

Understand Cisco Umbrella Roaming Client Probes

Contents

[Introduction](#)

[Background Information](#)

[Details on Probes \(debug.opendns.com\)](#)

Introduction

This document describes the health checks performed by Umbrella roaming client uses to monitor changes in network and connectivity.

Background Information

The Cisco Umbrella roaming client performs relatively aggressive health checking to monitor for changes in network and DNS connectivity; this lets the Umbrella roaming client provide as seamless an experience as possible in dynamic network environments.

In router/firewall logs, you could notice a lot of packets being sent to debug.opendns.com. This is the domain used by the Umbrella roaming client to determine certain characteristics about DNS connectivity, and whether connectivity is possible over certain protocols and ports. See [Roaming Client Prerequisites](#) for more information.

Details on Probes (debug.opendns.com)

These health checks are referred to as "probes". These probes are performed every 10 seconds:

- Virtual Appliance Probe (for each DNS server specified in active network adapters)
- Protected Network Probe (for each DNS server specified in active network adapters)
- Encrypted Probe
- Transparent Probe

In a typical network, using two DNS servers supplied by DHCP, the Umbrella roaming client sends 2160 probes per hour.

Because the packets are so small and are using the UDP protocol, which has very low overhead, the traffic generated by the Umbrella roaming client probes is relatively insignificant; all in a day's work for UDP and DNS.

If you are running hundreds or thousands of Umbrella roaming clients on a single network, we recommend ensuring that the UDP timeout on your network is around 10-15 seconds. We have found that some networks employ a 30-60+ UDP timeout. This is much higher than typically expected between a host and destination for UDP packets.

Please contact Support with further inquiries.