

- [Contents](#)
- [1 Introduction](#)
 - [1.1 What is NEPM?](#)
 - [1.2 What makes NEPM unique?](#)
 - [1.3 What can NEPM do for me?](#)
- [2 Quick Start](#)
 - [On Windows host systems:](#)
 - [On Unix/Linux/BSD host systems:](#)
- [3 Installation](#)
 - [3.1 Installation pre-requisites](#)
 - [3.1.1 Host systems](#)
 - [3.1.1.1 Operating System](#)
 - [3.1.1.2 Disk](#)
 - [3.1.1.3 Perl](#)
 - [3.1.2 Telnet](#)
 - [3.2 Builder and Courier installation.](#)
 - [3.3 Installing the Windows NT Event Log monitoring option \(WNTELC\)](#)
- [4 Configuration](#)
 - [4.1 General configuration guidelines and assumptions](#)
 - [4.2 Configuration Without Using the Unified Management Console](#)
 - [4.2.1 Configuring the Courier control file by text editor](#)
 - [4.2.2 Configuring the Courier control file general parameters \(required\)](#)
 - [4.2.2.1 Configuring the Courier control file target system lines \(required\)](#)
 - [4.2.2.2 Configuring the Courier control file file-capture sub-entries](#)
 - [4.2.2.3 Courier control file examples and discussion](#)
 - [4.2.3 Configuring the Builder control file](#)
 - [4.2.3.1 Configuring the Builder control file general parameters \(required\)](#)
 - [4.2.3.2 Configuring the Builder control file message match-text and performance monitoring section \(optional\)](#)
 - [4.2.4 Scheduling runs manually using cron and/or the Task Scheduler \(command line arguments\)](#)
 - [4.3 Configuring the optional WNTELC tool on Windows NT/2000/XP target systems - none required.](#)
 - [4.4 Configuring for security](#)
 - [4.5 Configuring data capture from isolated nets](#)
- [5 Operation](#)
 - [5.1 Memory requirements](#)
 - [5.2 Startup](#)
 - [5.3 Automatic operation](#)
 - [5.4 Manual operation](#)
 - [5.5 Remote operation](#)
- [6 Alerts and reports](#)
- [7 Upgrading](#)
- [8 Troubleshooting](#)
 - [8.1 Login Problems](#)
 - [8.2 Erroneous Reports](#)
 - [8.3 Data Capture Delays](#)
 - [8.4 Data Capture Errors](#)
- [Appendix A: Specifications](#)
- [Appendix B: Regular expression equivalents to common command line prompts](#)
- [Appendix C: Telnet Servers](#)
 - [If you are using a Microsoft Telnet Server...](#)
 - [If you are using a third party Telnet Server...](#)
 - [If you are using the Telnet Server for Windows supplied with NEPM...](#)
 - [Purchasing the unlimited-time Telnet Server for Windows...](#)
- [Appendix D: Acronyms and names](#)



Network Equipment Performance Monitor

Local Edition 2.4

User Guide

Revision 060302

www.nepm.net

Copyright © Nova Software, Inc. 2002-2006 All rights reserved. www.nova-sw.com

"Innovation + Implementation" and "Mincode" are service marks of Nova Software

Contents

Search for any phrase in this guide by using your browser's search tool under the ``Search:find...`` or ``Edit:find...`` menu item. The links in the table of contents will take you directly to a topic.

1 Introduction

1.1 What is NEPM?

NEPM monitors and reports uptime, critical events and their predecessors, access rates, byte transfer rates, and error rates for network node equipment. Hardware and software elements within the nodes are tracked and reported separately but in a common format that makes possible direct comparison. True hardware uptime is reported so that hardware and software performance can be separated from that of the communications link and from each other. Summary reports and alerts aggregate a view of an entire network's status onto a single page. Equipment behind firewalls can be reported on from elsewhere. Equipment monitored can be Windows or Linux/UNIX servers, or any processor based system that logs events to non-volatile storage and has a telnet/rlogin/ssh/IP stream-mode interface. Reports are provided via web pages posted to a web server for instant availability. E-mailed text alerts provide instant notification of threshold settings which have been exceeded.

NEPM comprises two principal elements, the Courier and the Builder. These programs can be run on separate host systems or the same system. This split architecture permits monitoring equipment behind multiple remote firewalls from a central location. The Courier telnets to a list of network nodes in sequence, captures specified log files and mails them to the Builder. The Builder reads this mail, archives it, and analyzes the logs for uptime, specified critical events and performance, and reports the results via web pages. Alerts are mailed when performance or event rates cross specified thresholds. When the Builder and Courier run on the same host system files may also be transferred between them through the filesystem rather than by mail.

The Builder and Courier are run as often as required, under control of the cron utility on UNIX systems or the task scheduler on WinNT/2000. On a small-to-medium sized network the Courier would typically be run once daily during the night to capture and mail all the data, and the Builder run daily, slightly later, to generate daily reports. On a larger network, or if there is a need for results closer to real time, capture and report runs could be scheduled at eight or four hour intervals, hourly or even more often. Capture, courier, and analysis of the data on one system normally requires no more than a minute for typical log sizes and system and network speeds. Quasi-real-time update cycles can be instituted on selected monitored systems when needed, allowing their states to be monitored nearly continuously via the web reports.

Courier and Builder are configured, managed and controlled thru a web browser interface, the Unified Management Console. This interface provides complete local or remote control including configuration, execution, and automatic scheduling in a visual, easily followed format with informative, context-sensitive, help links for each item. For those who prefer Courier and Builder may also be configured directly thru their self-documenting text based control files using any text editor. The two methods of configuration may be used interchangeably for complete flexibility. Only the management console provides automatic scheduling, however. Default values are provided for most parameters. These make it possible to get started using NEPM with a minimum of configuration.

A third element, WNTSLC, is also part of NEPM. When installed on WinNT based computers it makes it possible to capture and analyze the event log on these systems.

1.2 What makes NEPM unique?

- Only NEPM gives you instant discovery of causes thru hyperlinked predecessor events.
- Only NEPM pinpoints failures instantly thru hyperlinked reports
- Only NEPM monitors behind remote firewalls as easily as locally
- Only NEPM will micromonitor performance when you need it.
- Only NEPM gives you full remote control of all functions thru a browser interface.

- Only NEPM monitors isolated sub-nets such as lab and test systems.

1.3 What can NEPM do for me?

Specific applications of NEPM include

- Network element and total network uptime tracking
- Intrusion and/or other critical event tracking
- Troubleshooting network problems to root cause
- Server performance tracking
- Testing and qualification of new network equipment
- Centralized archiving and access to all log files.
- Tracking and documenting SLA's, QOS, uptime guarentees, and other contractual agreements
- Separation of hardware and software contributions to downtime
- Providing a common system and report format for both UNIX and WinNT equipment
- Performance comparisons of products from different vendors
- Server log analysis
- Router, switch, or hub performance tracking

In general any requirement for detection, graphing, and notification of rare and/or recurring logged events can be handled by NEPM.

2 Quick Start

Follow these steps to benefit from your download at once:

On Windows host systems:

- Open a web browser session at the Favorite "NEPM Unified Management Console" or go to "http://nepm_host_pc_name:40000/openumc?upld=NTstartup.ccf".
- Click on the 'Configure log capture' link to open that page to begin.
- Fill in the five required double-starred (**) items of configuration for log capture.
- Save it (click "Save All") with a filename whose extension is .ccf in the "Save as..." box.
- Click on the 'Configure reports' link.
- Enter the five required items (**) of configuration for report building.
- Save it with the **same** filename **except with the extension .bcf**.
- Click on the green 'Make/Update reports' button.
- Click on the 'View reports' link to see your new reports when report building finishes.
- Configure automatically scheduled log capture and report building and begin enjoying effortless network monitoring!
- REMEMBER TO:
 - Click on the help link next to any configuration entry for guidance on completing that item.
 - Consult the remainder of this User Guide for more in-depth information.

On Unix/Linux/BSD host systems:

- Start the NEPM daemon on your system if it is not already started. In the NEPM:LE home directory (by default \Nova-sw\NEPMLE) type at a command prompt: umc
- Open a web browser session at "http://nepm_host_system_name:40000/openumc?upld=unix_qs.ccf"
- Fill in the five required double-starred (**) items of configuration for log capture.
- Save it (click "Save All") with a filename whose extension is .ccf in the "Save as..." box.
- Click on the 'Configure reports' link.
- Enter the five required items (**) of configuration for report building.
- Save it with the **same** filename **except with the extension .bcf**.
- Click on the green 'Make/Update reports' button.
- Click on the 'View reports' link to see your new reports when report building finishes.

- Configure automatically scheduled log capture and report building and begin enjoying effortless network monitoring!
- REMEMBER TO:
 - Click on the help link next to any configuration entry for guidance on completing that item.
 - Consult the remainder of this User Guide for more in-depth information.

Install Courier on a remote host best situated for data capture from the target systems to be monitored. It can also be installed on the same host as Builder if you do not need the remote network capture feature. Setup your automatic log capture schedule with UMC. Install Builder on a host best situated for running and displaying the reports and setup its automatically scheduled report building with UMC. Your reports will be updated automatically on the schedule you have created and may be viewed at any time locally or remotely without further effort.

Configuration for both WinNT and Unix target systems can be combined into one Courier and one Builder control file if desired. It may be more convenient, however, to use separate Courier control files for each type of target system to make best use of NEPM's defaulting system for quick configuration. If you need NEPM's targsys components for monitoring your Windows Server target systems, especially the Windows Event log monitoring tool, install them by running the executable ``NEPMLETS.exe" on each target system.

3 Installation

3.1 Installation pre-requisites

3.1.1 Host systems

3.1.1.1 Operating System

NEPM runs under WinNT 4.0, Windows 2000/2003, Windows XP, and most versions of Unix, Linux and BSD .

3.1.1.2 Disk

Approximately 3 Mbytes of disk space is required for a full installation of NEPM. If you are installing NEPM only from the zip file approximately 500 Kbytes is required.

Data storage requirements for Builder are very dependent on the number of elements monitored, number and time period of reports, etc. A small system can be created that will use no more than 2 Mbytes for data. Full-fledged systems will, of course, be much larger than this. The greatest portion of the data storage is normally for archiving of couriered log files and mail messages and is user controllable via the Builder control file. This portion of Builder data storage can be set as low as zero if you wish. Disk space in the web server directory for display of the reports is also dependent on the same factors, with 10 Mbytes being a base number for a small system.

Courier does not use any local data storage space on its host system.

3.1.1.3 Perl

Perl and its required components install with NEPM if you have downloaded the full version. If you have a pre-installed version of perl that you prefer to use and have downloaded the NEPM zip file without perl please note the following:

Builder and Courier run on Perl 5.6.1 or later. Check your perl version by typing at a command prompt:

```
perl -v
```

Upgrade your perl version if required, or install the one which comes with NEPM. Multiple perl installations can safely coexist on one host system.

Verify that Compress::Zlib version 1.08 or higher is part of your perl installation by typing at the command prompt:

```
perl -e "use Compress::Zlib 1.08; print 'OK';"
```

If you receive a message of 'OK' this module has already been installed as part of your distribution. If you receive a message including the phrase *Can't locate Compress/Zlib...*, or an indication that your revision level is too low then Compress::Zlib version 1.08 or higher must be added to your installation.

3.1.2 Telnet

A stream-mode telnet server (daemon) must be running on all monitored systems. NEPM's Courier adapts automatically to telnet servers which require both a user ID and password to login, a user ID only without a password, a password only without a user ID, or neither.

Satisfactory stream-mode telnet servers are almost always already installed and on running UNIX and UNIX-like systems and on most high-end routers, switches and hubs. Consult your system documentation if installation and/or configuration of a telnet server is required. UNIX telnet servers may also be obtained from www.sourceforge.org or www.gnu.org.

Windows 2000/2003/XP now comes with a native telnet server which can be configured for stream mode. It is version 5.1 or later. Open your "services" window in the Control Panel to enable and run this server. Refer to your Windows documentation or search <http://msdn.microsoft.com> for "tntsvr" for details on installing and configuring this server. Windows NT 4.0 and older Windows 2000 systems may have telnet servers without a stream mode (console/window mode only). If so purchase the Nova Software server or upgrade to a more recent version of the Microsoft native server with stream capability. Download the free "Services for UNIX" version 3.5 or later from microsoft.com and install the MS native telnet server components therein to obtain stream capability on any WinNT class Windows system. Refer to the Appendix or go to <http://www.nepm.net/telnet.html> for detailed instructions.

Nova Software offers an economical telnet server with volume pricing for Windows systems that is configured specifically to work with NEPM's Courier. This server will also correctly relay a telnet session when used in conjunction with its related telnet client. For security it is limited to two simultaneous connections and limits those accounts which may login via telnet. It self-configures during installation, speeding and simplifying setup of target WinNT systems for use with NEPM. This server installs on port 1023 to avoid conflicting with any existing telnet server, but can be changed to any port you wish after installation. Refer to the Appendix on Telnet Servers. An evaluation version of this server is included with all NEPM download files.

You may also obtain a general purpose stream-mode server from third parties such as Pragma Systems (www.pragmasys.com), Seattle Labs, or Georgia Softworks. Tests of third-party and shareware telnet servers other than these three have revealed operational deficiencies in their stream mode that prevent correct and/or reliable operation. We strongly recommend using only one of the above third-party servers on Windows target systems to obtain correct results with NEPM. Be sure to include an account configured in stream-mode for NEPM when configuring your server according to the manufacturer's installation directions.

See the Appendix on Telnet Servers in this User's Guide for further details or go to <http://www.nepm.net/telnet.html>

3.2 Builder and Courier installation.

On Windows NT-based systems simply double click on the self-installing executeable and follow the instructions on the screen. All NEPM components, perl, and supporting perl components are installed beneath the installation directory that you chose. You must be in an administrator account or have service installation privileges to run this installation successfully.

On Unix's untar the tarball in a directory of your choice to install all NEPM components, perl and supporting perl components beneath that directory: `tar -x -z -f NEPMMLL.tar.gz`. Set permissions as desired.

If you have chosen the zip file version without perl simply unzip it into the directory of your choice, using WinZip, PKZip or

equivalent on Windows, or unzip, PKZip or equivalent on UNIX. These tools may be obtained at www.winzip.com, www.pkware.com, and www.info-zip.org, respectively.

None of the NEPM distributions makes any changes in your PATH environment variable.

3.3 Installing the Windows NT Event Log monitoring option (WNTLTC)

To monitor the system and application logs on Windows NT/2000 a specialized Event Log-accessing application is required since Windows locks the Event Log against normal read access. For NEPM this tool is named WNTLTC and is included with the TargSys self-installing executable that is a part of all installation kits. Copy and run the TargSys installation executable on each WinNT system to be monitored. Follow the instructions that appear on your screen during installation. You must be in an administrator account or have service installation privileges to run this installation successfully.

If you plan to monitor only, for example, IIS or MExchange logs on WinNT systems WNTLTC is not required, although this choice would forgo any additional information that these applications write to the Event Log.

The TargSys components also include a specialized stream-mode telnet server for monitored systems which can be installed at the same time as WNTLTC.

These components will require 1.5 Mbytes of disk space on each target system for the completed installation. No other disk space is required (there is no data storage required by NEPM on target systems.)

Contact support@nova-sw.com if you would like an unattended-install version of the NEPM TargSys components to push out automatically to a large number of systems in your network.

4 Configuration

Open a browser session at the favorite "NEPMLE Unified Management Console" or at `http://<nepm_host_system_name>:40000/openumc` to access the Unified Management Console, where `<nepm_host_system_name>` is the network name of the NEPMLE host computer. Select the control filename you wish to create or edit and follow the guidance in the help file links to complete configuration.

For additional information review the Courier help file [here](#). and the Builder help file [here](#).

Once NEPM is configured, setup any target system (TargSys) components on WinNT systems to be monitored, as described above.

NEPM may also be configured manually as described below under the manual configuration section. It is also possible to edit a control file manually some of the time and thru the management console the rest of the time. Comments in control files are not preserved by the management console, however, although all data entries are.

4.1 General configuration guidelines and assumptions

Use multiple control files to simplify configuration or allocate network management responsibility. For example, one individual can create a pair of control files for monitoring the Unix portion of an organization's network. Another individual does the same for monitoring the WinNT portion of the network. These control files are scheduled to run at different times. Similarly, multiple Courier control files can be created to make maximum use of its default capability. For example a group of Solaris-based systems with common configuration is polled with one file, a Linux group with another, a WinNT with a third, etc. In this case each file only needs to enter the standard configuration once in the control file's default values, rather than on each line for each item of equipment, saving time, simplifying any changes later, and reducing the chance for error. The automatic schedule can then be setup to invoke the Courier multiple times in sequence, once with each file, thereby doing the same job as a single full size control file and crontab or scheduler entry.

Monitored systems are tracked and reported by domain, OS type, and hostname which prevents any ambiguity in reports.

The first date in a log file to be analyzed must be the earliest and the last the latest. All other entries in the file are assumed to lie between these two, ideally in strict chronological order for shortest running time.

We recommend configuring monitored systems to record the maximum amount possible in the logs. Use NEPM to provide centralized log management and archiving and keep log space used on target systems small while deriving maximum benefit from each target system's native reporting capabilities.

Performance monitoring will give the best results if all log information is configured to go into a single log. Use NEPM to separate access rates, bytes-transferred rates, and error rates while maintaining the time relationship and sequence of all the events.

Server and other logs recording a source ip address must record numeric addresses, not urls, to be useable with NEPM. Analysis of server logs recording browser url's is not supported in this version. Contact sales for a quote if you require this feature.

Mail client authentication for relaying mail via an SMTP mail server is not supported in the Local Edition. The Courier and Builder hosts must typically be members of the SMTP server's IP domain to be able to relay the couriered files. The server must also be configured for this option. Some SMTP servers can also be configured to allow relaying from specific source ip addresses outside of their domain.

4.2 Configuration Without Using the Unified Management Console

NEPM is most easily and quickly configured thru its Unified Management Console rather than by text editor. This web browser interface provides:

- Convenient and informative help links for each configuration entry.
- Selected default entries to get you started as quickly as possible.
- Automated scheduling, eliminating the need to setup 'at' or 'cron' jobs manually.
- Control of manual execution and review of results.

If you need finer control over your configuration, however, or simply prefer to, NEPM can be configured by text editor in three steps:

- Edit, add, and delete entries in the Courier and Builder control files. Some entries in each file are required so this step is always required. [Default entries for monitoring Apache on a Red Hat Linux 6 system are provided. You can change these (and most other defaults) to suit your needs.]
- Create a cron or Task Scheduler job for each,
- Set up NEPM-supplied target system (TargSys) components on Windows NT monitored systems if needed,

Control files may be edited with any text editor that will not insert extraneous formatting. A word wrap feature will make it easier to view and edit lines exceeding one screen width.

Separate alternate values for entries from the active one at the beginning of the line with a ; (no leading space.) This method makes it possible to easily switch between settings without having to refer to other documents to look up alternate values.

The Courier control file configures

- Which systems on the network are monitored,
- What elements on those systems are monitored,
- Which log files are captured to do this monitoring, and

A default set of elements and file locations for Apache on Red Hat Linux 6 and ISS on WinNT are provided. System location entries (IP addresses) for all monitored systems must be entered.

The Builder control file configures

- Which events are searched for and reported on,
- Threshold settings for triggering alerts,
- The maximum size of the data and log file archives,
- The maximum time period covered by reports (data tracking time limit or data age).
- Which performance measures are to be calculated and reported, and the time bins to be used for each.

Common event matching messages for Apache on Red Hat Linux 6 and ISS on WinNT are included.

Both control files include a short section of required entries such as mail servers' names, mail account names and passwords, and NEPM license keys.

The cron or Task Scheduler setup controls the timing of the Courier and Builder runs.

Multiple domains can be monitored by using multiple Courier control files, one for each domain, with a separate Courier run for each. The Builder will automatically segregate and report each domain's results separately without special configuration, additional control files or runs.

4.2.1 Configuring the Courier control file by text editor

The sample Courier control file is self-documented internally with both general instructions, and comments directly at the point of each entry that describe its purpose, its default value, range of acceptable values, and null value where applicable. The intent is to make it possible to understand and set up the control file quickly by simply reading through it, without needing to refer to any external documentation. Review that file first, and then the additional points, samples and discussion here for more detail as needed.

[Review a sample Courier control file here.](#)

4.2.2 Configuring the Courier control file general parameters (required)

Refer to the comment text in the control file itself first. The following notes supplement those comments.

The mail sending account on the primary and secondary mail servers must be the same (same username and password.)

A valid, unique ``from" email address must always be provided for each Courier. The domain in the Courier's mail address is used by the Builder to identify the domain of the incoming messages and keep them segregated by domain, whether files are sent by the filesystem or by email.

The choice of transferring files between Courier and Builder by email or by the files system is controlled entirely by the mail host server URL entry in this section of the Courier's control file: Enter 0 to transfer files via the file system, or a valid mail server URL to mail them. Builder always looks for email first. If any is found the transfer directory is never checked by Builder in that run. If there is no mail Builder checks its transfer directory, if one has been entered. This algorithm means that some care must be exercised when switching back and forth, or when using multiple Couriers with some mailing files and some transferring. Builder runs must be scheduled so as to insure that some occur when the mail is empty in order for the transfer directory to be read and processed.

The file transfer location may be on another machine on the network if the directory is mounted (Unix) or mapped (WinNT) onto the local filesystem. Use drive letter syntax on Windows -- UNC pathnames are not supported in this release. The same location relative to the machine on which Builder is running must be entered in the appropriate place in the Builder's control file as well, of course.

Any missing directories in the path you specify are created automatically for you, saving an extra step when you want to create a new directory, but also with the consequence that mis-typing a directory name creates a new one and puts the files

there rather than where you intended. Type carefully and be sure to verify your input before running the control file.

Be certain to provide a directory name for this file system transfer entry if you elect the log management option on one or more of your systems. This option deletes the log on the original host after reading it. Should mailing via both the primary and secondary mail servers fail the log is written to this location in the file system to save it, insuring that no logs are lost. (Each file is written with a unique filename so that there is no danger of overwriting if the Courier must store more than one in the file system.) Transfer the file manually (e.g. as an email attachment) to the transfer directory on the Builder system and run Builder manually to process it later. The summary printed by the Courier at the end of each run gives the number of files successfully mailed and saved to disk.

Command line prompt equivalents are required to set two default values, and in the target system lines. These prompts must be entered as perl regular expression equivalents of the prompts. See the Appendix for brief notes on creating regular expression equivalents for common prompts.

4.2.2.1 Configuring the Courier control file target system lines (required)

Refer to the comment text in the control file itself first. The following notes supplement those comments.

Prompts, usernames, or passwords of '0' in the control file will not be recognized by the Courier and cannot be used. '0' is used as placeholder and null value entry for those items.

If you have entered default settings in the control file, and wish to have no value on a particular target system line for that sub-entry simply enter '0' in that location on that line. This is particularly important if a default privileged password is entered. It will fill that sub-entry in any empty target system lines, forcing Courier to attempt to increase its privilege level before beginning file capture. Override this behavior with a zero in the privileged password location when a default is used. The same caution and override apply to the 'delete log files after capturing them' entries.

4.2.2.2 Configuring the Courier control file file-capture sub-entries

Refer to the comment text in the control file itself first. The following notes supplement those comments.

Filepathnames with spaces are accepted. DO NOT enclose such names in double quotes (``). The character '|' is used instead as the separator to protect spaces in filenames (only in the target system lines of the NEPM Courier control file.)

Each line in the target system section of the Courier control file represents one network node or one item of equipment. Each node may be monitored by one or more groups or types of files. For example, a web server may be monitored by its own access log as well as by the system log. Within each of these independent file groups the filenames must be ordered left to right oldest to newest. The groups may be entered in either order. Time ordering of related files is required by run time tracking for calculating downtime, which depends on files arriving in chronological order. Time gaps in the data received are assumed to represent unmonitored periods and cannot be made up by sending a missing file after intervening ones have been received and analyzed.

Use ::EventLog_System, ::EventLog_Application, ::EventLog_Security, or ::EventLog_DNS without any pathname to capture the respective WinNT eventlog. Use NO extra spaces on either side of this type of log name. This syntax tells the NEPM Courier to invoke WNTLTC on the remote system to capture the Event Log indirectly since it is locked against direct read access by the operating system.

Use ::DatedLogs in place of any log filenames to capture dated logs on WinNT whose file name changes daily, or hourly, etc., such as IIS logs ncyymmdd.log or inyyddd.log in which the six digit year, month, and day are part of the filename. Precede the ::DatedLogs part with the normal pathname in standard format. Use NO extra spaces on either side of this type of log name. This syntax tells the NEPM Courier to capture the latest two *.log files in this directory, rather than requiring you to enter their names directly in the control file.

4.2.2.3 Courier control file examples and discussion

Refer to the comment text in the control file itself first. The following notes amplify those comments.

Some (notably RedHat Linux) systems use automatic periodic rotation of logs and names such that the current log is always named, e.g. 'log', the immediately previous one is 'log.1', the one prior to that 'log.2' etc. up to some maximum. When this system is in use NEPM should be setup to capture both the immediately previous log (generally with the .1 suffix) and the current log file in order to capture all the events at the boundary between two logs. This condition can be relaxed (i.e. only the latest log captured, typically the one w/o the number suffix) if the Courier data capture run is scheduled to occur **immediately** prior to the time of log rotation, thereby insuring that all the events in that file get scanned just before it gets renamed by the log rotater.

If more than one file of a related group is to be captured and Couriered, they must be listed in the control file in chronological order. For example if 'messages.1' and 'messages' are both to be captured from a UNIX system with log rotation in operation, then 'messages.1', normally the earlier log, is captured and transmitted first, and 'messages' second. This requirement is also described in the comments in the sample Courier control file and elsewhere in this guide.

The maximum file size that can be captured is 20 MegaBytes. When files larger than this are encountered only the last 20 MB of the file are captured and a warning issued. This limit can be relaxed on systems with sufficient available memory (and vice versa.) Send a request to NEPM Support via the form provided on the NEPM web site support page to receive instructions and cautions for changing it.

For safety, when log management is enabled (i.e. deletion of log files on monitored systems, after capture), be certain to provide a Courier directory specification in the Courier control file, even if file mailing is selected. This will insure that logs are able to be saved on the local file system should both the primary and secondary mail servers be down.

4.2.3 Configuring the Builder control file

The sample Builder control file is self-documented internally with both general instructions, and comments directly at the point of each entry that describe its purpose and use, range of acceptable values, and null value where applicable. The intent is to make it possible to understand and set up the control file quickly by simply reading through it, without needing to refer to any external documentation. Review that file first, and then the additional points, samples and discussion here for more detail.

[Review a sample Builder control file here.](#)

4.2.3.1 Configuring the Builder control file general parameters (required)

Refer to the comment text in the control file itself first. The following notes amplify and supplement those comments.

Builder saves all the incoming files from Couriers in original, compressed form, and as expanded clear text files in the 'data/mail' and 'data/files' directories respectively underneath the NEPM root dir . The archive size limit setting controls the total disk space allocated to these archives. One tenth of the space is allocated to the clear text files, thereby preserving the most recent ones for easy review, and the remainder to the compressed files for long term archiving. Mail files can be re-expanded and reported by simply submitting them to Builder again on the command line as described elsewhere in this guide. If several control files are being used regularly they will all store files into the archive. Its size can be most conveniently controlled by setting the archive size limit value in one file that runs most often and leaving it set to 0 (no control) in all the others. This method provides one point of control.

Each performance threshold value applies to all eligible elements. Performance threshold settings represent rates per hour.

4.2.3.2 Configuring the Builder control file message match-text and performance monitoring section (optional)

Refer to the comment text in the control file itself first. The following notes amplify those comments.

Use care when entering message texts in the event messages section of the Builder's control file. Extra spaces, including

those at the end can cause a message not to be matched in a log. The safest method is to copy the desired message text at its source and paste it directly into the control file, being certain to exclude all extraneous characters such as dates, times and spaces.

Use the shortest invariant text possible to distinguish message events to be trapped for best performance. Do not include variable text such as date, time, IP addresses, urls, etc. in message entries in the Builder's control file. All original message text following the matched text is displayed in the Event report detail, so if the match text is taken from the first part of the text all of the message text will be reported.

Three performance reports are currently provided by NEPM: (1) Accesses per specified unit of time, (2) KBytes or MBytes transferred per specified unit of time, and (3) Errors per specified per unit of time. These measures are invoked by including the phrase (1) Accesses, or (2)KBytesTransferred or MBytesTransferred, or (3) Errors, respectively, somewhere in the performance item name (case insensitive.) The default unit of time for each report type if none is specified is one hour. Only one report of each type may currently be run on an element such as a web server, i.e. three in total. Each report type has its unit of time specified independently so that, e.g., Errors per day, KBytes transferred per hour and Accesses per four hours can all be tracked simultaneously on one element. You may run reports on as many elements at a time as you wish, e.g. on both an Apache and an IIS web server at the same time. These reports currently run only on logs in NCSA (common) or IIS native log format. Contact Nova Software to receive a quote on reporting performance on other log formats.

Performance measures are identified by a name (alphanumeric only), underscore ,and unit of time given as iDjHkMIS. This unit of time specification defines the size of the bin used in the reports performance graph, e.g. Accesses_2H30M or Accesses_2hours30minutes both calculate and display the number of accesses per 2-1/2 hours. Time indicators can be upper or lower case and can appear in any order. Any other information after the underscore is ignored. If no valid time information is found after the underscore, a zero time bin is specified. If there is no underscore preceding the unit of time specification the time bin is set to one hour. Performance time bins can therefore range from 1 second to 28 days 23 hours 59 minutes and 59 seconds. CAUTION: Specifying a very short time bin (minutes or seconds only) will lengthen run times noticeably, create very large data files, and reports that can take a very long time to load into a web browser. Such settings should only be used on a very short span of data to avoid such problems.

4.2.4 Scheduling runs manually using cron and/or the Task Scheduler (command line arguments)

On Unix systems use the cron facility. Type 'man cron' at the command prompt on your system for a description of this tool, and 'man crontab' for instructions on using it.

On WinNT systems open 'Services' in the control panel and verify that 'Task Scheduler' is present, started, and set for automatic startup. Type 'at /?' at the command line for instructions on setting up tasks in the task scheduler service. Note that the command line 'at' scheduler is a separate program from the the GUI 'Task Scheduler' on Windows. When running alone 'at' has a broader and deeper set of features than 'Task Scheduler'. When the 'Task Scheduler' service is running 'at' runs under it and is limited to compatible features.

Be aware that only certain accounts may be allowed to schedule jobs on a particular host. On Windows 'at' access may be restricted to those accounts with administrator privileges. On UNIX crontab use may be restricted to those in /etc/crontab.allow (if present) and not in crontab.deny (if present.)

On either type of OS if you have installed perl with NEPM invoke Courier or Builder from the NEPM/LE home directory with the command:

```
Builder <control filepathname>  
    or  
Courier <control filepathname>
```

On systems employing Unix-style log rotation, as discussed earlier in this guide, the most efficient scheduling algorithm is to run immediately (e.g. < 1 minute) prior to the rotation time. The goal is to collect each file just before its renaming by the rotater so that no events are missed. This can be very difficult to accomplish in practice due to varying clock offset between systems, random variations in the time it takes to collect prior files due to system and network loading, etc. The safer

approach is to always capture the current and immediately preceding files. NEPM collects and analyzes all the events across the boundary so none are missed. Later retransmissions of the same file are detected and ignored. This approach eliminates the complication of the coupling between cron runs on different systems and gives greater scheduling flexibility at some cost in additional network traffic and redundant processing. Use of the log management (delete-after-capture) option will reduce network loading and redundant processing in this latter case.

Some systems, such as IIS, can set a fixed log file size and start a new file, numbered consecutively when each one fills. With such systems a simple strategy is to enable log management and set the limiting log size to the 20 MB NEPM limit and then poll frequently enough to insure that the log never fills and starts another. Alternatively, use the ::Datedlogs syntax documented in the Courier control file if multiple date-time-based log files are created by IIS. The Courier run interval must be chosen to span less than the time of two log files.

Builder and Courier run intervals need not be the same. Lockstep scheduling will, of course, give the promptest access to fresh data reports.

Run the Builder often enough so that memory requirements are not too large. It processes all incoming mail messages in memory.

The Courier polling interval need not be uniform, i.e. equi-spaced. It might be desirable, for instance, to schedule the Courier to run more frequently during high traffic periods and less often at other times, providing a closer level of monitoring when it's likely to be most needed. If this approach is combined with the log management option network traffic will also be minimized and NEPM run times kept shorter.

4.3 Configuring the optional WNTSLC tool on Windows NT/2000/XP target systems -- none required.

The WNTSLC tool needs no configuration on target systems.

4.4 Configuring for security

The Courier control file, which contains telnet passwords, must be kept under tight control by a single individual for highest security. It is recommended that the Courier program be run only under the user ID of this individual and that access to the control file by all others be denied, for greatest security.

We also strongly recommend the use of a single new account uniquely for NEPM access (such as NEPMRLC, as used by the NEPM telnet server for WinNT) on all target systems. Privileges on this account should be restricted to read and execute access only, and ideally only in the directories from which logs are read by NEPM, so as to minimize any potential for damage from a compromised password.

Assigning telnet for NEPM to a non-standard port number helps slightly to obscure it from simple port scanners on the open Internet. This is the default on the WinNT telnet server supplied with NEPM.

Running the Courier only against target systems inside the same firewall as itself will provide the best security.

The Builder control file contains the password to its own mail account and should likewise be kept tightly secured.

4.5 Configuring data capture from isolated nets

NEPM 2.2 and later can monitor systems on isolated networks, such as lab or other internal networks, which lack a direct external connection. At least one host on the network must have a second port accessible externally via telnet. This host acts as a monitoring gateway for the isolated net: All systems on the net are monitored via this gateway.

In the Courier control file enter a target system line for this gateway host with the address of its secondary telnet port and an OS type of *relay*. Follow this line with a normal target system data capture line for a system on the isolated net. Data capture

and analysis from the target system occurs normally. Enter such a pair of lines for each system being monitored on the isolated net. No special entries are required in the Builder control file -- data archiving and analysis is controlled in the same way as is all other data. Data capture and Couriering is transparent to the existence of the gateway host.

No data capture occurs from the relaying host when *OS Type* is set to *relay*. Enter a separate, normal data capture line, with true OS type, to capture data from this host.

Multi-hop relaying through two or more intermediate gateway hosts in series can be done.

When the gateway host is a WinNT based system the NEPM-supplied telnet server and client, or an equivalent, must be used to relay successfully. The Microsoft native telnet components do not relay correctly. When using the telnet components supplied with NEPM on WinNT enter ``pragma_relay" for the OS type. Only the WinNT gateway host must use the higher functioning telnet components: Other WinNT target system components on the isolated net that are not relaying will function satisfactorily with the native streaming-capable MS telnet server (i.e version 5.1 or later. See the Appendix on telnet servers.)

Sample relay entries are shown in the sample Courier control file included with your download.

5 Operation

During execution both Builder and Courier provide a running report of their own status. The current task running along with errors and warnings is displayed. Full diagnostic information in English is provided to make quick diagnosis of problems possible. There are no numeric error codes to be looked up in tables elsewhere. Errors display within the context of the currently running task to aid in rapid troubleshooting. A summary of each run and its error and warning count is displayed at the end.

Files are mailed or transferred between Courier and Builder in compressed, anonymous base64 encoded format. They cannot easily be read by someone who accidentally intercepts one, but are not secure against a determined attack.

The Builder deletes incoming mail from its POP3 server or filesystem directory as soon as it is successfully read and archived on disk its *data/mail* directory. In normal operation the Builder's mail incoming account will remain nearly empty. If the archiving fails for any reason the mail is left on the mail server so that it can be retrieved and deleted manually.

5.1 Memory requirements

Builder and Courier require adequate free memory when they are running based on the size of the logs to be processed. Allow 100 Mbytes (including perl and NEPM program memory need) if you expect to be routinely processing many logs at a time up to the normal 20 Mbyte limit, and correspondingly less for fewer and smaller logs. This should be physical memory, not virtual memory which would slow execution excessively.

5.2 Startup

A complete set of existing log files going back days, weeks or months can be collected at startup simply by listing them in order in the Courier control file, e.g.

```
<<System>>|/var/log/messages.4|/var/log/messages.3|/var/log/messages.2|/var/log/messages.1|/var/log/messages|
```

and running this control file once manually. This one run will produce reports of all the existing history up to the present. While it would be possible to continue running this way indefinitely, it is very inefficient to do so. Change the file lists to capture only the last two files after this during automated polling for best results. The data age value in the Builder control file must be set longer than the period covered by the full file set for this method to work.

5.3 Automatic operation

Two Builder control file options aid automatic operation:

(1) The delete-file-after-capture option, also referred to as log management, allows all the logs on the remote systems to be

collected and archived automatically at a central location as part of the NEPM operation. This saves storage on the remote systems, makes system-to-system log comparison easier, and makes secure long term archiving possible. All files received by Builder are saved both in compressed mail format, and uncompressed log format, with identifying header information (time of collection, filename and path, hostname, etc.) These archives make it simple to quickly review recent logs in their entirety when needed, and maintain a more extensive archive due to the high compression of the raw logs. The Builder can re-analyze any of the archived mail logs with the original control file to reproduce the original reports or with a different control file to perform a new, different analysis.

(2) The archive size limit parameter defines the maximum total disk space consumed by the two types of archived files, clear-text logs and compressed mail, up to 4.2 gigabytes. Each run of Builder checks the total space occupied by these two archives and deletes the oldest files, if necessary, until the total falls below the limit. This makes it possible to run Builder indefinitely without consuming the entire disk of the host. The total space given is allocated 10% to the latest clear-text logs and 90% to the compressed mail files. This makes it possible to review recent logs directly while maintaining a long-term archive. Cleartext logs can be reconstructed at any time from the compressed mail files by running Builder on them again. Add the pathname of the compressed mail file to be re-run as the second command line parameter when running Builder from a command prompt. (This feature is not available in the Management Console.)

5.4 Manual operation

Builder and Courier can be run manually at any time, of course, in addition to automatically scheduled execution. Manual runs to re-analyze existing mail files in the archive are invoked following the instructions given at the beginning of the Builder program file.

5.5 Remote operation

The Unified Management Console (UMC) of NEPM contains a built-in web server to allow remote management of NEPM and viewing of reports. You can navigate instantly between management and report viewing at any time. UMC runs as a daemon or service on the host computer so that this feature is available at all times that the host is running. With Internet Explorer connect to the UMC web server with the favorite "NEPMLE Unified Management Console" that is automatically installed by NEPM in the Window favorites. On any system enter "http://<nepm_host_name>:40000/" in the browser's address bar to connect to the web server, where <nepm_host_name> is the network name of the computer hosting NEPM.

There are two cautions when operating NEPM remotely:

1. UMC is a single-user system -- only one user may access the system at a time.
2. File browse buttons in the UMC management screens browse the local file system, but NEPM only loads control files from its own host system, so the browse button is only useful when working locally on the NEPM UMC system. When working remotely enter the full path and file name of the control file that you wish to access *on the NEPM UMC host system* directly into the input box adjacent to the browse button.

6 Alerts and reports

The timelines of downtime and events in the detail reports present a qualitative display of the occurrences versus time. For quantitative measurements use the tabular data below the timelines, identifying the areas of interest from the timeline. If the source logging software supports a time resolution of the events to one second is provided by these tables.

Each downtime and single event detail line includes a link to a list of the nine events immediately preceding that event. Click on the link to bring up these ten events in a separate window. The last event in the group of ten displayed at the top of that window is the trigger event. This feature makes it possible to quickly and easily identify and then begin alerting on a common precursor to a downtime event or other critical event. By identifying such events and listing them in the Builder's event message matching list you can be notified of critical events before they occur.

Alerts with any threshold-crossing values to report are saved in a directory named *Alerts* beneath the Builder's home

directory so that the alert history can be reviewed at any later time. Alerts in this directory are not deleted by the Builder. They must be deleted manually. The "No alerts" status report is not saved, only those with something to report. The current alert can always be viewed on the "Alerts Summary for the network ..." web page.

You can set very low positive threshold values (e.g. 0.0001) to generate an alert email on every monitored element. With these settings you will receive a complete report by email of your entire network's performance level on every data capture cycle.

The report web pages have been optimized for display in NetScape 6 or later and Internet Explorer 5 or later. Earlier versions of these browsers or others such as Opera may provide satisfactory results but are not currently supported. If you need support for such a browser contact sales@nova-sw.com.

Web page reports use only relative links for navigation between them. They can be saved as a group on a file system, or mailed as a group and the links between them will continue to work *if the directory structure is preserved*. These page links will not carry any base URL reference, protecting the confidentiality of secure web section, or one that is kept deliberately unlinked.

If the start time of a new file is within one day of the previous files' endtime NEPM assumes that any gap is due to a lack of events, not a missing file or down system. Conversely, beyond 24 hours the opposite assumption is made and a gap in the event monitoring is recorded. If these gaps exceed 10% of the total monitoring time, they are reported as unmonitored time.

If you are receiving reports with faulty data due to an inconsistent set of control file settings (e.g. capturing files older than the tracking period limit) simply delete the relevant files in the 'data' directory underneath the home directory of the Builder and start again with a consistent set of settings. Files are identified by element. Sub-directory structure within the data directory mirrors that of the network, starting from the IP domain.

Detail reports are updated only on filenames that are captured and processed each run. If you delete a file group from the Courier list the last report of that type posted to the web server will remain.

Performance graphs are always plotted out to the end of the current decade, filling any extra points with zeros. The performance data table following the graph gives the time and value of the last full data bin collected and analyzed, and ends with that value.

Partially filled bins are neither graphed nor tabulated on performance reports. For example, if a performance time bin is specified as four hours, and the most recently received file ends at the three hour point within the last bin, this bin is not displayed nor printed. It displays once a full four hours of data for it has been received and analyzed.

The performance summary calculates and displays a network average performance value. This average will only be meaningful if all the monitored items are measuring the same performance parameter with the same time binning. Ignore it otherwise. Users with a purchased license may edit their performance summary template to remove it if it causes confusion.

The Downtime Summary report displays the average downtime per monitored element and the total downtime on the network. Total network downtime is calculated by dividing the total hours down (i.e. summed over all monitored elements) by the total hours of monitoring (again summed over all monitored elements.)

The downtime and event timelines begin with the first time in the first file of a group that is Couried to the Builder after the report data files have been cleared. Exactly seven days (168 hours) of data are always displayed per line, but each line usually will not start on a day boundary (i.e. at midnight.) Typically a fractional day is displayed at the beginning and end of each line, with the total of these two segments summing to exactly 24 hours.

Downtime is calculated and displayed separately for each file type captured for each element. Thus, for example, a web server being monitored both by its own access log and the system log will list a separate downtime line in the summary for each filetype. Downtime calculated from different file types may not agree: Different downtime-tracking events may be logged to the two types of files by the element software. Display of both insures that you get a full set of information for

decision making.

7 Upgrading

Later minor version upgrades, releases, and patches can be used with your original Builder or Courier license keys. Simply unzip and copy the files to your working directories. It is good practice to rename or save elsewhere your working versions before copying in the new ones so that they can be restored should any problem develop with the new versions on your system.

An upgrade to a new major version of the Local Edition requires the purchase of a license upgrade and new license key. Generous credit is allowed for your original investment in the Local Edition. See www.nepm.net.

8 Troubleshooting

Builder and Courier report their step-by-step operation and all errors to STDOUT (the screen, when running manually.) Errors and warnings in English appear at their point of occurrence in this listing, making possible quick, effective troubleshooting with the context and details of the error apparent. There are no numeric error codes to be looked up in tables elsewhere. Redirect this output to a file (using '>') to capture it for later analysis and/or transmission to others. By checking this output, your control file entries, and the reports you should be able to troubleshoot almost any problem with a minimum of effort.

8.1 Login Problems

Courier reports its steps during connection and login. Examining these lines carefully and comparing them to the sequence and values expected by the target system telnet server will generally make it possible to solve login problems easily. If Courier prints no "Connected" message check its control file for the correct IP address for the target system. Check for a working TCP/IP connection between the Courier host system and the target. If/when the target system telnet server prompts for a username Courier prints "Sending username..." when responding, and similarly for password. The username sent is printed. Verify that it matches that expected by the target system. If the target system prompt after login does not match that supplied to Courier it will timeout repeatedly with timeout messages. Check that your regular expression equivalent of the prompt in the control file matches that of the target system, which is most often the cause of these timeout messages.

For severe connect and/or login problems Courier can be made to log each exchange of the telnet protocol with the target machine telnet server. Send a request to NEPM Support via the form provided on the NEPM web site support page to receive instructions and cautions for doing this.

8.2 Erroneous Reports

If you are receiving reports with faulty data due to an inconsistent set of control file settings (e.g. capturing files older than the data age limit) simply delete all the files in the directory below '<NEPM_LE_home>/data/your_domain/...' which carries the target system name corresponding to the faulty reports. Then start again with a consistent set of settings. Switching certain data capture and analysis settings for an existing data history can require clearing the corresponding report history by deleting data files. Sending out-of-sequence files can also occasionally require such a restart. Always be sure to list, capture, and analyze files of the same basename (group) for a target system in chronological order to minimize the need for this step. Files are identified by target system and element. Sub-directory structure within the data directory mirrors that of the network, starting from the IP domain.

8.3 Data Capture Delays

Courier uses a very long telnet timeout during data capture due to wide variations in network speeds and system loading. When the active link goes down during data capture Courier can appear hung while it is waiting to timeout. As with the filesize limit the default can be changed if it becomes a serious problem. Send a request to NEPM Support via the form provided on the NEPM web site support page to receive instructions and cautions for changing it.

8.4 Data Capture Errors

The primary cause of data capture errors is a prompt which is being matched in the captured text. Change the ``Prompt after Login" regular expression in the Courier control file to match a larger portion of the prompt, and/or change the prompt for your NEPM login account on the target machine to a string that will not match any text in your logs being captured, and put this prompt in your control file.

Appendix A: Specifications

1. External requirements

Access to a POP3 and an SMTP mail server are required.

2. Limits

The maximum amount that can be captured from one log file is set to 20Mb. Contact support@nova-sw.com if you need to increase this limit.

Archive size limit is 4.2 GB (2³²).

Appendix B: Regular expression equivalents to common command line prompts

```
(#\s*)$ is equivalent to #  
(>\s*)$ is equivalent to >  
(\$\s*)$ is equivalent to $  
(!\s*)$ is equivalent to !  
(:\s*)$ is equivalent to :
```

On WinNT we recommend using the regular expression `[[:upper:]]:(.*>\s*)$` for the typical prompt ending with > possibly followed by one or more spaces.

General rules: `\s*` represents zero or more spaces, `()$` means the expression inside the parentheses occurs at the end of the string, and `\$` represents just a dollar sign (i.e escapes its special meaning as end of string.)

Appendix C: Telnet Servers

If you are using a Microsoft Telnet Server...

Use version 5.1 or later of *tlntsvr.exe* (generally found on Win2003, WinXP and later systems, in the *WinNT\system32* directory). [To read a file's version number right click on the file in Windows Explorer, select "Properties", then the "Version" tab .] **Configure it for stream mode.** Version 5.1 and later can be configured for stream-mode operation and will work successfully with NEPM. Earlier versions of the MS native Telnet Server operate only in console-mode, sending one window of data at a time. In this mode the same data is sent more than once, along with extraneous cursor control characters, making it unusable for data capture. Replace such a server by downloading and installing the telnet server in the "Services for UNIX, version 3.5" package from Microsoft.

This package can be downloaded without charge from Microsoft, or may be obtained on CD-ROM. Go to

www.microsoft.com/windows/sfu

or search for a download titled ``Services for UNIX'' at msdn.microsoft.com. Run the 200+ Mb executable to self-extract it. Run its msi installer, choosing 'custom installation' and unselect all items except 'Remote Connectivity'. (Unselect the 'windows remote shell' component under 'Remote Connectivity'.) Complete the installation.

The telnet server component from the ``Services for UNIX'' package can also be installed from the command line, and includes an unattended remote installation option. Follow the instructions provided in the file *install.htm* in the top level directory of ``Services...''.

In some cases the required file *tnadmin.exe* from the unzipped *telnet* sub-directory may not be installed into *%SystemRoot%\system32*. In this case simply move a copy of this file directly into the *...system32* directory. Then run *tnadmin* from the command line to configure the server. Set the port number, the telnet server mode to stream mode (2) and the authentication method to 'Password' (4).

This telnet server is labeled version 8.0 as of this writing, although functionally it is nearly identical to version 5.1

This telnet server, even in stream-mode, will not relay a telnet session. If you need to relay Courier data collection through a WinNT system use the compatible server and client supplied with NEPM or an equivalent third party set.

If you are using a third party Telnet Server...

On WinNT be certain that the server is capable of and configured for stream-mode operation. Most UNIX servers operate satisfactorily in stream-mode.

Set the port number for that server to agree with that specified in your Courier control files. We recommend using both username and password for login for full security, and following the restricted single account method detailed below, in this case as well.

If you are using the Telnet Server for Windows supplied with NEPM...

This server provides satisfactory stream-mode operation and telnet relay with NEPM, and is automatically configured for stream-mode in the installation process. It includes a 30-day license for evaluation use. Purchase an unlimited-time license from Nova Software for long-term use.

- 1. Run the self-extracting installation file provided:**
Install the files into the directory of your choice when presented with the dialog.
- 2. Install the Telnet Server:**
Follow the installation instructions that appear on your screen following the file extraction step. The Telnet Server will be installed and ready to run upon successful completion. The default telnet port number is set to 1023 to avoid conflicting with any previous telnet server installation. If you wish to change it edit the port number entry in the file *Set_telnet_server_port_number.reg* with any simple text editor (e.g. Notepad). Double click on the revised file to read it into the registry and change to the new port number. Port 23 is the standard ``well known'' telnet port number. Restart the inetd service after changing the port number.
- 3. Create the domain or workgroup account:**
Create an account with the name NEPMRLC on the domain server or on the local machine. NEPM installs the telnet server with a default userid of NEPMRLC. Creating one account on the domain server to be accessed by all the target machines in the domain will simplify and speed the setup. This account must have 'logon locally' rights. Enter the account password in your NEPM Courier (RLC) control file line that accesses this machine. When the NEPM Courier logs onto the telnet server to capture log files the password will be verified using the Windows NT native security mechanism.

Add another userid to the telnet server by editing the `Add_telnet_user (Pragma) .reg` script with Notepad or another simple editor and then executing it (double click.) Enter the windows domain name of this target system and the new userid where shown in the file (3 places for each.) Correct the location of your WinNT directory if it is not the default value shown at the two UserShell... entries containing it, and correct the location of the NEPM targsys components under HomeDir if it is not the default shown.

Note that the telnet server maintains a list of authorized telnet login accounts distinct from valid accounts on the domain or host system, so a new account must be entered in both places. Only the userid is listed with the telnet server. Windows NT's native security mechanism provides the authentication.

4. **Operation**

Operation is fully automatic, with no user action required on any of the target systems. A small internet daemon, `inetdsvr`, runs as a service on each system looking for requests on the specified telnet port. When a request occurs the full telnet server is loaded to handle the request. This approach keeps the larger telnet server code out of main memory until it is actually needed. The `inetd` service starts automatically when WinNT starts.

This telnet server is limited to two simultaneous connections. It is installed and configured to require both a user name and password for each login.

5. **Security**

We strongly recommend the use of a single new account uniquely for NEPM access, such as `NEPMRLC`, on all target systems. Privileges on this account should be restricted to read and execute access only, and ideally only in the directories from which logs are read by NEPM, so as to minimize any potential for damage from a compromised password. Using a strong password is also vital: Use a made-up (non-vocabulary) word that includes upper and lower case letters, numbers, and special characters, and is at least 8 characters in length, and preferably longer.

Keeping the telnet port set to a non-standard, confidential value will help keep out casual intruders and simple scanners looking for standard ports. It will not provide security against a determined attacker.

6. **Troubleshooting**

Purchasing the unlimited-time Telnet Server for Windows...

Purchase Nova Software's unlimited-time telnet server and license at

www.nepm.net

After making your purchase you will receive by email a permanent license key and files and instructions for upgrading your evaluation version to purchased status.

Appendix D: Acronyms and names

ARB: Archive and report builder, most often called the Builder here.

Builder: NEPM's archiving, analysis and reporting piece

Courier: NEPM's data collector piece

Element: A replaceable software or hardware + software sub-system that functions as an entity on a network and logs status information to a disk file. Examples are network ports, operating systems, web server software packages such as Apache or IIS, and mail exchanger software packages (MTA's) such as Sendmail or MExchange.

Host: A computer system, either client or server.

IP: Internet Protocol

LAN: Local area network, using a limited-distance high speed data transmission method such as Ethernet.

Log or logfile: A line-by-line file of status information recorded to track events (and mal-functions) of an element. Each line at a minimum contains a date-time stamp and a code or status text.

NEPM: Network Equipment Performance Monitor

Node: A point where two or more segments on a network terminate. On wide-area IP networks routers and switches create *active nodes*. Servers are nodes on LANS.

OS: Operating System

POP3: Post Office Protocol 3, for receiving e-mail

RLC: Remote log courier, most often called the Courier here.

SMTP: Simple Mail Transfer Protocol, for sending e-mail

TargSys: Target system to be monitored by NEPM, usually a server, router, switch or hub running on a Unix-based, WinNT-based, or IOS-based operating system.

Telnet: A protocol for connecting to, logging in, and issuing commands on a remote computer system over the Internet

WAN: Wide area network, using a long-distance data transmission method for each segment such as that provided by the telephone network.

WinNT: Used here as an abbreviation for any one of Windows NT 4.0 Windows 2000/2003, or Windows XP. NEPM works only with Windows operating systems based on WindowsNT technology.

WNTLCL: Windows NT Event Log Capture, a tool written and supplied by Nova Software to read WinNT Event Log information via the command line on an actively running system.

[Back to the top.](#)