netTools

axence

User manual

Copyright © 2006-2014 Axence Software, Inc.

axence

Axence NetTools

Network tools

Axence Software, Inc

NetTools is great solution for fast network diagnostics. It consists of several powerful solutions: ping, MultiPing with a history of response time and packets lost for monitoring the availability of your hosts, trace, lookup, port scanner, network check & scan, and SNMP browser.

Axence NetTools

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

The entire risk of the use or the result of the use of this software and documentation remains with the user. No part of this documentation may be reproduced in any means, electronic or mechanical, for any purpose, except as expressed in the Software License Agreement.

This software and documentation are copyrighted. All other rights, including ownership of the software, are reserved to Axence Software, Inc.

Axence Software and Axence NetTools are trademarks or registered trademarks of Axence Software, Inc. All other product and brand names are trademarks or registered trademarks of their respective owners.

Contents

0

Part I netTools 2

1 Introducing netTools ... 2
2 What's new ... 2
3 System requirements ... 3
4 Available tools ... 4
5 Activation ... 5
6 Window layout ... 5

Part II How to...? 8

1 How to monitor my hosts? ... 8
2 How to check the availability of my hosts? ... 8
3 How to check where is the network problem? ... 8
4 How to check network quality and bandwidth? ... 8
5 How to scan ports, hosts, networks? ... 8
6 How to use SNMP? ... 8
7 How to use Wake On LAN feature? ... 9

Part III NetWatch - Host monitoring 12

1 NetWatch ... 12
2 Alerts ... 18
Alerts - General information ... 18
Setting alerts ... 20

Part IV WinTools 23

1 WinTools ... 23
2 Enabling WMI on remote computers ... 23
3 Cannot use WinTools ... 25

Part V Local info 27

1 Introduction ... 27
2 NetStat ... 27
3 Local IP info ... 29
4 ARP and routing table ... 29
5 Statistics ... 30

Part VI SNMP 33

1 SNMP ... 33
2 MIB files compiler ... 34

Part VII Other Tools 37

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

1 Ping 37
2 Trace 38
3 Lookup 39
4 Bandwidth 40
5 NetCheck 42
6 TCP/IP workshop 42
7 Scan host 43
8 Scan network 45
9 Command line 46

Index 48

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Part I

1 netTools

1.1 Introducing netTools

netTools - a great solution for measuring your network performance and quickly diagnosing network problems. Its most powerful component is graphical NetWatch with a history of response time and packets lost (for monitoring the availability of your hosts). It also consists of other popular tools like trace, lookup, port scanner, network scanner, and SNMP browser. What makes netTools unique, according to our customers, is the most highly intuitive user interface.

The current PDF version of the manual is available for downloading at:
http://axence.net/help/netTools/en/netTools.pdf

1.2 What's new

Version 5.0 (12/09/2012)

v5.0 introduces:

- NetWatch – not only PING anymore!
  - monitoring of TCP/IP services – monitoring the response time and lost packets percentage for the following services: HTTP, POP3, SMTP, FTP and 50 others
  - monitoring of any TCP port
  - DNS-based host identification; automatic address checking every 10 minutes
  - host export/import
  - support for TLS/SSL protocols in alert e-mails
- SNMP browser – MIB file compiler – allowing the addition of a new MIB database object in order to support new custom SNMP devices
- Traceroute – geographic host map – graphic information on subsequent hosts along the packets route.
- Geographical location – information on the geographical location (country) of a remote IP address (in tools: NetStat, NetWatch, Ping, Trace). This option may allow the detection of suspicious connections, e.g. to Russia or China, established by malware. Geographical information is also available for the address given in every tool.
- Wake on LAN as a parameter for netTools launch – remote starting or waking machines via network adapter

Version 4.0 (03/03/2009)

v4.0 introduces:

- netTools is now completely FREE and unlimited. However still requires free activation. After activation all tools remain active.
- Both Free Axence netTools and Axence netTools Proffessional discontinued - now we have Axence netTools Pro, which is a new free version.
- DNS resolver improved - all tools have independent resolvers and work faster.
- Node names in NetWatch - long awaited identification of monitored nodes.
- Several bug fixes.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Version 3.1 (10/09/2007)

v3.1 introduces:

- Command line. You can create shortcuts to perform repetitive tasks.
- Mail alerts fixed

Version 3.0 (11/13/2006)

Version 3.0 introduces several new tools, which will help you in everyday administrative tasks:

- **WinTools -** This tool is designed to list exhaustive system information from Windows computers (using WMI). It has several predefined queries allowing to read service list, disk information, process list etc. You can also define your own queries.
- **NetStat** - It displays the list of your computer's inbound and outbound network connections, including the information on open TCP and UDP ports, IP address, and connection states. NetStat also shows the process name using the connection (socket).
- **Local info** - Displays several tables with important information about local configuration: network statistics for TCP/UDP and ICMP, IP address table, ARP table, IP routing table, network adapter info.
- **TCP/IP workshop** - It provides you with the ability to establish low-level TCP and UDP connections to troubleshoot and test different networking services. With this tool you can send raw data to any port on the remote computer. You can also listen on any local port to see all data the remote computer sends.
- **E-mail alerting system improved in NetWatch** - The whole component responsible for sending alert e-mails has been rewritten to ensure it's reliability:
  - The program does not require any external SMTP server to send alert e-mails.
  - You can test it's operation to make sure all options are correctly entered.
  - While testing you will see messages describing potential problems.
  - The program saves a log with the information about every alert e-mail sent, so you could verify if it is working properly.

1.3 System requirements

Operating system

- Windows XP/2003/Vista/2008/7/2008R2/8/2012
- Administrator rights required (see the note below)

Hardware

- 500 MHz processor (or better)
- At least 128 MB RAM
- Video: 800x600 or more, high color
- Network adapter card connected to your LAN/WAN

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Administrator rights

To run properly computer administrator rights are required. Otherwise netTools cannot send ICMP requests - this Windows feature is strictly disabled for non-administrators. If you are administrator, but the program still warns about insufficient right, try running the program as administrator - select "Run as..." from the icon context menu and then provide credentials. This is especially important on Windows Vista and Windows 7.

Third party firewalls

If you have any third party firewall/antivirus that prevents ICMP/SNMP requests, please add netTools to its exception list.

1.4 Available tools

NetWatch
A robust tool which enables you to monitor the availability of several hosts and their response times simultaneously. You can also set several thresholds for netTools to notify you by e-mail, message, icon tray or sound in case of any problems (i.e. host not responding, slower connection, or too many packets lost).

NetWatch includes multiping with the best charts, with a history of response time and percentage of packets lost. Along with alerting, this is the most important part of netTools because it helps you track the availability of your hosts and estimate network load over time.

WinTools
This tool helps to deal with reading WMI information from Windows computers. It has several predefined WMI queries allowing to read service list, disk information, process list etc. You can also define your own queries.

Local info
Displays several tables with important information about local configuration: network statistics for TCP/UDP and ICMP, IP address table, ARP table, IP routing table, network adapter info.

NetStat (part of Local info)
It displays the list of your computer's inbound and outbound network connections, including the information on open TCP and UDP ports, IP address, and connection states. NetStat also shows the process name using the connection (socket).

Ping
A visual replacement for Windows ping, but with a 5-minute history. Very easy to use when you just need to check one host quickly.

Trace
This tool is not just a replacement for windows tracert. It shows you information about every host on the route, its response time, and packets lost. This lets you quickly determine where the problems are occurring. It's easy to locate hosts with degraded performance or that are just overloaded. Additionally, visual information on subsequent hosts along the packet route is displayed.

Lookup
This works like nslookup, but shows you all records at once. You do not have to worry about syntax or record names. And--of course – you get whois information about the domain you are querying.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

	Bandwidth Would you like to know how fast your network is? This is the tool for you. What's important- is that it will measure bandwidth without overloading your network.
	NetCheck With this tool, you can check the quality of network hardware in your LAN. Poor quality sockets or wires can slow a network down. Without NetCheck it's hard to find the cause.
	TCP/IP workshop It provides you with the ability to establish low-level TCP and UDP connections to troubleshoot and test different networking services.
	Scan host Allows you to check for all open ports and running services. It not only checks if the port is open, but also sends a request and checks whether a reply meets specific criteria. So you can be sure that the host is running HTTP, POP3, Oracle or other services (and not only has a specific port open). Port scanner can also discover some Trojans and spyware.
	Scan network Would you like to find all the nodes running in a network (even in a remote network)? No problem, just enter the IP range to check and you will quickly get a list of nodes and the services running on them.
	SNMP A full SNMP browser, which you can use even if you don't know a thing about SNMP. We have prepared several general categories for each system so you do not have to browse through thousands of SNMP parameters—although you can certainly do so if you are a networking pro.

1.5 Activation

You may freely use netTools for an unlimited time. However, after initial 30 days, free activation is required. Please follow the instructions in the program to activate it. All tools will be available after the activation.

1.6 Window layout

The netTools window layout is intuitive and very simple to use.

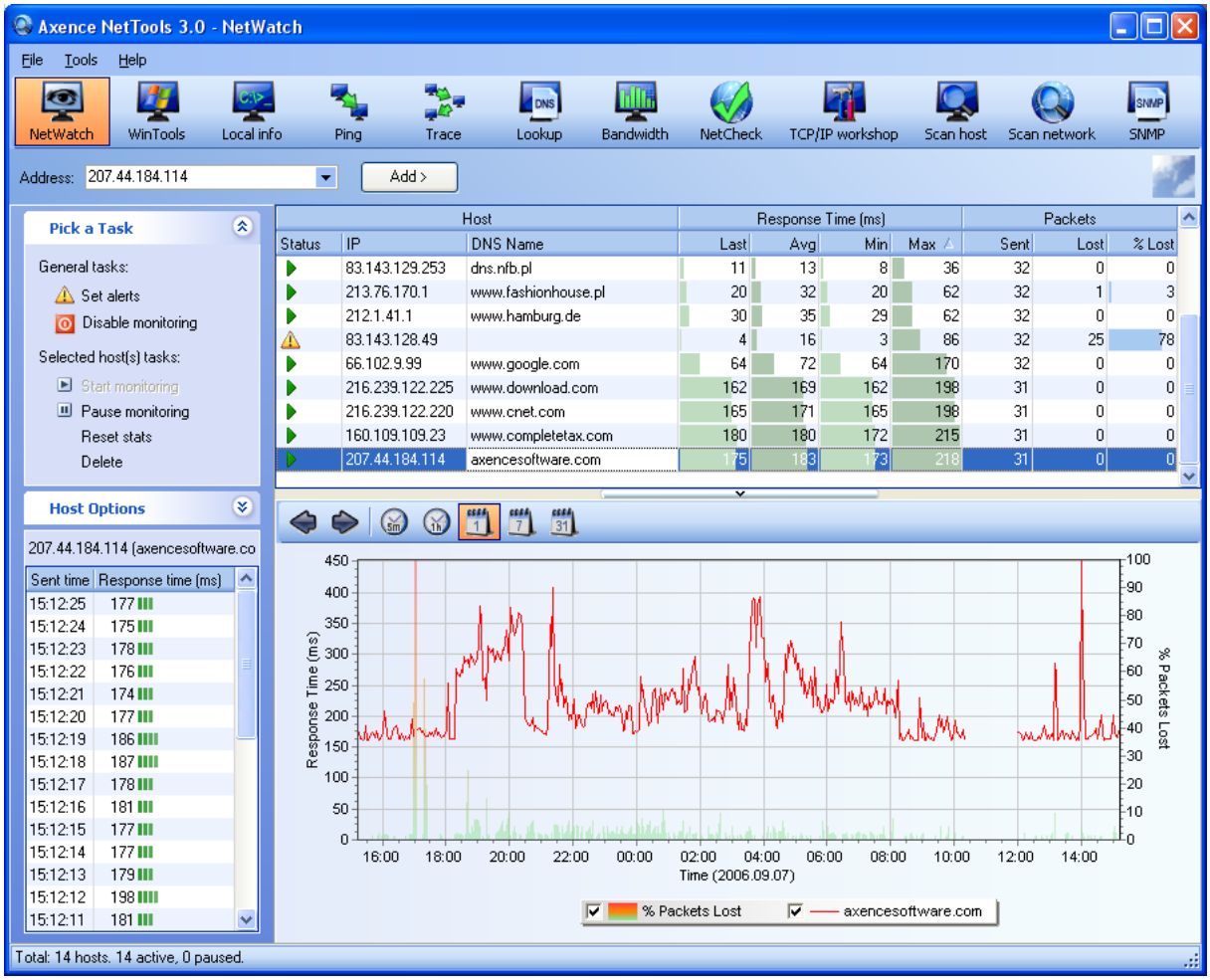
Navigation and address bar

The navigation and address bars are located at the top of the window. Use the navigation bar to select the tool you want to use and the address bar to enter the DNS name (or IP) of the host you want to check or scan (depending on the tool selected).

Sidebar

The sidebar is located on the left side of the window. It usually contains general information (like the number of packets sent) and options.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.



Main area

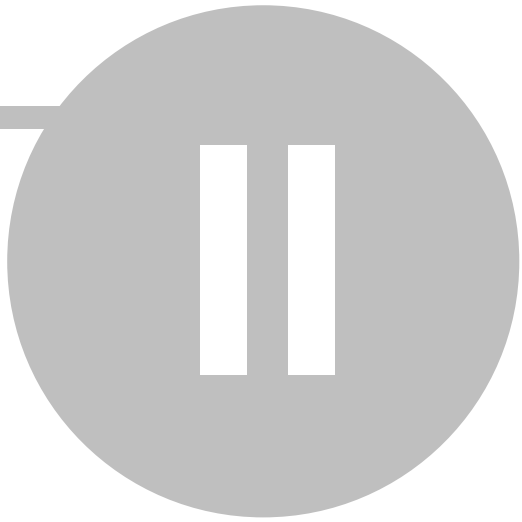
The main area includes different controls (grids, charts etc.) depending on the tool selected. In the example shown in the picture (NetWatch), this is a grid listing all hosts and a chart representing response times and packets lost.

Advertising box

The bottom left corner of the window contains an advertising box displaying information on Axence products.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Part



2 How to...?

2.1 How to monitor my hosts?

If you would like to monitor a host for a longer time use NetWatch. It checks hosts using ICMP (ping) and stores response time and percent of packets lost for future analysis. NetWatch not only monitors hosts but also can alert you about any problems using e-mail, message box, sound and icon tray.

To quickly check the availability of one host, use Ping tool.

2.2 How to check the availability of my hosts?

To quickly check the availability of one host, use the Ping tool. It sends ping (ICMP) packets to the host and presents the response time on a chart.

If you want to check the quality of the connection to this host, use Bandwidth. It will read out the network connection speed between your machine and the selected host.

2.3 How to check where is the network problem?

If you would like to locate a problematic host, use Trace. It will show you where the problem lies in the connection between you and the selected host. Trace shows response time and percentage of packets lost while checking each host on the route to the host being checked.

2.4 How to check network quality and bandwidth?

To check the quality of the connection to a selected host, use Bandwidth. It will measure the network connection speed between your machine and the selected host.

If you would like to check for wiring in your LAN network use NetCheck. It usually allows to detect malfunctioning sockets and wires.

2.5 How to scan ports, hosts, networks?

For scanning a host use Host scan tool. It will show you all the services and ports open on the host.

Scan network tool allows you to check for running hosts in a selected network. It lists all nodes and the services running on them.

2.6 How to use SNMP?

SNMP (Simple Network Management Protocol) is not so simple as the abbreviation indicates. But with SNMP tool, you can easily check all SNMP information on a host without knowing a thing about this protocol, OIDs etc.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

2.7 How to use Wake On LAN feature?

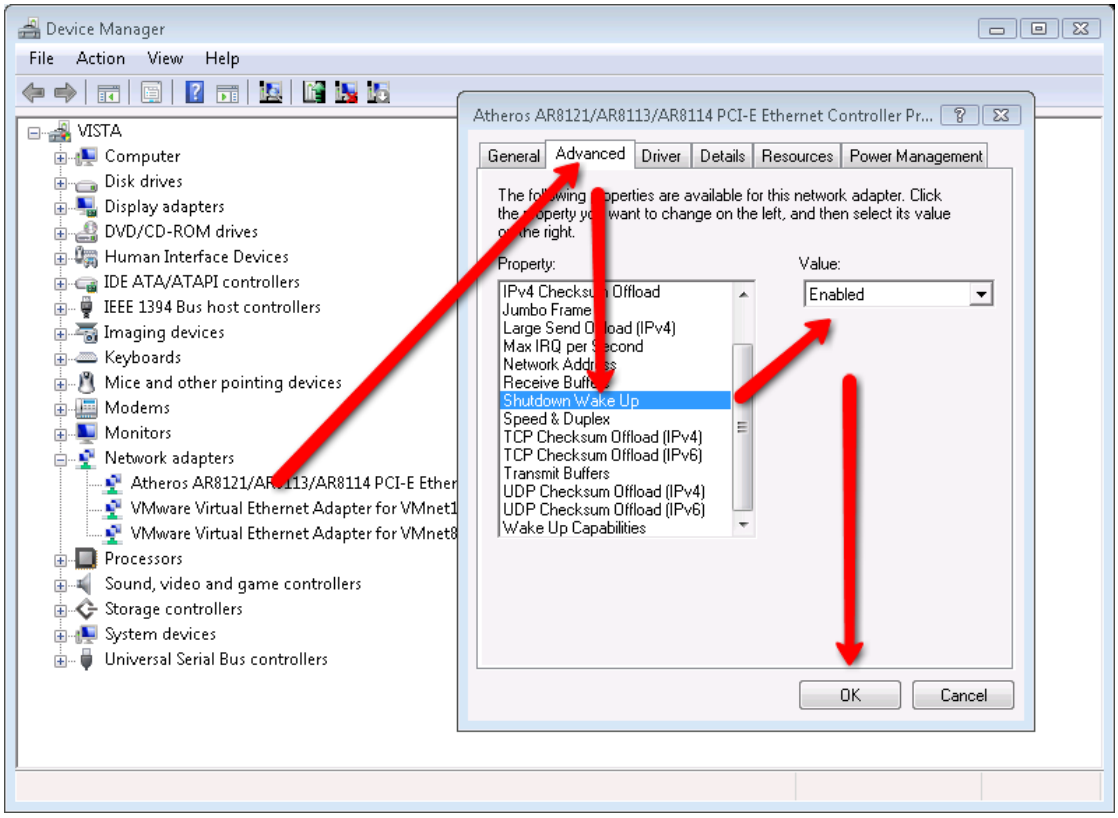
The Wake On LAN feature allows machines to be turned on remotely. It is available, if the MAC address of the machine to be turned on or woken up is known. Apart from this, the machine must be preconfigured (as described below) and, if the machine will be woken up from outside of LAN, port redirection must be set up in the router.

To turn on the specific monitored device, e.g. with NetWatch tool, right click the device and select **Tools | Wake On LAN** in the pop-up menu.

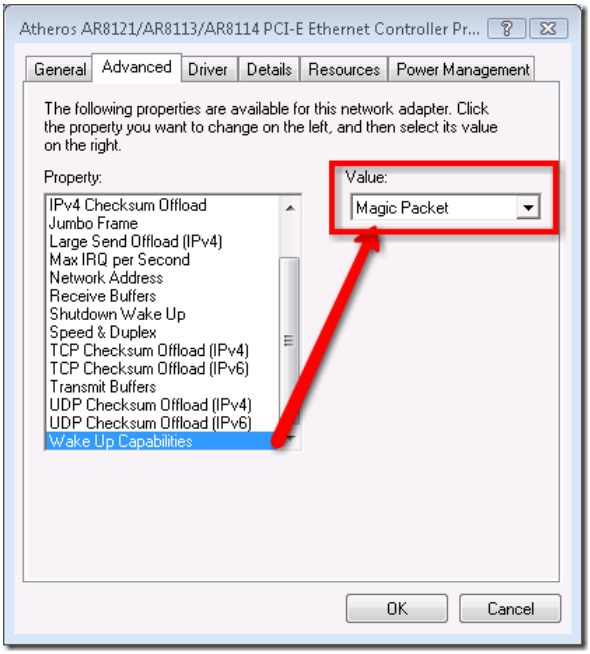
Configuration of the device to be woken up

The settings depend on a specific device. Examples of requirements and settings:

1. To enable Wake On LAN feature, an ATX power adapter, at least 1A, +5Vsb is necessary.
2. BIOS settings:
   in Power (Management) or Advanced tab, enable Wake On LAN – the option can have different names, e.g. Wake On LAN, MAC Resume From S3/S4, MACPME Power Up Control, Power On By Onboard LAN, Power Up By Onboard LAN, Resume by LAN, Resume By WOL, Resume on LAN, Resume on LAN/PME#, Wake on LAN from S5, Wake Up On LAN, WakeUp by Onboard LAN or WOL (PME#) From Soft-Off.
3. Network adapter settings:
   a. Navigate to network adapter settings in Windows | Control Panel | Device Manager.
   b. Set the options in Power Management tab to enable the waking up of the machine (option names depend on the network adapter, e.g. Allow the device to wake the machine from sleep mode).
   c. Enable waking and Wake On LAN in Advanced tab – option names can differ depending on the network adapter. Examples of settings are presented below:

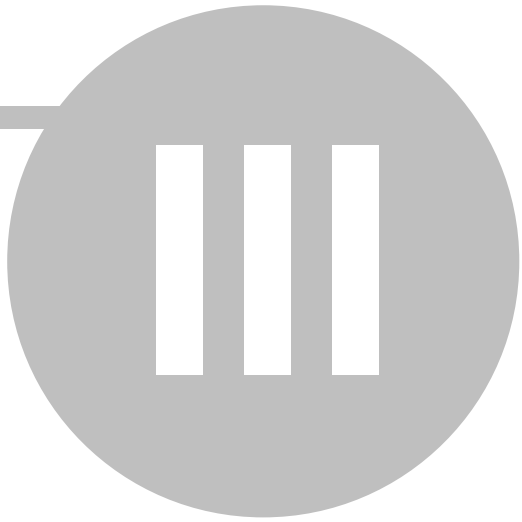


Copyright © 2005-2014 Axence Software, Inc. All rights reserved.



Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Part



3 NetWatch - Host monitoring

3.1 NetWatch

NetWatch is a sophisticated tool to monitor the availability of your hosts. It continuously sends ICMP (ping) packets to all hosts on the list and allows you to check response times and the number of lost packets. This tool provides a history of these values for reporting host status over time. NetWatch allows you to set several notifications in case of a host not responding or problems with a connection. Please refer to the Alerts section for more information.

To start monitoring a host

1. Select the **NetWatch** tool on the navigation bar.
2. Enter the host DNS name or IP address in the address bar.
3. Select type of monitoring: **TCP Port**, **PING** or other **Service**.
4. Click the **Add** button or press Enter.

Information provided

The main table presents basic information for each device: DNS name and IP address, geographic location of a remote IP address (helping to detect suspicious connections established by malware), response times (min/max/average), and the number of packets sent and lost.

On the main chart, you can see response times and % of packets lost for selected time. If you would like to see the exact values of response time in milliseconds, take a look at the grid placed in the sidebar. This grid stores response times for the last 5 minutes.

Main chart

On the main chart, you can see response times and % of packets lost for a selected time. Response time is presented as a line chart and % of packets lost is presented as a gradient area chart.

There is a toolbar located over the chart that lets you change chart type and time period:

Changing chart time period

You can see historical data in several time periods (e.g. the last 5 minutes, 1 hour, 1 day, 1 week and 1 month). To select the appropriate period, just select the corresponding icon on the chart toolbar.

To scroll the chart backward and forward, use the arrow icons located on the chart toolbar.

Options

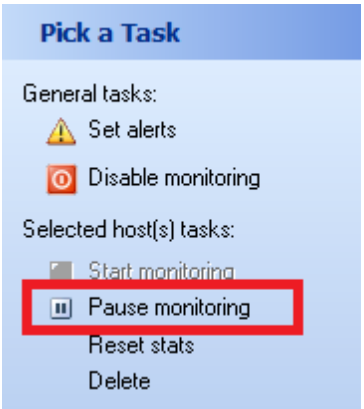
The user can select whether the device will be identified with IP address or DNS name. It is especially useful for services based on a variable IP address.

You may change monitoring frequency and timeout value for selected hosts. Just select a host or several hosts and enter the desired values in the **Options** section on the sidebar.

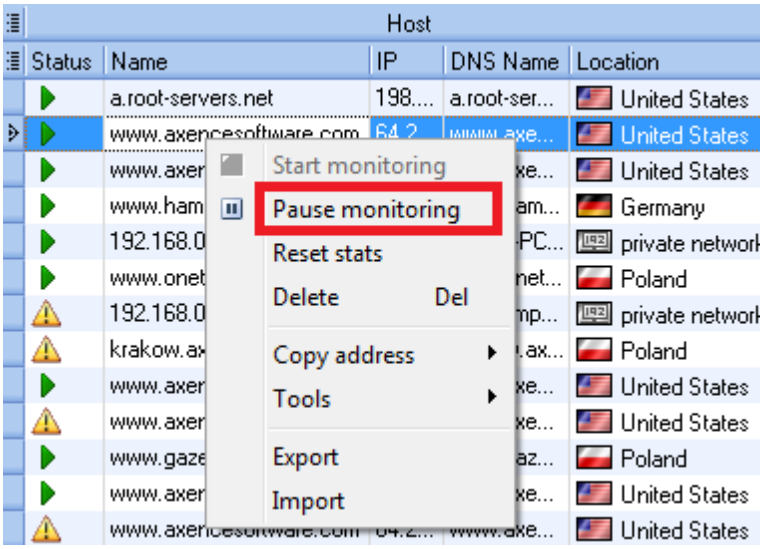
Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

To pause the monitoring of selected host(s)

1. Select a host or several hosts on the grid.
2. Select **Pause monitoring** option located in the **Pick a task** section on the sidebar.



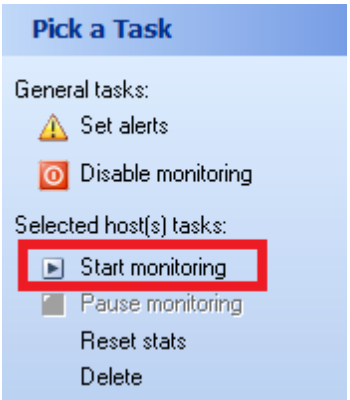
To stop the device monitoring, you can also right click the given device and select **Pause monitoring** in the pop-up menu.



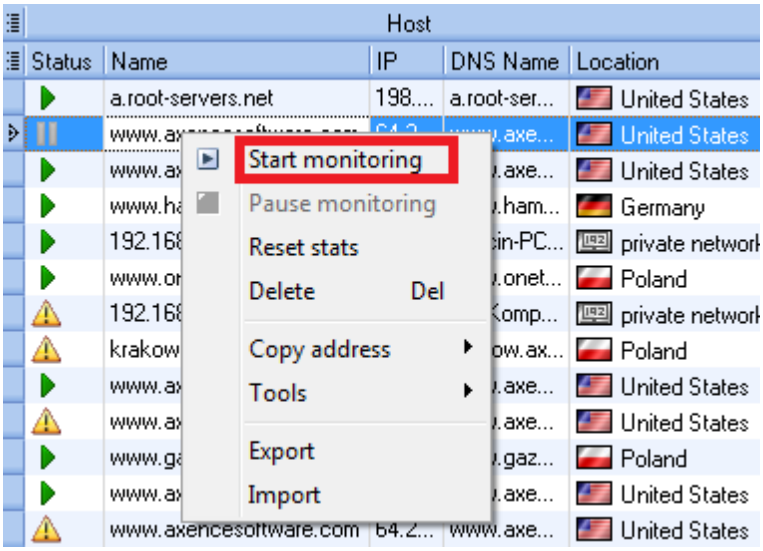
To resume monitoring selected host(s)

1. Select a host or several hosts on the grid.
2. Select **Start monitoring** option located in the **Pick a task** section on the sidebar.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

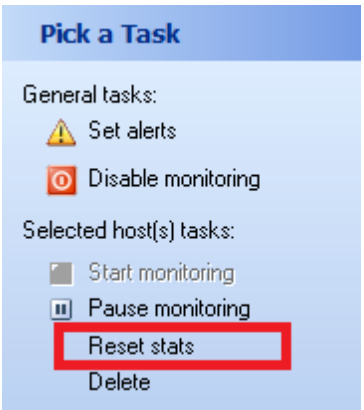


To run the device monitoring, you can also right click the device and select **Start monitoring** in the pop-up menu.



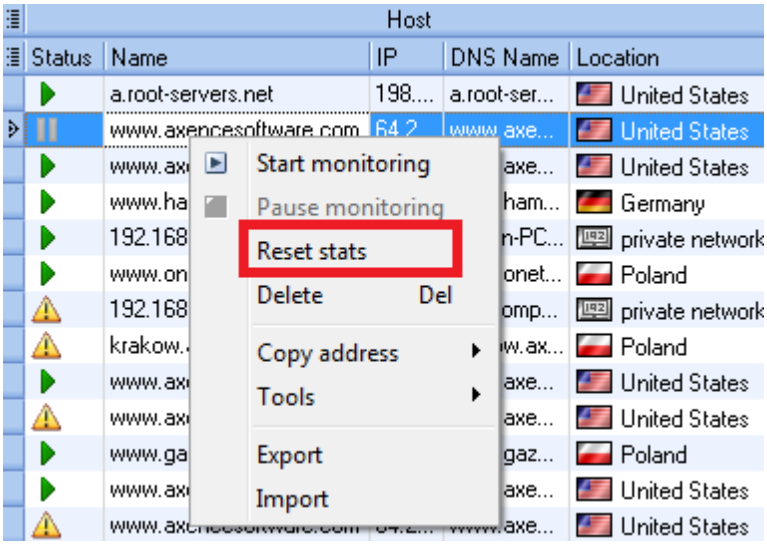
To reset statistics

1. Select a host or several hosts on the grid.
2. Select **Reset stats** option located in the **Pick a task** section on the sidebar.
3. The program will ask if you would also like to remove stored statistical data for selected hosts (response time and % of packets lost). If you no longer need them select **Yes** in the message box. If you want to retain them answer **No**.



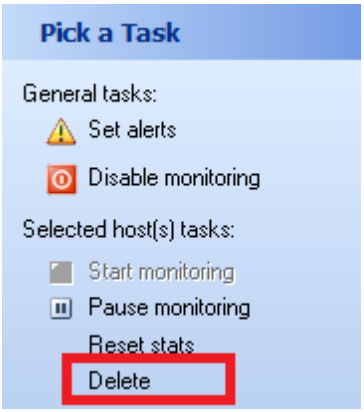
Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

To reset the device stats, you can also right click the device and select **Reset stats** in the pop-up menu.



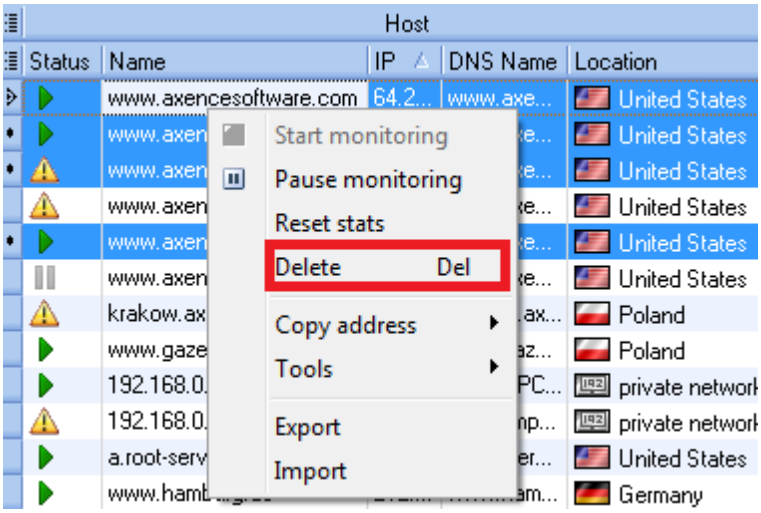
To remove a host or hosts

1. Select a host or several hosts on the grid.
2. Select **Delete** option located in the **Pick a task** section on the sidebar.
3. The program will ask if you would like also to remove stored statistical data for selected hosts (response time and % of packets lost). If you no longer need them select **Yes** in the message box. If you would like to retain them answer **No**. If you keep stored data, then they will be available when you add the same host again.



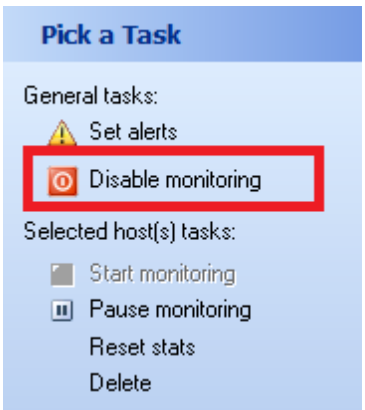
To remove the devices, you can also right click the device and select **Delete** in the pop-up menu or press **Del** button.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.



To disable/enable monitoring of all hosts

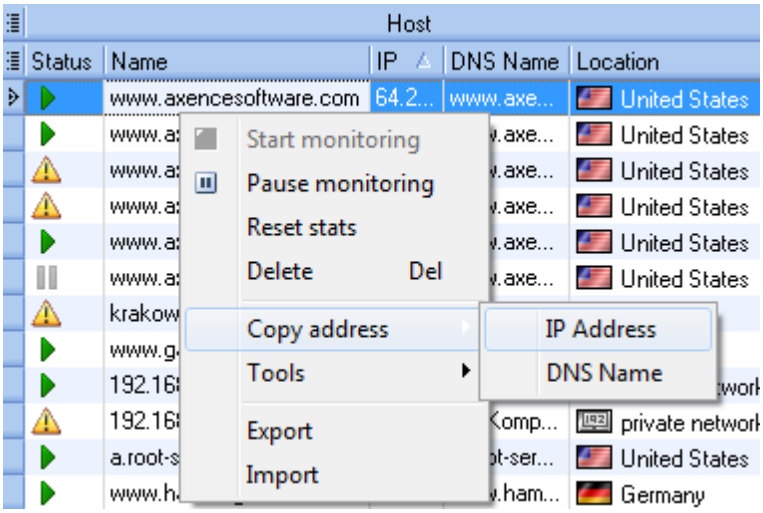
You can turn monitoring off completely by selecting **Disable monitoring** option located in the **Pick a Task** section on the sidebar. This does not change the status of any host (active/paused). **Enable monitoring** command turns monitoring back on after it has been suspended.



To copy a DNS name or IP address to clipboard

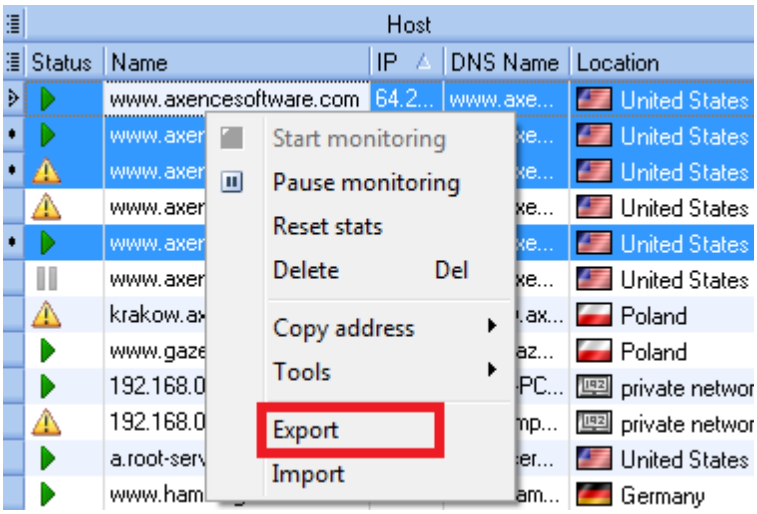
You can copy a DNS name or IP of the selected host to clipboard. Just right click a host in the grid and select **Copy address | IP Address** or **Copy address | DNS Name** from the context menu.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.



Data export

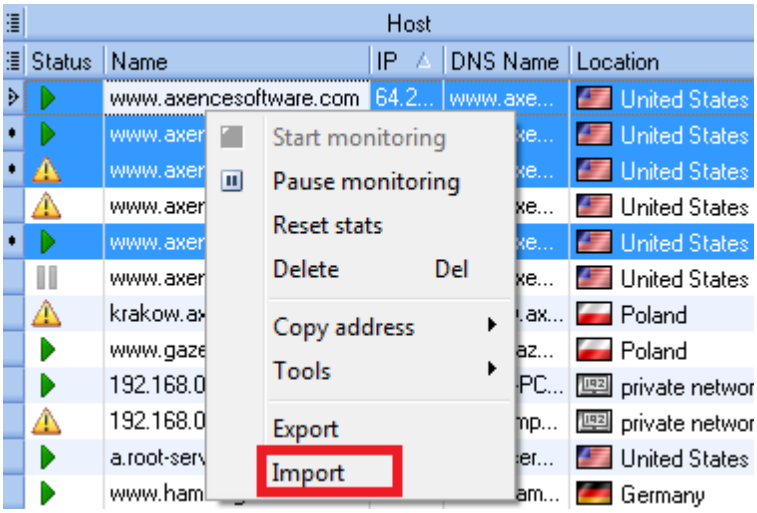
To export the table with device data, select **Export** in the context menu. Then choose one of the formats: **html**, **xml**, **txt**, **xls**, **json** (netTools file). If you want to export only the address list, select **Address list (*.txt)**.



Data import

NetWatch can import two types of data: a text file with a list of addresses and monitored services and netTools file in format json. To import the table with device data, select **Import** in the context menu.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.



Tools

The following tools can be used from the pop-up menu:

- Trace
- Lookup
- Bandwidth
- Wake On LAN

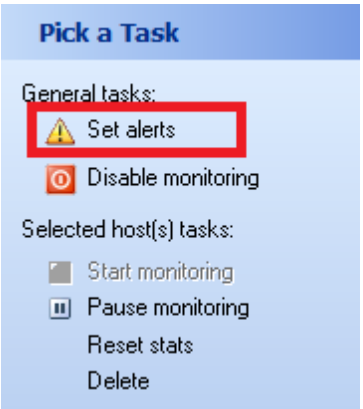
For more information, see the chapters about specific features.

3.2 Alerts

3.2.1 Alerts - General information

In case of any problem with a connection or a host being monitored, NetWatch can send a notification to the administrator. You can define several conditions when an alert event is generated and also several notification actions. netTools can also send a notification when a problematic situation ends - for example when a non responding host starts to respond.

To enable alarm, select **Set alerts** in the **Pick a Task** section on the side bar.



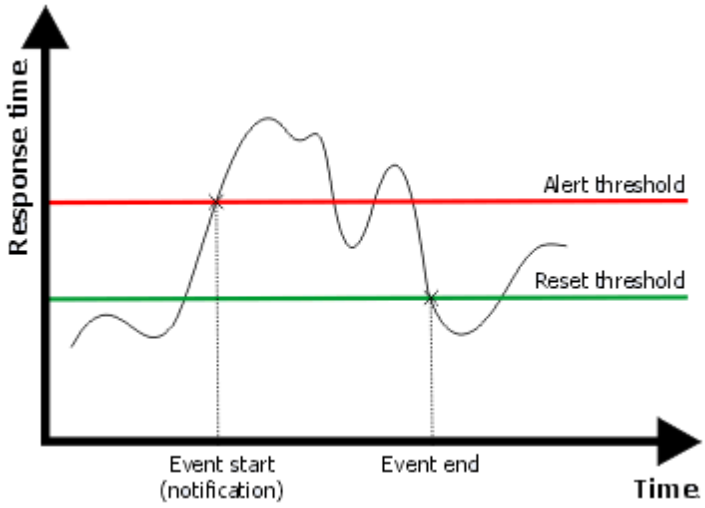
Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

When is an alert generated?

There are 3 conditions when the alert is generated (event types):

1. **Host not responding**. This means that the host is not responding to ping requests at all.
2. **Packet loss rate too high**. You can define the percentage of packets lost, that triggers the alert.
3. **Response time too high**. You can set the threshold for response time. After the average response time exceeds this threshold an event will be generated.

In points 2 and 3 you define the "reset" threshold for the event. This is important - otherwise an alert would be generated every time the condition is met. That could cause the same alert to be repeated every minute. The measured value must fall below the reset threshold before the next alert is generated. Please take a look at the chart below.



The red line indicates the alert threshold. When the response time or packet loss rate rises above this threshold an alert will be generated. But for the next alert to be generated this value must fall below the reset threshold. This prevents repeated alerts for the same event.

Notification of event end

For every event type, you can turn on notification about its end. For "Packet loss rate too high" and "Response time too high" events, you define the reset threshold. When the value falls below this threshold, the program considers the event to be finished. For "Host not responding" events, the connection is restored when the host responds to at least one ping request.

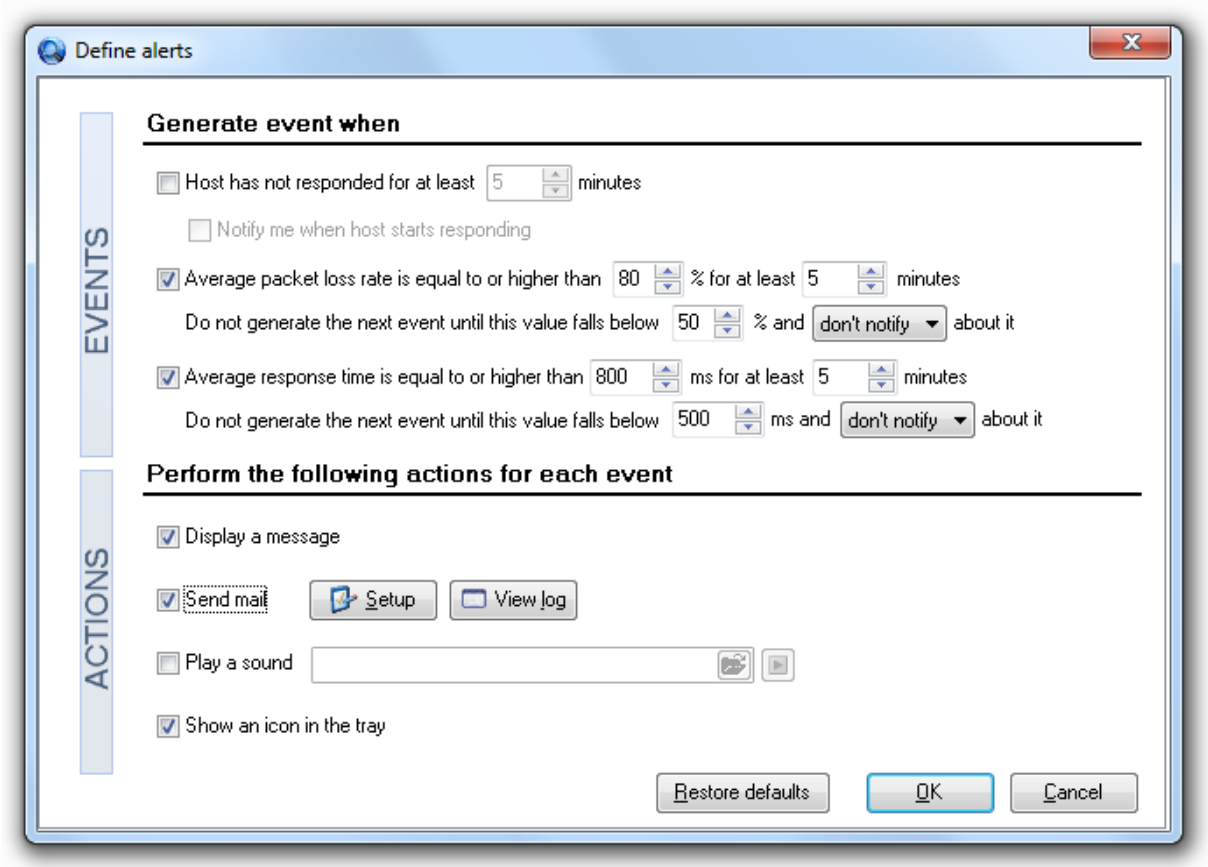
When the event ends and you turn on the notification for this event, the program will generate an action for such event.

Actions

You can define actions which will be executed for every event. The following actions are available:

1. **Message window**. In case of an alert, netTools will show a dialog box listing all the alerts that have been raised.
2. **E-mail**. netTools can send an e-mail to several addresses in case of an alert. This e-mail lists the host name/address and alert conditions.
3. **Sound**. The program can play a sound for every alert.
4. **Alert icon**. When the event is generated, the program icon in the tray will change to .

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.



3.2.2 Setting alerts

To set alerts properly you must define event conditions and configure actions. Please remember that defined actions are executed for every event.

To set alerts

1. Select the **NetWatch** tool on the navigation bar.
2. Click on the **Set alerts** button located in the **Pick a Task** section of the sidebar
3. Check the events you want to be generated.
4. Check the actions that the program should execute for every event.
5. Configure events and actions as further described.

Configuring "Host not responding" event

1. Check **Host has not responded**... event.
2. Enter the time in minutes after which an event will be generated.

Configuring "Packet loss rate too high" event

1. Check **Average packet loss rate**... event.
2. Enter the value of the event threshold - an event will be generated when the average packet loss rate is equal to or higher than the threshold value.
3. Enter the time in minutes after which an event will be generated.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

4. In the second line, enter the reset threshold value. The event will end after the percent of packets lost falls below this threshold.
5. Select **notify** from the combo box if you would like to be notified when the event ends (when the packet loss rate falls below the reset threshold value).

Configuring "Response time too high" event

1. Check **Average response time**... event.
2. Enter the value of the event threshold - an event will be generated when the average response time is equal to or higher than the threshold value.
3. Enter the time in minutes after which an event will be generated.
4. In the second line, enter the reset threshold value. The event will end after the response time falls below this threshold.
5. Select **notify** from the combo box if you would like to be notified when the event ends (when the response time falls below the reset threshold value).

Configuring actions

1. Check **Display a message** if you want netTools to show a dialog box with a list of alerts for every event.
2. Check **Send mail** if you want to be notified by e-mail.
3. If you turned on email notification then you need to setup this action.
4. If you want a sound to be played for each alert check **Play a sound**.
5. If you selected sound notification, enter the file name of the sound file. You may click on the icon located on the right side to select the file.
6. If you check **Show an icon in the tray** then netTools will show the icon in the icon tray during each event.

Configuring e-mail action

1. Open **Define alerts** window and click on the **Setup** button.
2. Enter the list of addresses to which you want send a message in the **Send notification to** field. Each address should be in separate line.
3. Enter the address of the mail server (SMTP/POP3).
4. If the server requires an authorization then check appropriate check box and enter your username and password in the **Username/Password** fields respectively.
5. Choose **Encryption** (No encryption, SSL v2/v3 or TLS).
6. Enter **Reply address** (most likely your e-mail address). This is very important - if this address is not set properly some mail servers may reject e-mail.
7. Now, click on the **Test** button and check if you received an e-mail. If not, verify the options.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Part IV

4 WinTools

4.1 WinTools

This tool is designed to list exhaustive system information from Windows computers (using WMI). It has several predefined queries allowing to read service list, disk information, process list etc. You can also define your own queries. Please read the topic Enabling WMI on remote computers prior to using WinTools to learn how to enable WMI on remote computer in order to read information from them.

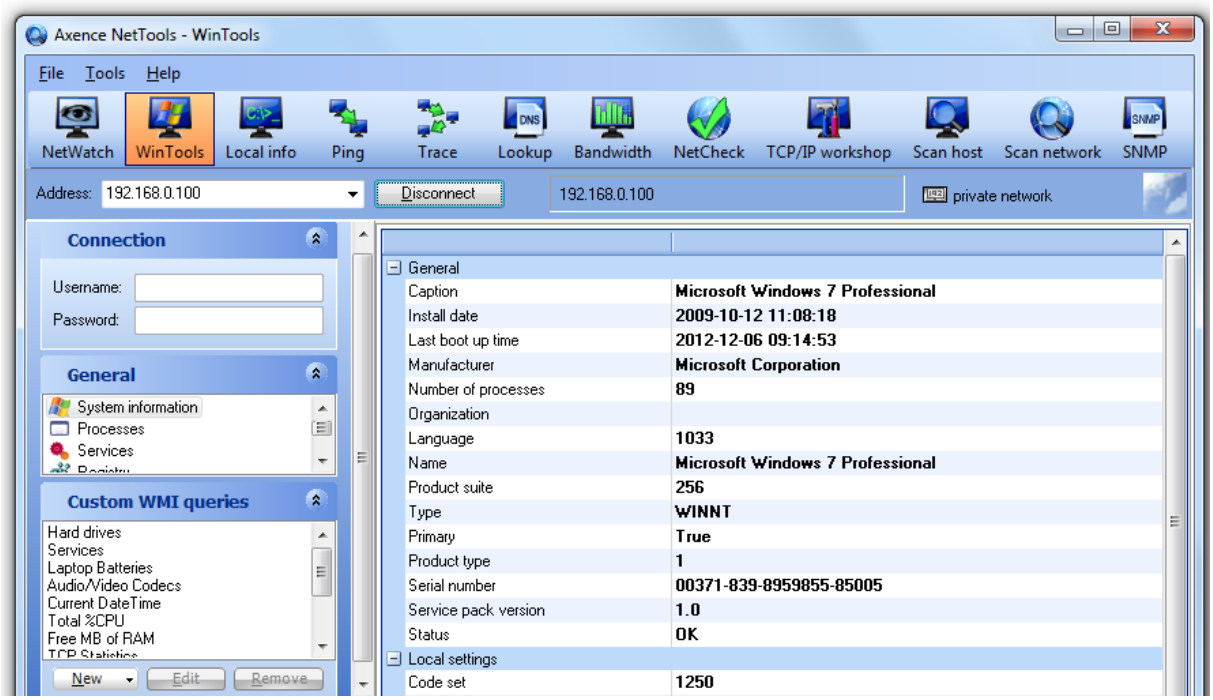
To use WinTools

1. Select **WinTools** tool on the navigation bar.
2. Enter the username (use username@domain for domain users) and password in the **Connection** sidebar group. This is required to read WMI information from the windows computer. This may not be necessary if you are already logged to this Windows machine.

Information provided

You can see very wide range of information by selecting the appropriate task on the **Tasks** sidebar. There are many predefined information tables in the **General** and **Custom WMI Queries** groups available.

You can define your own WMI queries to get required information. Just click **New** button at the bottom of the **Custom WMI Queries** group. This will allow you to define a query with visual query builder. You can also enter the WMI query manually - click arrow next to the **New** button and select **Enter query** menu.



4.2 Enabling WMI on remote computers

Enabling monitoring of Windows counters

WMI (used by Inventory, WinTools and Windows performance counters monitoring) is fully enabled by default on Windows 2003 Server. But you need to perform several operations if you would like to get

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

information from computers with Windows XP Professional, Vista, Windows 7, and newer. To speed up the whole operation we prepared a program (WMIEnable.exe) which automatically performs all necessary operations. To enable WMI, just run this program on the remote machine. You can run it from the login script, thus enabling WMI on all Windows machines in your network at once. If any other firewall is used on the remote machine, the following ports must be opened: TCP 135, 139, 445, 593.

To use WinTools or get inventory of Windows XP Home machine you need to remember that this systems must have exactly the same user and password as the user logged in on the machine running netTools and nVision.

WMIEnable

This program enables WMI on the Windows computers. This is exact list of operations performed by this program:

1. DCOM is enabled by setting registry key [HKEY_LOCAL_MACHINE\Software\Microsoft\OLE \EnableDCOM] value to "Y".
2. Remote UAC on Windows Vista is enabled by setting registry key [HKLM\SOFTWARE\Microsoft \Windows\CurrentVersion\Policies\system\LocalAccountTokenFilterPolicy] value to 1.
3. The WMI ports (TCP 135, 139, 445, 593) are opend on the Windows firewall by performing the following command: netsh firewall set service RemoteAdmin
4. Access to WMI on Windows Vista is enabled by adding firewall exception for "Windows Management Instrumentation (WMI)".
5. Authorization model is set to "Local user authorize as themselves" by setting registry key [HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Lsa\forceguest] value to 0.

In almost all cases the system restart is not necessary and WMI will be enabled right after the program execution, but you can also force Windows system restart after the above parameters are set by running the program with the **/restart** parameter. The program will not restart the system if it's not able to change system settings.

If the WMI is still not working

If you have run the WMIEnable program and WMI is still not working, then verify the following:

1. Enter Local Security Settings (secpol.msc /s) and select Local Policies -> User Rights Assignement -> Access this computer from network. Check if all necessary users/groups are added here. At least the Administrators group or Administrator should be present.
2. Enter Group Policy Settings (gpedit.msc) and select Windows Settings -> Security Settings -> Local Policies -> Security Options -> Network access: Sharing and security model for local accounts. Set it to "Classic - local user authorize as themselves".
3. Check if WMI is operational by running the following command: "**wbemtest**". WMI is running if this program can run properly.
4. Check if the following services are running:
   COM+ Event System
   Remote Access Auto Connection Manager
   Remote Access Connection Manager
   Remote Procedure Call (RPC)
   Remote Procedure Call (RPC) Locator
   Remote Registry
   Server
   Windows Management Instrumentation
   Windows Management Instrumentation Driver Extensions
   WMI Performance Adapter

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Workstation

Memory leaks with outdated Rpcrt4.dll

If monitoring Windows counters, please make sure that you have the latest Rpcrt4.dll installed. All previous versions cause serious memory leaks in the system, which can lead to the system crash. This problem is described by Microsoft at http://support.microsoft.com/?kbid=911262
For Windows XP your Rpcrt4.dll should have version 5.1.2600.2810 or higher.

4.3 Cannot use WinTools

This topic explains why WinTools are unable to connect to the remote node and what to do to enable all of the above tasks.

Why netTools can't do it

This tasks is performed with WMI protocol. So it must be enabled and available on the remote node. You have to make sure that WMI services are running, the authorization model is properly set and if all necessary ports are open on the firewall. And last but not least, you have to configure node credentials (username and password - use username@domain for domain users).

On computers with Windows XP Professional newer Windows systems WMI is blocked by the firewall and wrong authorization model. To automate these tasks we prepared a program (WMIEnable.exe) which performs all necessary operations. You can read more about WMIEnable.exe in the Monitoring Windows with WMI topic.

How to enable these tasks

Here is a list of steps you should take to enable WMI:

1. **Run WMIEnable.exe on the remote node.**
   This program is located in the programs directory and has to be copied to the remote computer. This program does the following:
   - Enables DCOM
   - Enables Remote UAC on Windows Vista
   - Sets the authorization model to "Local user authorize as themselves"
   - Configures Windows firewall to open all WMI ports
2. **Open WMI ports if necessary**
   If you are using any third party firewall on the remote node, then you need to open the following ports: TCP 135, 139, 445, 593
3. **Configure node credentials.**
   Enter the username (use username@domain for domain users) and password of the user with the administrator rights on the remote computer.

If it's still not working

Please go to Enabling WMI on remote computers topic to read how you can verify what's wrong.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Part V

5 Local info

5.1 Introduction

Displays several tables with important information about local configuration: network statistics for TCP/UDP and ICMP, IP address table, ARP table, IP routing table, network adapter info.

To see the local info

1. Select the **Local info** tool on the navigation bar.
2. Select the appropriate task to see the required information: NetStat to view all local TCP/IP connections, Local IP info, ARP and Routing table or Statistics.

Information provided

You can see several tables by selecting the appropriate task on the Tasks sidebar. There are several tables available:

- NetStat - list of all local connections
- Local IP info - IP address table, interfaces, adapters
- ARP & routing table - ARP table, routing table
- Statistics TCP/UDP/ICMP

Options

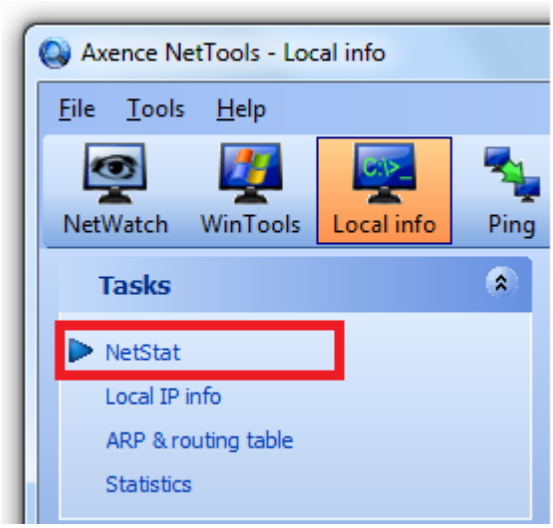
You may change refresh time. Just enter the desired values in the **Options** section on the sidebar.

5.2 NetStat

This tool is a replacement of the standard Windows NetStat command-line utility. It displays all the inbound and outbound connections to your computer and lists all open ports. Additionally, NetStat maps open ports and established connections to the owning application.

To start monitoring connections

1. Select **Local info** tool on the navigation bar.
2. Select **NetStat** task on the sidebar.



Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

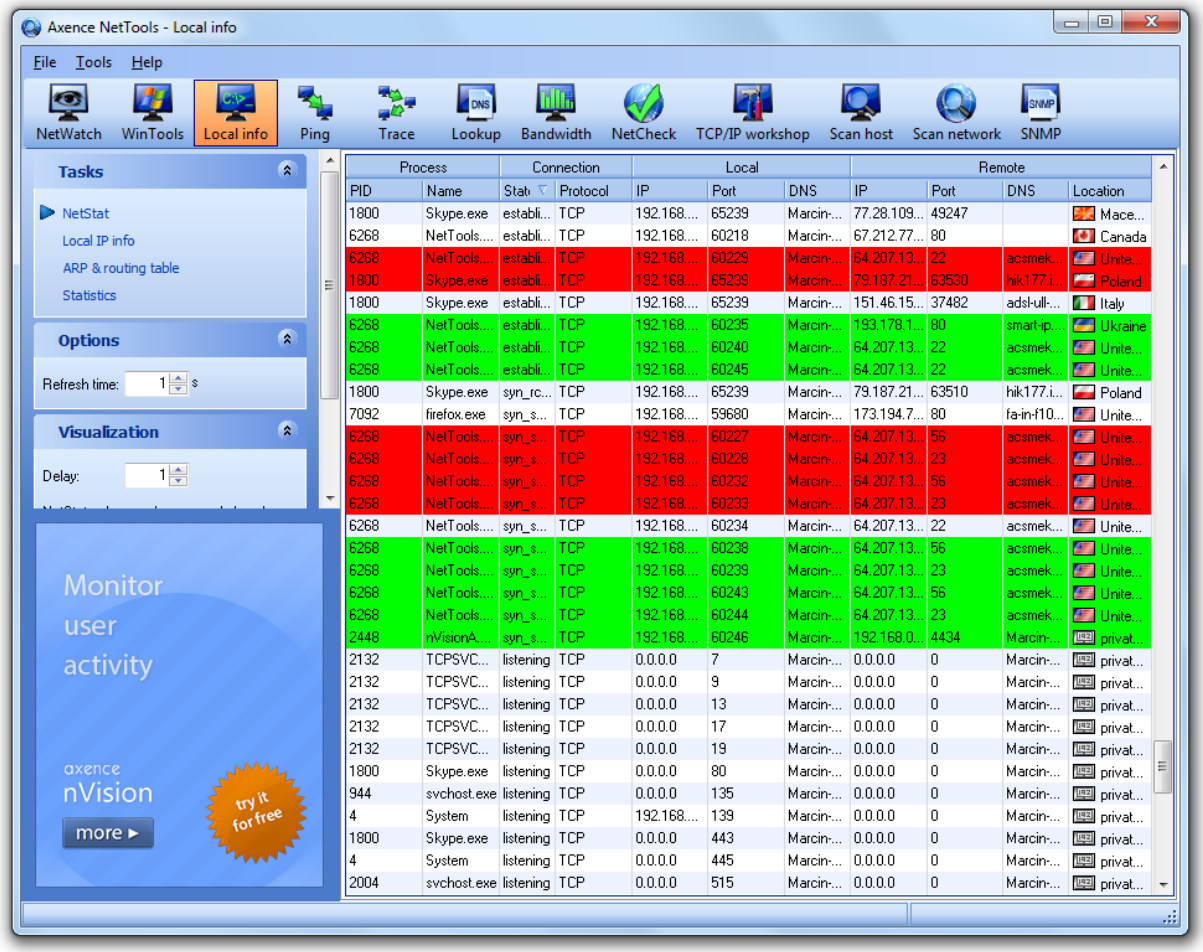
Information provided

In the main grid you can see all inbound and outbound connections listed. You can see process ID along with the process name, protocol and connection state, local and remote IP address/port.

When adding a new connection, NetStat colorizes it in green to indicate a new connection. Similarly, deleted connections are colorized in red, and then removed from the grid.

Options

You may change refresh time. Just enter the desired values in the **Options** section on the sidebar. You can also change colorization time.
The grid may be grouped and filtered. To group it just select the appropriate grouping option from the Visualization sidebar. To filter the data, use the arrows next to each column header.



Notes

- UDP connections have no state and local IP listed because of their nature.
- To copy the remote IP address or remote DNS name to clipboard, right click the given line in the table and select the appropriate option from the pop-up menu.

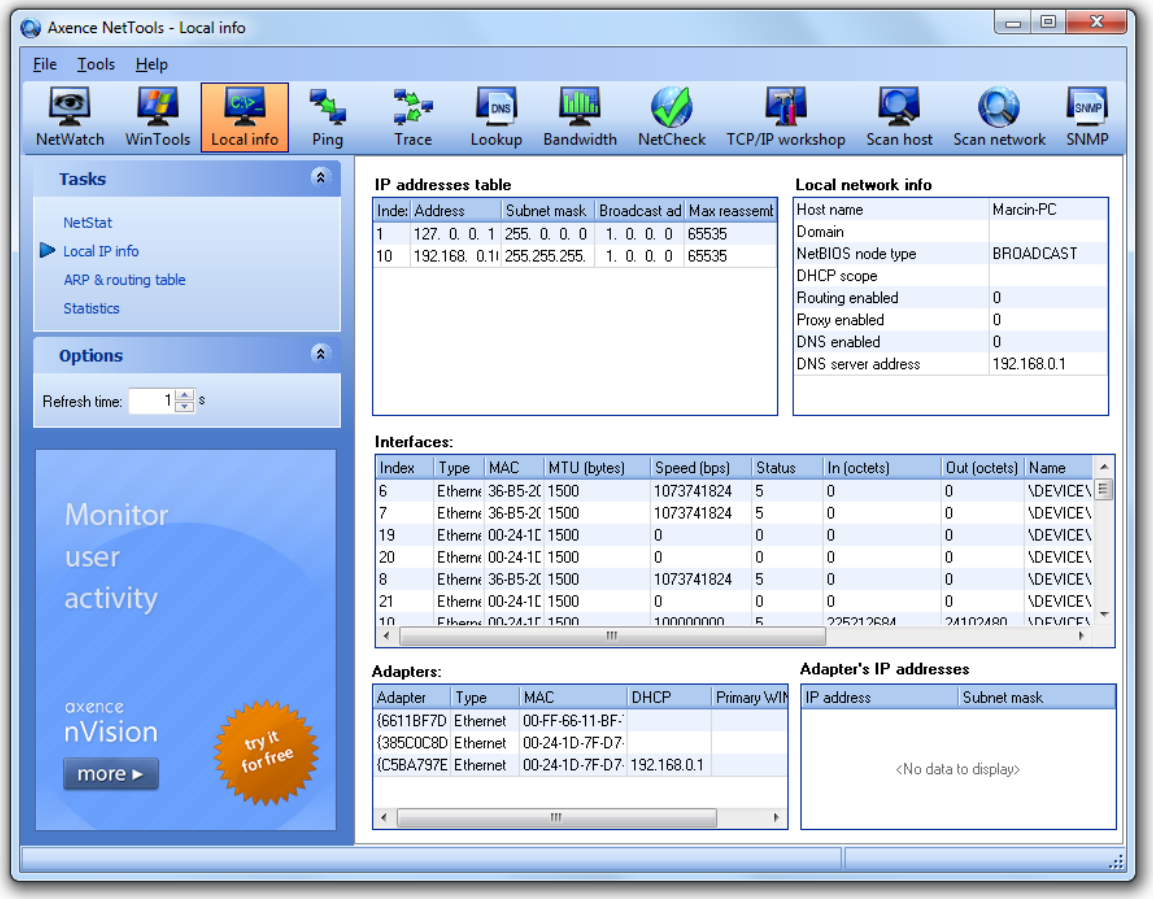
Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

5.3 Local IP info

The tool displays several tables with important information on local configuration: IP address table, LAN details, interfaces and network adapters.

To view the local IP information

1. Select **Local info** tool on the navigation bar.
2. Select **Local IP information** on the side bar.



Notes

- To copy the IP address to the clipboard, right click the given line in the IP address table and select **Copy IP address** from the pop-up menu.
- The pop-up menu also allows the use of the **Wake On LAN** feature. For more information, see the chapter How to use Wake On LAN feature?.

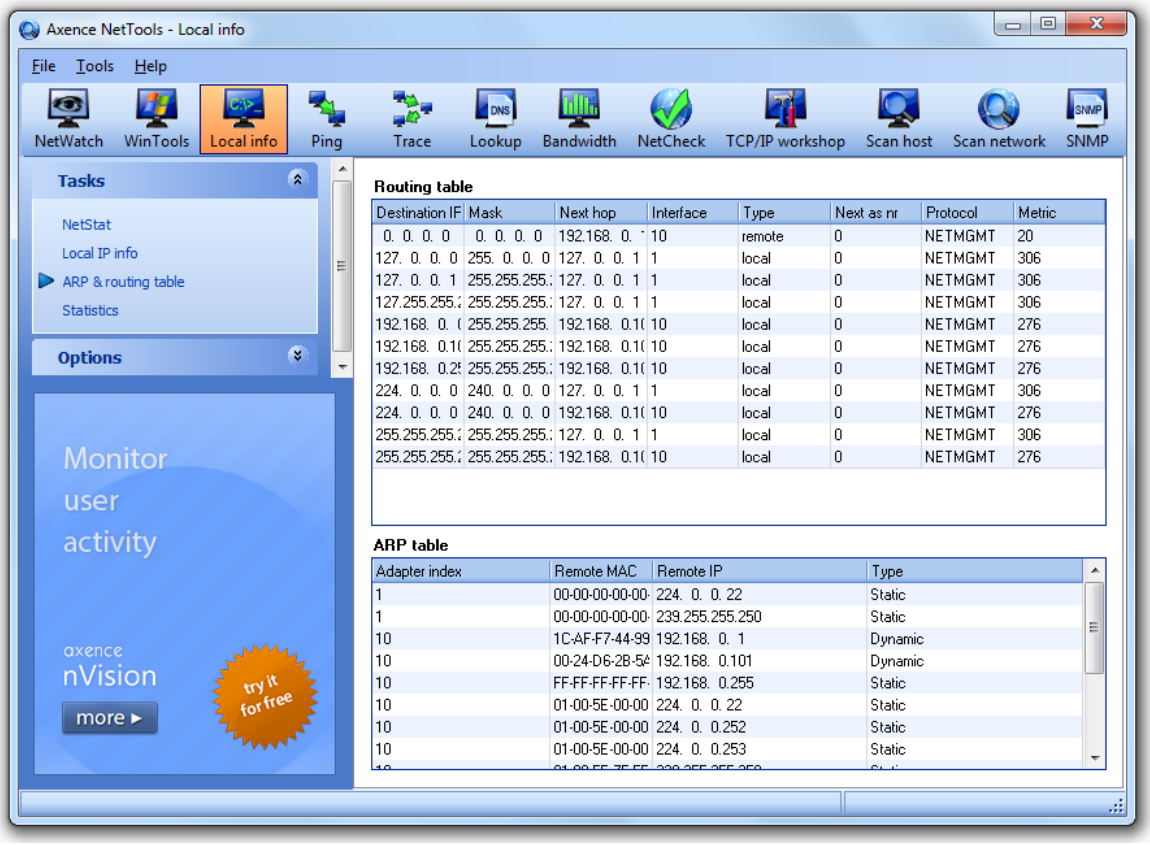
5.4 ARP and routing table

The tool displays the routing table and ARP table. The data presented in the ARP table are also used by the Scan Network tool to fill the MAC addresses.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

To view ARP and routing tables

1. Select **Local info** tool on the navigation bar.
2. Select **ARP & routing table** on the side bar.



Notes

- To copy the IP address to the clipboard, right click the given line in the IP address table and select **Copy IP address** from the pop-up menu.
- The pop-up menu also allows the use of the **Wake On LAN** feature. For more information, see the chapter How to use Wake On LAN feature?.

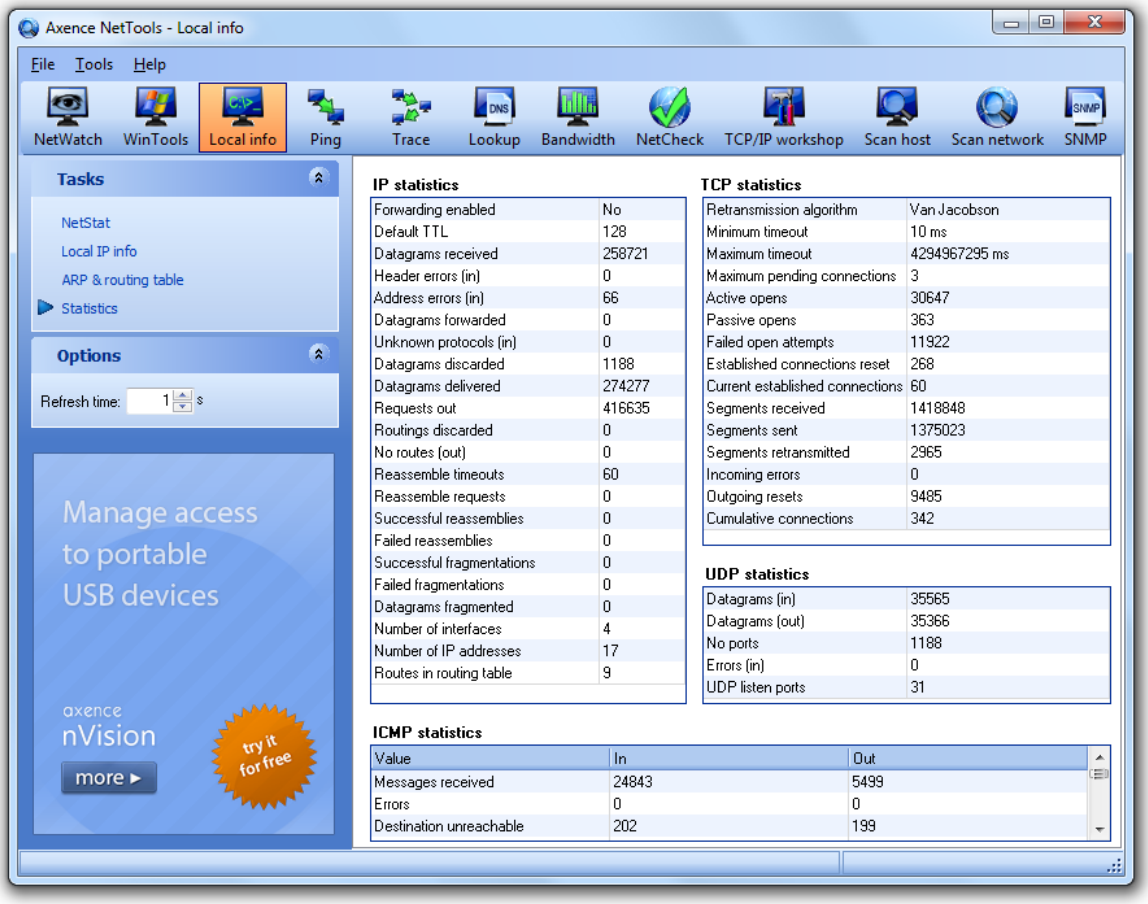
5.5 Statistics

The tool displays tables with IP, TCP, UDP and ICMP statistics.

To view the statistics

1. Select **Local info** tool on the navigation bar.
2. Select **Statistics** on the side bar.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.



Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Part VI

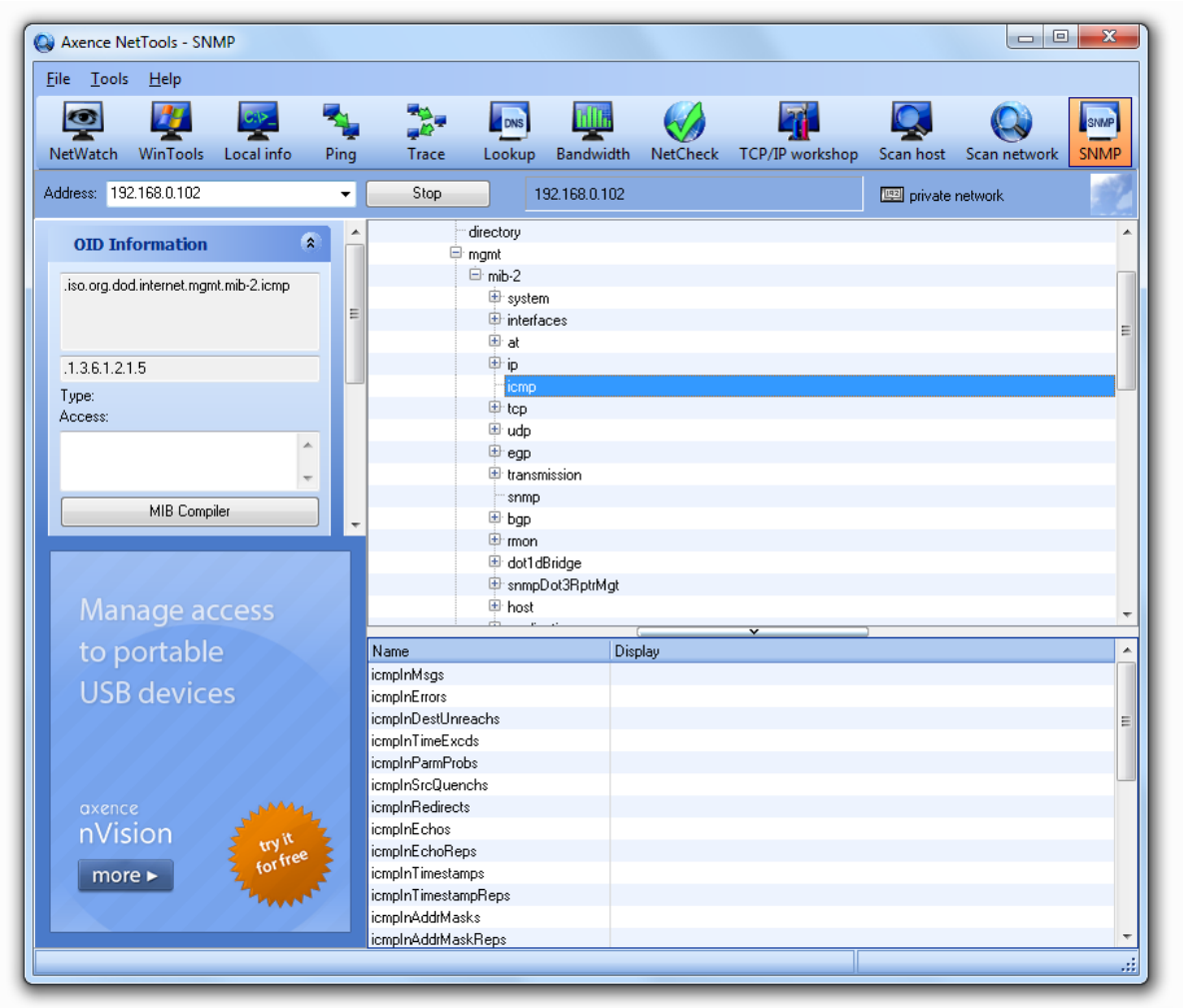
6 SNMP

6.1 SNMP

SNMP tools lets you browse a SNMP OID tree and view this information for a host. This information is provided by SNMP agents, which must be installed on the host being monitored.

To get SNMP information

1. Select the **SNMP** tool on the navigation bar.
2. Enter the host **DNS name** or **IP address** in the address bar.
3. Select OID category you would like to check in the MIB tree.
4. Click the **Check** button or press **Enter**.



Information provided

The program presents all OIDs available in selected OID category. If this is a table then all columns and rows will be displayed (in this case you may change column order and hide/show them).

General information about each OID is shown on the sidebar: OID name, type, access and short description.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Click **MIB Compiler** button to add a new MIB database object to handle any new SNMP devices. For more information, see the chapter MIB file compiler.

Options

With options, located on the sidebar you can change community, refresh time and timeout. Community is the password used by SNMP protocol. You have to provide the same string as in SNMP agent on the host you are checking. If you enter incorrect community you will not be able to retrieve any SNMP information.

Note

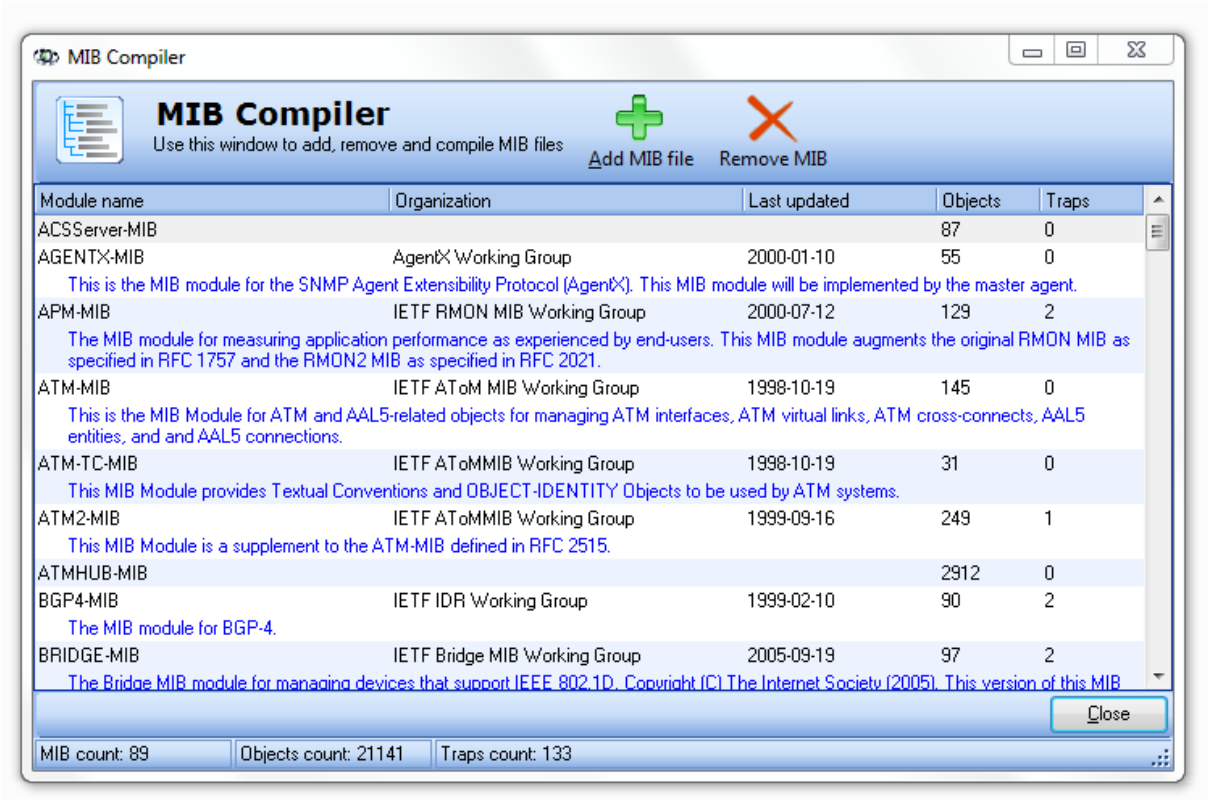
- On the right side of the address bar, you can see the name and IP address of the host currently being checked. You can copy the name or IP of the host to clipboard. Just right click the host name and select **Copy IP address** or **Copy DNS Name** from the popup menu.

6.2 MIB files compiler

MIB compiler enables you to add new MIB files, which facilitate SNMP information from all network devices: switches, routers, printers, VoIP devices etc. The program can now effectively monitor thousands of different SNMP devices.

To use MIB compiler:

1. Select **Tools | MIB compiler** option. A MIB compiler window will open.

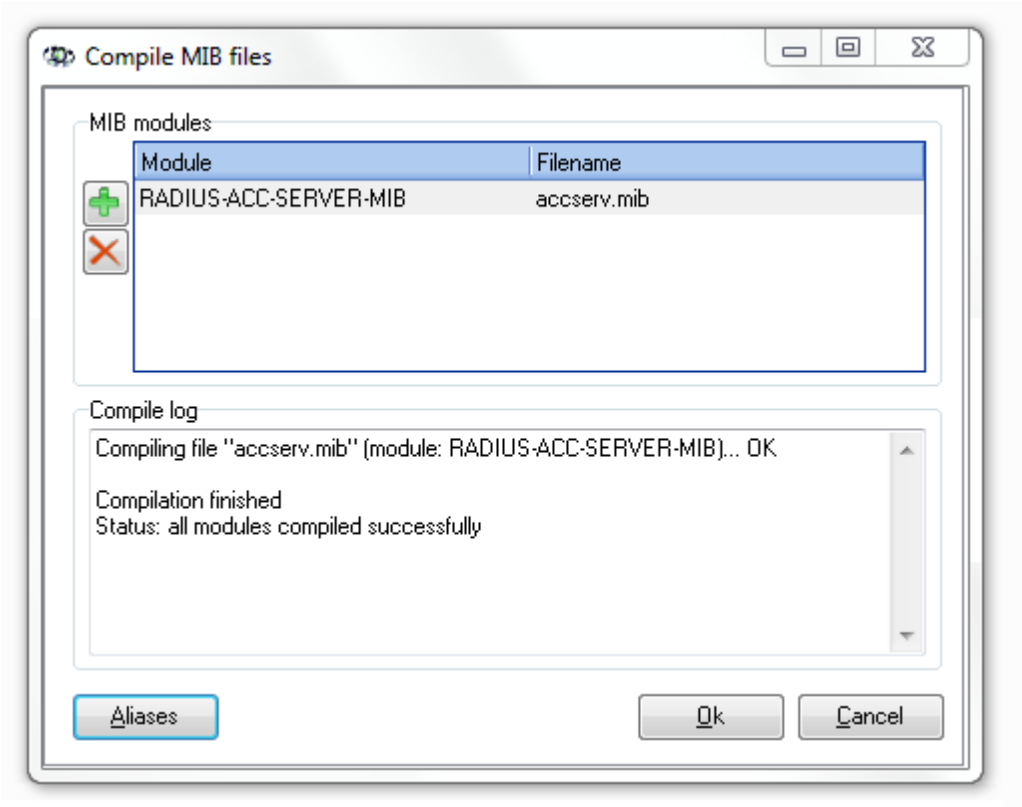


2. If you want to add a new file, click the

button.
3. Add a MIB module by clicking the button and selecting a file from its localization. Compile log is

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

shown after compilation.



4. You can also define aliases in the MIB Compiler aliases editor.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Part VII

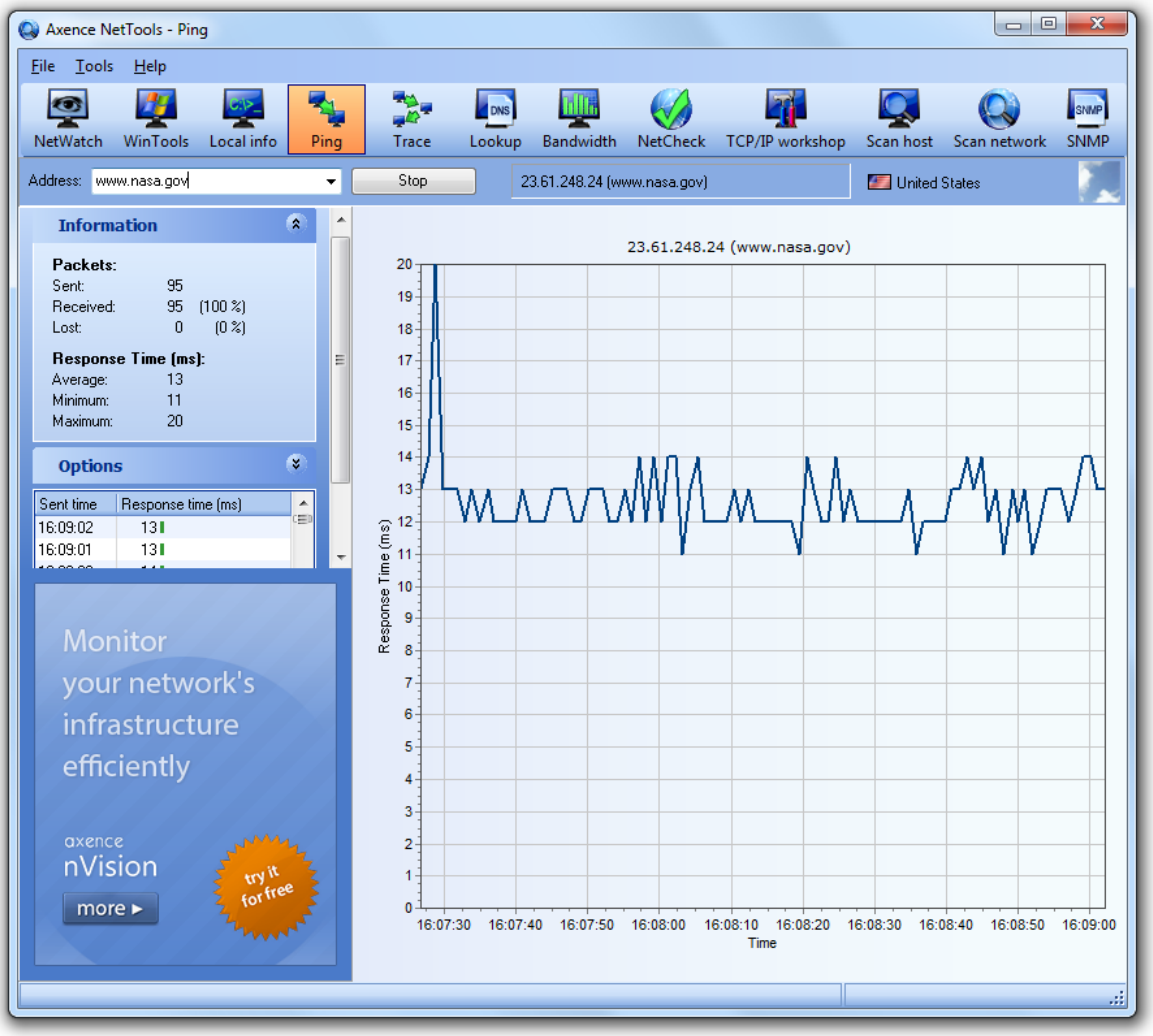
7 Other Tools

7.1 Ping

With the Ping tool, you can quickly check the connection to a host. It sends ICMP packets to the host and allows you to check response times and the number of lost packets.

To start monitoring a host

1. Select **Ping** tool on the navigation bar.
2. Enter host **DNS name** or **IP address** in address bar.
3. Click **Ping** button or press **Enter**.



Information provided

On the main chart you can see response times for the last 5 minutes. If you want to see the exact values of response time in milliseconds, take a look at the grid in the sidebar.

There is also general information available in the Information section on the sidebar: number of packets sent/lost and minimum/average/maximum response time in milliseconds.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Options

You may change monitoring frequency and timeout value. Just enter the desired values in the **Options** section on the sidebar.

Export

To export the image file with PING chart:

1. Right click the chart and select **Export**.
2. Enter the file name and select the file format: **bmp**, **emf** or **wmf**. **Save** the file.

Note

- Ping stores response information values for the last 5 minutes. Thus the main chart and the grid represent the last 5 minutes. To monitor a host for a longer time, use NetWatch.
- On the right side of the address bar, you can see the name and IP address of the host currently being checked. You can copy the name or IP of the host to clipboard. Just right click the host name and select Copy IP Address or Copy DNS Name from the popup menu.
- You can easily open the address in any other netTools utility by selecting one of the options: **Add to NetWatch**, **Trace**, **Lookup**, **Link usage** from the pop-up menu.
- Next to the device name, the geographic location (country) of the remote IP address is presented.

7.2 Trace

Trace tool allows you to check the connection to a host. In case of problems, you can see which hop is causing the problem. Trace shows response time and packet loss rate to each host on a route, so you can quickly locate the problematic one. In the bottom part of the window, a visual map of subsequent hosts along the packet route is displayed.

To start traceroute to a host

1. Select **Trace** tool on the navigation bar.
2. Enter host **DNS name** or **IP address** in the address bar.
3. Click **Trace** button or press **Enter**.

Information provided

General information about each hop is available in the main grid: hop number, DNS name and IP address, response times (min/max/avg), and number of packets sent and lost.

There is also total number of traces performed available in the **Options** Section on the sidebar.

Options

You can change trace frequency, timeout value and number of hops (TTL - time to live). With hops, you specify the maximum number of hosts to check. To change options, just enter the desired values in the **Options** section on the sidebar.

You can copy the name or IP of the host to clipboard. Just right click the selected host in the grid or a host name on the address bar and select **Copy IP address** or **Copy DNS Name** from the popup menu.

You can easily open any address from the table in any other netTools utility by selecting **Tools** and one

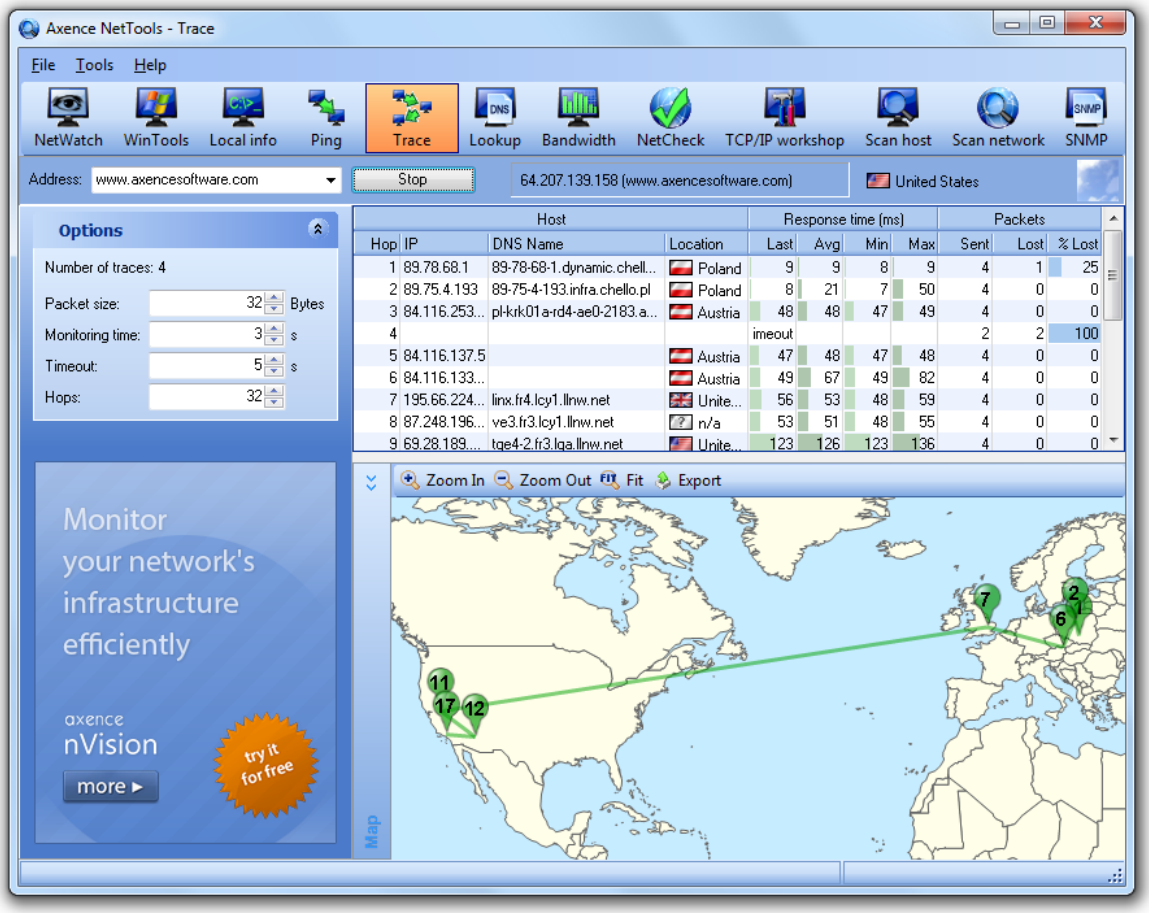
Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

of the options: **Add to NetWatch**, **Lookup**, **Link usage** from the pop-up menu.

Export

To export the table with device data, select **Export** in the pop-up menu. Then choose one of the formats: **html**, **xml**, **txt**, **xls**.

To export the map in **bmp** format, select Export, enter the file name and **Save**.



Note

- The name and IP address of the checked device is displayed on the right hand side of the address bar. It can be easily copied to the clipboard. Right click the field and select **Copy IP address** or **Copy DNS name** from the pop-up menu.
- Next to the device name, the geographic location (country) of the remote IP address is presented.

7.3 Lookup

Lookup is similar to nslookup tool, but it provides all the DNS information about a host and domain at once. You do not have to select any record type - you will see all the records in one table.

Additionally, lookup provides WHOIS information about a domain, even if you enter a host name (like www.google.com) rather than a domain.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

To lookup a host

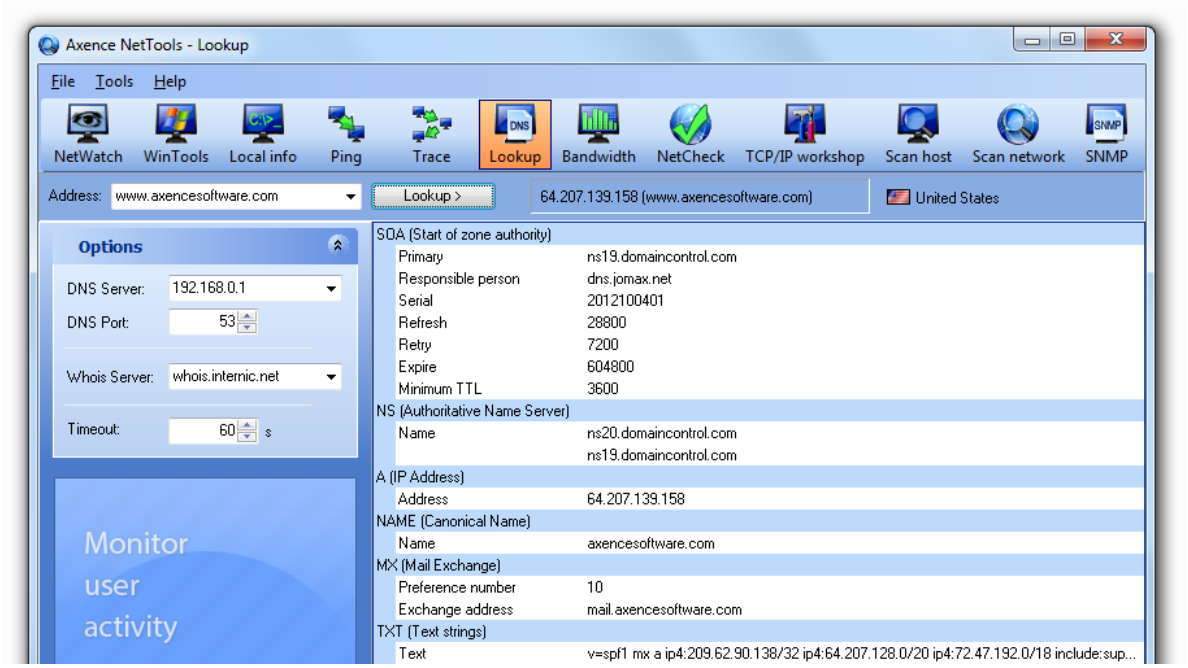
1. Select **Lookup** tool on the navigation bar.
2. Enter the host **DNS name** or **IP address** in address bar.
3. Click **Lookup** button or press **Enter**.

Information provided

All DNS records and whois information will be listed in one table. WHOIS information is listed at the bottom.

Options

You can change DNS and WHOIS server address, DNS port, and timeout value (for both services: DNS and WHOIS). Just enter the desired values in the Options section on the sidebar.



Note

- The name and IP address of the checked device is displayed on the right hand side of the address bar. It can be easily copied to the clipboard. Right click the field and select **Copy IP address** or **Copy DNS name** from the pop-up menu.
- Next to the device name, the geographic location (country) of the remote IP address is presented.

7.4 Bandwidth

The Bandwidth tool measures the data transfer rate of a connection to a host. This process does not overload the network.

To start measuring bandwidth

1. Select **Bandwidth** tool on the navigation bar.
2. Enter the host **DNS name** or **IP address** in address bar.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

3. Click **Bandwidth** button or press **Enter**.

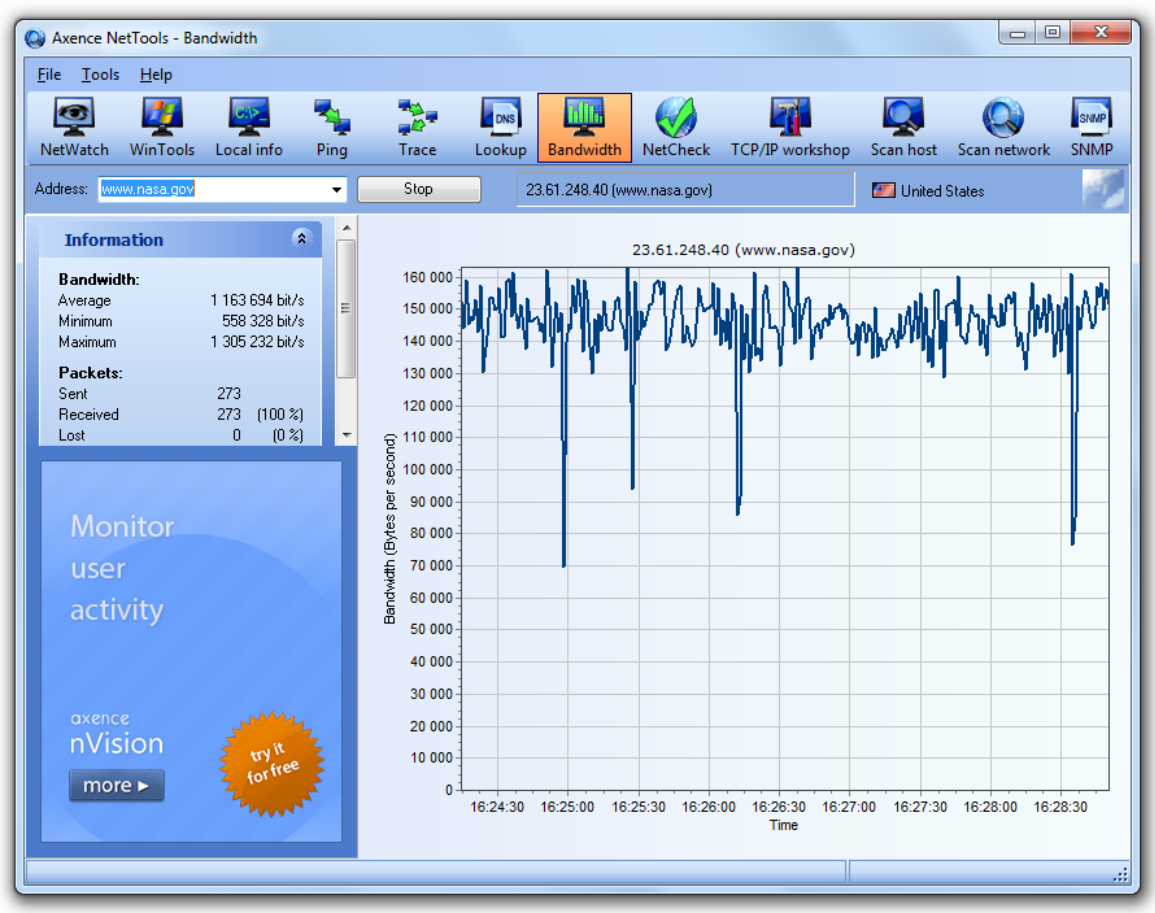
Information provided

On the main chart, you can see bandwidth for the last 5 minutes.

There is also general information available in the Information section on the sidebar: number of packets sent and minimum/average/maximum bandwidth.

Options

You can change measurement frequency, packet size and timeout. Just enter the desired values in the **Options** section on the sidebar. Changing packet size influences results. Some hosts may not accept packets that are too large. Remember to set a larger timeout value for larger packets.



Note

- Bandwidth stores response information values for the last 5 minutes. Thus, the main chart represents the last 5 minutes.
- On the right side of the address bar, you can see the name and IP address of the host currently being checked. You can copy the name or IP of the host to clipboard. Just right click host name and select **Copy IP address** or Copy **DNS Name** from the popup menu.
- Next to the device name, the geographic location (country) of the remote IP address is presented.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

7.5 NetCheck

With NetCheck, you can quickly check the quality of the connection to a host. It sends a series of ICMP packets of different sizes to detect any possible problems. NetCheck interprets the results so you do not even have to know much about network management.

To check the network connection to a host

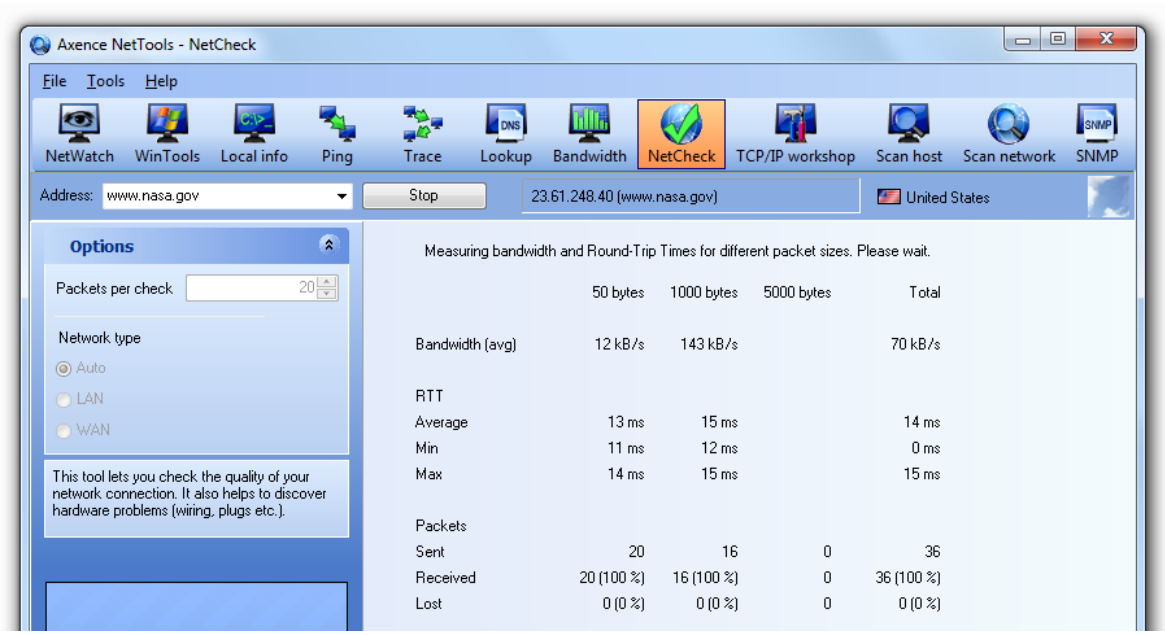
1. Select **NetCheck** tool on the navigation bar.
2. Enter the host **DNS name** or **IP address** in the address bar.
3. Click the **Net Check** button or press **Enter**.

Information provided

NetCheck presents information gathered during the network test. You will see bandwidth, response times, and packet loss rates for different packet sizes. When the check is finished, this tool will show you an interpretation of the results.

Options

You can change the number of packets the tool sends for each check. Just enter the desired value in the **Options** section on the sidebar.



Note

- On the right side of the address bar, you can see the name and IP address of the host currently being checked. You can copy the name or IP of the host to clipboard. Just right click the host name and select **Copy IP address** or **Copy DNS Name** from the popup menu.
- Next to the device name, the geographic location (country) of the remote IP address is presented.

7.6 TCP/IP workshop

TCP/IP workshop provides you with the ability to establish low-level TCP and UDP connections to troubleshoot and test different networking services. With this tool you can send raw data to any port on

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

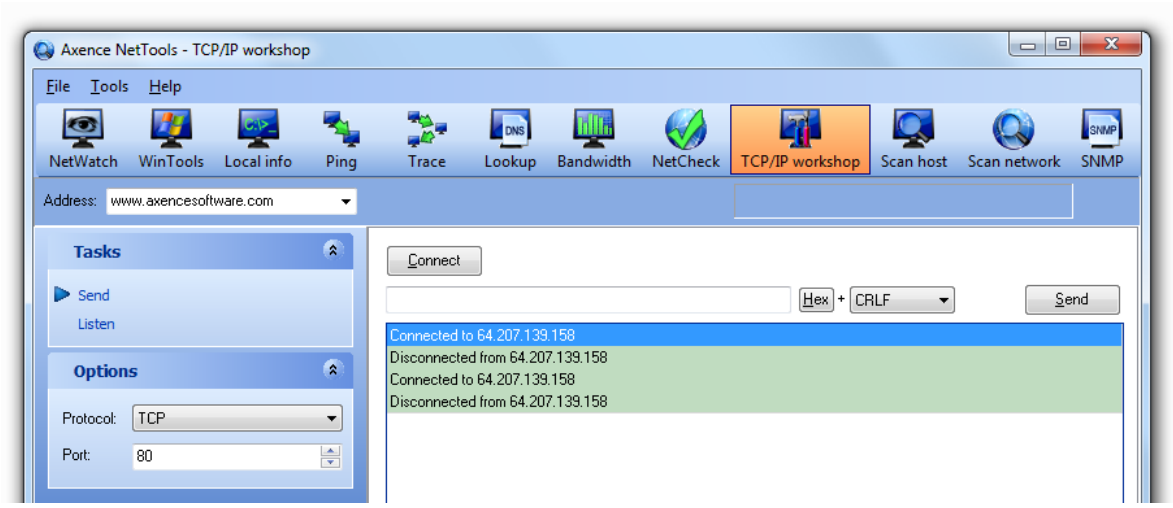
the remote computer. You can also listen on any local port to see all data the remote computer sends.

To use TCP/IP workshop

1. Select **TCP**/IP workshop tool on the navigation bar.
2. Select **Send** on the sidebar to connect to the remote TPC/IP port and send data or select **Listen** to start listening for incoming connections and data on the local port.
3. Enter the appropriate data and click **Connect** or **Listen** button respectively.

Options

You may change protocol and port which the tool is using. Just enter the desired values in the **Tasks** section on the sidebar.



7.7 Scan host

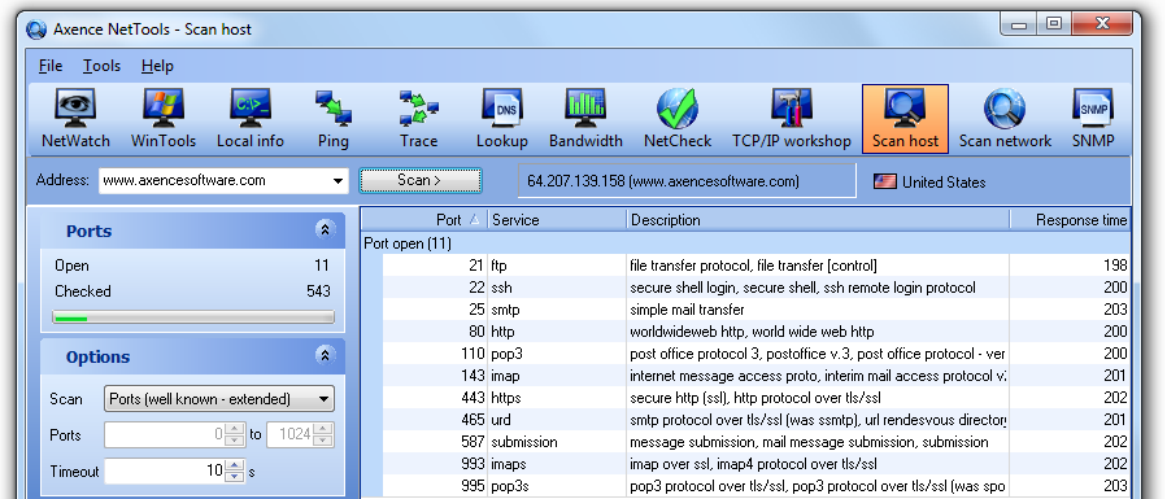
The Scan host tool lets you check for open TCP ports and running services on a selected machine. It lists all running services, checks open ports, and even tries to determine whether you have any Trojans running.

While scanning services, netTools sends a request and checks if the response matches specific criteria, which makes sure that a specific service is running on the port. This is important if more that one service may be using the selected port. It can scan services using both TCP and UDP.

To start scanning a host

1. Select **Scan host** tool on the navigation bar.
2. Enter the host **DNS name** or **IP address** in the address bar.
3. Option Scan on the sidebar lets you choose between scanning ports and services. Select the appropriate option from the drop down combo box.
4. If you selected scanning ports then enter start/stop port numbers in the fields below.
5. Click the **Scan** button or press **Enter**.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.



Information provided

The main grid shows information about running services or open ports (depending on what you are currently scanning).

Services are presented on the list in 3 groups:

Group	Description
Running	Service is running on the host
Probably running	There is a service running - it responded to request sent, but response did not meet criteria specified.
Port open	There is an open port, but there was no response at all from any service.

Information about the number of ports/services checked and running is also available in the Information section on the sidebar.

Options

Options allow you to change timeout and choose whether to scan services or ports:

Option	Description
Services	netTools will discover all services running on the host. It sends specific service requests and checks whether the response meets the defined pattern.
Ports (well known)	This option lets you scan for all the open ports defined on the well known port list.
Ports (well known - extended)	The same as the well known option, but it also includes many rarely-used services.
Ports (range)	Scans a defined range of ports.

Note

- On the right side of the address bar, you can see the name and IP address of the host currently being scanned. You can copy the name or IP of the host to clipboard. Just right click the host name and select **Copy IP Address** or **Copy DNS Name** from the popup menu.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

- Next to the device name, the geographic location (country) of the remote IP address is presented.

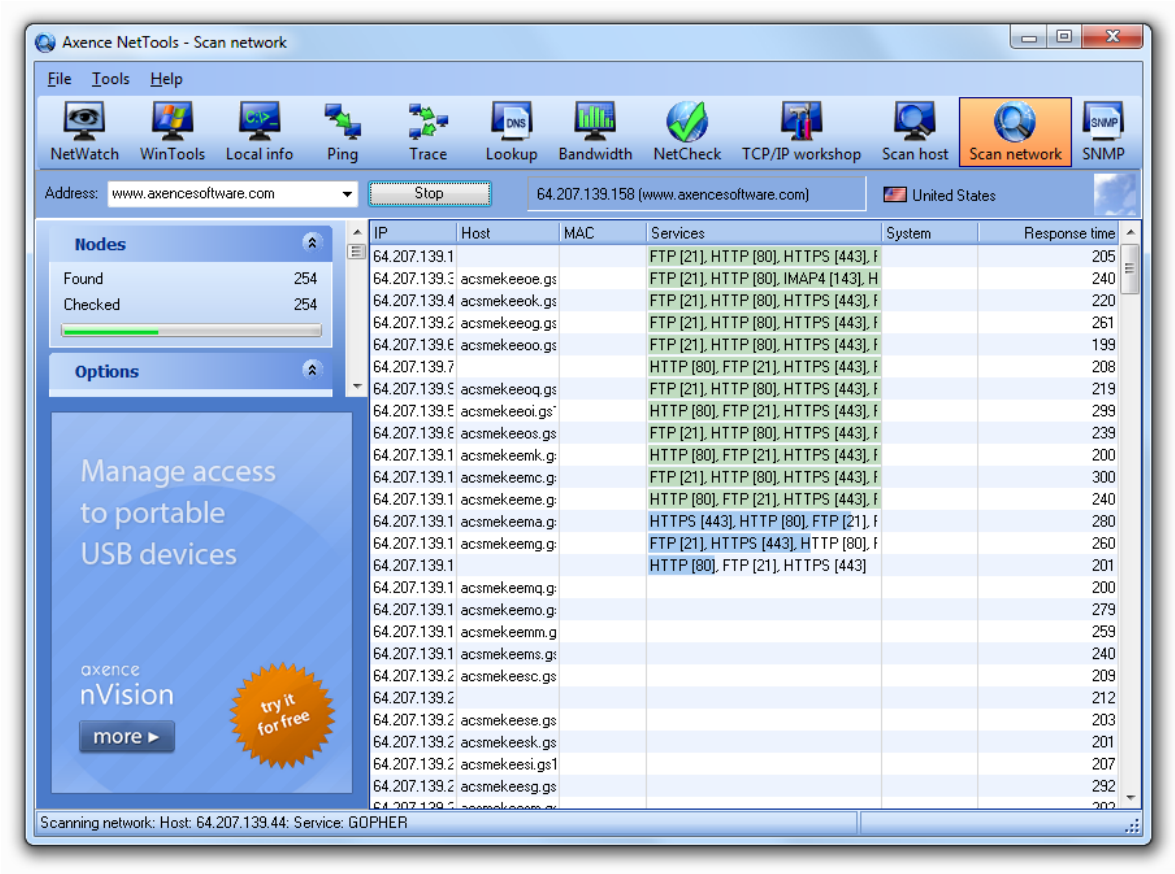
7.8 Scan network

The Scan network tool lets you check for running hosts in a selected network. It lists all the nodes and services running on them.

First, netTools discovers all running nodes with ICMP (Ping). So it can discover only the nodes that reply to such requests. Then it scans for services running on every available node. While scanning the service running on a discovered node, netTools sends a request and checks if the response matches specific criteria, which makes sure that a specific service is running on the port. This is important if more that one service may be using the selected port. It can scan services using both TCP and UDP.

To start scanning a network

1. Select **Scan network** tool on the navigation bar.
2. Enter the host **DNS name** or **IP address** in the address bar. netTools will scan the class C network containing this host. E.g., if you enter 192.168.0.34, then the program will scan the 255 addresses between 192.168.0.1 and 192.168.0.254.
3. Click the **Scan** button or press Enter.



Information provided

The main grid shows information about discovered hosts and services running or open ports. When you select a host on the list, you can see information about discovered ports/services in the Host Information section on the sidebar.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Information about the number of hosts checked and running is also available in the Information section on the sidebar.

Options

Options allow you to change timeout and choose to scan hosts only, or services or ports as well:

Option	Description
Hosts only	With this option, netTools will check only for running hosts. No other scanning will be performed.
Services	netTools will discover all services running on the host. It sends specific service requests and checks whether the response meets the defined pattern.
Ports (well known)	This option lets you scan for all the open ports defined on the well known port list.
Ports (well known - extended)	The same as the well known option, but it also includes many rarely-used services.
Ports (range)	Scans a defined range of ports.

Note

- You can copy the name or IP of the selected host to clipboard. Just right click the host name and select **Copy IP Address** or **Copy DNS Name** from the popup menu.
- Next to the device name, the geographic location (country) of the remote IP address is presented.
- MAC address is filled on the basis of data contained in ARP table in **Local info** and **SNMP** data.

7.9 Command line

netTools may be started with a command line parameters. This allows you to create shortcuts to quickly perform frequently used tasks. Command line syntax is:

netTools.exe -<tool> <node address> [parameters]

The following table describes how to run all tools

Property	Description
-netstat	This tool shows local information and does not require any address parameter.
-netwatch [node address]	Adds a node to NetWatch.
-wintools [node address] [user] [pass]	Starts WinTools on a provided address. Provide user/ password to automatically connect to the remote computer.
-ping [node address]	Starts Ping on a provided address.
-trace [node address]	Starts Trace on a provided address.
-lookup [node address]	Starts Lookup on a provided address.
-bandwidth [node address]	Starts Bandwidth on a provided address.
-netcheck [node address]	Starts NetCheck on a provided address.
-tcpipworkshop [node	Starts TCPIP Workshop on a provided address.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Property	Description
address]	
-scanhost [node address]	Scans a node with a provided address.
-scannetwork [node address]	Scans a network with a provided address.
-snmp [node address] [community]	Starts SNMP on a provided address. Provide SNMP Read community to automatically connect to the remote computer.

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

Index

- A -

Alerts 18
Setting 20
ARP 29
ARP table 27, 29

- B -

Bandwith measuring 8, 40

- C -

Command line 46

- H -

Host availability 8
Host monitoring 8, 12
Host scanning 8, 43
Hosts scanning/discovery 45

- I -

ICMP Statistics 27
Introduction 2

- L -

Layout 5
Lookup 39

- M -

MIB files compiler 34
Monitoring 12

- N -

NetCheck 42
NetStat 27
NetWatch 12
Network Adapter Info 27
Network capacity 40
Network problem - locating 8, 38
Network scanning/discovery 8, 45
NsLookup 39

- P -

Ping 12, 37
Port scanning/discovery 8, 43

- Q -

Quality of network connection 8
Quality of the connection 42

- R -

RAW TCP/IP data (send/receive) 42
Routing table 27, 29

- S -

Services scanning/discovery 8, 43, 45
SNMP 8
SNMP browser 33
Statistics
Adapters 29
ICMP 30
Interfaces 29
IP 30
TCP 30
UDP 30
System requirements 3

- T -

TCP Statistics 27
TCP/IP local conections 27
TCP/IP Statistics 27
TCP/IP workshop 42
Tools available 4
Traceroute 38
Troyans scanning/discovery 8

- U -

UDP Statistics 27

- V -

Versions 5

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.

- W -

Wake On LAN 9
What is NetTools 2
What's New 2
WHOIS 39
Window 5
Windows 23
WinTools
    Overview 23
    Troubleshooting 23, 25
WMI 23
WMI - Enabling 23

Copyright © 2005-2014 Axence Software, Inc. All rights reserved.