NETSCANTOOLS 4.2
User Manual

Manual Revision 0
June 1, 2001

Northwest Performance Software, Inc.

Welcome to NetScanTools Help!

NetScanTools 4.2 (tm) is latest edition of the popular NetScanTools family of internet utilities. It is the internet utility toolset targeted towards the home and small business user while NetScanTools Pro is targeted for the business user or network professional.

NetScanTool's set of TCP/IP utilities will help you gain insight into the inner workings of your network, diagnose problems and gather information not easily available with built-in operating system features.

NetScanTools retains the original goal of providing a flexible set of utilities completely contained in a single tabbed window. Nearly every tab provides the ability to print, save or email data gathered with the tool.

Click here to get started with NetScanTools.

Legal, Trademark and Copyright Acknowledgements

You can contact us here.

Contact Information

If you need to contact us...

Northwest Performance Software, Inc.
PO Box 148
Maple Valley, WA 98038-0148

Sales Office Toll Free Phone: (866) 882-3389
Sales Office Voice Phone: (425) 413-0354
24 Hour FAX--no voice: (425) 413-0639

Our office hours are from 8am to 5 pm Pacific Time, Monday through Friday excluding US holidays. This is the same time zone as Los Angeles. We are located near Seattle. If you call outside those hours, you will get Voice Messaging. If you do, please leave your name, company name, order number or serial number from the About tab (if you are a registered user), phone number and email address. Please indicate why you are calling. **Telephone support is for registered users only. Trial Version users may email to trialsupport@netscantools.com.**

Sales inquiries only to:
sales@netscantools.com
sales@nwpsw.com

Limited support is given by email to trial version users:
trialsupport@netscantools.com

Registered users have full email support:
support@netscantools.com

Requirements

- Windows NT 4 service pack 4 and above, Workstation or Server
- Windows ME
- Windows 98
- Windows 2000
- Windows 95 with Winsock 2.[1] (See http:\\www.netscantools.com\support.html for the Windows 95 Winsock 2 update download link.)
- 32 MBytes RAM
- 2 MBytes of hard disk space.
- TCP/IP network connection, either using a modem or network card.
- 800x600 display resolution, small fonts recommended

[1] Winsock is derived from the sockets concepts found in BSD (Berkeley Software Distribution) UNIX. NetScanTools requires Winsock 2 or above for proper operation.

Overview of NetScanTools

What Is It?

NetScanTools consists of many independent network functions joined together in a single tabbed window. Most functions are designed to run in separate threads so you can use several tabs simultaneously. This program operates best on the newer Windows platforms. For a full list of program hardware and software requirements, click here.

How Does It Work?

NetScanTools communicates primarily using the TCP/IP[2] protocol at the Winsock[3] level. NetScanTools does not rely on remote agents to gather information. Instead, it uses active probing and in some circumstances passive listening for gathering information. Active probing means that NetScanTools originates packets of information called datagrams and listens for responses to those packets. The responses are normally formatted into specific responses which are on a level above that of the transport level, such as a TCP[4] or UDP[5]. An example would be a name server response containing the IP address[6] of a host.

Flexibility

NetScanTools is flexible in that the order of the tabs and visibility of the tabs can be controlled. This allows you to customize NetScanTools to your needs whether beginning or advanced.

To learn about operating NetScanTools, click here.
To learn about each tab, click here.
To learn about the bottom row of buttons below the tabs, click here.
To view some general usage tips, click here.

Y2K information can be found here.

You can contact us here.

[2] TCP/IP means Transmission Control Protocol--TCP (see RFC 793) over Internet Protocol--IP (see RFC 791).

[3] Winsock is derived from the sockets concepts found in BSD (Berkeley Software Distribution) UNIX. NetScanTools requires Winsock 2 or above for proper operation.

[4] TCP means transmission control protocol as defined in RFC 793. It is intended to provide a highly reliable method of assuring delivery of packets between network connected computer systems and uses IP as a next level lower protocol layer.

[5] UDP means User Datagram Protocol and it defined in RFC 768. Unlike TCP, it does not provide a reliable protocol for assuring the delivery of packets between networked computer systems.

[6] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

Help Wizard Tab

About

The Help Wizard is designed to help you find the right tab functions to use given a set of known information.

The tab is divided into three sections. The top left section allows you to check a list of parameters that you have, such as an IP address or a hostname. After checking the appropriate boxes, you can press 'What Can I Do With This Info?' to make a list of topics appear on the right side Answers window. The lower left side window is a set of Frequently asked questions. Click on one to highlight it, then press the 'Show the Answers' button to make a list of topics appear in the Answers window.

Once you have found the answer you are interested in, double-click on it to activate the help file. In many cases you will be automatically switched to the tab that the help file addresses.

See Also...

Overview

The Mechanics: Operating NetScanTools

Starting NetScanTools

NetScanTools can be started from the Start Menu/programs/NetScanTools menu tree. Simply click on the NetScanTools program link. You may choose to make a desktop shortcut at any time. Locate the file 'nststd.exe' using Explorer, right click and drag it to the desktop. We strongly recommend starting NetScanTools **after** making your connection to a TCP/IP network through a Modem or Network Interface Card. This ensures that the Winsock has been properly updated with DNS server IP addresses.

Entering Data

Entering data or queries into NetScanTools is straightforward. Like most programs, NetScanTools expects a certain syntax or key sequence for the data types entered by the user.

Standard Data Types

The most common data types entered in NetScanTools are IP addresses and domain names. Some clients require special syntax which is covered in the client tab help.

IP Addresses

Internet protocol or IP addresses[7] are used much in the same way as a phone number, with each computer on an IP connected network having it's own unique 32 bit address. The IP addresses you will normally enter are a fixed format, although NetScanTools does have one unique exception to this rule when you use Whois to find IP address assignments. IP addresses are the decimal representation of four unsigned 8 bit data bytes, each separated by a period '.'. Because an 8 bit unsigned data byte can only represent numbers in the range of 0 to 255, each of the 'octets' or bytes separated by the periods are of this range. An IP address might be 10.1.5.2 or 10.3.66.254. It cannot be 10.3.66.286 -- remember this when you are looking a header of spam email which often has 'forged' IP addresses.

The one exception occurs when you are doing a Whois query on the owner of a range of IP addresses. In that case you would be entering a subset of the IP address. See the Whois section for full details.

Hostnames

Hostnames[8] are there for human readability--computers would much rather have the IP address. It is easier for humans to remember www.nwpsw.com than 10.1.53.67. A hostname consists of the name of a specific computer, a period '.', then the domain name (next section). A hostname is 'www' with the fully qualified domain name being www.nwpsw.com. The domain name is nwpsw.com.

Domain Names

Domain names[9] are used to define categories and ultimately hosts in DNS (Domain Name System--sort of a huge distributed phone book). A domain name for a US registered business is typically nwpsw.com or microsoft.com. There are other suffixes like edu for educational institutions, mil for military, net for network providers and so forth. Domain names are currently registered with a variety of companies whose charters are to record these names and map them into master domain records. All hosts within a domain are shown with the domain name as a suffix to the computer hostname.

Other Special Syntax

Certain other NetScanTools queries require special syntax such as http:// for the 'What's New at NWPSW' tab and user@company.net (an email address) for finger. Many NetScanTools tabs have a setup dialog box. Each of those setup dialogs has a different set of parameters that need to be entered. Many are numbers with automatic range checking, while some, like the proxy hostnames must be entered as a hostname with no suffixes. Whois queries often require their own special syntax which is often unique to the Whois Server Host.

Common Setup Information

Setup information varies with each client function. Many have numeric entry areas with a brief explanation above the edit box. Some, like Advance Query Setup, have several different kinds of entry: mutually exclusive radio buttons for choosing the current function, checkboxes for activating and deactivating options and edit boxes with a memory call a history list. Setup dialog information is stored in your computer's registry under HKEY_CURRENT_USER/Software/NWPS/NetScanTools/.

Tooltips

Tooltips are tiny yellow windows with a short descriptive phrase that pops up when you move your cursor over buttons or checkbox

---

[7] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

[8] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

[9] Domain Name is the name of the domain that a group of computer systems are assigned to. netscantools.com or nwpsw.com are domain names.

selections. Most NetScanTools controls have tooltips.

History Lists
History lists are present on nearly all client function tabs in NetScanTools. They provide a history of recent queries by saving for future recall hostnames, IP address and other types of queries. History lists are presented in the order of the most recently used entry.

How History Lists Work
History lists work by first taking the information entered, checking it against entries currently in the drop-down listbox, then moving up a match with a previous entry or entering the new entries. The last entered query is always shown in the entry box.

Editing History Lists
The only option you are allowed with the list box history entries is to clear the whole list. Press the 'C' button to the right of the listbox to clear the list.

Working With The Results
Each client function in NetScanTools accesses a different set of unique data. Some data are short and easy to assimilate, like daytime, while other data, like that generated by a domain listing, can be thousands of lines long. Fortunately, NetScanTools has several tools for searching and working with the results data.

Finding Text
Finding text in a results window is probably one of the most important time saving features in NetScanTools. To find text, enter the text you are interested in (case insensitive) and press Find First. If the text exists, it will be highlighted. You can find subsequent instances of the same text by pressing F3. For a complete explanation, see this topic.

Copying Text To The Clipboard
One of the most common things you will do while using NetScanTools is copying text to the clipboard. There are several methods that you can employ to copy text to the clipboard. For further explanation, see this topic.

Printing
Printing is useful for documenting results of many of the client functions. You can print all client function results window contents and certain specific other things like the Winsock Info tab. Printing requires access to a printer either attached to the current machine or via a network. Printouts have a date and timestamp at the top and most have a header explaining the type of information being printed. For further explanation, see this topic.

Tip: Most NetScanTools printouts look best using a 9 point Courier New TrueType font.

Saving To Disk
All NetScanTools client function results window contents can be saved to an ASCII text file on disk. To save results to a file, press the Save To File button at the bottom of the NetScanTools main window. This will activate the standard Save File dialog box from which you can navigate to the location that you want to store the file. Choose a name for the file that is meaningful for the results you are saving. The default filename is 'untitled.txt'. For further explanation, see this topic.

AutoPaste
'AutoPaste' is a very powerful feature that can save you typing strokes and it provides for greater accuracy when working with long hostnames and IP addresses. AutoPaste allows you to copy selected results area text or input text to a special clipboard-like transfer buffer. When you move to a new tab, this text is automatically pasted into the input area of each tab as it is selected. For further explanation, see this topic.

Appearance
The appearance of NetScanTools can be changed from the Preferences Tab. For further explanation, see this topic.

Fonts
Font selection is made from the Preferences Tab. The selected font affects all results windows and the printed results. The default font is 9 point Courier New. To select a different font, go to the Preferences Tab and press the Change Font button. For further explanation, see this topic.

Minimizing To Taskbar Tray
On Windows 95/98 and Windows NT 4.0, there is a part of the taskbar called the tray. In a default installation, this is the area on the right hand side where the clock appears. NetScanTools can be minimized to the taskbar tray area by checking the Minimize to Taskbar Tray checkbox on the Preferences tab. When you minimize NetScanTools, it will appear as a tray icon or a normal minimized program on the taskbar depending on your selection. For further explanation, see this topic.

The 'Stop' Button
The 'stop' button is common to many of the NetScanTools client tabs. Press it to stop the current activity.

Activating The Help File
There are two ways to activate the help file:

- Press the help button located in the lower right hand side of the main window adjacent the Exit button.

- Press the F1 function key located above the number row of your keyboard.

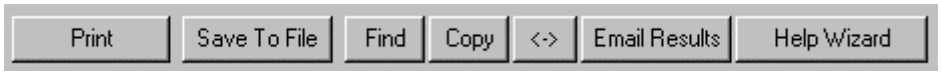
Exiting NetScanTools
To exit NetScanTools, locate the Exit button at the lower right section of the main window and click it. Any current network functions in progress will be terminated.

See Also...
The Functions Tabs
The Lower Button Row
Usage Tips
Welcome

The Lower Button Row

The lower button row is visible from each tab, however, not all buttons are active or behave exactly the same way depending on what tab is currently visible.

Click on the button below to activate help for that button.



or click on these links:
Print, Save To File, Find, Copy, <-->, Email Results, Help Wizard

Activating The Help File
There are two ways to activate the help file:

I. Press the help button located in the lower right corner of the main window adjacent the Exit button (see the buttons below).
II. Press the F1 function key located above the number row of your keyboard.

Exiting NetScanTools
To exit NetScanTools, locate the Exit button at the lower right section of the main window as shown above and click it. Any current network functions in progress will be terminated.

See Also...
The Function Tabs

Print Button

Printing

Printing is useful for documenting results of many of the client functions. You can print all client function results window contents and certain specific other things like the Winsock Info tab. Printing requires access to a printer either attached to the current machine or via a network. The client function results area must contain data to be printed. Printouts have a date and timestamp at the top and most have a header explaining the type of information being printed.

To print results, simple press the print button at the bottom of the NetScanTools main window. This activates the print dialog from which you can choose the printer and the number of copies you wish to print.

Printing uses the currently selected results area display font. You can set the fonts from the Preferences Tab.

Tip: Most NetScanTools printouts look best using a 9 point Courier New TrueType font.

Some special displays like the Port Probe, Ping, TraceRoute, etc. are going to print in formatted ASCII text. This means that the image you see in the results area will not be printed exactly as you see it. For instance, for a Ping print, the columns will be represented by the tab character. For the treeview displays like Port Probe, the levels of the tree are represented using multiple levels of indentation controlled by the number of tab characters used to represent the level.

See Also...

The Lower Button Row

Save To File Button

Save To File

As with printing, all NetScanTools client function results window contents can be saved to an ASCII text file on disk. To save results to a file, press the Save To File button at the bottom of the NetScanTools main window (see Figure above). This will activate the standard Save File dialog box from which you can navigate to the location that you want to store the file. You may also want to choose a name for the file that is meaningful for the results you are saving. The default filename is 'untitled.txt'.

See Also...

The Lower Button Row

Copy Button

Copying Text to the Clipboard

One of the most common things you will do while using NetScanTools is copying text to the clipboard. There are several methods that you can employ to copy text to the clipboard.

Method 1:

I. Highlight the desired text with your cursor.
II. Press Cntl-C (or Cntl-Insert) to copy the text to the clipboard.
III. Press Cntl-V (or Shift-Insert) to paste the text to the desired new location.

Method 2:

I. Highlight the desired text with your cursor.
II. Right click on the highlighted text to activate the text copying popup menu. Select 'copy' to copy the text to the clipboard.
III. Right click in the destination location to activate the text copying popup menu. Select 'paste' to paste the text to the desired new location.

Method 3:

This special method applies to Ping, TraceRoute, Database Tests, WinSock Info, Port Probe, NetBIOS Info, NetScanner only. Since these tabs use special display elements like list views and treeviews, you cannot simply highlight text and copy it.

I. Press the Copy button on the lower button row.
II. Data Viewer[10] will appear with a text representation of the results show on the tab. Use either of the previous two methods to copy from Data Viewer.

See Also...

The Lower Button Row

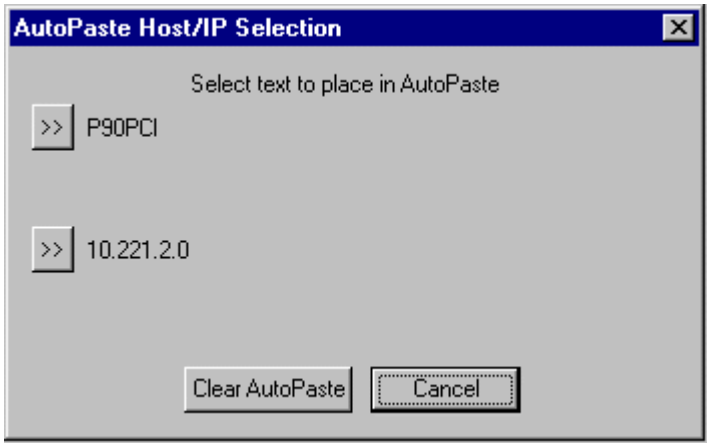
[10]The Data Viewer window is used to display text. You can copy text from Data Viewer by highlighting and right-clicking to bring up the edit menu. You can also locate and find any text (not case sensitive) using the Find and Find Again buttons. You can print or save the data to a file.

The Data Viewer window is use frequently throughout NetScanTools to display text from special display elements like listviews and treeviews.

AutoPaste (<-->) Button

AutoPaste

'AutoPaste' is a very powerful feature that can save you typing strokes and it provides for greater accuracy when working with long hostnames and IP addresses. AutoPaste allows you to copy selected results area text or input text to a special clipboard-like private transfer buffer. When you move to a new tab, this text is automatically pasted into the input area of each tab (if applicable) as it is selected. This is especially useful when you get Name Server Lookup results that show an IP address or hostname and you want to move to the Ping tab to ping the computer.



For the example shown above, the IP address 10.221.2.0, was highlighted in the results window and the word P90PCI was in the input edit box. To transfer the IP address 10.221.2.0 to all other tabs, then you would press the button next to the IP address. Once you select an IP address or hostname, it will be transferred to the other tabs each time you select a tab until you either clear the AutoPaste buffer or exit the program.

Clearing the AutoPaste Buffer. You can clear the AutoPaste buffer by pressing the Clear AutoPaste button in the selection dialog. Once the buffer is cleared, text selected in AutoPaste will no longer be transferred to each tab's input edit box.

Special Note about some of the tabs like NetScanner: AutoPaste will only transfer IP addresses into the Start and End IP address entry boxes. It transfers the same IP address into both boxes. It will not place Hostnames into the IP address entry boxes.

See Also...

The Lower Button Row

Email Results Button

Email Results

Press the Email Results button to email the text contents of each results area. The type of email subsystem varies with the selection you have made on the Preferences tab.

If you choose MAPI, NetScanTools will use the MAPI (Messaging API) subsystem to send your message. This works best on machines where Microsoft's Exchange or OutLook email services are the default. View an example here.

The other email option is SMTP (Simple Mail Transfer Protocol). The SMTP option bypasses any other email subsystems in your operating system and communicates directly to the SMTP email server of your choice. View an example here.

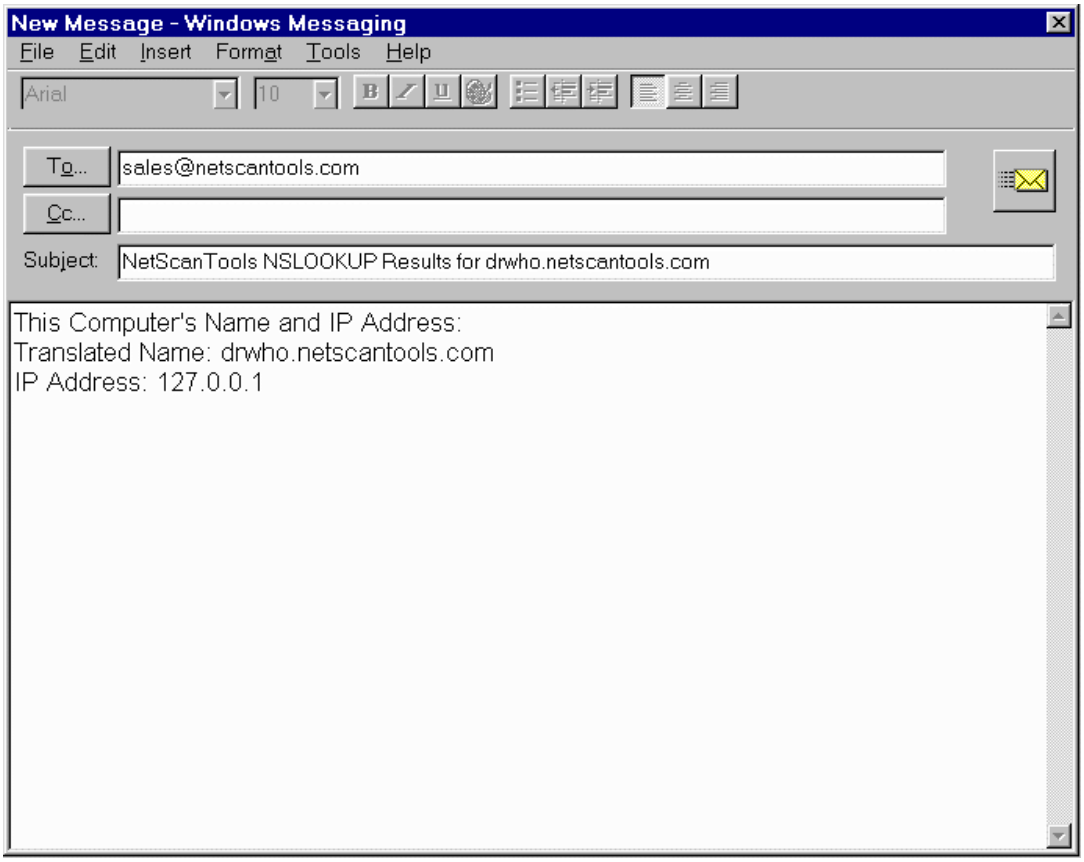
See Also...

The Lower Button Row

Email Results Using MAPI

About

This dialog is shown when the Email Results button is pressed AND the Email Results Button Protocol setting is set to MAPI on the Preferences tab.



Edit the message as required. You will need to enter a target email address.

If your system does not have Windows Messaging installed, you will see the image below. If that happens, either install Windows Messaging or select SMTP[11] on the Preferences tab.

See Also...

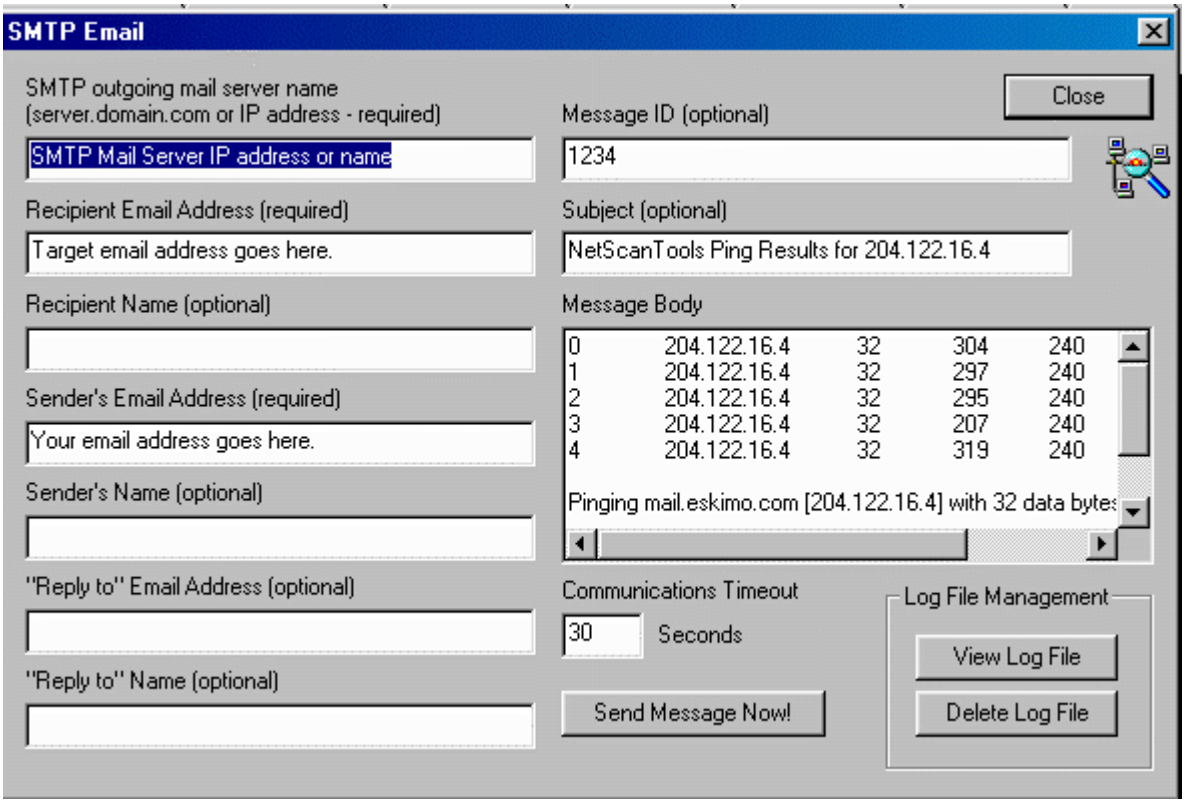
Lower Button Row
Preferences

[11] SMTP - **S**imple **M**ail **T**ransfer **P**rotocol. For more information, see RFC 821.

Email Results Using SMTP

About

This dialog is shown when the Email Results button is pressed AND the Email Results Button Protocol setting is set to SMTP on the Preferences tab.



Most of the above fields are self explanatory. The required fields must be filled in. The SMTP server field accepts an IP address[12] or hostname[13]. All fields with 'email address' must be of the form user@somecompanysomewhere.com.

The **Send Message Now!** button begins the mail sending process. If you wish to view the SMTP email log file, press the **View Log File** button. To delete the log file, press the **Delete Log File** button. The **Communications Timeout** field controls the amount of time that NetScanTools waits for responses from the SMTP server. The recommend value is 30 seconds.

See Also...

Lower Button Row
Preferences

[12] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

[13] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

Find Button

Find and Find Next

Finding text in a results window is probably one of the most important time saving features in NetScanTools. To find text, we will have to assume that you have some text to search through. Switch to a tab, make a query and NetScanTools will show some results. Once you have a set of results text, you can activate the Find dialog box by clicking on the Find button at the bottom of the NetScanTools window.

You then enter the text you are interested in (case insensitive) and press Find First. If the text exists, it will be highlighted. You can find subsequent instances of the same text by pressing F3. Here is an example:

Find Text Example

Many of the client functions contained in NetScanTools produce results which exceed the vertical window size of the results area. A good example is the 'whois' client. Entering a query such as the word 'Smith' (no quotes) produces a long list of all the persons named 'Smith' and companies with the name Smith in it. So how do you find the right text?

For this example, we are assuming that you are actively connected to a TCPIP network with unrestricted access to the Internet.

I. From the NetScanTools Whois tab, press the 'setup' button and set the following values:
   - whois.networksolutions.com for server. ('Smart Whois' will have no effect in this example)
   - Optionally, you may need to set your whois proxy if you are behind a firewall.
   - Close the whois setup by pressing OK.

I. Enter the word 'eskimo' (no quotes) in the whois query entry box and press the Query button. (note: you may use any other query string you wish)

II. When NetScanTools is done receiving the data from the whois server (this may take up to a couple of minutes), the NST logo will stop spinning. You should have several companies with the word eskimo in them.

III. Now press the Find button at the bottom of the NetScanTools window. You may also press cntl-F.

IV. Enter the text 'North' (no quotes) in the Find dialog and press Find First. The first occurrence of North should be highlighted. Note that this search engine is not case sensitive.

V. Press the F3 key to highlight subsequent occurrences.

Note: Find works differently with list views like Ping or TraceRoute. The specific text is NOT highlighted--only the row that the text appears on. For treeviews such as Port Probe, the whole entry is highlighted, not just the actual text that was found.

See Also...

Finding Text in a Results Window
The Lower Button Row

The Data Viewer window is used to display text. You can copy text from Data Viewer by highlighting and right-clicking to bring up the edit menu. You can also locate and find any text (not case sensitive) using the Find and Find Again buttons. You can print or save the data to a file.

The Data Viewer window is use frequently throughout NetScanTools to display text from special display elements like listviews and treeviews.

The Function Tabs

Each of the tabs in NetScanTools is designed to accomplish a certain set of goals and provide a common user interface for a widely varying set of individual functions.

Detailed help for each function tab:

About
Character Generator Client
Database Tests
Daytime
Echo
Finger
Help Wizard
IDENT Server
Launcher
Name Server Lookup
NetBIOS Info
NetScanner
Ping
Port Probe
Preferences
Quote
TCP Term
TimeSync
TraceRoute
What's New at NWPS Web Site
Whois
Winsock Info

Lower Button Row

To learn about the row of buttons below the function tabs, click here.

About Tab

About

This tab is used to display Registration Information, Copyright Notice, Version Information and Contact Information.

If you need to contact us, be prepared to provide the information from this tab.

Support Group

This group of buttons are intended to help our technical support personnel diagnose problems you may have.

- You may also be asked to provide the information about your NetScanTools file versions which is found by pressing the **File Versions** button.
- The **Registry Report** button is used to dump the NetScanTools setup information from the registry. You can copy the text from the Dataviewer window into any email program.
- The **Restore Defaults** button erases all the NetScanTools setup information and the history lists from the registry. History lists are the dropdown lists of previous queries or targets made on a tab. Use this button with caution.

See Also...

The Lower Button Row

Character Generator Client Tab

About

The Character Generator (or Chargen) client tab connects to and receives data from an RFC 864 Chargen Service. When a connection is made on the Chargen Server port, a stream of ASCII characters are sent as fast as the connection will allow. The purpose of this feature is to assist in testing network speed.

How it Works

The Character Generator Client tab can function as both a TCP[14] and a UDP[15] client. Normally you will want to run in TCP mode. This is because TCP is a reliable connection and will give you a better indication of the speed of the total network connection between your computer and that of the Chargen Server. When NetScanTools makes a connection to the Chargen Server, NetScanTools displays the first 1024 characters received. It then keeps receiving and displaying the effective characters per second until the Stop button is pressed. The limited display of characters is is done because updating the display with new characters significantly slows down the apparent speed of the network connection.

Information Returned by this Feature

This feature will assist you in determining the apparent speed of your network connection between your computer and the target computer.

Help Wizard Topics

- *Using Chargen to determine connectivity and link speed.* Enter the IP Address or hostname and press Connect. If the target is running a chargen server, you will see a response. If the target refuses your connection, you will see it in the response area. A refusal would mean that you can contact the host. This only works with TCP, UDP does not show refusals. Link speed is only shown if a chargen server is contacted.

Using Chargen

Select a host known to be running a Chargen Server either by hostname or IP address, then press the connect button. Once a connection is established you will see a pattern of characters, then updates of the results area will stop. Observe the apparent connection speed just above the results window.

The information you can gather from the Chargen Client is the total effective speed of your network connection between the two machines, including the effects of data compression, if any. Test data is normally compressed when it goes through a modem connection, so the characters per second display will often exceed the expected bandwidth of your modem.

TCP usage will show a relatively stable characters per second reading after some settling time has elapsed. UDP servers tend to send their characters in batches, so you will notice wide variations in the apparent speed of the connection.

Chargen is one of the 'Simple TCP/IP Services' optionally installed on Windows NT. The Simple TCP/IP Services are Chargen, Daytime, Discard, Echo and Quote.

Error Messages

The two most common error messages you will see are shown below.

```
Error getting host address:
Valid name format; No hostname or IP data record was found in the Name Server.
```

or

```
Error connecting to host:
The attempt to connect was refused.
```

The first error message means that the hostname requested could not be resolved to an IP address and the second error message means that the target host is either not running a Chargen Server, or it refused you access to a working Chargen Server using IP address accept/reject lists.

See Also...

Daytime
Echo
Quote
The Lower Button Row

[14] TCP means transmission control protocol as defined in RFC 793. It is intended to provide a highly reliable method of assuring delivery of packets between network connected computer systems and uses IP as a next level lower protocol layer.

[15] UDP means User Datagram Protocol and it defined in RFC 768. Unlike TCP, it does not provide a reliable protocol for assuring the delivery of packets between networked computer systems.

Database Tests Tab

About

Winsock is descended from sockets on the BSD UNIX operating system. As such, it carries with it several features like the hosts file[16] and two other lesser known, but useful files named protocol and services. The Protocol and Services database files have no file extension and are found in the Windows folder on Windows 95/98 and in the Windows\system32\drivers\etc folder on Windows NT. They are text files and their purpose is to translate human readable names of protocols and services to numbers and vice versa.

The format of the protocols database (the smallest and possibly the least useful database) is:

```
Protocol name  protocol number       #comment
```

A single entry in the protocols database looks like this entry for the IP protocol:

```
ip       0     IP       # Internet protocol
```

If your internet program requests the translation for the protocol 'ip', sockets translation functions will return the number zero (0). A much more useful database is the services database. The entries in this database are used for translating the names of services like 'ftp' to a number (21) used by sockets enable programs.

The format of the services database is:

```
service name   port number/protocol   aliases #comment
```

Since services can operate on both TCP and UDP ports, an entry can and frequently does consist of two lines depending on the protocol used as is shown in this example for the chargen service:

```
chargen            19/tcp    ttytst source
chargen            19/udp    ttytst source
```

So when an internet enabled program wants to know what TCP port the chargen service runs on, it queries the database using the translation functions which return port number 19.

Information Returned by this Feature

NetScanTools starts through a numeric incremental loop which queries the database for each protocol or service port number. There 256 protocol numbers and 65536 port numbers. The results are presented and displayed. If you get no results when you run either test, then the respective database may be missing or corrupted.

What Database Tests Are and...

Database tests strictly test the translation or mapping capabilities of the underlying Winsock protocols and services databases. You can use the resulting information to quickly determine the port number for a particular service or to determine if the databases were installed when TCP/IP was installed.

...***What They Are Not***

The database tests feature DOES NOT test ports for active services and it does not tell you what features or services are running on your computer. Use the Port Probe feature to tell you that information.

Using Database Tests

Select the database to test and press Analyze. Press Stop to stop the process. Press AutoSize[17] to automatically size the columns to the width of the data.

View Services Database, View Protocols Database

Press these buttons to view the contents of the databases.

Error Messages

There are no error messages for this feature.

See Also...

Port Probe
The Lower Button Row

[16] A hosts file is used on a local computer to rapidly resolve the name of a host or an IP address without necessitating the need to query a DNS. Winsock normally looks for and scans a hosts file prior to communicating with DNS.

[17] The AutoSize button causes all columns in a report style list view to be sized to the widest text string found in the column.

Daytime Tab

About

The Daytime protocol is defined in RFC 867. Daytime can be used as a quick way to determine the local time at that remote computer's location.

Information Returned by this Feature

When a host running a Daytime Server accepts an incoming connection, the Daytime Server immediately returns the time of day at the Server's location. There are several common formats used by networked systems. The format used by Windows NT is shown here:

```
[localhost]

Saturday, November 1, 1997 22:05:56

[End of daytime message]
```

Internet sites at many established (in internet years, that would be pre-1994) educational institutions will have a Daytime Server running at their location. To be really useful, you have to have a good idea as to where the site is located or at least what time zone the server is in. Doing a whois query on the domain would be useful in determining this.

Do not confuse this with the Time Sync tab. Time Sync uses Network Time Protocol clocks that are synchronized to high accuracies to distribute the current GMT or UTC time. Daytime protocol comes as a text string unlike the binary structures that comprise the Time Sync supported protocols. The information returned by the Daytime Protocol *may not* be year 2000 compliant and as a client application, NetScanTools cannot guarantee Y2K compliance of the data returned since it is generated and formatted external to NetScanTools.

Daytime is one of the 'Simple TCP/IP Services' optionally installed on Windows NT. The Simple TCP/IP Services are Chargen, Daytime, Discard, Echo and Quote.

Using Daytime

Enter a target hostname or IP address and press the Daytime button. If the target host is running a Daytime Server, you will see a connection being established and a text string representing the time of day at the target host's site.

Error Messages

The two most common error messages you will see are shown below.

```
Error getting host address:
Valid name format; No hostname or IP data record was found in the Name Server.
```

or

```
Error connecting to host:
The attempt to connect was refused.
```

The first error message means that the hostname requested could not be resolved to an IP address and the second error message means that the target host is either not running a Daytime Server, or it refused you access to a working Daytime Server using IP address accept/reject lists.

Year 2000 Compliance

NOTICE: This Information is designated as a Year 2000 Readiness Disclosure and the information contained herein is provided pursuant to the Year 2000 Information and Readiness Disclosure Act.

The daytime client is based on RFC 867 which defines the retrieval of an ASCII text string representation of the local time and date at a remote computer. NetScanTools simply connects to the remote host, requests the current daytime from the host and then displays the text string verbatim. The text displayed by NetScanTools is generated by the other host. Here is an example of the text generated by a Windows NT Daytime Service:

```
Monday, February 23, 1998 17:22:00
```

Some systems report the time in this format:

```
02 FEB 82 07:59:01 PST
```

Clearly, the second format violates year 2000 requirements, but the important thing to note in this example is that *NetScanTools DID NOT GENERATE the string nor did it attempt to alter the non-compliant date format, NetScanTools only reports the text string EXACTLY as sent to it by the other computer*.

See Also...

Character Generator Client

Echo
Quote
Time Sync
The Lower Button Row

Echo Tab

About

Echo is an RFC 862 TCP or UDP service which 'echoes' back all characters received on the port that it is listening on. Due to security considerations--specifically Denial of Service attacks, this feature is often disabled on internet connected computers.

Information Returned by this Feature - The alternative to Ping

Some computers are programmed to refuse to respond to ICMP echo request (type 8) packets. If you know the computer's IP address, you can use other techniques to determine if it is active. One technique is to try to see if the target computer will respond to an echo request.

Help Wizard Topics

- *Using Echo to determine connectivity.* Enter the IP Address or hostname and press Connect. If the target is running an echo server, you will be able to type in text and see a response. If the target refuses your connection, you will see it in the Echo Response area. A refusal would mean that you can contact the host. This only works with TCP, UDP does not show refusals.

Using Echo

To use the echo client you enter an IP address[18] or hostname[19], select TCP[20] or UDP[21] protocol, the press Connect. Once the connection is made, your cursor is automatically moved to the input area and you can begin typing in text. The echoed text will appear in the lower window along with any error messages. Disconnect from the echo server by pressing the Disconnect button.

UDP Protocol Notes

Since UDP protocol does not guarantee delivery of packets, it is an interesting exercise to target a computer running the echo service many hops away, then use UDP mode. Characters will be dropped and sometimes *interchanged or have their positions swapped* because UDP does not guarantee delivery or sequencing.

Echo is one of the 'Simple TCP/IP Services' optionally installed on Windows NT. The Simple TCP/IP Services are Chargen, Daytime, Discard, Echo and Quote.

Error Messages

TCP protocol will give you a valid indication of whether or not the connection was really made. UDP protocol will not do that because there is no handshaking to verify receipt of packets.

The two most common error messages you will see are shown below.

```
Error getting host address:
Valid name format; No hostname or IP data record was found in the Name Server.
```

or

```
Error connecting to host:
The attempt to connect was refused.
```

The first error message means that the hostname requested could not be resolved to an IP address and the second error message means that the target host is either not running a Echo Server, or it refused you access to a working Echo Server using IP address accept/reject lists.

See Also...

Character Generator Client
Daytime
Ping
Quote

---

[18] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

[19] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

[20] TCP means transmission control protocol as defined in RFC 793. It is intended to provide a highly reliable method of assuring delivery of packets between network connected computer systems and uses IP as a next level lower protocol layer.

[21] UDP means User Datagram Protocol and it defined in RFC 768. Unlike TCP, it does not provide a reliable protocol for assuring the delivery of packets between networked computer systems.

Finger Tab

About

The Finger tab provides a client interface to a finger server usually located on a remote computer. NetScanTools includes a Finger client that is compliant with RFC 1288 and it also includes a companion IDENT server which is often required to be concurrently operating by many finger servers before they return any information to you.

Information Returned by this Feature

Finger returns a set of information that is designed to be read by people, not programs. Although there are no strict formats, the RFC does provide some general guidelines. Typically, you will see the username or Login name, the person's real name as stored on the server, directory, last login time and mail reading status. Optional items include office location and phone number, terminal number, project and plan. Some finger implementations will include all of these items, but most will only show the login name and real name unless you ask for Verbose Format. Due to security considerations, many sites either do not respond to finger requests or they provide a very small amount of information.

Help Wizard Topics

- *Using Finger to gain user information.* Enter the email address and press Finger.

Setup

Press the **Setup** button to activate the Finger Setup dialog. You may enter the hostname or IP address of a finger proxy server here. To activate proxy usage, check the **Use Proxy Server** checkbox. Finger protocol also includes a 'backdoor' method of implementing proxies using a forwarding finger request. For example, if it is supported by the finger server, you can do things like finger user78@hostOne@hostTwo.

Using Finger

Finger queries are normally done using another user's email address. Basic Finger queries use the same exact syntax as an email address: `bulkEmailer@ASleasyCompany.com`

Simply enter the email address in the 'Enter Query' edit box, check or uncheck the 'Make Verbose Format Query' checkbox and then press the Finger button. If a finger server exists on the target computer, then you will get some sort of response.

Note that the '**Make Verbose Format Request**' checkbox adds the /W to the string sent to the finger server. This is the same as the UNIX syntax: finger -l user@aHostSomewhere.com. This instructs complying hosts to send expanded user information back to NetScanTools, if available. This option must be checked *prior* to making the finger request. *Not all hosts will respond to this command*. If unsure of the server's support for this feature, uncheck the checkbox.

Using Finger in conjunction with NSLOOKUP

Many email addresses are domain oriented instead of physical machine oriented. Domain oriented means is that the computer with the user you are trying to Finger does not really exist. Instead, all mail destined for that domain goes through a mail exchange computer (the MX records in the DNS). Determining the MX computer for a domain is relatively simple using NetScanTools--see the NSLOOKUP section for more information. First, try entering the exact email address into Finger and the press the Finger button. If you get a message like this:

```
Error getting host address:
Valid name format; No hostname or IP data record was found in the Name Server.
```

You are most likely dealing with a *domain* that uses one or more mail exchange computers. Now you have to do some detective work. You must take the domain name[22], let's use ASleasyCompany.com as an example and switch to the Name Server Lookup tab. Then follow these steps:

- Go to the Adv Qry Setup and verify that you are using a valid Current Server DNS, and set the Query Type to MX. *(Also be sure that your timeout is at least 15 seconds with 1 retry and Append Default Domain Name and Use Recursion are checked. If you are behind a firewall, you must use a DNS that is aware of domains outside your local behind-the-firewall network.)*
- Close the Adv Qry Setup by pressing OK.
- Enter ASleasyCompany.com into the query area and press NSLOOKUP.

```
Looking up [ASleasyCompany.com]

Server:  isumataq.eskimo.com
Address:  204.122.16.31

ASleasyCompany.com preference = 10, mail exchanger = mail2.ASleasyCompany.com
mail2.ASleasyCompany.com  internet address = 10.31.8.1
```

[22] Domain Name is the name of the domain that a group of computer systems are assigned to. netscantools.com or nwpsw.com are domain names.


```
[End Query]
```

The mail exchanger computer is the host that actually sends and receives email. Some domains have several mail exchanger computers. Each of those computers will need to be noted and checked.

Hint: Open a second instance of NetScanTools for the NSLOOKUP queries and do the Finger queries from the first instance--view them both simultaneously. Transfer data using copy and paste.

Now enter bulkemailer@mail2.ASleasyCompany.com into the Finger tab and press Finger. If the target host is running a Finger server, you may see something like:

```
[bulkemailer@mail2.ASleasyCompany.com]

Login name: host4\dave                  In real life: Dave Spammer
Directory: \users\d\dave
Last login Sat Nov 01 08:19:10 1998

Project:
Mail everyone on the internet my pyramid scheme sales message at least once a day.
Plan:
Collect all the email addresses of those who responded with 'remove' and sell them to people
like me.

[End of finger server message]
```

Interpreting the results
Finger is gives a small amount of data, and what you do get can be sometimes very useful. Finger is not implemented as widely as it once was.

Finger and the IDENT Server
As a security measure, many Finger Servers require you to identify yourself to them before they will send information about the user account you are 'fingering'. This is done using an RFC 1413 Ident (or Auth) request. The Ident protocol is fairly simple: when another computer (you) makes a network connection to the Finger Server port 79 on the target host, the IP address of the requesting computer (you) can be easily obtained through a simple sockets function call. The Finger Server computer then makes a counter connection to the requesting computer's IDENT port asking which user is connecting to the Finger Server port. The IDENT server then sends back the user name and other very brief information like the operating system type code. This is an example of what the IDENT server sends back:

```
1342, 79 : USERID : WIN32, US-ASCII : user
```

NetScanTools provides a fully configurable IDENT server which, when enabled, responds to IDENT requests from Finger Servers, or any other remote Server such as Whois, mail servers or even a web server.

Error Messages
Error messages that are most frequently seen while using Finger are shown here.

```
Error getting host address:
Valid name format; No hostname or IP data record was found in the Name Server.
```

This usually means that the email address is aliased to an email exchanging machine and the machine you are trying to Finger does not really exist. For example, if you are trying to get Finger information on John.Doe@somebigcompany.com, the host computer named somebigcompany.com may not really exist. This is normally a valid domain name and you can verify this with NSLOOKUP. The procedure for finding the MX machine for a domain is detailed above under **Using Finger in conjunction with NSLOOKUP**.

```
Error connecting to host:
The attempt to connect was refused.
```

If you try sales@nwpsw.com, you will most likely get the message explaining that the connection was refused by the remote host. This simply means one of two things--either the host nwpsw.com was not running a Finger Server or the Finger Server refused to allow you to gain information because of some security measures in place for that machine.

Finger Server Logging Warning
There are times when you will connect to a Finger Server and it will appear at first that you may get back a message, but instead, you get something like this:

```
[john.doe@somecomputer.com]
```



```
[End of finger server message]
```

There is nothing wrong with your computer or NetScanTools! The Finger Server has been configured to provide no information back to the Finger Client (you, using NetScanTools). You should *always* assume that the Finger Server is *logging* Finger requests, so keep this in mind if you use Finger frequently---this type of answer may be their way of logging your request.

Comments
The results from this tab can be printed, saved to a file, copied to the clipboard or emailed. The Clear Results[23] button clears the results display. The AutoClear[24] button clears the display each time a finger command is started.

See Also...
IDENT Server
NSLOOKUP
The Lower Button Row

[23] The results area of this tab are cleared when this button is pressed.

[24] AutoClear clears the results area of this tab each time a new function is activated.

How To Buy

About

This tab contains links to the most current ordering information for NetScanTools on our web site.
NOTICE: Prices and shipping charges are subject to change without notice.

Pricing for 1 copy:
$25 to obtain an unlock code for a downloaded copy.
$30 + shipping to obtain a CDROM.

Full pricing web page:
http://www.netscantools.com/nstpricing.html

How to Buy top page:
http://www.netscantools.com/howtobuy.html

Online Ordering:
http://www.netscantools.com/orderonline.html

Printable Orderform:
http://www.netscantools.com/nstorderform.html

Web site main page:
http://www.netscantools.com/
-or-
http://www.nwpsw.com/

Sales Phone:
Phone hours: 8am-5pm Pacific Time (Los Angeles time), Monday-Friday excluding US Holidays.
Toll Free: (866) 882-3389
(425) 413-0354
24x7 FAX: (425) 413-0639

Mailing Address:
Northwest Performance Software, Inc.
PO Box 148
Maple Valley, WA 98038-0148
USA

Payment types accepted: Visa, Mastercard, American Express, Novus, Discover, check, money order, purchase order.
Limitations apply to checks or purchase orders from non-US/Canada locations--please see our web site How to Buy page and click on the links for purchasing with checks or purchase orders:
http://www.netscantools.com/howtobuy.html

Last revised June 2001.

IDENT Server Tab

About

The IDENT Server tab controls the activities of the NetScanTools identification protocol server as defined in RFC 1413. The Ident Protocol (formerly known as Authentication Server Protocol) is intended to provide a means for determining the identity of a user of a TCP[25] connection. Some services, most often Finger and sometimes POP3 mail servers, require an IDENT server to be running on your system before they will respond with the information you are requesting from them. The IDENT server listens for incoming connections on port 113 (decimal).

Information Returned by this Feature

This feature logs incoming IDENT requests. This server *does send back a response* to the source of the IDENT request---however, only the information you wish it to see.

A **sample log file** fragment is shown here.

```
Mon, 07 Jun 1999 16:14:34 IP: 204.122.16.4 - 3120,110 : USERID : WIN32, US-ASCII : user
Mon, 07 Jun 1999 16:18:39 IP: 204.122.16.4 - 3146,110 : USERID : WIN32, US-ASCII : user
Mon, 07 Jun 1999 16:19:38 IP: 204.122.16.6 - 3152,21 : USERID : WIN32, US-ASCII : user
Mon, 07 Jun 1999 16:19:48 IP: 204.122.16.5 - 3152 , 21 : USERID : WIN32, US-ASCII : user
Mon, 07 Jun 1999 16:22:03 IP: 204.122.16.4 - 3169,110 : USERID : WIN32, US-ASCII : user
Mon, 07 Jun 1999 16:22:42 IP: 204.122.16.4 - 3173,110 : USERID : WIN32, US-ASCII : user
Mon, 07 Jun 1999 16:26:37 IP: 204.122.16.4 - 3181,25 : USERID : WIN32, US-ASCII : user
Mon, 07 Jun 1999 16:26:39 IP: 204.122.16.4 - 3181,25 : USERID : WIN32, US-ASCII : user
Mon, 07 Jun 1999 16:26:57 IP: 204.122.16.4 - 3187,110 : USERID : WIN32, US-ASCII : user
Mon, 07 Jun 1999 16:27:31 IP: 204.122.16.4 - 3190,110 : USERID : WIN32, US-ASCII : user
```

The format of the log file is date and time, followed by incoming IP address, then our source port number, a comma, the target port number that we are connecting to with another application, the operating system type (WIN32 always), the code page used and finally the username of the user whose process is accessing the target port on the other machine.

This example log file fragment is showing connections to POP3 (110) to get email from the server, connections to an FTP (21) port and connections to an SMTP (25) port to send email. Using the first entry as an example, the IDENT server is getting a request from the target machine (204.122.16.4) to identify the user who is connecting to port 110 from the user's machine port 3120. The IDENT server send backs a string to the target machine which is of the exact form:

```
3120,110 : USERID : WIN32 , US-ASCII : user
```

This is telling the target machine that the person attempting to get email from the POP3 server has a login name of 'user' and is running on a WIN32 machine (95, 98 or NT). Of course, we chose the login name 'user' ahead of time.

Configuring the IDENT Server

This section discusses the configuration of the server. Press the **Configure** button to reach the setup dialog box. This dialog box controls the type of message returned to the host making the IDENT request. The **Response Message Type** defaults to **USERID**. When USERID is selected, the User Name Reported Back to the requesting host is exactly what is entered in the entry area. In this example 'user' has been entered. It can be anything; the default is 'user'.

NOTE: all IDENT requests receive the information as specified in the Configure dialog box.

Other user-defined response types are:

- **Error - INVALID-PORT**. This message means that the local machine or target machines port number was not properly specified. This means that the TCP port was out of the 1-65535 range.
- **Error - NO-USER**. This message tells the requesting host that the user could not be identified or the port pair is not in use.
- **Error - HIDDEN-USER**. This message tells the requesting host that the port pair user was identified but the user has requested to remain anonymous.
- **Error - UNKNOWN-ERROR**. The IDENT server cannot determine the ownership of the port connection pair.

To log IDENT requests to the Ident log file, you must check the **Enable IDENT Request Logging** checkbox. For security reasons, this box is not checked by default (new in version 4.03).

You may clear the previous entries in the User Name entry area by pressing the button mark 'C' located to the right of the entry area.

To enable or disable the IDENT server, please check or uncheck the **Enable IDENT Server** checkbox on the IDENT Server tab as desired. You may verify that the server is operating by using the command line function 'netstat'. You can also manually test the IDENT server by using TCP Term to connect to the 'AUTH' port on 'localhost', then type some text and press enter.

See Also...

Finger

[25] TCP means transmission control protocol as defined in RFC 793. It is intended to provide a highly reliable method of assuring delivery of packets between network connected computer systems and uses IP as a next level lower protocol layer.

TCP Term
The Lower Button Row

Launcher Tab

About

Launcher is a simple program launcher. It works by using the program associations to determine which program to launch to connect to the given hostname[26] or IP address[27].

Information Returned by this Feature

Launcher does not actually directly return information. It launches other programs which are responsible for connecting to the target host and those programs interact with the target host.

Usage

Enter a hostname or IP address and press either the HTTP, FTP or Telnet button. NetScanTools signals the operating system that you would like to use the selected protocol to connect to the target host and it then selects the program which is normally used with those protocols. HTTP or FTP will usually launch your default web browser while Telnet will usually launch the built-in Telnet program. Once those programs are launched, use them to interact with the target and close those programs when you are finished.

Setup - Define Launch Executables

This set of buttons allows you to select either the default program registered on your system or one which you explicitly specify for the designated protocol. To specify a particular program to use for web (HTTP), press the Set HTTP Program button. Navigate to the executable file of the web browser, select it and press Open. To use the default program assigned for opening http addresses, press the Default button. This procedure also applies to FTP and Telnet.

See Also...

TCPTerm
The Lower Button Row

[26] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

[27] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

Name Server Lookup Tab

Overview

The Name Server Lookup tab is designed for making queries to DNS[28] servers. Simple Query allows you to quickly query your default system DNS with hostname[29] or IP address[30] queries. NSLOOKUP provides a fully flexible method of querying any DNS for specific records.You must be able to contact the DNS through your network. A related advanced function is List Domain (also known as Zone Transfer or AXFR).

Information Returned by this Feature

The functions found on this tab can provide information about a host, a domain or a set of IP addresses. The information can be as simple as the mapping between the IP address and the hostname or as complicated as a Zone Transfer of a whole domain.

Help Wizard Topics

- *Using Name Server Lookup to translate the IP Address to a hostname.* Enter the IP Address and press Simple Query.
- *Using Name Server Lookup to test for domain names based on that name.* Example: try appending .com or .net to create a domain name and press NSLOOKUP. Adv Qry Setup should be set to the ANY option.
- *Using Name Server Lookup to find the domain MX system.* See this example.
- *Using Name Server Lookup to find the domain authoritative name servers.* See this example.
- *Using Name Server Lookup to list all systems in the domain.* See this example.
- *Using Name Server Lookup to look for DNS operating system entries.* In Adv Qry Setup, set the Record Query Option to HINFO. Press OK, then enter the host or domain name and press NSLOOKUP.

The Controls in Depth

Who Am I?
Simple Query
Stop[31]
NSLOOKUP
List Domain
Adv Qry Setup
Clear Results[32]
AutoClear[33]

See Also...

NetScanner
The Lower Button Row

---

[28] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.

[29] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

[30] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

[31] The **Stop** button stops or cancels the current activity.

[32] The results area of this tab are cleared when this button is pressed.

[33] AutoClear clears the results area of this tab each time a new function is activated.

Simple Query

About

Simple Query is used to translate the hostname[34] of a computer to an IP address[35] or vice versa using the default DNS[36] assigned to your computer system. The hostname is normally a fully qualified domain name (FQDN), however, if your computer is configured with a default domain name (like yourowndomain.com) search list, non-FQDN names, such as **mail** will also be translated as "mail.yourowndomain.com". NetScanTools calls the Winsock[37] functions which automatically perform the translation.

Information Returned by this Feature

Simple Query returns the hostname, IP Address and any alias hostnames or IP addresses. This assumes that the DNS contains information about the hostname or IP address in question. If you need more advanced information such as an MX record, please see NSLOOKUP.

Example

Enter the name of the host or the IP address (xxx.xxx.xxx.xxx) and press **Simple Query**. The hostname resolution time will vary significantly due to a variety of factors: network connection speed, computer speed, DNS loading etc. If a hostname or IP address is in the **hosts** file located in your Windows directory tree (operating system dependent), the response will be immediate because Winsock normally looks at the hosts file before going to the DNS for name resolution.

```
[fred4.somedomainsomewhere.com]
Translated Name: fred4.somedomainsomewhere.com
IP Address: 10.1.5.2
```

For a hostname to IP address query, the results are typically the hostname in brackets, the translated name, which may be different than the original hostname and a list of IP addresses. Major sites, like www.cnn.com, may have a long list of IP addresses mapped to that hostname.

NetBIOS Machine Name Responses

There are times when you will make a query on an IP address and you will get something back like:

```
[10.1.5.2]
Translated Name: FRED
IP Address: 10.88.5.2
```

This is clearly ***not*** what you expected, ie. **fred4.somedomainsomewhere.com**. What you are seeing is NetBIOS machine name. Upon failure to resolve an IP address in DNS, one of the query actions that Windows makes is to directly contact the computer in question, in this case 10.88.5.2, and use a NetBIOS node status request to ask for the Windows computer name. If it is a Windows 95/98/NT computer without any firewall protections, it will likely answer as above.

IP Address to Hostname Lookups

Obtaining the hostname that is assigned to an IP address is simple, you enter the IP address and press Simple Query. If the IP address has a hostname assigned to it, a response will come back from the DNS containing that host's name. Not every IP address has a corresponding mapping in the DNS. Many times computers operated by businesses will have a computer with an IP address that does not appear in the DNS. This is frequently observed when you run the NetScanner utility.

Comments

You may ask *what good is this feature when you have advanced query around?*. This is a good question that actually does have an answer. Sometimes all you need is a quick name translation and it saves time by NOT having to go to the Advanced Query Setup and configuring the NSLOOKUP to give you an answer. And, it is sometimes not straightforward to determine the current DNS, especially if it has been assigned dynamically.

---

[34] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

[35] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

[36] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.

[37] Winsock is derived from the sockets concepts found in BSD (Berkeley Software Distribution) UNIX. NetScanTools requires Winsock 2 or above for proper operation.

Error Messages
The most common error message is this:

```
Error getting host address:
Valid name format; No hostname or IP data record was found in the Name Server.
```

It appears frequently when you are using Simple Query. This message tells you that DNS could not resolve the hostname to an IP address or vice versa.

See Also...
NSLOOKUP

Who Am I?

About

The **Who Am I** button queries winsock[38] for your computer name, then it uses your winsock computer name to request a hostname to IP address[39] translation from your default DNS[40].

Example

Press the **Who Am I** button. If you are connected to the internet or an internal TCP/IP[41] network with and IP address, you will likely get a message similar to this one:

```
This Computer's Name and IP Address:
Translated Name: myComputer
IP Address: 127.1.2.0
IP Address: 10.1.2.3
Alias: laptop
```

You can have multiple IP addresses assigned to your machine if you have two or more network cards or modems. Each of these will show as above.

Discussion

On Windows 95 operating systems you may get an answer similar to the following one if you are NOT connected to a network:

```
Error getting host address:
Valid name format; No hostname or IP data record was found in the Name Server.
```

Because of the differences in system architecture, Windows NT Winsock will report the name and IP addresses of your computer even if you are not online. If you have configured your NT system with a hostname and static IP address, it will appear if the **Who Am I** button is pressed.

See Also...

NSLOOKUP

[38] Winsock is derived from the sockets concepts found in BSD (Berkeley Software Distribution) UNIX. NetScanTools requires Winsock 2 or above for proper operation.

[39] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

[40] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.

[41] TCP/IP means Transmission Control Protocol--TCP (see RFC 793) over Internet Protocol--IP (see RFC 791).

Adv Qry Setup

Advance Query Setup is used to control the DNS[42] queries generated by the NSLOOKUP and List Domain functions. Simple Query is **not** affected by the settings here. The real power of NSLOOKUP over Simple Query is that you can specify the DNS you wish to use, either by hostname[43] or IP address[44]. This offers you an advantage by allowing you to use NSLOOKUP to compare and check the information about a domain on any accessible DNS servers anywhere in the world.

The setup dialog box is divided into several groups for clarity: Record Query Options, DNS Server Selection, DNS Connection and a set of other options.

Record Query Options
These options define the type of records which are requested when NSLOOKUP is used. These options include record types which are commonly found in most DNS entries: A, CNAME, HINFO, MX, NS, PTR, SOA, any TXT. The ANY record type is a wildcard which asks the server to return whatever it feels is necessary to describe the hostname/domain name in question.

We recommend starting with the ANY option for all hostnames or domain names. We recommend using the A or PTR record query when querying for information about an IP address.

Here is a brief description of the information provided by the most common record query types.

- **A** - The Address record is used to translate an IP address to a host name in the DNS zone. See PTR for mapping an IP address to a host name in the DNS reverse zone.
- **ANY** - This is the recommended type to use for general queries which *do not* involve resolving an IP address to a hostname. Default.
- **CNAME** - Returns the canonical name for a host; also known as the alias.
- **HINFO** - This record provides information about the hardware and software of the target system, if available.
- **MX** - The Mail Exchanger record is one of the most important records contained in DNS. This option provides a list of mail exchange servers (those running the SMTP service) assigned for that domain.
- **NS** - The Name Server record provides a list of DNS servers for the domain. Both Authoritative and Non-Authoritative Name Servers are normally reported.
- **PTR** - The pointer record is used to translate an IP address to a host name in the DNS reverse zone (in-addr.arpa DNS domain). See also the A record.
- **SOA** - The Start Of Authority record provides information about the DNS name server responsible for that domain. It is the first record in a set of DNS entries.
- **TXT** - A textual, descriptive entry.

DNS Server Selection

- The Current Server may be a hostname or IP Address. You may clear the list of servers by pressing the C button to the right of the entry area. This server must be accessible to your system.
- The Root Servers are a list of servers which are the controlling servers for the whole internet. A root server hostname must end with a period (.).

DNS Connection

- The Timeout entry is the number of seconds that NetScanTools's resolver will wait for a response from the current or root server. For nearby, fast servers, 5 seconds should be adequate. For server located many hops away, 15 seconds may be more appropriate.
- The Retries entry is the number of times that NetScanTools will resend the query. Default is 1.

Other Options

Append Default Domain Name. When checked, this option will append the default domain name as defined in your TCP/IP network settings to any non-fully qualified hostnames entered in the target field. A fully qualified hostname would be

---

[42] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.

[43] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

[44] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

mail.netscantools.com. A non-fully qualified hostname would be just the word mail. Default is checked.

Use Recursion. When checked, this option directs NetScanTools resolver to ask that query answers be made recursively. Default is checked.

Use Virtual Circuit (TCP). When checked, this option directs the NetScanTools resolver to make a TCP connection to the DNS rather than the standard UDP query. This applies to all queries except AXFR Zone Transfers. Zone Transfers are required to be TCP. Default is unchecked.

Keep TCP Connection Alive. When checked, this option keeps TCP connections to DNS open for faster query response. This option requires the Use Virtual Circuit option to be checked.

No Debug, 1, 2. These are debug levels which control how verbose the resolver is when reporting information back to NetScanTools. Default is No Debug.

Comments

- List Domain (Zone Transfer) uses the 'ANY' AXFR filtering.
- NetScanTools uses the Internet Class Option for all NSLOOKUP and List Domain Queries.
- **About Timeouts and Retries**. These entries control the amount of time to wait for the DNS to respond to your queries. The timeout field is in increments of seconds and starts when either the Adv Query or List Domain buttons are pressed. Another related control is the retries field. *Retries* controls the number of times NetScanTools retries or resends your query. Since these fields are related, they have a profound effect on each other. If you set the timeout for 10 seconds and the retries at 3, you will have a maximum of 30 seconds for a DNS query to be resolved in three ten second blocks.
- **Unsupported Records in DNS.** If the DNS does not support the record query you are requesting, it will either timeout and not return any information or return the SOA record in an attempt to direct you to the Start of Authority name server for that domain.
- If you are not currently connected to the Internet or an Intranet when you press the Adv Query button, or NetScanTools is unable to identify your default DNS, you will get a message like this one:

```
Setting up resolver with this name server.
*** Default servers could not be identified or are unavailable.
*** At a Windows NT command line type:
ipconfig /ALL to get the IP addresses of DNS servers used by your computer
*** On a Windows 95 computer:
locate and run winipcfg.exe to get the IP addresses of DNS servers used by your computer
*** Then use "A Q Setup" to specify a Name Server's name or IP address.
```

  This message means that you need to supply an IP address (preferred) or hostname of your default DNS in A Q Setup. Since you may not know the IP address of your default DNS, Windows 95/98 and NT all have built-in utilities for getting this information.

- **How to get your default DNS IP address.** Activate your network connection; once connected do one of the following:

  On Windows NT, type the command *ipconfig /ALL* in a DOS window command line.
  On Windows 95/98 type *winipcfg* in a DOS window or run winipcfg.exe using explorer. Press *More Info* and look for the DNS server box.

  Both utilities will supply the default DNS if you have an active network connection.

See Also...
List Domain
NSLOOKUP

List Domain

About

The List Domain feature is exact equivalent of the LS option in UNIX NSLOOKUP. It is also known as the AXFR Zone Transfer. It operates by making a TCP connection to the DNS[45] and requesting information about the complete zone. The purpose of a Zone Transfer is to update other DNS about the domain. NetScanTools List Domain uses the ANY option (not to be confused with the Record Query Options ANY option in Adv Qry Setup). The ANY option normally gives a complete listing of most of the records for each host in the domain.

Usage

To use List Domain, you must first identify the Authoritative Hosts for the domain you are interested in, then set the Current Server to one of those Authoritative Hosts and then use List Domain. Only Authoritative Hosts have domain lists, so it is important to set the current server to the proper host.

Example

Following these steps **may lead to a complete domain listing:

I. Determine the domain name. *Be sure to exclude the host name*. www.nwpsw.com is a hostname. nwpsw.com is a domain name.
II. Go to A Q Setup, select these options: ANY Query type, timeout=15, retries=1, Current Server= <your favorite fast DNS goes here>, Append default domain name can be uncheck though it is not required, Use Recursion is checked, and all other options are unchecked.
III. Close A Q Setup (this may take a minute while the IP address of your selected DNS is determined)
IV. Enter the domain name and press Adv Query.
V. If the domain name can be resolved by your DNS, you should get a response containing the names and IP addresses of the Authoritative Name Servers and possibly the Non-Authoritative Name Servers.
VI. **Optional:** Press the copy button to copy the full text of the results to the clipboard, open Notepad or equivalent, then paste the DNS info into the Notepad document for reference. You may need to try each of the Authoritative Name Servers in turn.
VII. Use your cursor to highlight, then right-click to bring up the copy popup menu and then copy one the Authoritative Hosts.
VIII. Paste the Authoritative Host's name into the Current Server edit box in A Q Setup (use ctrl-v or ctrl-insert).
IX. Close A Q Setup, enter the domain name if it was changed and press List Domain.

**There are times when the Authoritative Hosts will refuse to give domain listing information to just any IP address (like yours). You may have to try every listed Authoritative and Non-Authoritative Host and even then, you may not get information.

Here are the results for nwpsw.com:

First, the Adv Query results which give the Authoritative Server List at the bottom. The ANY option was selected.

```
Looking up [nwpsw.com]

Server:  DNS1.PRIMENET.NET
Address:  206.165.5.10

Non-authoritative answer:
nwpsw.com  nameserver = DNS1.simplenet.com
nwpsw.com  nameserver = DNS2.simplenet.com
nwpsw.com  nameserver = DNS3.simplenet.com
nwpsw.com
    origin = DNS1.simplenet.com
    mail addr = postmaster.simplenet.com
    serial = 1114207651
    refresh = 10800(3 hours)
    retry   = 3600(1 hour)
    expire  = 5184000(60 days)
    minimum ttl = 86400(1 day)

Authoritative answers can be found from:
nwpsw.com  nameserver = DNS1.simplenet.com
nwpsw.com  nameserver = DNS2.simplenet.com
nwpsw.com  nameserver = DNS3.simplenet.com
DNS1.simplenet.com internet address = 207.67.128.2
```

[45] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.


```
DNS2.simplenet.com internet address = 207.67.128.3
DNS3.simplenet.com internet address = 207.137.72.4

[End Query]
```

Choosing the Authoritative DNS.
The SOA record has an entry called origin. It is the primary DNS responsible for mapping this domain, so we will use it for the Current Server setting in A Q setup. In the previous listing, the other two nameservers are mirrors. Here are the results of the List Domain using the origin DNS:

```
Listing domain [nwpsw.com]

Server: DNS1.simplenet.com
Host or domain name            Resource Record Info.
 nwpsw.com.                     SOA   DNS1.simplenet.com postmaster.simplenet.com.
(1114207651 10800 3600 5184000 86400)
 nwpsw.com.                     NS    DNS1.simplenet.com
 nwpsw.com.                     NS    DNS2.simplenet.com
 nwpsw.com.                     NS    DNS3.simplenet.com
 nwpsw.com.                     MX    8    mail.nwpsw.com
 nwpsw.com.                     A     207.137.171.253
 mail                           CNAME mail1.simplenet.com
 ftp                            MX    8    mail.nwpsw.com
 ftp                            A     207.137.171.253
 www                            MX    8    mail.nwpsw.com
 www                            A     207.137.171.253
 nwpsw.com.                     SOA   DNS1.simplenet.com postmaster.simplenet.com.
(1114207651 10800 3600 5184000 86400)
Received 12 records.

[End Query]
```

What can we learn from this query?

Much. This is a very simple domain mapping with actually only two computers involved. One is used for email and the other is aliases or mapped with the same IP address for the domain names nwpsw.com, www.nwpsw.com and ftp.nwpsw.com. *Aliases* or CNAMEs map hostnames to another host or IP address. As you can see in the example, www.nwpsw.com actually has the same IP address as ftp.nwpsw.com. The first record for a domain in a DNS is the SOA record and it appears at the top. The NS records are next showing all the Authoritative Nameservers for the domain. What follows is a list of aliased computer names with corresponding IP addresses. The MX records show the name of the computer responsible for exchanging mail coming to the base domain, nwpsw.com.

Major Internet Service Providers and large companies without firewalls will often have several hundred to several thousand records in their DNS for a single domain. It is not possible to tell the size of a domain listing prior to beginning the Zone Transfer list of the domain.

And then there are other times...

Sometimes a DNS will not give you the information you expect. This is particularly true if you are not using an Authoritative Server for the domain or the Authoritative Server is configured to refuse this type of query, then you will get a somewhat useless response like the one below:

```
Listing domain [atestdomain.com]

Server: DNS1.simplenet.com
Host or domain name            Resource Record Info.
Received 0 records.

[End Query]
```

In the above listing, the DNS used for the current server is not an Authoritative Nameserver for the domain we are requesting information about. To get the information you want, you have to go through the process of locating the list of Authoritative Nameservers for that domain, then proceed from there using the steps covered in this section.

Security Issues.
Many network administrators now use a list of allowed IP addresses when determining which systems get response to a Zone Transfer request.

See Also...

NSLOOKUP
Simple Query

NetBIOS Info Tab

About

The NetBIOS Info tab provides information about NetBIOS[46] protocol network shares and LANA[47] adapters, both local and remote. NetBIOS is defined in RFCs 1001 and 1002, which are accessible from the RFC button on the NetBIOS Info Tab. The NetBIOS protocol operates independent of the TCP/IP[48] protocol but it can also operate as NetBIOS over TCP[49], NBT.

Information Returned by this Feature

The Shared Network Resources Information display lists the NetBIOS protocol networks, and the computers located on the network along with any shared devices or directories. The NetBIOS LANA information display lists the LANA number, MAC address[50], Max Datagram and Max Session Packet size for each LANA.

The NetBIOS Tab Controls

- **Refresh** - when pressed, this refreshes the information in both display windows.
- **Stop**[51] button - This button is used to stop any current Ping activity and to stop AutoPing.
- The Clear Results[52] button clears the results display.
- The AutoSize[53] button sizes the columns the results display to match the longest text string in each column.

Results Formatting

Results are displayed in spreadsheet format with user variable column widths. To change the column width, move your cursor over the heading bar to the vertical lines separating each column, press the mouse button and drag to the desired width. Columns can also be autoformatted to the longest string length by double-clicking on the column header separator to the right of the column. Columns can be automatically size to the longest length of the text in the column by pressing the AutoSize button.

The Results Display Columns - Shared Network Resources Information

Remote Name - This is the name of the network, domain, server or shared print device/drive/directory.
Comment - This is the comment field text that is set when the share is defined.
Type - One of either Network, Domain, Server or Share.
Local Name - the name of a local device if device is connected or remembered. This will normally be (null).
Network Provider - the name of the network provider owning this resource. This will normally be Microsoft Windows Network.

The Results Display Columns - NetBIOS Interface Information

LANA or System - This is number of the LAN Adapter found on your computer -or- the remote server name as shown in the Share Network Resources Information table.
MAC Address - This is the Media Access Control address of the interface whether a local LANA device or a remote interface on another computer.
Adapter Type - This is normally Ethernet, although it can be Token Ring or Unknown.
NetBIOS Revision - The revision of the underlying NetBIOS transport protocol layer.
Max Datagram - The maximum size of a datagram packet. Normally at least 512 bytes. This will be zero for remote interfaces.
Max Session Packet Size - The maximum size of a session data packet. This will be zero for remote interfaces.

See Also...

The Lower Button Row

---

[46] **N**etwork **B**asic **I**nput **O**utput **S**ystem - this is an application program interface which is used by software programs to communicate over a local area network.

[47] **L**ocal **A**rea **N**etwork **A**dapter -- see NetBIOS Info tab.

[48] TCP/IP means Transmission Control Protocol--TCP (see RFC 793) over Internet Protocol--IP (see RFC 791).

[49] TCP means transmission control protocol as defined in RFC 793. It is intended to provide a highly reliable method of assuring delivery of packets between network connected computer systems and uses IP as a next level lower protocol layer.

[50] **M**edia **A**ccess **C**ontrol Address is a 48 bit binary number used as a physical address which is theoretically unique for every network card manufactured. It is used by the ARP protocol to map an IP address to a MAC address.

[51] The **Stop** button stops or cancels the current activity.

[52] The results area of this tab are cleared when this button is pressed.

[53] The AutoSize button causes all columns in a report style list view to be sized to the widest text string found in the column.

NetScanner Tab

About

The NetScanner tab is one of the most powerful and popular features in NetScanTools. NetScanner sweeps a sequential IP address range and pings every IP address in that range of IP addresses. It will optionally translate the responding IP addresses[54] to hostnames[55], or run a whois query on the responding domain name or IP address. One of the most useful purposes for this tool is locating active computers on a subnet.

How it works

NetScanner is multi threaded meaning several IP addresses are targeted simultaneously. NetScanner works by sending an ICMP[56] echo request (Ping) packet to the currently selected IP address. It waits for the timeout period and looks for a returning ICMP echo reply packet. It makes other requests depending on the types of data you have asked for.

Help Wizard Topics

- *Using NetScanner to Ping the surrounding IP Address range.* Enter the target start IP Address and end IP Address of a range, then press Start. Any responding systems will show up in the list.
- *Using NetScanner to Ping the IP Address range assigned to a domain.* First try listing the domain. Now observe the IP addresses shown in the domain listing to find out the range spanned by the domain. You can also take the IP address of the web server in the domain and query Whois with the IP address to establish the range of IP address assigned to the domain. Once you have the range, enter it and press Start.

Setup

NetScanner Setup allows you to control several parameters of the ICMP Echo Request packet.

Configuring

Since NetScanner is capable of doing a variety of functions during a network sweep, you must decide on what you need from the sweep. As a minimum, NetScanTools requires a **starting and ending IP address** before a scan can be attempted. The ending IP address must be numerically greater than the starting IP address because NetScanTools increments through the range of IP addresses one IP address at a time. You are not limited to a subnet. Enter the IP addresses in the appropriate entry fields; note that they must be fully defined with no wildcard characters accepted: 127.0.0.1 etc.

Define the Ping packet parameters using the Setup dialog.

The **Whois** section allows you to query a whois server for the domain information regarding a responding IP address. The whois information that is retrieved is stored in text files on your hard drive. The whois response files are named somedomain.com.nsw; they have the .nsw extension. There are two selections in this group and one Whois Setup button:

- **Enable Whois Queries** - when checked, the domain name, if present, or IP address will be routed to the whois query engine for resolution. Default is unchecked.
- **Enable Smart Whois** - when checked, the whois query engine will automatically use the Smart Whois processor to determine which whois server to use. Default is checked and we recommend you leave it this way. WARNING: This checkbox also affects the same setting on the Whois tab.
- **Whois Setup** - this button activates the Whois setup dialog box. WARNING: Changes made here also affect the settings on the Whois tab.

If a whois query for a particular domain has previously been completed and stored on your hard drive, the same query will not be made again until the Clear Results button has been pressed AND you have allowed deleting the whois files.

Additional Options. On the right side under the column of buttons, you will find four checkboxes:

- **Translate IPs to Hostnames** - when checked, this instructs NetScanner to translate the IP addresses of the target hosts to hostnames.
- **Add Responding IPs to HOSTS file** - when checked, responding IP addresses with corresponding hostnames will be added to your hosts file for rapid name resolution. If you wish to edit the hosts file, press the **Edit Hosts File** button.

Once all these setup parameters have been defined, you are ready to proceed with a sweep.

---

[54] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

[55] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

[56] **I**nternet **C**ontrol **M**essage **P**rotocol - assists in determining when packet transmission errors have occurred.

Scanning a range of IP addresses
To begin your sweep, simply press the **Start** button. The sweep will commence using the parameters you set. As the sweep proceeds, you will see the target column filled first followed by the other columns as data becomes available.

Interpreting Results
Once a sweep is complete, you will see fields with data and some fields with N/R meaning No Response and some fields with a '-' symbol, meaning skipped. You can press the **AutoSize** button so that the column widths will match the data field lengths.

The Results Columns. The column labeled **Target IP** contains the IP Address of each host that was targeted. The column labeled **Hostname** contains the translated hostname for that IP address. This may be of the form somedomain.com as returned by DNS[57] or it may be an all capitalized NetBIOS machine name. The next column is labeled **Ping.** This column shows the ICMP response numeric type:code followed by an interpretive message or it shows an N/R for no response. The **Time** column contains the round trip time for the ping packet or the N/R message for no response. The **WHOIS** column displays whether or not data exists for the domain or IP address of the target host. A 'Y' symbol appears if the whois query was successful; if not, then N/R appears. If WHOIS queries are not enable, the dash symbol '-' will appear. The **Responding IP** column shows the IP address of the host that actually responded to the PING packet. Usually, this will be the same as the leftmost column, but if the host is not accessible due to a routing problem, the IP address of the responding computer will appear in this column.

Double Clicking. After a sweep is complete, you can double click on any row for a detailed report of the data shown in the column view. The report is presented in the Data Viewer[58] window as in this sample below:

```
Report on IP Address: 10.4.1.1, Hostname: P2000

Ping Packet Round Trip Time: 1 milliseconds
Responding IP Address: 10.4.1.1
************************************************

*******************
*    Whois Data    *
*******************

WHOIS data unavailable for NetBIOS machine names.

End of Report.
```

Edit Hosts File

Since the NetScanner tab has the ability to add the responding IP address/hostname pairs to the hosts file, we have included a hosts file[59] editor. Press the **Edit Hosts File** button to activate this simple text editor.

Your hosts file is found in the C:\windows directory on Windows 95/98 or in the C:\winNT\system32\drivers\etc directory on Windows NT. This text file has no file extension. DO NOT confuse it with hosts.sam which is the sample hosts file.

Some things to remember when you edit a hosts file:
- Comments are created by inserting the pound character '#' anywhere on a line. All text to the right of the # symbol is a comment.
- The IP address should begin in the first column of each line.
- Each entry is kept on an individual line.

[57] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.

[58] The Data Viewer window is used to display text. You can copy text from Data Viewer by highlighting and right-clicking to bring up the edit menu. You can also locate and find any text (not case sensitive) using the Find and Find Again buttons. You can print or save the data to a file.

The Data Viewer window is use frequently throughout NetScanTools to display text from special display elements like listviews and treeviews.

[59] A hosts file is used on a local computer to rapidly resolve the name of a host or an IP address without necessitating the need to query a DNS. Winsock normally looks for and scans a hosts file prior to communicating with DNS.

- The alias names follow the IP address separated by at least one white space character.

When you have completed editing your hosts file, press OK to save the changes.

See Also...
NetBIOS Info
Ping
TraceRoute
The Lower Button Row

NetScanner Setup

NetScanner Ping packet parameters are controlled using the NetScanner Setup dialog. After pressing the Setup button, you will see a dialog box nearly identical to the Ping setup dialog. You can control the packet timeout, the maximum life in hops (TTL=time-to-live), the base packet length, retries and fragmentation of the packet. Normally you will want to allow fragmentation and you may need to experiment with the values in this dialog. Slow networks will require different values than fast networks.

NetScanner Setup Parameters

NetScanTools allows you to vary several PING packet parameters.

The Packet Transmission Control Group

- **Packet Timeout** - this value, measured in milliseconds, defines the time each Ping thread will wait after sending out the ICMP Echo Request packet for the ICMP Echo Reply packet to come back from the target. Default is 3000 ms or 3 seconds.
- **Retries** - one packet is sent per IP address. Retries controls the number of additional packets sent. Default is 1.

The Packet Header Control Group

- **Packet Time To Live** - this is also known as TTL. It controls the time the packet will live on the internet in seconds. This is also the maximum number of hops or computers that the packet is allowed to pass through. Default is 64.
- **Don't Fragment Packets** - if checked, packets that exceed the MTU along the complete path to the target will not be delivered. If unchecked, packets exceeding the MTU will be fragmented and reassembled at the target. Default is unchecked.

Packet Data Definition

- **Packet Data Length** - this is the payload part of the ICMP Echo Request packet. You can specify any value between 8 and 16384 bytes. The first 8 bytes are reserved for timestamp purposes. Default is 16.

Ping Tab

About Ping

Ping originated as UNIX program. Ping uses a short burst of byte packets to elicit a response from a remote computer. It is used to determine connectivity between two networked computer systems.

Information Returned by this Feature

Ping provides information about the connectivity between your computer and another networked computer. It does this by sending an ICMP[60] (see RFC 792) Echo Request Packet (ICMP type 8) to the target host. If the target host receives the packet, it should respond with an ICMP Echo Reply Packet (ICMP type 0)--however, some computers deliberately block the return of Echo Reply Packets. By observing the round trip time for the ping packets, you can make some judgments about the quality of the route between your computer and the target host.

Help Wizard Topics

- *Using Ping to determine connectivity.* Enter the target IP Address or hostname and press Ping. If the status field shows 0:0 Echo Reply, you can contact the target.

Setup

To activate setup, press the Setup button.

Target Hostname or IP Address

You must enter a hostname[61] like www.netscantools.com or an IP address[62] like 10.2.3.4.

The Ping Tab Controls

The controls most essential to the basic operation of Ping are:

- **Ping** button - This button initiates a ping sequence.
- **Stop**[63] button - This button is used to stop any current Ping activity and to stop AutoPing.
- **Setup** button - This button activates the Setup Dialog.
- The Clear Results[64] button clears the results display.
- The AutoSize[65] button sizes the columns the results display to match the longest text string in each column.

The **Resolve IP Addresses to Host Names** checkbox, when checked, forces an IP address to be translated to it's corresponding hostname, if any. The result of the IP to hostname translation is shown in the lower status window along with the IP address. Ping will operate faster if the box is not checked because it does not have to ask for an IP address to hostname translation.

The **AutoPing** button activates the AutoPing sequencer which pings a specific IP address periodically according to the information provided in the Setup Dialog Box. To learn more about AutoPing, click here.

Results Formatting

Results are displayed in spreadsheet format with user variable column widths. To change the column width, move your cursor over the heading bar to the vertical lines separating each column, press the mouse button and drag to the desired width. Columns can also be autoformatted to the longest string length by double-clicking on the column header separator to the right of the column. Columns can be automatically size to the longest length of the text in the column by pressing the AutoSize button.

The Results Display Columns

- The **Ping Column** shows the ping packet number.
- The **Target Column** shows the IP address of the target system.

---

[60] **I**nternet **C**ontrol **M**essage **P**rotocol - assists in determining when packet transmission errors have occurred.

[61] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

[62] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

[63] The **Stop** button stops or cancels the current activity.

[64] The results area of this tab are cleared when this button is pressed.

[65] The AutoSize button causes all columns in a report style list view to be sized to the widest text string found in the column.

- The **Bytes Column** shows the size in 8 bit bytes of the data portion of the ICMP echo request packet sent to the target system..
- The **Time Column** displays the round trip time in milliseconds. This is the time it takes for a packet to be sent to us in response to a packet we sent. If you use the Winsock[66] 2 setting on the TTL compatibility section of the Preferences tab, you will get 1 millisecond resolution timing. The Automatic setting will result in approximately 10 millisecond resolution timing.
- The **TTL Column** displays the Time-To-Live value of the received ICMP packet..
- The **Status Column** shows the type of ICMP packet received in response to our ICMP packets. Type 0 is returned under normal circumstances. You will occasionally see other ICMP packet types reported. These are usually host or net unreachable or even source quench.

Right Click Menus
After a Ping sequence is complete, you can right click with your mouse in the results area to bring up a menu. This menu contains the following options:

- **Traceroute to Selected IP** - this takes the IP address found in the Target column and activates the Traceroute tab to traceroute to that IP address.
- **Display Ping Time Graph** - this activates the NST Graphing program using the data from the current Ping. It will show a graph (printable) much like the example here.

Comments
Ping also supports Path MTU Discovery per RFC 1191. If you have the Don't Fragment bit set by checking the box in Setup, and you attempt to Ping a host with an MTU larger than the routers can handle, the router will often send back an ICMP Destination Unreachable/Fragmentation Needed packet. This packet will have the low-order 16 bits of the ICMP header set to the MTU that is allowed for transmission of the packet to the next hop. If the MTU is non-zero, the status column will display the MTU needed.

See Also...
Echo
ICMP Packet Types
NetScanner
TraceRoute
The Lower Button Row

[66] Winsock is derived from the sockets concepts found in BSD (Berkeley Software Distribution) UNIX. NetScanTools requires Winsock 2 or above for proper operation.

Ping Tab Setup

PING Setup Parameters

NetScanTools allows you to vary several PING packet parameters. Normally you will want to allow fragmentation and you may need to experiment with the values in this dialog. Slow networks will require different values than fast networks.

The Packet Transmission Control Group

- **Time Between Packets** - this value, measured in milliseconds, defines the time NetScanTools waits between launching each separate Ping thread. Default is 200.
- **Packet Timeout** - this value, measured in milliseconds, defines the time each Ping thread will wait after sending out the ICMP Echo Request packet for the ICMP Echo Reply packet to come back from the target. Default is 3000 ms or 3 seconds.
- **Number of Packets Sent** - the number of packets sent. Default is 5.

The Packet Header Control Group

- **Packet Time To Live** - this is also known as TTL. It controls the time the packet will live on the internet in seconds. This is also the maximum number of hops or computers that the packet is allowed to pass through. Default is 64.
- **Don't Fragment Packets** - if checked, packets that exceed the MTU along the complete path to the target will not be delivered. If unchecked, packets exceeding the MTU will be fragmented and reassembled at the target. Default is unchecked.

Packet Data Definition

- **Packet Data Length** - this is the payload part of the ICMP Echo Request packet. You can specify any value between 8 and 16384 bytes. The first 8 bytes are reserved for timestamp purposes. Default is 32.

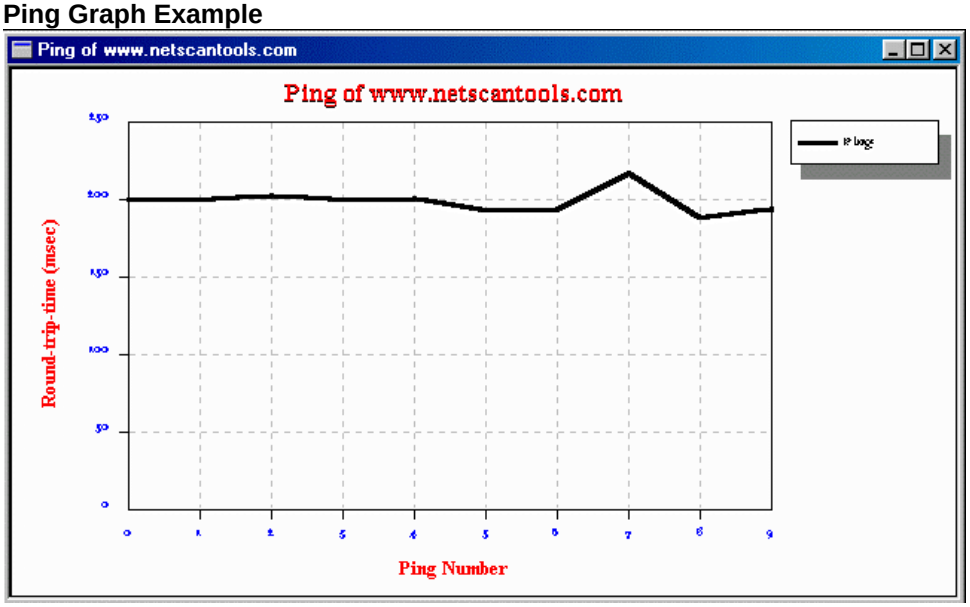
AutoPing Settings

- **Threshold % Non-Responding Pings** - when using AutoPing, if the number of non-responding pings exceeds this percentage of the number of packets sent, your machine will beep twice and an error entry will be logged in the AutoPing log. Default is 50.
- **Time Between Ping Sets (sec)** - the number of seconds between sets of ping packets. Note that after activating AutoPing, the first set of packets will be sent *after* this amount of time has past. Default is 30.
- **Log All Data** - when checked, all ping sequences and results are added to the log file. Default is unchecked.
- **Edit AutoPing Log** - this activates a text editor for working with the log file.

See Also...

NetScanner
Ping

Ping Graph Example



Port Probe Tab

About

Port Probe is an active scanning feature designed to determine which ports on a target computer are active and being used by services[67] or daemons. Port Probing is useful in determining what type of operating system and vulnerabilities a target host might have. Use it to test the response of scanning detection alarm programs. Because this feature can be used maliciously, we have included a warning dialog which is presented when you start a probe.

Information Returned by this Feature

Port Probe is capable of reliably identifying TCP[68] services. Since TCP allows a full connection, we can be sure that a service exists if a connection is made. Port Probe collects the banners or other returned data of any responding services.

The results are displayed in a tree-like view with color-coded icons and double-click drilldown to view the data returned when the connection was made.

Help Wizard Topics

- *Using Port Probe to test the target for services/daemons.* Enter the target IP Address, define a range of port numbers, then press Start. Any responding TCP ports will show up in the list. Once the scan is complete, double click on any entries with the 'D' in the green circle to view the data returned from the port. For a list of port numbers, see the Database Tests tab and press View Services Database.
- *Using Port Probe to test a port number for activity.* Enter the target IP Address, enter the port number in both the start and end port, then press Start. Any responding TCP port activity will show up in the list. Once the scan is complete, double click on any entries with the 'D' in the green circle to view the data returned from the port. For a list of port numbers, see the Database Tests tab and press View Services Database.
- *Using Port Probe to determine SMTP or FTP server type.* Enter the target IP Address, enter the port number (25 for SMTP, 21 for FTP) in both the start and end port, set the Wait After Connect value to 5000, then press Start. Any responding TCP port activity will show up in the list. Once the scan is complete, double click on any entries with the 'D' in the green circle to view the data returned from the port. For a list of port numbers, see the Database Tests tab and press View Services Database.

Setup

Since many of Port Probe setup parameters are changed frequently during use, the majority of the parameters can be changed on the main Port Probe tab. The following are explanations of each control in order of appearance and how they are used:

Host Range Radio Buttons

- **Probe Single Host** - this selection allows you to enter a single IP address of hostname in the edit box provided and probe it using Seq Probe.
- **Probe IP Range** - this selection allows you to enter a range of IP addresses in the edit boxes provided and probe each of them using Seq Probe.

Target IP Address Range Definition

- **Target Host Name or Start IP Address** - this entry field accepts either an IP address[69] or a hostname[70] depending on the Probe Single Host/Probe IP Range selection. This entry area has a 'C' button for clearing previous entries to the right of the entry area.
- **End IP Address** - this is the ending IP address. It must be numerically greater than the starting IP address. This entry area has a 'C' button for clearing previous entries to the right of the entry area.

Results Display Control Checkboxes

- **AutoClear** - when checked, the results tree is cleared as each function button is pressed. Default is checked.
- **Show non-responding ports** - when checked, all ports scanned are shown whether they respond or not--warning, this can be quite a few ports depending on the settings you choose. When unchecked, only the responding ports are displayed. Default is unchecked.

---

[67] A service or daemon is a program that listens for incoming connections on a TCP/IP port and responds accordingly. Examples are web servers or mail services like SMTP.

[68] TCP means transmission control protocol as defined in RFC 793. It is intended to provide a highly reliable method of assuring delivery of packets between network connected computer systems and uses IP as a next level lower protocol layer.

[69] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

[70] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

Port Range Definition
- **Start Port** - this entry area is the starting port. It may be any number between 1 and 65535. Default is 1.
- **End Port** - this entry area is the ending port. It may be and number between 1 and 65535 and it must be numerically greater than the start port number. Default is 256.

Connection Definition
- **Connection Timeout (ms)** - this number, in milliseconds (1000 ms = 1 second), defines how long each port probe thread waits for a connection to be established. Default is 3000.
- **Wait After Connect (ms)** - this number, in milliseconds, defines how long after a connection is made for data to be received from the connected port. Default is 3000.

Target Loading
- **Probe Delay (ms)** - this is the delay time between launching each port probe thread in milliseconds (1000 ms = 1 second). Each TCP port is tested per machine in a single thread. Default is 0. Use a value here if the prober runs too fast for the target machine to respond.

Action Buttons
Port Probe operates in one mode:

- **Sequential Probe.** This mode probes either a single host or a range of IP addresses based on the selection made in the Probe Single Host/Probe IP Range radio button group. It probes each host sequentially, that is the first, then the second etc., over the complete range of port numbers shown in the Starting and Ending Port entry areas.

Using Port Probe
Setup the parameters as described above and press Seq Probe. The icon images to the left of the port numbers indicate the confidence of the connection we made and they also indicate whether any data was received after making the connection.

Image Key
The image key on the tab has tooltips. Hold your cursor over each image in the key to get a brief explanation of the meaning of the image.

From left to right, the images are:
- A node or computer.
- A confirmed TCP connection.
- A confirmed TCP connection with data received from the port.
- An unused target port. The TCP connection was rejected.
- No response. This last image means that we received no communication back from the target host. It may be offline or it does not exist.

Viewing the Data from a Port
If you have a port with the image of a green circle with a question mark in it, there was data received from the target port. To view the data, double-click on the image. Data Viewer[71] will appear showing the text.

Example 1 - Connection to a Chargen server port.
Example 2 - Connection to an ftp port. Note that you can see what kind of ftp server they are using.

See Also...
Database Tests
NetScanner
Ping
The Lower Button Row

[71]The Data Viewer window is used to display text. You can copy text from Data Viewer by highlighting and right-clicking to bring up the edit menu. You can also locate and find any text (not case sensitive) using the Find and Find Again buttons. You can print or save the data to a file.

The Data Viewer window is use frequently throughout NetScanTools to display text from special display elements like listviews and treeviews.

Preferences Tab

About

Use the Preferences tab to set user preferences and control the general operation of the program.

How to Use the Preferences Tab

Each of the groups in this tab work independently of each other.

- **Font Settings - Results Display and Printouts Group.** Change the font used to display the results data and all of the printouts here. The name of the currently selected font and its size appear in the window. Press the **Change Font** button to activate the standard font selection dialog box. We recommend using Courier New, 9 point. You may choose any font installed on your system. For best results, use TrueType fonts.

- **Ping, TraceRoute, NetScanner TTL Compatibility Group.** The Automatic setting is the default and it normally defaults to using the operating system's ICMP DLL for transmitting and receiving ICMP packets. The Winsock 2 setting is *recommended* for Windows 2000, NT 4, ME, 98 and 95 (only if 95 is using Winsock 2 update).

- **Appearance Group.** This group allows you to control whether the program is minimized to the taskbar or the taskbar tray. Unchecked is the default for Minimize to Taskbar Tray. The Tab Ordering and Enabling button activates the Tab Order Editor. Click here to learn how to use the editor.

- **Email Results Button Protocol.** The MAPI selection directs all email resulting from pressing the Email Results button to go to the Windows Messaging subsystem using the **M**essaging **API**. MAPI is the default. To view the MAPI protocol as it appears on Windows NT 4, click here. The other selection is SMTP[72]. The SMTP directs all email resulting from pressing the Email Results button to use the Simple Mail Transfer Protocol to talk directly with a SMTP mail server. Learn more about the SMTP Email Results procedure here.

See Also...

NetScanner
NSLOOKUP
Ping
TraceRoute
The Lower Button Row

[72] SMTP - **S**imple **M**ail **T**ransfer **P**rotocol. For more information, see RFC 821.

Tab Order Editor

About

The Tab Order Editor is launched from the Appearance Group of the Preferences tab. It is used to define the order of appearance of tabs. It can also remove infrequently used tabs from the program.

As with most of the editors used in NetScanTools, you have a list of items that can be controlled by a set of buttons. The Current Visible Tab Order is shown on the left. It is a list of how the tabs now appear with the first visible tab shown at the top.

To move a tab up or down in the list, select it so that it is highlighted, then use the Up/Down buttons to move it.

To move a tab to the Tabs Not Visible list, highlight it in the Current Visible Tab Order list, then press the >> button to move it. Reverse the process to move a tab to the Current Visible Tab Order list from the Tabs Not Visible list.

NOTE: Changes you make to the tab order are NOT EFFECTIVE until NetScanTools is RESTARTED.

Quote Tab

About

This client function retrieves the 'quote of the day' from a target host per RFC 865. This is also known as QOTD or Cookie. The quotes are short sayings or messages which are usually randomly selected and therefore different for each client connection.

Information Returned by this Feature

If you get a quote, you know that you can connect to this computer and it appears that this service is operational.

Help Wizard Topics

- *Using Quote to determine connectivity and probable system type.* Enter the IP Address or hostname and press Connect. If the target is running a quote server, you will see a response. If the target refuses your connection, you will see it in the response area. A refusal would mean that you can contact the host. This only works with TCP, UDP does not show refusals. System type can be judged from the type of quote you get back to a certain degree--not guaranteed. Windows NT systems will have quotes mostly from Charles Dickens and George Bernard Shaw--unless the system owner has changed them.

Using Quote

Enter a target hostname or IP address and press the Quote button. If the target host is running a Quote Server, you will see a TCP[73] connection being established and NetScanTools will display a quote from the target host's server.

There is no set format for the quote messages. The RFC limits the text returned to a maximum length of 512 bytes.

Quote of the Day is one of the 'Simple TCP/IP Services' optionally installed on Windows NT. The Simple TCP/IP Services are Chargen, Daytime, Discard, Echo and Quote.

Error Messages

The two most common error messages you will see are shown below.

```
Error getting host address:
Valid name format; No hostname or IP data record was found in the Name Server.
```

or

```
Error connecting to host:
The attempt to connect was refused.
```

The first error message means that the hostname requested could not be resolved to an IP address and the second error message means that the target host is either not running a Quote Server, or it refused you access to a working Quote Server using IP address accept/reject lists.

See Also...

Character Generator Client
Daytime
Echo
The Lower Button Row

[73] TCP means transmission control protocol as defined in RFC 793. It is intended to provide a highly reliable method of assuring delivery of packets between network connected computer systems and uses IP as a next level lower protocol layer.

TCP Term Tab

About

TCP Term is a simple general purpose TCP protocol communication client that operates much like Telnet. TCP Term uses the Telnet protocol to exchange handshaking bytes between the client and server when the connection is made (However, TCP Term is not intended to be a full telnet program replacement, use it for simple text based communications via TCP protocol). You can use TCP term as a general purpose testing tool. One very good use is to connect to a mail server and verify a user. It can be used with most any service as a diagnostic tool, provided the target service can operate using ASCII text communication.

Help Wizard Topics

- *Using TCP Term to connect to a port on the target.* Enter the IP Address or hostname, enter the port number or port name and press Connect. If the target is running a server on that port, you will see a response. If the target refuses your connection, you will see it in the response area.
- *Using TCP Term to determine probable system type.* Enter the IP Address or hostname, enter the port number or port name of services like SMTP, FTP, or HTTP and press Connect. If the target is running a server on that port, you will see a response. If the target refuses your connection, you will see it in the response area. You will see a header from the server which indicates clues as to what operating system is being used.
- *Using TCP Term to verify an email address.* First, find the MX machine(s) for the domain part of the email address. Then use the MX machine address as the target. Enter SMTP into the Target Port. Connect and wait for the header. Then type HELO followed by a space and your machine name, hit enter. If you get a successful acknowledgement, then type VRFY followed by a space followed by the full email address, hit enter. You will see a response. Type the word QUIT and hit enter. The connection should close. If not, press Disconnect.

Setup

TCP Term is simple to configure. Before configuring, you must know two things:

A. The target host IP address or hostname.
B. The target service name or port number to connect with or select from ports previously entered.

Enter the target port name or port number into the **Target Port Name/No**. edit box. TCP Term also allows you to specify the source port number. Each connection between a client application like NetScanTools and the target host's service is made up of a source and destination port pair. With TCP Term, you can specify both. Normal operation is for NetScanTools to automatically select a source port number by checking the **Any Source Port** checkbox.

Enter the target host IP address[74] or Hostname[75].

In most cases, you will want to check the **Local Echo** checkbox. This means that, when checked, any characters you type are displayed locally on the data entry area.

Using TCP Term

Configure TCP Term as mentioned above and press the **Connect** button. If a connection is successful, the status area will display 'Connected to host' and the cursor will be placed in the data entry area. You may begin typing at this point (assuming you are familiar with the protocols used by the service you have connected to!).

To disconnect, press the **Disconnect** button and NetScanTools will immediately close the connection. Depending on the protocol of the service you connect with, the target host may terminate your connection early. If it does, the logo in the upper left hand corner will no longer spin and the Receiving data... message will change to Ready.

Error Messages

The most common error message you will see is this:

```
Error connecting to host:
The attempt to connect was refused.
```

This message means one of two things:

1. The most likely is that there is no service running on the target that you can connect to.
2. The least likely is that the target host is rejecting your connection based on the IP address you are connecting from.

---

[74] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

[75] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

Other messages you may see are:

```
The requested host is unreachable.
```

A dialog box with this message:

```
Port name not found--please enter the associated port number.
```

This message means that you entered a port name like 'xyz' and NetScanTools was unable to translate that port name into a port number. For more information about translation, see the Database Tests section.

See Also...
Database Tests
Port Probe
The Lower Button Row

TimeSync Tab

About

TimeSync allows your computer to communicate with precision internet based time servers for determining the current time. It also allows you to correct your computer clock to closely match the time at the time servers.

Information Returned by this Feature

TimeSync works with three protocols to establish the difference in time between your computer clock and the network time server clock. TCP[76] and UDP[77] protocol allow a one second resolution, while the high resolution SNTP (Simple Network Time Protocol) allows a theoretical 200 picosecond resolution.

Help Wizard Topics

- *Using TimeSync to synchronize your clock to network time servers.* Select a time server and protocol. Then press Query Time to test TimeSynchronization. If it communicates properly and your difference is under an hour, press TimeSync to change your computer clock to match the network time clock.

Using TimeSync

Select a time server either from the list found by pressing the [...] button or by viewing this detailed list of time servers along with usage rules. When you press the [...] button you will be presented with a list of time servers in a dialog box.

After selecting the server to use, select your time protocol that you wish to use. *Not all protocols are supported by every server.* The TCP and UDP protocols give a one (1) second resolution, while the SNTP protocol gives a much higher 200 picosecond resolution.

Once you have selected the protocol (SNTP for our example), you are ready to run a time query. Press **Check Time** to connect to the time server and get the current time at the server. If contact is made with the server, you will see a message like this one:

```
Time Server Clock: Monday, June 21, 1999 08:27:30, Delta: 0.012358 seconds
```

Below the status area, you will see a special message for SNTP protocol only. It describes the stratum, NTP version and type of server. Stratum can be 1 or 2, NTP version is typically 3 and the type can vary widely.

By pressing **TimeSync**, you will see a message like this one:

```
Time Server Clock: Monday, June 21, 1999 08:27:30, Delta: -0.007232 seconds before correction
```

***As a failsafe**, if the time difference between your computer clock and the server exceeds one (1) hour, you will be warned of that fact and you will be asked to manually move your clock closer to the correct time. The computer time will **not** be synced when you see this message.*

TimeSync Scheduler

The TimeSync scheduler allows you to schedule times when the TimeSync function will be activated to synchronize your computer clock to the last recently entered network time server clock. Changes made on the Scheduler dialog take effect upon restarting NetScanTools. The scheduler does not start NetScanTools, it expects NetScanTools to be running for the scheduled TimeSync event to take place. Descriptions of the scheduler options follow.

Enable TimeSync on Startup. The purpose of this checkbox is to attempt to synchronize your computer clock when NetScanTools starts. If you select this box, the last parameters used on the TimeSync tab are used to query a time server when the program starts. Also, checking this box overrides the tab ordering to a certain extent because the TimeSync tab will show as the first tab. Default is unchecked.

Frequency = Not active - the scheduler is not active except for the status of the Enable TimeSync on Startup checkbox state. Default.

Frequency = One time - select a date and time of the event.

Frequency = Hourly - select the minute that the event will occur on every hour.

Frequency = Daily - select the time of day that the event will occur on every day.

Frequency = Week days - select the time of day that the event will occur on Monday through Friday.

Frequency = Weekly - select the day of the week and time of day that the event will occur on once every week.

---

[76] TCP means transmission control protocol as defined in RFC 793. It is intended to provide a highly reliable method of assuring delivery of packets between network connected computer systems and uses IP as a next level lower protocol layer.

[77] UDP means User Datagram Protocol and it defined in RFC 768. Unlike TCP, it does not provide a reliable protocol for assuring the delivery of packets between networked computer systems.

Frequency = Monthly - select the day of the month and time of day that the event will occur on once every month. Warning: if you select a day greater than 28, TimeSync will not months with a total number of days less than the number you select.

Year 2000 Information

NOTICE: This Information is designated as a Year 2000 Readiness Disclosure and the information contained herein is provided pursuant to the Year 2000 Information and Readiness Disclosure Act.

TimeSync works using an external Network Time Protocol server as a reference for establishing the exact absolute UTC time. The network protocols used are based on RFC 868 for simple, 1 second resolution time establishment and RFC 2030 for higher resolution timing that accounts for packet round-trip-times when making timing calculations.

RFC 868 TCP and UDP Time Differential and Synchronizations are based on the simple connection by NetScanTools to the Network Time Server's NTP port, then receiving a 4 byte packet which represents the time relative to a fixed date. The time is the number of seconds since 00:00 (midnight) 1 Jan 1900 UTC. Since Windows makes calculations relative to 00:00 1 Jan 1970 UTC, a 70 year offset is accounted for. NetScanTools then calculates, using standard Windows time functions, the actual time relative to your time zone. Time differences and corrections are calculated using your system time and the time reported by the Network Time Server. The 4 byte number will be sufficient to represent times until the year 2036, by which time the RFC 868 protocol will be superseded and made obsolete as will NetScanTools.

The more complicated RFC 2030 SNTP protocol allows the client program (NetScanTools) to establish the sending and receiving times of the time packets sent and received, so that the delays in packet transmission over the internet can be accounted for. This will typically give accuracies in the millisecond range. As with the simpler RFC 868 protocol, the time is the number of seconds since 00:00 (midnight) 1 Jan 1900 UTC, which also means that this protocol will also be obsolete in 2036. The protocol also includes a seconds fraction 4 byte segment which provides a 200 picosecond precision. The protocol allows NetScanTools to "timestamp" the outgoing packet and then use the corresponding return "timestamp" to establish the round-trip-time delays. Then the delays can be removed mathematically. NetScanTools timestamps the outgoing packets with the origination time in UTC. All calculations ensure that time zones and delay times are accounted for and the calculations rely on key functions built into WIN32 to establish the local time offsets for display to the user.

See Also...
Daytime
The Lower Button Row

Time Servers

The current version of this page is available at:
http://www.eecis.udel.edu/~mills/ntp/servers.html

The following notice applies to the text following on this page and the two server lists:

```
The following copyright notice applies to all files collectively called the Network Time Protocol
Version 4 Distribution. Unless specifically declared otherwise in an individual file, this notice
applies as if the text was explicitly included in the file.
/***********************************************************************
 *                                                                     *
 * Copyright (c) David L. Mills 1992-1998                              *
 *                                                                     *
 * Permission to use, copy, modify, and distribute this software and   *
 * its documentation for any purpose and without fee is hereby         *
 * granted, provided that the above copyright notice appears in all    *
 * copies and that both the copyright notice and this permission       *
 * notice appear in supporting documentation, and that the name        *
 * University of Delaware not be used in advertising or publicity      *
 * pertaining to distribution of the software without specific,        *
 * written prior permission. The University of Delaware makes no       *
 * representations about the suitability this software for any         *
 * purpose. It is provided "as is" without express or implied          *
 * warranty.                                                           *
 ***********************************************************************/
```

These pages contain lists of Network Time Protocol (NTP) public time servers. They are provided for information purposes only and represents the best information available at the current date. It does not represent a commitment to provide connectivity or time service on the part of the operators involved. Further information of a technical nature can be obtained from the ntp@ni.umd.edu list. To subscribe to this list, contact mailto:ntp-request@transsys.com. Alternatively, if possible, please subscribe to the newsgroup comp.protocols.time.ntp which is gatewayed to the mailing list.

Please send corrections or additions to mailto:mills@udel.edu in HTML format as used in the list pages. If an error is found by other than the responsible person, please first request that person to submit the correction.

Rules of Engagement

As the load on the hosts supporting NTP primary (stratum 1) time service is heavy and always increasing, clients should avoid using the primary servers whenever possible. In most cases the accuracy of the NTP secondary (stratum 2) servers is only slightly degraded relative to the primary servers and, as a group, the secondary servers may be just as reliable. As a general rule, a secondary server should use a primary server only under the following conditions:

I. The secondary server provides synchronization to a sizable population of other servers and clients on the order of 100 or more.

II. The server operates with at least two and preferably three other secondary servers in a common synchronization subnet designed to provide reliable service, even if some servers or the lines connecting them fail.

III. The administration(s) that operates these servers coordinates other servers within the region, in order to reduce the resources required outside that region. Note that at least some interregional resources are required in order to ensure reliable service.

In order to ensure reliability, clients should spread their use over many different servers. As a general rule, no more than two clients per network should use the same server on another network; however, in order to simplify management of host configuration tables, many hosts on the same network may use the same (redundant) servers on the same network.

Unix users are strongly encouraged to adopt the latest NTP version software in the compressed tar distribution shown in the NTP home page (http://www.eecis.udel.edu/~mills/ntp/). Besides providing more accurate, reliable service, the latest version automatically increases the polling intervals for all peer associations, but without sacrificing performance. This can significantly reduce network loads, as well as the loads on the busy primary servers, some of which have over 700 clients.

Public NTP Time Servers

The list of primary (stratum 1) and secondary (stratum 2) designates the NTP time servers available for public access under stated restrictions. Each entry gives the host name, Internet address, approximate location and geographic coordinates (if available), synchronization source (stratum, type of radio or satellite receiver and host type), suggested service area, access policy (as notified) and responsible person name and e-mail address. Most servers indicate the NTP version as well. It is always wise to consult the

DNS to verify host addresses, which are changed from time to time. When more than one address is given, preference should given to each in order. All servers are equipped with uncompensated crystal-stabilized timebases, unless indicated otherwise.

It is very important that potential clients avoid use of servers not listed as open access, unless approved first by the responsible person. This especially includes indiscriminate use of servers not listed in the list, since this can be disruptive. The responsible person should always be notified upon establishment of regular operations with servers listed as open access. Please respect the access policy as stated by the responsible person. Servers listed as closed access should NOT be used without prior permission, since this may disrupt ongoing activities in which these servers are involved.

Accessing the Lists

Public NTP Primary Time Servers
Public NTP Secondary Time Servers

See Also...
Time Sync

TraceRoute Tab

About

TraceRoute is an extremely useful utility which shows the route your network packets are taking between your computer and a target host. This can be useful in determining the internet provider(s) that services a domain--more about that later.

Information Returned by this Feature

TraceRoute shows a list of computers that routed packets between your computer and a target computer. The mechanism for doing this is based upon the ICMP[78] protocol. Click here to learn how TraceRoute works.

Help Wizard Topics

- *Using TraceRoute to determine the packet transmission route.* Enter the IP Address or hostname and press Trace. The route will be displayed.
- *Using TraceRoute to determine upstream internet providers.* Enter the IP Address or hostname and press Trace. The route will be displayed. The second to last or third to last hops before the 0:0: Echo Reply hop are normally owned by the upstream providers. See also this article.

Setup

TraceRoute is fully configurable. Change the parameters in the Setup dialog box.

The TraceRoute Tab Controls

The controls most essential to the basic operation of TraceRoute are:

- **Trace** button - This button initiates a trace sequence.
- **Stop**[79] button - This button is used to stop any current trace activity.
- **Setup** button - This button activates the Setup Dialog.
- The Clear Results[80] button clears the results display.
- The AutoSize[81] button sizes the columns the results display to match the longest text string in each column.

The **Resolve IP Addresses to Host Names** checkbox, when checked, forces an IP address[82] to be translated to it's corresponding hostname[83], if any. The result of the IP to hostname translation is shown in the lower status window along with the IP address. TraceRoute will operate faster if the box is not checked because it does not have to translate IP addresses to hostnames.

Using TraceRoute - A Simple Example

When you first install NetScanTools, several assumptions are made about your system. If your system is standard with no additional special Winsock software, then you can enter a hostname or IP address and press Trace (obviously we're assuming you are connected to a network with at least one router).

Results Formatting

Results are displayed in spreadsheet format with user variable column widths. To change the column width, move your cursor over the heading bar to the vertical lines separating each column, press the mouse button and drag to the desired width. Columns can also be autoformatted to the longest string length by double-clicking on the column header separator to the right of the column. All columns can be automatically size to the longest length of the text in each column by pressing the AutoSize button.

The Results Display Columns

- The **Hop Column** shows the hop number.
- The **IP Column** shows the IP address of the intermediate router (hop). Any hops that do not return an ICMP message will be shown with a '*' symbol.

---

[78] **I**nternet **C**ontrol **M**essage **P**rotocol - assists in determining when packet transmission errors have occurred.

[79] The **Stop** button stops or cancels the current activity.

[80] The results area of this tab are cleared when this button is pressed.

[81] The AutoSize button causes all columns in a report style list view to be sized to the widest text string found in the column.

[82] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

[83] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

- The **Host Name Column** shows the hostname of the router. This is displayed if the Resolve IP addresses to host names checkbox is checked. If the IP address does not have a corresponding hostname, a '?' symbol will be shown in this column.
- The **Time Column** displays the round trip time in milliseconds. This is the time it takes for a packet to be sent to us in response to a packet we sent. If you use the Winsock[84] 2 setting on the TTL compatibility section of the Preferences tab, you will get 1 millisecond resolution timing. The Automatic setting will result in approximately 10 millisecond resolution timing.
- The **Status Column** shows nominal results in the example. All intermediate hosts in a TraceRoute will show Type 11, Code 0 or 11:0 under normal circumstances. Type 0 is returned by the last host. You will occasionally see other ICMP packet types reported. These are usually host or net unreachable or even source quench.

Right Click Menus
After a Traceroute sequence is complete, you can right click with your mouse in the results area to bring up a menu. This menu contains the following options:

- **Ping Selected IP** - this takes the IP address found in the Target column and activates the Ping tab to Ping that IP address.
- **Display Traceroute Time Graph** - this activates the NST Graphing program using the data from the current trace. It will show a graph (printable) much like the example here.

Interpreting the Results
The hop (router or gateway) number is displayed with the IP address of the responding hop and, it's hostname (optional--can be omitted for speed), the milliseconds it took from the time the packet was sent to the time a corresponding packet was received, the packet type received as a reply and the status. Note that some of the routers have names that are somewhat indicative of their function. You will frequently see names containing 'T1', 'T3', 'FDDI', etc., denoting the type of network hardware used. You can also tell the backbone network and some of the node locations. Unfortunately, not all routers and gateways have DNS entries, so NetScanTools places the famous '?' where the name should be. Remember, if you see a '?', NetScanTools has not failed, the DNS has not returned the hostname for that IP address. If you see the message **'Target not reached'** in the status area, increase the TTL setting in the setup dialog.

Advanced TraceRoute Usage
If you see that the first hop or two--or even three are always the same, you can go to the Setup Dialog and set the starting hop for the number following those 'static' hops. This will significantly speed up the trace function since NetScanTools will be starting at a router further out than your immediate gateway.

Another thing that TraceRoute can do is assist in determining MTU. By checking the 'Don't Fragment Packets' checkbox, ICMP packets will not be fragmented as they are forwarded towards their destination. If a router refuses to pass ICMP packets over a certain size, you will see the 'No packet received from this hop.' message. If the hop number keeps increasing and you still see that message, then it means one of three things:

1. ICMP packets are blocked beyond that router.
2. The target host or routers to it are down.
3. You have exceeded the MTU for that router.

If you think that number 3 may be the problem, then try reducing the packets size to see if the packets pass. If not, then numbers 1 and 2 may be the problem.

Other ICMP considerations
Many routers and especially gateways to destination networks will not respond to ICMP packets. This is often by design. Since you (and hackers) can use Ping, TraceRoute, and NetScanner to determine the topology of a remote network, many companies have deliberately turned off response to ICMP packets. Other reasons include prioritizing--some routers place such responses on a low priority and may not get around to responding to your packets until your Timeout setting has expired.

Error messages
Though it is not really an error message, the '?' symbol will frequently show up in the hostname field during a trace. This simply means that the DNS could not resolve the responding IP address of the router into an actual hostname. This may be due to a DNS timeout or there may actually be no record of that IP address in the DNS. In other words, it's not really an error.

Normally, each intermediate hop will return 'Type 11', packet Time Exceeded (timeout) or 'Type 0', Echo Reply, which is only returned by the target host. Other types are possible. These include types like Network or Host Unreachable.

See Also...
ICMP Packet Types
Name Server Lookup
NetScanner
Ping
Preferences
The Lower Button Row

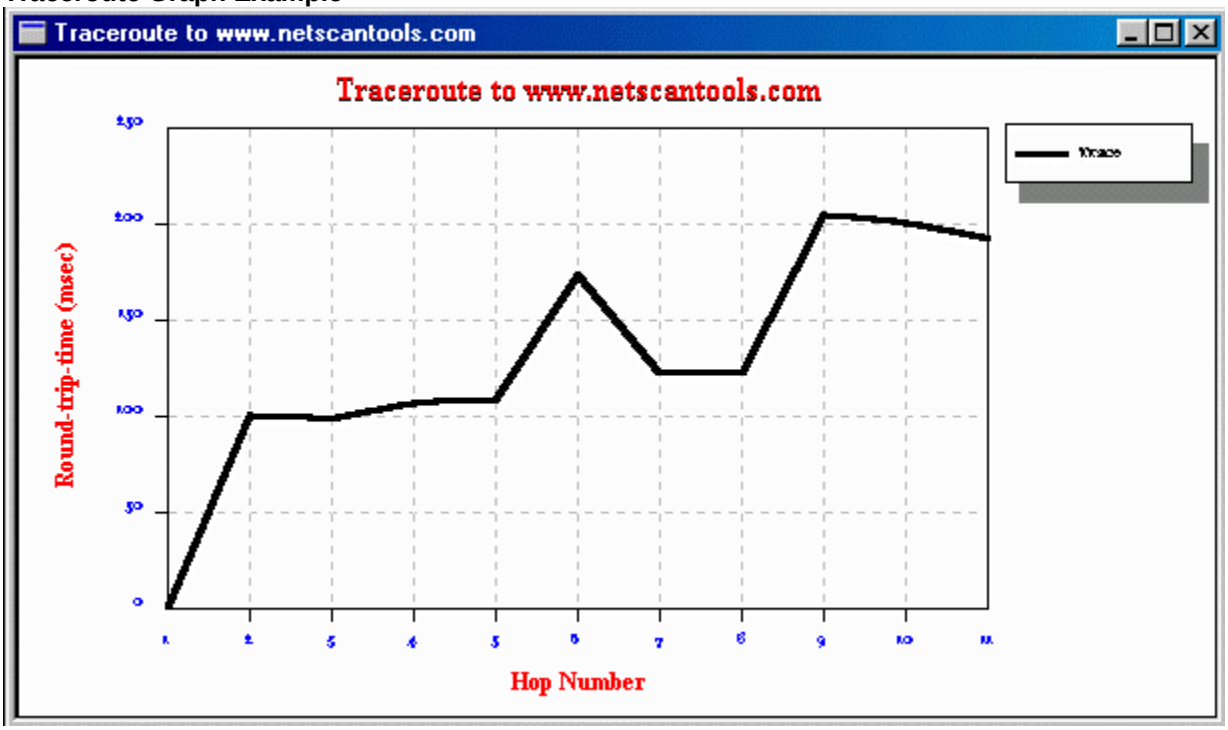
[84] Winsock is derived from the sockets concepts found in BSD (Berkeley Software Distribution) UNIX. NetScanTools requires Winsock 2 or above for proper operation.

TraceRoute Tab Setup

To activate TraceRoute Setup, press the Setup button on the TraceRoute Tab. With this dialog box, you have control over:

- The **Starting Hop** is the first router that you want to show. On most ISP connections, the first two or three hops are always the same. Use this setting if you want to eliminate the first 'n' hops from your TraceRoute report. Default is 1.
- The **Packet Timeout**, in milliseconds, which is how long wait for a packet to come back before either completing the current hop trace attempt or retrying the current packet with the same TTL value. Default is 2000 (2 seconds).
- The **Packet Length in Bytes** which is how many data bytes in the packet. The first 8 data bytes are reserved for timing purposes. Default is 32 bytes.
- The number of **Retries**. If a packet fails to come back, NetScanTools tries to send the same packet again this many times. Default is 1.
- The maximum **Packet Time-To-Live** on the internet which is measured in seconds, but is also effectively the maximum number of hops the packet can traverse in one direction. Default is 16.
- The **Don't Fragment Packets** bit in the IP header. This tells each router not to fragment the packet as it is passed along to the next router. You can use this information to locate bottlenecks and determine the Maximum Transmission Unit (MTU) for the path your packets are taking. Default is not checked.

Traceroute Graph Example



What's New at NWPS Web Site Tab

About

This tab is your portal into the current news from the Northwest Performance Software, Inc. web site. This tab can serve as very simple web page analysis tool. You can use it to view the html web page source code and view the informational headers which are hidden from view by most web browsers.

Help Wizard Topics

- *Using What's New to determine web server type.* Enter a URL for the site and press Get URL. Once the URL is received, UNCHECK the Display HTTP headers and HTML Tags box. Look for the Server: entry in the header.
- *Using What's New to grab the URL web page.* Enter a URL for the site and press Get URL.

Setup

The primary purpose of the setup dialog is to tell NetScanTools to setup a CERN compatible proxy if your location requires you to use one. Please click here to learn how to use the Setup Dialog.

Using the 'What's New' Features

When you select the 'What's New' tab for the very first time after starting NetScanTools, a special web page query goes out to our web site asking for a specific page--the whatsnew.html page.

Viewing Hidden Headers and HTML Tags

Every web page that you get from a web server has a header full of information about the web page. It usually tells you the type of web server software used at the web site, the time of web page creation, the web page size and other useful parameters. To view hidden headers, uncheck the **Display HTTP Headers and HTML Tags** checkbox.

See Also...

TCPTerm
The Lower Button Row

What's New Setup

Normally this is only required for users who must use NetScanTools from behind a company firewall. In order to get information from the untrusted side of the firewall to where the user is (normally on the trusted side), most companies set up a proxy server across the firewall. The proxy's purpose is to take trusted side web page requests and pass them across the firewall to the target web servers, then take the information received from the web server and pass it back to the trusted side web browser.

To setup NetScanTools to take advantage of proxy servers, you will need to know some things about the proxy before using the Setup Dialog. First you must know the hostname or IP address of the proxy server. When you know what it is, you must enter it into the Proxy Server field. Second, and equally important, you must know the TCP port number which is used by the Proxy Server for HTML communications. Normally, web servers operate using port 80 for non-secure HTML traffic, however, Proxy Servers can operate on any available port. You will probably need to check with your Network Administrators for this number. If in doubt, try port 80. To complete the Proxy Setup, change the radio button from Direct Internet Connection (normal for non-proxy users) to the CERN Proxy setting. Note: CERN is the European Laboratory for Particle Physics; see www.cern.ch.

See Also...
What's New at NWPS Web Site

Whois Tab

About Whois

Whois is a utility that acts as a client interface to a remote server database of domain or IP address registries. One of the largest domain registry databases is maintained by Network Solutions, Inc., currently serves as a registry for the majority of domains ending with 'com', 'net', 'org', or 'edu'. Other organizations maintain Whois databases for other domain extensions.

Information Returned by this Feature

When you run a Whois query you will generally get back a set of information which can be very general or even somewhat minimal (the UK whois server is an example of minimal), or as in the case of some Whois servers like RIPE.net, extensive information about the domain registrant can come back. If you are running a query on a single domain, you will usually get back information about the registrant like the Administrative Contact, the Billing Contact and the Technical Contact. Some domain registrants try many things to protect their privacy. Some entries show no names or have invalid email addresses and sometimes they even have missing phone numbers and addresses---but this is not the norm. This information is publicly available, however, is not to be used for profit or resold and is generally reasonably accurate, however, the accuracy of the information will vary with the age of the entry.

Help Wizard Topics

- *Using Whois to determine IP Address ownership.* Enter the IP Address and press Query.
- *Using Whois to determine upstream internet providers.* Enter the IP Address or the domain name and press Query. The name server entries or the netblock entries will show the parent IP address range.
- *Using Whois to find the domain owner for the hostname.* Remove the hostname[85] from the domain name[86], enter it and press Query.
- *Using Whois to find the domain owner.* Enter the domain name and press Query.
- *Using Whois to see if the email address is listed as a domain contact.* Turn off Smart Whois, select the whois server you want to check, press Setup and enter the server name into the default server field and press OK. Then enter the email address and press Query.
- *Using Whois to search for a name in the domain database.* Turn off Smart Whois, select the whois server you want to check, press Setup and enter the company name or the most unique part of a person's name into the default server field and press OK. Then enter the email address and press Query.

Using Whois

Regardless of whether you use SmartWhois or not, all queries follow the same format, either enter a domain name or an IP address[87]. nwpsw.com is a domain name, www.nwpsw.com or mail.nwpsw.com are not domain names, they are hostnames. Other special queries can be made. Enter the word 'help' and press query to obtain help from a specific whois server on the format of the special queries.

There are two modes that NetScanTools Whois client runs for doing standard, simple queries. The first mode is easy to use and is specifically designed to assist you in making Whois queries where you would be frequently changing the whois server. The '**Smart Whois**' mode uses the domain extension to determine which Whois Server should be sent the query. If you are trying to query on nwpsw.com, it sends the query to whois.networksolutions.com. If you are trying to query on af.mil, it sends the query to whois.nic.mil and so forth. Currently, NetScanTools supports around 40 domain name extensions and all IP addresses. The starting point for all IP address queries is whois.arin.net.

The second is the most basic mode where the 'Smart Whois' checkbox is *not checked*. In this mode you are completely responsible for deciding which Whois Server to use for your queries. In other words, all queries are directed to the default Whois Servers defined in the Whois Setup dialog box.

To use the Whois Setup dialog box, press the setup button from the Whois tab. The Whois Server that you enter must be of the form 'whois.networksolutions.com', or 'xyz.nic.jkl', or it may be an IP address. If you are located behind a firewall, check with your firewall administrator to see if they have set up a Whois Proxy Server. If they have a proxy server designed to forward Whois queries, then you can use the Proxy Server name entry area in the Setup dialog box to define the Proxy Server.

Smart Whois

This option is enabled by default and is enabled whenever the **Enable Smart Whois** checkbox is checked. To query on a domain (microsoft.com, nwpsw.com, att.net, af.mil, etc.), just enter the domain name and press the Query button. This also works for IP

---

[85] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

[86] Domain Name is the name of the domain that a group of computer systems are assigned to. netscantools.com or nwpsw.com are domain names.

[87] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

addresses--enter the IP address and press query. You must decide ahead of time whether or not to use Smart Whois--however, we recommend using it for most queries.

Whois Servers/Choosing a Server Yourself
Since domain names are assigned by various entities around the world, you must know which registration entity controls each domain in order to gain information by the domain. Historically domains registrations with the extensions . com, .edu, .net and .org were maintained by a private company, Network Solutions, Inc. This changed during 1999. Please see www.internic.net for a list of all the new domain registrars. You can request a limited list of whois servers by pressing the 'Enum Hosts' button. This button issues a request to a database which will send a list of whois servers to you. This list is maintained at a University and is updated every three to six months.

Example Query
In this example, we are using fictitious information.

```
[Query: SomeCompanySomewhereThatDoesNotExist.com, Server: whois.networksolutions.com]


Registrant:
Some Company Somewhere That Does Not Exist, Inc. (SCSTDNEINC-DOM)
   PO Box 987654321
   Anytown, WA 99999-9999
   US

   Domain Name: SOMECOMPANYSOMEWHERETHATDOESNOTEXIST.COM

   Administrative Contact:
      Doe, John  (JD99999)  john.doe@ SOMECOMPANYSOMEWHERETHATDOESNOTEXIST.COM
      253-999-9999 (FAX) 253-999-9876
   Technical Contact, Zone Contact:
      ABCDEF HOSTMASTER  (HC98765432-ORG)  hostmaster@UPSTREAMISPWHOGETSMONEY.COM
      777-999-9999
Fax- 777-999-9876
   Billing Contact:
      Doe, John  (JD99999)  john.doe@ SOMECOMPANYSOMEWHERETHATDOESNOTEXIST.COM
      253-999-9999 (FAX) 253-999-1234

   Record last updated on 27-Jul-97.
   Record created on 15-Jun-93.
   Database last updated on 26-May-98 06:34:47 EDT.

   Domain servers in listed order:

   NS1.SOMENAMESERVER.COM        10.1.2.3
   NS2.SOMENAMESERVER.COM        10.1.2.4

[End of Whois message]
```

See Also...
NetScanner
The Lower Button Row

Whois Setup

About

Whois Setup is intended to provide the default whois servers which are used when a domain name or IP address is NOT found in the Smart Whois database. There are entry fields provided for setting the default whois servers and a proxy server.

Default Whois Server - General Queries

The server specified in this entry field is used whenever the Smart Whois parser cannot associate the domain name with a specific whois server. It is also used if the Enable Smart Whois checkbox is unchecked. You can enter the hostname[88] or IP address[89] of a whois server. To the right of the entry field is a button labeled [...]. When pressed, it provides a list of whois servers from the Smart Whois database. Default is whois.networksolutions.com. On the farthest right is a box labeled 'Port'. This is the port number to use with the default whois server. Normally this is 43, but if you are using rwhois, you can enter the port number of the rwhois server, typically 4321.

Step One .com, .net, .org, .edu Whois Server

This server is queried first to determine the actual whois host which has the information you require. *This only applies to the .com, .net, .org, .edu domain extensions.* To the right of the entry field is a button labeled [...]. When pressed, it fills the history list with a list of whois servers. Default is whois.crsnic.net. Alternative is whois.internic.net.

Smart Whois Default Server for IP Address Queries

The server specified in this entry field is used whenever the Smart Whois parser cannot determine the server associated with IP address that was entered. You can enter the hostname or IP address of a whois server. To the right of the entry field is a button labeled [...]. When pressed, it provides a list of whois servers from the Smart Whois database. Default is whois.arin.net.

Proxy Setup

The server specified in this entry field is used as a proxy server whenever the Use Proxy Server checkbox is checked. Default is not checked.

[88] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

[89] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

Winsock Info Tab

About
This tab gives basic information about the active Windows Sockets (Winsock) software interface layer that is running on your computer system.

Using Sockets Version
Normally, this will show 2.0. This is because NetScanTools requests Winsock version 2.0. NetScanTools does not support Winsock 1.1.

Highest Supported Sockets Version
This is the highest version of Winsock that is supported by your Winsock implementation. Windows NT 4.0 introduced sockets 2.0 compatibility, so the native Winsock will report 2.2. Windows 98 will also report Winsock 2.

Status
This will normally say 'Running.' or 'Running on Windows 95' etc. Note: The Winsock on Windows NT 4 occasionally says 'Running. (Duh)'. Just so you know, this is **not** a message generated by NetScanTools, it comesfrom the Winsock.

Description
This field is filled with information generated by the Winsock implementation itself. On Windows NT 4, the text is 'WinSock 2.0.'

Maximum Sockets
The value varies with the type of operating system and the type of Winsock being used. This value is usually 0 or 32767.

Maximum UDP Datagram
The value varies with the type of operating system and the type of Winsock being used. On Windows NT 4, this value is 0.

Vendor Information
Vendor information is normally 'Not Available' for standard implementations of Microsoft's Winsock as installed with Windows 95, 98,and NT 4. If the vendor has provided any information in this field, NetScanTools will display that information.

Socket Types Supported
Three types are normally supported.

- **Stream Sockets** - This is what is used by TCP[90] to make a connection oriented socket.
- **UDP Datagram Sockets** - This is what is known as a connection-less socket. That is, there is no guarantee that the packets reach their intended destination.
- **Raw Sockets** - This type of socket allows the programmer full control (in theory) over the contents of the message and the header being sent out of the socket. It is found on Windows NT 4 and Windows 98. It is not found on Windows NT 3.5x or Windows 95 with standard Microsoft supplied Winsocks (Microsoft has made available for download a Winsock 2 upgrade for use on Windows 95).

See Also...
Preferences
The Lower Button Row

[90] TCP means transmission control protocol as defined in RFC 793. It is intended to provide a highly reliable method of assuring delivery of packets between network connected computer systems and uses IP as a next level lower protocol layer.

AutoPing

AutoPing

NetScanTools also has an automated feature called AutoPing. AutoPing sends a group of Ping Packets to a target on a scheduled basis. This feature is useful for determining if a remote site is down or watching the connection to identify intermittent connectivity problems. You can also use it for a keep-alive feature if your connection is normally dropped after a period of time due to inactivity. A log file is kept which will either log only the missing packet errors or log all data. The log file can be viewed from the Setup Dialog. When AutoPing is active, all other Ping Tab features are disabled.

See Also...

Ping
Ping Setup

Finding an Upstream Internet Provider

Background

The first question you may ask is 'What does this mean and what good is it?'. Very often we receive spam suggesting that we come to a specific site, usually given in the form of an IP address, like http://10.1.2.3/getrichquick.html. Obviously, they don't give you a way to remove your name from their list. The email headers are forged, and if they give you a 'remove' email address, it's either bogus or a email address collection account which confirms to the spammer that your email address is good. One thing you can do is complain to their upstream provider. All of these web sites have an upstream provider. You can use NetScanTools to find their upstream provider.

Assumption #1: they have given you a valid URL to come visit.

For the following example, you must be actively connected to a TCPIP network PRIOR to starting NetScanTools.

Getting the upstream provider.

I. Start NetScanTools.

II. Carefully copy the IP address or hostname into the TraceRoute tab. Be sure you get it right so you don't falsely accuse anyone. DO NOT include the http:// part or any /getrichquick.html pages in the info you enter. Just the name or IP address. For the following fictitious example we are using 10.8.3.56.

III. Press the 'Trace' button.

IV. You should see the results similar to these as shown below:

```
...
8 10.1.5.6 router24.theUpstreamProvider.net 250 type 11
9 10.8.3.1 gateway.theSpammer.com 250 type 11
10 10.8.3.56 ? 350 type 0
```

What you are after is the either the second to last or third to last hop (as in the example). Then you would email your complaint to abuse@theUpstreamProvider.net. Be nice to them, remember, they didn't originate the spam. If they get enough complaints they may deal with it.

See Also...

TraceRoute
Usage Tips

Finding Text in a Results Window

Background

Many of the client functions contained in NetScanTools produce results which exceed the window size of the results area. A good example is the 'whois' client. Entering a query such as the word 'Smith' (no quotes) produces a long list of all the persons and companies with the name Smith in it. So how do you find the right text?

For the following example, we are assuming that you are actively connected to a TCPIP network.

Using the Find text button

I. From the NetScanTools Whois tab, press the 'setup' button.
II. Set the following values: whois.internic.net for server (Optionally, you may need to set your whois proxy if you are behind a firewall.)
III. Close the whois setup by pressing OK.
IV. Enter the word 'eskimo' (no quotes) in the whois query entry box and press the Query button. (note: you may use any other query string you wish)
V. When NetScanTools is done receiving the data from the whois server (this may take up to a couple of minutes), the NST logo will stop spinning. You should have several companies with the word eskimo in them.
VI. Now press the Find button at the bottom of the NetScanTools window. You may also press cntl-F.
VII. Enter the text North in the Find dialog and press Find First. The first occurrence of North should be highlighted. Note that this search is not case sensitive.
VIII. Press the F3 key to highlight subsequent occurrences.

*Note that Find works differently on special view tabs like ping or port probe. It highlights the whole row, not just the characters it found.

See Also...

Find Button
Usage Tips

Finding the Authoritative Nameserver for a Domain

Background

Each domain has a DNS name server or servers which are called Authoritative Name Servers. It is responsible for maintaining accurate information about that domain. Usually one name server is a primary called the Start of Authority and it is almost always mirrored to one or more backup name servers. NetScanTools can locate the Authoritative Name Server(s) for any domain.

For the following example, you must be actively connected to a TCPIP network PRIOR to starting NetScanTools.

Finding the Authoritative Nameserver for a Domain.

I. Start NetScanTools.

II. On the Name Server Lookup tab, press the Setup... button, check to be sure that a name server IP address or hostname is entered in the Current Server edit box and select NS (Name Server) for query type. Then Press OK to close. (NOTE: NetScanTools makes every attempt at automatically determining the default name server for your computer and places it in the Current Server box)

III. On the Name Server Lookup tab, enter a domain name like nwpsw.com and press the Adv Query button.

IV. You should see the results showing the Authoritative Name Server(s) as shown below.

```
Looking up [nwpsw.com]
Server: NS2.NETDIRECT.NET
Address: 204.120.164.4


Non-authoritative answer:
nwpsw.com nameserver = NS2.resolver.net
nwpsw.com nameserver = NS1.resolver.net


Authoritative answers can be found from:
NS2.resolver.net internet address = 207.137.171.3
NS1.resolver.net internet address = 207.137.72.3


[End Query]
------------------------------------------------------------------------
```

I. Now copy NS1.resolver.net or NS2.resolver.net to the clipboard, and go back to the Setup dialog.

II. Enter either of those name servers into the current server edit box, select SOA for query type and press OK.

III. On the Name Server Lookup tab, enter nwpsw.com and press the Adv Query button.

IV. You should see the results showing the Start of Authority Name Server (origin entry) as shown below.

```
Looking up [nwpsw.com]


Server: NS1.resolver.net
Address: 207.137.72.3


nwpsw.com
origin = NS1.resolver.net
mail addr = postmaster.resolver.net
serial = 1121226758
refresh = 10800(3 hours)
retry = 3600(1 hour)
expire = 5184000(60 days)
minimum ttl = 86400(1 day)
nwpsw.com nameserver = NS1.resolver.net
nwpsw.com nameserver = NS2.resolver.net
NS1.resolver.net internet address = 207.137.72.3
NS2.resolver.net internet address = 207.137.171.3


[End Query]
```

See Also...

NSLOOKUP
Usage Tips

Getting your IP address

Background

Many ISPs (internet service providers) configure their PPP connections to give out IP addresses to users as they log in. This means you will usually get a different IP address each time you connect to the internet. The same is true for DHCP[91] clients in large intranets. How do you use NetScanTools to find out your IP address?

For the following example, you must be actively connected to a TCPIP network PRIOR to starting NetScanTools.

Getting your IP address.

I. Start NetScanTools and switch to the Name Server Lookup tab.
II. View your IP address(es) on the Name Server Lookup tab as shown below:

```
This Computer's Name and IP Address:
Translated Name: p166.eskimo.com
IP Address: 203.28.133.4
IP Address: 10.2.5.7
```

This example has more than one IP address because it is a multi-homed system. It has more than one TCPIP network card or modem (NDISWAN) connection. Most users will only have one IP address listed.

See Also...

Name Server Lookup
Usage Tips

[91] DHCP - Dynamic Host Configuration Protocol. A method of dynamically assigning an IP address, subnet mask and default gateway from a DHCP server responsible for the subnet. See RFC 1542.

How to Detect Link Layer MTU using Ping

Background

NetScanTools includes a feature as part of the Ping tab utility: control of the Don't Fragment IP header bit. Packets travel from one place to another across many different types of routers. Some packets may need to be split into more than one packet because of limitations on the size of a packet through a router. The maximum size of a packet allowed to pass between two systems is the Maximum Transmission Unit or MTU. If a packet needs to be split and the Don't Fragment bit is set, the router returns an ICMP message to the sender indicating that the packet needs to be fragmented. This message, along with other techniques, can be used to determine the MTU. This value can vary depending on the path your packets take.

For the following example, we are assuming that you are actively connected to a TCPIP network.

Method for determining MTU

I. From the NetScanTools Ping tab, press the "setup" button.
II. Set the following values:
- Time Between Packets: 200
- Packet Timeout: 5000 for internet via ISP, 1000 for Intranet
- Packet TTL: 64
- Number of Packets Sent: 5
- Packet Length: 64
- Don't Fragment Packets checkbox MUST BE CHECKED

I. Select a host the you know you can reach with Ping, like www.nwpsw.com, and press the Ping button.
II. Increase the Base Packet Length several hundred bytes at a time, until you no longer receive a type 0 response. Then narrow it down to the highest byte count just before you no longer receive the type 0 response.
III. Calculate the MTU using the method below after you have determined the largest packet you can send.

How to calculate the link layer MTU once you have determined the largest packet you can send

Take the number of bytes in the results display, add 20 for the IP header and 8 for the ICMP header and you have the link layer MTU between your computer and the other host system. For Windows NT 4.0 on an ethernet system, this value will typically be 1500 (1472 data + 20 IP Header + 8 ICMP header).

NOTE: Some ISPs may limit the ICMP data packet byte count, such as to 64 bytes, in an effort to reduce exposure to denial of service attacks.

See Also...

Ping
Usage Tips

ICMP Packet Types

This is a brief overview of some of the more common types of ICMP packets sent and received by NetScanTools. Each type may have one or more subtypes called codes. In results reporting, NetScanTools functions will report the ICMP type followed by a colon character, then the code with a human readable explanation.

Type 0 - Echo. This packet is used by features like Ping or NetScanner to test the connectivity between your computer and a target host.
Type 8 - Echo Reply. This packet is sent in response to a Type 0 Echo packet by a target host.
Type 3 - Destination Unreachable. This packet, which has several codes, is sent to a host when the router or host is unable to deliver a datagram to its intended target.
Type 4 - Source Quench. This packet is sent to a host when the target is unable to keep up with the packets coming from the source system. It requests the source host to reduce the rate of data transmission.
Type 5 - Redirect. This packet, which has several codes, is used to tell a source host to redirect its transmissions to a different gateway. This packet contains the address of the correct gateway.
Type 11 - Time Exceeded. This is sent by a router or gateway when it finds that the TTL parameter has reached zero. The packet is sent to the source host and it includes the IP address of the router that sent it. This packet type is seen as the intermediate hops in TraceRoute.
Type 12 - Parameter Problem. This packet is sent to a source host if the datagram was discarded by the gateway or host due to a problem with the header parameters.
Type 13, 14 - Timestamp and Timestamp Reply. These packets are used to help determine the time it takes for systems to communicate with each other.
Type 15, 16 - Information Request and Information Reply. A now obsolete method of determining what network a host resides on.
Type 17, 18 - Address Mask Request and Address Mask Reply. This packet set is used to determine the subnet mask for a target host.

See Also...
NetScanner
Ping
TraceRoute

Listing all computers in a domain--(zone transfer)

Background

Last week's topic was about locating an Authoritative Name Server. Once you know the Authoritative Name Server for a domain, you can usually get a list of all computers recorded in that DNS for the domain.

For the following example, you must be actively connected to a TCPIP network PRIOR to starting NetScanTools.

STEP 1: Finding the Authoritative Nameserver for a Domain.

I. Start NetScanTools.

II. On the Name Server Lookup tab, press the Setup... button, check to be sure that a name server IP address or hostname is entered in the Current Server edit box and select NS (Name Server) for query type. Then Press OK to close. (NOTE: NetScanTools makes every attempt at automatically determining the default name server for your computer and places it in the Current Server box)

III. On the Name Server Lookup tab, enter a domain name like nwpsw.com and press the NSLOOKUP button.

IV. You should see the results showing the Authoritative Name Server(s) as shown below.

```
Looking up [nwpsw.com]
Server: NS2.NETDIRECT.NET
Address: 204.120.164.4


Non-authoritative answer:
nwpsw.com nameserver = NS2.resolver.net
nwpsw.com nameserver = NS1.resolver.net


Authoritative answers can be found from:
NS2.resolver.net internet address = 207.137.171.3
NS1.resolver.net internet address = 207.137.72.3


[End Query]
------------------------------------------------------------------------
```

I. Now copy NS1.resolver.net or NS2.resolver.net to the clipboard, and go back to the Setup dialog.

II. Enter either of those name servers into the current server edit box, select SOA for query type and press OK.

III. On the Name Server Lookup tab, enter nwpsw.com and press the NSLOOKUP button.

IV. You should see the results showing the Start of Authority Name Server (origin entry) as shown below.

```
Looking up [nwpsw.com]


Server: NS1.resolver.net
Address: 207.137.72.3


nwpsw.com
origin = NS1.resolver.net
mail addr = postmaster.resolver.net
serial = 1121226758
refresh = 10800(3 hours)
retry = 3600(1 hour)
expire = 5184000(60 days)
minimum ttl = 86400(1 day)
nwpsw.com nameserver = NS1.resolver.net
nwpsw.com nameserver = NS2.resolver.net
NS1.resolver.net internet address = 207.137.72.3
NS2.resolver.net internet address = 207.137.171.3


[End Query]

------------------------------------------------------------------------
```

STEP 2: Using the Authoritative Nameserver for a Domain with List Domain.

I. On the Name Server Lookup tab, press the Setup... button, and enter the hostname or IP address of one of the Authoritative Name Servers in the Current Server edit box. (In this example it would be: NS1.resolver.net or NS2.resolver.net) Then Press OK to close.

II. On the Name Server Lookup tab, enter a domain name like nwpsw.com and press the List Domain button.
III. After a little waiting, you should see domain listed--this can be very large depending on the domain--several thousand records.

Typical output:

```
Listing domain [nwpsw.com]

Server: NS1.resolver.net
Host or domain name Resource Record Info.
nwpsw.com. SOA NS1.resolver.net postmaster.resolver.net. (1121226758
10800 3600 5184000 86400)
nwpsw.com. NS NS2.resolver.net
nwpsw.com. NS NS1.resolver.net
nwpsw.com. MX 8 mail.nwpsw.com
nwpsw.com. A 207.137.171.253
mail A 209.75.46.2
ftp MX 8 mail.nwpsw.com
ftp A 207.137.171.253
www MX 8 mail.nwpsw.com
www A 207.137.171.253
nwpsw.com. SOA NS1.resolver.net postmaster.resolver.net. (1121226758
10800 3600 5184000 86400)
Received 11 records.

[End Query]
```

ERROR CONDITIONS. If you get a listing that looks like this:

```
Listing domain [nwpsw.com]

Server: isumataq.eskimo.com
Host or domain name Resource Record Info.
Received 0 records.

[End Query]
```

Then you have the wrong DNS (not an Authoritative DNS) for that domain. OR, that DNS you have selected has been programmed to reject NetScanTools list request because your IP address is not on the list of allowed computers for Zone Transfers--try another of the Auth Servers for that domain--most domains have more than one.

See Also...
List Domain
Name Server Lookup
NSLOOKUP
Usage Tips

MX Record Example

Background

Many large corporations and ISPs use email addresses similar to user@someBigCompany.com. Unfortunately someBigCompany.com is just an email alias meaning the email is actually handled by one or more mail exchange machines like smtp.someBigCompany.com. Once you have the actual MX machine name, you can use Finger on user@smpt.someBigCompany.com with much better success. How do you use NetScanTools to find out the real name of the mail machine that handles the email?

For the following example, you must be actively connected to a TCPIP network PRIOR to starting NetScanTools.

Getting the MX machine name.

I. Start NetScanTools.
II. On the Name Server Lookup tab, press Adv Qry Setup.
III. For Query Type, select MX and click OK.
IV. Enter nwpsw.com and press Adv Query. Note: your name server will be different.

```
Looking up [nwpsw.com]

Server: isumataq.eskimo.com
Address: 204.122.16.31

nwpsw.com preference = 8, mail exchanger = mail.nwpsw.com
nwpsw.com nameserver = NS1.resolver.net
nwpsw.com nameserver = NS2.resolver.net
mail.nwpsw.com internet address = 209.75.46.2
NS1.resolver.net internet address = 207.137.72.3
NS2.resolver.net internet address = 207.137.171.3

[End Query]
```

The mail exchanger (MX record) is listed. Many times you will get multiple mail exchangers with varying numerical preferences. The MX record with the lowest preference number is the one that SMTP mail programs try first, followed by the next lowest number.

See Also...

MX Record
NSLOOKUP
Usage Tips

NSLOOKUP

About

NSLOOKUP is derived from and functions similarly to the UNIX utility of the same name. The purpose of NSLOOKUP is to query DNS[92] name servers for specific record types. Adv Qry Setup allows you to set the parameters to use when performing the query.

Information Returned by this Feature

NSLOOKUP queries a selected DNS for specific record entries, such as A, MX, NS, PTR, about a hostname[93], domain name[94] or IP address[95]. This assumes that the selected DNS contains information about the hostname, domain name or IP address in question.

Setup

To use NSLOOKUP, you must first set the Adv Qry Setup options to the records you are interested in, and the current server you wish to work with. The current server must be a reliable, accessible DNS. For queries involving general hosts on the Internet, your DNS will most likely be one that has general access to the Internet. If you can only access DNS behind a firewall, be aware that unless the DNS is updated with information from outside the firewall, the only information it will contain are records relating to hosts behind the firewall.

General Rules of Operation

- SOA is the Start of Authority which basically means the DNS which contains the master records identifying computers that belong to a domain. It may have one or more mirrors. If you want to do a List Domain you must set the current server to the SOA for the domain you are interested in.
- If you have a hostname or a domain name that you want information about, you can use just about any of the record query types.
- If you have an IP Address, you must use either the A record query or the PTR record query. Any other selections with an IP address will result in an error message.

Examples of Common Queries

A Record - Address record.
ANY Record - Wild card record retrieval.
CNAME Record - Canonical name record (alias).
MX Record - Mail Exchange record.
NS Record - Name Server record.
PTR Record - Reverse DNS pointer record.
SOA Record - Start of Authority record.

See Also...

Simple Query

[92] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.

[93] Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

[94] Domain Name is the name of the domain that a group of computer systems are assigned to. netscantools.com or nwpsw.com are domain names.

[95] Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

A Record

This is an example of using the A record DNS[96] query type with NSLOOKUP. For this example, we will assume that you have selected a current accessible DNS server, and that the following Adv Qry Setup options are set (all other options are at default settings):

- **Retries** = 1
- **Timeout** = at least 10 seconds

A Example

The A record query is used to translate an IP address to a hostname. If you enter anything other than an IP address such as a hostname or domain name, you will get an error if this record query type is selected.

- In the Adv Qry Setup dialog, set the Query Type to the A selection. Press OK and wait for the DNS you have selected to be acknowledged.
- Enter the IP address of the host for which you want find the Forward DNS record name. Example: **10.1.2.3**
- Press NSLOOKUP.

If the IP address has a corresponding hostname entry in the DNS, you will see a message similar to this:

Successful IP to Hostname Translation Message

```
Looking up [10.1.4.77]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

Name:    sg1.nwpsw.com
Address:  10.1.4.77

[End Query]
```

If the IP address does not have a hostname, then you will see a message similar to this one or a timeout message:

Unsuccessful IP to Hostname Translation Message

```
Looking up [10.1.4.77]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** NS1.SPRINTLINK.NET can't find 10.1.4.77: Non-existent host/domain

[End Query]
```

Timeout Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** NS1.SPRINTLINK.NET can't find nwpsw.com: No response from server

[End Query]
```

See Also...
NSLOOKUP
PTR Record

[96] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.

ANY Record

This is an example of using the ANY record DNS[97] query type with NSLOOKUP. For this example, we will assume that you have selected a current accessible DNS server, and that the following Adv Qry Setup options are set (all other options are at default settings):

- **Retries** = 1
- **Timeout** = at least 10 seconds

ANY Example

The best starting point for a domain name or hostname query is the ANY record query. It will usually return information about the authoritative and non-authoritative hosts for the hostname or domain and it will frequently return other helpful information like MX records as a bonus.

- In the Adv Qry Setup dialog, set the Query Type to the ANY selection. Press OK and wait for the DNS you have selected to be acknowledged.
- Enter the hostname (ex. www.nwpsw.com) or domain name (ex. nwpsw.com) which you would like information about.
- Press NSLOOKUP.

If the DNS has information about the host or domain you will see a message similar to this:

Successful ANY Retrieval Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

Non-authoritative answer:
nwpsw.com  nameserver = NS1.SIMPLENET.NET
nwpsw.com  nameserver = NS2.SIMPLENET.NET

Authoritative answers can be found from:
nwpsw.com  nameserver = NS1.SIMPLENET.NET
nwpsw.com  nameserver = NS2.SIMPLENET.NET
NS1.SIMPLENET.NET     internet address = 209.132.1.21
NS2.SIMPLENET.NET     internet address = 209.132.2.21

[End Query]
```

If there is no information available, you will most likely see an authoritative response message or a timeout message:

Authoritative Response Message:

```
Looking up [netscantools.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** NS1.SPRINTLINK.NET can't find netscantools.com: Non-existent host/domain

[End Query]
```

Timeout Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** NS1.SPRINTLINK.NET can't find nwpsw.com: No response from server
```

[97] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.


```
[End Query]
```

The information you get will vary depending on the type of information that the DNS has available for your query. Sometimes a DNS will return only the non-authoritative and/or the authoritative DNS hostnames. Other records you will commonly see are the SOA record and MX records.

See Also...
NSLOOKUP

CNAME Record

This is an example of using the CNAME record DNS[98] query type with NSLOOKUP. For this example, we will assume that you have selected a current accessible DNS server, and that the following Adv Qry Setup options are set (all other options are at default settings):

- **Retries** = 1
- **Timeout** = at least 10 seconds

CNAME Example

The CNAME record query is used to translate a hostname to any canonical names (aliases) it may have.

- In the Adv Qry Setup dialog, set the Query Type to the CNAME selection. Press OK and wait for the DNS you have selected to be acknowledged.
- Enter the hostname for which you want find the CNAME records. Example: www.cnn.com
- Press NSLOOKUP.

If the hostname has a corresponding CNAME entry in the DNS, you will see a message similar to this:

Successful CNAME Retrieval Message

```
Looking up [www.cnn.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

Non-authoritative answer:
www.cnn.com   canonical name = cnn.com

Authoritative answers can be found from:
<snip>

[End Query]
```

If the hostname does not have a CNAME entry, then you will see a message similar to this one or a timeout message:

Unsuccessful CNAME Message

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

nwpsw.com
     origin = ns1.simplenet.net
     mail addr = postmaster.simplenet.net
     serial = 1254287052
     refresh = 10800(3 hours)
     retry   = 3600(1 hour)
     expire  = 5184000(60 days)
     minimum ttl = 28800(8 hours)

[End Query]
```

If there are no CNAME records available, the DNS is directing you to the SOA Record for the domain for the most accurate records.

Timeout Message:

```
Looking up [www.somehostsomewhere.com]
```

[98] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.


```
Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** NS1.SPRINTLINK.NET can't find www.somehostsomewhere.com: No response from server

[End Query]
```

See Also...
NSLOOKUP

MX Record

This discussion provides an example of using the MX record DNS[99] query type with NSLOOKUP. For this example, we will assume that you have selected a current accessible DNS server, and that the following Adv Qry Setup options are set (all other options are at default settings):

- **Retries** = 1
- **Timeout** = at least 10 seconds

MX Example

The MX record query type is use to access information about the mail exchange computer(s) for a domain. This query will return the actual hostname(s) computers running the SMTP (Simple Mail Transfer Protocol) service.

- In the Adv Qry Setup dialog, set the Query Type to the MX selection. Press OK and wait for the DNS you have selected to be acknowledged.
- Enter the domain name (ex. nwpsw.com) which you would like information about.
- Press NSLOOKUP.

Successful MX Retrieval Message:

If the DNS has information about the domain you will see a message similar to this:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

nwpsw.com  preference = 100, mail exchanger = SG1.NWPSW.COM
nwpsw.com  preference = 50, mail exchanger = MX2.NWPSW.COM
nwpsw.com  preference = 10, mail exchanger = MX1.NWPSW.COM
SG1.NWPSW.COM                internet address = 10.3.66.8
MX2.NWPSW.COM                internet address = 10.3.66.8
MX1.NWPSW.COM                internet address = 10.3.66.8

[End Query]
```

If there is no information available, you will most likely see a message indicating no records available, a timeout or an SOA record:

No Records Available Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** No mail exchanger (MX) records available for nwpsw.com

[End Query]
```

Non-authoritative SOA Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

nwpsw.com
     origin = ns1.simplenet.net
     mail addr = postmaster.simplenet.net
     serial = 1254287052
```

[99] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.


```
     refresh = 10800(3 hours)
     retry   = 3600(1 hour)
     expire  = 5184000(60 days)
     minimum ttl = 28800(8 hours)

[End Query]
```

Timeout Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** NS1.SPRINTLINK.NET can't find nwpsw.com: No response from server

[End Query]
```

See Also...
MX Record Example
NSLOOKUP

NS Record

This discussion provides an example of using the NS record DNS[100] query type with NSLOOKUP. For this example, we will assume that you have selected a current accessible DNS server, and that the following Adv Qry Setup options are set (all other options are at default settings):

- **Retries** = 1
- **Timeout** = at least 10 seconds

NS Example

Every domain or host within a domain has its name to IP address mapping stored in a Name Server. The hostname is for the convenience of human users---computers use the IP addresses. The NS record query is used to gain a list of both Authoritative and non-Authoritative (backup) name servers for a domain or host.

- In the Adv Qry Setup dialog, set the Query Type to the NS selection. Press OK and wait for the DNS you have selected to be acknowledged.
- Enter the domain name (ex. nwpsw.com) or hostname which you would like information about.
- Press NSLOOKUP.

Successful NS Retrieval Message:

If the DNS has information about the domain you will see a message similar to this:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

nwpsw.com  nameserver = ns1.simplenet.net
nwpsw.com  nameserver = ns1.simplenet.net
ns1.simplenet.net     internet address = 209.132.1.21
ns1.simplenet.net     internet address = 209.132.1.21

[End Query]
```

If there is no information available, you will most likely see a message indicating no records available, a timeout or a SOA record:

No Records Available Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** No name server (NS) records available for nwpsw.com

[End Query]
```

Non-authoritative SOA Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

nwpsw.com
     origin = ns1.simplenet.net
     mail addr = postmaster.simplenet.net
     serial = 1254287052
     refresh = 10800(3 hours)
```

[100] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.


```
     retry   = 3600(1 hour)
     expire  = 5184000(60 days)
     minimum ttl = 28800(8 hours)

[End Query]
```

Timeout Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** NS1.SPRINTLINK.NET can't find nwpsw.com: No response from server

[End Query]
```

See Also...
NSLOOKUP

PTR Record

This discussion provides an example of using the PTR record DNS[101] query type with NSLOOKUP. For this example, we will assume that you have selected a current accessible DNS server, and that the following Adv Qry Setup options are set (all other options are at default settings):

- **Retries** = 1
- **Timeout** = at least 10 seconds

PTR Example

The PTR record is similar to the A record, except for the information returned is in the reverse DNS. As with the A record, you are only allowed to enter an IP address; hostnames or domain names are not acceptable entry types. If a hostname is entered, an SOA record will normally be returned.

- In the Adv Qry Setup dialog, set the Query Type to the PTR selection. Press OK and wait for the DNS you have selected to be acknowledged.
- Enter the IP Address (ex. 10.2.3.5) which you would like information about.
- Press NSLOOKUP.

Successful PTR Retrieval Message:

If the DNS has information about the IP address you will see a message similar to this:

```
Looking up [10.122.16.44]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

44.16.122.10.in-addr.arpa name = sg2.nwpsw.com
16.122.10.in-addr.arpa name nameserver = ns1.simplenet.net
16.122.10.in-addr.arpa name nameserver = ns2.simplenet.net
ns1.simplenet.net     internet address = 209.132.1.21
ns1.simplenet.net     internet address = 209.132.1.21

[End Query]
```

If there is no information available, you will most likely see a message indicating no records available, a timeout or a SOA record:

Authoritative Answer, Non-existent IP address Message:

```
Looking up [10.3.2.59]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** NS1.SPRINTLINK.NET can't find 59.2.3.10.in-addr.arpa.: Non-existent host/domain

[End Query]
```

Server Failed to Find a Record Message:

```
Looking up [10.3.2.59]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** NS1.SPRINTLINK.NET can't find 59.2.3.10.in-addr.arpa.: Server failed

[End Query]
```

[101] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.

Non-authoritative SOA Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

nwpsw.com
     origin = ns1.simplenet.net
     mail addr = postmaster.simplenet.net
     serial = 1254287052
     refresh = 10800(3 hours)
     retry   = 3600(1 hour)
     expire  = 5184000(60 days)
     minimum ttl = 28800(8 hours)

[End Query]
```

Timeout Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** NS1.SPRINTLINK.NET can't find nwpsw.com: No response from server

[End Query]
```

See Also...
A Record
NSLOOKUP

SOA Record

This discussion provides an example of using the SOA record DNS[102] query type with NSLOOKUP. For this example, we will assume that you have selected a current accessible DNS server, and that the following Adv Qry Setup options are set (all other options are at default settings):

- **Retries** = 1
- **Timeout** = at least 10 seconds

SOA Example

The SOA or Start of Authority record is the first record entry in DNS for a particular domain. It defines several parameters about the responsible name server and the updating information for the DNS. From an information gathering standpoint, there are two important things are found in the SOA record. The first is the name of the Authoritative Name Server for that domain. The second is the email address of the responsible person for that DNS. This email address is usually presented as something like **hostmaster.nwpsw.com** by the NetScanTools report. In case you are wondering why it does not look like a normal email address, this is the way it appears in the DNS. The actual email address is **hostmaster@nwpsw.com**.

- In the Advanced Query Setup dialog, set the Query Type to the SOA selection. Press OK and wait for the DNS you have selected to be acknowledged.
- Enter the domain (ex. nwpsw.com) which you would like information about.
- Press NSLOOKUP.

Successful SOA Retrieval Message:

If the DNS has information about the domain you will see a message similar to this:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

Non-authoritative answer:
nwpsw.com
       origin = DNS1.simplenet.com
       mail addr = postmaster.simplenet.com
       serial = 1114207651
       refresh = 10800(3 hours)
       retry   = 3600(1 hour)
       expire  = 5184000(60 days)
       minimum ttl = 86400(1 day)

Authoritative answers can be found from:
nwpsw.com  nameserver = ns1.simplenet.net
nwpsw.com  nameserver = ns1.simplenet.net
ns1.simplenet.net     internet address = 209.132.1.21
ns1.simplenet.net     internet address = 209.132.1.21

[End Query]
```

If there is no information available, you will most likely see a message indicating no records available, a timeout or a SOA record:

No Records Available Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** NS1.SPRINTLINK.NET can't find nwpsw.com: Non-existent host/domain

[End Query]
```

[102] **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.

Non-authoritative SOA Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

nwpsw.com
     origin = ns1.simplenet.net
     mail addr = postmaster.simplenet.net
     serial = 1254287052
     refresh = 10800(3 hours)
     retry   = 3600(1 hour)
     expire  = 5184000(60 days)
     minimum ttl = 28800(8 hours)

[End Query]
```

Timeout Message:

```
Looking up [nwpsw.com]

Server:  NS1.SPRINTLINK.NET
Address:  204.117.214.10

*** NS1.SPRINTLINK.NET can't find nwpsw.com: No response from server

[End Query]
```

See Also...
NSLOOKUP

NetScanTools and your Hosts file

Background

Microsoft Windows NT and 95/98 both use a derivative of Berkeley Unix Sockets called 'Winsock'. Historically, it was common for Unix machines to use a 'hosts' file for rapid translation of hostnames to IP addresses and vice versa without going to a DNS or other name server. This has been carried over into the Windows TCP/IP environment, although most people don't use the hosts file. (DO NOT confuse the 'hosts' file with the LMHOSTS file. They are not the same. LMHOSTS is used for LAN Manager Hosts translation.) This week's discussion will cover the hosts file location, format and the effects of using it with NetScanTools.

Hosts file location

The hosts file is located in different places depending on the operating system you are using. Note that the hosts file DOES NOT HAVE A FILE EXTENSION. DO NOT confuse it with hosts.sam (the sample hosts file) or LMHOSTS or lmhosts.sam.

```
Windows 95/98:
%win95folder%\hosts
Note: Windows 95 does not always have a hosts file installed by default. NetScanTools will offer
to create a simple one if a hosts file is not found.

Windows NT:
%winNTfolder%\system32\drivers\etc\hosts
```

Format of the hosts file

The format of a hosts file is very simple. Each entry consists of a single IP address followed 'aliases' or human readable text names for the IP address such as www.nwpsw.com. There are some rules to a hosts file: each IP address must start in the leftmost column of the line. Only one IP address per line. Each alias must be separated from the IP address or other aliases by at least one whitespace character. Comments begin with a # symbol.

What NetScanTools does with the hosts file?

As mentioned above, some systems may not have a hosts file installed. This is mostly true for Windows 95. NetScanTools will offer to create a simple one if a hosts file is not found. The simple hosts file consists of one entry:

```
127.0.0.1 localhost
```

This is known as the *loopback address*.

NetScanTools can also add the IP address and hostname of responding computers while doing a sweep of IP addresses during NetScanner. Because the hosts file is case sensitive, each entry is added in normal and upper case. In order to use this option, you must select the corresponding checkbox on the NetScanner tab to activate it.

Problems encountered when using a hosts file

Since the hosts file is static and must be maintained by YOU, the user of your computer, there is a risk that entries in the hosts file will become out of date. For instance, if your own computer name and IP address were in the file and you changed internet providers, your IP address would change. Then NetScanTools would report your OLD IP address when it starts up if you DID NOT change the IP address in your hosts file. This is because Winsock searches the hosts file FIRST before going to any DNS or WINS to resolve the name. The same thing would also apply to any other hosts you've added using NetScanner. So, if you use the hosts file, YOU MUST MAINTAIN IT.

See Also...

NetScanner
Usage Tips

Ping and TraceRoute ICMP packet types

Background

When using NetScanTools, you may have noticed that the Ping and TraceRoute results areas include a field called 'Type'. This field is reporting the type of ICMP packet received in response to the ICMP echo request Type 8 packet NetScanTools sends. Normally, the type field will show either a Type 11 'Time Exceeded' or Type 0, Echo Reply. Other types are possible depending on the response of routers between you and the target host.

Other 'Type' Field Codes

List of common types that NetScanTools may report during Ping or TraceRoute:

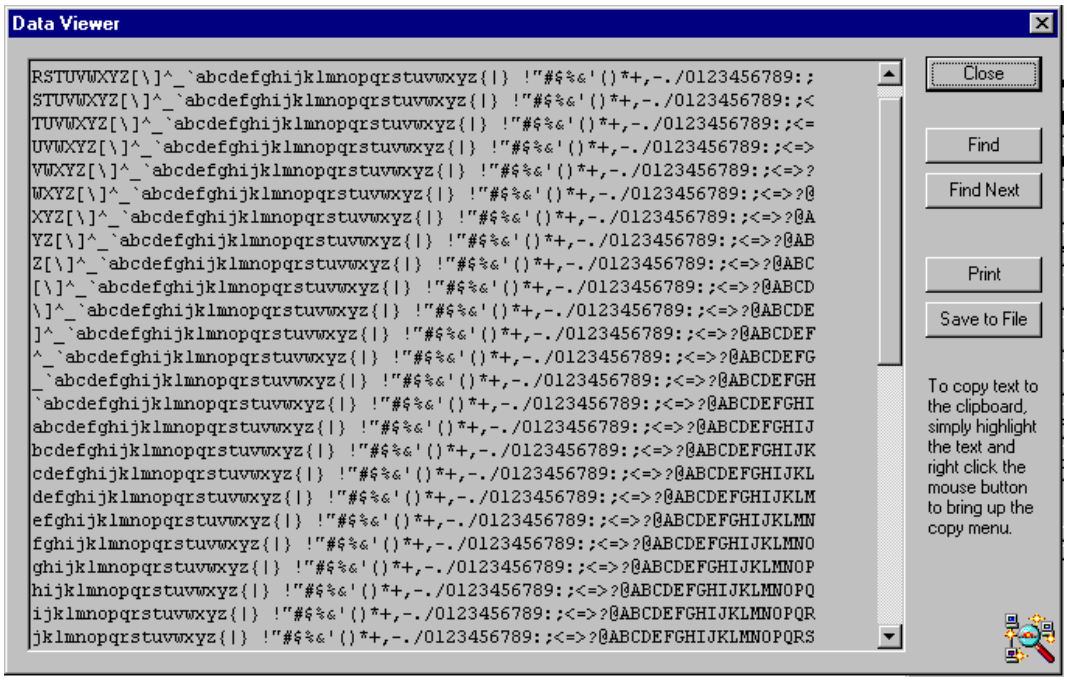
- 0 - Echo Reply - this is sent back by the target host we were trying to reach.
- 3 - Destination Unreachable - this comes in several flavors or 'Codes', some of which you won't see using NetScanTools:
  - 0 - Net Unreachable
  - 1 - Host Unreachable
  - 2 - Protocol Unreachable
  - 3 - Port Unreachable
  - 4 - Fragmentation needed and Don't Fragment was set
  - 5 - Source Route Failed
  - 6 - Destination Network Unknown
  - 7 - Destination Host Unknown
  - 8 - Source Host Isolated
  - 9 - Communication with Destination Network is Administratively Prohibited
  - 10 - Communication with Destination Host is Administratively Prohibited
  - 11 - Destination Network Unreachable for Type of Service
  - 12 - Destination Host Unreachable for Type of Service
- 4 - Source Quench - unlikely, but the router wants NetScanTools to stop sending ICMP packets so quickly.
- 11- Time Exceeded - sent to us by routers along the way to our target host. It means that our ICMP echo request packet expired.
- 12- Parameter Problem - the packet was corrupted when received by that router.

See Also...

Ping
TraceRoute
Usage Tips

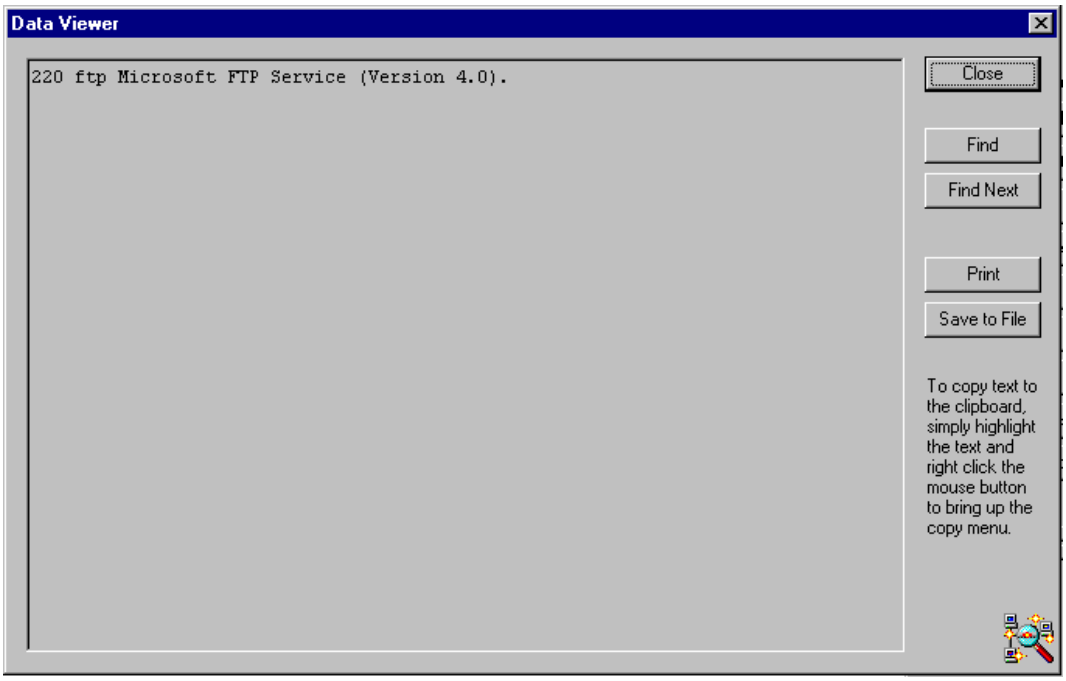
Port Probe Example 1

Connection to a Chargen Server. Back to Port Probe.



Port Probe Example 2

Connection to an FTP port. Back to Port Probe.



Public NTP Primary Time Servers

Last update: 21 January 2001 UTC

Active Servers

I. AU ntp.cs.mu.OZ.AU (128.250.36.2)
Location: The University of Melbourne, Melbourne Australia.
Geographic Coordinates: 37:48:06S 144:57:44E
Synchronization: NTP V3 primary (GPS clock), Sun Sparc2/SunOS 4.1.4
Service area: Australia, New Zealand, PACCOM (by prior arrangement)
Access policy: open access, please limit to two peer hosts per site
Contact: David Hornsby (ntp@cs.mu.OZ.AU)

II. AU ntp.marine.csiro.au (140.79.17.101)
Location: CSIRO Marine Laboratories, Hobart, Tasmania, Australia
Geographic Coordinates: 42:53:14S, 147:20:18E
Synchronization: NTP V3 primary (TrueTime XL-DC GPS clock), SGI/Unix
Service Area: AARNet
Access Policy: open access
Contact: Paul Tildesley (Paul.Tildesley@marine.csiro.au)
Note: ntp is an alias and the IP address may change; please use DNS.

III. AU ntp.mel.nml.CSIRO.AU (138.194.21.154)
Location: CSIRO Division of Materials Science and Technology, Melbourne, Australia.
Geographic Coordinates: 37:54:25S 145:08:05E
Synchronization: NTP V4, primary clock is a HP 5071A Caesium Beam Frequency Standard (synchronized to UTC Australia via a common view GPS link) via a custom interface, backup is a Truetime GPS receiver, Linux
Service Area: AARNet
Access Policy: open access
Contact: time@tip.csiro.au
Note: This NTP server is operated by the CSIRO National Measurement Laboratory, Sydney, Australia.

IV. AU ntp.nml.csiro.au (130.155.98.1)
Location: CSIRO National Measurement Laboratory, Sydney, Australia.
Geographic Coordinates: 33:46:58S 151:09:06E
Synchronization: NTP V4, primary clock is a HP 5071A Caesium Beam Frequency Standard (designated as UTC Australia) via a custom interface and a Leitch CSD-5300 Master Clock System Driver, backup clocks are a Truetime GPS receiver and a Hewlett Packard GPS receiver, Linux
Service Area: AARNet
Access Policy: open access
Contact: time@tip.csiro.au

V. AU ntp.per.nml.csiro.au (130.95.156.206)
Location: Physics Department,University of WA, Perth, Australia.
Geographic Coordinates: 31:58:43S 115:49:00E
Synchronization: NTP V4, primary clock is a rubidium oscillator (synchronized to UTC Australia via a common view GPS link) via a custom interface, backup is a Motorola UT Oncore GPS receiver, Linux
Service Area: AARNet
Access Policy: open access
Contact: time@tip.csiro.au
Note: This NTP server is operated by the CSIRO National Measurement Laboratory, Sydney, Australia.

VI. BR ntp1.rnp.br (200.19.119.69)
Location: Brazilian Research Network/Rede Nacional de Pesquisa (RNP)
Geographic Coordinates: 15=B0 48.275963' S, 47=B0 52.904663' N, 1101.146m (WGS-84)
Synchronization: NTP V4 Primary (Trimble Palisade GPS), FreeBSD/Unix
Service Area: Brazil
Access Policy: Open access to stratum 1, stratum 2 within Brazilian Research Network (RNP). Others by prior arrangement only.
Contact: ntp-admin@rnp.br

VII. CA clock.cmc.ec.gc.ca
Location: Canadian Meteorological Centre, Dorval, Québec, Canada
Synchronization: NTP V3 primary (GOES OM/DC-468 clock), HP-UX/Unix
Service Area: Econet (Environment Canada national network)
Access Policy: open within Econet. Outside by prior arrangement only.
Contact: (ntp-admin@cmc.ec.gc.ca)

VIII. CA clock.uregina.ca (142.3.100.2)

Location: University of Regina, Regina, Saskatchewan, Canada
Geographic Coordinates: 50:25N , 104:35W
Synchronization: NTP V4 Primary (GPS clock), PC/FreeBSD
Service Area: SASK#net, CA*net, Canada
Access Policy: open to stratum2 time servers, others by arrangement.
Contact: Mark Haidl (timekeeper@uregina.ca)
Note: for reliable access please notify with IP of your server

IX. CA tick.usask.ca (128.233.3.100)
Location: University oc Saskatchewan, Saskatoon, Saskatchewan, SK, Canada
Geographic Coordinates: 52:08:01N,106:38:11W
Synchronization: NTP V3 Primary (GOES clock), DEC Mips/Unix
Service Area: SASK#net, CA*net, Canada
Access Policy: open access, prior arrangment required
Contact: Alfred Hovdestad (alfred.hovdestad@usask.ca)
Note: priority given to local regional sites
Note: tick.usask.ca and tock.usask.ca share a single GOES receiver

X. CA tock.usask.ca (128.233.3.101)
Location: University oc Saskatchewan, Saskatoon, Saskatchewan, SK, Canada
Geographic Coordinates: 52:08:01N,106:38:11W
Synchronization: NTP V3 Primary (GOES clock), DEC Mips/Unix
Service Area: SASK#net, CA*net, Canada
Access Policy: open access, prior arrangment required
Contact: Alfred Hovdestad (alfred.hovdestad@usask.ca)
Note: priority given to local regional sites
Note: tick.usask.ca and tock.usask.ca share a single GOES receiver

XI. CH swisstime.ethz.ch (129.132.2.21)
Location: Integrated Systems Laboratory, Swiss Fed. Inst. of Technology, CH 8092 Zurich, Switzerland
Geographic Coordinates: 47:23N, 8:32E
Synchronization: NTP primary (DCF77 clock), Sun-4/SunOS 4.1.3
Service Area: Switzerland/Europe
Access Policy: open access
Contact: Andi Karrer (time@iis.ee.ethz.ch)

XII. CL ntp.dgf.uchile.cl (146.83.8.200)
Location: Dpto. Geofísica, Universidad de Chile. Santiago, Chile.
Geographic Coordinates: Lat: 33° 27.19'S. Lon: 70° 39.70'W. Alt: 533m.
Synchronization: NTP V3 primary (GOES OM/DC-468 clock), SunSparc10/SunOS 4.1.3.
Service area: REUNA and interconnected networks, Chile.
Access Policy: open access, please send a message to notify.
Contact: Gonzalo Pérez (gperez@dgf.uchile.cl)
Note: ntp is an alias and the IP address may change; please use DNS.

XIII. DE ntp0.fau.de (131.188.34.75)
Location: University Erlangen-Nuernberg, D-91058 Erlangen, FRG
Geographic Coordinates: 49.573N 11.028E (from Meinberg GPS 166)
Synchronization: NTP V3 primary (GPS receiver (<<1us)), Sun SS12/Unix SunOS 5.6
Service Area: Germany/Europe
Access Policy: open access, pick one of ntp{0,1,2}.fau.de
Contact: The Timekeepers (time@informatik.uni-erlangen.de) Note: IP addresses are subject to change; please use DNS

XIV. DE ntp1.fau.de (131.188.34.45)
Location: University Erlangen-Nuernberg, D-91058 Erlangen, FRG
Geographic Coordinates: 49.573N 11.028E (from Meinberg GPS 166)
Synchronization: NTP V3 primary (DCF77 PZF receiver (<50us)), Sun E3000 SunOS 5.6
Service Area: Germany/Europe
Access Policy: open access, pick one of ntp{0,1,2}.fau.de
Contact: The Timekeepers (time@informatik.uni-erlangen.de)
Note: IP addresses are subject to change; please use DNS

XV. DE ntp2.fau.de (131.188.34.107)
Location: University Erlangen-Nuernberg, D-91058 Erlangen, FRG
Geographic Coordinates: 49.573N 11.028E (from Meinberg GPS 166)
Synchronization: NTP V3 primary (DCF77 PZF receiver (<50us)), Sun SS10/SunOS 5.6
Service Area: Germany/Europe
Access Policy: open access, pick one of ntp{0,1,2}.fau.de
Contact: The Timekeepers (time@informatik.uni-erlangen.de)

Note: IP addresses are subject to change; please use DNS

XVI. DE ntpa2.kph.uni-mainz.de (134.93.132.118)
Location: Johannes Gutenberg-University, Institut fuer Kernphysik, Mainz, Germany
Synchronization: NTP V3 with DCF77 receiver, K6/Linux
Service Area: University of Mainz and all European Community Countries ONLY! Exceptions are only given to Switzerland, Poland and Czech Republic.
Access Policy: Open access for stratum 2 servers if e-mail is sent in order to notify. Users from outside the service area will be ignored if the contact is kept alive for a longer period. Stratum >2 servers will be ignored, too. Computers, connected via dialin or computers that have unresolvable IP-numbers will be ignored from every location! Consult http://wwwa2.kph.uni-mainz.de/ntpa2/ for details!
Contact: wwwa2@kph.uni-mainz.de

XVII. DE ntps1-0.cs.tu-berlin.de (130.149.17.21)
Location: Technische Universitaet Berlin, D-10587 Berlin, FRG
Geographic Coordinates: 52.518N 13.326E
Synchronization: NTP V3 primary (Meinberg GPS 166), Sun 4/65 SunOS4.1.3
Service Area: Germany/Europe
Access Policy: open access
Contact: Gerard Gschwind (gg@cs.tu-berlin.de)

XVIII. DE ntps1-0.uni-erlangen.de (131.188.1.40)
Location: University Erlangen-Nuernberg, D-91058 Erlangen, FRG
Geographic Coordinates: 49.573N 11.028E (from Meinberg GPS 166)
Synchronization: NTP V3 primary (GPS receiver (<<1us)), Sun SS2/Unix SunOS 4.1.3
Service Area: Germany/Europe
Access Policy: open access, pick one of ntps1-{0,1,2}.uni- erlangen.de
Contact: Frank Kardel, Rainer Pruy (time@informatik.uni-erlangen.de)

XIX. DE ntps1-1.cs.tu-berlin.de (130.149.17.8)
Location: Technische Universitaet Berlin, D-10587 Berlin, FRG
Geographic Coordinates: 52.518N 13.326E
Synchronization: NTP V3 primary (Meinberg GPS 166), SunS10-402 SunOS5.4
Service Area: Germany/Europe
Access Policy: open access
Contact: Gerard Gschwind (gg@cs.tu-berlin.de)

XX. DE ntps1-1.rz.Uni-Osnabrueck.DE (131.173.17.7)
Location: University of Osnabrueck, D-49069 Osnabrueck, FRG
Synchronization: NTP V3 primary (DCF77 clock), Sun/Unix
Service Area: Germany/Europe
Access Policy: open access
Contact: Gernot Skalla (timeadm@Uni-Osnabrueck.DE)

XXI. DE ntps1-1.uni-erlangen.de (131.188.1.45)
Location: University Erlangen-Nuernberg, D-91058 Erlangen, FRG
Geographic Coordinates: 49.573N 11.028E (from Meinberg GPS 166)
Synchronization: NTP V3 primary (DCF77 PZF receiver (<50us)), Sun 4/690/SunOS 4.1.3
Service Area: Germany/Europe
Access Policy: open access, pick one of ntps1-{0,1,2}.uni- erlangen.de
Contact: Frank Kardel, Rainer Pruy (time@informatik.uni-erlangen.de)

XXII. DE ntps1-2.uni-erlangen.de (131.188.1.31)
Location: University Erlangen-Nuernberg, D-91058 Erlangen, FRG
Geographic Coordinates: 49.573N 11.028E (from Meinberg GPS 166)
Synchronization: NTP V3 primary (DCF77 PZF receiver (<50us)), Sun 4/490/SunOS 4.1.3
Service Area: Germany/Europe
Access Policy: open access, pick one of ntps1-{0,1,2}.uni- erlangen.de
Contact: Frank Kardel, Rainer Pruy (time@informatik.uni-erlangen.de)

XXIII. DE ptbtime1.ptb.de (194.95.250.35)
Location: Physikalisch-Technische Bundesanstalt (PTB), Braunschweig, Germany
Synchronization: NTP V3 primary (Primary standards CS1, CS2), HP9000/744/HP-UX
Service Area: Germany/Europe, others by arrangement
Access Policy: open access, please send a message to notify.
Contact: Dieter Sibold, Ronald Scheffler (ntp-admin@ptb.de)0
Note: ptbtime1.ptb.de is an alias and the IP address may change; please use DNS.

XXIV. DE ptbtime2.ptb.de (194.95.250.36)

Location: Physikalisch-Technische Bundesanstalt (PTB), Braunschweig, Germany
Synchronization: NTP V3 primary (PTB's primary standards CS1, CS2), HP9000/744/HP-UX
Service Area: Germany/Europe, others by arrangement
Access Policy: open access, please send a message to notify.
Contact: Dieter Sibold, Ronald Scheffler (ntp-admin@ptb.de)
Note: ptbtime2.ptb.de is an alias and the IP address may change; please use DNS.

XXV. DE rustime01.rus.uni-stuttgart.de (129.69.1.153)
Location: Computer Center University of Stuttgart, D-70550 Stuttgart, Germany
Geographic Coordinates: 48:47N, 9:10E
Synchronization: NTP V3 primary (Meinberg DCF-77 PZF 535/TCXO), IBM RS6000-250, AIX 4.x
Service Area: Germany/Europe
Access Policy: open, preferred for stratum-2 servers providing synchronization to local networks; appreciate email notification
Contact: Walter Wehinger (wehinger@rus.uni-stuttgart.de)

XXVI. FR canon.inria.fr (192.93.2.20)
Location: INRIA, Rocquencourt (near Paris), France
Synchronization: NTP V3 primary (GPS), Datum TymServe 2100L
Service Area: France/Europe
Access Policy: open access, please send a message to notify
Contact: ntp-adm@inria.fr
Note: We use a Datel RCH208 clock with SER024 V24 interface.

XXVII. FR chronos.cru.fr
Location: University of Rennes 1, Britany, France
Synchronization: NTP V3, Datum TymServe 2100L with GPS
Service Area: France/Europe
Access Policy: open access to stratum-2 servers, send a message to notify
Contact: timemaster@cru.fr
Note: use DNS for IP address

XXVIII. FR ntp-p1.obspm.fr
Location: LPTF - Observatoire de Paris, France
Synchronization: NTP V3, Datum TymServe 2100 with 1PPS
Service Area: France/Europe
Access Policy: open access to stratum-2 servers, send a message to notify
Contact: lptfop@obspm.fr
Note: use DNS for IP address. Ref: 1PPS from Atomic Clock

XXIX. FR ntp-sop.inria.fr (138.96.64.10)
Location: INRIA, Sophia Antipolis (French Riviera, near Nice), France
Synchronization: NTP V3 primary (GPS), PC/Linux
Service Area: RENATER, R3T2, France/Europe
Access Policy: open access, please send a message to notify
Contact: ntp-adm@sophia.inria.fr, More help?
Note: We use a MC2 Starsync GPS EISA card

XXX. HK clock.cuhk.edu.hk (137.189.6.18)
Location: The Chinese University of Hong Kong.
Geographic Coordinates: 22:25:10N,114:12:22E
Synchronization: NTP V3 Primary (TSS-100 GPS clock)
Service Area: Hong Kong, China & South East Asia
Access Policy: open access
Contact: Nicky Leung (nicky-leung@cuhk.edu.hk)
Note: IP addresses are subject to change; please use DNS

XXXI. IT tempo.cstv.to.cnr.it (150.145.33.1)
Location: CSTV of National Research Council, Torino, Italy
Geographic Coordinates: 45:00:54N, 7:38:20.7E, 306.6H
Syncronization: NTP V3 primary (IEN CTD clock), DecSystem 5500/Ultrix 4.4
Service Area: Italy/Europe
Access Policy: open access
Contact: Fabrizio Pollastri (pollastri@cstv.to.cnr.it)
Note: information at http://www.cstv.to.cnr.it/toi

XXXII. IT time.ien.it (193.204.114.1)
Location: IEN Galileo Ferraris, Torino, Italy
Synchronization: NTP primary (Cesium Beam Frequency Standard), Sun/Unix
Service Area: Italy/Europe

Access Policy: open access
Contact: denasi@ien.it

XXXIII. JP clock.nc.fukuoka-u.ac.jp (133.100.9.2)
Location: Fukuoka university, Fukuoka, Japan
Geographic Coodinates: 130:21.81E, 33:32.87N
Synchronization: NTP V3.3 primary (GPS clock), Heliostation 400/SunOS 4.1.3
Service Area: Japan/Pacific area
Access Policy: open access
Contact: TSURUOKA Tomoaki (tsuruoka@fukuoka-u.ac.jp), YOSHIMURA Kenji (yosimura@tl.fukuoka-u.ac.jp)
Note: We use a TRAK 8810 GPS STATION CLOCK and a Furuno Electric Co.'s GN-72 GPS receiver respectively.

XXXIV. JP clock.tl.fukuoka-u.ac.jp (133.100.11.8)
Location: Fukuoka university, Fukuoka, Japan
Geographic Coodinates: 130:21.81E, 33:32.87N
Synchronization: NTP V3.3 primary (GPS clock), Heliostation 400/SunOS 4.1.3
Service Area: Japan/Pacific area
Access Policy: open access
Contact: TSURUOKA Tomoaki (tsuruoka@fukuoka-u.ac.jp), YOSHIMURA Kenji (yosimura@tl.fukuoka-u.ac.jp)
Note: We use a TRAK 8810 GPS STATION CLOCK and a Furuno Electric Co.'s GN-72 GPS receiver respectively.

XXXV. MX cronos.cenam.mx
Location: Centro Nacional de Metrologia, Queretaro, Mexico
Geographic coordinates: 20:32:9.6 N, 100:16:18 W, +1912
Synchronization: Interlock algorithm with direct 1 pps from primary
frequency standard of CENAM, UTC(CENAM)
Service Area: All Mexico and USA
Access policy: Open access
Contact: J. Mauricio Lopez R., jlopez@cenam.mx , 52 4 211 0543

XXXVI. NL ntp0.nl.net (193.67.79.202)
Location: NLnet, Amsterdam, The Netherlands
Synchronization: NTP primary (GPS), Sun/Unix SunOS 4.1.3
Service Area: The Netherlands/Europe
Access Policy: open access
Contact: beheer@nl.net

XXXVII. NL ntp1.nl.net (193.79.237.14)
Location: NLnet, Amsterdam, The Netherlands
Synchronization: NTP primary (GPS), Sun/Unix SunOS 4.1.3
Service Area: The Netherlands/Europe
Access Policy: open access
Contact: beheer@nl.net

XXXVIII. NL ntp2.nl.net (193.79.237.30)
Location: NLnet, Amsterdam, The Netherlands
Synchronization: NTP primary (GPS), Sun/Unix SunOS 4.1.3
Service Area: The Netherlands/Europe
Access Policy: open access
Contact: beheer@nl.net

XXXIX. NO time.service.uit.no
Location: The EDB Centre, University of Tromsoe, Norway
Synchronization: NTP V3 primary (GPS clock), HP-UX/Unix
Service Area: NORDUnet
Access Policy: semi-open access, prior arrangment required
Contact: (timekeeper@uit.no)

XL. NZ clock1.canterbury.ac.nz (132.181.12.13)
Location: Computer Science Department, University of Canterbury
Synchronization: NTP V4 primary (Trimble Palisade GPS), Sun/Sparc
Service Area: New Zealand
Access Policy: restricted to stratum-2 servers providing synchronization to local networks of ten or more hosts, by prior arrangement
Contact: Pete Glassenbury (pete@cosc.canterbury.ac.nz)
Note: IP addresses are subject to change; please use DNS

XLI. PL vega.cbk.poznan.pl (150.254.183.15)
Location: Astrogeodynamical Observatory, Space Research Centre, Borowiec, Poland
Synchronization: NTP V3 primary (Caesium clock), PC Pentium, RedHat Linux

Service Area: Poland/Europe
Access Policy: open access
Contact: Robert Diak (kondor@cbk.poznan.pl), Jerzy Nawrocki (nawrocki@cbk.poznan.pl)

XLII. SE time1.stupi.se (192.36.143.150)
Location: Stupi AB, Stockholm, SWEDEN
Synchronization: NTP V3 primary (Saphir Cesium Beam Standard/GPS), BSDI Unix
Service Area: SUnet, NORDUnet
Access Policy: open access
Contact: Peter Lothberg (roll@Stupi.SE)

XLIII. SE time2.stupi.se (192.36.143.151)
Location: Stupi AB, Stockholm, SWEDEN
Synchronization: NTP V4 primary (HP5071, FreeBSD)
Service Area: Europe
Access Policy: open access
Contact: roll@stupi.se (Peter Lothberg)

XLIV. SG jamtepat.singnet.com.sg (165.21.110.7)
Location: SingNet, Singapore
Geographic Coordinates: 1.292N 103.808E (GPS WGS84)
Synchronization: Datum Tymserve 2100-GPS
Service Area: STIX/Asia (outside Singapore), others by arrangement
Access Policy: port access granted by arrangement
Contact: timekeeper@singnet.com.sg

XLV. SI goodtime.ijs.si (193.2.4.2)
Location: J. Stefan Institute, Ljubljana, Slovenia
Geographic Coordinates: 46° 2.517' N, 14° 29.241' E, +363 m (WGS84)
Synchronization: NTP V4 primary (Trimble Palisade GPS), Compaq (DEC) Alpha / Tru64 Unix with MICRO_TIME kernel option
Service Area: Slovenia, European academic community, others by arrangement
Access Policy: restricted to servers providing synchronization to ten or more hosts, please send notification before regular use
Contact: Mark Martinec (timekeeper@ijs.si); More info?
Note: NTP V4 clients preferred for their lower load and better accuracy; IP address subject to change

XLVI. UK chronos.csr.net 194.35.252.7 (CNAME ntp.csr.net)
Location: Computing Systems Research Ltd. United Kingdom
Geographic Coordinates: 0:49:10W 52:14:54N (480578m 261841m)
Synchronization: NTP V4 primary (Odetics GPS), Sun/Sparc Solaris 2.6
Service Area: United Kingdom Western Europe
Access Policy: open access
Contact: C Buckingham (chrisb@csr.net)

XLVII. UK ntp2.ja.net (193.63.94.26)
Location: University of London Computer Centre, UK
Synchronization: NTP V3 primary (MSF clock), Sun/Unix
Service Area: JANET
Access Policy: closed access, see notes below.
Contact: jips-nosc@nosc.ja.net
Note: This server is part of the JANET NTP service and is available for JANET stratum-2 clients and for peering with external stratum-1 clocks. Any external stratum-1 peering requests should be emailed to the Contact address.

XLVIII. US AK ntp.alaska.edu (199.165.76.11) (CNAME ntp-ua.usno.navy.mil)
Location: University of Alaska, Fairbanks, AK (147 50 59.7W 64 51 27.3N WGS84)
Synchronization: NTP V3 primary (GPS)
Service area: Pacific Northwest, others by arrangement
Access Policy: open access for stratum 2 servers
Contact: Rich Schmidt, US Naval Observatory (res@tuttle.usno.navy.mil)

XLIX. US CA clepsydra.dec.com (16.1.0.4, 204.123.2.5)
Location: DEC Western Research Laboratory, Palo Alto, CA
Synchronization: NTP V3 primary (GPS clock), PC/BSDI 2.1
Service Area: NSFNET, BARR region
Access Policy: open access, send email to notify before using
Contact: ntp-admin@pa.dec.com
Note: The host name is an alias used only for time service.

L. US CA clock.isc.org (192.5.5.250)
Location: Internet Software Consortium, Palo Alto, CA

Geographic Coordinates: 122 9 41 W / 37 26 35 N
Synchronization: NTP primary (GOES clock), BSD UNIX
Service Area: BARRnet, Alternet-west, CIX-west
Access Policy: open access
Contact: Paul Vixie (paul@vix.com)

LI. US CA clock.sgi.com (192.48.153.74)
Location: Silicon Graphics Computer Systems, Inc., Mountain View, CA
Synchronization: NTP V3 primary (TrueTime 600 GPS/Precision Standard Time WWV), SGI Challenge L/Irix
Service Area: North America
Access Policy: open to stratum-2 time servers, others by arrangement.
Contact: Bowen Goletz, (ntp-admin@sgi.com)

LII. US CA clock.via.net (209.81.9.7)
Location: ViaNet Communications, Palo Alto, CA, USA
Synchronization: NTP V3 with Trimble Pasisade GPS receiver/FreeBSD
Service Area: All areas
Access Policy: open access
Contact: Joe McGuckin (joe@via.net)

LIII. US CA gpstime.trimble.com 206.40.88.30
Location: Sunnyvale, CA US
Synchronization: NTP primary (GPS clock), Trimble Palisade on Windows NT 4.0
Service Area: Western US
Access Policy: open access, stratum 3 or higher requested
Contact: Sven Dietrich, sven_dietrich@trimble.com or zane_brady@trimble.com

LIV. US CA montpelier.ilan.caltech.edu (131.215.254.2) CNAMES: montpelier.caltech.edu, ntp-caltech.usno.navy.mil
Location: California Institute of Technology, Pasadena, CA
Synchronization: NTP V3 primary (GPS clock)
Service area: USA Pacific timezone, others by arrangement
Access Policy: open access for stratum 2 servers
Contacts: Rich Schmidt, US Naval Observatory (res@tuttle.usno.navy.mil),
Heather Sherman, California Institute of Technology, (network@caltech.edu)

LV. US CA nist1.datum.com (63.149.208.50)
Location: Datum Inc., Bancomm-Timing Division, San Jose, California
Synchronization: ACTS dial-up using lockclock algorithm; DEC Alpha UNIX
Service Area: Primarily networks in Western US
Access Policy: Open to stratum-2 servers and others by arrangement.
Contact: Judah Levine (jlevine@boulder.nist.gov) 303 492-7785

LVI. US CA nist1.sjc.certifiedtime.com (207.126.103.204)
Location: Abovenet, San Jose, California
Synchronization: ACTS dial-up using lockclock algorithm; DEC Alpha UNIX
Service Area: Western US
Access Policy: Open to stratum-2 servers and others by arrangement
Contact: Judah Levine (jlevine@boulder.nist.gov) 303 492-7785

LVII. US CA ntp-cup.external.hp.com (192.6.38.127)
Location: Cupertino CA (SF Bay area) 37:20N/122:00W
Synchronization: NTPv3 primary, HP-UX/Palisade-GPS
Service Area: West Coast USA
Access Policy: open access
Contact: timer@cup.hp.com
Note: no need to notify for access, go right ahead!

LVIII. US CA ntp.nasa.gov (143.232.55.5)
Location: NASA Ames Research Center, Moffett Field, CA
Synchronization: NTP primary (WWVB clock), Sun/Unix
Service Area: NSFNET, BARR region, NASA NSN, DOE ESNET, DDN
Access Policy: prior permission required
Contact: clockmaster@ntp.nasa.gov

LIX. US CA tick.gpsclock.com (216.152.68.16)
Location: GPSClock.com headquarters, San Jose, CA
Geographic Coordinates: 37:16:37N, 121:53:31W
Synchronization: NTP V4 primary, GPSClock model 200 hard PPS, Linux

Service Area: US Pacific, Abovenet/PAIX region
Access Policy: Open to stratum 2 servers for 10 or more hosts, others upon request
Contacts: David Schwartz (clock@gpsclock.com)

LX. US CA tick.ucla.edu (164.67.62.194) CNAMEs: navobs1.ucla.edu, time.ucla.edu
Location: UCLA, Los Angeles, CA
Synchronization: NTP V3 primary (GPS) HP9000/747i
Service area: Pacific time zone, others on request
Access policy: open access to stratum-2 servers and to UCLA clients
Contacts: Rich Schmidt (res@tuttle.usno.navy.mil), Scott Burris (scott@cns.ucla.edu)

LXI. US CA timekeeper.isi.edu (128.9.176.30)
Location: USC Information Sciences Institute, Marina del Rey, CA
Geographic Coordinates: 33:58:49N, 118:26:20W (USGS map NAD27)
Synchronization: NTP V3 primary Datum Tymserve 2100-GPS
Service Area: CalRen2, Los Nettos region
Access Policy: open access
Contact: Information Processing Center (action@isi.edu)

LXII. US CA tock.gpsclock.com (216.152.68.20)
Location: GPSClock.com headquarters, San Jose, CA
Geographic Coordinates: 37:16:37N, 121:53:31W
Synchronization: NTP V3 primary, GPSClock model 200 hard PPS, FreeBSD
Service Area: US Pacific, Abovenet/PAIX region
Access Policy: Open to stratum 2 servers for 10 or more hosts, others upon request
Contacts: David Schwartz (clock@gpsclock.com)

LXIII. US CA usno.pa-x.dec.com (204.123.2.72) CNAME: navobs1.pa-x.dec.com
Location: Systems Research Center, Compaq Computer Corp. Palo Alto, CA (122 9 41.7 W 37 26 42.6 N WGS84)
Synchronization: NTP V3 primary (GPS)
Service area: USA Pacific and Mountain timezones, others by arrangement.
Access Policy: open access
Contact: Rich Schmidt, US Naval Observatory (res@tuttle.usno.navy.mil) Paul Flaherty, Digital Equipment Corp.(flaherty@pa.dec.com)

LXIV. US CO navobs1.usnogps.navy.mil (204.34.198.40) CNAME: tick.usnogps.navy.mil
Location: Falcon AFB, Colorado
Geographic Coordinates: 104 31 30 W, 38 48 30 N WGS84
Synchronization: NTP V3 primary (USNO Alternate Master Clock H-maser) HP9000/747i
Service area: USA Pacific and Mountain timezones, others by arrangement.
Access Policy: open access
Contact: Rich Schmidt, US Naval Observatory (res@tuttle.usno.navy.mil)

LXV. US CO navobs2.usnogps.navy.mil (204.34.198.41) CNAME: tock.usnogps.navy.mil
Location: Falcon AFB, Colorado
Geographic Coordinates: 104 31 30 W, 38 48 30 N WGS84
Synchronization: NTP V3 primary (USNO Alternate Master Clock H-maser) HP9000/747i
Service area: USA Pacific and Mountain timezones, others by arrangement.
Access Policy: open access
Contact: Rich Schmidt, US Naval Observatory (res@tuttle.usno.navy.mil)

LXVI. US CO time-a.nist.gov (129.6.15.28) New Access policy: Open only to existing users; other users please use time-b or time-c instead.

LXVII. US CO time-a.timefreq.bldrdoc.gov (132.163.135.130, 132.163.4.101)
Location: NIST Boulder Laboratories, Boulder, Colorado
Synchronization: Direct 1 pps from clock ensemble; lockclock algorithm and ACTS dial-up as backup; DEC Alpha/UNIX
Service Area: NSFnet, WESTnet
Access Policy: Open to stratum-2 servers, others by arrangement; please use only one of the servers as primary with the other as a backup.
Contact: Judah Levine (jlevine@time.nist.gov) 303 492 7785.

LXVIII. US CO time-b.timefreq.bldrdoc.gov (132.163.135.131, 132.163.4.102)
Location: NIST Boulder Laboratories, Boulder, Colorado
Synchronization: Direct 1 pps from clock ensemble; lockclock algorithm and ACTS dial-up as backup; DEC Alpha/UNIX
Service Area: NSFnet, WESTnet
Access Policy: Open to stratum-2 servers, others by arrangement; please use only one of the servers as primary with the other as a backup.
Contact: Judah Levine (jlevine@time.nist.gov) 303 492 7785

LXIX. US CO time-c.timefreq.bldrdoc.gov (132.163.135.132, 132.163.4.103)
Location: NIST Boulder Laboratories, Boulder, Colorado
Synchronization: Direct 1 pps from clock ensemble; lockclock algorithm and ACTS dial-up as backup; DEC Alpha/UNIX.
Service Area: NSFnet, WESTnet
Access Policy: Open to servers with at least 10 clients; others by arrangement. please use only one of these servers primary with the other as backup.
Contact: Judah Levine (jlevine@time.nist.gov) 303 492 7785.

LXX. US CO time-d.timefreq.bldrdoc.gov (132.163.135.133, 132.163.4.104)
Location: NIST Boulder Laboratories, Boulder, Colorado
Synchronization: interlock algorithm with direct 1 pps from clock ensemble as backup; DEC Alpha/UNIX.
Service Area: NSFnet, WESTnet
Access Policy: Used for testing and algorithm development. NOT for general use.
Contact: Judah Levine (jlevine@time.nist.gov) 303 492 7785

LXXI. US CO time.nist.gov (192.43.244.18)
Location: National Center for Atmospheric Research, Boulder, Colorado
Geographic Coordinates: 39:58:43.44N 254:43:32.5E +1840m (WGS 84)
Synchronization: ACTS dial-up with NTP backup, DEC Alpha UNIX Service Area: NSFnet, WESTnet
Access Policy: open to stratum-2 servers and others by arrangement
Contact: Judah Levine (jlevine@time.nist.gov), (303) 492-7785

LXXII. US CO utcnist.colorado.edu (128.138.140.44)
Location: JILA Laboratory, University of Colorado
Synchronization: ACTS dial-up using lockclock algorithm; DEC Alpha UNIX
Service Area: Western US
Access Policy: Open to All Colorado users, other stratum-2 servers; others by arrangement
Contact: Judah Levine (jlevine@boulder.nist.gov) 303 492-7785

LXXIII. US DC ntp2.usno.navy.mil (192.5.41.209)
Location: U.S. Naval Observatory, Washington, DC
Geographic Coordinates: 77 03 57.7W 38 55 14.1N WGS84
Synchronization: NTP V3 primary (USNO Master Clocks 1,2, and GPS)
Service area: USA Eastern timezone, others by arrangement
Access Policy: open access for stratum 2 servers
Contact: Rich Schmidt, US Naval Observatory (res@tuttle.usno.navy.mil)

LXXIV. US DC tick.usno.navy.mil (192.5.41.40)
Location: U.S. Naval Observatory, Washington, DC
Geographic Coordinates: 38:55:14.01 77:03:58.03 (GPS WGS84)
Synchronization: NTP V3 primary (USNO Master Clock 2, H-maser), HP9000/747i
Service Area: NSFNET
Access Policy: open access
Contact: Rich Schmidt (res@tuttle.usno.navy.mil)

LXXV. US DC tock.usno.navy.mil (192.5.41.41)
Location: U.S. Naval Observatory, Washington, DC
Geographic Coordinates: 38:55:14.01 77:03:58.03 (GPS WGS84)
Synchronization: NTP V3 primary (USNO Master Clock 2, H-maser), HP9000/747i
Service Area: NSFNET
Access Policy: open access
Contact: Rich Schmidt (res@tuttle.usno.navy.mil)

LXXVI. US DE mizbeaver.udel.edu (128.4.1.2)
Location: University of Delaware, Newark, DE
Geographic Coordinates: 39:40:48.425N, 75:45:02.392W (GPS WGS84)
Synchronization: NTP V4 primary (GPS clock), TrueTime NTS-200-GPS
Service Area: CAIRN, Abilene/vBNS
Access Policy: closed access, except for stratum-2 servers providing synchronization to local networks of ten or more hosts
Contact: Dave Mills <mills@udel.edu>
Note: This server does not implement the NTP control-message protocol

LXXVII. US DE ntp1.delmarva.com (138.39.7.20)
Location: Conectiv Communications, Newark DE
Synchronization: NTP primary (GPS clock), Odetics GPS Receiver and Sun Sparc 5
Service area: Cable & Wireless Network (formerly MCInet)
Access policy: open access
Contact: John K. Scoggin (john.scoggin@conectiv-comm.com)

LXXVIII. US DE ntp1.nss.udel.edu (128.175.60.175)
Location: University of Delaware, Newark, DE
Geographic Coordinates: 39:40:35.8N, 75:44:36.6W (GPS WGS 84)
Synchronization: NTP V3 Primary (GPS clock), TrueTime NTS-100-GPS
Service Area: BBN Planet SER
Access Policy: closed access, except for stratum-2 servers providing synchronization to local networks of ten or more hosts
Contact: Ron Reisor (ron@udel.edu)
Note: This server does not implement the NTP control-message protocol.

LXXIX. US DE rackety.udel.edu (128.4.1.1)
Location: University of Delaware, Newark, DE
Geographic Coordinates: 39:40:48.425N, 75:45:02.392W (GPS WGS84)
Synchronization: NTP V4 primary (GPS clock), Sun IPC/SunOS 4.1.3
Service Area: CAIRN, Abilene/vBNS
Access Policy: closed access, except for stratum-2 servers providing synchronization to local networks of ten or more hosts
Contact: Dave Mills <mills@udel.edu>

LXXX. US FL ntp-s1.cise.ufl.edu (128.227.205.3) (CNAME ntp- ufl.usno.navy.mil)
Location: University of Florida, Gainesville, FL
Synchronization: NTP V3 primary (TrueTime GPS-VME)
Service area: Eastern time zone US
Access Policy: open access for stratum 2 servers and UFL clients,others by arrangement
Contacts: Rich Schmidt, US Naval Observatory
CISE, Univ. Florida

LXXXI. US GA navobs1.gatech.edu (130.207.244.240) CNAMES: tick.gatech.edu, ntp-gatech.usno.navy.mi
Location: Georgia Institute of Technology, Atlanta, GA
Geographic Coordinates: 84 23 40.9W 33 46 30.0N WGS84
Synchronization: NTP V3 primary (GPS clock)
Service area: USA Eastern timezone, others by arrangement
Access Policy: open access for stratum 2 servers
Contacts: Rich Schmidt, US Naval Observatory (res@tuttle.usno.navy.mil),
Ray Spalding, Georgia Institute of Technology, (cc100aa@xray.oit.gatech.edu)

LXXXII. US IL ntp0.mcs.anl.gov (140.221.8.88) (CNAME ntp- anl.usno.navy.mil)
Location: Argonne National Laboratories, Chicago, IL
Synchronization: NTP V3 primary (Brandywine Syncclock32/Oncore GPS)
Service area: Central time zone US
Access Policy: open access for stratum 2 servers and ANL clients,others by arrangement
Contacts: Rich Schmidt, US Naval Observatory Bill Nickless, Argonne National Labs

LXXXIII. US IL truechimer.cso.uiuc.edu (128.174.5.58)
Location: University of Illinois, Urbana-Champaign, IL
Synchronization: NTP V3 primary (WWVB clock), IBM-RS6000/250
Service Area: CICNET, Midwest, NCSA region
Access Policy: closed access except for peers that meet the three conditions outlined in the "Time Servers" section of this file. State agreement with those conditions in notification message. All others may use the ntp-{0,1,2}.cso.uiuc.edu stratum 2 servers.
Contact: Charley Kline (kline@uiuc.edu)
Note: truechimer is a DNS CNAME. The host with the WWVB clock will always have the truechimer alias.

LXXXIV. US IN darkcity.cerias.purdue.edu(128.10.252.7)
Location: CERIAS, Purdue University, West Lafayette, IN
Synchronization: NTP primary (GPS), Datum TymServe 2100L
Service Area: Indiana
Access Policy: open access, please send a message to notify
Contact: Gene Spafford (spaf@cerias.purdue.edu)

LXXXV. US MA bonehed.lcs.mit.edu (18.26.4.105)
Location: Massachusetts Institute of Technology, Cambridge, MA
Synchronization: Motorola Oncore UT+ GPS, xntp3-5.90, FreeBSD 3.2
Service Area: Eastern US
Access Policy: open access
Contact: Robert Morris (rtm@lcs.mit.edu)

LXXXVI. US MA clock.osf.org (130.105.4.59)
Location: Open Software Foundation, Cambridge, MA
Synchronization: NTP primary (WWV clock), i586/OSF1
Service Area: NSFNET, NEARnet region
Access Policy: open access

Contact: Paul Groff (groff@osf.com)
Note: prior permission to access required

LXXXVII. US MA tick.mit.edu (18.145.0.30) CNAME: navobs1.mit.edu
Location: Massachusetts Institute of Technology, Cambridge, MA
Synchronization: NTP V3 primary (GPS) HP9000/747i
Service Area: eastern time zone, others on request
Access Policy: open access to stratum-2 servers and to MIT clients
Contacts: Rich Schmidt (res@tuttle.usno.navy.mil)

LXXXVIII. US MD time-b.nist.gov (129.6.15.29)
Location: NIST Central Computer Facility, Gaithersburg, Maryland
Synchronization: ACTS dial-up using lockclock algorithm, DEC Alpha/UNIX
Service Area: NSFnet, SURAnet
Access Policy: Open to stratum-2 servers, others by arrangement; please use one of the servers as primary with the other as a backup.
Contact: Judah Levine (jlevine@time.nist.gov) 303 492 7785

LXXXIX. US MD umd1.umd.edu (128.8.10.1)
Location: University of Maryland, College Park, MD
Synchronization: NTP V3 primary (WWVB clock), Fuzzball
Service Area: NSFNET, SURA region
Access Policy: closed access, except for stratum-2 servers providing synchronization to local networks of ten or more hosts
Contact: Michael Petry (petry@ni.umd.edu)

XC. US ME ntp.colby.edu (137.146.210.250) (CNAME ntp-colby.usno.navy.mil)
Location: Colby College, Waterville, ME
Geographic Coordinates: 69 39 42.0 W, 44 33 48 N WGS84
Synchronization: NTP V3 primary (GPS)
Service area: Northeastern US & Canada, others by arrangement
Access Policy: open access for stratum 2 servers
Contacts: Rich Schmidt, US Naval Observatory (res@tuttle.usno.navy.mil), Jeff Earickson, Colby College (jaearick@colby.edu)
Note: IP addresses are subject to change; please use DNS.

XCI. US MO navobs1.wustl.edu (128.252.19.1) CNAME: tick.wustl.edu
Location: Washington University, St. Louis, MO
Synchronization: NTP V3 primary (GPS) HP9000/747i
Service area: USA Central timezone, others by arrangement.
Access Policy: open access
Contact: Rich Schmidt,US Naval Observatory (res@tuttle.usno.navy.mil)

XCII. US NC ncnoc.ncren.net (192.101.21.1)
Location: MCNC, Research Triangle Park, NC
Synchronization: NTP V3 primary (WWVB clock), Netclock/2, Sun 4/65
Service area: NC-REN region
Access Policy: NC-REN region, other use by prior arrangement
Contact: Tim Seaver (tas@ncren.net, clockmaster@ncren.net)

XCIII. US NC terrapin.csc.ncsu.edu 152.1.58.124
Location: North Carolina State University, Raleigh, NC
Synchronization: NTP primary (GPS clock), Trimble Palisade
Service Area: South Eastern US
Access Policy: open access
Contact: Sven Dietrich, NCSU, sven@terrapin.csc.ncsu.edu

XCIV. US NY nist1.nyc.certifiedtime.com (208.184.49.9)
Location: Abovenet, New York City, New York
Synchronization: ACTS dial-up using lockclock algorithm; DEC Alpha UNIX
Service Area: North Eastern US
Access Policy: Open to stratum-2 servers and others by arrangement
Contact: Judah Levine (jlevine@boulder.nist.gov) 303 492-7785

XCV. US OH lerc-dns.lerc.nasa.gov (128.156.1.43)
Location: NASA Lewis Research Center, Cleveland, OH
Synchronization: NTP Primary (WWVB clock), Sun/Unix Service Area: NSFNET, OARNET
Access Policy: open access
Contact: Joe Rossoll (yyjer@scivax.lerc.nasa.gov)

XCVI. US PA gps1.otc.psu.edu (128.118.25.12)
Location: Penn State University, University Park, PA

Geographic Coordinates: 40:47:58.1N, 77:51:44.8W (USGS 40077-G7-TF-024)
Synchronization: NTP V3 primary (GPS), TrueTime XL/DC NTP module
Service Area: Internet2, vBNS, CERFnet(AT&T IP Services), PSC/NCNE, CASC.
Access Policy: closed access, except for stratum-2 servers providing synchronization to local networks of ten or more hosts; others by arrangement only
Contact: John Balogh <JDB@psu.edu>
Note: the IP address for gps1.otc.psu.edu may change; please use DNS. This hardware does not support rdate or daytime protocols; NTPv3 only.

XCVII. US PA otc1.psu.edu (128.118.46.3)
Location: Penn State University, University Park, PA
Synchronization: NTP V3 primary (WWV clock), Sun/Unix
Service Area: NSFNET, PREPNET, JvNCnet
Access Policy: open access
Contact: John Balogh (JohnBalogh@psu.edu) (no longer: jdb@ecl.psu.edu)

XCVIII. US PA wwv.otc.psu.edu (128.118.46.3)
Location: Penn State University, University Park, PA
Geographic Coordinates: 40:47:58.1N, 77:51:44.8W (USGS 40077-G7-TF-024)
Synchronization: NTP V3 primary (Traconex/PSTI-1020 WWV clock), Sun/Unix
Service Area: Internet2, vBNS, CERFnet(AT&T IP Services), PSC/NCNE, CASC.
Access Policy: open access
Contact: John Balogh <JDB@psu.edu>
Note: wwv.otc.psu.edu is the CNAME for this service. The IP address WILL change sometime after mid-year 1999; please use DNS.

XCIX. US TX tick.uh.edu (129.7.1.66) CNAME: time.uh.edu
Location: University of Houston, Houston, TX
Geographic Coordinates: 29:43:37N,95:20:22W
Synchronization: NTP V3 primary (GPS) HP9000/747i
Service Area: US Central time zone, others on request
Access Policy: open access to stratum-2 servers and to UH clients
Contacts: Rich Schmidt (res@tuttle.usno.navy.mil), Alan Pfeiffer- Traum (apt@uh.edu)

C. US VA nist1.dc.certifiedtime.com (216.200.93.8)
Location: Abovenet, Vienna, VA
Synchronization: ACTS dial-up using lockclock algorithm; DEC Alpha UNIX
Service Area: Primarily networks in Eastern US
Access Policy: Open to stratum-2 servers and others by arrangement.
Contact: Judah Levine (jlevine@boulder.nist.gov) 303 492-7785

CI. US WA bigben.cac.washington.edu 140.142.16.34 (CNAME ntp-wu.usno.navy.mil)
Location: University of Washington, Seattle, WA
Synchronization: NTP primary (GPS clock), HP9000/747i HPUX
Service Area: Pacific Northwest
Access Policy: open access to Pacific Time Zone stratum 2's and to Univ. of Washington clients; others by arrangement
Contact: Rich Schmidt, USNO, res@tuttle.usno.navy.mil, Bill Mar, Univ. of Washington (bmar@cac.washington.edu)

CII. US WA time-nw.nist.gov (131.107.1.10)
Location: Microsoft Corporation, Redmond, Washington
Synchronization: ACTS Dial-up and lockclock algorithm, DEC Alpha/UNIX
Service Area: NorthWestNet, NSFnet
Access policy: open to stratum-2 servers and others by arrangement.
Contact: Judah Levine (jlevine@time-a.timefreq.bldrdoc.gov) (303) 492-7785

CIII. US WI ben.cs.wisc.edu (128.105.201.11)
Location: Computer Science Department, University of Wisconsin-Madison
Geographic Coordinates: 89:24:30W, 43:08:00N
Synchronization: NTP V4 primary (Odetics GPS), Sun/Sparc
Service Area: US/any
Access Policy: One primary and one secondary per domain, by request
Contact: David Thompson (ntp-admin@cs.wisc.edu)
Note: IP addresses are subject to change; please use DNS

Discontinued Service

bitsy.mit.edu
chronos.univ-rennes1.fr
clock.llnl.gov
fuzzy.nta.no

ntp.cc.utexas.edu
ntp.syd.dms.csiro.au
ntp.tip.csiro.au
ntp0.sdd.hp.com
ntp0.ja.net
ntp1.sony.com
utcnist1.reston.mci.net
wave.mbari.org
wwvb.erg.sri.com
wwvb.isi.edu
wwwa2.kph.uni-mainz.de
y2k-test.timefreq.bldrdoc.gov

See Also...

Time Servers
Time Sync

Public NTP Secondary Time Servers

Last update: 21 January 2001 UTC

Active Servers

I. AR tick.nap.com.ar (200.49.40.1)
Location: Network Access Point, Buenos Aires, Argentina
Synchronization: NTP V3 secondary (stratum 2), Cisco IGS 12.0
Service Area: Argentina
Access Policy: open access, please send a message to notify
Contact: Pablo J. Fritz (timekeeper@nap.com.ar)
Note: tick.nap.com.ar is a CNAME

II. AR time.sinectis.com.ar (200.16.183.2)
Location: Sinectis S.A., Buenos Aires (Argentina)
Geographic Coordinates: 3432'S, 5820'W
Service Area: Argentina
Synchronization: NTP secondary (stratum 2)
Access Policy: open access, please send a message to notify.
Contact: Pablo Cingolani, Levan Djaparidze (timekeeper@sinectis.com.ar)
Note: time is an alias and the IP address may change; please use DNS.

III. AR tock.nap.com.ar (200.49.32.1)
Location: Network Access Point, Buenos Aires, Argentina
Synchronization: NTP V3 secondary (stratum 2), Cisco IGS 12.0
Service Area: Argentina
Access Policy: open access, please send a message to notify
Contact: Pablo J. Fritz (timekeeper@nap.com.ar)
Note: tock.nap.com.ar is a CNAME

IV. AU augean.eleceng.adelaide.edu.au (129.127.28.4)
Location: University of Adelaide, South Australia
Synchronization: NTP secondary (stratum 2), Sun-4/75/Unix
Service area: AARNet
Access policy: open access, please send a message to notify
Contact: systems@eleceng.adelaide.edu.au

V. AU ntp.adelaide.edu.au (129.127.40.3)
Location: University of Adelaide, South Australia
Synchronization: NTP V3 secondary (stratum 2), Digital AlphaStation 255/233 Unix
Service Area: AARNet
Access Policy: open access
Contact: Chris Farmer (chris.farmer@adelaide.edu.au)

VI. AU ntp.saard.net (203.21.37.18)
Location: The University of Adelaide, Adelaide, South AUSTRALIA
Synchronization: NTP secondary (stratum 2), DEC 3000/300L OSF/1
Service Area: AARNet
Access Policy: open access
Contact: Danielle Hopkins (dani@itd.adelaide.edu.au)

VII. AU time.deakin.edu.au (128.184.1.1)
Location: Deakin University, Victoria
Synchronization: NTP V4 secondary (stratum 2)
Service Area: AARNET, Australia wide
Access Policy: open access, please send a message to notify
Contact: Ben McConaghy (benmc@deakin.edu.au)

VIII. AU time.esec.com.au (203.21.84.4)
Location: eSec Limited, Flemington, Victoria, Australia
Synchronization: NTP secondary (stratum 2), PC/OpenBSD
Service area: Telstra Internet, and the rest of Australia
Access policy: open access
Contact: timemaster@esec.com.au
Note: Formerly known as "time.aba.net.au".

IX. BR ntp.cais.rnp.br (200.144.121.33)
Location: Brazilian Research Network/Rede Nacional de Pesquisa (RNP)

Synchronization: NTP V4 Secondary (stratum 2), Sun SPARC10/Solaris,
Service Area: Brazil
Access Policy: Open access to stratum 2 and stratum 3 NTP servers. Please, send a mail to notify.
Contact: ntp-admin@cais.rnp.br

X. BR ntp.pop-df.rnp.br (200.19.119.119)
Location: Brazilian Research Network/Rede Nacional de Pesquisa (RNP)
Syncronization: NTP V4 Secondary (stratum 2), FreeBSD/Unix
Service Area: Brazil
Access Policy: Open access to stratum 2 and stratum 3 NTP servers. Please, send a mail to notify.
Contact: ntp-admin@pop-df.rnp.br

XI. BR ntp1.pucpr.br (200.192.112.8)
Location: Brazilian / Pontificia Universidade Catolica do Parana
Synchronization: NTP V4 secondary (stratum 2),
Sun SPARC4/Solaris 7
Service =C1rea: Brazil
Access Policy:open access to stratum 2 server
Contact: ntp1@pucpr.br

XII. CA ntp1.cmc.ec.gc.ca
Location: Canadian Meteorological Centre, Dorval, Québec, Canada
Synchronization: NTP V4 secondary SGI/Unix
Service Area: Eastern Canada
Access Policy: open access
Contact: (ntp-admin@cmc.ec.gc.ca)

XIII. CA ntp2.cmc.ec.gc.ca
Location: Canadian Meteorological Centre, Dorval, Québec, Canada
Synchronization: NTP V4 secondary SGI/Unix
Service Area: Eastern Canada
Access Policy: open access
Contact: (ntp-admin@cmc.ec.gc.ca)

XIV. CA tick.utoronto.ca (128.100.103.252)
Location: University of Toronto, Toronto, Ontario, CANADA
Synchronization: NTP V3 secondary (stratum 2), Sparc 10, Solaris 2.5.1
Service Area: Eastern Canada
Access Policy: open access, send email to notify.
Contact: Russell Sutherland (russ@madhaus.cns.utoronto.ca)
Note: IP addresses are subject to change; please use DNS

XV. CA time.chu.nrc.ca (209.87.233.53)
Location: National Research Council of Canada, Ottawa, Ontario, Canada
Geographic Coordinates: 45:17:41N, 75:45:27W
Synchronization: NTP V3 secondary (stratum 2), PC/Linux
Service Area: Canada
Access Policy: open access
Contact: time@nrc.ca
Note: IP address subject to change; please use DNS.

XVI. CA time.nrc.ca (132.246.168.148)
Location: National Research Council of Canada, Ottawa, Ontario, Canada
Geographic Coordinates: 45:27N, 75:37W
Synchronization: NTP V3 secondary (stratum 2), PC/Linux
Service Area: Canada
Access Policy: open access
Contact: time@nrc.ca
Note: time is an alias and the IP address may change; please use DNS.

XVII. CA timelord.uregina.ca (142.3.100.15)
Location: University of Regina, Regina, Saskatchewan, Canada
Geographic Coordinates: 50:25N , 104:35:20 W
Synchronization: NTP V3 secondary (stratum 2), Sun Sparc 5
Service Area: SASK#net, CA*net, Canada
Access Policy: open access
Contact: Mark Haidl (timekeeper@uregina.ca)
Note: please limit to one or two hosts per site.

XVIII. CA tock.utoronto.ca (128.100.100.128)
Location: University of Toronto, Toronto, Ontario, CANADA
Synchronization: NTP V3 secondary (stratum 2), Sparc 5, Solaris 2.5
Service Area: Eastern Canada
Access Policy: open access, send email to notify.
Contact: Russell Sutherland (russ@madhaus.cns.utoronto.ca)
Note: IP addresses are subject to change; please use DNS

XIX. CH bernina.ethz.ch (129.132.98.11)
Location: Swiss Fed. Inst. of Technology, CH 8092 Zurich, Switzerland
Geographic Coordinates: 47:23N, 8:32E
Synchronization: NTP secondary (stratum 2), Sun SS10-51/SunOS4
Service Area: Switzerland/Europe
Access Policy: open access
Contact: Adam Feigin (time@iis.ee.ethz.ch)

XX. DK clock.netcetera.dk (130.228.230.2)
Location: Copenhagen, Denmark, Europe
Synchronization: NTP secondary (stratum 2), i386/Linux
Service area: Denmark, Scandinavia, Northern Europe
Access policy: open access, please send a message to notify
Contact: ask@netcetera.dk
Note: clock is an alias and the IP address may change; please use DNS

XXI. DK clock2.netcetera.dk (194.192.207.9)
Location: Copenhagen, Denmark, Europe
Synchronization: NTP secondary (stratum 2), i386/Linux
Service area: Denmark, Scandinavia, Northern Europe
Access policy: open access, please send a message to notify
Contact: ask@netcetera.dk
Note: clock2 is an alias and the IP address may change; please use DNS

XXII. ES slug.ctv.es [194.179.52.14] (will add an alias for this purpose)
Location: Altea (Alicante/SPAIN)
Synchronization: Stratum-2/i486DX2/66/Linux
Service Area: Spain
Access Policy: Public (glad to receive a note)
Contact: Luis Colorado (luis.colorado@slug.ctv.es)

XXIII. FI tick.keso.fi (194.215.108.15)
Location: Keski-Savon Oppimiskeskus, Pieksamaki, Finland, Europe
Synchronization: NTP-3, i686/Linux
Service area: Finland
Access policy: open access, please send a message to notify
Contact: root@keso.fi
Note: tick is an alias, please use DNS

XXIV. FI tock.keso.fi (194.215.108.18)
Location: Keski-Savon Oppimiskeskus, Pieksamaki, Finland, Europe
Synchronization: NTP-3, i586/Linux
Service area: Finland
Access policy: open access, please send a message to notify
Contact: root@keso.fi
Note: tock is an alias, please use DNS

XXV. FR ntp.obspm.fr
Location: Observatoire de Paris-Meudon, Meudon, France
Synchronization: NTP V3, DEC Alpha / Digital Unix
Service Area: France/Europe
Access Policy: open access, but please send a message to notify
Contact: lptfop@obspm.fr
Note: use DNS for IP address.

XXVI. FR ntp.univ-lyon1.fr (134.214.100.6)
Location: CISM, Lyon, France
Synchronization: NTP V3 secondary (stratum 2), Sun SS10
Service Area: France, Switzerland, Italy, Europe
Access Policy: open access
Contact: ntp-adm@univ-lyon1.fr

Note: consult DNS to get host address, ntp is an alias.
Note: we would appreciate getting a little note if you make regular use of this server, so that we can put you on our NTP mailing-list.

XXVII. FR ntp.via.ecp.fr (138.195.130.70)
Location: VIA, Ecole Centrale Paris, France
Synchronization: ntp v4.0.99c (stratum 2), Debian GNU/Linux x86
Service Area: France/Europe
Policy: open access, send email to notify. Please limit access to one or two hosts per site (large sites should set up their own ntp server)
Contact: ntpadmin@via.ecp.fr

XXVIII. HR zg1.ntp.carnet.hr (161.53.2.70)
Location: CARNet (Croatian Academic and Research Network), Zagreb, Croatia
Synchronization: NTP V4 secondary (stratum 2), Sun Sparc/Solaris
Service Area: Croatia/Europe
Access Policy: open access, glad to receive a note
Contact: ntp@carnet.hr
Note: IP address subject to change; better use DNS

XXIX. HR zg2.ntp.carnet.hr (161.53.123.4)
Location: CARNet (Croatian Academic and Research Network), Zagreb, Croatia
Synchronization: NTP V4 secondary (stratum 2), Sun Sparc/Solaris
Service Area: Croatia/Europe
Access Policy: open access, glad to receive a note
Contact: ntp@carnet.hr
Note: IP address subject to change; better use DNS

XXX. HR st.ntp.carnet.hr (161.53.30.3)
Location: CARNet (Croatian Academic and Research Network), Split, Croatia
Synchronization: NTP V4 secondary (stratum 2), Sun Sparc/Solaris
Service Area: Croatia/Europe
Access Policy: open access, glad to receive a note
Contact: ntp@carnet.hr
Note: IP address subject to change; better use DNS

XXXI. HR ri.ntp.carnet.hr (161.53.40.3)
Location: CARNet (Croatian Academic and Research Network), Rijeka, Croatia
Synchronization: NTP V4 secondary (stratum 2), Sun Sparc/UNIX
Service Area: Croatia/Europe
Access Policy: open access, glad to receive a note
Contact: ntp@carnet.hr
Note: IP address subject to change; better use DNS

XXXII. HR os.ntp.carnet.hr (161.53.200.8)
Location: CARNet (Croatian Academic and Research Network), Osijek, Croatia
Synchronization: NTP V4 secondary (stratum 2), Sun Sparc/Solaris
Service Area: Croatia/Europe
Access Policy: open access, glad to receive a note
Contact: ntp@carnet.hr
Note: IP address subject to change; better use DNS

XXXIII. HU time.kfki.hu (148.6.0.1)
Location: KFKI Research Institute for Particle and Nuclear Physics, Budapest, Hungary
Synchronization: NTP secondary (stratum 2), Sun/Solaris
Service Area: HUNGARNET
Access Policy: open access, send email to notify.
Contact: time@sunserv.kfki.hu

XXXIV. IE ntp.maths.tcd.ie
Location: School of Mathematics, Trinity College, Dublin, Ireland.
Synchronization: NTPV4 secondary (stratum 2), Intel, FreeBSD 2.2
Service Area: Ireland, UK
Access Policy: open access, please send a message to notify.
Contact: time@maths.tcd.ie
Note: ntp.cs.tcd.ie, ntp.maths.tcd.ie and ntp.tcd.ie peer together over local area net. It is normally sufficient just to pick one machine to peer with.

XXXV. IT ntps.net4u.it (195.32.52.129)
Location: 4u Srl, Vercelli, Italy

Synchronization: NTP secondary (stratum 2), Linux 2 on Intel PII 300MHz
Service area: Italy
Access policy: open access, please send a message to notify
Contact: timemaster@net4u.it

XXXVI. JP ntp.cyber-fleet.net[203.139.30.195]
Location: Cyber Fleet, Inc., Tokyo, Japan
Geographic Coordinates: 35:43:59N, 139:40:50E
Synchronization: NTP V4 secondary (stratum 2), PC BSD/OS
Service Area: Japan/East Asia
Access policy: open access, please send a message to notify
Contact: pdp@cyber-fleet.net

XXXVII. KR time.nuri.net[203.255.112.4]
Location: Inet, Inc., Seoul, Korea
Geographic Coordinates: 37:29:52N, 127:02:15E
Synchronization: NTP V3 secondary (stratum 2), Sun-SS20/Solaris 2.6
Service Area: Korea, Japan, Hong Kong / East Asia
Access policy: open access
Contact: ntp-admin@nuri.net
Note: IP addresses are subject to change; please use DNS

XXXVIII. MX ntp2a.audiotel.com.mx (200.34.146.67)
Location: Audiotel office, Mexico D.F., Mexico
Synchronization: NTP V3 secondary (stratum 2), NeXTstation/33
Service Area: Avantel, MCINet, Mexico
Access Policy: open access, but please send a message to notify.
Contact: Pedro Resendiz (resendiz@audiotel.com.mx)

XXXIX. MX ntp2b.audiotel.com.mx (200.34.146.68)
Location: Audiotel office, Mexico D.F., Mexico
Synchronization: NTP V3 secondary (stratum 2), NeXTstation/33
Service Area: Avantel, MCINet, Mexico
Access Policy: open access, but please send a message to notify.
Contact: Pedro Resendiz (resendiz@audiotel.com.mx)

XL. MX ntp2c.audiotel.com.mx (200.34.146.69)
Location: Audiotel office, Mexico D.F., Mexico
Synchronization: NTP V3 secondary (stratum 2), NeXTstation/33
Service Area: Avantel, MCINet, Mexico
Access Policy: open access, but please send a message to notify.
Contact: Pedro Resendiz (resendiz@audiotel.com.mx)

XLI. NG ntp.supernet300.com (216.72.109.4)
Location: Supernet300, Lagos, Nigeria
Synchronization: NTP secondary (stratum 2), PC/Linux
Service Area: Western Africa, primarily Nigerian NITEL backbone
Access Policy: Open access, please send an email to notify before use.
Contact: timelords@supernet300.com
Note: Please use the DNS name-the IP address can (and likely will) change.

XLII. NO fartein.ifi.uio.no (129.240.64.3)
Location: University of Oslo, Norway
Geographic Coordinates: 59:56:32N, 10:43:22E
Synchronization: NTP secondary (stratum 2), DEC Alpha OSF/1 V4.0
Service Area: NORDUnet
Access Policy: open access
Contact: Jens Thomassen (timekeeper@ifi.uio.no)

XLIII. NO time.alcanet.no (use DNS)
Location: Alcanet International, Oslo, Norway
Synchronization: NTP V3 secondary (stratum 2), PC/Linux
Service Area: Europe=20
Access Policy: open access, notify message appreciated
Contact: timekeeper@alcanet.no=20

XLIV. NZ ntp.massey.ac.nz (130.123.123.253)
Location: Massey University, Palmerston North, New Zealand
Synchronisation: NTP V3 (stratum 2), Digital Unix 4.0E, Alpha

Service Area: New Zealand
Access Policy: Open access within New Zealand, send email to notify.
Contact: ntp@massey.ac.nz
Note: IP addresses are subject to change; please use DNS

XLV. NZ truechimer.waikato.ac.nz (130.217.76.32)
truechimer1.waikato.ac.nz (130.217.76.32)
truechimer2.waikato.ac.nz (130.217.66.13)
truechimer3.waikato.ac.nz (130.217.76.30)
Location: The University of Waikato, Hamilton, New Zealand
Synchronisation: NTP V3 (stratum 2), Linux on Intel
Service Area: New Zealand
Access Policy: Open access within New Zealand, send email to notify.
Contact: ntp@waikato.ac.nz
Note: IP addresses are subject to change; please use DNS

XLVI. PL info.cyf-kr.edu.pl: 149.156.4.11
Location: Academic Computer Centre, CYFRONET, Krakow, Poland
Synchronization: NTP V3 secondary (stratum 2), HP/Unix
Service Area: Poland/Europe
Access policy: open access, please send a message to notify
Contact: Jerzy.Pawlus@cyf-kr.edu.pl

XLVII. PT bug.fe.up.pt (193.136.54.1)
Location: Oporto University, Portugal
Synchronization: NTP secondary (stratum 2), i486/Linux
Service Area: Portugal/Europe
Access Policy: For use only by prior arrangement. Mail
timemaster@bug.fe.up.pt for more information.

XLVIII. RU ntp.landau.ac.ru (193.233.9.7)
Location: Landau Institute for Theoretical Physics, Moscow, Russia
Synchronization: NTP V4 secondary (stratum 2), PC/FreeBSD
Service area: Russia
Access policy: open access
Contact: Dmitry Sivachenko (dima@Chg.RU)

XLIX. RU ntp.psn.ru (194.149.67.130)
Location: Pushchino, Moscow region, Russia
Geographic Coordinates: 54:50N, 37:37E
Synchronization: NTP secondary (stratum 2), Alpha/Linux
Service area: Russia
Access policy: open access, please send a message to notify
Contact: clockmaster@psn.ru

L. RU sign.chg.ru (193.233.46.10)
Location: Scientific Center in Chernogolovka, Moscow region, Russia
Synchronization: NTP V3 secondary (stratum 2), PC/FreeBSD 3.1
Service Area: Russia
Access Policy: open access, please send e-mail to notify.
Contact: Andrew Neporada (andrew@chg.ru) or time@sign.chg.ru

LI. SE ntp.lth.se (130.235.20.3)
Location: Lund Institute of Technology, Lund, Sweden
Synchronization: NTP V3 secondary (stratum 2), Sun/Solaris
Service Area: Sweden, NORDUnet
Access Policy: open access, send email to notify. Please limit access to one or two hosts per site (large sites should set up their own ntp server)
Contact: timemaster@lth.se

LII. SG ntp.shim.org
Location: Singapore
Synchronization: NTP secondary (stratum 2), Intel/Linux
Service Area: Singapore
Access Policy: open access
Contact: Dr Ivan Shim

LIII. SI sizif.mf.uni-lj.si (193.2.69.15)
Location: Institute of Biophysics, University of Ljubljana, Slovenia

Geographic Coordinates: 46:03:09N, 14:30:40E
Synchronization: NTP V3 secondary (stratum 2), HP/Unix
Service Area: Slovenia/Europe
Access Policy: open access, please send a message to notify
Contact: Primoz Peterlin (time@biofiz.mf.uni-lj.si)

LIV. SI hmljhp.rzs-hm.si (193.2.208.12)
Location: Hydrometeorological Institute of Slovenia, Ljubljana, Slovenia
Geographic Coordinates: 46°3.915'N, 14°30.809'E, +340 m (WGS84)
Synchronization: NTP V4 secondary, HP/HP-UX
Service Area: Slovenia/Europe
Access Policy: open access, please send a message to notify
Contact: Metod Kozelj (metod.kozelj@rzs-hm.si)

LV. SI ntp1.arnes.si (193.2.1.66)
Location: ARNES (Academic and Research Network of Slovenia), Ljubljana, Slovenia
Synchronization: NTP V4 secondary (stratum 2), Sun Sparc/Solaris
Service Area: Slovenia/Europe
Access Policy: open access, glad to receive a note
Contact: ntp-admin@arnes.si
Note: IP address subject to change; better use DNS

LVI. SI ntp2.arnes.si (193.2.1.92)
Location: ARNES (Academic and Research Network of Slovenia), Ljubljana, Slovenia
Synchronization: NTP V4 secondary (stratum 2), Sun Sparc/Solaris
Service Area: Slovenia/Europe
Access Policy: open access, glad to receive a note
Contact: ntp-admin@arnes.si
Note: IP address subject to change; better use DNS

LVII. SI time.ijs.si (193.2.4.6)
Location: J. Stefan Institute, Ljubljana, Slovenia
Geographic Coordinates: 46:02:35N, 14:29:17E (WGS84)
Synchronization: NTP V4 secondary (stratum 2), DEC Alpha / Digital Unix
Service Area: Slovenia/Europe
Access Policy: open access, glad to receive a note
Contact: Mark Martinec (timekeeper@ijs.si)
Note: IP address subject to change; better use DNS

LVIII. SI time.ijs.si (193.2.4.6)
Location: J. Stefan Institute, Ljubljana, Slovenia
Geographic Coordinates: 46° 2.517'N, 14° 29.241'E (WGS84)
Synchronization: NTP V4 secondary (stratum 2), Compaq (DEC) Alpha / Tru64 Unix with MICRO_TIME kernel option
Service Area: Slovenia/Europe
Access Policy: open access, glad to receive a note
Contact: Mark Martinec (timekeeper@ijs.si); More info?
Note: IP address subject to change; better use DNS

LIX. UK ntp.cs.strath.ac.uk (130.159.196.123, 130.159.196.125)
Location: Dept. Computer Science, Strathclyde University, Glasgow, Scotland.
Geographic Coordinates: 04:14W, 55:52N
Synchronization: NTP V3 secondary Sun/Unix
Service Area: UK/Europe/any
Access Policy: open access
Contact: Ian Gordon (ntp@cs.strath.ac.uk)
Note: IP addresses are subject to change; please use DNS

LX. UK ntp.exnet.com (194.207.34.9)
Location: ExNet Ltd, London, UK
Synchronization: NTP secondary (stratum 2), Sun-4/Unix
Service area: UK/Europe/any
Access policy: semi-open access, please send message first for access
Contact: sysadmin@exnet.com or dhd@exnet.com
Note: Please see our Web page before using. Please use CNAME ntp.exnet.com since IP address may well change.

LXI. UK ntp0.uk.uu.net 158.43.128.33
Configuration: NTP V3 secondary (stratum 2), Sun sparc Ultra, Solaris 7, xntpd 3-5.93
Location: Cambridge, UK
Service Area: UUNET (formerly known in the UK as PIPEX); UK

Access Policy: Semi-open access. These are primarily for use by UUNET customers who may use them without asking, but others are welcome to peer if they give notice.
Contact: timelord@uk.uu.net
Note: This service is supported on a best-effort basis, but is not guaranteed. UUNET customers should peer with all three: ntp0.uk.uu.net, ntp1.uk.uu.net, and ntp2.uk.uunet.

LXII. UK ntp1.uk.uu.net 158.43.128.66
Configuration: NTP V3 secondary (stratum 2), Sun sparc Ultra, Solaris 7, xntpd 3-5.93
Location: Cambridge, UK
Service Area: UUNET (formerly known in the UK as PIPEX); UK
Access Policy: Semi-open access. These are primarily for use by UUNET customers who may use them without asking, but others are welcome to peer if they give notice.
Contact: timelord@uk.uu.net
Note: This service is supported on a best-effort basis, but is not guaranteed. UUNET customers should peer with all three: ntp0.uk.uu.net, ntp1.uk.uu.net, and ntp2.uk.uunet.

LXIII. UK ntp2.uk.uu.net 158.43.192.66
Configuration: NTP V3 secondary (stratum 2), Sun sparc Ultra, Solaris 7, xntpd 3-5.93
Location: London, UK
Service Area: UUNET (formerly known in the UK as PIPEX); UK
Access Policy: Semi-open access. These are primarily for use by UUNET customers who may use them without asking, but others are welcome to peer if they give notice.
Contact: timelord@uk.uu.net
Note: This service is supported on a best-effort basis, but is not guaranteed. UUNET customers should peer with all three: ntp0.uk.uu.net,

LXIV. UK ntp2a.mcc.ac.uk (130.88.202.49)
Location: University of Manchester, Manchester, England
Synchronization: NTP secondary (S2), Sun/SunOS
Service Area: UK
Access Policy: Open Access
Contact(s): timelords@mcc.ac.uk
Note: Please use DNS for address, subject to change

LXV. UK ntp2b.mcc.ac.uk (130.88.200.98)
Location: University of Manchester, Manchester, England
Synchronization: NTP secondary (S2), PC/FreeBSD
Service Area: UK
Access Policy: Open Access
Contact(s): timelords@mcc.ac.uk
Note: Please use DNS for address, subject to change

LXVI. UK ntp2c.mcc.ac.uk (130.88.200.4)
Location: University of Manchester, Manchester, England
Synchronization: NTP secondary (S2), PC/FreeBSD
Service Area: UK
Access Policy: Open Access
Contact(s): timelords@mcc.ac.uk
Note: Please use DNS for address, subject to change

LXVII. UK ntp2d.mcc.ac.uk (130.88.203.12)
Location: University of Manchester, Manchester, England
Synchronization: NTP secondary (S2), SGI/Irix
Service Area: UK
Access Policy: Open Access
Contact(s): timelords@mcc.ac.uk
Note: Please use DNS for address, subject to change

LXVIII. UK tick.tanac.net (195.112.34.51)
Location: Wibble UK, Aylesbury, Buckinghamshire UK
Synchronization: NTP secondary (stratum 2), i686/Linux 2.2
Geographic Coordinates: 51 49 00 N 00 48 00 W
Service area: United Kingdom
Access policy: open access, please send a message to notify
Contact: ntp@tanac.net

LXIX. US CA ns.scruz.net (165.227.1.1)
Location: scruz-net, inc. Santa Cruz, CA USA
Synchronization: NTP V3 secondary (stratum 2), BSD on Intel

Service area: Western USA (MAE-West attached)
Access policy: open access (scruz-net customers use both ns.scruz.net and nic.scruz.net, others please use one or the other, not both... please drop us a note if you're using the server so we can keep you on our status list)
Contact: Matthew Kaufman (matthew@scruz.net)

LXX. US CA ntp.ucsd.edu (132.239.254.49)
Location: UCSD Academic Computing Services/Network Operations, San Diego, CA
Synchronization: NTP secondary (stratum 2)
Service Area: CERFNET; NSFNET, SDSC region and nearby
Access Policy: open access, please send a message to notify.
Contact: timekeeper@ucsd.edu

LXXI. US CA ntp1.mainecoon.com (63.192.96.2)
Location: Quincy, California
Geographic Coordinates: 39:56.863N, 120:54.657W
Synchronization: NTP V4 secondary (stratum 2) P-II/X86 Solaris 2.7
Service Area: North America
Access Policy: Open Access, please drop us a note so we can add you to our mailing list.
Contact:time@mainecoon.com or Chris Kennedy (chris@mainecoon.com)
Note: ntp1 is a CNAME for time service. Please use DNS; IP assignments subject to change.

LXXII. US CA ntp2.mainecoon.com (63.192.96.3)
Location: Quincy, California
Geographic Coordinates: 39:56.863N, 120:54.657W
Synchronization: NTP V4 secondary (stratum 2) Sun 4/75 Solaris 2.7
Service Area: North America
Access Policy: Open Access, please drop us a note so we can add you to our mailing list.
Contact:time@mainecoon.com or Chris Kennedy (chris@mainecoon.com)
Note: ntp2 is a CNAME for time service. Please use DNS; IP

LXXIII. US CA time.five-ten-sg.com (205.147.40.34)
Location: Lake Arrowhead, CA, USA
Synchronization: NTP V4 secondary (Stratum 2), Linux/intel
Service Area: within 100ms of Digilink.net
Access Policy: open access, email for firewall access first
Contact: carl@five-ten-sg.com

LXXIV. US DE louie.udel.edu (128.175.1.3)
Location: University of Delaware, Newark, DE
Synchronization: NTP V3 secondary (stratum 2), Sun SPARC10/Solaris 2.6
Service Area: CAIRN, Abilene/vBNS
Access Policy: open access
Contact: Dave Mills <mills@udel.edu>

LXXV. US GA ntp.shorty.com (208.21.108.186)
Location: CNSG, Atlanta, GA
Synchronization: NTP secondary (stratum 2), PC/Linux
Service Area: Southeast United States
Access Policy: Open access, please send an email to notify before use.
Contact: timelords@shorty.com
Note: Please use the CNAME ntp. IP addresses can (and likely will) change.

LXXVI. US GA rolex.peachnet.edu (198.72.72.10)
Location: PeachNet NOC, Kennesaw, GA
Synchronization: NTP secondary (stratum 2), Sun Sparc/Unix
Service Area: PeachNet (Georgia), Southeast U.S.A. Netwise close to UUNET and BBN
Access Policy: open access, please send a message with the hostname and/or address of your NTP client to notify.
Contact: timekeeper@peachnet.edu
Note: For single NTP clients, we prefer you poll Timex.PeachNet.EDU. For NTP servers which support large NTP domains please use Rolex.PeachNet.EDU. Please use the CNAME as IP addresses may change.

LXXVII. US GA timex.peachnet.edu (131.144.4.21)
Location: PeachNet NOC, Kennesaw, GA
Synchronization: NTP secondary (stratum 2), Sun Sparc/Unix
Service Area: PeachNet (Georgia), Southeast U.S.A. Netwise close to UUNET and BBN
Access Policy: open access, please send a message with the hostname and/or address of your NTP client to notify.
Contact: timekeeper@peachnet.edu
Note: For single NTP clients, we prefer you poll Timex.PeachNet.EDU. For NTP servers which support large NTP domains please use Rolex.PeachNet.EDU. Please use the CNAME as IP addresses may change.

LXXVIII. US IL ntp-0.cso.uiuc.edu (130.126.24.53)
Location: University of Illinois, Urbana-Champaign, IL
Synchronization: NTP secondary (stratum 2), Cisco-ASM/4
Service Area: CICNET, Midwest, NCSA region
Access Policy: open access
Contact: Charley Kline (kline@uiuc.edu)
Note: select one of (ntp-0.cso.uiuc.edu, ntp-1.cso.uiuc.edu, ntp- 2.cso.uiuc.edu) to equalize load. Use names rather than IP addresses if possible. The ntp-N aliases follow wherever the service is moved to.

LXXIX. US IL ntp-1.cso.uiuc.edu (130.126.24.24)
Location: University of Illinois, Urbana-Champaign, IL
Synchronization: NTP secondary (stratum 2), Cisco-ASM/4
Service Area: CICNET, Midwest, NCSA region
Access Policy: open access
Contact: Charley Kline (kline@uiuc.edu)
Note: select one of (ntp-0.cso.uiuc.edu, ntp-1.cso.uiuc.edu, ntp- 2.cso.uiuc.edu) to equalize load. Use names rather than IP addresses if possible. The ntp-N aliases follow wherever the service is moved to.

LXXX. US IL ntp-1.mcs.anl.gov (140.221.9.20)
Location: Argonne National Laboratory, near Chicago, IL
Synchronization: NTP V3 secondary (stratum 2), Sun Sparcstation
Service Area: NSF/ANSNet, CICNet, NetIllinois, ESNet, others welcome
Policy: open access, please send a message to notify
Contact: Systems Staff (ntp-contact@mcs.anl.gov)
Note: IP addresses are subject to change; please use DNS

LXXXI. US IL ntp-2.cso.uiuc.edu (130.126.24.44)
Location: University of Illinois, Urbana-Champaign, IL
Synchronization: NTP secondary (stratum 2), Cisco-ASM/4
Service Area: CICNET, Midwest, NCSA region
Access Policy: open access
Contact: Charley Kline (kline@uiuc.edu)
Note: select one of (ntp-0.cso.uiuc.edu, ntp-1.cso.uiuc.edu, ntp- 2.cso.uiuc.edu) to equalize load. Use names rather than IP addresses if possible. The ntp-N aliases follow wherever the service is moved to.

LXXXII. US IL ntp-2.mcs.anl.gov (140.221.9.6)
Location: Argonne National Laboratory, near Chicago, IL
Synchronization: NTP secondary (stratum 2), Sun Sparcstation 2
Service Area: NSF/ANSNet, CICNet, NetIllinois, ESNet, others welcome
Access Policy: open access, please send a message to notify
Contact: Systems Staff (ntp-contact@mcs.anl.gov)
Note: IP addresses are subject to change; please use DNS

LXXXIII. US IN gilbreth.ecn.purdue.edu (128.46.129.93, 128.46.141.93, 128.46.147.93, 128.46.148.93, 128.46.171.93)
Location: Purdue University Engineering Computer Network, West Lafayette, IN
Synchronization: NTP V3 secondary (stratum 2), Sun SPARCserver 1000/Solaris 2.3
Service area: NSFNET, CICNET area
Access policy: open access
Contact: Mike Moya (moyman@ecn.purdue.edu)

LXXXIV. US IN harbor.ecn.purdue.edu (128.46.128.76, 128.46.129.76, 128.46.154.76)
Location: Purdue University Engineering Computer Network, West Lafayette, IN
Synchronization: NTP V3 secondary (stratum 2), Sun-4/75+/Solaris 2.3
Service area: NSFNET, CICNET area
Access policy: open access
Contact: Mike Moya (moyman@ecn.purdue.edu)

LXXXV. US IN molecule.ecn.purdue.edu (128.46.129.95, 128.46.132.95, 128.46.136.95, 128.46.145.95, 128.46.167.95, 128.46.169.95, 128.46.181.95)
Location: Purdue University Engineering Computer Network, West Lafayette, IN
Synchronization: NTP V3 secondary (stratum 2), Sun SPARCserver 1000/Solaris 2.3
Service area: NSFNET, CICNET area
Access policy: open access
Contact: Mike Moya (moyman@ecn.purdue.edu)

LXXXVI. US KS ntp1.kansas.net (199.240.130.1)
Location: KansasNet OnLine Services, Manhattan, KS
Synchronization: NTP V3 secondary (stratum 2), Linux on Intel
Service area: Central USA / Great Plains

Access policy: open access to ntp1.kansas.net *or* ntp2.kansas.net; customers may use both servers.
Contact: support@kansas.net

LXXXVII. US KS ntp2.kansas.net (199.240.130.12)
Location: KansasNet OnLine Services, Manhattan, KS
Synchronization: NTP V3 secondary (stratum 2), Linux on Intel
Service area: Central USA / Great Plains
Access policy: open access to ntp1.kansas.net *or* ntp2.kansas.net; customers may use both servers.
Contact: support@kansas.net

LXXXVIII. US MA timeserver.cs.umb.edu (158.121.104.4)
Location: UMass-Boston CS dept, Boston, MA
Synchronization: NTP V3 secondary (stratum 2), DEC/Ultrix
Service Area: Service Area: New England
Access Policy: Open. Please notify
Primary Contact: Rick Martin (rickm@cs.umb.edu)
Secondary Contact: Leonard David (ldavid@cs.umb.edu)

LXXXIX. US MN ns.nts.umn.edu (128.101.101.101)
Location: Minneapolis, MN
Synchronization: NTP secondary (stratum 2), Sun/SunOS 4.1.3
Service Area: CICNET region
Access Policy: open access, please send a message to notify.
Networking & Telecommunications Services (nts@nts.umn.edu)
Note: select one of ns.nts.umn.edu or nss.nts.umn.edu to equalize load

XC. US MN nss.nts.umn.edu (134.84.84.84)
Location: St Paul, MN
Synchronization: NTP secondary (stratum 2), Sun/SunOS 4.1.3
Service Area: CICNET region
Access Policy: open access, please send a message to notify.
Networking & Telecommunications Services (nts@nts.umn.edu)
Note: select one of ns.nts.umn.edu or nss.nts.umn.edu to equalize load

XCI. US MO everest.cclabs.missouri.edu (128.206.206.12)
Location: University of Missouri-Columbia, Columbia, MO, USA
Synchronization: NTP secondary (stratum 2), SGI Indigo R4000/IRIX 5.3
Service Area: MOREnet
Access Policy: open access, please send a message to notify
Contact: Paul Walmsley (ccshag@cclabs.missouri.edu) or timemaster@cclabs.missouri.edu

XCII. US NC clock1.unc.edu (152.2.21.1)
Location: University of North Carolina-Chapel Hill, Chapel Hill, NC
Geographic Coordinates: 35:54N, 79:03W
Synchronization: NTP secondary (stratum 2), Sun4/SunOS/xntpd (V3)
Service Area: CONCERT region
Access Policy: CONCERT region, others by prior arrangement
Contact: Timekeeper (timekeeper@clock1.unc.edu) NOTE: The default restriction on this host is "noserve". Hosts outside the service area must make prior arrangements to receive time service.

XCIII. US NE allison.radiks.net(205.138.126.83)
Location: Radiks Internet Access Omaha, NE
Synchronization: NTP secondary (stratum 2), Slackware 7 Linux
Service Area: Midwest USA
Access Policy: open access
Contact: Kyle Barrett(spoon@allison.radiks.net)
Note: allison.radiks.net is a CNAME

XCIV. US NV cuckoo.nevada.edu (131.216.1.101)
Location: University of Nevada System Computing Services, Las Vegas,NV
Synchronization: NTP V3 secondary (stratum 2), DEC Alpha/Unix
Service Area: NevadaNet, NSFNET, SDSC region
Access Policy: open access, please send message to notify
Contact: Systems Group (software@nevada.edu)
Note: cuckoo.nevada.edu is a CNAME for alphabits.nevada.edu

XCV. US NV tick.cs.unlv.edu (131.216.16.9)
Location: UNLV College of Engineering, Las Vegas, NV
Synchronization: NTP V3 secondary (stratum 2), Mips/Unix

Service Area: Sprintnet
Access Policy: open access
Contact: <jay@egr.unlv.edu>
Note: select one of tick.cs.unlv.edu or tock.cs.unlv.edu at random to equalize load

XCVI. US NV tock.cs.unlv.edu (131.216.18.4)
Location: UNLV College of Engineering, Las Vegas, NV
Synchronization: NTP V3 secondary (stratum 2), Mips/Unix
Service Area: Sprintnet
Access Policy: open access
Contact: <jay@egr.unlv.edu>
Note: select one of tick.cs.unlv.edu or tock.cs.unlv.edu at random to equalize load

XCVII. US NY ntp.ctr.columbia.edu (128.59.64.60)
Location: Columbia University Center for Telecommunications Research; New York City, NY
Synchronization: NTP secondary (stratum 2), Sun/Unix
Service Area: Sprintlink/NYSERnet
Access Policy: open access, authenticated NTP (DES/MD5) available
Contact: Seth Robertson (timekeeper@ctr.columbia.edu)
Note: IP addresses are subject to change; please use DNS

XCVIII. US NY ntp0.cornell.edu
Location: Cornell University, Ithaca, NY
Synchronization: NTP secondary (stratum 2), Sun/Unix
Service Area: NYSERNet, NYSERNet 2000, Internet2/Abilene, vBNS
Access Policy: open access
Contact: Phil Pishioneri (pgp1@cornell.edu)
Note: IP addresses are subject to change; please use DNS.
Note: Open access for clients, though an email is appreciated (especially if peering).

XCIX. US NY ntp1.magenet.com (206.20.254.50)
Location: Valley Of The Mage Consulting, Islandia, New York, USA
Synchronization: NTP secondary (stratum 2), 2xi686/Linux 2.4
Service area: New York City, USA
Access policy: open access, please contact by e-mail to let us know you are using it.
Contact: Brian Bruns (bruns@magenet.com)

C. US NY sundial.columbia.edu (128.59.35.142)
Location: Morningside Campus, Columbia University, New York, NY
Synchronization: NTP V3 secondary (stratum 2), Sun Sparc10 model 40
Service Area: NYSERnet
Access Policy: open access
Contact: timekeeper@columbia.edu

CI. US NY timex.cs.columbia.edu (128.59.16.20)
Location: Columbia University Computer Science Department, New York City, NY
Synchronization: NTP secondary (stratum 2), Sun/Unix
Service Area: PSINET; NSFNET, NYSER region
Access Policy: open access, authenticated NTP (DES/MD5) available
Contact: James Tanis (timekeeper@cs.columbia.edu)
Note: IP addresses are subject to change; please use DNS

CII. US OK constellation.ecn.uoknor.edu (129.15.22.8)
Location: University of Oklahoma, Norman, Oklahoma, USA
Synchronization: NTP secondary (stratum 2), Mac Quadra 700/A/UX 3.0
Service Area: Midnet
Access Policy: open access
Contact: Robert Shull (rob@mailhost.ecn.uoknor.edu)

CIII. US OR tick.koalas.com (207.48.109.6)
Location: Koala Computers, Coos Bay, OR
Geographic Coordinates: 43.36N 124.19W
Synchronization: NTP V3 Secondary (Stratum 2), PC/Linux
Service Area: Northwestern U.S.
Access Policy: open access
Contact: (webmaster@koalas.com)

CIV. US PA clock-1.cs.cmu.edu (128.2.250.95)
Location: Carnegie Mellon University Computer Science, Pittsburgh, PA

Synchronization: NTP V3 secondary (stratum 2), Sun Sparc/Solaris 2.5.1
Service Area: PSC region
Access Policy: semi-open access; for use only by prior arrangement
Contact: Help@cs.cmu.edu
Note: The host name is an alias used only for time service.

CV. US PA clock-2.cs.cmu.edu (128.2.222.8)
Location: Carnegie Mellon University Computer Science, Pittsburgh, PA
Synchronization: NTP V3 secondary (stratum 2), Sun Sparc/SunOS 4.1.4
Service Area: PSC region
Access Policy: semi-open access; for use only by prior arrangement
Contact: Help@cs.cmu.edu
Note: The host name is an alias used only for time service.

CVI. US PA clock.psu.edu (128.118.25.3)
Location: Penn State University, University Park, PA
Geographic Coordinates: 40:47:58.1N, 77:51:44.8W (USGS 40077-G7-TF-024)
Synchronization: NTP V3 secondary (stratum 2), Sun/Unix
Service Area: Internet2, vBNS, CERFnet(AT&T IP Services), PSC/NCNE, CASC.
Access Policy: open access
Contact: John Balogh <JDB@psu.edu>
Note: clock.psu.edu is a CNAME for otc2.psu.edu

CVII. US PA fuzz.psc.edu (128.182.58.100)
Location: Pittsburgh Supercomputing Center, Pittsburgh, PA
Synchronization: NTP V3 secondary (stratum 2), DEC5000/200
Service area: NSFNET, PSC region
Access policy: open access, but please send a message to notify.
Contact: noc@psc.edu

CVIII. US PA ntp-1.ece.cmu.edu 128.2.236.71
Location: Carnegie Mellon Electrical and Computer Engineering, Pittsburgh, PA
Geographic Coordinates: 40:26N, 79:57W
Synchronization: NTP V3 secondary (stratum 2), IBM 40P/AIX 4.1.5
Service Area: PREPNET, PSC region
Access Policy: open access, please notify
Contact: ECE Facilities (gripe@ece.cmu.edu)
Note: Name is an alias for use by NTP.

CIX. US PA ntp-2.ece.cmu.edu 128.2.25.7
Location: Carnegie Mellon Electrical and Computer Engineering, Pittsburgh, PA
Geographic Coordinates: 40:26N, 79:57W
Synchronization: NTP V3 secondary (stratum 2), IBM 40P/AIX 4.1.5
Service Area: PREPNET, PSC region
Access Policy: open access, please notify
Contact: ECE Facilities (gripe@ece.cmu.edu)
Note: Name is an alias for use by NTP.

CX. US TX ntp.cox.smu.edu (129.119.80.126)
Location: Cox School of Business, Southern Methodist University, Dallas, TX
Synchronization: NTP V3 secondary (stratum 2), DEC 3000/300LX AXP DEC OSF/1 AXP
Service Area: NSFNET, SESQUI region
Access Policy: open access
Contact: Allen Gwinn (allen@mail.cox.smu.edu)
Note: Please send e-mail letting us know you will be using ntp.cox.smu.edu. ntp.cox.smu.edu is a CNAME for nyse.cox.smu.edu.

CXI. US TX ntp.fnbhs.com (209.144.20.76)
Location: First National Bank of Hughes Springs, TX
Synchronization: NTP secondary (stratum 2), Debian Linux 2.1
Service area: Northeast Texas
Access policy: open access, please send a message to notify
Contact: walterp@fnbhs.com

CXII. US TX ntp.tmc.edu (128.249.1.10)
Location: Baylor College of Medicine, Houston, Tx
Synchronization: NTP secondary (stratum 2), Sun/Solaris
Service Area: NSFNET, SESQUI region
Access Policy: open access
Contact: Postmaster (postmaster@tmc.edu)

CXIII. US TX ntp5.tamu.edu (165.91.52.110)
Location: Texas A&M University, College Station, TX
Synchronization: NTP secondary (stratum 2, ver. 3), SPARCstation 10/Solaris 1.x
Service area: NSFNET, SESQUI region, THEnet, TAMUSDSN
Access policy: open access
Contact: NTP Administrator (ntp@tamu.edu)

CXIV. US TX tick.greyware.com (207.55.146.19)
Location: Greyware Automation Products, Plano, TX
Synchronization: NTP secondary (stratum 2), Windows NT
Service Area: South-Central US, others by arrangement
Access Policy: open access for any server with 50+ clients
Contact: techsupport@greyware.com
Note: IP may change, please use DNS name. Other protocols offered include TIME-UDP, TIME-TCP, and Domain Time II

CXV. US TX tock.greyware.com (207.55.146.54)
Location: Greyware Automation Products, Plano, TX
Synchronization: NTP secondary (stratum 2), Windows NT
Service Area: South-Central US, others by arrangement
Access Policy: open access for any server with 50+ clients
Contact: techsupport@greyware.com
Note: IP may change, please use DNS name. Other protocols offered include TIME-UDP, TIME-TCP, and Domain Time II

CXVI. US VA ntp-1.vt.edu (198.82.162.213)
Location: Virginia Tech Computing Center, Blacksburg, VA, USA
Synchronization: NTP V 3 secondary (Stratum 2), DEC Alpha
Service Area: southeastern US, anyplace netwise close to vBNS
Access Policy: open access
Contact: Valdis.Kletnieks@vt.edu
Note: ntp-1.vt.edu is currently a CNAME for vtserf.cc.vt.edu. This is however subject to change, please use the CNAME.

CXVII. US VA ntp-2.vt.edu (198.82.161.227)
Location: Virginia Tech Computing Center, Blacksburg, VA, USA
Synchronization: NTP V4 secondary (Stratum 2), RS/6000-F40
Service Area: southeastern US, anyplace netwise close to vBNS
Access Policy: open access
Contact: Valdis.Kletnieks@vt.edu
Note: ntp-2.vt.edu is currently a CNAME for proxy.cc.vt.edu. This is however subject to change, please use the CNAME.

CXVIII. US VA ntp.cmr.gov (140.162.8.3)
Location: Center for Seismic Studies, Arlington, VA
Geographic Coordinates: 38:53:50N, 77:04:34W
Synchronization: NTP V3 secondary (stratum 2), Sun-Sparc-5, Solaris 5.5.1
Service Area: NSFNET, SURA region
Access Policy: open access
Contact: timekeeper (timekeeper@cmr.gov)

CXIX. US WA clock.tricity.wsu.edu (192.31.216.30)
Location: Washington State University Tri-Cities, Richland, WA
Synchronization: NTP secondary (stratum 2), DS5000/Ultrix
Service Area: NSFNET, NorthWestNet
Access Policy: open access
Contact: postmaster@beta.tricity.wsu.edu)

CXX. US WA ntp.tcp-udp.net (use DNS)
Location: Mill Creek, Washington, USA
Geographic Coordinates: 47:51:40.7N 122:11:23.5W
Synchronization: NTP secondary (stratum 2), i486/Linux
Service Area: Northwest USA
Access Policy: Open access **after** reading our time server usage notes.
Contact: **timekeeper** at the above domain.

CXXI. US WI ntp1.cs.wisc.edu (128.105.39.11)
Location: Computer Science Department, University of Wisconsin-Madison
Geographic Coordinates: 89:24:30W, 43:08:00N
Synchronization: NTP V4 secondary Solaris 2.7
Service Area: US/any
Access Policy: open access
Contact: David Thompson (ntp-admin@cs.wisc.edu)

Note: IP addresses are subject to change; please use DNS

CXXII. US WI ntp2.cs.wisc.edu (128.105.38.11)
Location: Computer Science Department, University of Wisconsin-Madison
Geographic Coordinates: 89:24:30W, 43:08:00N
Synchronization: NTP V4 secondary Solaris 2.7
Service Area: US/any
Access Policy: open access
Contact: David Thompson (ntp-admin@cs.wisc.edu)
Note: IP addresses are subject to change; please use DNS

CXXIII. US WI ntp3.cs.wisc.edu (128.105.37.11)
Location: Computer Science Department, University of Wisconsin-Madison
Geographic Coordinates: 89:24:30W, 43:08:00N
Synchronization: NTP V4 secondary Solaris 2.7
Service Area: US/any
Access Policy: open access
Contact: David Thompson (ntp-admin@cs.wisc.edu)
Note: IP addresses are subject to change; please use DNS

CXXIV. VE ntp.linux.org.ve (150.188.8.196)
Localizaci: VELUG, Grupo de Usuarios Linux de Venezuela
Sincronizaci: NTP secundario (stratum 2), Pentium/Linux
=Area de Servicio: Arica
Potica de Acceso: Abierta, por favor enviar e-mail para notificar
Contacto: time@linux.org.ve

CXXV. ZA ntp.cs.unp.ac.za (143.128.82.200)
Location: Natal University, Pietermaritzburg, South Africa
Synchronization: NTP V3 secondary (stratum 2), SGI Indy/Irix6.2
Service area: South Africa
Access policy: open access, please send a message to notify
Contact: sysadmin@cs.unp.ac.za

CXXVI. ZA ntp.cs.unp.ac.za (143.128.82.200)
Location: Natal University, Pietermaritzburg, South Africa
Synchronization: NTP V3 secondary (stratum 2), SGI Indy/Irix6.2
Service area: South Africa
Access policy: open access, please send a message to notify
Contact: sysadmin@cs.unp.ac.za

Discontinued Service

black-ice.cc.vt.edu
chime.utoronto.ca
chime1.surfnet.nl
churchy.udel.edu
delphi.cs.ucla.edu
dominator.eecs.harvard.edu
eagle.tamu.edu
finch.cc.ukans.edu
fuzz.sura.net
gazette.bcm.tmc.edu
kuhub.cc.ukans.edu
lassen.slc.ca.gov
libra.rice.edu
ntp.olivetti.com
ntp1.ossi.com
ntp1.sura.net
ntp2.ossi.com
ntp2.sura.net
salmon.maths.tcd.ie
smart1.svi.org
tick.anice.net.ar
ticktock.wang.com
time.software.net
tmc.edu
tock.anice.net.ar
vtserf.cc.vt.edu

wuarchive.wustl.edu
www1.cmc.ec.gc.ca
www2.cmc.ec.gc.ca
xfiles-jr.esa.lanl.gov
xfiles.esa.lanl.gov

See Also...

Time Servers
Time Sync

TraceRoute - How It Works

How TraceRoute Works

The NetScanTools implementation of TraceRoute varies a bit from the standard UNIX traceroute by the type of packets sent to the target host system. Most UNIX systems send a UDP[103] packet to a high port.

TraceRoute starts by sending an ICMP Echo Request packet (see RFC 792 for the ICMP types) to the target host with a TTL value of 1 (unless you specify otherwise). *TTL (Time To Live) is a field in the IP header used to define the amount of time that a packet is allowed to live in the internet.* Then it waits a specified time for a response and sends another packet with a TTL of 2 and so forth. Each router beyond your system decrements the TTL value found in the header; if it sees that the value is zero, it discards your Echo Request packet, then it returns another ICMP message back to your computer's IP address with the ICMP type field set to Time Exceeded. When it does this, the IP address of the router's interface nearest to your system is placed in the IP header source field. This address is displayed by NetScanTools and the IP address is translated to a hostname if so desired and the hostname exists in your DNS.

An interesting digression to this discussion is that the IP address you see for each host along the route is usually only one of two or more IP addresses assigned to that machine. The IP address you see is that of the network interface nearest to your computer. You do not see the IP address of the network interface connecting from the intermediate router to other computers.

After using this utility for awhile, you will discover that the first hop or two or three will always be the same (through your default gateway), but from some point on, the route will begin to vary greatly with the target host. Packets may not even travel the same route twice en route to a destination. This is due to network loading or other changes in the routing tables. Your packets may travel through several hops on one internet backbone provider, then switch to another backbone provider before reaching a gateway to the final host.

See Also...

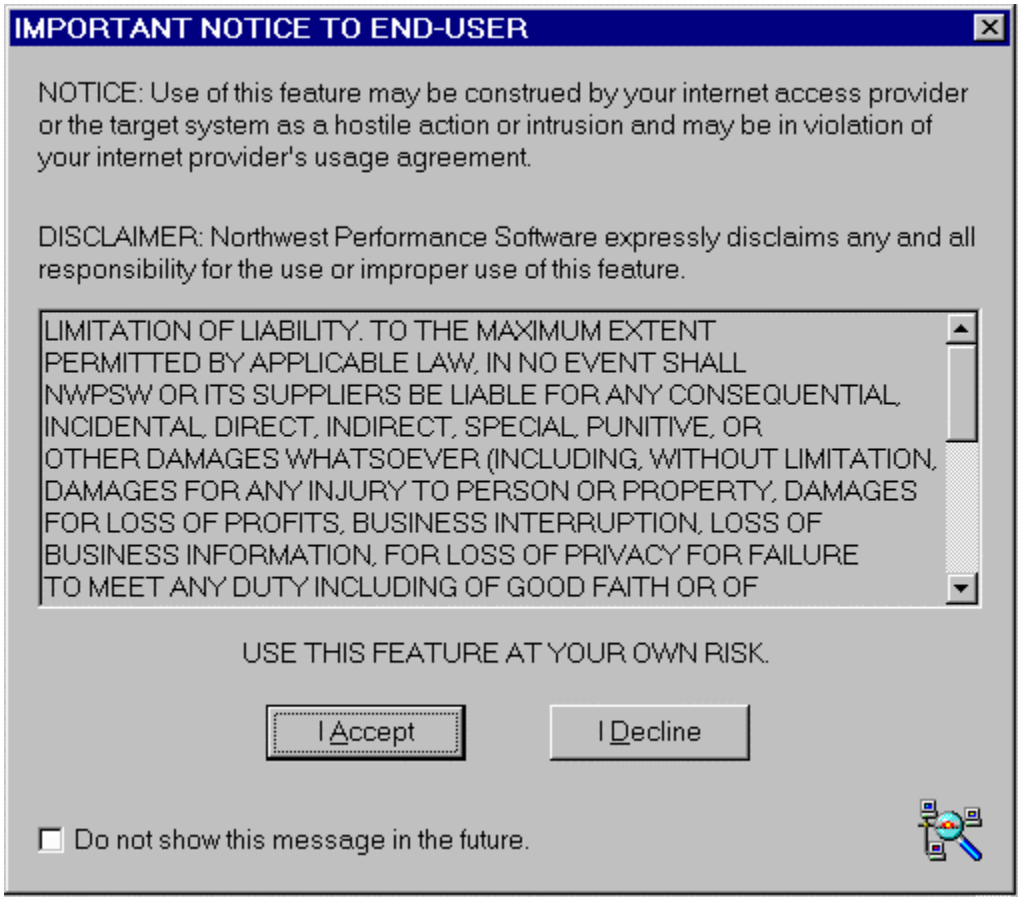
TraceRoute
TraceRoute Setup

[103] UDP means User Datagram Protocol and it defined in RFC 768. Unlike TCP, it does not provide a reliable protocol for assuring the delivery of packets between networked computer systems.

Usage Warning Dialog

The feature you have selected may be used in a malicious manner. Please review the following dialog box. You can Accept or Decline to continue. You can also permanently decline to view this dialog by checking the '**Do not show this message in the future.**' checkbox.

This dialog is displayed for the Port Prober.



Using AutoPaste

Background

NetScanTools has a button located next to the copy button with a strange label: '<->'. This button activates the AutoPaste feature. AutoPaste takes text from the input area of the current tab or any highlighted text in a results area and presents it to the user for inclusion into the AutoPaste buffer. Text in the AutoPaste buffer is automatically pasted into the input area of any tab that you switch to. This is very useful for transferring IP addresses and long hostnames between tabs.

For the following example, you must be actively connected to a TCPIP network PRIOR to starting NetScanTools.

Using AutoPaste.

I. Start NetScanTools.

II. On the Name Server Lookup tab, enter www.nwpsw.com and press the Simple Query button.

III. When you see the results, highlight the IP address and press the <-> button at the bottom of the main window.

IV. You will be presented with the AutoPaste Host/IP Selection dialog box. The IP address that you highlighted will appear on the top line with a '>>' button to the left. The query text 'www.nwpsw.com' will appear in the lower line, also with a '>>' button. Select either one by pressing the '>>' next to it. The dialog box will disappear and the text you selected will appear in the input area of the other client function tabs when you switch to them.

Note: you can clear the AutoPaste buffer by pressing the '<->' button and clicking on the Clear AutoPaste button. You can also clear it by exiting and restarting NetScanTools. NetScanner and some other tabs will only display IP addresses contained in the AutoPaste buffer; it will not paste hostnames.

See Also...

AutoPaste
Usage Tips

Viewing Hidden Headers in Web Pages

Background

Web pages (HTML or HTM) contain formatting information to tell your web browser how to format the page. They also contain headers which can tell you a lot about the web server software residing on the machine that sent you the web pages to view. Typical things that you might see are the type and version of web server software used, the creation date (in GMT) of the web page, and the number of bytes in the web page HTML file. For the following example, you must be actively connected to a TCPIP network PRIOR to starting NetScanTools.

Grabbing a web page.

I. Start NetScanTools.
II. Switch to the 'What's New at NWPSW' tab. (The first time you do this after the program has been started, it will automatically get the Latest News web page from us.)
III. Enter any URL in normal format: http://www.nwpsw.com/index.html
IV. Press the 'Get URL' button.
V. Check the 'Display HTTP Headers and HTML Tags' checkbox.
VI. You should see the results similar to these as shown below:

```
HTTP/1.0 200 OK
Server: Netscape-Enterprise/2.01
Date: Mon, 05 Jan 1998 15:35:46 GMT
Accept-ranges: bytes
Last-modified: Sun, 04 Jan 1998 15:16:59 GMT
Content-length: 2597
Content-type: text/html

What's New at Northwest Performance Software, Inc for Jan 4, 1998
Maple Valley Weather: rain Hi: 39 deg F
```

See Also...

Usage Tips
What's New at NWPSW

Y2K Information

NOTICE: This Information is designated as a Year 2000 Readiness Disclosure and the information contained herein is provided pursuant to the Year 2000 Information and Readiness Disclosure Act.

NetScanTools contains two functions which are time sensitive. All other functions are not known to be time sensitive.

Time Sensitive Functions with individual Y2K information on their respective help topices:

Time Sync
Daytime

All printouts with dates use 4 digit dates when printing.

AutoClear AutoClear clears the results area of this tab each time a new function is activated.

AutoSize The AutoSize button causes all columns in a report style list view to be sized to the widest text string found in the column.

Clear Results The results area of this tab are cleared when this button is pressed.

Data Viewer Window The Data Viewer window is used to display text. You can copy text from Data Viewer by highlighting and right-clicking to bring up the edit menu. You can also locate and find any text (not case sensitive) using the Find and Find Again buttons. You can print or save the data to a file.

The Data Viewer window is use frequently throughout NetScanTools to display text from special display elements like listviews and treeviews.

DHCP DHCP - Dynamic Host Configuration Protocol. A method of dynamically assigning an IP address, subnet mask and default gateway from a DHCP server responsible for the subnet. See RFC 1542.

DNS **D**omain **N**ame **S**ervice - This is a distributed, static database which allows computer users to specify computer nodes by names rather than by IP addresses. It is known as BIND under BSD UNIX and is commonly hosted on Unix platforms, although DNS is provided with Windows NT 4.0 Server.

Domain Name Domain Name is the name of the domain that a group of computer systems are assigned to. netscantools.com or nwpsw.com are domain names.

Hostname Hostname is the name of a host or computer system connected to a network. This name typically appears in a DNS. A hostname normally contains the name of the host with the domain name appended. Example: www.netscantools.com

Hosts File A hosts file is used on a local computer to rapidly resolve the name of a host or an IP address without necessitating the need to query a DNS. Winsock normally looks for and scans a hosts file prior to communicating with DNS.

ICMP **I**nternet **C**ontrol **M**essage **P**rotocol - assists in determining when packet transmission errors have occurred.

IP IP means internet protocol as defined in RFC 791. A method of transmitting packets of data called datagrams between source and destination computer systems. Each computer is identified by a fixed length address called an IP address.

IP Address Also known as IPv4. A 32 bit address that uniquely identifies a computer network node to other network nodes. IP addresses are most commonly represented as four decimal groups of octets separated by decimal points. An IP address of 10.1.5.3 is the same as the four bytes: 0x0A010503 in hexadecimal network byte order. Spammers sometimes take advantage of a more obscure representation of an IP address as a single number, ie. http://167838979/spam.html where 167838979 is the decimal representation of 10.1.5.3.

LANA **L**ocal **A**rea **N**etwork **A**dapter -- see NetBIOS Info tab.

MAC address **M**edia **A**ccess **C**ontrol Address is a 48 bit binary number used as a physical address which is theoretically unique for every network card manufactured. It is used by the ARP protocol to map an IP address to a MAC address.

NetBIOS **N**etwork **B**asic **I**nput **O**utput **S**ystem - this is an application program interface which is used by software programs to communicate over a local area network.

Services A service or daemon is a program that listens for incoming connections on a TCP/IP port and responds accordingly. Examples are web servers or mail services like SMTP.

SMTP SMTP - **S**imple **M**ail **T**ransfer **P**rotocol. For more information, see RFC 821.

Stop The **Stop** button stops or cancels the current activity.

TCP TCP means transmission control protocol as defined in RFC 793. It is intended to provide a highly reliable method of assuring delivery of packets between network connected computer systems and uses IP as a next level lower protocol layer.

TCP/IP TCP/IP means Transmission Control Protocol--TCP (see RFC 793) over Internet Protocol--IP (see RFC 791).

UDP UDP means User Datagram Protocol and it defined in RFC 768. Unlike TCP, it does not provide a reliable protocol for assuring the delivery of packets between networked computer systems.

Winsock Winsock is derived from the sockets concepts found in BSD (Berkeley Software Distribution) UNIX. NetScanTools requires Winsock 2 or above for proper operation.

