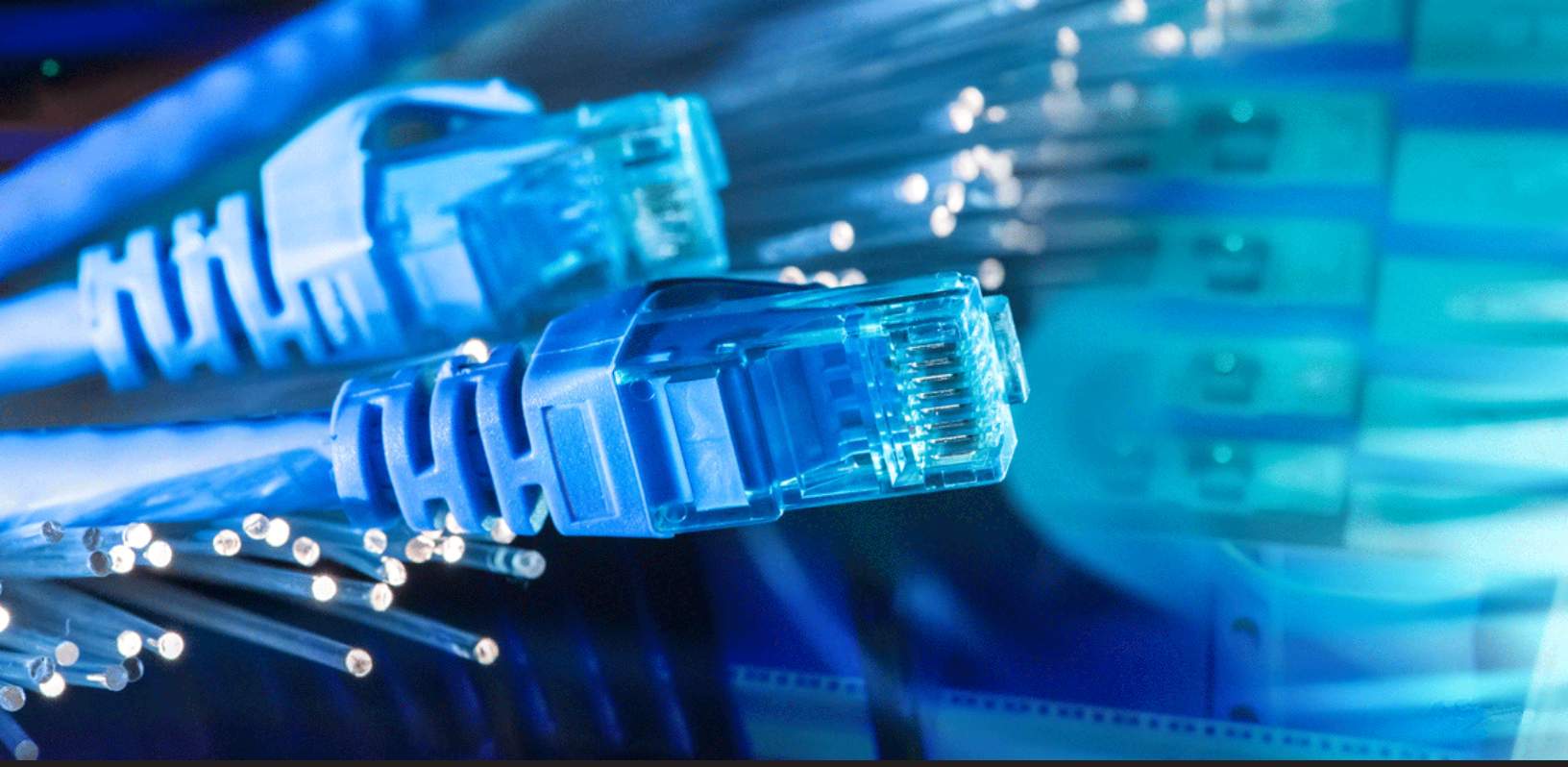

# How to Troubleshoot Networks with Traceroutes

Devolutions

## THERE ARE A VARIETY OF TOOLS AVAILABLE

When it comes to troubleshooting network problems, there are a variety of tools available, from speed tests to network monitoring software. Each tool has its purpose, and plays an integral part in optimizing network performance, but some tools play a bigger part than others.

Traceroute is one of the most popular tools that network engineers and IT geeks use to troubleshoot networks. Invented in 1987, traceroutes are still highly relevant and frequently used today.

To help you learn more about traceroutes and the role they play in monitoring network performance, the network experts over at Obkio released a series of articles called The Traceroute Series, which explains everything you need to know about troubleshooting networks with traceroutes.

Here is a summary of the series and all the topics!

## 1. What Are Traceroutes & How Do They Work?

First invented in 1987, traceroutes are considered the most commonly used tool to troubleshoot network issues. A traceroute traces the IP route from a source to a destination inside of an IP network. It collects data to show users the routers and round-trip latency from the source to each of the routers.

Traceroutes work using an 8-bit field in the IP header, called time-to-live (TTL). The traceroute software uses the TTL to discover the routers between a source and a destination. Learn more about how traceroutes work in the full article.

## 2. Identify Network Issues with Traceroutes

You can identify network issues with traceroutes by analyzing two metrics for each hop or router: latency and packet loss. The latency refers to the time difference between when a packet was sent and when a response was received. Packet loss refers to the percentage of sent packets which never received a response out of the total number of sent packets.

Traceroutes monitor both of these important metrics and identify network issues based on the results.

## 3. Why Routers Drop Packets or Have High Latencies

There are different reasons why a single router can drop traceroute packets or have higher latencies, and it doesn't necessarily point to any network performance degradation.

There's a general rule of thumb when looking at packet loss from a traceroute, and that is: if the packet loss doesn't continue with the following hops, then it's not a network issue.

## 4. Decode the Hidden Information from Traceroute DNS

The hostname of the traceroute hops can provide a lot of information about the real path from the source to the destination. There are four pieces of information that you can decode from traceroute DNS:

- The ISP operating the router
- The city where the router is located
- The router name, number, or unique ID
- The ingress interface or port through which the traceroute packet came on the router

## 5. How to Catch Reverse Path Issues

When looking at a traceroute, people often forget that traffic on the Internet is asymmetrical most of the time. This is called Hot Potato Routing.

To help troubleshoot issues further, traceroutes give you data from sources and destinations that are in the same ISP. This gives you a reverse traceroute to compare the data and catch reverse path issues.

## 6. Share a Traceroute with an ISP NOC

Whether a network problem is located in your ISP's network or somewhere else on the Internet, reach out to your ISP's NOC (Network Operation Center) to help troubleshoot. Explain to them the issue with the following information:

- IP addresses of the Source and the Destination
- A traceroute from Source to Destination
- A traceroute from Destination to Source
- Historical traceroutes where everything is running fine (if you have them)
- A way to replicate the issue (more on that later!)

A good traceroute tool or network performance monitoring software will allow you to share a traceroute with your ISP so they get all the data they need.

## 7. Load Balancing and Multiple Paths on Traceroutes

To increase capacity between routers, many IT specialists choose to have more than one connection between them. If at any point a router does not support higher speed interfaces, the only solution to support a higher capacity would be to aggregate two or more ports together.

There are usually two possible configurations that allow you to set up multiple connections between routers: the Link Aggregation and the Equal Cost Multi Path (ECMP).

For the more accurate data, you need a Traceroute software that allows you to choose which ports to use. Therefore, you can use ICMP to have an easy-to-read traceroute or use TCP (or UDP) with random ports to see the full paths between the source and the destination. Learn more about the impact of load balancing and multiple paths on traceroutes.

## 8. Traceroutes Inside MPLS Networks

Service providers (SP) and large enterprises use MPLS (Multiprotocol Label Switching) networks to better segment and manage their networks. There are two aspects of MPLS networks that affect traditional IP traceroutes: ICMP Tunneling and TTL Propagation.

With ICMP Tunneling, latency and the packet loss are different, even if the network path is the same. So latency may take a big jump and then stay the same for hops that are far away from each other.

With TTL propagation, each time it reaches a router, it is decremented by one. When TTL propagation is disabled, some routers are not visible in the traceroute.

MPLS networks change the way we look at traceroutes without giving us the exact picture of what is going on, so it's important to understand how they can alter the data.

Traceroutes are an extremely useful tool to help you troubleshoot network problems. But they are an advanced tool, which is why it's important to understand how to use traceroutes and when to fully leverage the information they provide!