paul Mockapetris
Designed DNS protocol

November 1987

Paul Mockapetris
Published RFC 1035

2001

State of DNSSEC
RFC 3130

2013

Edward Snowden
Publicized passive surveillance

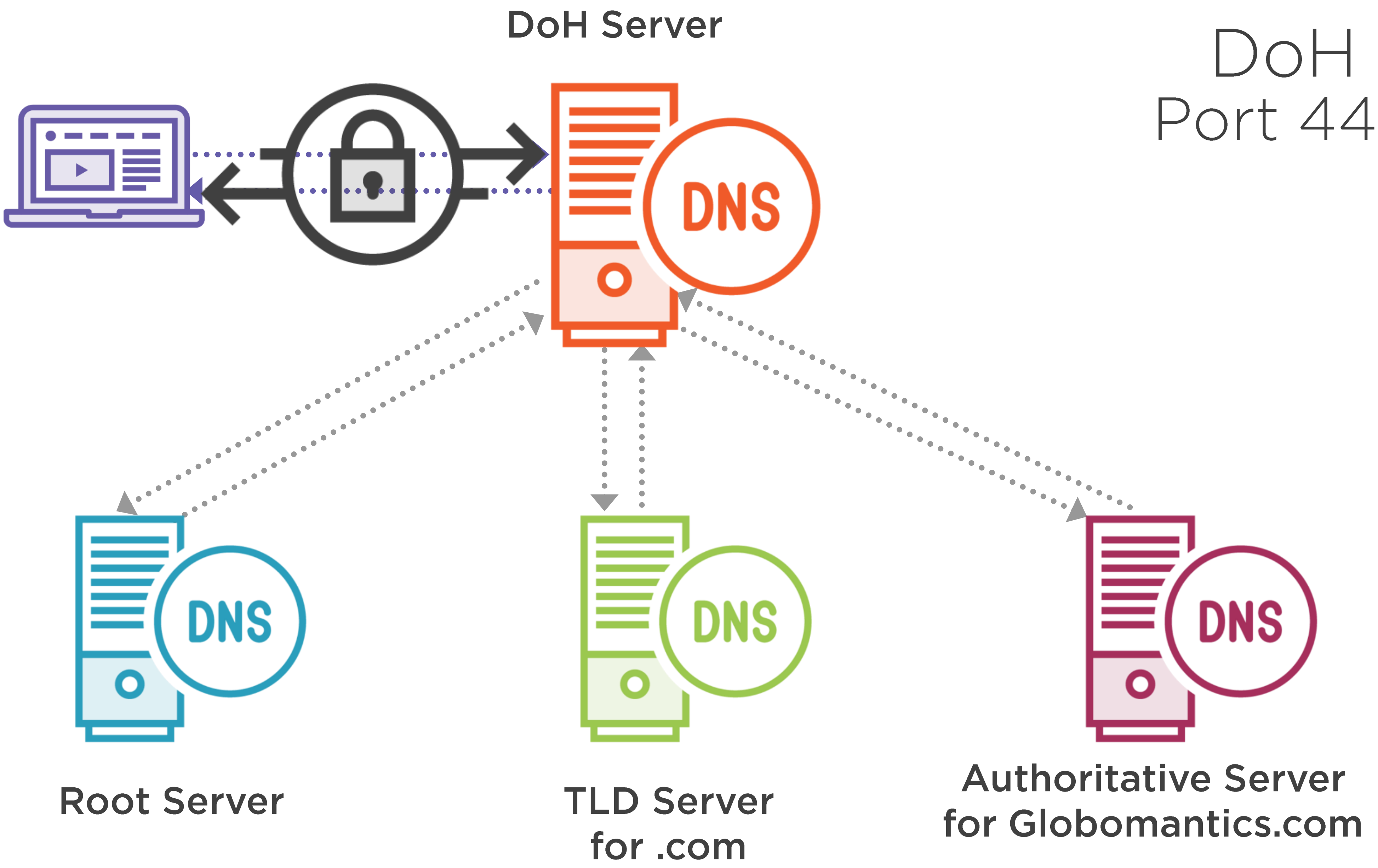
2016

DNS over TLS DoT
RFC 7858

2018

DNS over HTTPS DoH
RFC 8484

DoH
Port 443


DoH Server
DNS
DNS
Root Server
DNS
TLD Server
for .com
DNS
Authoritative Server
for Globomantics.com

Demo

Configure DoH at the client

Summary

Examine how clients obtain DNS server information

Clear DNS cache

Implement DNS over HTTPs (DoH) and DNS over TLS (DoT)

Up Next:
Modifying DNS Configuration for Servers