Portmon
Enterprise Edition

http://www.sysinternals.com

Portmon is an application that lets you monitor serial and parallel activity on your local system, or any computer on the network that you can reach via TCP/IP. It is the most powerful tool available for tracking down port-related configuration problems and analyzing application port usage.

Portmon works on Windows NT 4.0, Windows 2000, Windows 95 and Windows 98. Note: if you want to run *Portmon* on Windows 95 you must install the WinSock2 update, available for free download from Microsoft's Web site.

Systems Internals™

Simply execute the *Portmon* program file (Portmon.exe) and *Portmon* will immediately start capturing port output. Note that if you run *Portmon* on Windows NT/2000 Portmon.exe must be located on a non-network drive and you must have administrative privilege. Menus, hot-keys, or toolbar buttons can be used to clear the window, save the monitored data to a file, search output, and change the window font.

As events are printed to the output, they are tagged with a sequence number. If your system generates port activity faster than *Portmon* is capable of collecting and displaying, gaps in the sequence numbers may result

Each time you exit *Portmon* it remembers the position of the window, the widths of the output columns, the font selection, configured filters, and the time-stamp mode.

Capture

You control *Portmon*'s capture mode by toggling capture-on and capture-off with the 🔍 toolbar button, the **Capture|Capture Events** menu entry, or the Ctrl+E hot-key sequence. *Portmon* does not capture any data from the computer you are currently viewing when its capture-mode is off.

Port Selection

When you are capturing port output from a Windows NT/2000 system you can control which ports *Portmon* will capture from. Use the **Capture|Ports** menu to select or deselect serial and parallel for capture. *Portmon* remembers what ports are selected when you exit it, and the next time you start *Portmon* only the ports that were selected will be selected for capturing. Note that if a port is already in use by an application *Portmon* may not be able to connect to it. In such cases you must start *Portmon* before you start the application that uses the port.

Portmon has several features that can help you zoom-in on the port output you are interested in. These capabilities include searching, filtering, and limiting the number of output lines saved in the display.

Clearing the Display

To reset the output window, use the **Edit|Clear Display** menu item, toolbar button, or Ctrl+X hot-key sequence. This also causes the sequence number to be reset to 0.

Searching

If you want to search for a line containing text of interest you use the find dialog. The find dialog is activated with the Ctrl+F hot-key sequence, the **Edit|Find** menu entry, or the toolbar button. If the search you specify matches text in the output window, *Portmon* will highlight the matching line and turn off the display's auto-scroll in order to keep the line in the window. To repeat a successful search, use the F3 hot-key.

Filtering

Another way to isolate output that you are interested in is to use *Portmon*'s filtering capability. Use the **Edit|Filter/Highlight** menu item, toolbar button, or Ctrl-L hot-key to activate the filter dialog. The dialog contains two edit fields: include and exclude. The include field is where you enter substring expressions that match port output lines that you want *Portmon* to display, and the exclude field is where you enter text for output lines that you do not want *Portmon* to display. You can enter multiple expressions, separating each with a semicolon (';'). Do not include spaces in the filter expression unless you want the spaces to be part of the filter. Note that the filters are interpreted in a case-insensitive manner, and that you should use '*' as a wildcard.

As an example, say you want *Portmon* to display port output that contains either "temp" or "winnt", but want to exclude lines that contain word "system32". To configure *Portmon*'s filters for this you enter "*temp*;*winnt*" for the include filter and "*system32*" for the exclude filter.

Highlighting

Portmon also has another type of filtering: highlighting. If you want output lines that contain certain text to be highlighted in the *Portmon* output window, enter a highlight filter. Use the same syntax just described for include and exclude filters. As soon as you enter a highlight filter all output lines that match the filter will be highlighted for easy recognition.

To change the colors used for the foreground and background of highlighted lines, choose the **Edit|Filter/Highlight Colors** menu item. You will be asked to pick colors from a palette, and your choices will be remembered by *Portmon* from run to run.

Display Mode (Hex/ASCII)

Use the **Options|Show Hex** menu item or the ab toolbar button to toggle the format *Portmon* uses to display read and write buffer data. You can toggle between hexadecimal and ASCII output. When *Portmon* is displaying ASCII format it will show a '.' for unprintable bytes.

MaxBytes

The size of the buffer that *Portmon* uses to format read and write buffer output is specified with the **Edit|Max Bytes** dialog. By default, *Portmon* limits the amount of data displayed. If you are displaying data in hexadecimal format, then the actual amount of read or write data displayed can be calculated by taking *MaxBytes* and dividing by three (since each byte of data requires three characters of output to display it in hex format). If you are displaying data in ASCII format then there is a one-to-one correspondence between the value of *MaxBytes* you set and the amount of read or write data displayed.

History-Depth

A final way to control *Portmon* output is to limit the number of lines that are retained in the display.

You use the **Edit|History-Depth** menu item, toolbar button, or the Ctrl+H hot-key sequence to activate the history-depth editor. Enter the number of output lines you want *Portmon* to retain and it will keep only that number of the most recent output lines, discarding older ones. A history-depth of 0 represents no limit on output lines retained.

You do not need to use the history-depth feature to prevent all of a system's virtual memory from being consumed in long-running captures. *Portmon* monitors system memory usage and will go into a low-memory state when it detects that memory is running low. *Portmon*'s low-memory state consists of it not capturing further output until the low-memory condition is no longer in effect.

Portmon lets you both save and print captured output.

Saving Output

You can save the contents of the *Portmon* output window as a text file (.log extension) using the **File|Save** or **File|Save As** menu items, or the Ctrl+S hot-key sequence.

Using **Edit|Copy** or the Ctrl+C hot-key sequence you can copy the output contained within selected output lines to the clipboard.

Logging to a File

To have *Portmon* log output to a file as it displays it, use the **Edit|Log to File** or **Edit|Log to File As** menu items, the 💾 toolbar button, or the Ctrl+O hot-key sequence. Log file settings you specify include the name of the log file, the maximum size it should be allowed to grow, and whether or not *Portmon* should restart the log or append to it if the file specified already contains output.

When logging is active the log file toolbar button will look like 💾. To stop logging simply select the toolbar button or the **Edit|Log to File** menu item. A log file maximum size of 0 signifies no limit on the log file size. If the log file's maximum size is reached logging to the file stops and the logging toolbar button changes to 💾.

If you are monitoring port activity on multiple remote computers and enable logging to a file, all output is logged to the file you specify. Ranges of output from different computers are separated with a header that indicates the name of the computer from which the subsequent records were recorded.

Printing Output

You can use **File|Print** or **File|Print Range** to print the contents of the display to a printer. Choose **Print Range** if you only want to print a subset of the sequence numbers displayed, or **Print** if you want to print all the output records. The Ctrl+P hot-key sequence corresponds to **File|Print**.

Using the **Print Range** dialog you can also specify whether or not sequence numbers and timestamps will be printed along with the output. Omitting these fields can save page space if they are not necessary. The settings you choose are used in all subsequent print operations.

In order to prevent wrap-around when output lines are wider than a page, consider using landscape mode instead of portrait when printing.

There are a number of options that let you adjust several characteristics of *Portmon*, including the way that it behaves and looks.

Timing Format

Portmon displays time stamps of captured output in one of two formats: as clock-time (the time of day), or as relative time. When displaying relative time *Portmon* represents the time of a output record as the difference between its timestamp and the timestamp of the first record in the display. This mode is helpful when you debug timing-related problems. Use the **Options|Clock** Time menu item, 🕒 toolbar button, or Ctrl+T hot-key sequence to toggle between clock time and relative time modes.

Show Time

The show time option lets you automatically hide or make visible the timing information *Portmon* displays for each logged event. You may want to hide timing information to make more efficient use of screen space if you are not interested in it.

Auto Scroll

Use the **Options|Auto Scroll** menu item, ⤓ toolbar button, or Ctrl+A hot-key sequence to toggle *Portmon* between auto-scroll and non-auto scroll modes. When in auto-scroll mode *Portmon* will always keep the most recent output visible in the display window.

Hiding the Toolbar

You can gain more display space by hiding the *Portmon* toolbar. Use the **Options|Hide Toolbar** menu item or Ctrl+B hot-key sequence to toggle the toolbar's presence. *Portmon* will remember the toolbar state when you exit it and restore the same state the next time you start it.

Changing the Font

Use the **Edit|Font** menu entry to open a font-selection dialog where you can choose a font that *Portmon* will use in its output window.

Always on Top

To keep *Portmon* as the top-most window on the desktop, use the **Options|Always On Top** menu item. Selecting the menu item a second time will toggle off the always-on-top mode.

Portmon has advanced remote monitoring capabilities that allow you to view port activity generated on remote systems from a central location. The remote systems must be accessible via TCP/IP. *Portmon* lets you monitor multiple remote systems simultaneously, using a hot-key or a menu selection to switch between them. If both the computer you are running the *Portmon* GUI on (the server) and the system you want to monitor (the client) are running Windows NT/2000, and they are in the same Network Neighborhood, then *Portmon* will automatically install its client software on the client. For all other combinations you must manually install and start *Portmon*'s client software on the client.

Manual Client Startup

If either the server or the client is running Windows 9x, or the server and client are not mutually accessible via the Windows Network Neighborhood, then you must manually start the *Portmon* client on the client computer. To do this, run the *Portmon* program on the client and specify "/c" as a command-line argument:

```
Portmon /c
```

The *Portmon* client window will appear and indicate that it is waiting for a connection from the *Portmon* server.

After you have started the *Portmon* client use the **Computer|Connect** menu item or Ctrl+R hot-key sequence of the *Portmon* server to open a computer connection dialog. In the dialog enter the name or IP address of the client computer. If the client computer is in the server's Network Neighborhood you can also use the browse button in the dialog to open a view of the Network Neighborhood and visually select the client computer.

If you want to run the client in a "headless" mode, specify "/s" (silent) in addition to the "/c" command-line argument when you start the *Portmon* client. This will cause the *Portmon* client to not display a window, and to remain active until the current user logs out, silently connecting with and disconnecting from *Portmon* servers.

Use the "/e" option when starting the client if you want it to notify you when server connections break. When a server connection is broken and this switch is specified you must close the notification window before the client will accept further connections.

If you specify "/?" *Portmon* will tell you its supported command-line options.

Automatic Client Startup

Automatic startup is not supported on the Alpha.

If both the client and server are running Windows NT/2000 and are in the same Network Neighborhood, there is no need for you to install the *Portmon* client on the client computer. Instead, specify the client computer name or address in the connection dialog as you would if you were connecting to a manually started *Portmon* client, and *Portmon* will automatically install and start the *Portmon* client on the client computer. When you disconnect from the client *Portmon* uninstalls its client software for you. In case you want to clean up client files after a non-graceful exit of the server, simply reconnect to the client computer and disconnect gracefully.

The *Portmon* server will always attempt an automatic install, and if that fails it falls back on trying to connect to a manually installed client.

When a remote capture session is established *Portmon* creates a new computer view for the session. The active computer view is the one that has captured output displayed in the *Portmon* GUI, and is identified on the *Portmon* title bar. To switch from one computer view to another select the desired view, which is listed by computer name, in the **Computer** menu. Alternatively, you can use Ctrl+Tab to cycle through the computer views.

The state of global capture and output window column sizings for newly established remote session are adopted from the current settings of the local view (the view of the computer on which the *Portmon* is executing). Changes you make to these settings only apply to the active computer view.

Disconnecting a Remote Session

When you are through capturing port activity on a remote system, make the view for the computer from which you want to disconnect the active view and then use the **Computer|Disconnect** menu entry to close the session.

When you exit *Portmon* it saves the state of the local view, including the width of the display columns, and *Portmon* applies those settings the next time you start it.

Portmon allows you to open multiple *Portmon* windows on the same computer, allowing you to capture output from different computers into different windows. This is an alternative to connecting to multiple computers from the same *Portmon* window, and is desirable when you wish to simultaneously view different output sources.

By default, when you start the first *Portmon* window on a computer it connects with the local computer. This means that it captures and displays any output generated on the computer. You can open a second instance of *Portmon* either by starting it again, or by selecting the **File|New Window** menu entry.

You can use the **Computer|Connect Local** menu entry to connect *Portmon* to the local computer, and choose the **Computer|Disconnect** menu entry to disconnect from the local computer when it is selected as the active computer view within a *Portmon* window. Note that only one *Portmon* instance can be connected to any computer at a given time.

If you start a new *Portmon* window by executing the program again the configuration settings *Portmon* uses reflect those of the last *Portmon* window that was closed. If you start a new *Portmon* window using the **File|New Window** menu entry, the configuration settings are adopted from the window in which you select the menu item.

If you encounter a problem while running *Portmon*, please visit the **Systems Internals** web site (http://www.sysinternals.com) to see if an update has been released that might correct the bug. If the problem has not been fixed, please submit a thorough report of the problem, including information on your system configuration and details on how to reproduce the problem, to:

mark@sysinternals.com