NetScanTools® Pro Monthly Newsletter

www.netscantools.com

June/July 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...

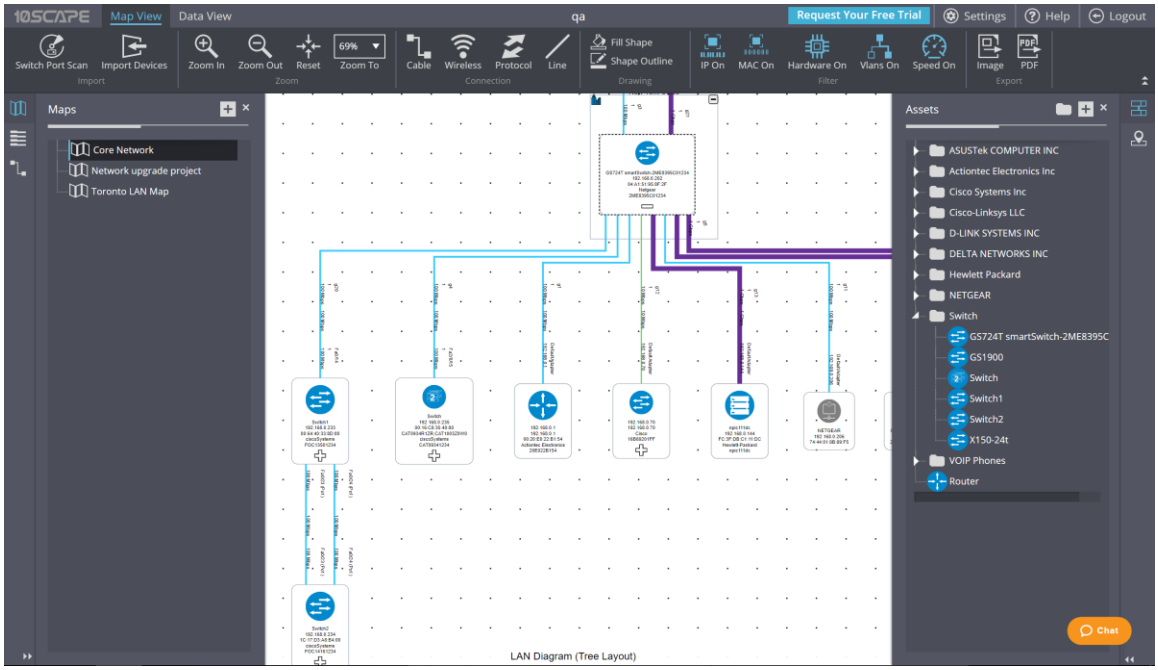
What happened to June? We delayed the June newsletter because of the new export feature in the Managed Switch Port Mapping Tool. Check out the npcap/WinPcap article.

-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 adds export of both Switch List and single switch manual mapping data in a format suitable for import into 10SCAPE's visual mapping system. Learn more here: http://www.switchportmapper.com/visual-network-mapping.htm



Managed Switch Port Mapping Tool v2.76 released

Managed Switch Port Mapping Tool v2.76 introduces export to 10SCAPE and an important SQLite update.

Another usability improvement was in the Switch List Device Settings Editor. A new separation has been introduced allowing you to define whether the new device is a switch or another device used for gathering ARP data. If you choose switch, it automatically creates an associated Switch Group. This group can be edited later, but it makes it quicker to build your Switch List from Switch Groups.

2.76 July 7, 2017

-Added export of results for 10SCAPE network mapping software. Column Order and Visibility Editor now has a default button for 10SCAPE required columns.

-Maximum width of the IP address column has been increased to allow up to 4 IP Addresses separated with commas.

-When adding a switch using Switch Lists/Device Settings Editor/Add New Switch it also automatically adds the switch to the Switch Group list.

-Fixed problem introduced in 2.74 by changing some SNMP request methods.

-Changed terminology from Server/Router 1/2 to Router/Server 1/2.

-Improved mapping of legacy Dell 3024, 3048, 5012 switches.

-Updated SQLite to version 3.19.3

-Updated MAC address/Manufacturer database.

Download the 'installed' version 2.75 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.

SMBv1 changes affect NetScanTools Pro tools

As you may already be aware, the WannaCry and related viruses that exploit insecure SMBv1 have changed the way the Network Shares – SMB Tool operates.

If you go into Programs and Features/Windows Features and uninstall SMB 1.0/CIFS File Sharing Support, it removes the 'Computer Browser' service. If the Computer Browser service is gone this tool will not work anymore - some information is shown but no shares are shown. In Windows 7, 8, 10 and the Server OSs you can use PowerShell commands to disable SMBv1 without uninstalling the SMBv1 support entirely. Please visit this Microsoft web page for those commands:

https://support.microsoft.com/en-us/help/2696547/how-to-enable-and-disable-smbv1-smbv2-and-smbv3-in-windows-and-windows

How to use npcap instead of WinPcap for NetScanTools Pro/LE

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.

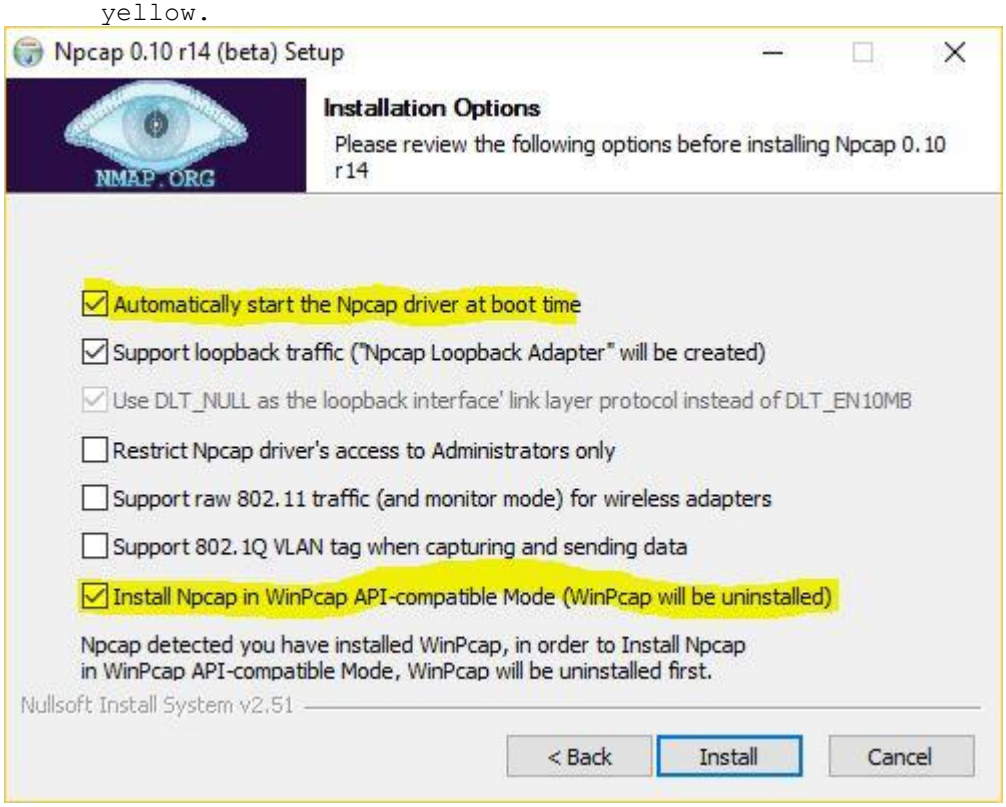
Npcap is the solution.

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.



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 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.

NetScanTools.com Website Redesign

As you are probably aware the NetScanTools.com website is very dated and based on Frontpage along with using Flash for ornamentation. This is changing every day. We are continuing the process of switching to Bootstrap. We are using the Unify template from wrapbootstrap.com. Here are a few examples of pages already changed:

http://www.netscantools.com/nstpro_passive_discovery.html

http://www.netscantools.com/nstpro_whois.html

http://www.netscantools.com/nstpro_port_scanner.html

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