NetScanTools® Pro
Monthly Newsletter
www.netscantools.com

February 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…

I've been working on two things during February: continuing the NetScanTools.com website revision and the Managed Switch Port Mapping Tool has been released.

-Kirk

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/nst_le_main.html

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

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

Managed Switch Port Mapping Tool v2.73 February 23, 2017

Managed Switch Port Mapping Tool v2.73 has a new feature and a few improvements and fixes. The new feature is the ability to export results in JSON format – more on that below.

Other improvements focused on Cisco switches specifically a better way to determine which ports are used and unused for the web page reports. Previously (and for other switch brands) the report was created by counting the 'up' and 'down' ports. Now it retrieves more specific information from Cisco IOS and reports how long a port has been down so the user can make a more informed choice as to whether the port is actually being used. In other words, the device attached to the port could be temporarily turned off and yet the port is still technically 'used'.

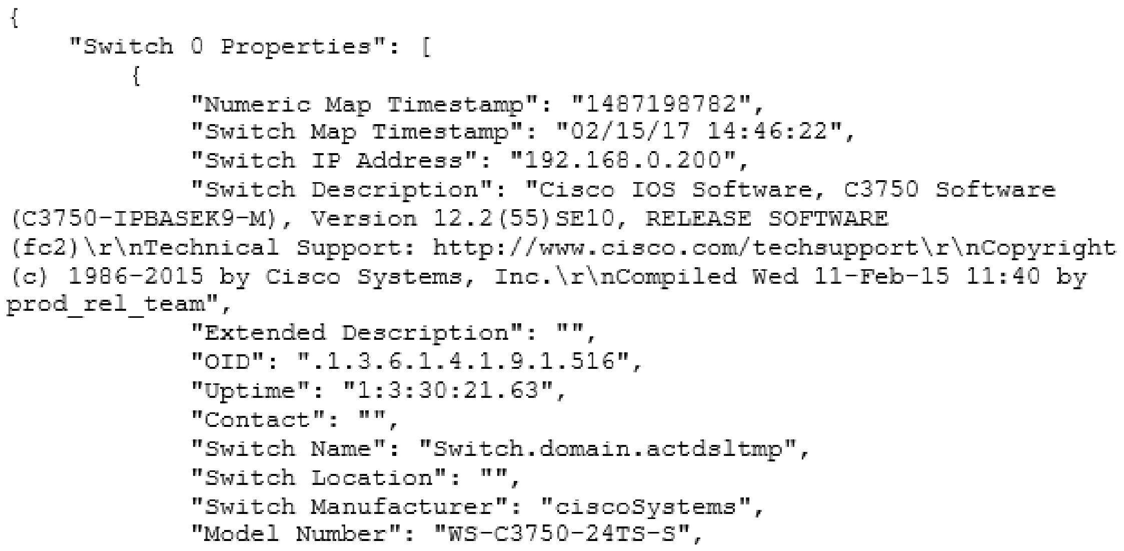
Related to the used/unused port issue is a new test to verify that required ifType and Status columns are active and visible to correctly determine port states. If they are not visible, you will be informed how to turn them on using the Column Order and Visibility Editor. This applies to all switch brands.

A new limit was added to the IP column. In previous versions the algorithm searched for MAC addresses and returned as many IP addresses as were found. A user sent us a screenshot where there were in excess of 50 IP addresses for the one MAC address. The limit is now 16 and you can control it in Global Settings.

Another noticeable fix is to the situation (rare) where the switch does not return the mapping between bridge ports and ifIndex port values. It was offset by one row in previous versions.

Other minor fixes were to XML exporting and an improved method of checking tables on startup.

JSON Exporting – verbose 'human readable' format. This was added in 2.73 and you can access it by clicking on Review History in the left control panel. Then select either Switch List or Manual and select the list to export or the single switch mapping to export. You can export it with the extension json, txt or doc. If you export a list, all the switches in the list will be represented in the report. Example of what the switch properties section looks like:



```
{
    "Switch 0 Properties": [
        {
            "Numeric Map Timestamp": "1487198782",
            "Switch Map Timestamp": "02/15/17 14:46:22",
            "Switch IP Address": "192.168.0.200",
            "Switch Description": "Cisco IOS Software, C3750 Software
(C3750-IPBASEK9-M), Version 12.2(55)SE10, RELEASE SOFTWARE
(fc2)\r\nTechnical Support: http://www.cisco.com/techsupport\r\nCopyright
(c) 1986-2015 by Cisco Systems, Inc.\r\nCompiled Wed 11-Feb-15 11:40 by
prod_rel_team",
            "Extended Description": "",
            "OID": ".1.3.6.1.4.1.9.1.516",
            "Uptime": "1:3:30:21.63",
            "Contact": "",
            "Switch Name": "Switch.domain.actdsltmp",
            "Switch Location": "",
            "Switch Manufacturer": "ciscoSystems",
            "Model Number": "WS-C3750-24TS-S",
```

Download the 'installed' version 2.72 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.

Version 2.73 Release Notes. February 23, 2017

- Added JSON file exporting from Review History. Both single switch manual mapping and switch list mapping export are available.
- Added 16 IP limit to number of IPs shown in the results grid for a single MAC address. It can be changed in Global Settings.
- Improved algorithm for determining used/unused ports in Cisco IOS switches. It now shows the time since the last packet came into a port. This gives you a better understanding of how long the port has remained unused.
- Improved algorithm for determining used/unused ports by making sure required ifType and Status fields are active and visible. Enable them in Settings and Tools/Column Order and Visibility Editor.
- Corrected row offset issue where if switch does not provide bridge to ifIndex mapping, the ifIndex is used to complete the mapping.
- Fixed several issues with exporting to XML. For example, page height and width are now limited correctly and will not produce a warning on opening the file in a spreadsheet application.
- Moved 2 transient SQL tables into the working database.
- Improved method used on startup to check tables for changed/added columns.
- Updated dates to 2017.
- Updated SQLite to version 3.17.0
- Updated MAC address/Manufacturer database.

Switch Port Mapper Column Order and Visibility Editor

Customers have been surprised when they ask for something in the Managed Switch Port Mapping Tool only to find out it's been in there for years. Usually it involves the columns that are NOT visible. The default set of visible columns is outnumbered by the not visible set of columns you can show. That set of invisible, available columns will be added to in the next release.

How to get there. Click on the Settings and Tools menu item, then on Column Order and Visibility Editor (about 2/3 way down). The left side list are the columns that are available to be shown. The right side list shows the columns that are shown and the order that they are in. You can move a column from the left side to the right side to make it visible and you can change the order of the visible columns. Note that some columns are specific to certain brands like Cisco.

Try it out, look for new columns in the next release.

About the NetScanTools Pro Duplicate IP Scanner

Lately the Duplicate IP Scanner has been getting more attention by people looking at the NetScanTools Pro Demo. One thing they ask for is how to find duplicates on other subnets. We tell them that they have to connect the computer running NetScanTools Pro to that subnet. Why? Because this is an ARP based tool and ARP is not routed.

The tool works by sending ARP packets to IPv4 addresses. If two devices have the same IP addresses, two replies will come back. How can two IPs have the same address? With difficulty because operating systems like Windows try to detect that problem when they obtain an IP from a DHCP server. The most typical way duplicates happen is to have more than one DHCP server on a network segment with overlapping ranges or by having a static IP device (maybe a printer) having it's IP not excluded when setting up the range on a DHCP server. No matter how it happens, the effect is that communication on the subnet to the devices sharing an IP is hampered due to an IP address having two different MAC addresses.

When running the scanner, run it more than once because replies to our broadcast ARP packets may not come back the first time from both devices.

USB version users – database cleanup

This applies to both NetScanTools Pro and the Managed Switch Port Mapping Tool USB Versions. As you may know, both applications save data to an SQLite history database which is located on the USB flash drive. The database file can grow quite large – particularly in the case of the switch port mapper. We recommend 'cleaning up' the database periodically by either deleting all records or some of the records by date. If you want to back it up before cleanup, simply copy the database somewhere safe while the application is NOT RUNNING. These instructions work for both the USB and installed versions.

How to do this for NetScanTools Pro USB Version:

1. Start NetScanTools Pro.
2. Click on left control panel Program Info, then on Database Maintenance.
3. Select 'Erase all Results Tables' or 'Erase Results Older than' with the appropriate option and follow the directions.
4. Press 'Refresh Database Statistics' to see the change in size.

How to do this for the Managed Switch Port Mapping Tools USB Version:

1. Start the Managed Switch Port Mapping Tool.
2. Click on left control panel Review History.
3. Delete Results by Date or by Selected Results are along the bottom of the window. You may also Delete All Results.
4. Changes will be reflected in the Current History Database Size field near the middle left side of the window.

NetScanTools Pro 11.81 released Dec 16, 2016

This version has significant changes to the SNMP Scanner and ARP Scanner. The SNMP Scanner now has three new columns that you can populate with a specific OID query to the responding targets. Use this for serial or model numbers or whatever you need. The ARP Scanner has a new column that gives you a way to make notes or comments about a specific device. The notes are tied to the MAC address so they will reappear every time that MAC address is seen regardless of the current IP address.

Important fixes: we removed the requirement to have VC++ 2013 runtime installed. We also created a functionally equivalent for the broken GetBestRoute IP Helper API function on Windows 10.

Additional changes were made to assure that the selected WinPcap interface is the correct one for monitoring or sending packets to the targets. Those changes depended partly on a functioning GetBestRoute and now it works right.

We are also working to be sure that npCap (from the nmap project) can be successfully used as long as it is installed in 'WinPcap compatibility' mode.

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!

11.81 Release Notes

- Removed the requirement for using Visual C++ 2013 runtime.
- ARP Scanner: new comments column. Comments are saved by MAC address - allows you to add a friendly name of the target or something more descriptive than the IP address.
- ARP Scanner, Promiscuous Mode Scanner, ARP Ping, Duplicate IP Scanner now have improved checks to confirm target is on same subnet as the outgoing interface.
- DNS Core and DNS Advanced now have buttons to give you quick access to the other DNS tool.
- DNS Traffic Monitor: fixed startup interface selection problem for when more than one interface is present.
- Packet Viewer: change for systems using npCap (from nmap) instead of WinPcap to allow longer time for capture file to close before using it to update display.
- Passive Discovery: improved capture filter sanity checks.
- SNMP Dictionary Attack (accessed from SNMP Advanced Tool): added tests to verify selected WinPcap interface can receive packets from the target. Heading columns now shown on opening of previously saved XML results.
- SNMP Scanner (accessed from SNMP Advanced Tool): added tests to verify selected WinPcap interface can receive packets from the target. Heading columns now shown on opening of previously saved XML results. Added three (3) new optional user defined OIDs to retrieve - press Settings to add them. SNMP error messages can now be optionally ignored. Improved retrieval of SNMP data after initial scan is complete.
- GetBestRoute IP Helper API function stopped working correctly with release of Windows 10 Anniversary Edition - a functional replacement has been added. This affects a number of WinPcap related tools.
- Increased WinPcap error buffer string size.
- Manifests have been added to assure version helper functions return correct information.
- Installer no longer automatically overwrites SNMP Dictionary Attack dictionary file.
- Compiled on Windows 10 Anniversary Edition.
- Updated SQLite to version 3.15.2
- Updated MAC address/Manufacturer database.
- Updated IP to Country database.

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