NetScanTools® Pro Monthly Newsletter

www.netscantools.com

September 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...

Three releases (actually almost 4) since the last newsletter. More on the way. Important new topics below – check them out.

-Kirk

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.

Managed Switch Port Mapping Tool v2.77.1 released August 30, 2017

Managed Switch Port Mapping Tool v2.77.1 is a minor update with a couple of fixes and new serial and model retrieval for Adtran switches.

Here are the changes in this release.

- Fixed Max Bulk Reps value when you open the Import Devices in Switch Lists/Device Settings Editor. Importing list of devices automatically creates a switch group entry for each device making it faster to create a switch list. Imported devices now show in the list after the import is complete.

- Serial number and model are now retrieved for Adtran switches.

- Updated SQLite to version 3.20.1

- Updated MAC address/Manufacturer database.

Download the 'installed' version 2.77.1 from SwitchPortMapper.com and install it over the top of your current installed version.
http://www.switchportmapper.com/

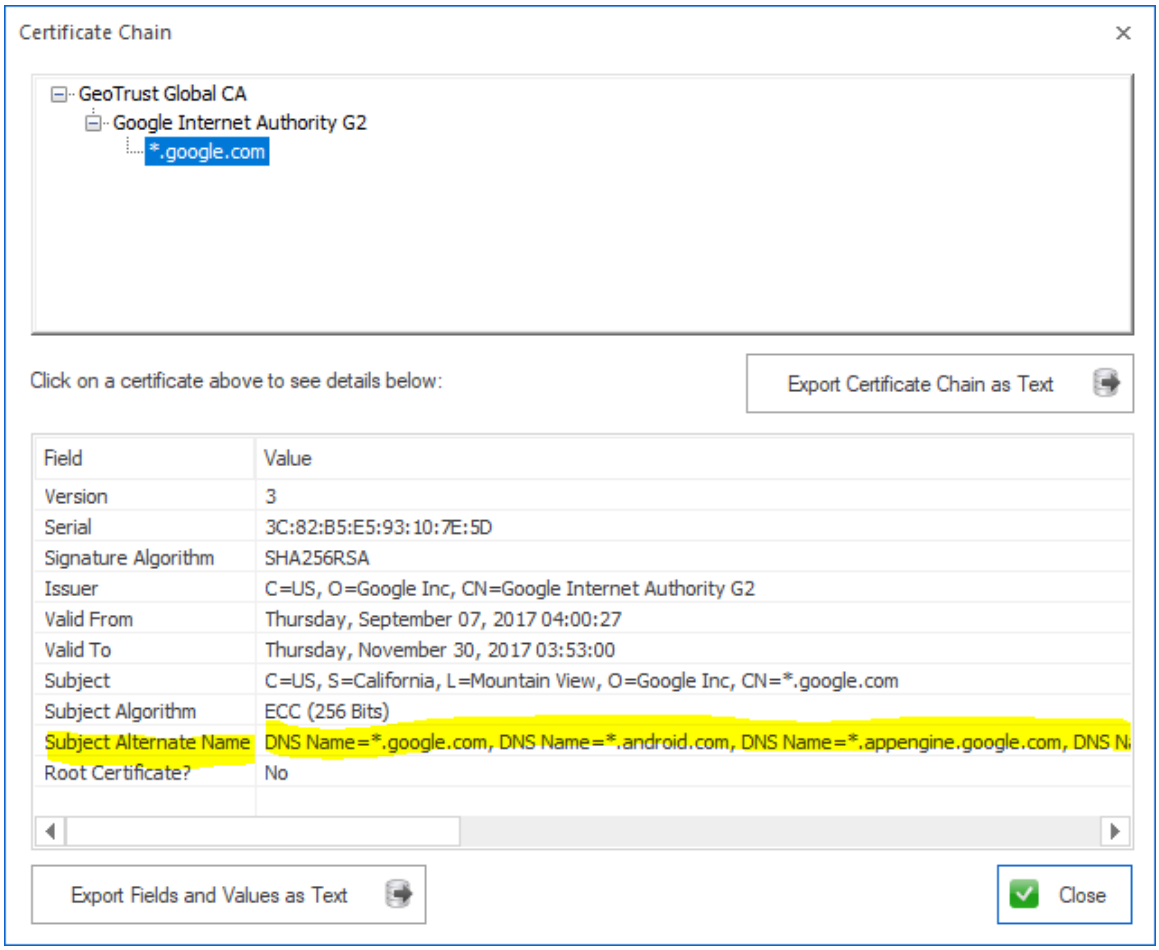
USB version users need to use the Help Menu/Check for Update selection to obtain the upgrade patch.

Managed Switch Port Mapping Tool v2.77.2 in testing

Managed Switch Port Mapping Tool v2.77.2 improves the reporting of Link Aggregation for Force10 switches. It is currently in testing and may be available by the time you read this. Please click on Help Menu/Check for Update to find out.

SSL Certificate Scanner Standalone 2.50 released Sept 13, 2017

We added parsing of Subject Alternative Name (SAN) fields. This important new addition shows up when you right click and use View Certificate Chain. Click on the bottom certificate and you will see the SAN fields. These fields are more important than ever because they identify alternate names for a server. In the image below you can see all the alternative names allowed in the google.com certificate.



Changes in this release.

- Added parsing of Subject Alternative Name (SAN) fields. Shown in the certificate chain. Right click to access.
- 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.
- Updated SQLite to version 3.20.1

For more information about this simple standalone tool, visit:
https://www.netscantools.com/ssl-certificate-scanner-standalone.html

The changes in the standalone version are reflected in the same tool included with NetScanTools Pro.

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)

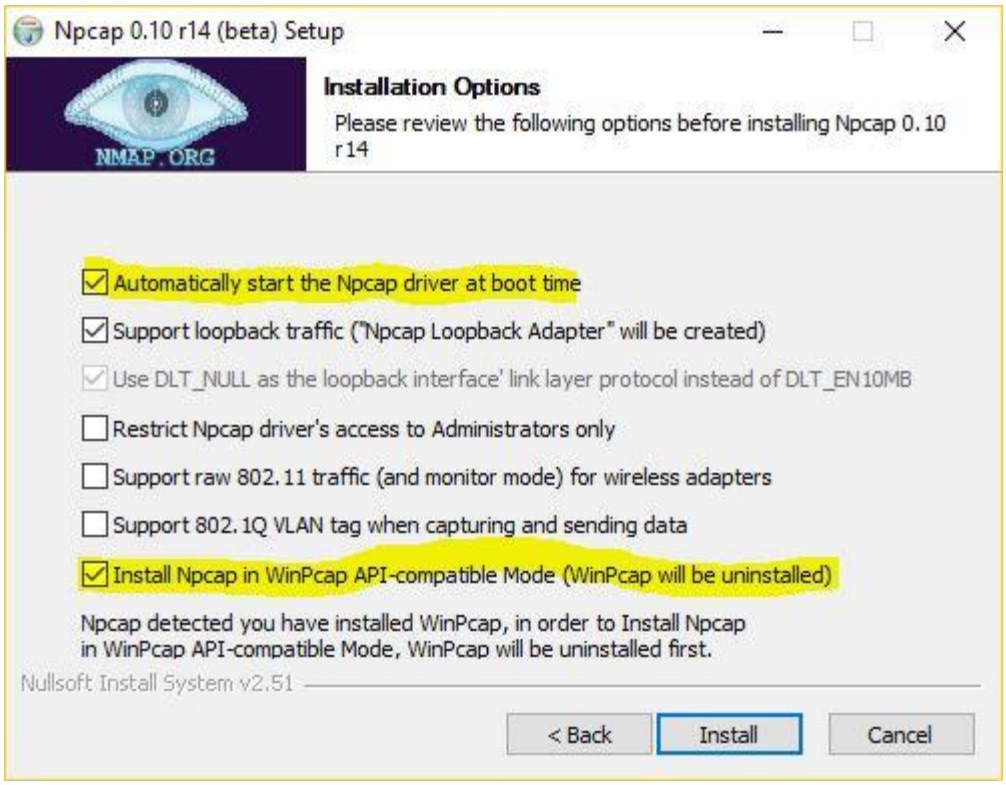
WinPcap has not been significantly worked on by its maintainers for several years now and is getting stale. While it still does work on Windows 10, I would not expect that work forever. Case in point: during the Windows 10 betas the NDIS 5 portion of the network software was deprecated for a version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

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

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.

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