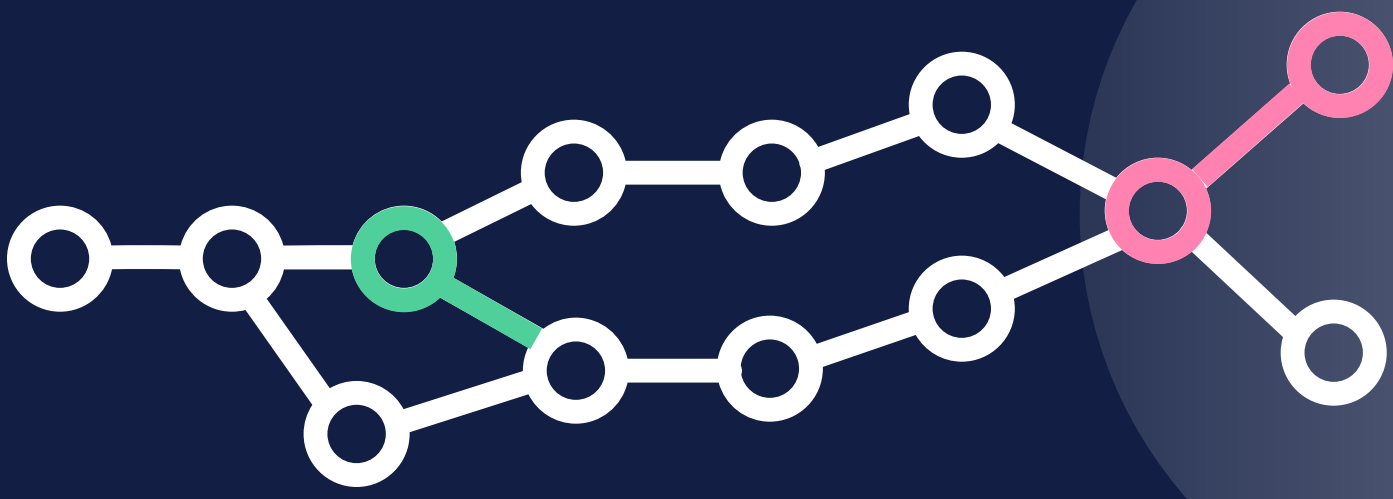
Monitoring Network Protocols

HANDBOOK



catchpoint™

Network performance is one of the biggest impediments to ensuring great end-user experiences online. The availability and performance of internet protocols such as BGP, DNS, TCP, NTP, and SSH can all affect business's bottom one. Unfortunately, these pieces are often taken for granted, and as a result, there are serious implications to application performance and digital experiences when something goes wrong.

To meet the increasing complexity of multi-cloud environments, Network Operations Centers must have visibility into the different network layers in order to proactively manage and monitor its health. Knowing how critical network components are performing is a key to delivering the best possible digital experiences. Critical questions the network can help answer with regard 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?

ROUTE HEALTH

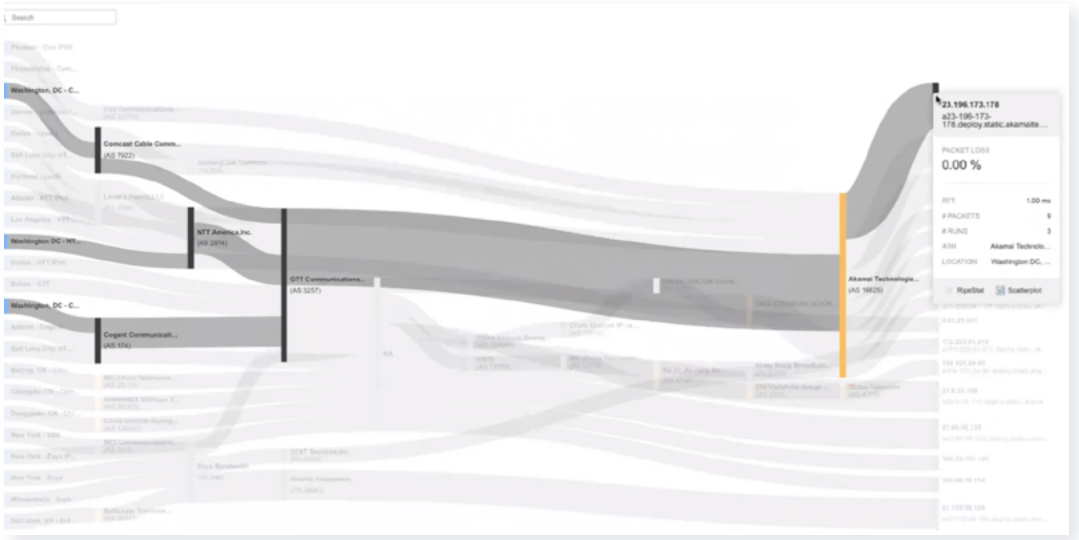
Ping & Traceroute

Ping and Traceroute go hand in hand and are two of the most common tools used to troubleshoot network performance issues by recording the path and measuring latency. Any device with an IP address such as a router or a server can be tested with a ping. Ping is often used to test network connectivity by measuring the behavior of a few packets between the source and destination host. These packets can be sent using Internet Control Message Protocol (ICMP), Transmission Control Protocl (TCP), or User Datagram Protocol (UDP). Additionally, Ping measures round trip time (RTT)—the time it takes to send and receive a single packet between two hosts—which can give an indication of the distance between the client and server, and the quality of the network.

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

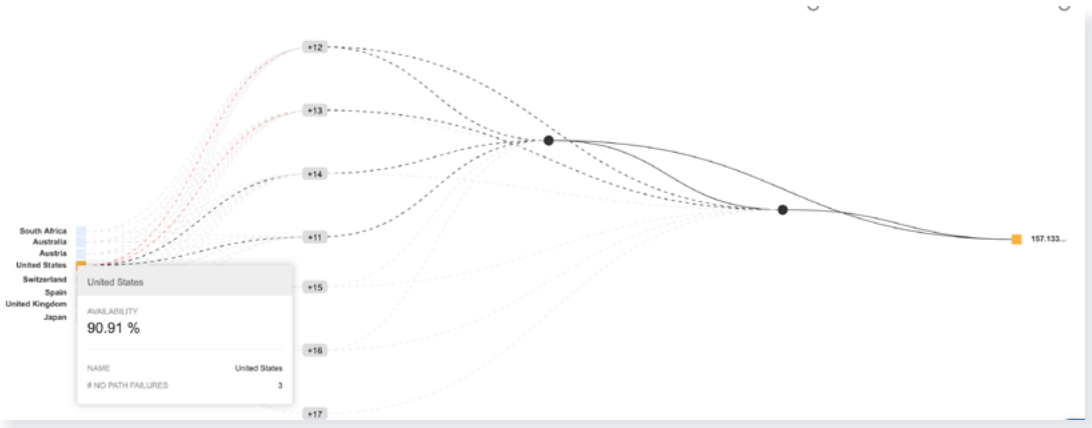
Ping provides basic information on the latency and availability between two hosts. Traceroute goes a step further by highlighting the physical path taken, providing detail on the time it took for the packets of data to travel between each router (or "hop") along the way. Knowing there is loss or latency on the path is one thing, but knowing where the issue is occurring can help resolve problems faster. The Catchpoint platform collects data from every hop and visualizes it in both logical autonomous system (AS) Sankey diagrams, as well as IP/hop-by-hop views, providing visibility into the health of every router in the network path.



Within Catchpoint, both Ping and Traceroute can be run as standalone tests, or alongside other Layer 4+ tests, such as web browser, web transaction, API, DNS, websocket, HTML, FTP, SMTP, and more. You can also test via the various protocols like ICMP, TCP, and UDP. Each tool can also be enabled to run automatically on test failures.

BGP

Border Gateway Protocol (BGP) is a standardized gateway protocol to exchange data and routing information between neighboring AS's on the internet. The data collected guides routing decisions across the internet, choosing its path using the "BGP Best Path" selection algorithm. A change in BGP routes – either due to misconfigurations, route leaks due to improper filtering, or malicious route hijacks – can cause availability and performance issues.

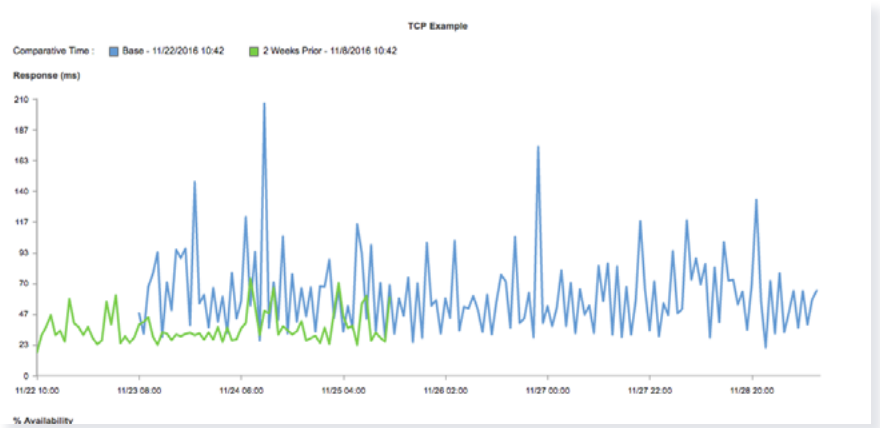


BGP routing information and visualizations are available as a standalone monitor within Catchpoint. If packets are dropping, BGP information can be used to gain insight into whether the issue was caused by a peering change, a route flap, or a route hijack.

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 source and destination. This agreement is established during the TCP connection and is referred to as the TCP 3-way handshake. It can be measured using the 'Connect' metric inside the Catchpoint analytics platform.



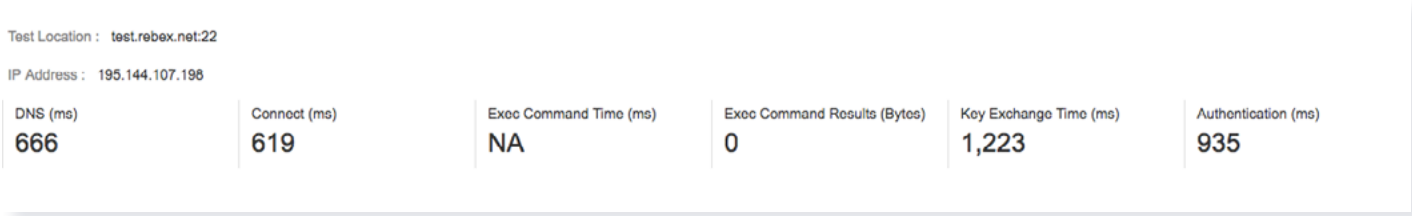
In addition to TCP data being available in web and transaction tests, a TCP monitor can be set up in Catchpoint to test the performance and availability of a connection to a given host and port. When a failure occurs on a TCP test, additional troubleshooting tools are available to verify the failure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

MQTT

As the prevalence of IoT devices increases, so do does the need for monitoring the Message Queuing Telemetry Transport (MQTT) protocol, which sits on top of the TCP/IP protocol and is used for Machine-to-Machine (M2M) communication. MQTT tests are available as a standalone monitor within Catchpoint, where they assess the performance and availability of IoT devices by measuring the time it takes for communications to be sent and received by different devices.

SSH

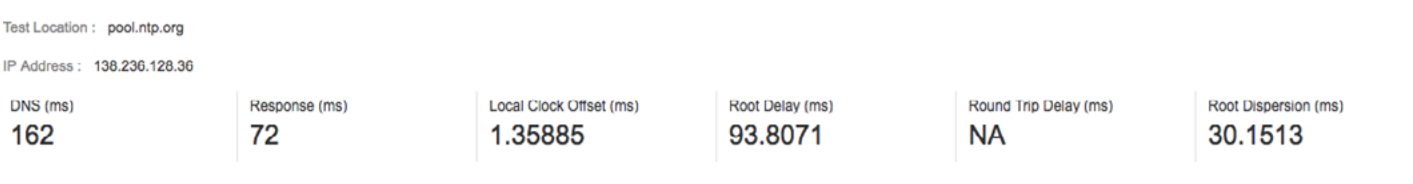
Secure Shell (SSH) is a protocol used to securely perform network services over an unsecured network. It is frequently used to login to a computer remotely to perform actions on the system. The SSH monitor connects to and runs shell commands to gather performance telemetry from a server.



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.

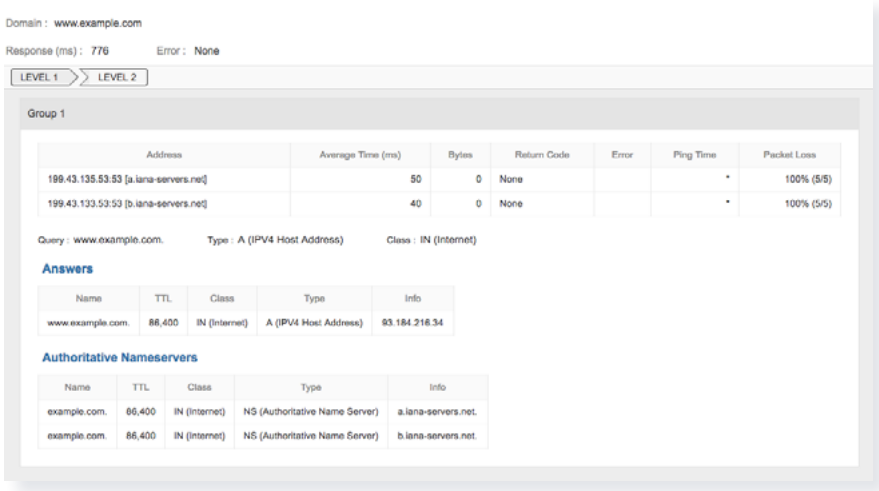
NTP monitors provide response time measurements, delays, errors, and clock offsets to ensure reliable service and prevent issues. These can be used to test the availability of a given NTP server, as well as determine the relative performance and time variations to the reference clock.



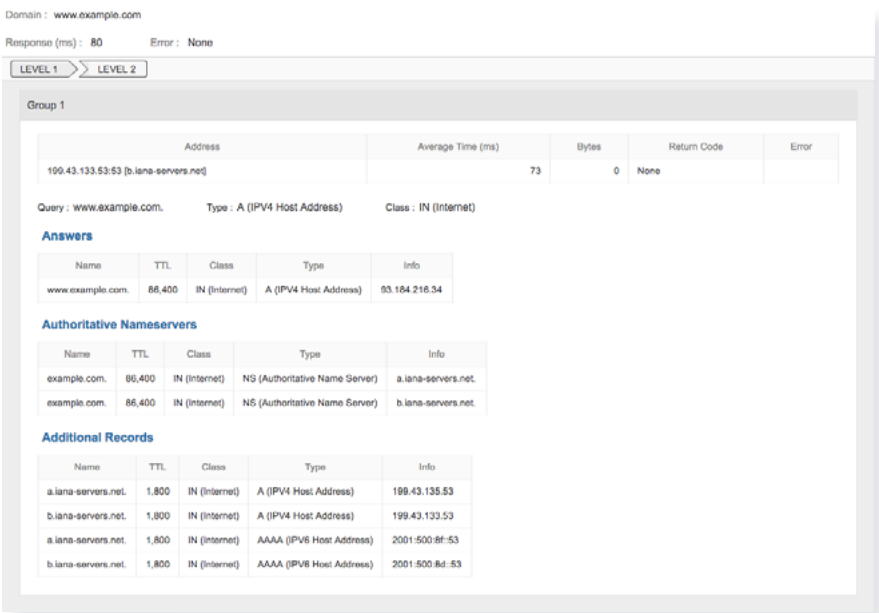
DNS

Translating domains into IP addresses is a key component of application delivery. Without the Domain Name System (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 local ISP resolver, a third-party resolver, the root servers, a generic top-level domain server, or the authoritative servers require appropriate diagnostic tools.

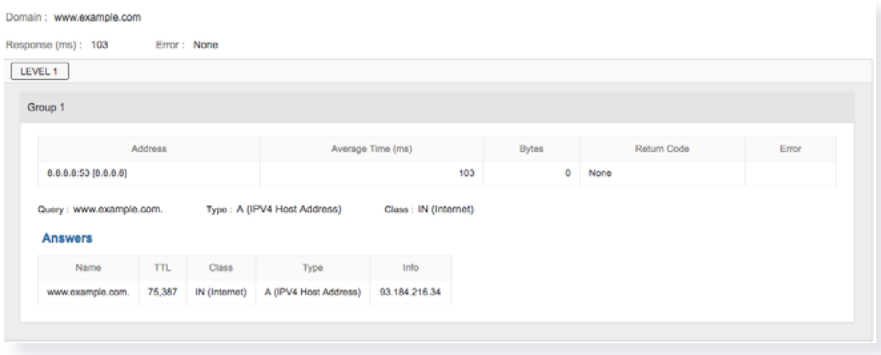
Running synthetic and instant tests can reveal and pinpoint issues with DNS performance. Catchpoint offers three types of DNS tests to identify where problems are: Direct DNS, Experience DNS or DNS traversal tests.



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 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.



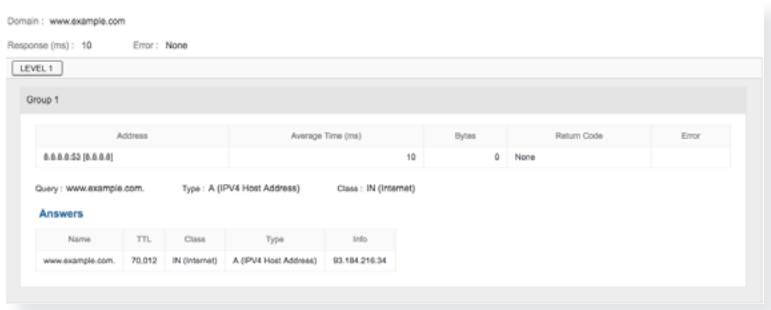
DNS Direct tests are executed from an individual DNS resolver either by IP address or domain name. They can also be used to test third party resolvers such as Google's public DNS resolver to ensure settings are consistent.

IPv4 vs. IPv6

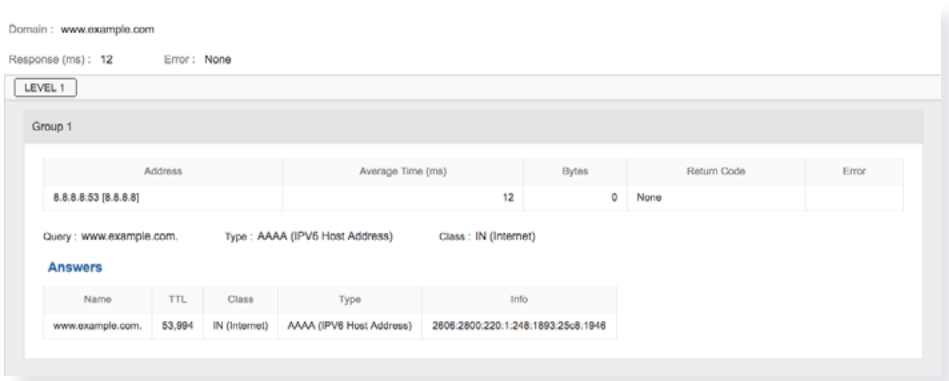
There are currently two versions of the Internet Protocol (IP) to identify devices; IPv4 and IPv6. IPv4 uses a 32-bit addressing scheme, which equals about 4 billion unique IP addresses. As the internet grew in popularity, it became apparent the available pool of IPv4 addresses would be exhausted, which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

IPv4



IPv6



Alerts

One of the most critical part of any synthetic monitoring strategy is the alerting capability of the various tests that you have running at any given time. Catchpoint provides advanced alerting options across different test types, including the various network monitors like DNS, BGP, Traceroute, etc. Being notified to errors in the DNS resolution, BGP route paths, and host failures in a timely fashion can help organizations resolve issues before they impact end users.