NetScanTools® Pro Monthly Newsletter

www.netscantools.com

December 2017

http://twitter.com/netscantools

http://www.facebook.com/NetScanTools

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

http://netscantools.blogspot.com/

In this newsletter:

News...

From the Editor...

You may have noticed there was no November newsletter – this was actually an oversight because I was so busy with improvements to NetScanTools Pro and the Managed Switch Port Mapping Tool and of course, the holiday season. There are several very important topics in this newsletter. I recommend reading everything to learn about new features and upcoming changes.

Happy New Year!

-Kirk

Managed Switch Port Mapping Tool v2.79.1 released December 11, 2017

Managed Switch Port Mapping Tool v2.79.1 is a minor update that had a fix to the new dot1x column data display algorithm. It also updated the MAC Address/Manufacturer database.

Download the 'installed' version 2.79.1 from SwitchPortMapper.com and install it over the top of your current installed version.
http://www.switchportmapper.com/

USB version users need to use the Help Menu/Check for Update selection to obtain the upgrade patch. Please see important USB version topic in this newsletter.

Managed Switch Port Mapping Tool v2.79 released December 4, 2017

Managed Switch Port Mapping Tool v2.79 adds a new IEEE 802.1x column (dot1x), improves HP trunk/LAG reporting and an algorithm change to compensate for a switch data reporting problem.

New dot1x column – this shows information about the dot1x configuration on a per port basis. Keep in mind that implementations do vary slightly between manufacturers and we are only reporting the values we find at the moment. Add the column by clicking on Settings and Tools menu/Column Order and Visibility Editor.

HP trunk/LAG reporting – we now display manually created trunks that do not use LACP. These trunks are shown with the prefix Trunk -> in the interface type column.

Cisco Small Business series switches of the SG220 family were not showing MAC addresses or the columns depending on the MAC addresses. This is due to a problem with the data they report which is inconsistent with other SB series switches, so we now compensate for this issue.

Here are the changes in this release.

- Added new dot1x column to display IEEE 802.1x information. See menu item Settings and Tools/Column Order and Visibility Editor.
- Improved HP trunk/LAG reporting by now reporting manual trunks that do not use LACP. These types of trunks are prefixed by Trunk -> in the type column.
- Certain models of Cisco Small Business switches like SG220 series do not correctly report the status of a learned device mac address. Algorithm changes were made to allow for this issue.
- All columns required by 10SCAPE export are now included in the default column set.
- Algorithm change to Export to 10SCAPE.

- Last switch results after mapping a switch list now have column widths automatically size.
- SNMP Walk Tool now has dot1x preset.
- Fixed problem graying out Export to XML button in Review History.
- Updated MAC address/Manufacturer database.

Managed Switch Port Mapping Tool v2.78 released November 8, 2017

Managed Switch Port Mapping Tool v2.78 adds a new option for exporting the results of a switch list mapping to XML. Improvements were made to the Review History window and several changes were made to LLDP reporting.

New multi-switch XML export – we have always had saving the currently viewed results grid to Microsoft Excel Schema XML using the right click menu – but it was only a single switch mapping. Now there is a new export specifically for exporting the results of a Switch List mapping to XML. When you open it (not import) in Excel, each switch mapped in the list appears as a separate sheet. You have to first map the switches using Switch List Mode. Then you press Review History and select that switch list from the available results and press Export to XML. Next open the XML file with Excel and you get to see the results grids of all the mapped switches at the same time.

Review History/Searching previous results – since work was being to create the XML export, we decided to improve and expand the searching to include the LLDP and CDP columns. Search results are now shown in descending order with newest first and the formatting has been improved.

LLDP – several minor changes were done including better parsing of the MAC and IP addresses and we now show the interface manufacturer based upon the MAC address. This will help you quickly identify the attached device that generated the LLDP data.

Here are the changes in this release.

- New XML export option for Switch Lists from Review History. When the XML export is opened in Microsoft Excel, each switch results appear as a separate sheet. Each row in a multi-row port (ports with more than one mac address) are shown as separate rows in the XML output. Export progress is now shown on the bottom status bar.
- Review History/Searching now has selections for searching LLDP and CDP for text strings. Searching now defaults to 'Contains' if no options are selected and the search results shown in the right hand list are a bit wider. Search results are now shown in descending order - newest at the top. 'RecNo' in the two lists have been changed to 'No.".

- Corrected reporting of Switch Operational State for Extreme Networks switches.
- Corrected and removed '00 00' showing in Interface Alias column for Force10 switches.
- Warning is now shown if 10SCAPE export does find LLDP data for the switches. Switches with no reported LLDP data are shown. Export progress is now shown on the bottom status bar.
- Added new right click menu option to clear both the results grid and the Switch Info left control panel window.
- Improved parsing of MAC and IP addresses from LLDP data.
- Added Interface Manufacturer derived from remote MAC address in LLDP.
- Moved four tables from spmap database to working database.
- Updated SQLite to version 3.21.0
- Updated MAC address/Manufacturer database.

New Tool coming in the next NetScanTools Pro Release

We have had a lot of requests for an SMB version scanner. It will be in the next release coming in January. It shows each of the SMB versions that the target operating system is capable of communicating with. Watch our Facebook page for more information.

Windows XP Support Ending

It has been nearly 4 years since Microsoft stopped supporting Windows XP and we have now run into issues that mean we have to stop supporting it – at least for the USB versions. When we release the next NetScanTools Pro and Managed Switch Port Mapping Tool versions, we will no longer test on XP and the USB versions will require Windows Vista or newer for operation.

Tip: What to do when switches partially map ie. show few MAC Addresses.

Sometimes you may run into a switch that is configured the same as other switches that map fine, yet when you map it you see everything but the MAC address column and columns that depend on the MAC addresses like IP address and hostname.

The problem may be that the switch is too busy. The default setting for Bulk Reps is 8 which means that we make one request and the switch can reply with up to 8 responses combined in one packet. Try reducing that value (see switch settings) to 2 or even 1.

A customer ran into this issue recently with very busy stacked Cisco 3850 running IOS-XE Software, Version 03.06.06E RELEASE SOFTWARE (fc1) and solved it by reducing that value to 2.

NetScanTools Pro 11.83 released September 15, 2017

This release improves the user experience in several areas and the UI is less cluttered.

Back when we started adding tools that depended on WinPcap, a computer typically had one interface that WinPcap could use for receiving or sending packets. That has all changed. VPNs, Virtual Machines and secondary network interfaces can all potentially add WinPcap compatible interfaces and those interfaces all show up in the WinPcap Interface dropdown list. The problem is that prior to v11.83 you had to select the right WinPcap compatible interface or the tool did not work right and you saw a message to select the correct interface. What v11.83 brings is automatic selection of the interface based on the input you give. This applies to a number of tools in NetScanTools Pro like ARP Scanner, Ping, Traceroute and others. You will still have to select the correct interface in many of the separately launched tools like Packet Capture or Passive Discovery because those tools are listening tools rather than 'packet sending/listening' tools.

Over the past few years typical monitor sizes (pixels HxW) has radically increased. We originally designed NetScanTools Pro to accommodate monitors as low as 800x600 but I personally use a pair of 1920x1080 monitors. I reviewed our web traffic on Google Analytics and found that nobody is using 800x600 or even 1024x768 so this new version of NetScanTools Pro expands the layout of the buttons and other controls on the right side and spreads them out as a first step towards reducing clutter.

Another annoyance was the 169.254.x.x popup message that appeared on startup, usually if you had Npcap installed instead of WinPcap. The message is gone and 169.254.x.x interfaces are not included in any tool (except those that show interfaces) since they are auto-assigned IP addresses from the operating system and actually not functional.

Many other changes and they are listed below. If you have an active maintenance plan you can download 11.83 through the Help menu/Check for New Version.

Speaking of the full installer – save it in a safe place and replace any old versions. We constantly run across users who have reinstalled or moved their software to a new computer and they do so by using an old installer. Sometimes the installer is many, many versions older - so SAVE the latest one and discard the old ones!

11.83 Release Notes

- Usability improvement: Tools that depend on selecting the right WinPcap compatible interface now automatically select the interface based on the target entered. This includes ARP Ping, ARP Scanner, DHCP Server Discovery, Duplicate IP Detection, OS Fingerprinting, Ping - Enhanced, Port Scanner, Promiscuous Mode Scanner, and Traceroute. 'Launched' monitoring tools still require you to select the interface to monitor.
- Reports now have expanded information regarding the settings used for these tools (most are in the 'Notes' section of the report): Packet Flooder, Ping - Enhanced, Ping Scanner, Port Scanner, and Traceroute.
- DHCP Server Discovery now times out quicker if the local port 68 is in use and any network adapters with the IP starting with 169.254.x.x are not shown in the list because they are inactive.
- Maintenance Plan Expiration and other startup messages that appear before the main window is active are now force to appear as the topmost window. This stops the problem of starting NetScanTools Pro and not seeing anything because a startup message window was behind another window.
- Ping Scanner now includes a right click menu option to use your web browser to connect with the selected IP address.
- Fixed minor memory leak in Network Interfaces and Statistics.
- Removed startup message about 169.254.x.x interfaces which shows up more frequently if Npcap is installed instead of WinPcap.
- Began the first steps of a UI improvement by expanding the area used by the tools in the right hand panel. Our research shows that most displays are now wide enough for us to de-clutter the right hand side by making it wider and moving controls.
- Ping: changed the default header acknowledgment field value to 0.
- Traceroute: added header acknowledgment field as a user defined field in Settings.
- SSL Certificate Scanner: Added parsing of Subject Alternative Name (SAN) fields. Shown in the certificate chain. Previous retrievals of SSL certificates are noted in the grid when you edit or start the software. Right click to access the certificate chain. Added more parsing of signature algorithms so OIDs will be less likely to show up.
- Graphical Traceroute: Added Reset Statistics button.
- SNMP and SNMP Advanced: default bulk reps is now 8. Suggest lowering to 8 if you are using SNMPv2c or SNMPv3.
- USB Version Only: startup on a host running Npcap now works correctly.
- Updated SQLite to version 3.20.1
- Updated MAC address/Manufacturer database.
- Updated IP to Country database.
- Updated dates in all subprograms to 2017.

NetScanTools Pro USB Version Issues on Windows 10

I guess it was inevitable. Since before 2010 we have included special version (last updated in 2010) of WinPcap on the NetScanTools Pro USB version distribution. This WinPcap self-installs a driver at run time, hence our longstanding requirement for using 'Run as administrator'. Apparently it is no more. At least on Windows 10 and probably other versions of Windows that are being updated. Some recent change in Windows prevents this self-install and driver run from happening.

Since WinPcap is no longer being updated, you have two options. If you have a USB version older than 11.82 you will need to install regular WinPcap from winpcap.org on the host if NetScanTools Pro gives error messages. If you have 11.83 you can also install Npcap in WinPcap compatibility mode as an alternative to WinPcap. Npcap is under active development.

Bottom line: the host must have WinPcap (winpcap.org) or Npcap (nmap.org/npcap) installed for NetScanTools Pro USB version to work.

Using npcap instead of WinPcap for NetScanTools Pro/LE (revised)

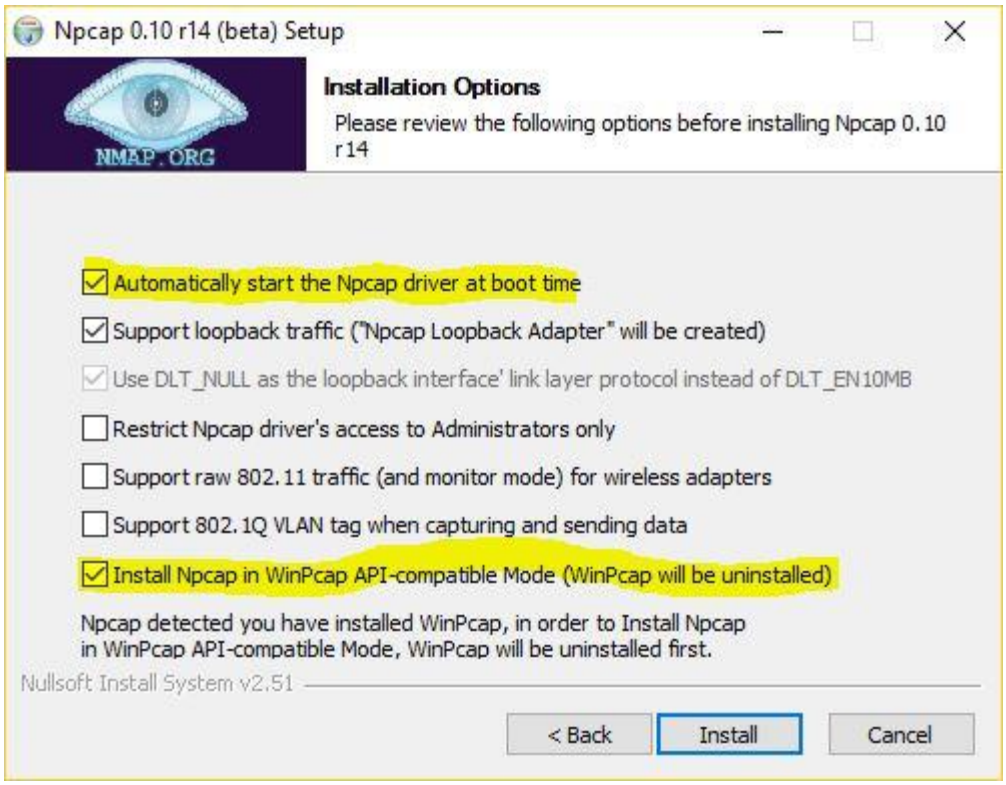
WinPcap has not been significantly worked on by its maintainers for several years now and is getting stale. While it still does work on Windows 10, I would not expect that work forever. Case in point: during the Windows 10 betas the NDIS 5 portion of the network software was deprecated for a version or two. This broke WinPcap 4.1.3. But some changes were made in Windows and WinPcap has worked again for a number of major Windows 10 revisions including the latest Creators Update. But that could easily change.

Npcap is the solution.

Npcap is a WinPcap fork created and supported by the nmap people. It is based on the newer and faster NDIS 6 and has had many releases even this year. We cannot distribute it with our software, but you can download it as an end user.

How to use install npcap instead of WinPcap:

1. Do not uninstall WinPcap!
2. Download the latest npcap installer from nmap.org/npcap
3. Install npcap and be sure to use the settings highlighted in yellow (if you are using NetScanTools Pro in a Virtual Machine, like VMware we recommend clearing (uncheck) the 'Support loopback traffic' option. Use 'bridge' mode with VMs.



What to do if there are problems installing npcap. If there is a problem it is because WinPcap could not be totally removed. This is what to do:

Try this manual removal of WinPcap – especially if WinPcap has been 'uninstalled':

1. Open an Administrator command prompt (or PowerShell) and type> net stop npf followed by enter - you may see a message about it successfully stopped or not found - either is good. Close the command prompt.

2. Remove the directory c:\program files (x86)\WinPcap if it exists (64 bit OS) or c:\program files\WinPcap (32 bit OS).

3. Search for and delete all instances of packet.dll and wpcap.dll in c:\windows. You may find them in c:\windows\system32 and in c:\windows\SysWOW64. Also delete c:\windows\system32\drivers\npf.sys (do not delete npfs.sys - be careful!)

4. open regedit. Remove HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\WinPcap (64 bit OS) or Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WinPcap (32 bit OS)

5. Remove HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst (64 bit OS) or Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Uninstall\WinPcapInst (32 bit OS)

6. Remove HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\npf and close regedit.

7. Reinstall winpcap downloaded from www.winpcap.org. Reboot and try NetScanTools Pro and Wireshark.

8. Once they have been verified to work, try installing npcap again using the earlier steps.

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