



January 2008 Newsletter

In this newsletter:

- **New Release - NetScanTools Pro 10.54, November 28, 2007**
- **Windows Vista 32/64 Bit and NetScanTools Pro**
- **Maintenance Plan – NetScanTools Pro**
- **New Power User Tip for NetScanTools Pro**
- **How to Upgrade NetScanTools Pro**
- **New Release - Managed Switch Port Mapping Tool 1.80, January 2, 2008**
- **FAQs - Managed Switch Port Mapping Tool**
- **New Websites Up and Running**
- **Coming Soon – NetScanTools Pro Self-Paced Training**
- **SHARKFEST 2008**
- **Contact Information**

Now that the holidays are over we are getting back to normal here in Sequim – so here is our first newsletter of 2008. Long time readers will notice that we have expanded the newsletter with new topics. We wish you a successful and Happy New Year.

New Release - NetScanTools Pro 10.54, November 28, 2007

This release made several important changes to NetScanner (Ping Sweep), OS Fingerprinting and the Automated tools. As usual, there were also some bug fixes. All the databases were updated and WinPcap was updated to version 4.0.2. The program now fully runs on Windows Vista but we still intend to make some additional changes in a later version to discontinue use of the registry and move the final sections of the program to VC++2005 (v8).

The last few versions have made extensive internal changes to Ping, Traceroute, Packet Generator (we moved custom ICMP packet generation from Ping to Packet Generator), Network Topography, Name Server Lookup, RPCInfo, Automated Tools and more.

You can view the full list of changes by release from within NetScanTools Pro by selecting Online/NetScanTools Pro News or going to this URL:
<http://www.netscantools.com/nstpronews.html>

Upgrading: If you need help upgrading to 10.54, please see the section later in this newsletter.

Newsletter continues on the next page

Windows Vista 32/64 Bit and NetScanTools Pro

NetScanTools Pro 10.54 has been successfully tested on **both** Windows Vista 32 (x86) and 64 bit (x64). It is a 32 bit application that operates in wow64 in Vista 64. We do not have a native x64 binary at this point. We suggest choosing 'Run as administrator' if WinPcap is not automatically started under Vista or if you are seeing no data when you expect data. WinPcap is set to start at boot if you select that option during NetScanTools Pro installation. If you do not start WinPcap at boot, you will have to do 'Run as administrator' every time or set the start menu/desktop link properties to have those privileges. You can stop WinPcap by typing **net stop npf** at a command prompt – elevated privileges may be required.

The USB version has also been tested on Vista 64 and it operates correctly. You will always need to use 'Run as administrator' with the USB version because WinPcap is not pre-installed on the system you are using it on.

Maintenance Plan - NetScanTools Pro

An active maintenance plan allows you to obtain the NetScanTools Pro 10.54 installed version by full download from our secure site. One year of maintenance (beginning at date of purchase) is included with a new or upgrade license. A core benefit of the plan is the ability to download updates. In calendar year 2007 we released 6 updates mostly targeted towards Windows Vista compatibility and 5 updates in calendar year 2006.

We have noticed that some people have allowed their maintenance plan to expire. The cost to renew the plan increases if you wait to renew over 30 days beyond the maintenance plan expiration date. If you are unsure when your plan expires, please feel free to contact us by email or phone (see end of newsletter for contact information). Of course you can always continue using the program even after the maintenance plan expires, but you will not get any changes or updated databases.

New Power User Tip for NetScanTools Pro

This is a new topic in our newsletter. We want to highlight a part of the program you may not be aware of. All tips refer to the latest version, currently 10.54.

Did you know that our Packet Viewer tool can provide trace data to Wireshark? The Packet Viewer tool is found by clicking on the Tools left control panel group, then on Tools (alpha order)/Packet Viewer. Click on the **Start Packet Viewer** button to launch the program.

To capture packets select Allow All Packet Types, then select your available WinPcap compatible interface by IP address and press Start Capture. As the capture progresses, you will see a received packet count number incrementing just below the Stop Capture button.

After pressing Stop Capture, you will see a list of packets in the display grid. You can right click on any packet and choose "View Selected Single Packet Data in built-in Hex Viewer". This gives you a quick breakdown of the packet header information. If you need to know more details or have a complete packet disassembly, right click and select "View All Packet Capture Data in external Network Protocol Analyzer" and it will launch Wireshark to view the working packet capture file – that is, if Wireshark is installed. To get the Wireshark packet capture and analysis program, go to <http://www.wireshark.org/>. If you are interested in learning more about

Wireshark, there is going to be a conference in California called SHARKFEST. More information about SHARKFEST is found at the end of this newsletter.

You can also save a single packet or the whole working packet capture file to a file so that you can work with it later either using our Packet Viewer or using Wireshark. These options are also in the right click menu. The packet capture files are saved with the extension .cap which is normally associated with the Wireshark program.

How to upgrade NetScanTools Pro

We have heard from some customers that they do not know how to upgrade to the latest version or they paid for their maintenance plan and never received any upgrades. The ability to upgrade your software has *always* been right there within the software.

How to upgrade:

1. You must have the NetScanTools Pro installed. It must be registered AND you must have applied the "NST Pro 10 Registration Code" message we sent back to you – if it is not registered, our secure site will not have any unique login credentials for you.
2. Start NetScanTools Pro and click on the Online group in the left panel. Then click on the Check for New Version icon. Once the web page appears in the right pane, you will see the Login link text. (**NEW:** Version 10.54 adds a Check for New Version link to the Help menu)
3. After clicking on the Login text, you will see a popup asking for a username and password. Those are found in the Login Access Credentials area as shown in the image on the next page. **The username and password ARE CASE SENSITIVE.** We recommend using copy and paste.

If your access credentials do not work, it is highly likely that your maintenance plan expired or you have a typo in your username or password. Please contact us with the username and password you are using and we can check your status (*if you do not send us the username and password you are trying to enter, we will have to ask you for it resulting in additional delays*).

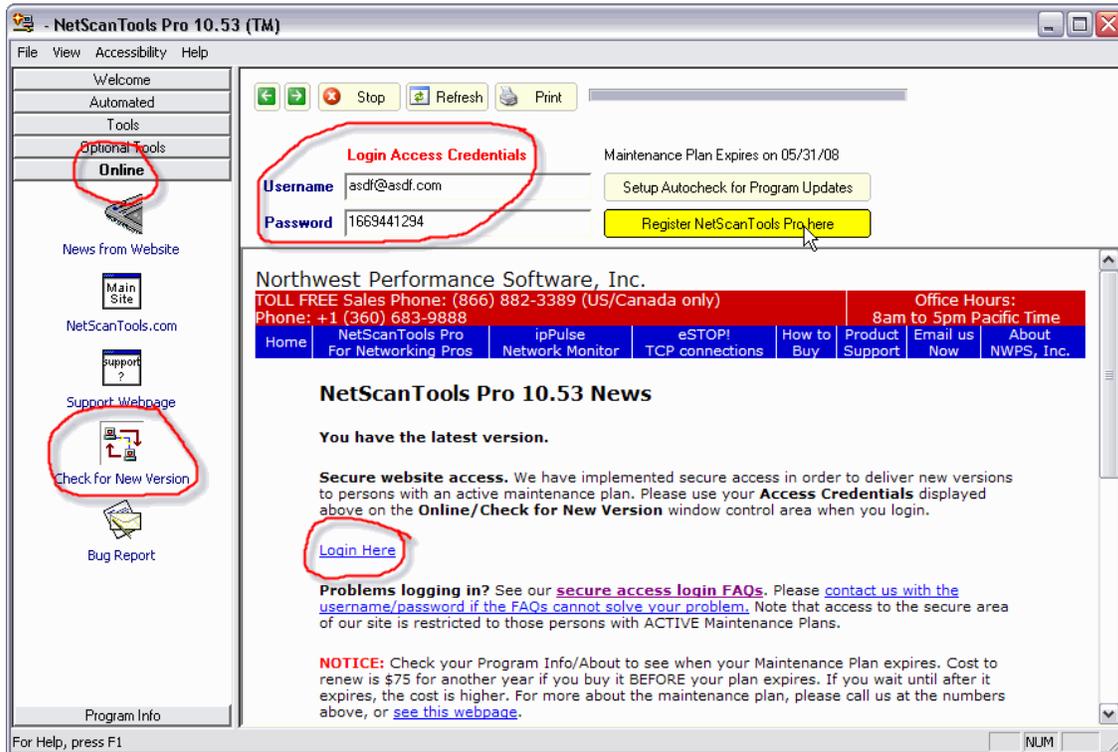
You must have a valid maintenance plan to download an upgrade.

Once you have logged in to the secure server, the **full download** is ready for installation by those of you with installed versions. You will need your CDKEY/serial number to run the installer – see the About NetScanTools Pro window to get it. Please install over the top of your current installation.

USB Version users can download an upgrade patch from this same window. The latest version of the Managed Switch Port Mapping Tool is also available for download from this window.

Newsletter continues on the next page

The image below shows where in the program you need to go to login to our secure site.



New Release - Managed Switch Port Mapping Tool 1.80, January 2, 2008

1.80 is the fifth release since our last newsletter in August. The frequency of releases is directly due to valuable input and suggestions from users – keep those suggestions coming! Some highlights of those releases:

- More methods of retrieval of ARP tables.
- Ping Sweep for refreshing ARP tables prior to retrieval.
- Better HTML report formatting and analysis.
- Enhanced VLAN identification including reporting of multiple VLANs per port if the switch supports it.
- Reporting of assigned VLANs even if the port is unused.
- Improved duplex reporting.
- Ability to map Netgear, D-Link, Nortel and Linksys switches and report enhanced device information about each one.
- Reporting of switch port speeds exceeding 1 Gbs.

We are working towards making this tool the leader in manufacturer independent switch mapping tools. We are well on the way towards this goal with many new additional features planned for release in 2008.

More information about the Managed Switch Port Mapping tool:

<http://www.netscantools.com/spmapmain.html>

You can visit this URL to immediately download the trial:

<http://www.netscantools.com/switchportmapperdownload.html>

FAQs - Managed Switch Port Mapping Tool

We have included this article again in this issue.

Lately we have noticed some questions regarding the use of the Switch Port Mapping Tool that continue to come up. We would like to address three of the most common points.

1. **We frequently hear from people who would like to be able to import the results directly into Microsoft Excel.** The XML export option is designed for exactly that purpose. Any version of Excel 2002/2003/2005 can directly open (not import) the XML file we generate. To export in XML, right click in the results and choose Export XML/Save Results or press the floppy disk save icon on the toolbar or choose File/Export XML/Save Results. Then select the header or left column options, and finally save the file with the XML type selected. Use File/Open in Excel to open the saved file. It will bring in the formatting including row heights, column widths and coloring. More determined people can even import the XML file into Access.
2. **"I have several switches and every time I change between them I have to re-enter the IP address and community name".** We addressed this with the release of 1.50 several months ago. 1.50 introduced the use of an SQLite database to save many things including the IP addresses and community names of devices. We introduced what we call Switch Configurations. A Switch Configuration is defined as the unique combination of the Switch IP Address, Primary Server IP Address and Secondary Server IP Address. You can access previous Switch Configurations by pressing the blue button with the three dots in it to the immediate right of the Switch IP Address entry field. This allows you to change between previous switch query configurations quickly. Additionally, the other two blue buttons next to the Primary and Secondary IPs allow access to the list of previously queried SNMP devices (including the switches) and you can select the IP and community name that matches the IP from the list. These settings are saved on a per user basis, so if another user logs into the computer and uses the Switch Port Mapping Tool, they will have their own personalized database with their own separate Switch Configurations. You can view many of the tables that have contain this information by going to the main window and pressing Database Maintenance button and selecting the table.
3. **"The results show many MAC addresses, but almost no IP addresses. Why isn't it working right?"** It is working fine given the input data – the problem is in the ARP table data sources you are providing. The switch does not keep track of IP addresses it keeps track of the MAC addresses of devices attached to a particular port. Finding an IP address given a MAC address is difficult. To do that we need accurate, well populated ARP tables. ARP tables map IP addresses to MAC addresses for use in Ethernet networks. There are four methods for gathering ARP tables and all the ARP tables are combined into one ARP table in the SQLite database. The switch is queried for its ARP table and so is your computer. The two remaining sources are the Primary and Secondary Server/Router devices. These devices should be located on the same network segment as the devices the switch is keeping track of and they are critical in building the Combined ARP Table. If you do not use one or both of these devices for ARP queries, you will have a small Combined ARP Table and the program will not be able to associate IP addresses with MAC addresses. You can view your Combined ARP Table by pressing

the Database Maintenance button and selecting the Combined ARP Table view. This is best done after querying a switch. By default the Combined ARP Table is cleared on exit, but you can change that behavior in Setup. The HTML report that appears in your web browser at the end of a switch map query shows the count of the number of items found in each device ARP table under the heading Summary of ARP Table. This summary shows the contribution each device is making to the Combined ARP Table and will help you decide the quality of the contribution from each of the four sources of ARP tables.

Coming Soon - NetScanTools Pro Self-Paced Training

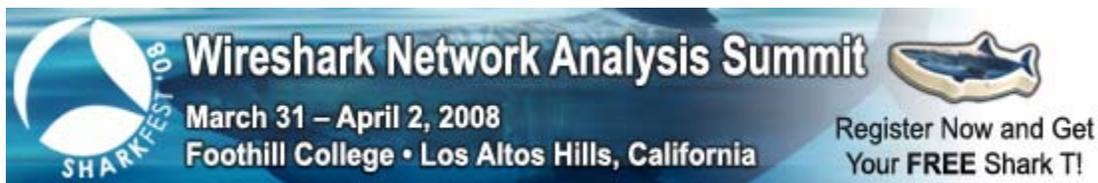
We are partnering with the Protocol Analysis Institute to develop quality in-depth self-paced training on reconnaissance, traceback, troubleshooting and network discovery techniques using NetScanTools Pro. The course will be defined as a new "Laura Chappell presents(TM)" course to be available through NetScanTools.com, Wireshark University and Protocol Analysis Institute web sites. More details to be announced soon.

SHARKFEST 2008

First Annual SHARKFEST Event for Wireshark Users and Developers

CACE Technologies and Wireshark University host the 1st Annual SharkFest Event March 31 – April 2, 2008 at beautiful Foothill College in Los Altos Hills, California USA. Join us for 3 days of training and discussions on network analysis, troubleshooting, security, Wireshark development, communications dissection and more!

Please visit <http://www.cacetech.com/SHARKFEST.08/> for more information.



New Websites Up and Running

We now have created two new websites for showcasing our products: www.switchportmapper.com and www.nstpro.com. They are currently basic sites focused on our products and we intend to significantly improve them in the coming months.

Contact Information

If you have any questions or suggestions, please feel free to email.

Northwest Performance Software, Inc.
PO Box 1375
Sequim WA 98382-1375
(360) 683-9888
www.netscantools.com
sales [at] netscantools [dot] com