NetScanTools® Pro Monthly Newsletter

www.netscantools.com

August 2017

http://twitter.com/netscantools

http://www.facebook.com/NetScanTools

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

http://netscantools.blogspot.com/

In this newsletter:

News

News...

From the Editor...

What happened to summer? Lots of work done this summer and a number of changes coming to NetScanTools Pro that will make it much easier to use some of the tools.

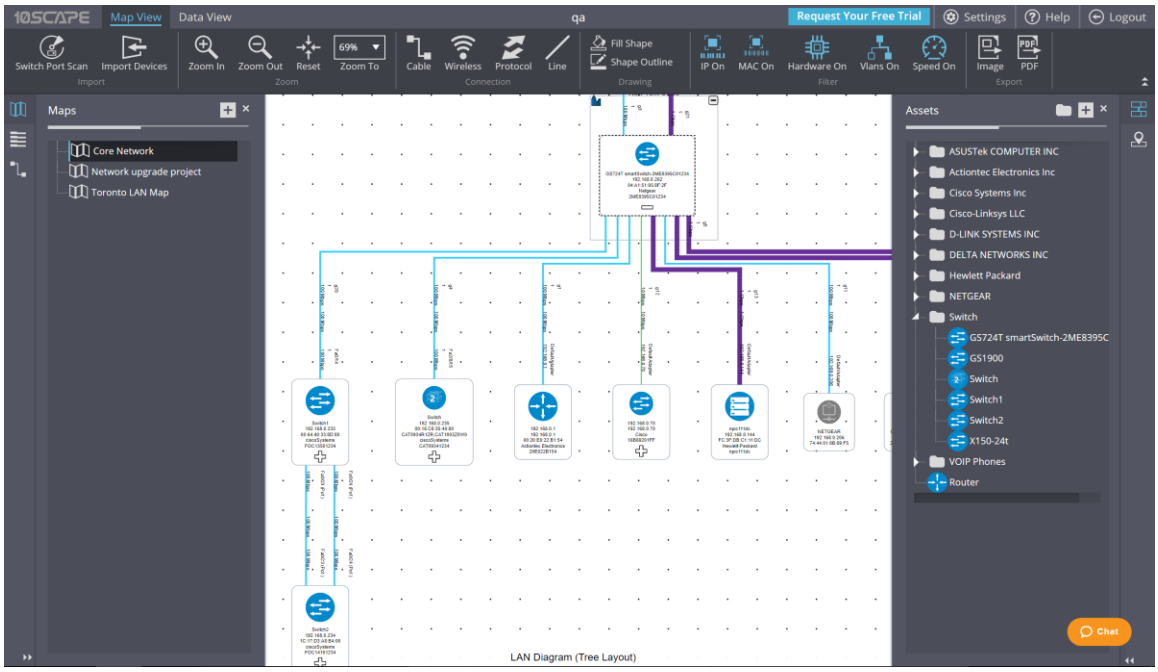
-Kirk

Visual Network Mapping

Visual Network Mapping is something many Switch Port Mapper users have asked about. We now have an answer. Yes, it can be done. Over the past few months we have been collaborating with the folks at 10SCAPE. They have a cloud based visual network mapping system that uses Spiceworks as a data source. Now the Managed Switch Port Mapping Tool has been added as a data source. Release 2.76 added export of both Switch List and single switch manual mapping data in a format suitable for import into 10SCAPE's visual mapping system. Version 2.77 improved the export and added better support for Juniper, Force10 and other switch brands.

Learn more here:
http://www.switchportmapper.com/visual-network-mapping.htm

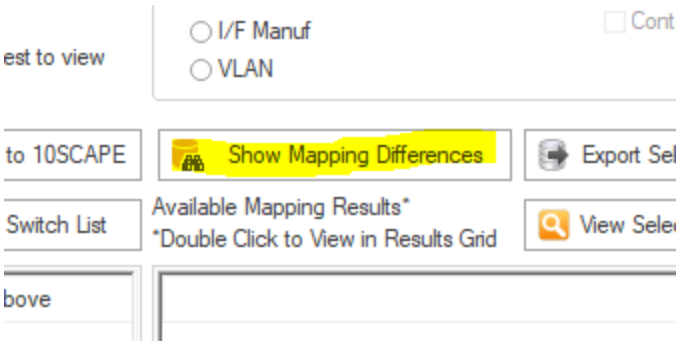
Video:
https://embedwistia-a.akamaihd.net/deliveries/19c84581f1deb70c211fa84dc19dfc20bb468459.jpg?image_play_button_size=2x&image_crop_resized=960x540&image_play_button=1&image_play_button_color=54bbffe0



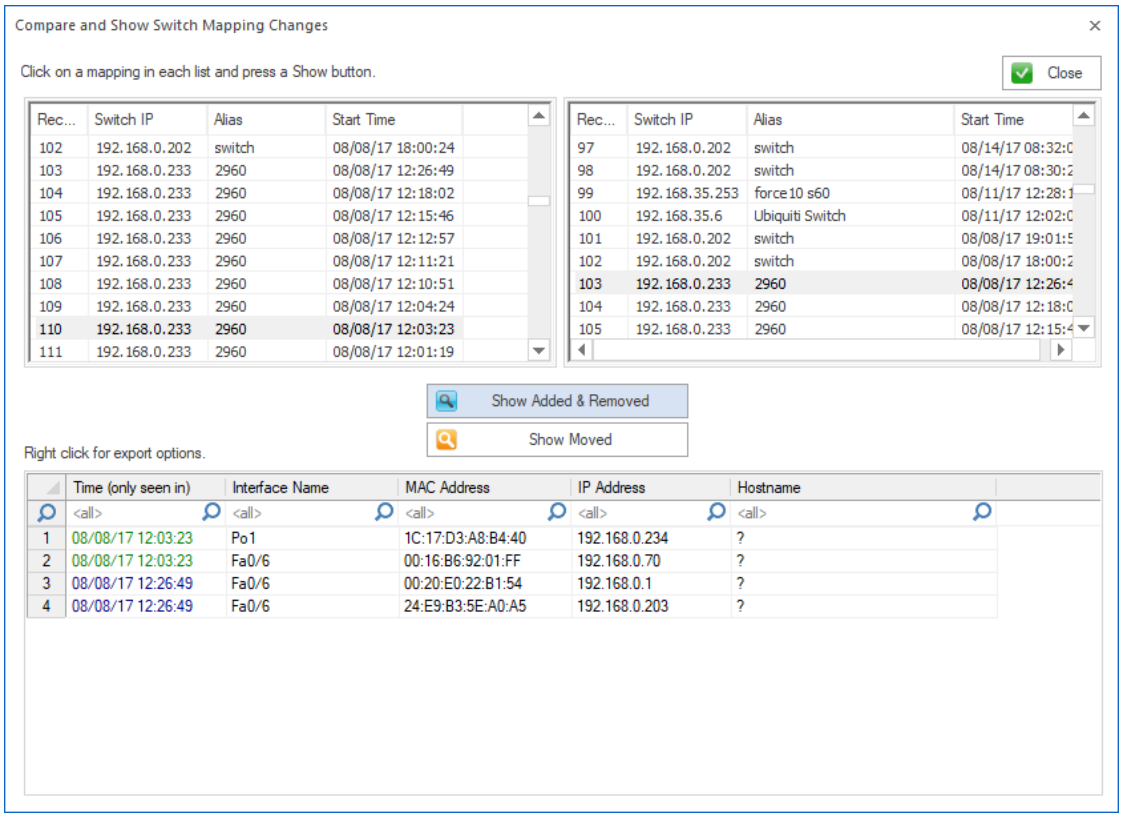
Managed Switch Port Mapping Tool v2.77 released August 18, 2017

Managed Switch Port Mapping Tool v2.77 adds several features to enhance the user experience plus new features including one that has been requested a number of times for several years.

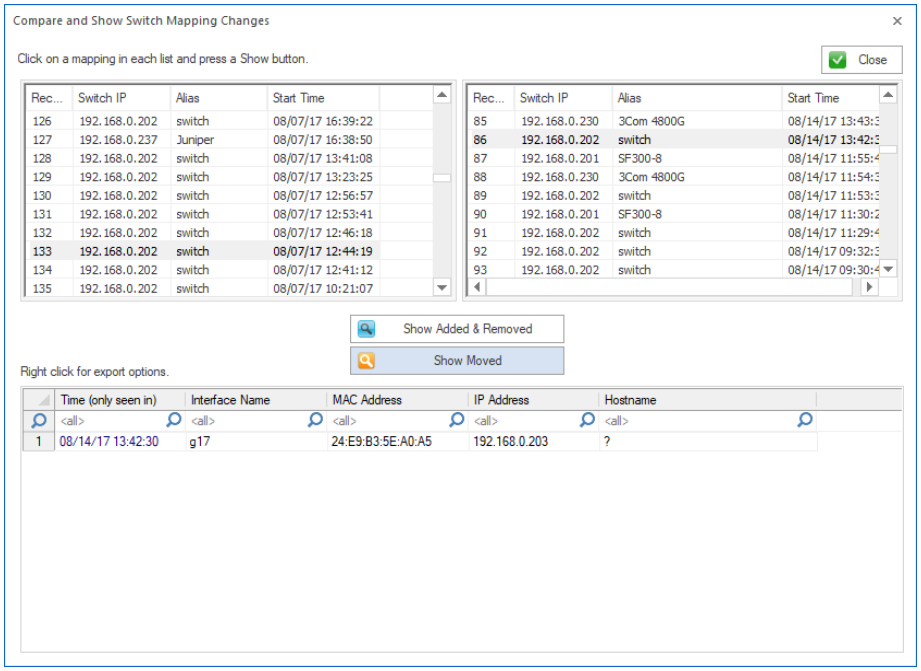
One of the most requested features (for years) is this: a way to compare two mappings of the same switch to see what has changed. It is now there under Review History (left control panel):



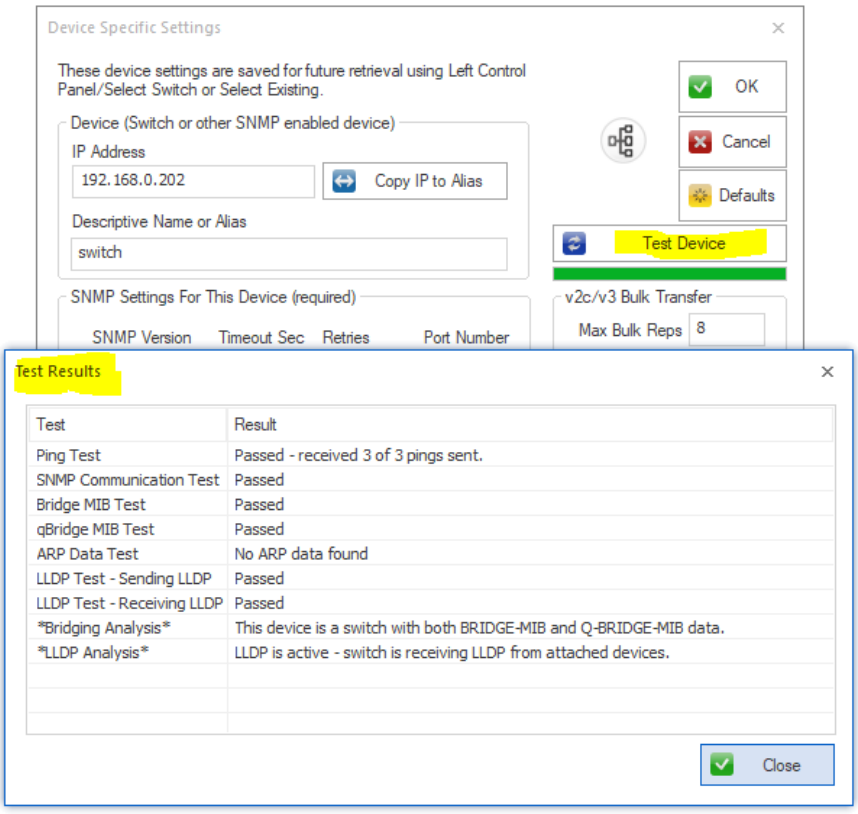
Select at mapping from the left list, then select one from the right list. Press 'Show Added & Removed' to see a list of what is present only in the first mapping (green) and the second mapping (blue) as shown below.



To see a list of devices moved from one port to another between mappings, press Show Moved. The final port that the device was moved to is shown in the list.



Another major addition is the 'Test' button. You can find it in the device settings. It give you a way to see if the device (switch or router or other) can be pinged and communicated with using the SNMP settings you have entered. See below:



Do you have Juniper, Ubiquiti and Force10 switches? We improved support for those switches and we even found that some models of Adtran switches can be mapped – but not all.

Full list of changes in this revision.

2.77 August 18, 2017

-Added button in Review History for comparing and displaying the differences between two mappings of the same switch at different times. One selection shows the difference between information present on the first switch mapping vs the second switch mapping. The other selection shows movement of a device from one port to a new port. The results of the comparisons may be saved/exported/printed.

-Added Test button to Device Settings. Use it to verify the device is reachable with Ping and verify your SNMP settings are correct. It also can tell you if it is a switch or a different kind of SNMP enabled device.

-The target switch is now tested near the start of the mapping to see if it really is a switch, if not a 'do you want to continue' question is asked.

-Additional sources of warning messages during SNMP single parameter retrievals were identified and the warning suppressed. The warnings were sometimes interpreted by users as errors and slowed the mapping process.

-New Command Line option (-txt) to save the results of a mapping to a hybrid tab/CSV delimited text file. Columns are represented by tabs and rows within a multi-row cell are represented by commas.

-Improved export to 10SCAPE. If required columns are missing, a warning is now shown at export.

-Column Order and Visibility Editor: the 10SCAPE defaults button now turns off the Ping Sweep warning (see Global Settings to reactivate it).

-Global Settings: the Display Ping Sweep Not Configured warning message is now disabled by default.

-Global Settings: when switch group specific settings (like MAC limit per port) are changed, the changes are now saved to the currently shown left panel switch group.

-Switch List Editor: show final report and show individual reports are now unchecked by default.

-Framework: menu and toolbar are now fixed in place and not dockable.

-Framework: top titlebar is now correctly updated to show the switch info when the mapping is complete.

-Juniper, Force10 and Ubiquiti switches are now processed correctly and manufacturer specific details are now retrieved.

-Some models of Adtran switches are now supported.

-Juniper switches now show the vlan name, internal vlan number and vlan tag as follows with the tag in curly braces: MYVLAN(5){100}. Other switch brands will continue to show MYLAN(5) or 5 where 5 is the vlan number.

-In order to speed up the switch list mapping process, the column widths are no longer automatically resized in list mode.

-VLAN identification for older 3COM switches was improved.

-Improvements to data shown in vlan columns.

-Fixed SQL syntax problem in lldpLocChassisId when subtypes 1-7 are present.

-Fixed usability problem with device settings editor where selections from existing community names would not appear to 'stick'.

-Fixed XML export where switch information is added in the left column.

-Added System Description to CDP data.

-New information added to SNMP Error Report.

-Changed Review History icon.

-Updated SQLite to version 3.20.0

-Updated MAC address/Manufacturer database.

Download the 'installed' version 2.77 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.

SNMPv2c/3 Bulk Transfer/Max Bulk Reps (Managed Switch Port Mapping Tool and NetScanTools Pro)

SNMP v2c and v3 have a method for requesting bulk transfers of data. This means one request and many responses – a way to reduce SNMP bandwidth.

There is a limit to what can come back that depends on the number of records available and their size. Initially we set the default at 32 but in practice we have found that the default should be 8. This means that if you are doing a 'walk' of a table, up to 8 records will be returned for one query. If you are using more than 8 right now, we recommend going down to 8 or even lower if you are not getting any

data and you expect to get data. Some devices will not return any data if you say you can accept more than it plans on sending you. See SNMP Settings for Max Bulk Reps

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

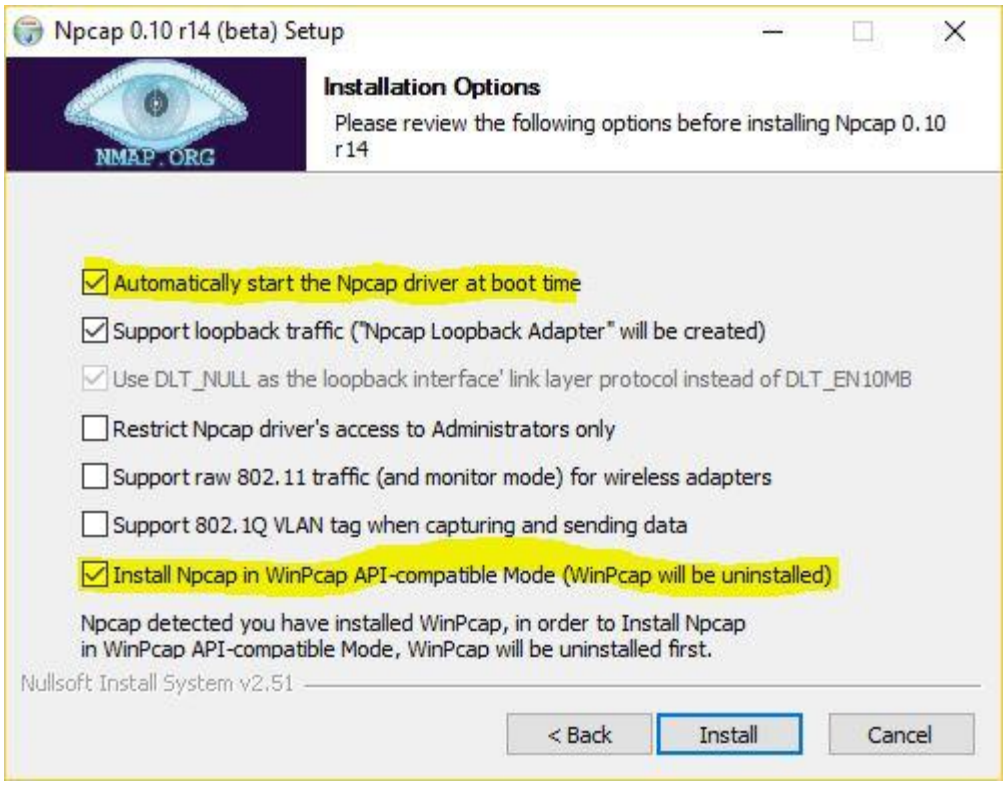
WinPcap has not been significantly worked on by its maintainers for several years now and is getting stale. While it still does work on Windows 10, I would not expect that work forever. Case in point: during the Windows 10 betas the NDIS 5 portion of the network software was deprecated for a version 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.

NetScanTools Pro Revision in work

NetScanTools Pro is being revised. Changes implemented so far include automatic selection of the appropriate WinPcap listening/transmission interface for several tools. This will make it easier to use when multiple WinPcap compatible interfaces are present. Watch our Facebook and Twitter feeds for more information.

NetScanTools Pro – Did you know?

NetScanTools Pro has a full PDF manual. It is located here for the installed version:
C:\Program Files (x86)\NWPS\NetScanTools Pro\docs

Or in the docs subdirectory in the USB version.

NetScanTools Pro 11.82 released March 14, 2017

This version has significant changes to the SNMP tools and the DHCP Server Discovery Tool.

Most SNMP tools now accept IPv6 address input – this is big because IPv6 is making significant inroads in networking. If your switch or other device talks SNMP, you can use either IPv4 or IPv6 to do a 'walk' of an OID or MIB. If you are talking to a switch or printer on a link local address starting with FF80:, you do not need to use percent followed by Scope ID, just use the address like you would a global address. *The SNMP Scanner and SNMP Dictionary Attack Tools continue to only accept IPv4 addresses.*

The changes to DHCP Server Discovery are pretty big. We had users tell us that it was not always displaying every DHCP server on the LAN (DHCP is limited to your local network segment). Eventually we were able to reproduce the issue and came up with a solution similar to other tools in NetScanTools Pro. You now have to select the WinPcap interface of the network interface you are using (if your computer has more than one). It now shows all responding DHCP servers.

Another expanded tool is the 'Get Basic DNS Records' in the DNS Tools – Core. If you see NS or MX record responses, you now also see the IPv4 A records and IPv6 AAAA records for that particular NS or MX record.

There are a number of other smaller changes and fixes.

Please update soon. You will need an active maintenance plan to do so. Click on Help/Check for New Version for the download links to the full installer. USB users are downloading an upgrade patch.

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!

11.82 Release Notes

- ARP Scan: Fixed problem where popup messages relating to updating the IP/MAC Address Database due to an IP address change would stop the scanning process. Hostnames are now correctly added if the IP/MAC address does not exist or is changed in the IP/MAC Address Database.
- DHCP Server Discovery: Revised method used for receiving and displaying DHCP Servers. Prior method did not always display every responding DHCP server.
- DNS Tools Core: Get Basic DNS Records now shows the A (IPv4) and AAAA (IPv6) records for any NS and MX responses.
- Network Connection Endpoints and others depending on operating system identification: corrected problems when used on Windows 8.1.
- SNMP Core and Advanced: Both tools now accept IPv6 addresses (do not include scope ID) for the target address. SNMP Scanner and SNMP Dictionary attack continue to only accept IPv4 addresses.
- Whois: DNS entered by user is now used for all DNS queries. Incoming data no longer causes autoscrolling to the end of the data.
- Updated SQLite to version 3.17.0
- Updated MAC address/Manufacturer database.
- Updated IP to Country database.
- Updated dates to 2017

Code signing now uses both SHA256 and SHA1 for maximum operating system portability.

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