**https://www.comparitech.com/net-admin/network-troubleshooting-tools/**

**11 Best Network Troubleshooting Tools for Network Administrators**

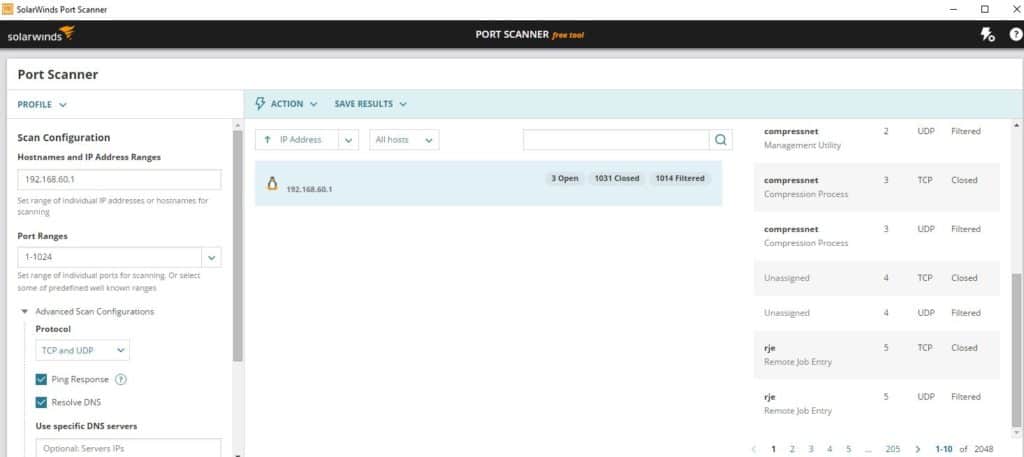
1. [**SolarWinds Port Scanner (FREE DOWNLOAD)**](https://www.comparitech.com/go/solarwinds-free-port-scanner-free-download-2/l/list+ctn006+v1/d/81905/d/81905/) – Free tool to check the ports on your network devices to ensure that you don’t have unattended ports open.
2. [**Paessler Network Troubleshooting with PRTG (FREE TRIAL)**](https://www.comparitech.com/go/paessler-prtg-network-troubleshooting-free-trial-2/) – Infrastructure management system that includes port monitoring.
3. **Ping** – Simple command line utility that checks on the speed of connections.
4. **Tracert** – Free command line utility that lists the probable hops to a network or internet destination address.
5. **Ipconfig** – This command line tool reports the IPv4 and IPv6 addresses, subnets, and default gateways for all network adapters on a PC.
6. **Netstat** – This tool displays active connections on your computer.
7. **Nslookup** – Available for Windows, Unix, Linux, and Mac OS, this tool gives you DNS server diagnostics.
8. **Speed and up/down test sites** – A list of websites that will test your internet connections.
9. **Sysinternals** – Set of Microsoft tools for Windows that help troubleshoot and configure Active Directory.
10. **Wireshark** – Free packet sniffer that will help you analyze traffic flows.
11. **Nmap** – Network security and monitoring tool that needs a companion utility, Zenmap, as a user interface.

**The main causes of network problems, such as slow speeds, dropped connections, and packet loss center on overloaded network devices, such as switches and routers, or missing information in your routing table and other system databases, such as the DNS server or the DHCP system.**

## The best network troubleshooting tools

Like with most jobs, when it comes to network troubleshooting, the tools you use can make a world of difference. When curating this list we considered the reliability of the tool in use in diverse situations, ease of setting up and use, documentation and support, and how up to date the software is kept.

### [1. SolarWinds Port Scanner****(FREE DOWNLOAD)****](https://www.comparitech.com/go/solarwinds-free-port-scanner-free-download-2/l/header+ctn006+v1/d/81905/d/81905/)

[](https://www.comparitech.com/go/solarwinds-free-port-scanner-more-information-2/l/image+ctn006+v1/d/81905/d/81905/)

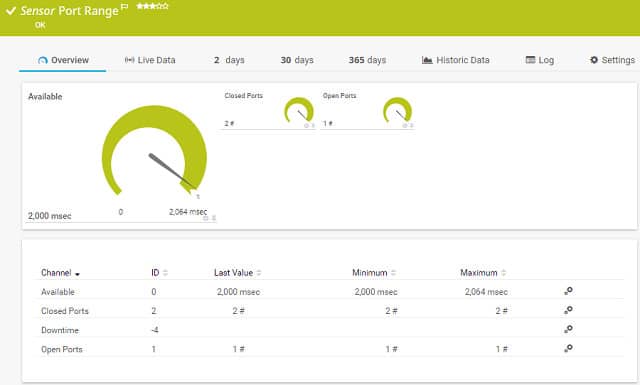
[SolarWinds free port scanner](https://www.comparitech.com/go/solarwinds-free-port-scanner-more-information-2/l/inline+ctn006+v1/d/81905/d/81905/) offers benefits similar to those of the popular nmap port scanner (which we discuss in this list too) with a GUI that is intuitive and easy to get started with. If you’re looking to dive right into the world of network troubleshooting and port scanning, this tool is a great place to start. The ease of use helps eliminate some of the technical barriers to entry other similar tools may have.

[Free Download:SolarWinds Port Scanner Tool](https://www.comparitech.com/go/solarwinds-free-port-scanner-free-download-2/l/cta+ctn006+v1/d/81905/d/81905/)

This scanner is a portable executable that can be run on Windows operating systems. In addition to scanning TCP and UDP ports to determine whether they’re open/closed/filtered, SolarWinds Port Scanner can detect MAC addresses and operating systems. Scan results can be saved in .csv, .xlsx, or .xml format. You can download SolarWinds Port Scanner for free [here](https://www.comparitech.com/go/solarwinds-free-port-scanner-free-download-2/l/cta+ctn006+v1/d/81905/d/81905/).

[SolarWinds Port ScannerDownload FREE TOOL at SolarWinds.com](https://www.comparitech.com/go/solarwinds-free-port-scanner-free-download-2/l/button+ctn006+v1/d/81905/d/81905/)

### [2. Paessler Network Troubleshooting with PRTG (FREE TRIAL)](https://www.comparitech.com/go/paessler-prtg-network-troubleshooting-free-trial/)

[](https://www.comparitech.com/go/paessler-prtg-network-troubleshooting-free-trial-3/)

[Paessler’s PRTG](https://www.comparitech.com/go/paessler-prtg-network-troubleshooting-free-trial-4/) is a complete monitoring system. It can help you with troubleshooting because it is able to track performance issues right down the protocol stack and identify the root of the problem. Port monitoring is one of the troubleshooting techniques that you can use with this tool.

**The PRTG system includes two port monitoring sensors**. One homes in on a specified port on a particular device, the other will check a range of port numbers. This tool only monitors TCP ports. The port range sensor has one extra feature that the single port sensor does not have. You can set it to check the port with TLS protection. Both sensors report on the response time of the port and whether it is open or closed.

PRTG includes network traffic analysis tools to help you troubleshoot delivery speeds. The tool includes a range of traffic monitoring techniques including route tracing to a destination with Traceroute and a Ping sweep, which will give you the response times to each node on your network. A packet sniffing utility can tell you which applications and endpoints are producing excessive traffic and you can query network devices to see which are congested to the point of queuing.

Paessler built a tool that covers servers and applications as well as network statuses, port response times, and services to monitor all conditions that can cause software performance problems. If you’ve got VMs on your network, PRTG can sort through their underlying connections, services, servers, and operating software. That monitoring is constant, so you will be able to trace back through events to spot the source of any performance issues.

Paessler delivers PRTG as a cloud service or you can install the software on your premises. The tool installs on Windows Server environments. You can use the system for free for up to 100 sensors. Paessler offers a [30-day free trial](https://www.comparitech.com/go/paessler-prtg-network-troubleshooting-free-trial-5/) with unlimited sensors so you can assess the monitoring and troubleshooting tool.

[Paessler PRTG Network MonitorDownload 30-day FREE Trial](https://www.comparitech.com/go/paessler-prtg-network-troubleshooting-free-trial-6/)

### 3. Ping

[Ping](https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ping) is the ideal command to use when you need to confirm network connectivity, at the IP level, between two hosts, or to confirm the TCP/IP stack is working on your local machine. A successful ping confirms network connectivity between the two hosts and it also gives reports on packet loss. Below is an example of a successful run of the ping command to the  “google.com” remote host.

C:\Users>ping google.com

Pinging google.com [172.217.9.46] with 32 bytes of data:

Reply from 172.217.9.46: bytes=32 time=38ms TTL=56

Reply from 172.217.9.46: bytes=32 time=12ms TTL=56

Reply from 172.217.9.46: bytes=32 time=14ms TTL=56

Reply from 172.217.9.46: bytes=32 time=12ms TTL=56

Ping statistics for 172.217.9.46:

Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),

Approximate round trip times in milliseconds:

Minimum = 12ms, Maximum = 38ms, Average = 19ms

In addition to confirming IP connectivity to “google.com”, these results confirm that we are able to properly resolve domain names (i.e. DNS is working on the local machine).

That **Loss** figure that you see in the last line of the ping output is the number of lost packets followed by the packet loss rate in brackets.

A few pro-tips for working with the ping command for advanced troubleshooting:

* Use ping –t to continuously ping a host. For example:

ping –t google.com

would continue to ping google.com until the ping was interrupted. Press control-c (the “CTRL” and “C” keys) to end a continuous ping.

* If you cannot ping domain names like google.com, but you can ping IP addresses on the Internet like 8.8.8.8 (Google’s DNS servers), you may have a DNS-related problem.
* If you cannot ping IP addresses on the Internet like 8.8.8.8, but you can ping hosts on your Local Area Network (LAN), you may have a problem with your default gateway.
* You can use “ping localhost”, “ping::1”, or “ping 127.0.0.1” to test the TCP/IP stack on your local machine. “localhost” is a name that resolves to one of the loopback addresses of a local machine, “::1” is an IPv6 loopback address, and “127.0.0.1” is an IPv4 loopback address.

### 4. Tracert

[Tracert](https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/tracert) is similar to ping, except it leverages Time To Live (TTL) values to show how many “hops” there are between two hosts. This makes it a helpful tool in determining where a network connectivity breakdown is occurring. Basically, tracert helps you understand if the router or network that is down between your computer and a remote host is one you control or not. Again using google.com as an example, we can see there were 10 hops between our PC and google.com.

C:\Users>tracert google.com

Tracing route to google.com [172.217.4.78]

over a maximum of 30 hops:

 1    1 ms   1 ms 3 ms  192.168.1.1

 2  246 ms    49 ms 56 ms  10.198.1.177

 3   58 ms    48 ms 54 ms  10.167.184.102

 4   63 ms    55 ms 85 ms  10.167.184.107

 5   50 ms    55 ms 56 ms  10.164.72.244

 6   72 ms   365 ms  69 ms 10.164.165.43

 7   92 ms    61 ms 45 ms  209.85.174.154

 8   67 ms    42 ms 58 ms  108.170.244.1

 9  372 ms    66 ms 46 ms  216.239.51.145

10    64 ms  73 ms 44 ms  lga15s47-in-f78.1e100.net 172.217.4.78]

Trace complete.

### 5. Ipconfig

Determining the IP settings on your computer is an important part of network troubleshooting. The [ipconfig](https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/ipconfig) command helps you do just that. Entering ipconfig at a command prompt will return IPv4 and IPv6 addresses, subnets, and default gateways for all network adapters on a PC. This can be helpful in determining if your computer has the right IP configuration. Additionally, ipconfig can be used to change or update select IP settings.

Pro-tips for working with ipconfig:

* If ipconfig returns an IP address that starts with 169.254 (e.g. 169.254.0.5), your PC is likely configured for DHCP but was unable to receive an IP address from a DHCP server.
* Use ipconfig /all to get the full TCP/IP configuration information for all network adapters and interfaces.
* Use ipconfig /release to release the current DHCP assigned network parameters.
* Use ipconfig /renew to renew the current DHCP assigned network parameters.
* Use ipconfig /flushdns to clear the DNS cache when troubleshooting name resolution issues.

### 6. Netstat

[Netstat](https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/netstat) allows you to display active connections on your local machine. This can be helpful when determining why users are unable to connect to a given application on a server or to determine what connections are made to remote hosts from a computer. Entering netstat at the command prompt will display all active TCP connections. Adding parameters to the netstat command will extend or alter the functionality. Here are a few helpful netstat commands and what they do:

* netstat –a displays all active TCP connections and the TCP and UDP ports a computer is listening on.
* netstat –n displays all active TCP connections just like the netstat command, but it does not attempt to translate addresses or port numbers to names and just displays the numerical values.
* netstat –o displays all active TCP connections and includes the process ID (PID) for the process using each connection.

You can combine different parameters to extend the functionality of netstat. For example, netstat –ano would display all active TCP connections and the TCP and UDP ports a computer is listening on, use numerical values, and report the PID associated with the connections.

### 7. Nslookup

[nslookup](https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/nslookup) is a useful command line utility that enables DNS troubleshooting and diagnostics. Nslookup is available on Windows and \*nix operating systems.  There are a variety of use cases for this flexible utility and it can be run in interactive mode or by entering commands directly at the command prompt.

To help you get started, we’ll review some nslookup commands that are helpful in three of the most common use cases: finding an IP address based on a domain name, finding a domain name based on an IP address, and looking up email servers for a domain. Below are examples of how to do each from a Windows command prompt.

**Finding an IP address based on a domain name:**

C:\Users>nslookup google.com

Server:  ns2.dns.mydns.net

Address:  192.168.247.45

Non-authoritative answer:

Name: google.com

Addresses:  2607:f8b0:4009:805::200e

      172.217.10.46

The output above shows us that the DNS server used on our local machine was ns2.dns.mydns.net and since ns2.dns.mydns.net is not an authoritative name server on Google’s domain, we get a “Non-authoritative answer”.  If we wanted to specify a different DNS server in our query, we simply add the DNS server’s domain name or IP address after the command, like this (using the [1.1.1.1 DNS server from CloudFlare](https://www.comparitech.com/blog/vpn-privacy/cloudflare-dns-how-to/)).

C:\Users>nslookup google.com 1.1.1.1

Server:  1dot1dot1dot1.cloudflare-dns.com

Address:  1.1.1.1

Non-authoritative answer:

Name: google.com

Addresses:  2607:f8b0:4009:812::200e

      216.58.192.174

#### Finding a domain name based on an IP address

Finding a domain name based on an IP address is similar to the previous process, you simply use an IP address instead of the domain name after the “nslookup” command. For example to find out what the fully-qualified domain name (FQDN) for the IP address 8.8.8.8 is we would use the command below:

C:\Users>nslookup 8.8.8.8

Server:  ns2.dns.mydns.net

Address:  192.168.247.45

Name: google-public-dns-a.google.com

Address:  8.8.8.8

Based on the output, we can see that the FQDN associated with 8.8.8.8 is “google-public-dns-a.google.com” which makes sense given 8.8.8.8 is one of the two popular [public DNS servers available from Google](https://developers.google.com/speed/public-dns/).

#### Looking up email servers for a domain

Sometimes you may need to determine what email servers are available on a domain. To do that, we simply need to specify that we are looking for MX records using the –ty switch. In the example below, we’ll check what mail servers are returned for gmail.com:

C:\Users>nslookup -ty=mx gmail.com

Server:  ns2.dns.mydns.net

Address:  192.168.247.45

Non-authoritative answer:

gmail.com    MX preference = 40, mail exchanger = alt4.gmail-smtp-in.l.google.com

gmail.com    MX preference = 5, mail exchanger = gmail-smtp-in.l.google.com

gmail.com    MX preference = 30, mail exchanger = alt3.gmail-smtp-in.l.google.com

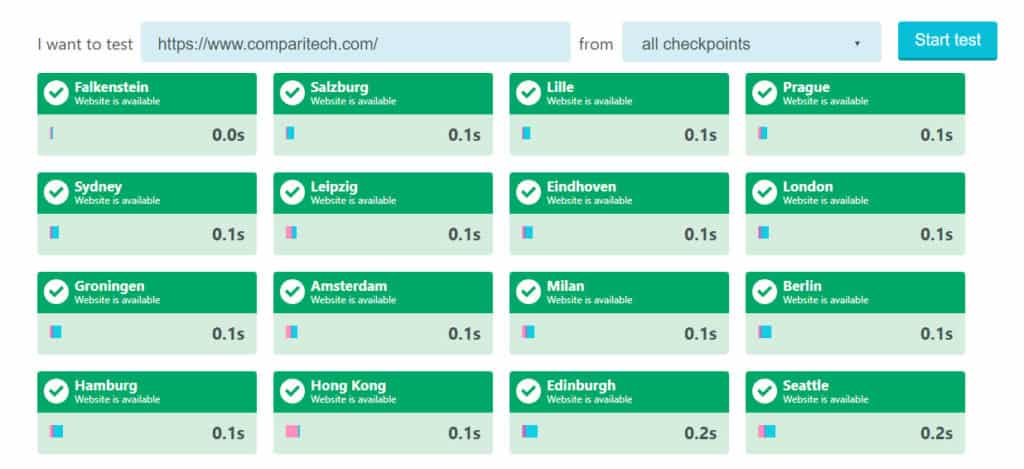
gmail.com    MX preference = 10, mail exchanger = alt1.gmail-smtp-in.l.google.com

gmail.com    MX preference = 20, mail exchanger = alt2.gmail-smtp-in.l.google.com

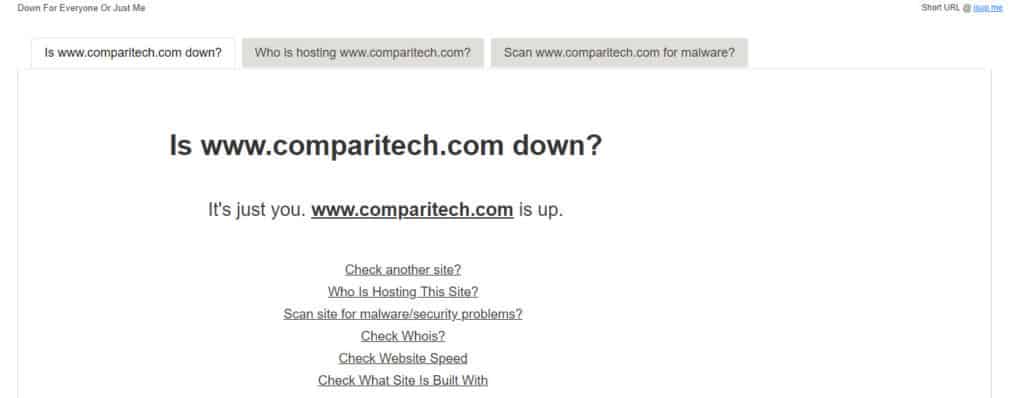
Here, five mail servers were returned along with an MX preference value. The lower the MX preference value, the higher the priority of that server (i.e. those servers should be used first).

### 8. Speed and up/down test sites

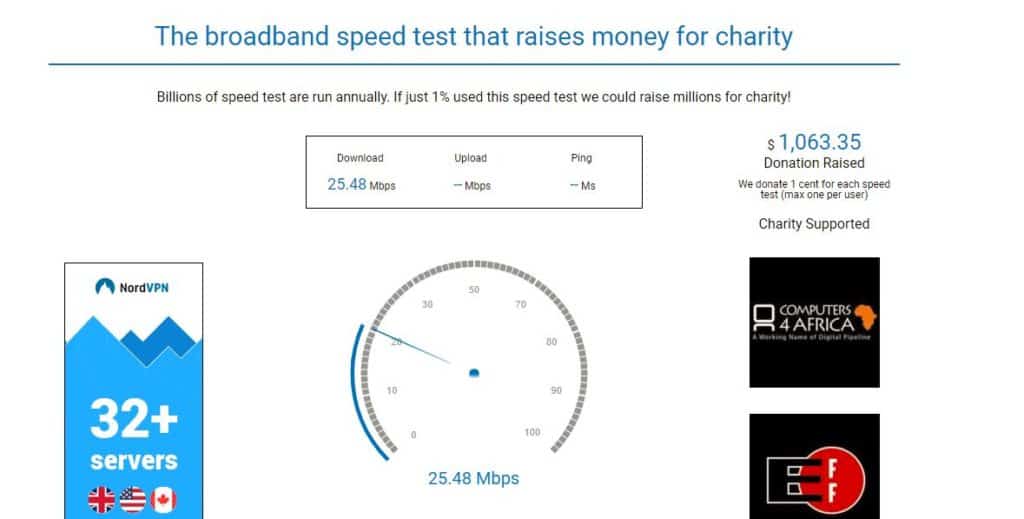
Sometimes you need to start troubleshooting by determining if the issue is with client computers accessing a website or with the website itself. There are a number of sites that can help you do just that. For example, [Uptrends’ uptime check tool](https://www.uptrends.com/tools/uptime) allows you to check the status and response time for a website from checkpoints across the globe.

[](https://cdn.comparitech.com/wp-content/uploads/2018/06/uptrends.jpg)

This can be especially helpful if you need to determine why some users can reach your site and others cannot. For a more simple, but more ad-heavy, up/down check you can try [Down For Everyone Or Just Me](https://downforeveryoneorjustme.com/).

[](https://cdn.comparitech.com/wp-content/uploads/2018/06/everyone-or-me.jpg)

Alternatively, you may want a quick and easy way to test your upload and download speeds to see if you have a bandwidth or latency issue. Our [broadband speed test](https://www.comparitech.com/internet-providers/speed-test/) is a great way to do just that and help raise money for charity.

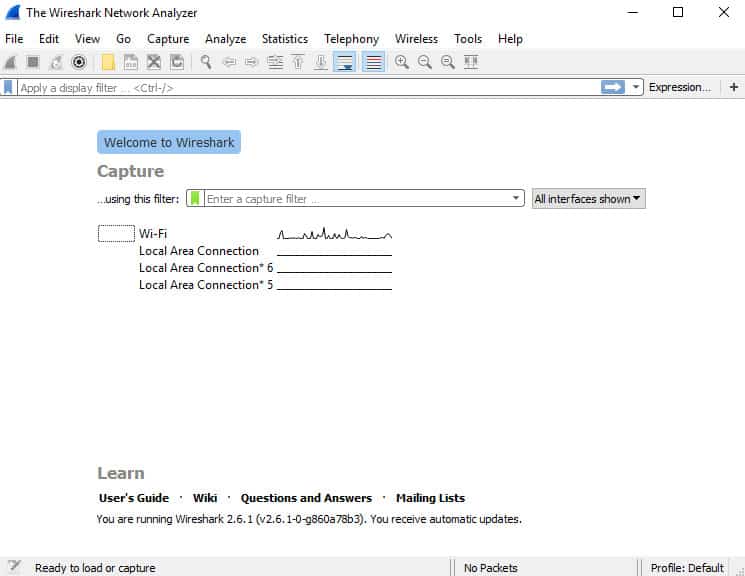
[](https://cdn.comparitech.com/wp-content/uploads/2018/06/comparitech-speed-test.jpg)

### 9. Sysinternals

Windows administrators that require advanced network diagnostic and troubleshooting tools will be well served by Microsoft’s [Sysinternals networking utilities](https://docs.microsoft.com/en-us/sysinternals/downloads/networking-utilities). The Sysinternals utilities include tools that can help troubleshoot and configure Active Directory (AD), like [AD Explorer](https://docs.microsoft.com/en-us/sysinternals/downloads/adexplorer) and [AD Insight](https://docs.microsoft.com/en-us/sysinternals/downloads/adinsight). Other tools can help measure network performance ([PsPing](https://docs.microsoft.com/en-us/sysinternals/downloads/psping" \t "_blank)), scan file shares ([ShareEnum](https://docs.microsoft.com/en-us/sysinternals/downloads/shareenum" \t "_blank)), list or run processes remotely ([PsTools](https://docs.microsoft.com/en-us/sysinternals/downloads/pstools" \t "_blank)), and more. If you only require one or a few of the Sysinternals utilities, you can install them separately as opposed to downloading the entire Sysinternals Suite.

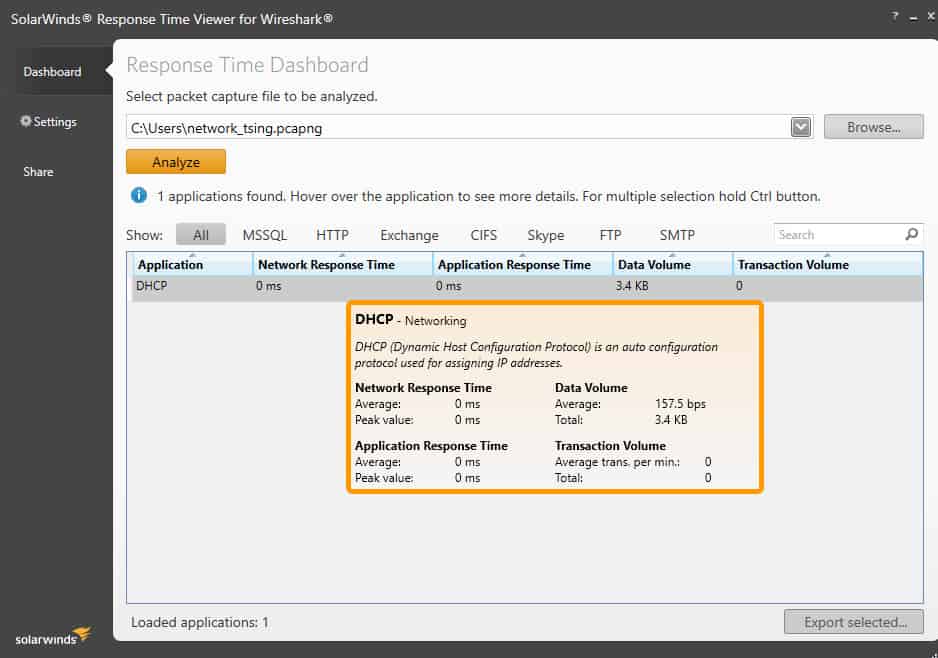
### 10. Wireshark

[Wireshark](https://www.wireshark.org/) is a protocol analyzer and one of the go-to networking tools for organizations of all sizes when network issues need to be troubleshooted with a high level of granularity. The benefit of using Wireshark to analyze network traffic is you will be able to view the raw network packets, and this will often allow you to identify the root cause of an issue. This can be especially helpful in situations where it is unclear which application is not doing what it is supposed to or when you try to reverse engineer the functionality of a poorly-documented program. The tradeoff here is that you will have a lot of data to parse through, so some technical knowledge may be required to drill down and identify the important information. You can download Wireshark for free [here](https://www.wireshark.org/#download).

[](https://cdn.comparitech.com/wp-content/uploads/2018/06/wireshark3.jpg)

On Windows operating systems, link-layer packet captures with WireShark are often made possible using [Winpcap](https://nmap.org/npcap/) (either Winpcap or [Npcap](https://nmap.org/npcap/) is required). In addition to enabling WireShark on Windows, Winpcap can enable the powerful [Windump](https://www.winpcap.org/windump/default.htm) command line utility which is Windows answer to the popular [tcpdump](https://linux.die.net/man/8/tcpdump) program found on many \*nix operating systems. For a deeper dive on Winpcap, Windump, and tcpdump, check out our [recent article on packet sniffers and network analyzers](https://www.comparitech.com/net-admin/packet-sniffer-network-analyzers/).

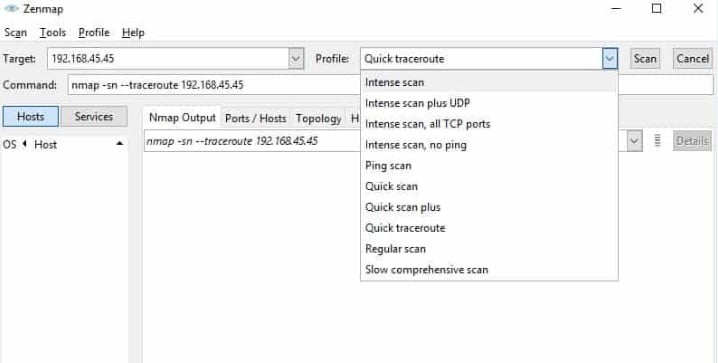
While WireShark is an excellent tool, the data generated isn’t always the easiest for the uninitiated to understand. If you are looking for a way to better visualize and parse through the data generated using WireShark, [SolarWinds Response Time Viewer](https://www.comparitech.com/go/solarwinds-response-time-viewer-for-wireshark-free-download/l/inline+ctn006+v1/d/81905/d/81905/) can help. This tool enables users to load and analyze .pcap files and provides easy to read summaries of the response times and data volumes.

[](https://www.comparitech.com/go/solarwinds-response-time-viewer-for-wireshark-free-download/l/image+ctn006+v1/d/81905/d/81905/)

[SolarWinds Response Time Viewer for WireSharkDownload FREE Tool](https://www.comparitech.com/go/solarwinds-response-time-viewer-for-wireshark-free-download/l/button+ctn006+v1/d/81905/d/81905/)

### 11. Nmap

[Nmap](https://www.comparitech.com/net-admin/free-port-checkers/) is a popular security auditing and network exploration tool released under a custom open source license based on GPLv2. While the most popular use cases for nmap are security scans and penetration testing, it can prove quite helpful as a network troubleshooting tool as well. For example, if you are dealing with an unfamiliar app and want to find out what services are running and which ports are open, nmap can help. Nmap itself uses a command line interface (CLI), but that doesn’t mean you are out of luck if you prefer a graphical user interface (GUI). [Zenmap](https://nmap.org/zenmap/) is the official nmap GUI and is a good way for beginners to start working with nmap. For more on Zenmap and a deeper dive on nmap, check out our [10 Best Free Port Checkers for 2018](https://www.comparitech.com/net-admin/free-port-checkers/) article.



## ****Summary****

The tools we discussed here are great to have in your network toolbox and we recommend giving some of them a try the next time you find yourself dealing with a head-scratching network troubleshooting scenario. Did we leave any of your favorite network troubleshooting tools out or do you have questions about the tools we mentioned here? Let us know in the comments section below.