NetScanTools® Pro
Monthly Newsletter
www.netscantools.com

January 2020

https://twitter.com/netscantools

https://www.facebook.com/NetScanTools

https://www.youtube.com/user/netscantools

https://netscantools.blogspot.com/

In this newsletter:

News

- **Managed Switch Port Mapping Tool 2.84.3 Released Jan 27, 2020**
- **Coming up in 2020**
- **NetScanTools Pro 11.90.1 Released Sept 19, 2019**
- **NetScanTools Pro Requirements**

News...

From the Editor...

Welcome to 2020. NetScanTools is now 25 years old – the original software was released in 1995. Have a great year.

-Kirk

Managed Switch Port Mapping Tool 2.84.3 Released Jan 27, 2020

This release is the first in a long time to improve Spanning Tree Protocol status reporting.

A customer pointed out that the switch port mapper was reporting N/A in the Spanning Tree Protocol (STP) Status column for his Dell N2000 and N3000 series switches. After a few inquiries we determined that we should obtained our own new N2024 for testing. We determined that we could add the necessary changes to show STP status for these switches. At the same time we also added similar code changes for some models of Netgear switches including the GS724T and FSM7326P switches

and related models. Now these Dell and Netgear switches report STP status instead of simply 'N/A'.

As usual we updated SQLite to the latest available version and updated the mac to manufacturer database. Since it is now 2020, all dates have been updated.

These are the changes in v2.84.3.

-Added methods for obtaining Spanning Tree Protocol data from Dell N series switches and two flavors of Netgear switches that do not report STP data in the normal location.
-Minor change to VLAN reporting algorithm for Cisco IOS and related switches.
-Updated MAC address/Manufacturer database.
-Updated SQLite to version 3.31.0
-Updated dates to 2020

Coming up in 2020

Several of our software products will be updated soon to reflect version changes in SQLite. We are going to be working with a certain famous packet analysis trainer this year – more on that later. A new release of NetScanTools Pro will be ready in the first quarter.

NetScanTools Pro 11.90.1 Released Sept 19, 2019

This release fixes some issues with the database that results are automatically saved to and it improves the operation of some tools.

Windows 10 security changes – notably Controlled Folder Access which is part of Windows Security Ransomware Protection – was preventing our access to the results database. That database has always been located in the Documents folder. Users would see the SQLite error message SQLITE_CANTOPEN(14). Users would have to whitelist/exclude the NetScanTools Pro application so that we can read/write the documents folder. While I understand their intent, Microsoft makes it very difficult for small developers – NetScanTools Pro is not in their automatically approved software list. We moved the default location to C:\Users\%username%\AppData\Roaming\NWPS\NetScanToolsPro

Both ARP Scanner and the related tool Duplicate IP Scanner now let you define how many ARP packets to send to each IP address. It now defaults to 3 where it was 1 in the past. This gives a better chance for each target IP to respond in a timely manner to the ARP packets.

PingTrend now has better axis labeling and the list of dropped packets can be exported to a CSV text file.

Click on Help menu/Check for Update to get the latest version – however, you must have an active maintenance plan to get this new version. USB version users will be downloading a patch – follow the directions carefully. Installed version users will be installing over the top of their current installed version.

NetScanTools Pro Requirements

This is a reminder of what we recommend for using NetScanTools Pro effectively.

- This software is x86/x64, is does not support ARM processors.
- WinPcap is now quite old and we now recommend using Npcap within the confines of their licensing requirements. We cannot distribute Npcap.
- WinPcap and Npcap are x86/x64 only – no ARM support yet.
- The USB version requires WinPcap or Npcap to be installed and operational on the host machine.
- Wired ethernet and WiFi connections are usually supported. WinPcap/Npcap will provide a list of supported interfaces on the tools that require use of either packet driver.

Contact Information

If you have any questions or suggestions, please feel free to email.

Northwest Performance Software, Inc.
PO Box 1375
Sequim WA 98382
(360) 683-9888
www.netscantools.com
sales [at] netscantools [dot] com

'NetScanTools Pro', 'NetScanTools Standard', 'NetScanTools Basic', 'NetScanTools LE', 'ipPulse', 'Northwest Performance Software' and 'NetScanTools.com', are trademarks of Northwest Performance Software, Inc. 'NetScanTools' is a registered trademark of Northwest Performance Software, Inc.

Other names and trademarks are the property of their respective owners.