Understand DNS Traffic Geographical Location Routing

Contents

Introduction

This document describes how to understand DNS Traffic Geographical Location Routing in Cisco Umbrella.

Prerequisites

Requirements

There are no specific requirements for this document.

Components Used

The information in this document is based on Cisco Umbrella.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Overview

Sometimes, you can notice your DNS traffic is being routed to a data center (DC) that is not the closest location to you. You also notice higher latency when being routed to one location versus another.

Umbrella utilizes anycast routing. Every data center announces the same IP addresses. BGP then takes care of the rest, routing requests transparently to the fastest available location.

When you configure your network to send DNS queries to 208.67.222.222 and 208.67.220.220, your DNS traffic could be routed through any of the locations listed on Umbrella's System Status page, depending on geographical distance, peering, congestion, and other measures. Umbrella represents its locations by their IATA 3-letter airport code.

Technical Details

Due to limited peering arrangements with some ISPs (mostly in China), the RTT (Round Trip Time) to the closest Cisco Umbrella data center depends on geographic location and connection type. For example, most customers within China are routed to Umbrella's Tokyo, Hong Kong, or Singapore locations.

Umbrella only provide DNS answers to your queries. The routing to the destination is handled by the paths between the ISP and the target host; Umbrella cannot control the route your traffic takes to reach our data centers. However, with careful peering arrangements, Umbrella can influence the route taken.

Checking Which DC Your DNS Traffic is Routed to

This information can be found by simply running a DNS query for a TXT record from which.opendns.com. This is a simplified return of the debug.opendns.com command which only returns data center locale information. For example:

```
nslookup -type=txt which.opendns.com.
```

Among the output, you want to look for a line similar to this:

```
which.opendns.com text = "m41.pao"
```

The response contains the resolver that responded to the query, including its location represented by its IATA 3-letter airport code. In this case, the server is `m41.pao`, which is in Palo Alto, USA, or "PAO".

See Umbrella's [System Status page](#) to see all of Umbrella's server locations. See List of airports by IATA code for a full list of IATA 3-letter airport codes.

Troubleshooting Latency

If your DNS traffic is being routed to a DC that is very far from your actual location and is causing a greater latency, it is possible that you are using a remote-access VPN. Try your queries again while disconnected from the VPN to confirm this is the case.

You can also find that your ISP has an actual egress point (geographical location where the traffic leaves their network to reach the "wider Internet") that is also nowhere near you. Some ISP's do this sort of thing in order to cut costs. You could live in the same town as one of Umbrella's DC's, but because your ISP is hitting the Internet from another city, the RTT to another of our DCs could be faster, and therefore that location would be used.

If you are experiencing location/latency problems and have ruled out VPNs, please contact Umbrella Support.