Port Scanner © 1995 Blue Globe Software

Port Scanner is shareware.

You are permitted to examine Port Scanner for 30 days to determine if it meets your needs. If you continue to use Port Scanner beyond this period, you are required to obtain a shareware license from Blue Globe Software. See the enclosed order details for information on acquiring a shareware license.

Port Scanner 1.1 Help

Port Scanner Order Information

Version 1.2b1

Port Scanner is distributed by Blue Globe Software as shareware.

GRANT. Blue Globe Software ("Blue Globe") hereby grants you a non-exclusive license to use its accompanying software product ("Software"), free of charge for 30 days from the time you first acquire it. This period is intended as a means for you to evaluate the Software and determine if you wish to continue its use. If, after this period, you intend to continue using the Software you must acquire a shareware license for the Software from Blue Globe.

Shareware licenses are available to students of registered education institutions for $10 (US). Licenses to all other users are $30 (US). In addition, site-licensing is available (see the accompanying registration form). A shareware license permits you to: use the Software on a single computer; copy the Software onto a second computer so long as the first and second computers are not used simultaneously; copy the Software for archival purposes, provided that all the original help files and documents are contained with the original. Title, ownership rights, and intellectual property rights in and to the Software shall remain in Blue Globe. The Software is protected by the copyright laws of Canada and international copyright treaties.

OBTAINING A SHAREWARE LICENSE:
1) Print out and fill in the registration form (register.doc) that came with your copy of Port Scanner, or write down the following information (please print neatly) on a sheet of paper:

> Name, Company, Street Address, City, Province/State, Postal/Zip Code, Country, Email Address, Phone number (optional), Type of registration (student or standard), and the payment amount you have enclosed.

2) Mail the registration information from step 1, along with your payment in US funds (sorry, no credit cards are accepted), to:

> Blue Globe Software
> PO Box 8171
> Victoria, BC
> CANADA V8W 3R8

3) Within seven days of your registration being received, you will be sent a serial number. This serial number, when combined with your full name, will allow you to disable the shareware messages that appear as Port Scanner starts and quits, and will enable the ability to use more than five lines in a scanning script.

DISCLAIMER OF WARRANTY. The Software is provided on an “AS IS” basis, without warranty of any kind, including without limitation the warranties of merchantability, fitness for a particular purpose and non-infringement. The entire risk as to the quality and performance of the Software is borne by you. Should the Software prove defective, you and not Blue Globe assume the entire cost of any service and repair. This disclaimer of warranty constitutes an essential part of the shareware license. SOME STATES DO NOT ALLOW EXCLUSIONS OF AN IMPLIED WARRANTY, SO THIS DISCLAIMER MAY NOT APPLY TO YOU AND YOU MAY HAVE OTHER LEGAL RIGHTS THAT VARY FROM STATE TO STATE OR BY JURISDICTION.

LIMITATION OF LIABILITY. UNDER NO CIRCUMSTANCES AND UNDER NO LEGAL THEORY, TORT, CONTRACT, OR OTHERWISE, SHALL BLUE GLOBE OR ITS SUPPLIERS OR RESELLERS BE LIABLE TO YOU OR ANY OTHER PERSON FOR ANY INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY CHARACTER INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF GOODWILL, WORK STOPPAGE, COMPUTER FAILURE OR MALFUNCTION, OR ANY AND ALL OTHER COMMERCIAL DAMAGES OR LOSSES. IN NO EVENT WILL BLUE GLOBE BE LIABLE FOR ANY DAMAGES IN EXCESS OF BLUE GLOBE’S LIST PRICE FOR A LICENSE TO THE SOFTWARE, EVEN IF BLUE GLOBE SHALL HAVE BEEN INFORMED OF THE POSSIBILITY OF SUCH DAMAGES, OR FOR ANY CLAIM BY ANY OTHER PARTY. THIS LIMITATION OF LIABILITY SHALL NOT APPLY TO LIABILITY FOR DEATH OR PERSONAL INJURY TO THE EXTENT APPLICABLE LAW PROHIBITS SUCH LIMITATION. FURTHERMORE, SOME STATES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF INCIDENTAL OR CONSEQUENTIAL DAMAGES, SO THIS LIMITATION AND EXCLUSION MAY NOT APPLY TO YOU.

TERMINATION. This license will terminate automatically if you fail to comply with the limitations described above. On termination, you must destroy all copies of the Software.

What is Port Scanner?

Port Scanner is a tool that allows you to scan a group of IP addresses looking for the presence of specific incoming TCP/IP ports. This is a large benefit to anyone managing a TCP/IP network, or to anyone who is concerned with the possible security risks that some TCP/IP tools present to their network.

Using an intuitive interface that allows you to specify the start and end addresses of a scan, you can quickly check a specific machine, a subnet, or an entire domain. Port Scanner comes predefined to scan for the most common TCP/IP services, and provides a quick way to add new ports to any scan. In addition, Port Scanner lets you scan a subset of the existing ports, and to save subsets into named groups for easy recall. Scan results can be easily printed or save to a file.

Port Scanner requires a WinSock compatible TCP/IP stack, and is fully Windows 95 compatible.

See Also: How do I license my copy?

How Does it Work?

Port Scanner starts at the location you specify as the Start Address and traverses every valid IP number until it reaches the location you specify as the End Address. At every step in the scan, Port Scanner attempts to open a connection to every port you have selected in the Port List. If a successful connection is made, Port Scanner records that information in the results file.

See Also: How do I license my copy?

Specifying Scan Addresses

You inform Port Scanner which addresses you want it to scan by specifying a start and an end address. Port Scanner will check every valid TCP/IP address between the two addresses you specify.

The start address is entered into the Start Address field.
The end address is entered into the End Address field.

An address may be specified using its IP name (which is easier to remember), or its IP number. If an IP name is used, Port Scanner will convert the name into its matching IP number before beginning the scan.

If the end address you specify has a numerically smaller IP number than the start address, Port Scanner will reverse their order before beginning the scan.

If you wish to convert an IP name into its IP number, click the button labeled DNR next to the appropriate address.

Automating Port Scanner

You can have Port Scanner automatically carry out an entire batch of scans by creating a scanning script. Once you have created your scan script, you tell Port Scanner to use it by checking the box labeled *Use scanning script* on the main Port Scanner window. To specify the scan script you would like Port Scanner to use, click the small folder icon next to the text field.

Creating a Scanning Script

A scanning script is a text file that contains one line for each scan you want Port Scanner to carry out. The format of a line is as follows:

```
<start address>,<end address>,<port set name>,<full pathname for results file>
```

For example, let's assume that Port Scanner has been set up with two scan sets, one called *ftp* and another called *mail*. If you wanted to automatically scan for all FTP connections in your engineering and finance subnets, and for all mail connections in your admin subnet, you would place the following lines in a text file:

```
firstbox.engineering.biz.com,lastbox.engineering.biz.com,ftp,c:
\temp\results1.txt
firstbox.finance.biz.com,lastbox.finance.biz.com,ftp,c:\temp\results2.txt
firstbox.admin.biz.com,lastbox.admin.biz.com,mail,c:\temp\results3.txt
```

When Port Scanner reads this file it will run three different scans. One from firstbox to lastbox in engineering.biz.com, looking for all ports in the *ftp* scan set, another from firstbox to lastbox in finance.biz.com, looking for all ports in the *ftp* scan set, and finally, a scan from firstbox to lastbox in admin.biz.com, looking for all ports in the *mail* scan set. The results of each of these scans will be automatically saved into the filename listed on the script line.

Any errors found in the script file will be saved into a log file named *scanerr.txt*. This file is always placed in the same directory as Port Scanner itself.

Converting IP Names into IP Numbers

Both the Start Address and End Address fields have a button to their right labeled **DNR**. Clicking one of these buttons will convert its matching address field from an IP name into an IP number. This procedure is called **D**omain **N**ame **R**esolving (hence the button's name), and it uses the domain name server(s) you specified when you installed your WinSock driver.

If the name in an address field is already a valid IP number, nothing will take place. If the name you have entered cannot be converted into an IP number, either because it is invalid, or because the domain name servers are not responding, an alert will be displayed.

See also: Specifying Scan Addresses

Starting a Scan

Once you have entered IP names or IP numbers into the Start Address and End Address fields, clicking the **Start Scan** button will begin a new scan.

Before a scan begins, Port Scanner will verify that both addresses you have entered are valid. If either address is invalid, an alert will be displayed and the scan will not proceed.

See also: Specifying Scan Addresses

Start Address

The value in the **Start Address** field is where Port Scanner will begin its scan. This value can be entered as either an IP name, or an IP number. Clicking the DNR button next to this field will convert the value from an IP name into its IP number equivalent.

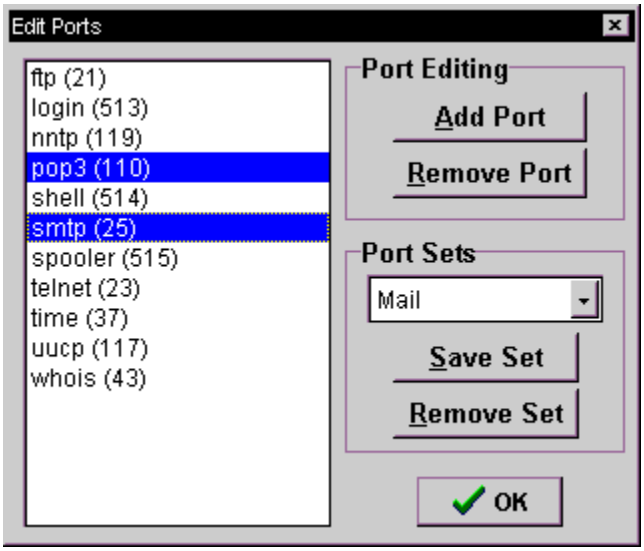
End Address

The value in the **End Address** field is where Port Scanner will end its scan. This value can be entered as either an IP name, or an IP number. Clicking the DNR button next to this field will convert the value from an IP name into its IP number equivalent.

The Edit Ports Window

Port Scanner can only scan for those ports that it is aware of. Though it comes with many of the most common TCP/IP ports already included, you may have need to add, or remove, ports of your own. In addition, you may find yourself repeating many specific types of scans. The Edit Ports window is where you manipulate the list of ports that Port Scanner knows about, and where you can group these ports into scanning sets.

To view Port Scanners Edit Ports window, select the **Edit Ports...** command from the main windows **File** menu.



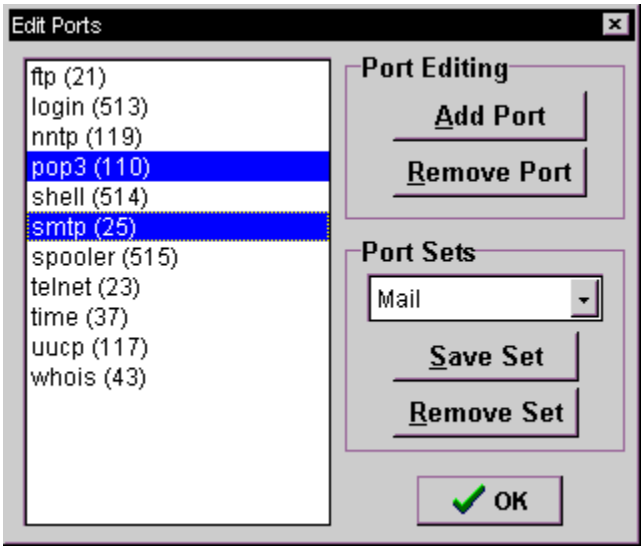
This window consists of three main sections:

Port List
This is a scrolling list containing all the ports that are available for scanning.

Port Editing
This section contains buttons used to add or remove ports from the list.

Port Sets
This area contains a popup list of port sets, and the buttons used to create and remove these sets.

Adding or Removing Ports

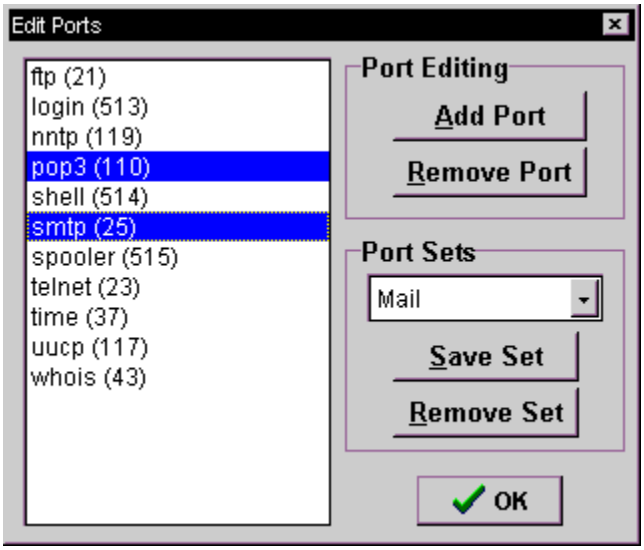


The Port Editing section contains two buttons. These are used to add or remove ports from Port Scanners list.

When the **Add Port** button is clicked, a dialog will appear prompting you to enter the name and port number of the new entry. Use this button to add any ports you want to scan that are not already in the list. If the new port already exists in the list, it will not be added.

A click on the **Remove Port** button will delete the currently highlighted port(s) from the list.

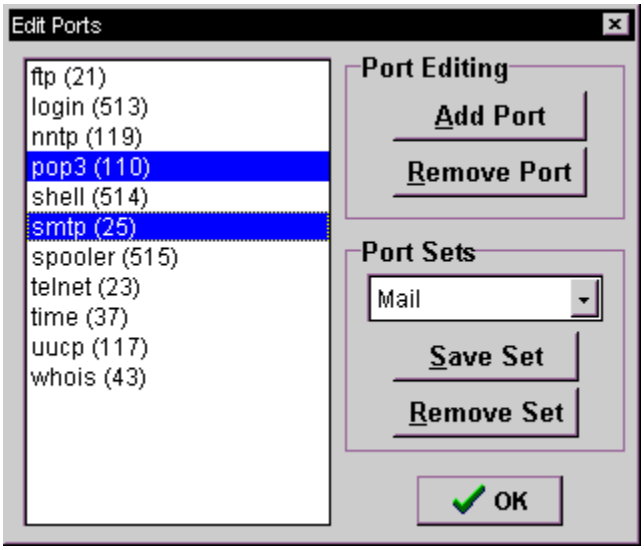
Selecting Scan Ports



Although Port Scanner can have many ports in its list, only those that are highlighted will be included during a scan. This allows you to keep many ports inside Port Scanner for reference, without having them all active during each scan. For example, in the window pictured here, only the pop3' and smtp ports will be scanned.

To select a port from the list, simply click on it with the mouse. To select a group of ports, click on the first one, and shift-click on the last. To select disjoint ports, ctrl-click on each one.

Saving Port Sets



The Port Sets section is used to manipulate port sets. A Port Set is a quick way to highlight an entire group of ports in the port list. For example, if you routinely scan for FTP, Telnet, and HTTP ports, you could place those ports into a port set so you could select them quickly. Common examples of port sets might be mail services (smtp, pop2, pop3), and web services (http, ftp, nntp, smtp).

The popup list is used to select the current port set. When a set is chosen, the ports it references will be highlighted in the list, and all others will be deselected. Note that whenever you click in the port list, the current port set is deselected.

When you click the **Save Set** button you will be asked to name the new Port Set. All ports that are highlighted at the time you click this button will be added to the new set.

The **Remove Set** button will display a list of all Port Sets, prompting you to select the set you want to delete. Note that deleting a Port Set will not delete any of the ports that it references.

The Results Window

When a new scan begins, Port Scanner displays the Results window. This window contains four important elements:

Status
The status indicator displays the current IP address of the port being scanned.

Progress Bar
The progress bar indicates how much of the scan has been completed. This bar is updated every time Port Scanner moves on to a new IP address.

Results Field
This is a large scrollable area that contains the results of the current scan. Every IP address that is scanned will be printed into this area, followed by any ports that were found to be active at that address. If no ports are listed, Port Scanner was unable to locate any of the selected ports at that IP address.

Stop button
A click on this button will stop the current scan.

Printing or Saving Scan Results

Once a scan is complete, you have the option of saving the results to a file or printing them to a printer. To save the results to a file, choose **Save As...** from the File menu. To print the results, choose **Print...** from the File menu.

Port Scanner can only have one Results window open at a time. Therefore, you will not be able to begin a new scan until the current Results window has been closed.

Port Scanner Preferences

Select the **Preferences...** command from the main windows **File** menu to display Port Scanners preferences. This window contains settings that effect various aspects of Port Scanners behavior.

Timeout each scan attempt after...
This is the first setting in the Preferences window. It indicates how many seconds Port Scanner will wait before it determines that a particular port does not exists during a scan. Setting this number smaller than five seconds will result in quicker scans, but may cause some ports to remain undetected on slow networks. Five seconds is usually a good value for this field, though you may want to increase this number if your network is slow. Experiment by scanning the slowest machine on your network for a port you know exists. The lowest value that still allows Port Scanner to detect that port is the value you should probably use.

Play this sound upon completion...
If this box is checked Port Scanner plays a sound when it completes each scan. The field below this checkbox contains the full pathname of the .WAV file that Port Scanner will play. To specify a different .WAV file, click the small folder button (it looks like this ).