Protocol Deep Dive: DNS

EXPLORING DNS TERMINOLOGY AND USE CASES

Betty DuBois

PACKET DETECTIVE

@PacketDetective www.bettydubois.com

Module Goals

Describe the Purpose of DNS

Observe DNS Queries and Responses Using Wireshark

Discover Different Query Types Using Wireshark

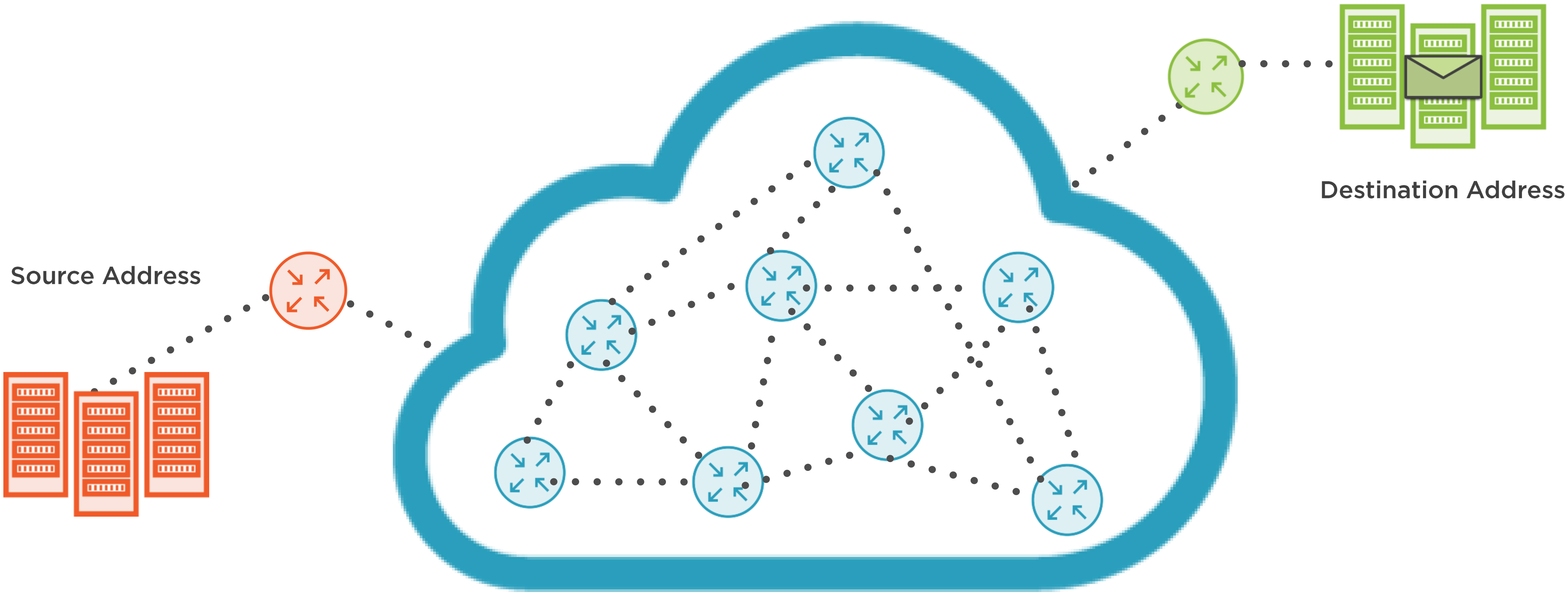
“Internet Grows to 370.1 Million Domain Name Registrations at the End of the Second Quarter of 2020”

www.BusinessWire.com

Why Do We Need DNS?

Human-Friendly Name	Machine-Friendly Numbers
dns.google.com	8.8.8.8
app.pluralsight.com	104.18.114.44
www.globomantics.com	52.88.138.56
linkedin.com	2620:109:c002::6cae:a0a

Routing Requires Addresses Not Names



<table>
<tr><td>Ethernet</td><td>IP4 or IP6
Source | Destination</td><td>TCP</td><td>TLS   DATA</td></tr>
</table>

Packet

Gabriela

GLOBOTICKET

A Globomantics Company

- Gabriela and a local server
- DNS query and response

DNS Query and Response - Local Server

A Salesperson Opens Application

DNS Query Sent

DNS Reply with Address

Demo

DNS query and reply

How to find just the one you want in Wireshark

DNS fields

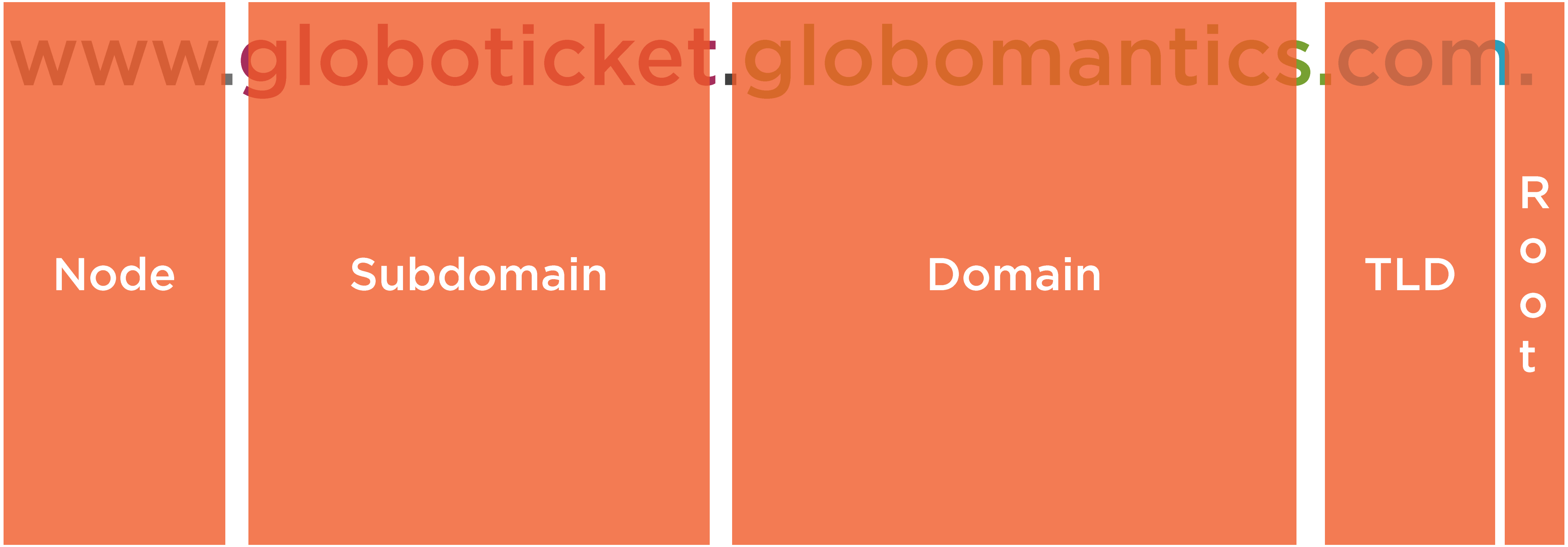
One DNS Database???

Back in the beginning of the Internet, yes. But there were also only 4 networks. Now it is a distributed database.

A Database of Records

Name/Node	Record Type	Address
dns.google.com	A (IP4)	8.8.8.8
app.pluralsight.com	A (IP4)	104.18.114.44
www.globomantics.com	A (IP4)	52.88.138.56
linkedin.com	AAAA (IP6)	2620:109:c002::6cae:a0a

Labels in a Domain Name



www.globoticket.globomantics.com.

Node

Subdomain

Domain

TLD

Root

Domain namespace - a distributed database

Domain namespace is divided into Zones

Root Domain

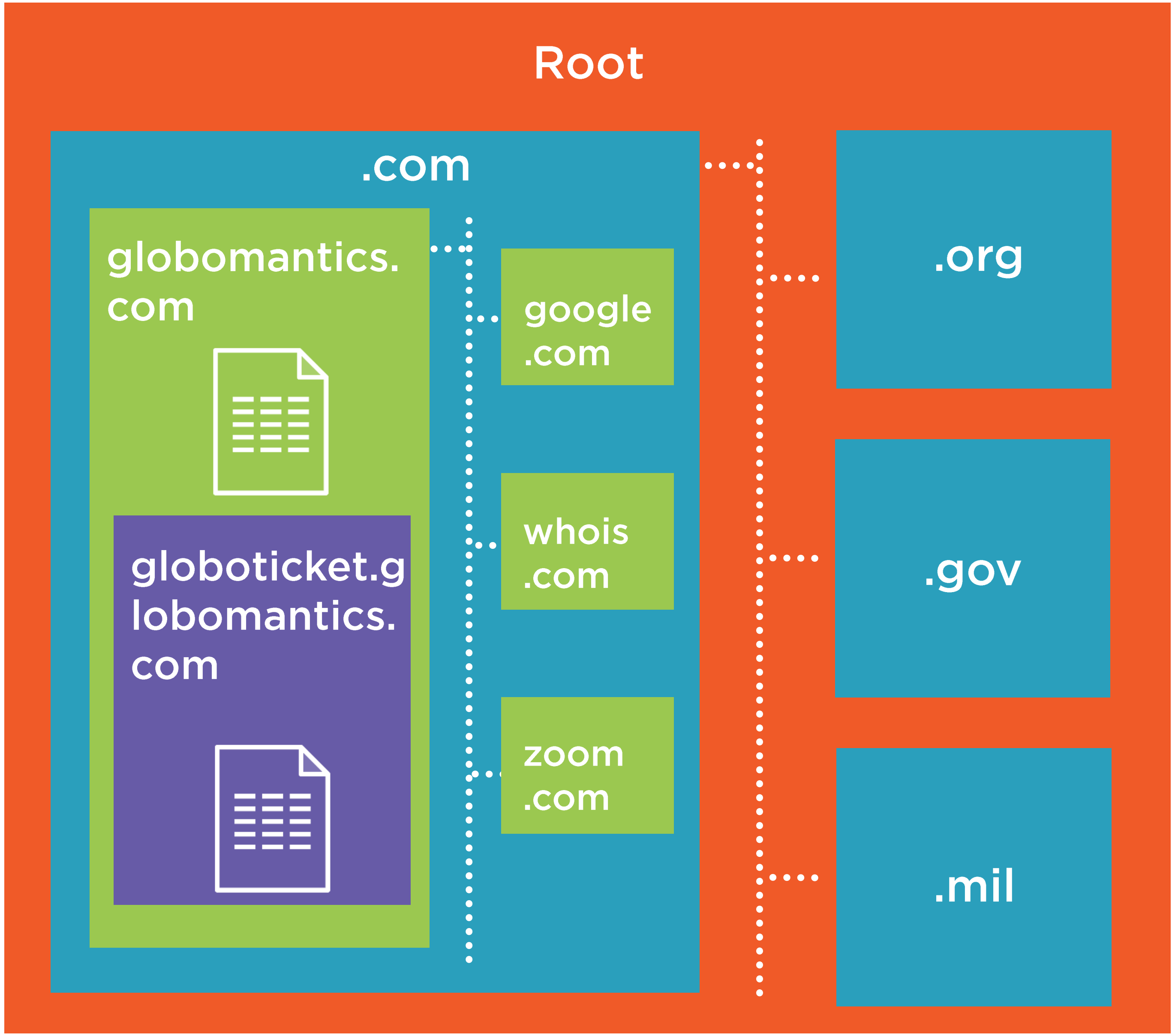
Top Level Domains (TLD)

Lower Level Domains

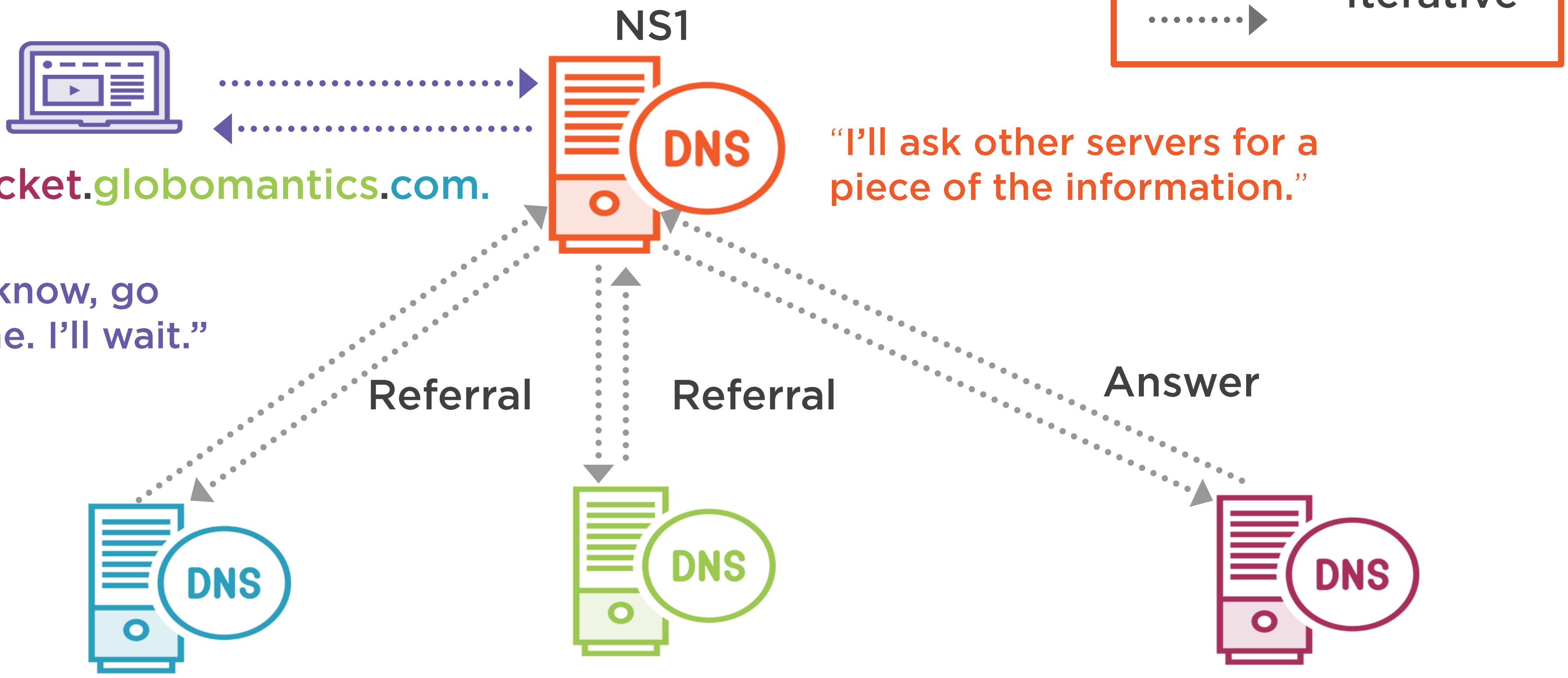
Records

Subdomains

Records



Query Types



"I'll ask other servers for a piece of the information."

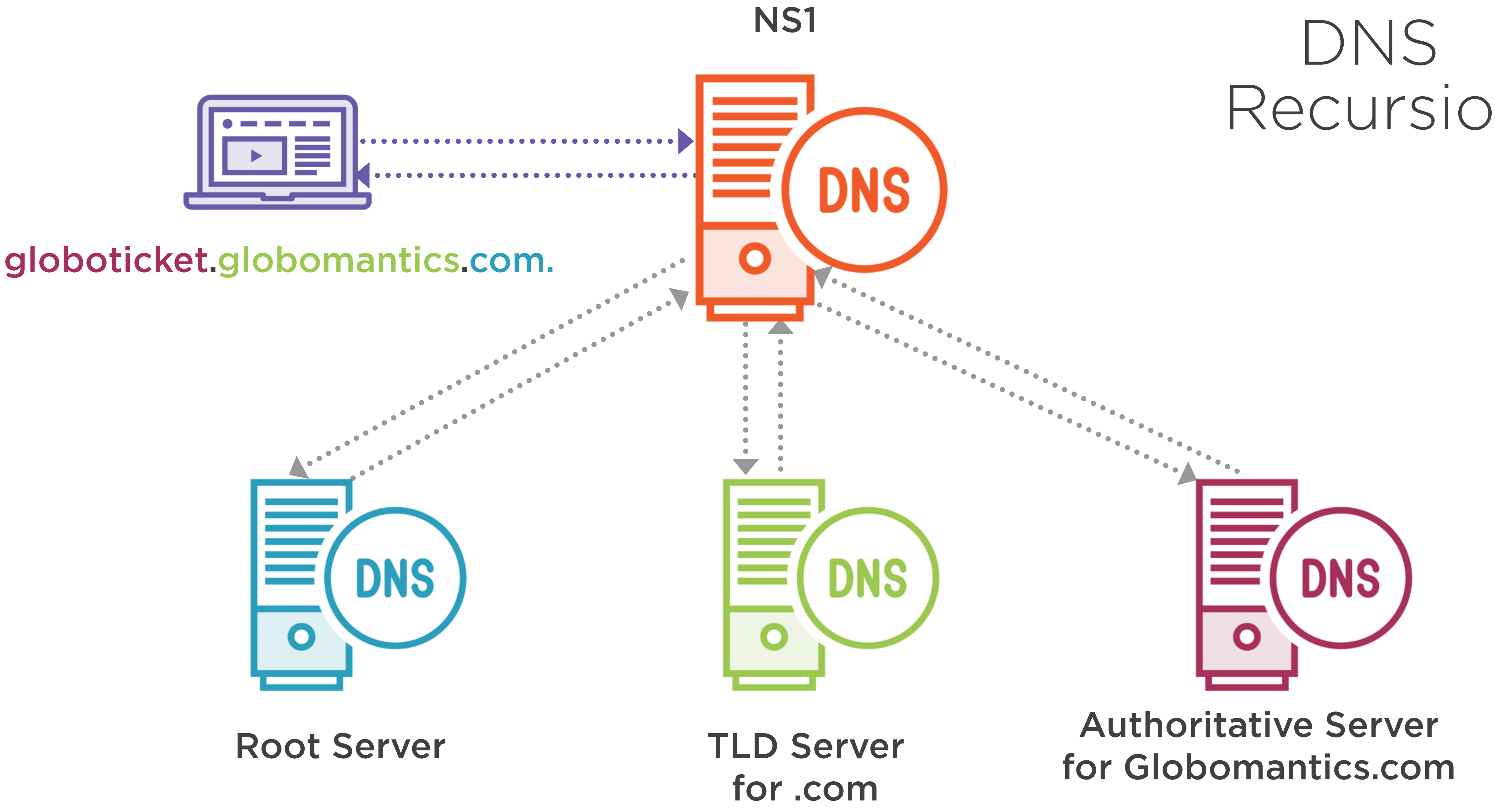
"If you don't know, go find out for me. I'll wait."

Root Server

TLD Server for .com

Authoritative Server for Globomantics.com

DNS Recursion


NS1
globoticket.globomantics.com.
DNS
DNS
DNS
DNS
Root Server
TLD Server for .com
Authoritative Server for Globomantics.com

Demo

Capture an iterative query at the client with Wireshark

Capture iterative and recursive queries at the server with dumpcap

Compare PCAPs using Wireshark

Summary

Filter to a single query/response

Minimize your footprint on the server by capturing at the command line

Use Wireshark to recognize both types of queries

Up Next:
Configuring DNS for Clients