

NetScanTools® Pro



Monthly Newsletter

www.netscantools.com

February 2014

 <http://twitter.com/netscantools>

 <http://www.facebook.com/NetScanTools>

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

 <http://netscantools.blogspot.com/>

In this newsletter:

News

- **Managed Switch Port Mapping Tool 2.30 released February 26, 2014**
- **We are now using a content download service**
- **NetScanTools® Pro - next update coming soon**
- **Are you having problems pasting text?**
- **NetScanTools® Pro Version 11.53 released November 1, 2013**
- **You have the NetScanTools Pro® Maintenance Plan, but you are still many versions behind – why?**

News...

From the Editor...

So much to do, not enough hours in the day!

-Kirk

Managed Switch Port Mapping Tool 2.30 Released February 26, 2013

This release has very important major changes to the way Ping Sweep operates. Ping Sweep ranges are now kept separately for each switch meaning better accuracy when using Ping Sweep – keep those ranges small, in other words make the Ping Sweep ranges correspond to actual used IP ranges that are handled by the switch. There is also a new way to retrieve IP/MAC addresses from devices responding to Ping Sweep. We also made a terminology change to reduce confusion with established practices.

Details of the changes in version 2.30 February 26, 2014

- Terminology change: 'Switch Groups' is the new name for Switch Configurations. This should reduce confusion with 'config' as defined by Cisco.
- Major Operational Change to Ping Sweep: Ping Sweep ranges are now specific to each Switch. This means that each Switch can now have a separate Ping Sweep IP range saved only for that Switch. This also extends to Switch Lists - in previous versions Ping Sweep was only done at the beginning of the Switch List execution. Now it is done for each Switch Group in the list that has Ping Sweep activated and configured with IP ranges. Ping Sweep ranges should be chosen to be the active IP ranges handled by the switch. Ping Sweep now also allows setting of ping packet timeout and retries. (Note: on first use of 2.30, the original Ping Sweep ranges will be copied to each Switch Ping Sweep range. You will need to edit the Ping Sweep range for each switch.)
- Added new method of obtaining MAC/IP Address entries: if a Ping Sweep ping response comes back, a name request is made to the target and responses are used to match IP addresses to MAC addresses (typically only Windows and Apple computer targets will respond).
- Reviewing History: when a previous switch mapping is loaded back into the results grid, the switch IP address now appears in the top program titlebar and the settings for that switch IP address are loaded into the left control panel. Now the user can turn on or off a port on that switch without manually loading the switch settings.
- Added a button to activate the Ping Sweep Editor from the Switch Group Editor.
- Fixed problem with Deleting old history data. Selections labeled 14 days and older were not working correctly.
- Updated SQLite to version 3.8.3.1
- Updated MAC address/Manufacturer database.

Get the new release at SwitchPortMapper.com.

NetScanTools® Pro – next update coming soon

In case you are wondering when the next update is coming, well it's coming along well. As you may be aware, ICAAN has approved quite a few new Top Level Domains (TLDs). We are adding support for as many of those that have whois servers as possible. TLDs like photo, build, club, pics and more will be included in the whois domain database meaning you will be able to do a whois query on the new domains.

The SSL Certificate Scanner now has a way to show and export the details of the certificate chain up to the root certificate.

Other changes are in work including recognizing when a security or anti-virus program is interfering with your need to paste from the clipboard into NetScanTools Pro. Ping Scanner (AKA Ping Sweep or NetScanner) will have a new shortcut button to scan a /24 network with one button push.

Look for the next release very soon.

Are you having problems pasting text?

Recently we had two NetScanTools Pro users (one in the US and one in Australia) report they could not paste text into NetScanTools Pro and one of them could not even complete registration. No matter what they did the pasting operation did not work. Ctrl-v or right click paste did not work at all. But they could paste into notepad.

The problem was narrowed down to this by one user and confirmed by the other: they were both running a popular security package called Webroot® SecureAnywhere for PC. One of its many functions is to prevent access to the clipboard from applications it is unfamiliar with. The application does this to stop clipboard stealing programs (like keyloggers) from obtaining private data and using it somehow. In this case the users were both using the same security app, but there may be other security apps that do the same thing: if the security program does not recognize the program requesting text from the clipboard during the paste operation, it empties the clipboard before it can be pasted.

The solution is simple:

1. Open Webroot® SecureAnywhere.
2. Click on the gear next to Identity Protection
3. Click on the Application Protection tab
4. Locate NetScanTools Pro (or the Managed Switch Port Mapping Tool) in the list and click on the Allow button. Copy and paste should now operate normally. If it does not, please contact Webroot® technical support.

The instructions above are unique to that application and there are probably others doing similar blocking techniques, so you will need to look for an application whitelisting method similar to the one above.

NetScanTools® Pro version 11.53 released November 1, 2013

This release is a very important release in that it corrects problems sending packets via WinPcap through Wifi interfaces and secondary network interfaces.

WiFi: Users have told us that *some?/many?/too many?* WiFi interfaces could not be opened for sending and receiving packets with WinPcap (all of our test interfaces worked fine). For example, in Ping you could not use the WinPcap ping modes with the selected WiFi interface – you got a message saying it 'could not open interface for packet sending. Please exit and restart NetScanTools Pro'. This was because the interface could not be opened in the default Promiscuous Mode. This has been fixed and any related error

messages have been significantly improved to tell you and us what the problem actually is.

Multiple Network Interfaces: Ping or Traceroute might be showing you two interfaces, one wired and one wireless, but we recently found you could only send and receive packets from the first interface in the list. That problem has been fixed.

Here are the details of the changes in v11.53.

NOTE: The following WinPcap related changes affect ARP Ping, ARP Scan, Duplicate IP Address Scanner, OS Fingerprinting, Packet Capture Playback, Packet Generator, Ping, Port Scanner, Promiscuous Mode Scanner, Traceroute, Connection Monitor, Packet Capture, Passive Discovery, SNMP Dictionary Attack and SNMP Scanner.

- Changed the way WinPcap supported interfaces are opened so that adapters that do not support promiscuous mode will be opened. This primarily affects WiFi adapters.
- Fixed a problem where if the computer has more than one WinPcap capable interface, packets exiting the secondary interface were not being assigned the correct MAC address of the default gateway for the secondary interface network.
- Significantly expanded error message reporting that appears if opening a WinPcap interface fails.
- Removed support for versions of WinPcap older than 3.1.

Other Changes:

- DHCP Server Discovery: added DHCP Server MAC Address column.
- DNS Tools - Core/Edit Hosts File, TimeSync: fixed administrator privileges detection so the 'privileges required' message will only appear if you do not have enough privileges. Also affects some portions of Network Connection Endpoints.
- Packet Generator/Packet Capture Playback: added support for opening and playing .pcap files in addition to .cap files.
- Ping Enhanced: fixed problem where TCP Ping was not sending a number of packets beyond the number shown in the Settings/TTL field. Default TTL (Max Hops) now set to 255.
- Updated SQLite to 3.8.1
- Updated database files.

You have the NetScanTools® Pro Maintenance Plan, but you are still many versions behind – why?

We see this all the time when people register. We see it when they renew their maintenance plan - we check the logs and see that they have never logged in and downloaded updates. For whatever the reason, the question remains, why are they installing 11.01 (for example) when we are at 11.42?

There are many good reasons to install the latest version: First of all is bug fixes, secondly there are new tools introduced with each .1, .2, .3, .4 etc. edition and thirdly, there are database updates.

OK – A Quick Review on upgrading to a new version. First thing you need is an active NetScanTools Pro maintenance plan. Start NetScanTools Pro and click on Help/Check for New Version. An embedded browser window opens up on the right side of the program. Click on the download link, a popup window appears. Enter your login credentials (shown to you in the program right above the embedded window) and download the zip file. Exit NetScanTools Pro and run the contents of the zip file which is actually a full install. Restart it and verify the latest 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

'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.