

Understanding DistributedDirector DRP–RTT Metric

Document ID: 21969

Introduction

Prerequisites

- Requirements
- Components Used
- Conventions

Director Response Protocol

Director Response Protocol Round Trip Time Metric

- How Does DRP–RTT Work?

Common Issues with DRP–RTT

- RTT Query Mistaken for a Zone Transfer
- Firewalls

Related Information

Introduction

This document describes the function, purpose, and behavior of DistributedDirector's Direct Response Protocol–Round Trip Time metric (DRP–RTT).

Prerequisites

Requirements

Readers of this document should have knowledge of these topics:

- Cisco DistributedDirector product line or the DistributedDirector IOS feature
- DistributedDirector's DRP
- Domain Name System (DNS) functions

Components Used

The information in this document is based on these software and hardware versions:

- DistributedDirector software 11.1(18)IA and later.
- Director Response Protocol (DRP) server agent support (which is enabled on a Cisco router) is available in Cisco IOS® software Releases 11.3 and 11.3 T. Use of the DRP protocol in the DistributedDirector System Software Release 11.1(18)IA and later requires the use of the updated DRP agent support in routers with Cisco IOS Release 11.3(2)T and later.
- More DRP parameters were added in 12.1(5)T (**ip director drp retries** and **ip director drp timeout** commands).
- More DRP parameters were added in 12.2(4)T3 (**ip director drp rttprobe** command).

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, make sure that you understand the potential impact of any command.

Conventions

For more information on document conventions, refer to the Cisco Technical Tips Conventions.

Director Response Protocol

DRP is a query/response protocol used by the DistributedDirector to transmit metric information, such as routing topology and transmission delay, between designated DRP agents and requesting DNS servers. Using DRP, the DistributedDirector gathers routing metrics from specified DRP agents and maps the domain in question to the best physical server for that client based on the metric information.

DRP uses UDP port 1974 for both receiving and destination (reserved with IANA).

Director Response Protocol Round Trip Time Metric

The DRP–RTT metric is gathered by sending a DRP request to all DRP–associated routers, asking them for the round–trip time between themselves and the client, which refers to the DNS server. This metric is used to direct the client to the server that is likely to have a minimum link latency to the client.

How Does DRP–RTT Work?

The RTT probe is a TCP SYN–ACK sent from the DRP routers to the client's referring DNS server with the default source and destination port 53. This requires the target DNS server to send a TCP RST (as defined in TCP RFC #793). The time from when the SYN–ACK is sent and TCP reset is returned is measured in milliseconds and used as a metric to determine the closest server.

This design uses the connection oriented properties of TCP in effort to resolve to the destination IP address that has the lowest latency between the client and server. An ICMP echo request (ping) was not used here because of the inherent low–priority of ICMP traffic. In 12.2(4)T, however, the command **ip director drp rttprobe** was introduced to allow ICMP probes.

Common Issues with DRP–RTT

RTT Query Mistaken for a Zone Transfer

The DNS RFC states that in the event a DNS query exceeds the 512k UDP packet size limit, the server will reply to that request in UDP with the truncate bit set. Setting this bit will notify the referring DNS server to resend the original DNS request via TCP. Customers in the past have seen the TCP port 53 RTT probe coming from a DRP router and assumed that either the DRP agent was attempting to do a zone transfer, or that there is some attempt of security breach without understanding that this behavior is within the RFC standard.

Firewalls

While TCP RFC #793 states a TCP reset should be sent for unsolicited requests, some firewalls will prefer to drop unsolicited TCP packets. If there is a firewall between the querying DRP router and the requesting DNS server that drops the RTT probe, then this metric will not be able to provide an accurate metric.

Related Information

- **DistributedDirector Hardware Support**
 - **Cisco DistributedDirector Downloads** (registered customers only)
 - **Technical Support – Cisco Systems**
-

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2009 – 2010 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 30, 2006

Document ID: 21969
