NetScanTools®

Newsletter

May 2026

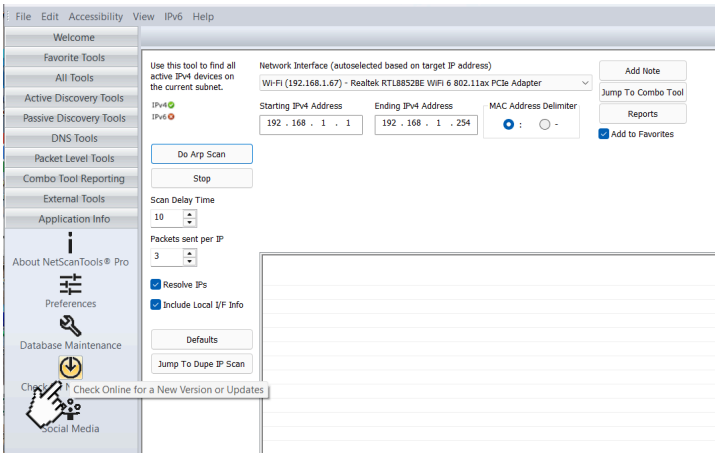
In This Issue

NST Pro 11.95.5 Available Now**

The new release is available. This update features performance and database updates across several tools, including faster Promiscuous Mode Scanning, improved DHCP/ARP functionality, and refreshed SQLite, MAC vendor, and IP geolocation databases.

How to access:

1. Open **NetScanTools Pro**
2. Go to **Application Info** at the bottom of the navigation bar
3. Select **Check for New Versions**
4. Enter your user name and Password (*Located on the Check for New Versions page within NST Pro*)



***Requires an active maintenance plan for access*

How to Investigate Phishing Attacks With NST Pro

AI has reportedly increased the volume of phishing attacks by 49%, and makes them 7X more effective. Source: KnowBe4

Here's a list of what you can do to investigate suspicious behavior using NST Pro:

Investigation Goal	Best NetScanTools® Pro Tools	What You Can Do
Analyze Suspicious Email Domains	DNS Tools – Advanced (SPF/DMARC/DKIM), DNS Tools – Core	Validate SPF, DMARC, DKIM, MX, TXT, and other DNS records used in phishing campaigns.
Research Domain Ownership & Hosting	Whois / RDAP, IP to Country	Investigate registrars, ASN ownership, abuse contacts, hosting providers, and geographic location.
Inspect Suspicious URLs & Redirects	HTTP Header Viewer	Follow redirects, inspect HTTP headers, and review suspicious web pages without full browser rendering.
Analyze SSL/TLS Infrastructure	SSL Certificate ScannerWhois / RDAP	Review certificate chains, SANs, TLS versions, and correlate related phishing infrastructure.
Check Reputation & Blacklists	Realtime Blacklist Check, DNS Tools – Advanced	Determine whether domains or IPs appear on spam or malware reputation lists.
Trace DNS & Network Paths	DNS Tools – Core (DiG / DiG +trace)Traceroute / Network Routing Visualizer	Investigate DNS delegation paths and trace routes to suspicious infrastructure.

Investigation Goal	Best NetScanTools® Pro Tools	What You Can Do
Analyze Suspicious Email Domains	DNS Tools – Advanced (SPF/DMARC/DKIM), DNS Tools – Core	Validate SPF, DMARC, DKIM, MX, TXT, and other DNS records used in phishing campaigns.
Collect & Correlate Indicators (IOCs)	Packet CaptureResults Database & Export Features	Capture evidence, collect IPs/domains/URLs, and export findings for reporting or case documentation.
Investigate Local Network Activity	ARP ScanSMB Scanner	Identify suspicious devices, exposed SMB services, and unexpected hosts on the local subnet.

Possible Switch Shortage Coming

Evaluate Your Risk

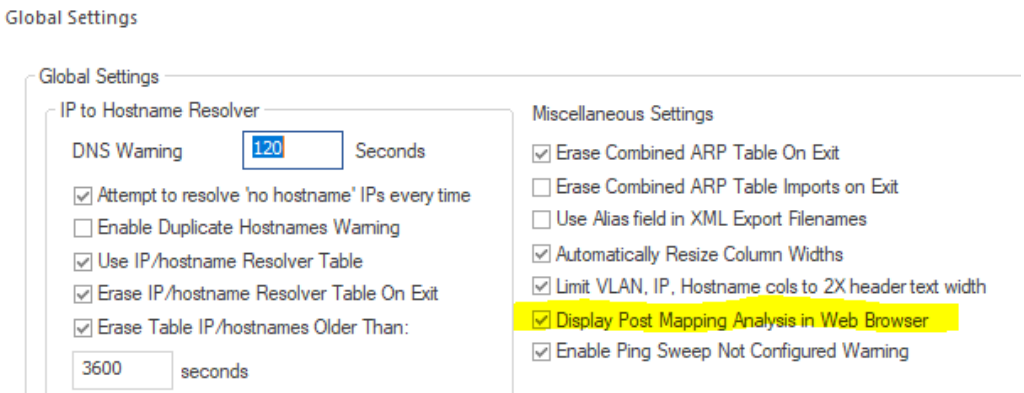
Per a report from Network World, the increased demand for switches from data centers is brewing up a shortage of layer 2 and 3 switches. Lead times and prices are both reportedly rising as a result.

Switchport Mapping Tool users can take action proactively by evaluating their network's current saturation.

To do so, **open the Switchport Mapping Tool**:

1. **Enter your switch access credentials** first or select a previously entered switch

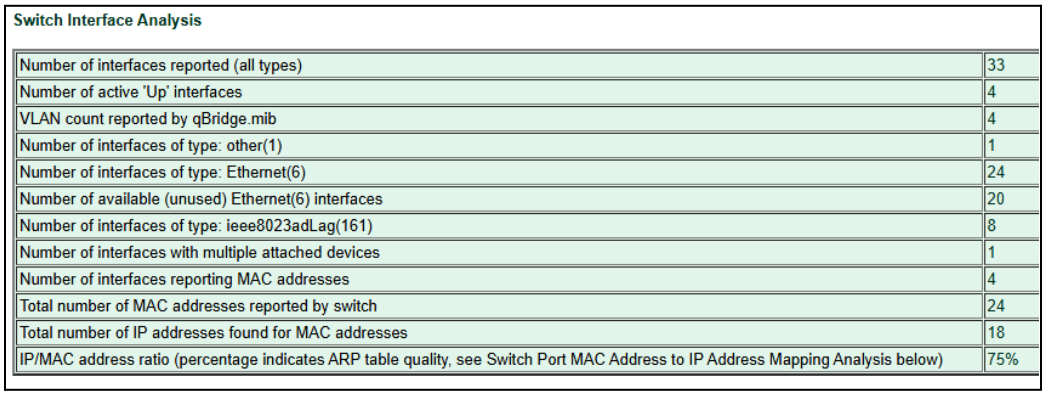
2. Select '**Display Post Mapping**



Analysis in Web Browser' in *'Global Settings'*

3. Map the Switches

Results populate in the Web Browser ➡️



Switch Interface Analysis

Number of interfaces reported (all types)	33
Number of active 'Up' interfaces	4
VLAN count reported by qBridge.mib	4
Number of interfaces of type: other(1)	1
Number of interfaces of type: Ethernet(6)	24
Number of available (unused) Ethernet(6) interfaces	20
Number of interfaces of type: ieee8023adLag(161)	8
Number of interfaces with multiple attached devices	1
Number of interfaces reporting MAC addresses	4
Total number of MAC addresses reported by switch	24
Total number of IP addresses found for MAC addresses	18
IP/MAC address ratio (percentage indicates ARP table quality, see Switch Port MAC Address to IP Address Mapping Analysis below)	75%

You can also use a previous mapping using 'Review History' -> right click in the results and select **'Show Switch Mapping Analysis in Web Browser'**

Missing IPs on Layer 3 Switches? Try this

We came across a unique issue a customer was experiencing while configuring the Switch Port Mapping Tool . Their Layer 3 switches were returning MAC addresses for connected devices, but many expected IP addresses were missing from the map. The cause turned out to be IP phones using Ethernet pass-through ports for connected computers — the switch could see the downstream device MACs, but those computer IPs had not yet populated the switch ARP table. **The issue was ultimately resolved by enabling a Ping Sweep across the relevant IP ranges**, which prepopulated the ARP table and significantly improved discovery results.

If your environment includes Layer 3 switches with IP phones and workstation pass-through connections, you may be missing valuable endpoint visibility during switch mapping.

Try this: Utilize a Ping Sweep to assist in prepopulating the switch ARP table with the missing computer ARP entries.

Missing IPs on Layer 3 Switches Cont.

Solution Instruction:

1. Open the left control panel Ping Sweep Range Editor.
2. Enter a start and end IP range using the known or expected ranges the computer IP's should be found in.
3. Press Add IP Range to Ping Sweep List. If other ranges are required, enter and add them. Note that this only applies to the switch being scanned at the time.
4. Close and ensure that Enable Ping Sweep is checked.
5. Remapping the switch may improve the results since the target computers are now being pinged.

Additional Note:
If other SNMP devices like layer 3 switches, routers or servers/printers are found in the network, you can add them in Router/Srv 1 and/or 2. It will only retrieve ARP tables from these devices.

Troubleshooting Resources Help Guides and Workflows for NST Pro

Our team is working to create troubleshooting guides for the most common problems faced by our customers. The intention is to have a cache of helpful resources for faster, easier workflows within NetScanTools. Below are some initial examples, currently available as a PDF upon request.

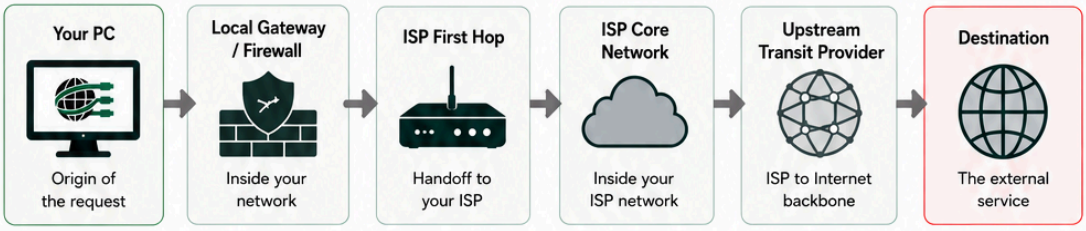
NetScanTools®

PROVE IT'S NOT US, IT'S UPSTREAM

Use Traceroute - Graphical

to Identify Where Network Problems Begin

Traceroute - Graphical helps you visually detect where latency or packet loss starts, so you can confidently show the issue is **upstream**.

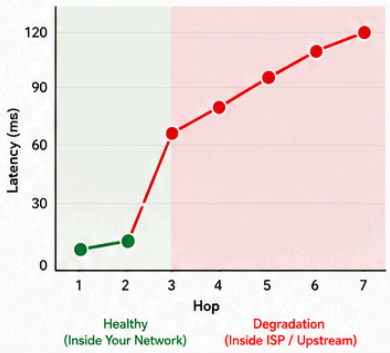


HOW TO TEST

1. **Open Traceroute - Graphical**
   Go to: Manual Tools → Traceroute - Graphical
2. **Enter a Stable External Target**
   Examples: 8.8.8.8, 1.1.1.1, your SaaS provider, or affected public service
3. **Click Start**
   Let it run for several minutes during the issue.
4. **Review the Results**
   Look for **degradation that begins and persists through later hops.**

EXAMPLE: PERSISTENT DEGRADATION BEGINS AFTER ISP HANDOFF

Hop	Host	Avg (ms)	Loss %
1	192.168.1.1	1	0%
2	10.0.0.1	3	0%
3	68.86.101.1	65	5%
4	68.86.96.6	82	8%
5	68.86.80.1	108	15%
6	204.79.197.201	118	18%
7	8.8.8.8	121	20%



Internal hops (1–2) are fast and stable.
Persistent degradation begins after ISP handoff (hop 3) and continues.
This suggests the degradation begins **upstream** of the local network.

Isolated latency spikes that do not continue downstream are often caused by ICMP rate limiting or router prioritization.

STRONG EVIDENCE PATTERNS

Sudden Latency Jump
Latency is low in your network but degrades after the ISP edge.

Packet Loss Begins Upstream
No loss internally, but loss starts after the ISP handoff.

Multiple External Targets Affected
Same issue occurs when testing different destinations.

MAKE IT EASY TO PRESENT

Use Continuous Monitoring
Let the trace run during outages, slowdowns, or user complaints to capture the problem in real time.

Export or Share Results
Right-click in the results grid to:
- Save results
- Print
- View in browser
- Copy results

Compare Internal vs External
Run traces to an internal server (should be stable) and an external target (showing issue). This strengthens your case.

ADDITIONAL TOOLS

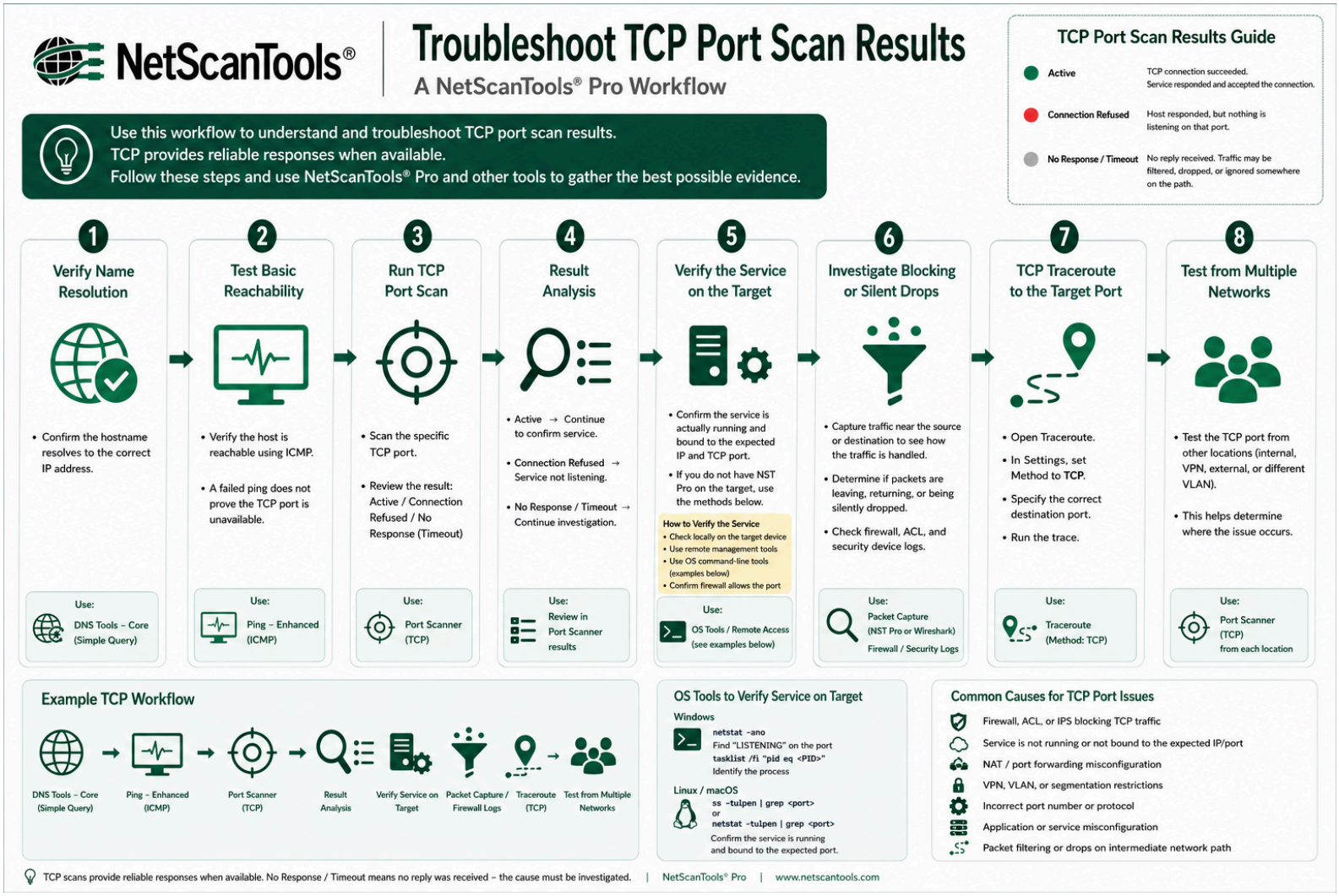
Network Routing Visualizer
Visually map routes to multiple destinations and see where paths diverge or degrade.

Traceroute (Standard)
Use different methods (ICMP, TCP, UDP) to test how traffic is handled across the network.

The Bottom Line

Traceroute - Graphical gives you clear, visual proof of where problems start.
When degradation begins after your network, you can confidently show the issue is upstream.

More Tools. Better Visibility. Faster Answers. | www.netscantools.com



Thank you all for reading and for your loyal support, it's our pleasure to serve you!

– NetScanTools®