catchpoint

Troubleshooting Network Protocols in a Complex Digital Environment

Introduction

As digital technology is being applied to more facets of society, the network is evolving. Cloud migration and the maturity of mobile technology has led to digital transformation and the Internet of Things. This growth has in turn led to greater focus and transformation of traditional networks. According to Gartner "digital business initiatives are more reliant on network connectivity, compared to traditional business, driving hypersensitivity toward network downtime."

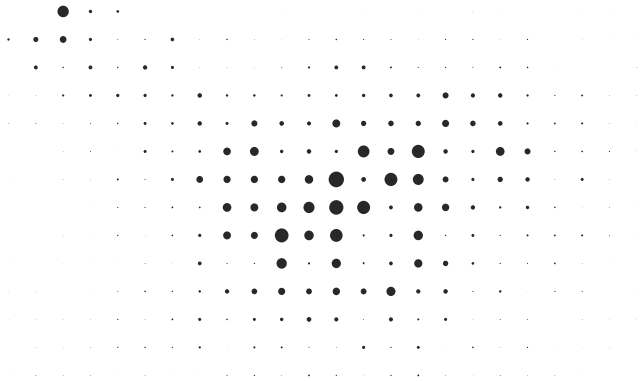
As network and infrastructure components play a vital role in application delivery it is more important than ever to manage and monitor the network. To ensure an application is available and responding within appropriate thresholds, these components need to be monitored.

Critical questions the network can help answer in regards to application performance include:

- Is a location reachable?
- How long does it take to reach a location?
- What is the path to reach a location?
- Can information be sent and received?
- Is the correct information being returned?

Monitoring only HTTP is not enough. Any protocol that is business critical should be monitored and that includes network protocols such as TCP, DNS, NTP and SSH. These are pieces that may be taken for granted but if something goes wrong there are serious implications to application performance and the digital experience.

As network infrastructures get more complex with multiple cloud vendors responsible for delivering a single application, the risks to the organization increases. Knowing how critical network components are performing is a key to delivering the best digital experience possible.



Route Health

Ping and Traceroute

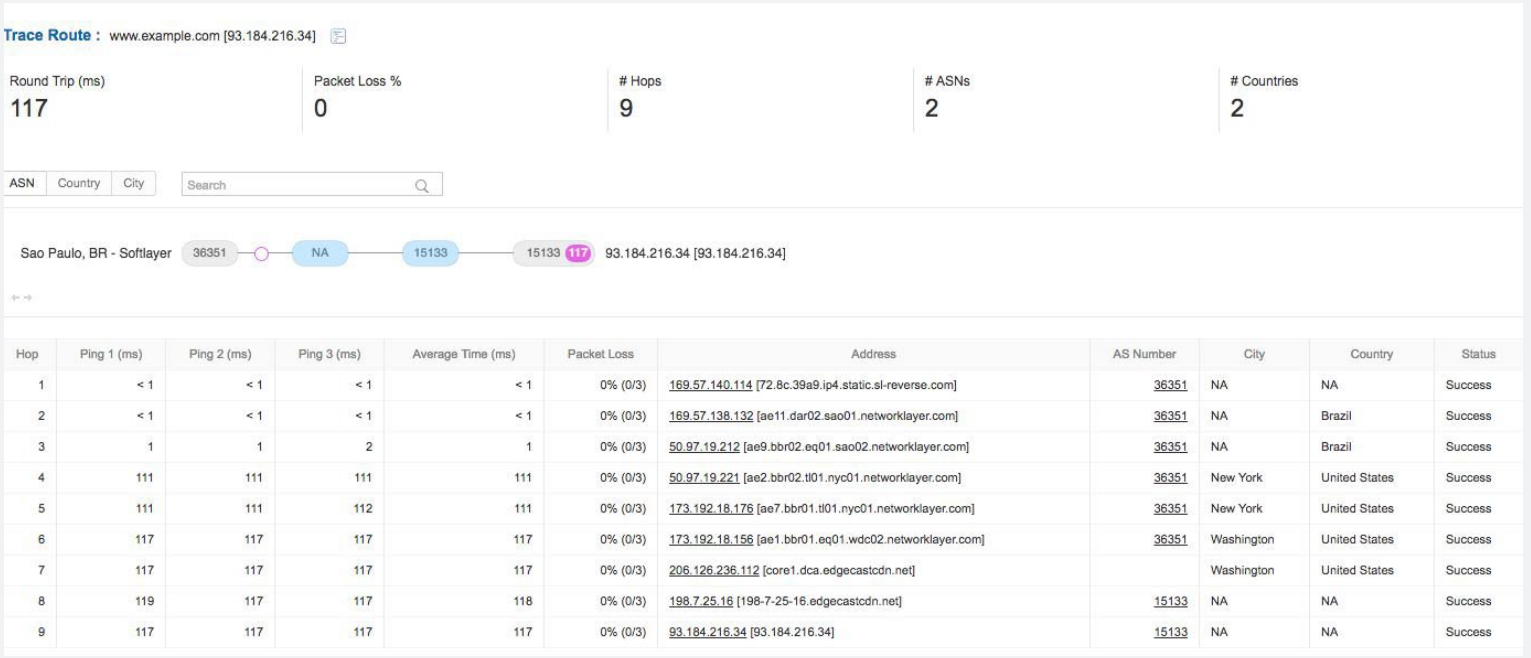
Ping and traceroute go hand in hand and are two of the most common tools used to troubleshoot network performance issues and measure latency. Latency is the measure of the time it takes to get from the sender to the server, typically measured in milliseconds. There are different factors that can influence how long it takes to reach a location such as distance, the quality of the network and transmission medium.

Ping tells us the round-trip time between the sender and server while traceroute shows us the path to get to the server. Ping measures round-trip latency by sending packets via Internet Control Message Protocol (ICMP), TCP or UDP. Ping is also used to test network connectivity by measuring packet loss between source and server. Any device with an IP address such as a router or a server can be tested with a ping.

Ping : www.example.com

Ping 1 (ms)	Ping 2 (ms)	Ping 3 (ms)	Ping 4 (ms)	Ping 5 (ms)	Average Time (ms)	Packet Loss	Address	Status
156	155	156	156	156	156	0% (0/5)	93.184.216.34 [www.example.com]	Success

Traceroute goes a step further than ping showing the path taken between the sender and the server and how long it takes to travel between the various hops. Knowing there is latency on the path is one thing, but knowing where the latency is occurring can help resolve problems faster.



Trace Route : www.example.com [93.184.216.34]

Round Trip (ms)	Packet Loss %	# Hops	# ASNs	# Countries
117	0	9	2	2

ASN | Country | City | Search

Sao Paulo, BR - Softlayer — 36351 — NA — 15133 — 15133 117 — 93.184.216.34 [93.184.216.34]

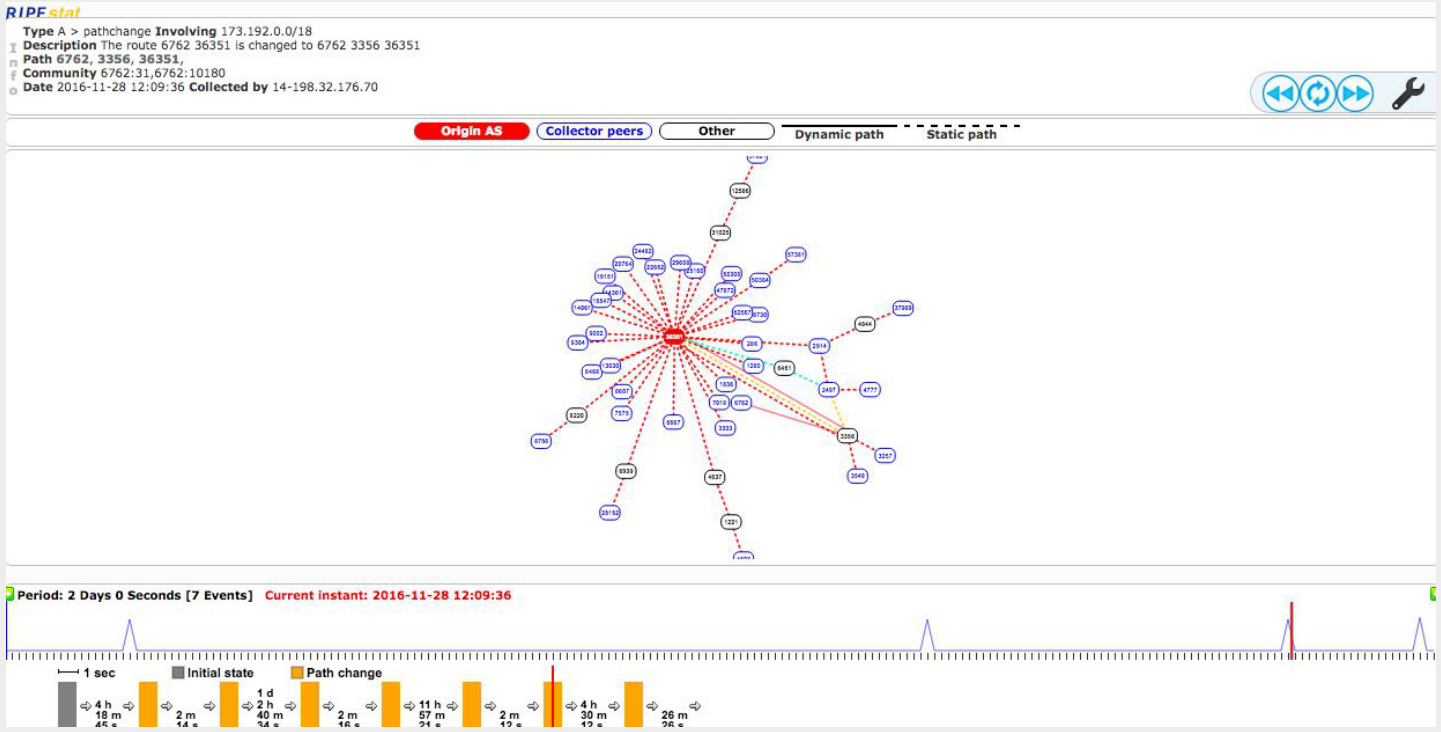
Hop	Ping 1 (ms)	Ping 2 (ms)	Ping 3 (ms)	Average Time (ms)	Packet Loss	Address	AS Number	City	Country	Status
1	< 1	< 1	< 1	< 1	0% (0/3)	169.57.140.114 [72.8c.39a9.ip4.static.sl-reverse.com]	36351	NA	NA	Success
2	< 1	< 1	< 1	< 1	0% (0/3)	169.57.138.132 [ae11.dar02.sao01.networklayer.com]	36351	NA	Brazil	Success
3	1	1	2	1	0% (0/3)	50.97.19.212 [ae9.bbr02.eq01.sao02.networklayer.com]	36351	NA	Brazil	Success
4	111	111	111	111	0% (0/3)	50.97.19.221 [ae2.bbr02.tl01.nyc01.networklayer.com]	36351	New York	United States	Success
5	111	111	112	111	0% (0/3)	173.192.18.176 [ae7.bbr01.tl01.nyc01.networklayer.com]	36351	New York	United States	Success
6	117	117	117	117	0% (0/3)	173.192.18.156 [ae1.bbr01.eq01.wdc02.networklayer.com]	36351	Washington	United States	Success
7	117	117	117	117	0% (0/3)	206.126.236.112 [core1.dca.edgecastcdn.net]		Washington	United States	Success
8	119	117	117	118	0% (0/3)	198.7.25.16 [198-7-25-16.edgecastcdn.net]	15133	NA	NA	Success
9	117	117	117	117	0% (0/3)	93.184.216.34 [93.184.216.34]	15133	NA	NA	Success

Within Catchpoint, ping and traceroute can be enabled to run automatically on test failures. They do not provide in-depth analysis into the performance of an application but can help identify or rule out issues on the network.

BGP

Border Gateway Protocol (BGP) is a standardized gateway protocol to exchange data and routing information among autonomous systems (AS) on the internet. The data collected guides routing decisions across the internet, typically by choosing the shortest path. A BGP misconfiguration can cause availability and performance issues.

BGP routing information and visualizations are available from Traceroute tests in Catchpoint through a partnership with RIPEstat. If packets are dropping, BGP information can be used to gain insight into whether the issue was caused by a peering change, route flapping, or route hijacking.

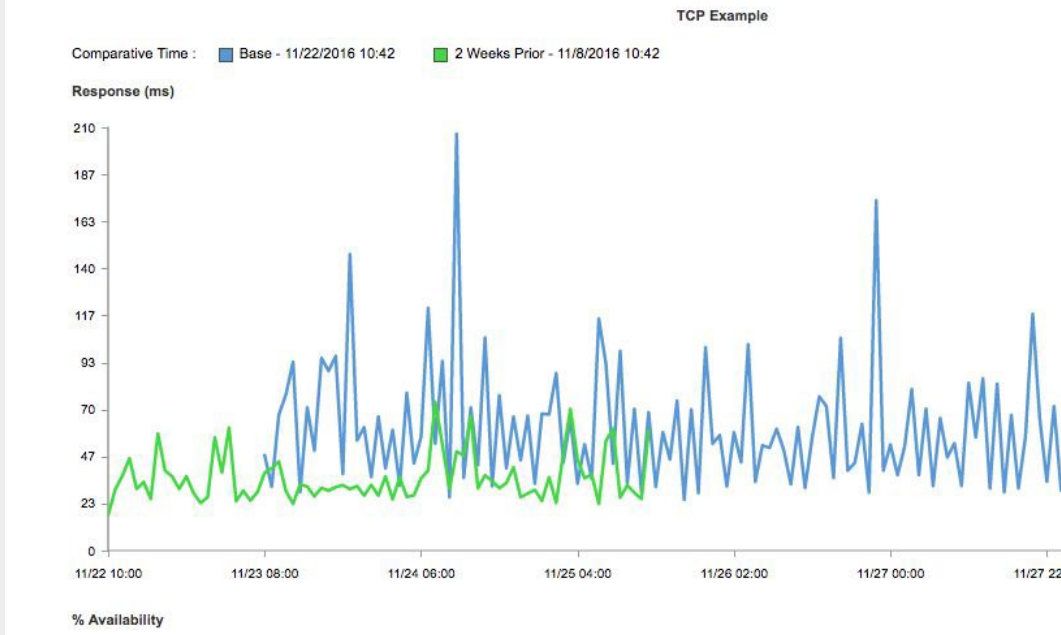


Connectivity

TCP

Once we know the route is healthy and the host is reachable, the next step is determining whether information can be transferred back and forth between the two end points. TCP is the transport protocol used to relay information reliably between two end points. Before information can be sent or received there needs to be an agreement between the client and the server. This agreement is established during the TCP connection and is also referred to as a 3-way handshake.

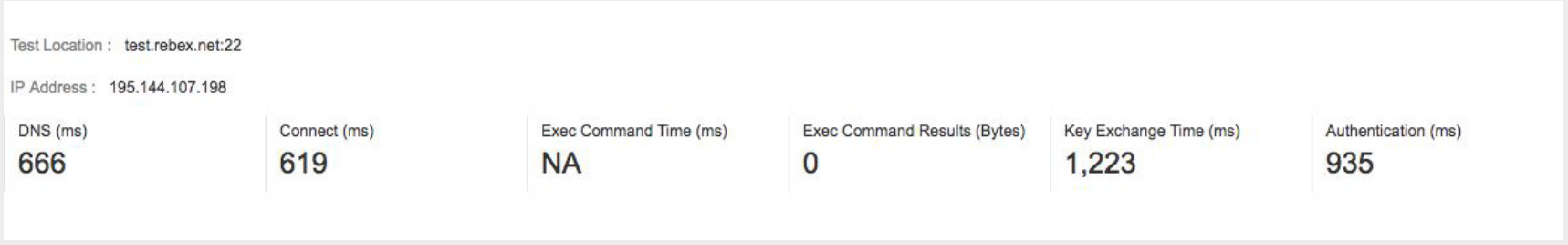
In addition to TCP data being available in web and transaction tests, a TCP monitor can be set up in Catchpoint to test the performance and availability of a connection to a given host and port. When a failure occurs on a TCP test additional troubleshooting tools are available to verify a failure or collect debugging information.



SSH

Secure Shell (SSH) is a protocol used to securely perform network services over an unsecured network. It is frequently used to login to a computer remotely to perform actions on the system.

The SSH monitor connects to and runs shell commands to measure performance of a server.

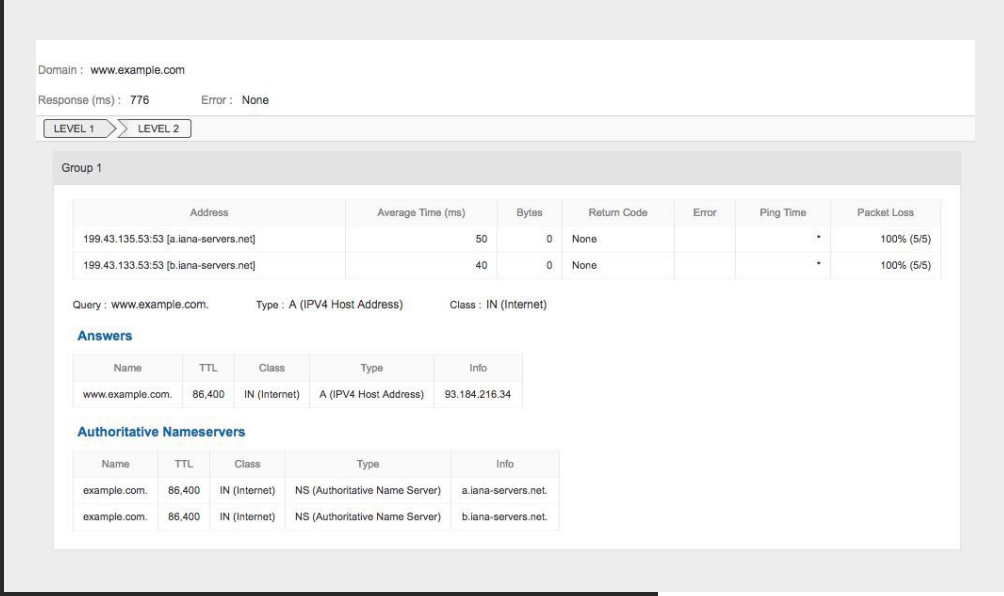


DNS

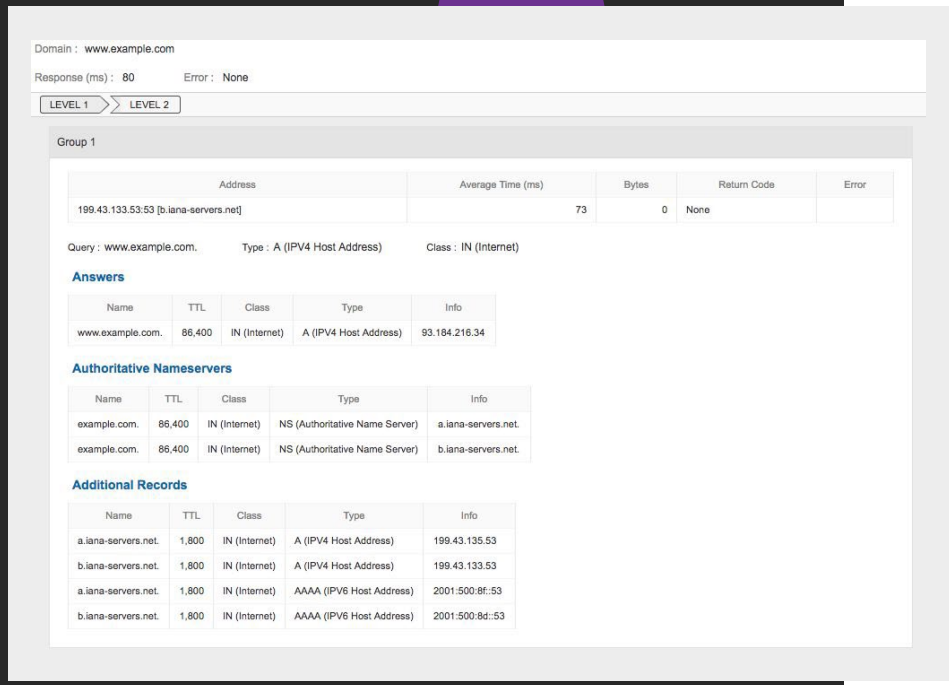
Translating domains into IP addresses is a key component of application delivery. Without DNS, a device has no way of knowing where to go to get the information they need. DNS is a multi-layered service, a fault at any layer results in poor performing or inaccessible applications. Determining whether the fault is with the end user's ISP, a third-party DNS resolver, the root servers, the top-level DNS servers, or the authoritative servers requires appropriate diagnostic tools.

Running synthetic and instant tests can reveal and pinpoint issues with DNS performance. Catchpoint offers three types of DNS tests to identify where problems are: Direct DNS, Experience DNS or DNS traversal tests.

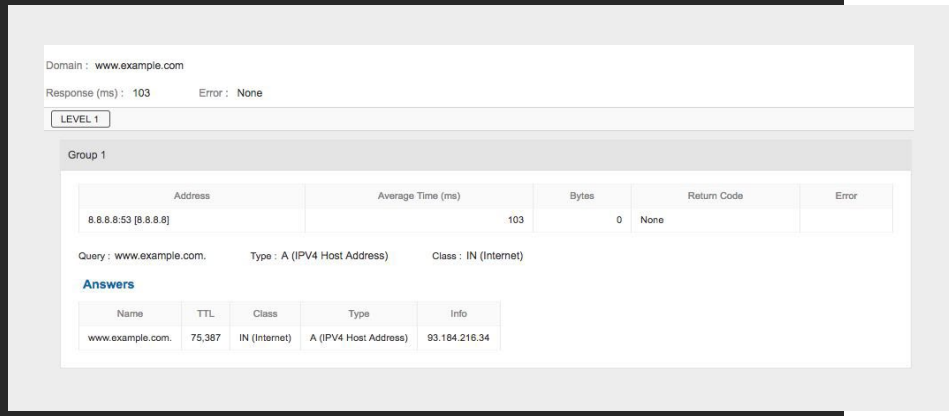
DNS Traversal tests should be used when you see a RUM or synthetic measurement with increased DNS times but all other metrics are fine. Traversal tests query each server in the DNS route to identify the source of failure or performance issue. If results indicate the issue is related to a single or a few servers, move onto a DNS Direct test.



DNS traversal tests are only available for instant tests and should be used to debug and isolate issues seen in DNS experience or other synthetic tests.

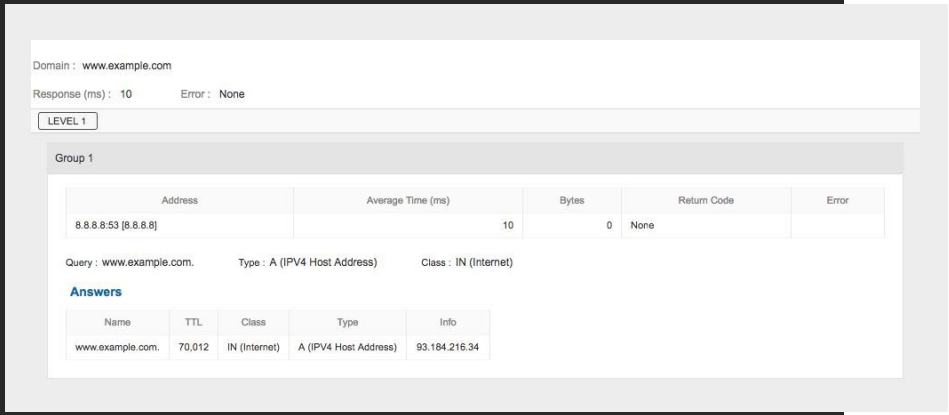


DNS Experience tests simulate how users will resolve DNS from their devices. Tests are executed against randomly selected servers from each level of the DNS route. The availability, response time and validity of the response is tested to protect organizations from DNS Cache Poisoning. Multiple requests are issued in succession to reveal whether a problem is related to all name servers or isolated to one. If results indicate the issue is related to a single or a few servers, move onto a DNS Direct test.

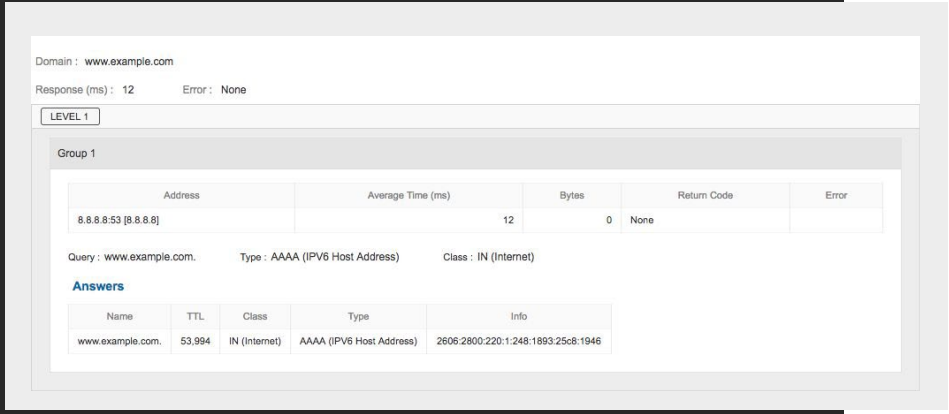


DNS Direct tests are executed from an individual DNS resolver either by IP address or domain name. They can also be used to test third party resolvers such as Google's public DNS resolver to ensure settings are consistent.

IPv4



IPv6



IPv4 vs IPv6

There are currently two versions of the Internet Protocol (IP) to identify devices: IPv4 and IPv6. IPv4 uses a 32-bit addressing scheme which equals about 4 billion unique IP addresses. As the internet grew in popularity, it became apparent the available pool of IPv4 addresses would be exhausted which led to the creation of IPv6. IPV6 is a 128-bit hexadecimal address separated by colons. IPv4 and IPv6 address co-exist, for example the domain www.example.com has both an IPv4 **(93.184.216.34)** and an IPv6 **(2606:2800:220:1:248:1893:25c8:1946)** address.

The need to support both IPv4 and IPv6 complicates DNS testing as you need to ensure DNS resolution is occurring successfully for both protocols. DNS tests can be configured to test over either IPv4 or IPv6.

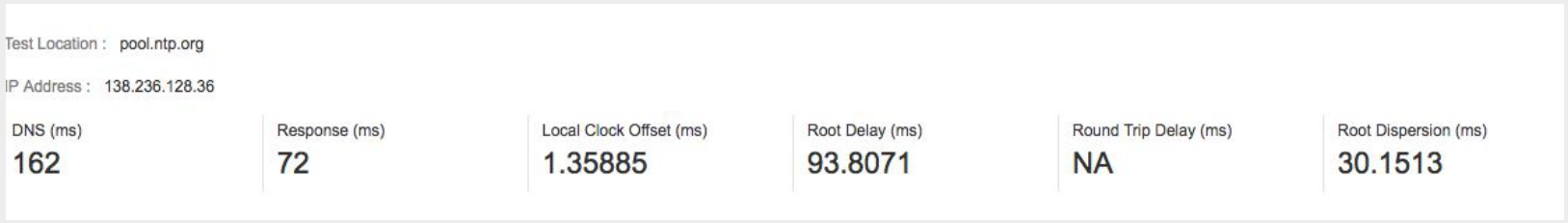
Alerts

Record validation can be applied to DNS alerts to not only ensure that thresholds aren't being passed but that the correct information is being returned. Alerts can detect DNS poisoning, ensure TTL policies are adhered to, and determine if IPv6 resolution is working correctly. Being notified to DNS errors in a timely fashion can help organizations resolve issues before they impact end users.

NTP

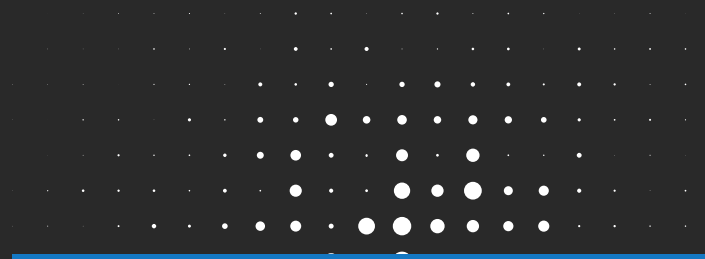
Network Time Protocol (NTP) is a mechanism used to synchronize computer clocks to common reference clocks throughout the Internet or within a private network. Poor time synchronization can impact routing, caching, security, financial transactions, and the ability for users to log-in.

NTP monitors provide response time measurements, delays, errors, and clock offsets to ensure reliable service and prevent issues. These can be used to test the availability of a given NTP server, as well as determine the relative performance and time variations to the reference clock.



A Different Approach to Digital Experience Monitoring

Catchpoint is a leading digital experience intelligence company that provides unparalleled insight into your customer-critical services to help you consistently deliver amazing digital experiences. Catchpoint is the only performance digital experience monitoring platform that provides integrated synthetic and real user monitoring, comprehensive test types, real-time analytics, and a diverse node network to help you continuously preempt performance issues and optimize service delivery. More than 400 customers in over 30 countries trust Catchpoint to strengthen their brands and grow their businesses.



16 Smart Monitors

Real browser, multi-transaction, HTML code, API, streaming, DNS, FTP, TCP, SMTP, ping, trace route, SSH, NTP, IMAP and web socket

Deepest and broadest diagnostics: 100 days of object level data; 3 years of raw aggregate data.

About Catchpoint

Catchpoint is the Internet Resilience Company™. The top online retailers, Global2000, CDNs, cloud service providers, and xSPs in the world rely on Catchpoint to increase their resilience by catching any issues in the Internet Stack before they impact their business. Catchpoint's Internet Performance Monitoring (IPM) suite offers synthetics, RUM, performance optimization, high fidelity data and flexible visualizations with advanced analytics. It leverages thousands of global vantage points (including inside wireless networks, BGP, backbone, last mile, endpoint, enterprise, ISPs and more) to provide unparalleled observability into anything that impacts your customers, workforce, networks, website performance, applications and APIs.

catchpoint