
# Location Aware DDoS Attacks

Jose Avila III & Keith Myers

EU Sec West 2010: Amsterdam, NL

# Who are we?

## Jose Avila III

Jose Avila is the Director of Creative Development Services and a key research component for ONZRA. Jose has spent an astounding amount of time dealing with DNS implementations and security. He has also worked on improving the intelligence and capabilities of web application fuzzers and audit tools. Previously, Jose was a member of NeuStar's Software Architecture Review Board providing guidance on future application development and security. Jose has also lead many of their enterprise grade development projects including their Managed Internal DNS service that was globally deployed in some of the world's largest networks. Jose recently presented the paper "Recursive DNS Cache Auditing" at OARC, spoken at Black Hat, presented at RSA, and has given lectures at several universities hoping to bring security awareness to future developers. Jose also enjoys tequila tasting and collecting.

# Who are we?

## Keith Myers

Keith Myers is the Operational Director at ONZRA. Before ONZRA Keith worked as the very first employee at the Black Hat Enterprise and spent some years building Black Hat Training, managing the Black Hat Consulting team, and building anonymous communication channels. After that Keith held several technical security positions at financial institutions and consulting companies penetrating networks and exploiting systems before settling in at ONZRA. Keith also enjoys producing and playing house music.

# Introduction

## Abstract

**Part 1: DNS & DDoS Overview**
Here we will cover the basics of DNS

**Part 2: Enumerating Networks Today**
Here we will cover different network configurations and how to enumerate them.

**Part 3: EDNS Client IP**
Here will cover the EDNS Client IP Draft that is up for proposal with backing from some heavy jitters like google.

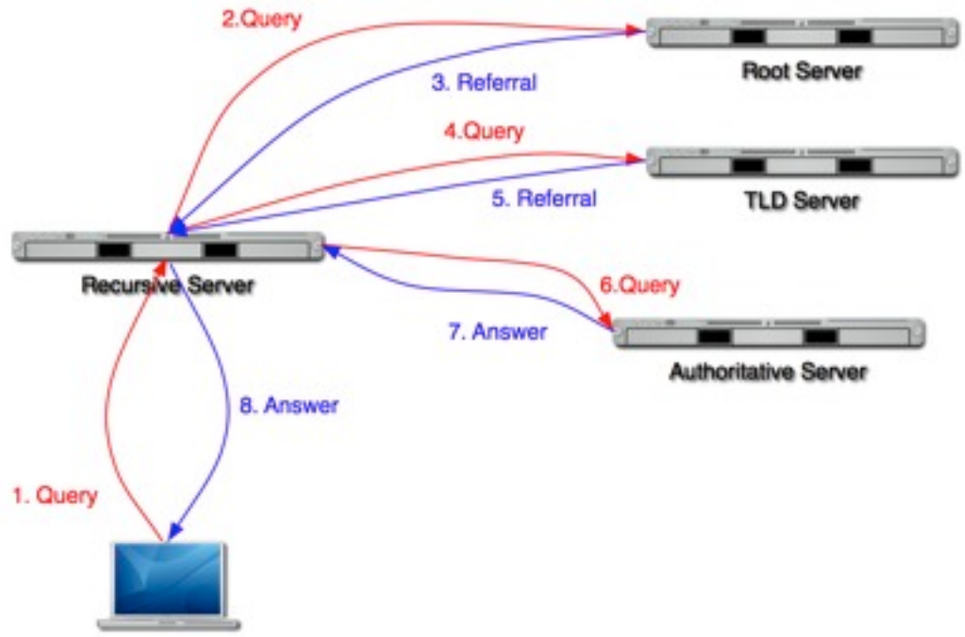
**Part 4: Using EDNS Client IP for a DDoS**
Finally we get to how better location awareness provided by the IETF Draft can lead to more intelligent Location Aware DDoS Attacks.

**Part 5: Network Enumeration Tool**
A small tool we built.

# Part 1: DNS Overview

## Introduction

The DNS Protocol was invented in 1983 to allow for the resolution of names to IP addresses. Since then it has has acquired minor extensions such as EDNS0



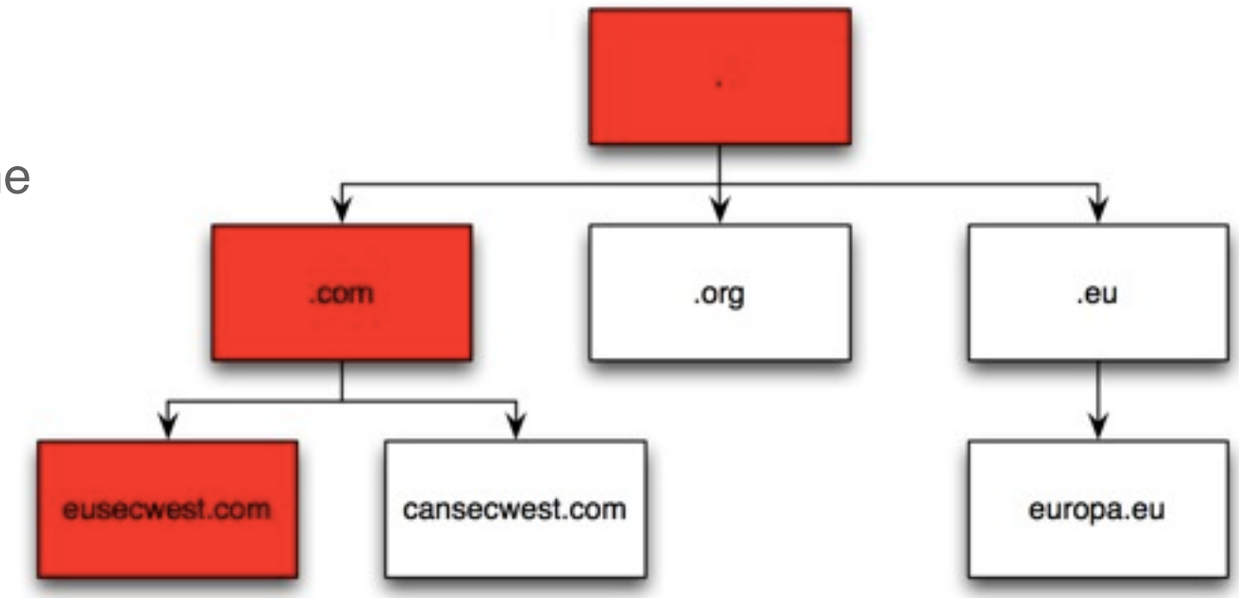
# Part 1: DNS Overview

## Tiers

**Root Zone**
The root zone is the first zone in the tier. It tells you what servers are responsible for what domains

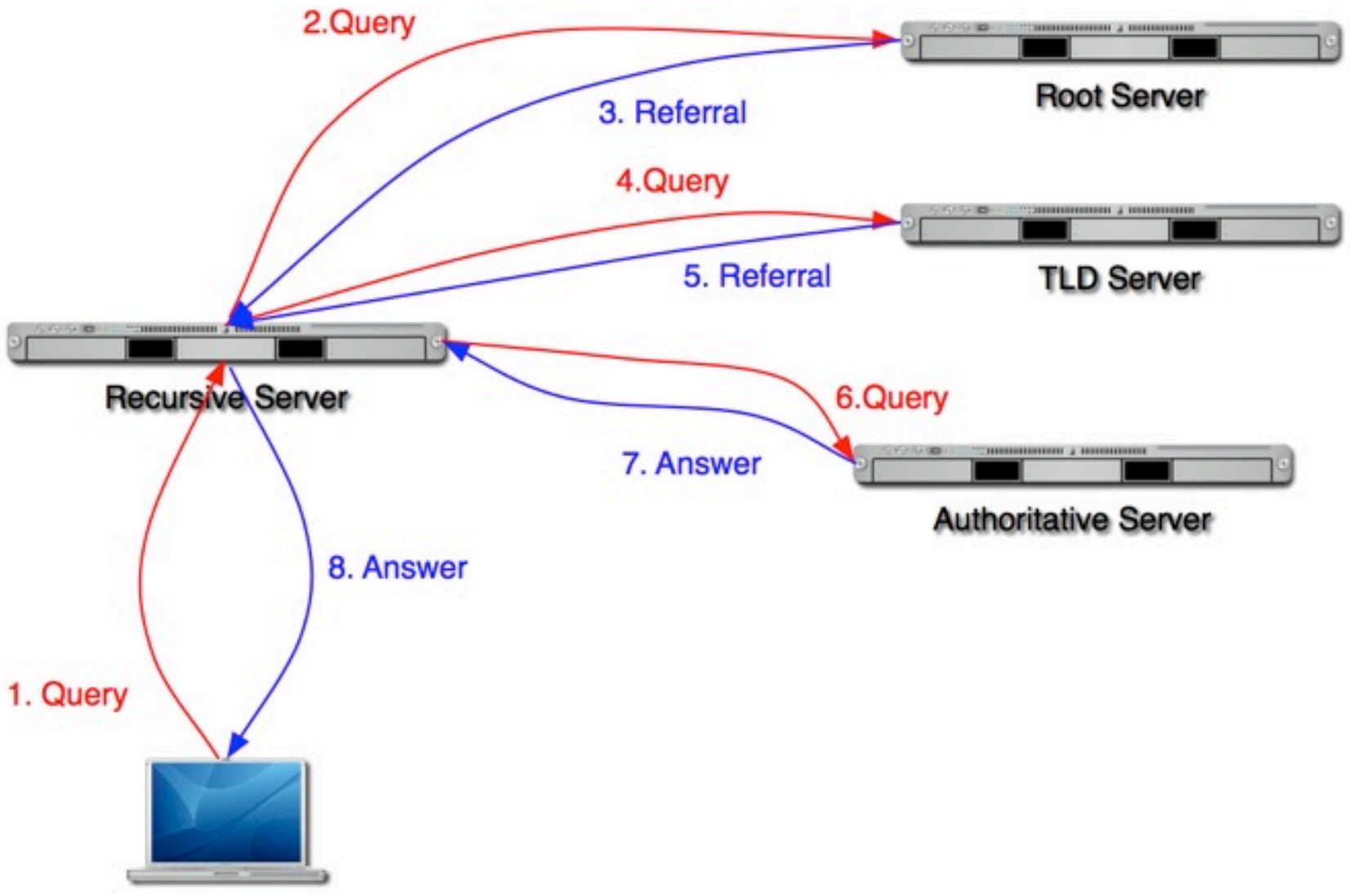
**Top Level Domains**
These TLDs tell you who is responsible for the next hop down.

**How does this all come together?**
...



# Part 1: DNS Overview

## How Does DNS Work?



# Part 1: DNS Overview

## Record Types

**NS Records**
NS Records will tell you what name server is responsible for a domain

**A Records**
A Records give you an IP address for a requested domain name. You can have multiple A records in a single response.

**CNAME Records**
CNAME, or Alias Records point to another FQDN... You can have multiple CNAME records in a single response. Frequently large sites will have alias records pointing to other Content Delivery Networks whom will control their own DNS, etc.

**OPT Records**
OPT Records can be added to a DNS Packet in the request or response

# Part 1: DNS Overview

What is EDNS0?

## Definition

Extension mechanism for DNS, allowing for additional information to be passed in DNS Packets. The first set of EDNS0 extensions were released in 1999 by the IETF in RFC 2671

| RFCs |
| --- |
| 2671 |

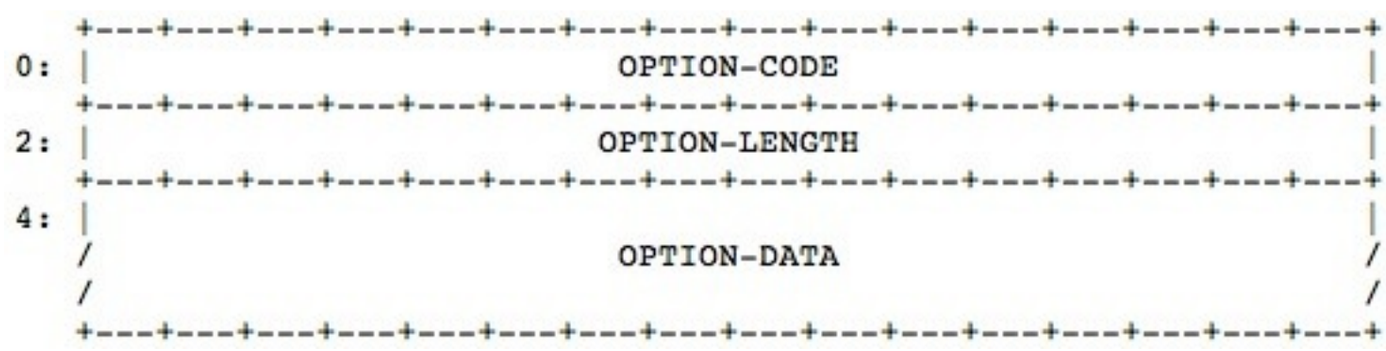
# Part 1: DNS Overview

## EDNS0 Components

**Name, Type, Etc.**

**Option Codes**
Option Codes are assigned by IANA

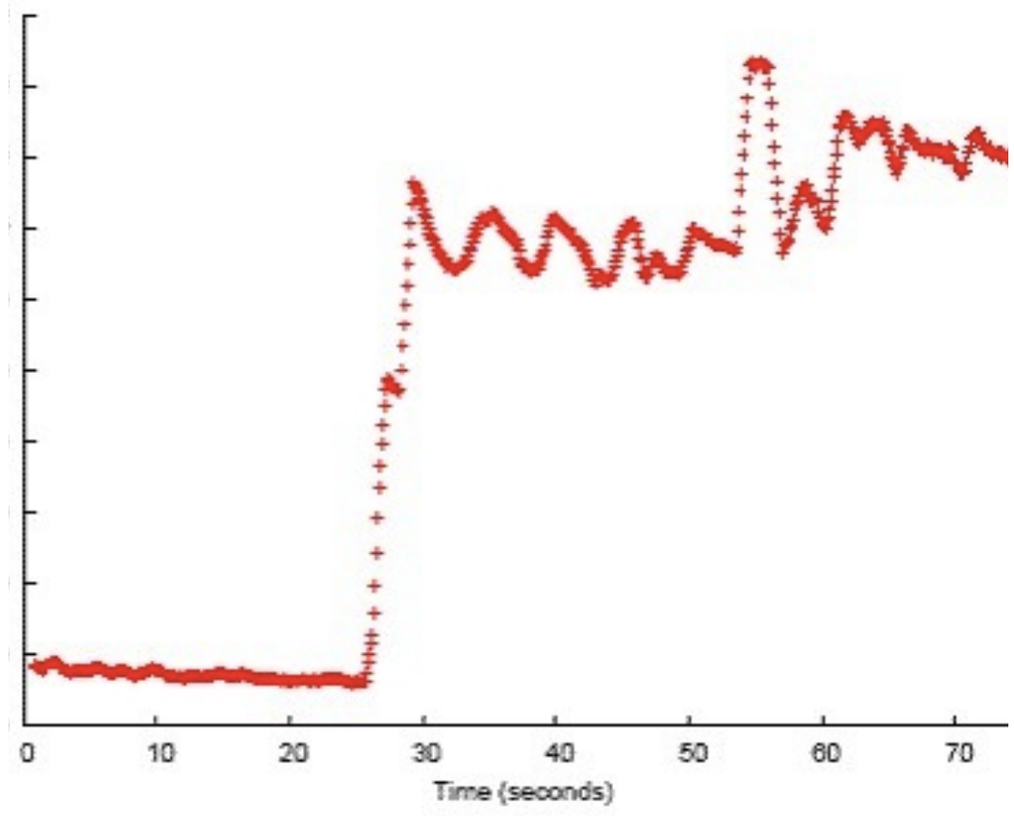
**Option Values**
Option values can be of variable length. (their length is specified in the packet



# Part 1: DDoS Overview

## What is a DDoS

A DDoS Is a Distributed Denial of Service attack. This attack can comes from many sources and it's goal is to render a service ineffective for valid users. This talk is going to focus primarily on target acquisition



# Part 1: DDoS Overview

## Mitigating a DDoS

**There is not just one source!**
DDoS traffic by nature is distributed, and thus you can not just ban one source

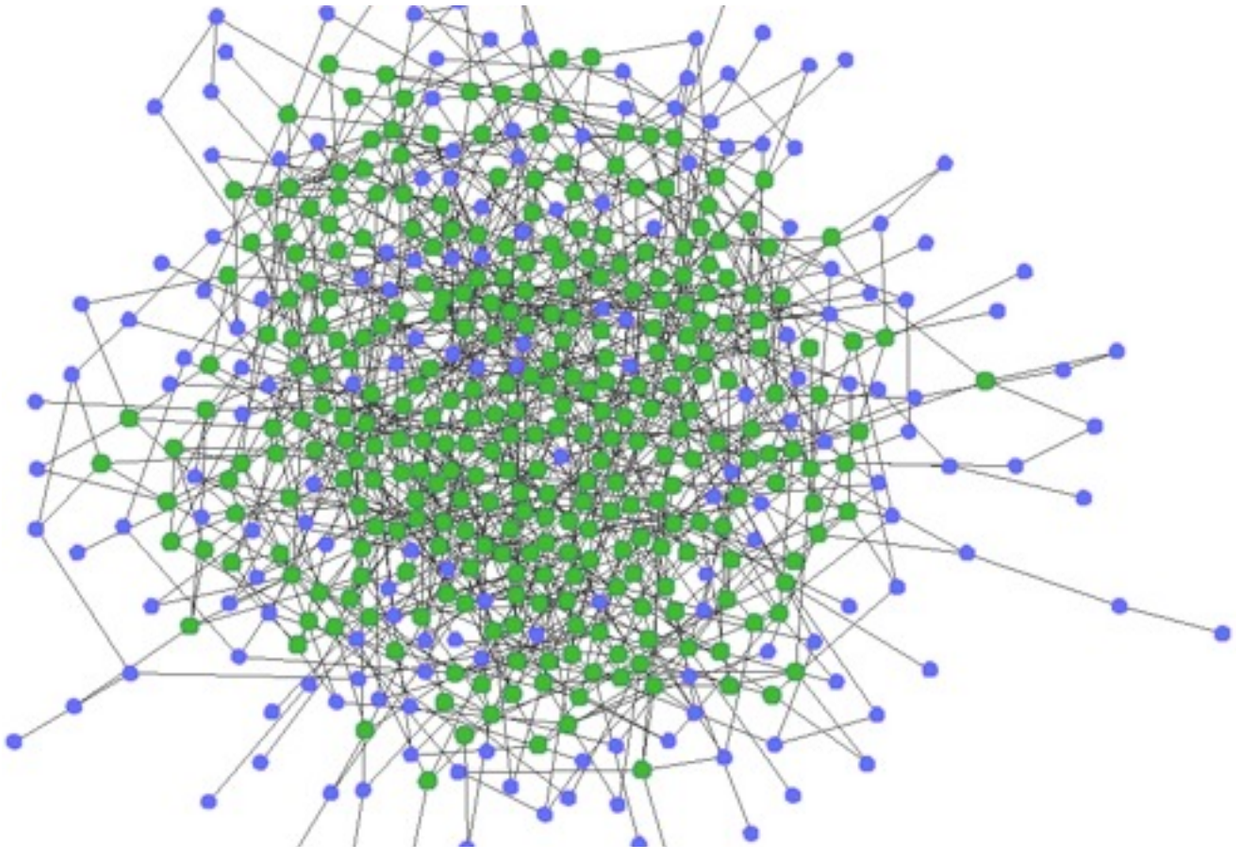
**Identifying bad traffic and getting it filtered.**
This can be a challenge as traffic can be made to look like legitimate requests consuming legitimate resources

**Authoritative DNS Example**

# Part 2: Enumerating Networks Today

## Introduction

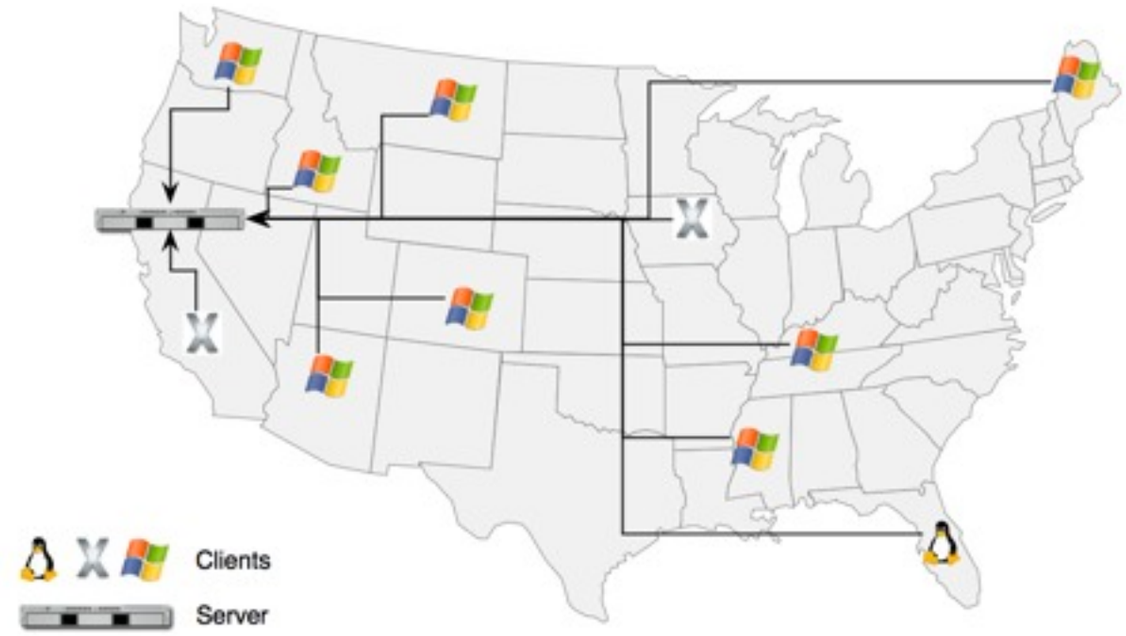
Knowing your target is an important component of any attack. This section will discuss common ways services announce them selves and show you how to enumerate them.



# Part 2: Enumerating Networks Today

## Single Host Server

**1. A Single Host Server**
The server is announced from one physical location, and one physical server.



# Part 2: Enumerating Networks Today

## Single Host Server

**Announced in one location**

While some servers may appear to be just one server, they may actually be announced via BGP any cast (Many root DNS servers announce this way!)

**This is not necessarily one physical server**

This could be a load balancer.

```
$ dig eusecwest.com. @ns0.titanit.net.

; <<>> DiG 9.6.0-APPLE-P2 <<>> eusecwest.com. @ns0.titanit.net.
;; global options: +cmd
;; Got answer:
;; ->>HEADER<<- opcode: QUERY, status: NOERROR, id: 56712
;; flags: qr aa rd; QUERY: 1, ANSWER: 1, AUTHORITY: 2, ADDITIONAL: 2
;; WARNING: recursion requested but not available

;; QUESTION SECTION:
;eusecwest.com.                 IN      A

;; ANSWER SECTION:
eusecwest.com.          3600    IN      A       69.31.185.85

;; AUTHORITY SECTION:
eusecwest.com.          3600    IN      NS      ns0.titanit.net.
eusecwest.com.          3600    IN      NS      ns1.titanit.net.

;; ADDITIONAL SECTION:
```

# Part 2: Enumerating Networks Today

## Single Host From a Pool

**How to detect this?**
This can be detected by querying the authoritative server multiple times.

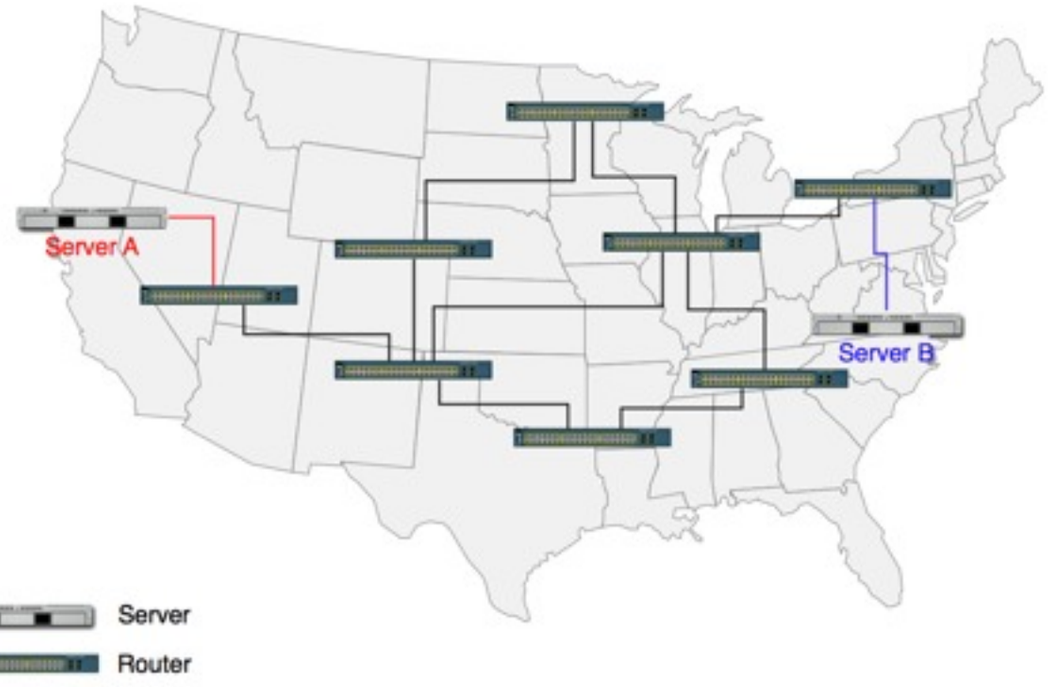
**This makes enumeration a bit harder**

# Part 2: Enumerating Networks Today

## BGP AnyCast

**1. A Single Host Server**
The server is announced from one physical location, and one physical server.

**2. BGP Anycast**
Here BGP is used to announce one particular IP address in multiple locations. The client is routed to the closest server by the routers the client traverses through.



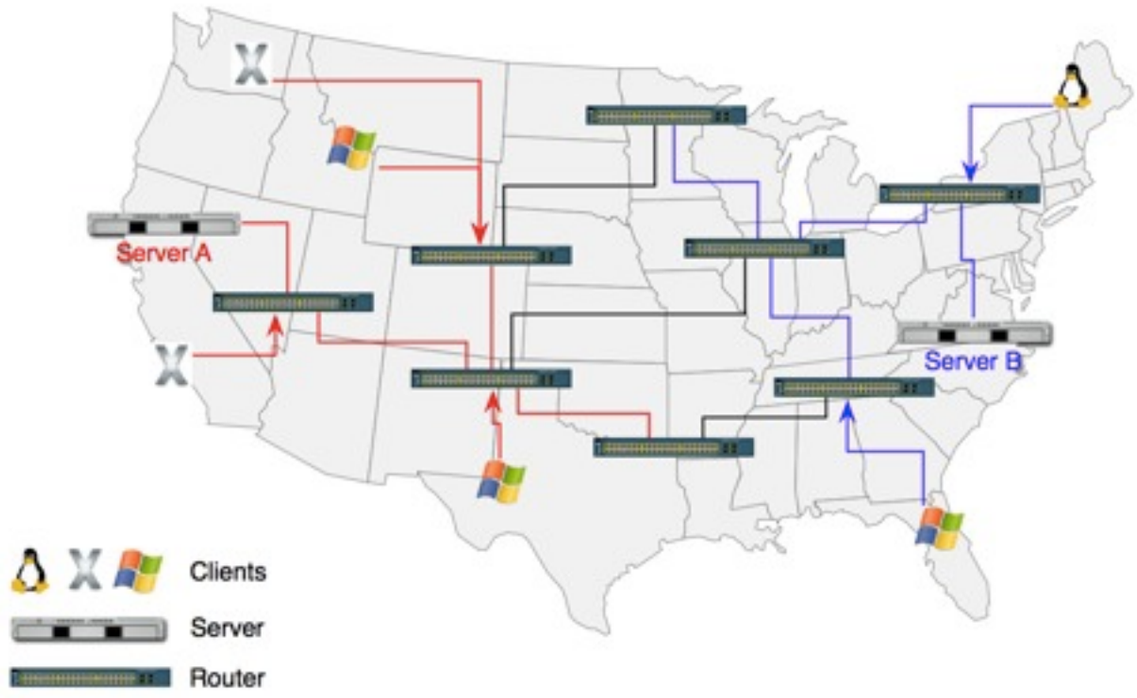
# Part 2: Enumerating Networks Today

## Services

**What services heavily utilize anycast?**
- Root DNS Servers
- Authoritative DNS Servers
- Recursive DNS Servers

**Benefits of Anycasting?**
An anycast network can help protect against DDoS attacks

**Downsides**
Not all services can be anycasted

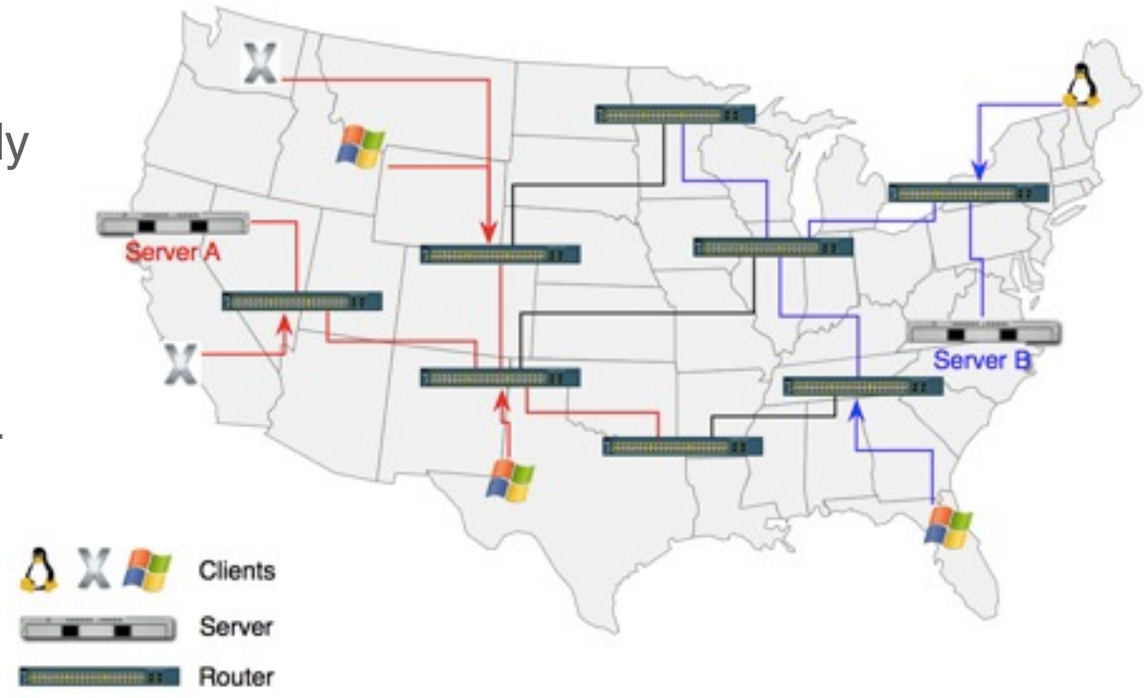


# Part 2: Enumerating Networks Today

## Enumerating a BGP AnyCast Network

**What is an ASN?**
Autonomous System Number. This is a globally unique number identifying a network.

**What is an AS Path**
A path explains what networks a packet would traverse to get to the final destination. A router with multiple peering points can have multiple paths to the same destination




**Detecting BGP Anycast**
Look at the ASN Paths for the announcements at different points. In a BGP Anycast scenario the destination closest to the target will most likely change.

**Query multiple public peering points**
BGP Routing information can be extrapolated from many peering points with a series of BGP commands.

# Part 2: Enumerating Networks Today

## An example...

```
lg.sp.ptt.br> show ip bgp 4.2.2.1
BGP routing table entry for 4.0.0.0/9
Paths: (15 available, best #5, table Default-IP-Routing-Table)
  Not advertised to any peer
  28001 22548 3549 3356, (aggregated by 3356 4.69.130.10)
    200.219.130.61 from 200.219.130.61 (200.3.12.1)
      Origin IGP, localpref 100, valid, external, atomic-aggregate
      Last update: Mon Jun  7 14:34:04 2010

  22548 3549 3356, (aggregated by 3356 4.69.130.10)
    200.160.0.136 from 200.160.0.136 (200.160.0.136)
      Origin IGP, localpref 100, valid, external, atomic-aggregate
      Community: 3549:2355 3549:30840
      Last update: Sat Jun  5 19:10:29 2010

28220 4230 3356, (aggregated by 3356 4.69.130.22)
  200.219.130.75 from 200.219.130.75 (189.124.128.128)
    Origin IGP, localpref 100, valid, external, atomic-aggregate
    Last update: Sun May 30 02:42:21 2010

28571 1916 20080 23148 3356, (aggregated by 3356 4.69.130.22)
  200.219.130.4 from 200.219.130.20 (143.107.255.15)

8055 6762 3356, (aggregated by 3356 4.69.130.22)
  200.219.130.6 from 200.219.130.6 (200.160.48.11)
    Origin IGP, localpref 100, valid, external, atomic-aggregate
    Community: 8055:6762 8055:65535
    Last update: Mon Jun  7 22:42:24 2010

28124 18479 7162 15201 10429 12956 3356, (aggregated by 3356 4.69.130.80)
  200.219.130.79 from 200.219.130.79 (187.16.26.179)
```

**Note the blue highlights**

This is the AS Path

# Part 2: Enumerating Networks Today

## An example...

```
lg.sp.ptt.br> show ip bgp 4.2.2.1
BGP routing table entry for 4.0.0.0/9
Paths: (15 available, best #5, table Default-IP-Routing-Table)
  Not advertised to any peer
  28001 22548 3549 3356, (aggregated by 3356 4.69.130.10)
    200.219.130.61 from 200.219.130.61 (200.3.12.1)
      Origin IGP, localpref 100, valid, external, atomic-aggregate
      Last update: Mon Jun  7 14:34:04 2010

  22548 3549 3356, (aggregated by 3356 4.69.130.10)
    200.160.0.136 from 200.160.0.136 (200.160.0.136)
      Origin IGP, localpref 100, valid, external, atomic-aggregate
      Community: 3549:2355 3549:30840
      Last update: Sat Jun  5 19:10:29 2010

28220 4230 3356, (aggregated by 3356 4.69.130.22)
  200.219.130.75 from 200.219.130.75 (189.124.128.128)
    Origin IGP, localpref 100, valid, external, atomic-aggregate
    Last update: Sun May 30 02:42:21 2010

28571 1916 20080 23148 3356, (aggregated by 3356 4.69.130.22)
  200.219.130.4 from 200.219.130.20 (143.107.255.15)

8055 6762 3356, (aggregated by 3356 4.69.130.22)
  200.219.130.6 from 200.219.130.6 (200.160.48.11)
    Origin IGP, localpref 100, valid, external, atomic-aggregate
    Community: 8055:6762 8055:65535
    Last update: Mon Jun  7 22:42:24 2010

28124 18479 7162 15201 10429 12956 3356, (aggregated by 3356 4.69.130.80)
  200.219.130.79 from 200.219.130.79 (187.16.26.179)
```

# Part 2: Enumerating Networks Today

## An example...

```
lg.sp.ptt.br> show ip bgp 4.2.2.1
BGP routing table entry for 4.0.0.0/9
Paths: (15 available, best #5, table Default-IP-Routing-Table)
  Not advertised to any peer
  28001 22548 3549 3356, (aggregated by 3356 4.69.130.10)
    200.219.130.61 from 200.219.130.61 (200.3.12.1)
      Origin IGP, localpref 100, valid, external, atomic-aggregate
      Last update: Mon Jun  7 14:34:04 2010

  22548 3549 3356, (aggregated by 3356 4.69.130.10)
    200.160.0.136 from 200.160.0.136 (200.160.0.136)
      Origin IGP, localpref 100, valid, external, atomic-aggregate
      Community: 3549:2355 3549:30840
      Last update: Sat Jun  5 19:10:29 2010

28220 4230 3356, (aggregated by 3356 4.69.130.22)
  200.219.130.75 from 200.219.130.75 (189.124.128.128)
    Origin IGP, localpref 100, valid, external, atomic-aggregate
    Last update: Sun May 30 02:42:21 2010

28571 1916 20080 23148 3356, (aggregated by 3356 4.69.130.22)
  200.219.130.4 from 200.219.130.20 (143.107.255.15)

8055 6762 3356, (aggregated by 3356 4.69.130.22)
  200.219.130.6 from 200.219.130.6 (200.160.48.11)
    Origin IGP, localpref 100, valid, external, atomic-aggregate
    Community: 8055:6762 8055:65535
    Last update: Mon Jun  7 22:42:24 2010

28124 18479 7162 15201 10429 12956 3356, (aggregated by 3356 4.69.130.80)
  200.219.130.79 from 200.219.130.79 (187.16.26.179)
```

| Neighbor ASNs |
|---|
| 3549 |
| 4230 |
| 23148 |
| 6762 |
| 12956 |

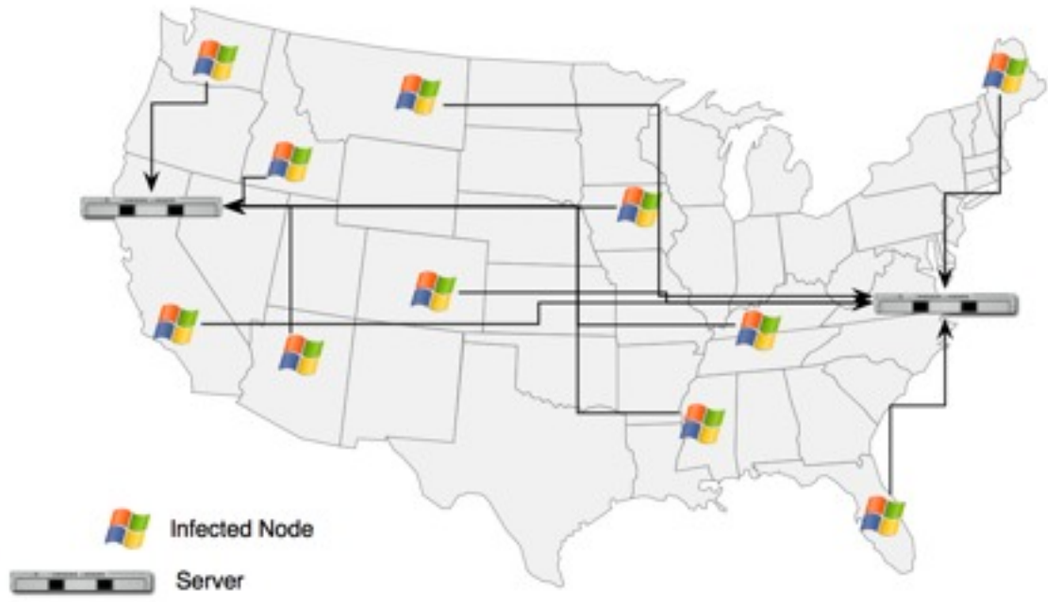
# Part 2: Enumerating Networks Today

## Round Robin DNS

**1. A Single Host Server**
The server is announced from one physical location, and one physical server.

**2. BGP Anycast**
Here BGP is used to announce one particular IP address in multiple locations. The client is routed to the closest server by the routers the client traverses through.

**3. Round Robin DNS.**
Advertise a set of records for your servers all at once. Clients get directed to one of the servers in the set. This server may not be nearest to them



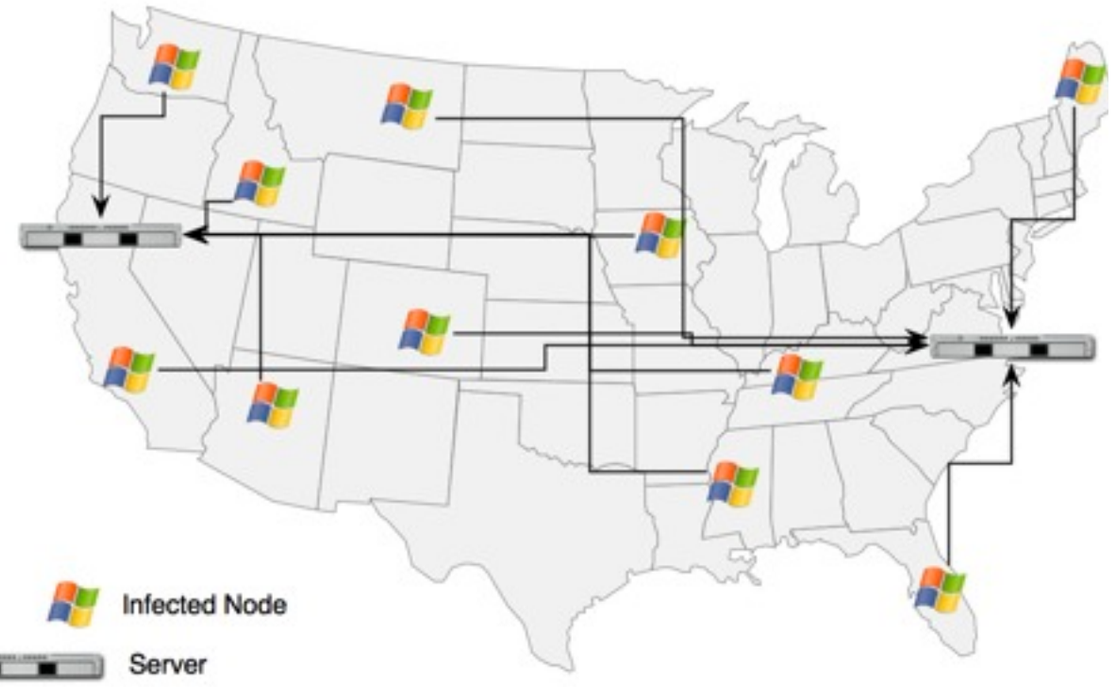
# Part 2: Enumerating Networks Today

## Round Robin DNS

**How do clients get directed?**
Clients will randomly choose one of the many records in the recordset.

**Downsides?**
More latency for clients.

**Records may be announced from a pool**
Records could be announced at random from a pool of available resources making the enumeration of the entire pool more difficult



# Part 2: Enumerating Networks Today

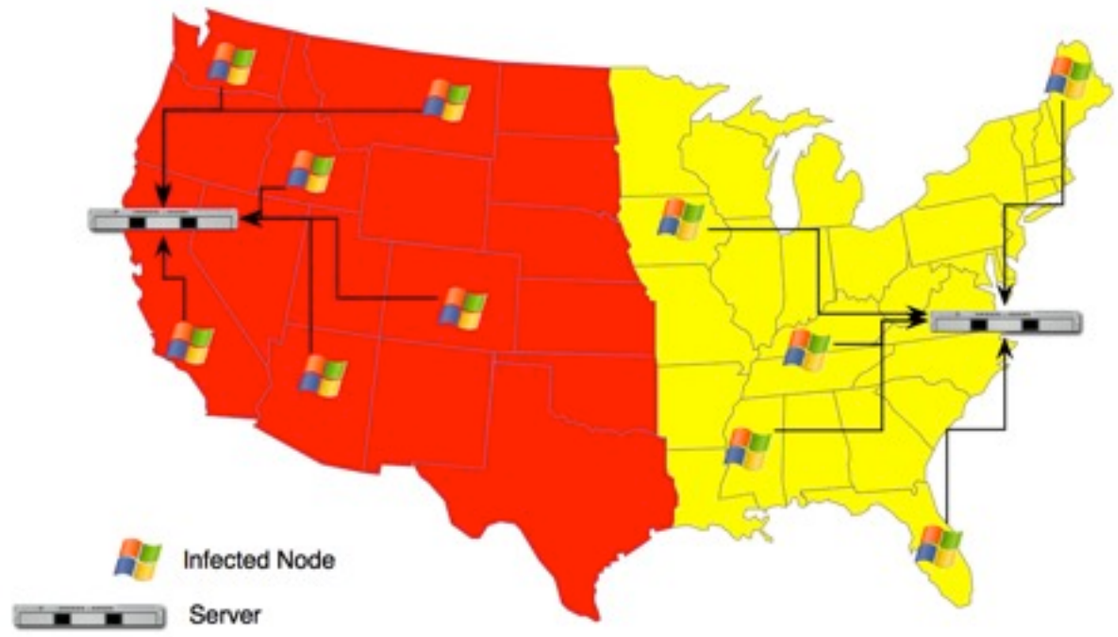
## Directional DNS

**1. A Single Host Server**
The server is announced from one physical location, and one physical server.

**2. BGP Anycast**
Here BGP is used to announce one particular IP address in multiple locations. The client is routed to the closest server by the routers the client traverses through.

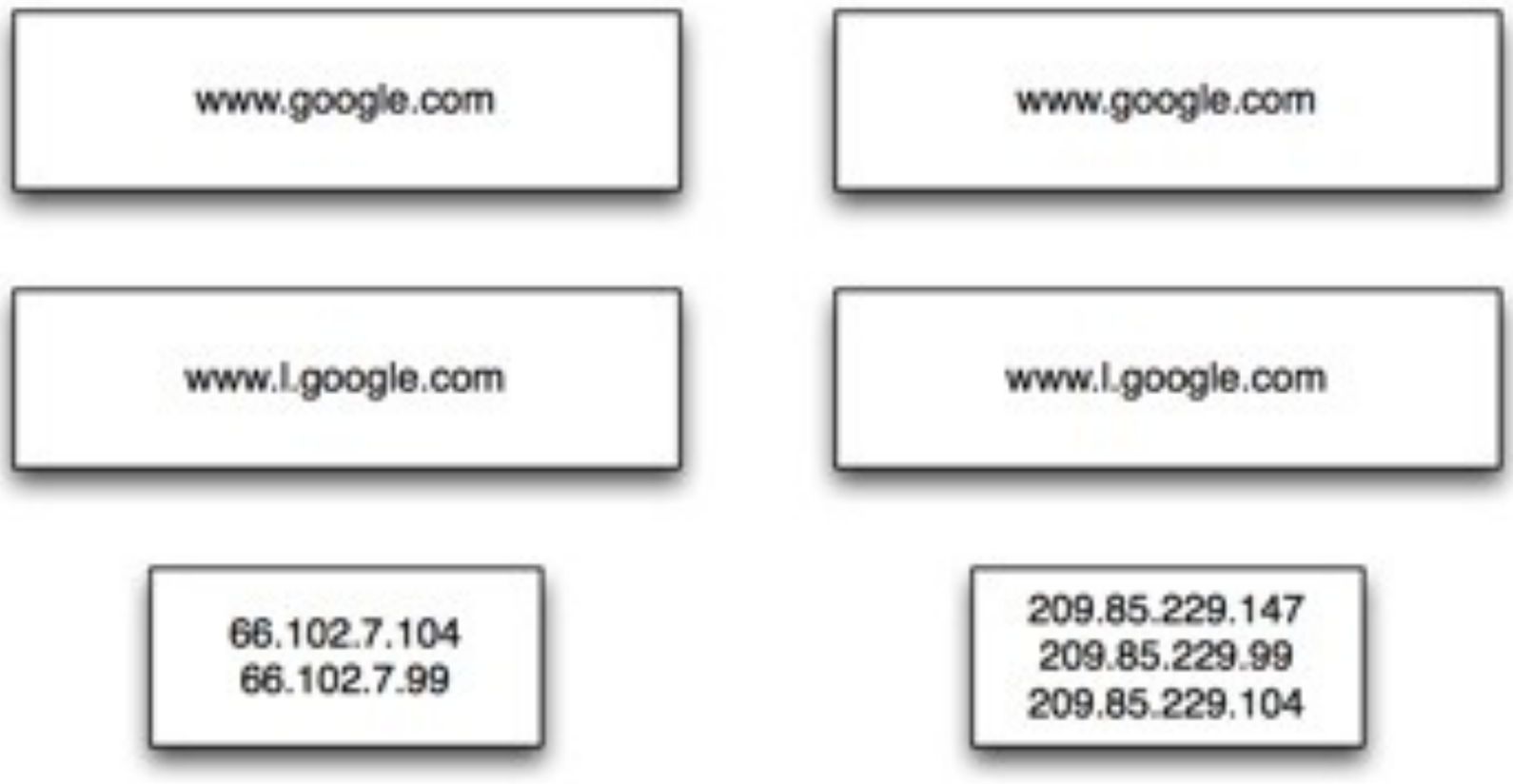
**3. Round Robin DNS.**
Advertise a set of records for your servers all at once. Clients get directed to one of the servers in the set. This server may not be nearest to them

**4. Directional DNS**
Authoritative name servers respond with records that are closest to the recursive DNS server that requested the domain.



# Part 2: Enumerating Networks Today

It's in use today

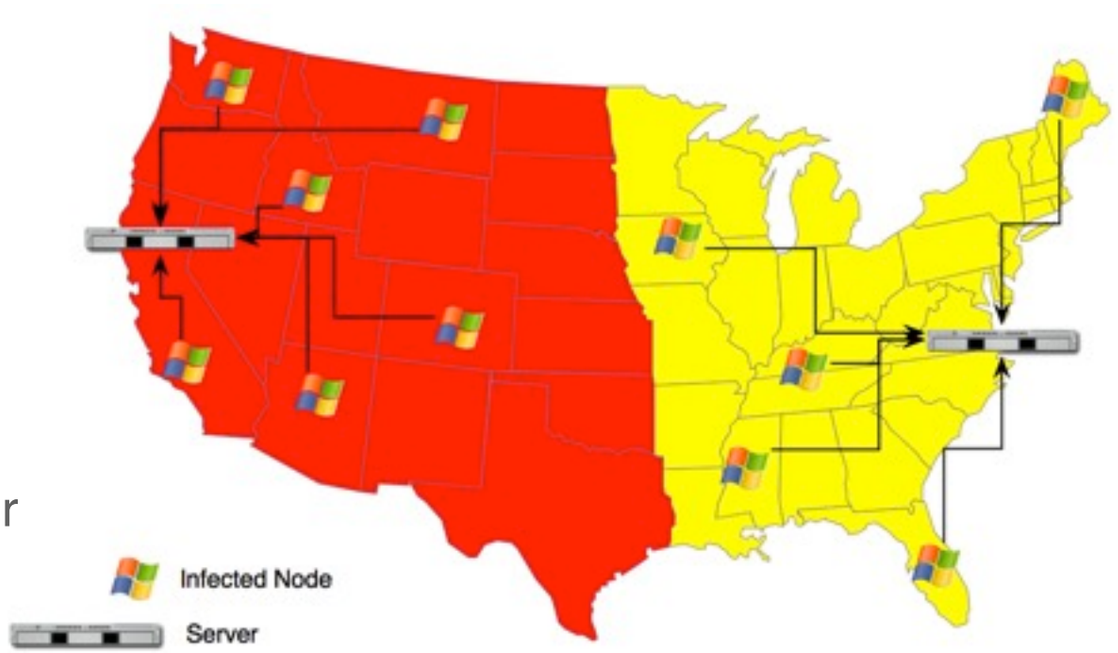


# Part 2: Enumerating Networks Today

## Directional DNS

**How is DNS Resolved (Source IP)**
When an authoritative DNS server gives a response for a fqdn, it may use the source ip address of the inbound query.

**How is DNS Resolved (BGP Anycast)**
More common, authoritative DNS servers may be announced via BGP Anycast. Clients will speak to the authoritative DNS server that is nearest to that client. Each BGP Anycast server will respond with different results.




**Problem**
You may not get the closest server to you

**Solution**
EDNS Client IP

# Part 3: EDNS Client IP

## Introduction

EDNS Client IP allows for the location based responses authoritative servers give to be based off of the client's location rather than the recursive DNS server's location.

# Part 3: EDNS Client IP

Where to find it, & Who's backing the draft?

http://tools.ietf.org/html/draft-vandergaast-edns-client-ip-01

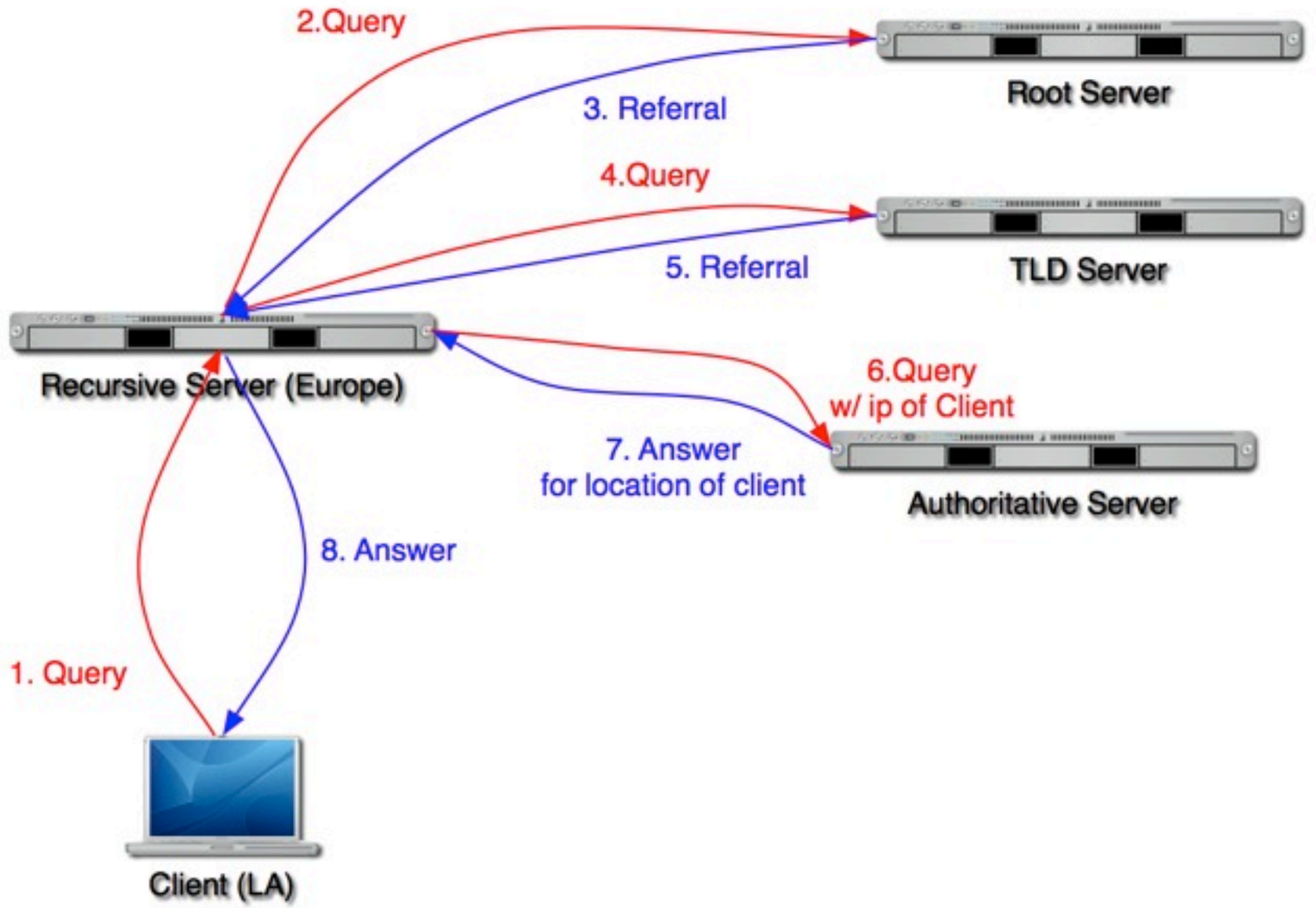

C. Contavalli & W. Van der gaast


D. Rodden


S. Leach

# Part 3: EDNS Client IP

## How Does DNS Work w/ EDNS Client IP?



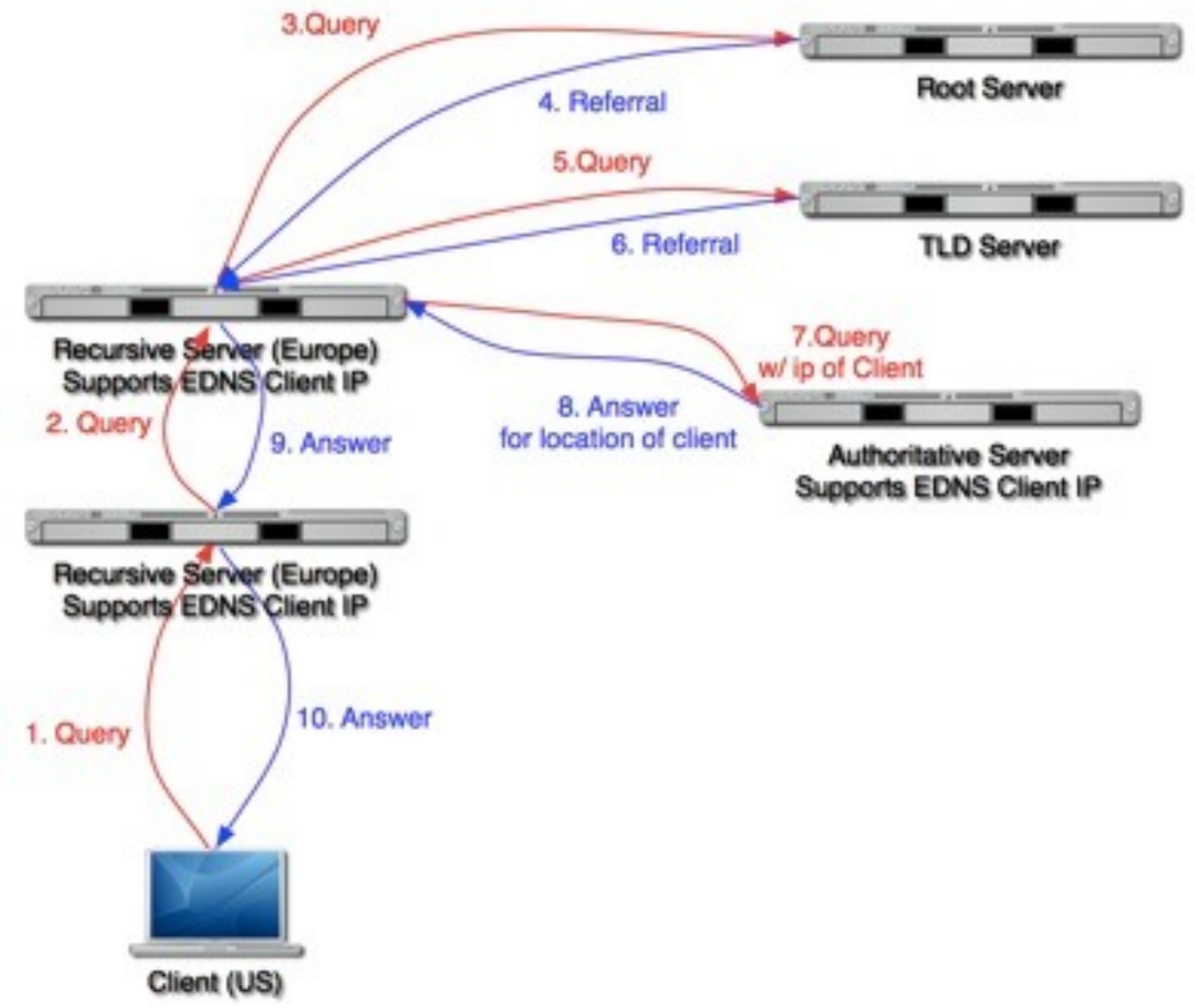
# Part 3: EDNS Client IP

## Cascaded Recursive Servers

"If an Intermediate Nameserver supporting edns-client-subnet receives a query that already has a valid edns-client-subnet option, this option MUST be passed through as-is and MUST NOT be modified."

**What does this mean?**
Recursive DNS Servers in tiered cascaded environments can pass edns client ip options.

**Network Enumeration?**
This makes network enumeration simple as you could query the recursive server for all network ranges.



# Part 3: EDNS Client IP

What does it do?

## Before

Authoritative name servers would base the resulting DNS Response off the location of the recursive DNS Server, when the recursive could be in a different geographic location than the client

## After

Recursive DNS Servers have the option to pass the originating source network of the client upstream to the Authoritative DNS Servers. This allows the DNS Server to make a more intelligent response providing a closer server to the client.

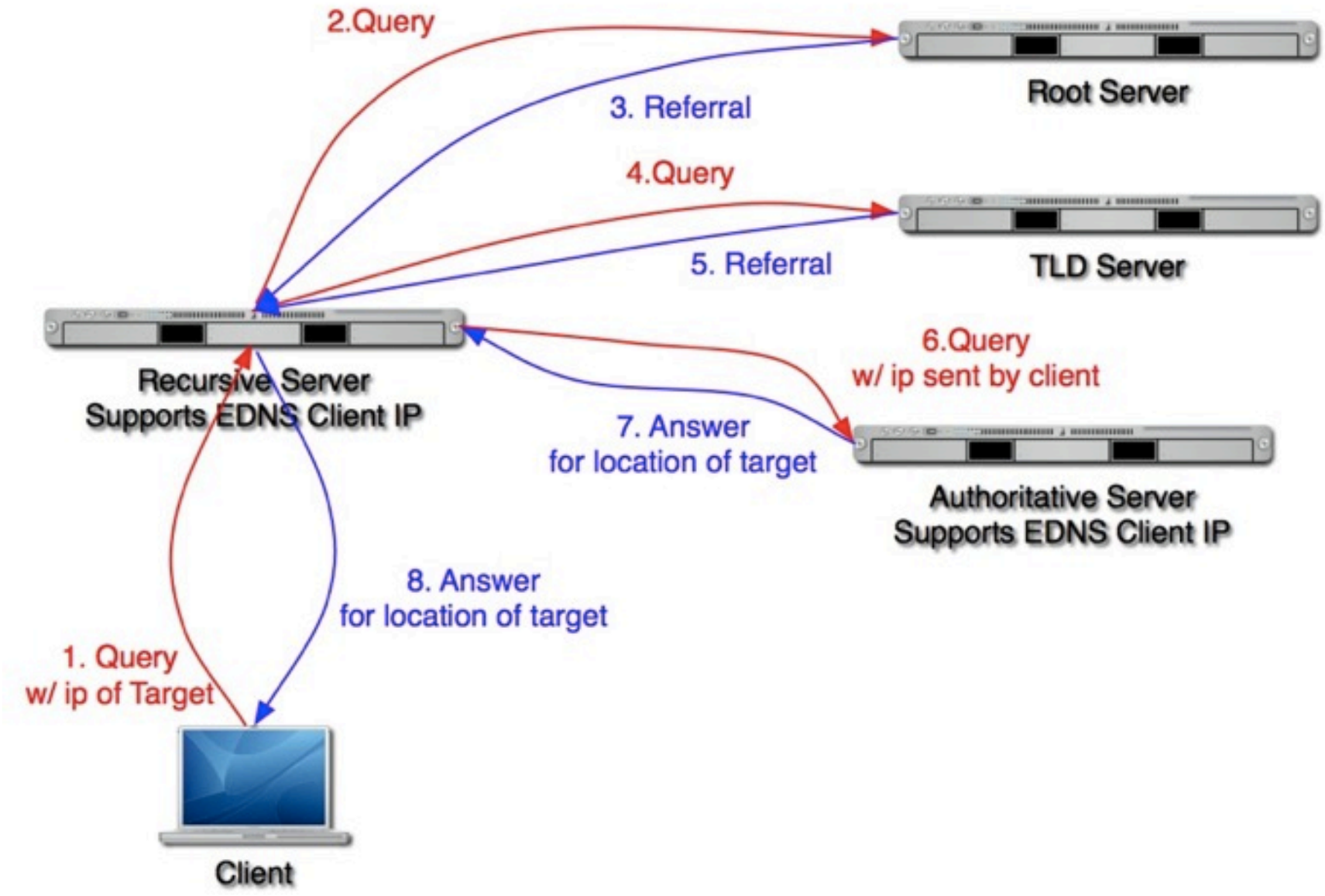
# Part 4: Using EDNS Client IP for a DDoS

## Introduction

Using EDNS Client IP, it will be possible to launch more geographically targeted attacks!

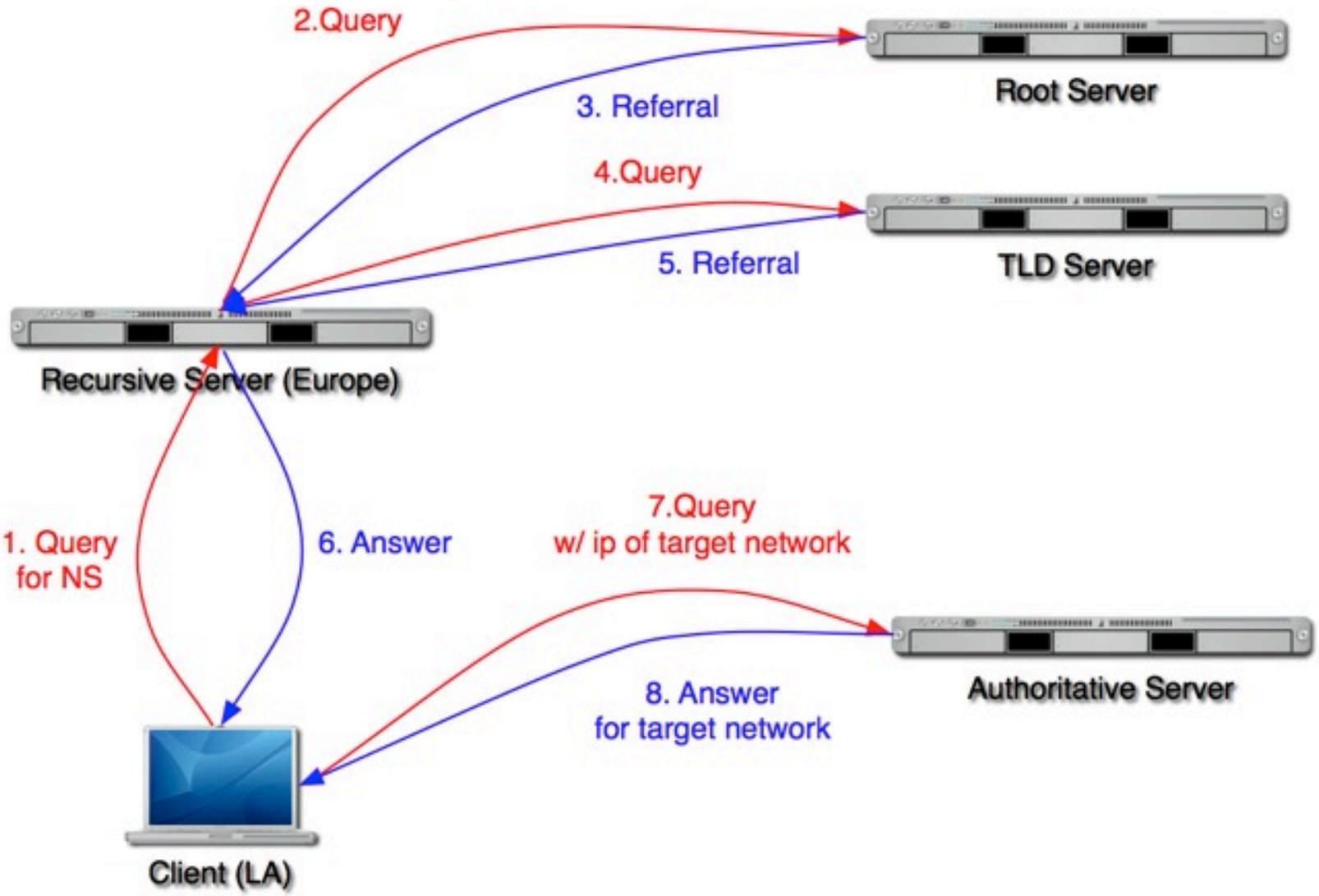
# Part 4: Using EDNS Client IP for a DDoS

## How does it work?



# Part 4: Using EDNS Client IP for a DDoS

## What if the recursive does not support edns-client-ip?



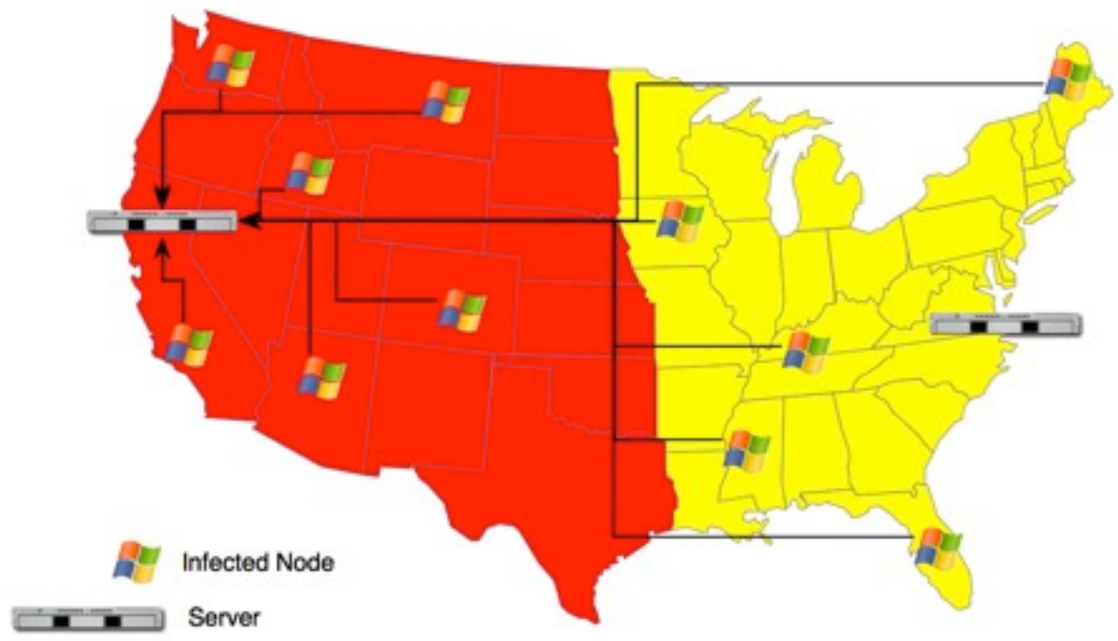
# Part 4: Using EDNS Client IP for a DDoS

## Why can't we do this today?

**Each bot would find a separate host.**

**What if we just attacked the IPs?**
We would have to constantly update the attacked ips as DNS Changes.

**What if we change the recursive server?**
There would be more of a single point of failure.



# Part 4: Using EDNS Client IP for a DDoS

## What does this mean?

**We can also enumerate the network!**

**How would we do this?**
Query the authoritative servers pretending to be a recursive server asking on behalf of many clients from different locations

# Part 5: Network Enumeration Tool

A Tool For Enumerating Networks

Our Network Enumerator tool will take the hard work out of enumerating  a network.

# Part 5: Network Enumeration Tool

## So what does it do?

**How do we enumerate directional services?**
We use our cache of known recursive servers in different geographic locations.

**How do we detect BGP Anycast?**
Query route servers

**Why did we develop this?**
There was not an existing looking glass for geographical DNS Lookups or network enumeration.

**Who is your daddy and what does he do?**
I'm a cop you idiot!

```
$ python enumerate.py --host=www.onzra.com
Found 1 IP Addresses
['216.240.35.194']

$ python enumerate.py --host=www.google.com
Found 2 IP Addresses
['66.102.7.104', '66.102.7.99']
This name is being launched using directional DNS (10 Networks found)
Network: ['66.102.7.104', '66.102.7.99']
Network: ['64.233.189.104']
Network: ['209.85.227.99', '209.85.227.103', '209.85.227.106', '209.85.227.104',
'209.85.227.105', '209.85.227.147']
Network: ['74.125.43.103', '74.125.43.104', '74.125.43.105', '74.125.43.106',
'74.125.43.147', '74.125.43.99']
Network: ['209.85.231.104']
Network: ['209.85.135.104', '209.85.135.105', '209.85.135.106', '209.85.135.103',
'209.85.135.99', '209.85.135.147']
Network: ['66.249.89.99', '66.249.89.104']
Network: ['72.14.254.104']
Network: ['74.125.47.99', '74.125.47.147', '74.125.47.104', '74.125.47.105',
'74.125.47.106', '74.125.47.103']
Network: ['209.85.229.104', '209.85.229.99', '209.85.229.147']

$ python enumerate.py --host=udns1.ultradns.net
Found 1 IP Addresses
['204.69.234.1']
IP: 204.69.234.1 is anycasted from at least 3 neighboring ASNs: 3549,7473,3741
```

NZRA

# Where to find the content?

**Latest Slides.**
http://www.ONZRA.com/research/whitepapers/

**Tool Downloads.**
http://www.ONZRA.com/research/products/

ONZRA

# Questions?

For additional help, find us at the bar