

TPS[®]/NFM

NetWork File Manager

GENERAL INFORMATION



©TPS[®] Systems, Inc.
14100 San Pedro Avenue, Suite 600
San Antonio, TX 78232-4399
Phone: (210) 496-1984
Fax: (210) 490-6805
Email: sales@tps.com
http://www.tps.com

Overview

What is NFM?

Welcome to the power, flexibility, and versatility of the TPS®/Network File Manager (NFM). NFM provides advanced file transfer capability while maintaining a comfortable level of familiarity for long-time IBM® NetView Distribution Manager™ Users. TPS®/NetWork File Manager is a Client/Server system designed to distribute files and other resources throughout a corporation's internal network. This robust, but easily, manageable file transfer mechanism allows files to be managed through a central server with file distribution taking place from the server to the client or among clients (peer-to-peer).

TPS®/NetWork File Manager Server is responsible for the management of the transmission of data from a source location to a target location. The NetWork File Manager system allows a user to customize this process through the use of transmission plans. Transmission plans detail the types of transfer, the files to be transferred, the nodes involved, and various other control factors. While remaining extremely flexible, transmission plans allow repetitive tasks to be performed on a regular basis with little or no user intervention. A single server or multiple servers can be configured depending on the complexity and capacity of the network. Authorized personnel using a browser interface or a stand-alone windowing application on certain operating systems easily manipulate the configuration and management of the file transmissions within the network. The TPS®/NetWork File Manager system uses TCP/IP sockets to communicate with NFM client enabled nodes and additionally manages FTP file transfers with non-client nodes. Network bandwidth can be managed utilizing IP-multicasting and TPS®/NFM's network throttling feature.

TPS®/NetWork File Manager Client is a multi-threaded program that executes at the node level and extends the server functions throughout the network. The Client executes commands from the server(s) to distribute files within the network. Direct peer-to-peer transmission can then be managed from a single server or multiple servers. (Each server considers the other servers as Clients.) The peer-to-peer transmission can be made directly from one Client to another without the file passing through a repository on the Server, thus, reducing network traffic.

TPS®/NetWork File Manager Interface is a JAVA-based user interface operating from via a browser, directly, or stand-alone Windows application.

Highlights

- JAVA-based browser interface gives the ability to monitor and configure activity anywhere on the network based on security levels.
- Custom plan builder to control step-by-step file transfers and program execution.
- Sophisticated scheduler that provides automation of plan execution, including calendar-based repetition.
- Dynamic monitoring capabilities for viewing plans in progress.
- Detailed error reporting capabilities.
- Remote file browsing capabilities.
- Peer-to-peer file transfers
- Transfers on demand – Quick Functions.
- Transfer files with or without client software.
- Multiple Simultaneous Transfers
- FTPS and HTTPS Transfers.
- Extensive logging capabilities.
- Report activities by exporting data to third party databases.
- NetView-like transmission plans terminology.
- Encrypted Session Support.
- Local and Remote Command-line interface (Event Driven).
- File Synchronization.
- File Streaming/Trickle.
- Encryption and Compression.
- Checkpoint restart and transfer retries.
- Ability for wild card and/or environment variable substitution of file names.
- IP Multi-casting.
- Bandwidth Management and Performance Monitoring.
- User Authentication utilizing Radius, LDAP, and Active Directory.

Benefits

- Conserve your valuable host / mainframe resources.
- Extend mission-critical information delivery throughout your extended network enterprise.
- Schedule file transfers at times most cost effective and advantageous to your organization.
- Create potent B2B (business-to-business) exchanges with your suppliers, business partners and customers.
- Maintain ROI (return on investment) for existing legacy applications and systems while leveraging new technologies.
- Rich and easy-to-use management features ensure effective control of information throughout your network environment.
- Automate repetitive tasks and create powerful data collection and distribution routines.
- *Highly scalable, modular adaptability and support for a broad range of multiple open system platforms and SNA and TCP/IP protocols.*
- Reliable multi-level program security and audit trail capabilities provide you with a practical means for having secure data transmissions and comprehensive reporting.
- Robust data compression speeds delivery of crucial information to various business points, applications and users.
- Comprehensive end-to-end solution for rapid deployment of software and data across the extended enterprise including corporate and remote Mobile devices, POS devices, ATMs, Internet kiosks and newer information appliances such as smart phones, PDAs, etc.
- Provides an essential tool for automating the enterprise exchange of data in the business environment by:
 - Transferring outbound data to multiple sites in one multi-cast session
 - Launching select business application processes remotely when required
 - Optimizing bandwidth connections for faster data transmission and shorter connection times
 - Ensuring the integrity and conformity of targeted remote systems
- Near “real-time” collection of data through the use of file streaming/trickle enables organizations to accelerate their ability to enhance operational efficiencies to make faster, more informed decisions.
- Empower companies to improve customer satisfaction and leverage their data for competitive advantage.
- Provides a comprehensive and effective instrument to help support large-scale data movement between a variety of applications and systems for better information sharing.

Scalability

One of the critical features necessary for a growing business is network scalability. Whether you are looking for a simple file distribution package for a small network of stores, or a full network management solution for 50,000 stores, your network management software should be able to grow as your business grows. The TPS®/NFM network management suite was designed with this kind of growth and scalability in mind. Specific features designed for growth and scalability include:

1) Simple but sophisticated plan configuration:

The TPS®/NFM software plan configuration is designed to be a high-level, simple interface that hides most of the complex details of information distribution, remote execution, recovery, redundancy and auditing. Network plan steps and phases are configured to operate on groups of files and groups of source/destination nodes. These groups can also be nested into groups of groups. This architecture can be used for a simple one level hierarchical distribution environment or, in very sophisticated store and forward architectures, in an infinite variety of configurations that can grow as your business needs grow.

Another strong feature of TPS®/NFM is the ability to manage the network from any HTML browser with an intranet connection to the NFM server. This allows for scheduled operations that can be monitored from one or several remote locations at once. Configuration management operations, monitoring and maintenance can be achieved from a single network operations center, or distributed across several remote managers taking responsibility for different operations within the network.

2) Network distributed architecture:

The TPS®/NFM application software is designed to operate in a true network distributed environment, with functionality distributed across multiple servers and clients within the network. Many network management applications rely on centralized servers that advertise scalability, but only if the centralized server is migrated to a more powerful processor. The TPS®/NFM software can be configured for a traditional hierarchical network with a centralized data source or a decentralized network topology. This distributed architecture contains no single point of failure, or bottleneck to limit network growth. The NFM clients themselves, transferring files and information in a true peer-to-peer fashion accomplish the bulk of the processing and bandwidth overhead. The NFM servers act as network managers assigning workloads to the NFM clients, collecting audit information and statistics, and verifying information delivery. A single NFM server can easily coordinate the actions of hundreds of NFM client file repositories, moving data to and from thousands of NFM end clients. As your network grows, additional NFM servers can be added for load distribution and redundancy. Whether your requirement is to move data to and from a single centralized OS/390 mainframe in a traditional hierarchical network, or to move data through a heterogeneous network with advanced store and forward processing on intermediate network servers, the NFM network plans can be easily configured for simple or complex distribution requirements, with full customization and interfacing to customer software on each client.

3) Support for a wide range of software platforms:

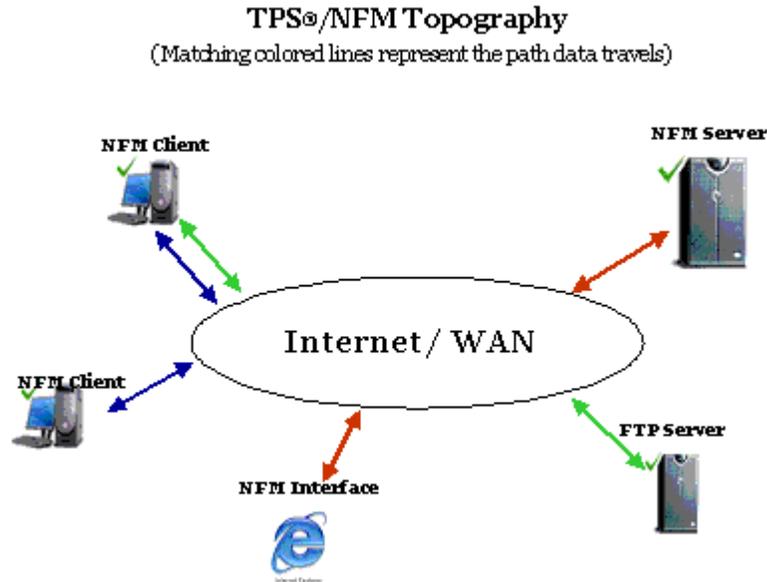
Your network management solution should be able to run on a wide variety of operating system platforms. A company that starts out with a single computer platform can easily be faced with the need to expand to other vendor platforms via company mergers, acquisitions and growth. Your network management software needs to keep up with these changes. TPS® Systems has over 35 years of experience working with UNIX vendors, Microsoft Windows, and IBM legacy platforms. Whether your business is based on IBM's OS/390 with IBM 4690 store controllers in the field, or a mixture of Microsoft® Windows®, Sun® Unix®, IBM® AIX®, SCO®, and Linux platforms, TPS® offers a wide and expanding list of system platform support for NFM clients and servers.

TPS®/NetWork File Manager

4) Support for a wide range of network environments:

Your network management solution should be able to run across multiple heterogeneous networks, taking advantage of newer technologies like IP multicasting as well as the potential to integrate into existing legacy distribution methods. TPS®/NFM is designed to run on TCP/IP, the protocol that integrates more heterogeneous networks as well as the Internet itself. In addition, TPS® Systems also has over 35 years experience working with legacy protocols like IBM SNA, BISYNC and X.25. The TPS®/NFM customization capability makes it possible to interface with existing file distribution mechanisms including TCP/IP FTP, HTTP(S), legacy IBM 2780/3780 file transfer for SNA or BISYNC, or proprietary custom distribution methods. Whether your company acquires the need to support an existing legacy environment, or your company wants to take advantage of the latest technologies including IP multicasting for network router or satellite distribution, TPS® Systems has a full range of communication and network experience to meet your changing requirements for growth and scalability.

Topography



System components

NFM consists of four primary components that are available for a combination of multiple operating systems. These include the following:

- NFM server
- NFM client
- NFM non-client node
- NFM user interface

NFM server

The NFM server is the main 'engine' of the NFM system. It contains all configurations for the NFM system in database form at one central location. The NFM server runs as a series of unattended programs that respond to dialog from the NFM user interface as well as handles all scheduled and 'on demand' operations involving NFM remote stations (or nodes).

NFM client

The NFM client refers to any node that is running the NFM client software. The client is responsible for performing requests from the NFM server to send and receive files as well as local program execution. Like the server, the client runs unattended with no local user interface. The NFM client is also responsible for supporting the remote file browsing capability inherent to the system.

The client is capable of performing file transfers directly between itself and another NFM client node. A peer-to-peer transfer of this type is still controlled by the NFM server but the data is sent directly between the clients. This reduces bandwidth requirements at the server while still maintaining centralized control.

Because of the peer-to-peer nature of the NFM system, the NFM server computer must also be defined as an NFM client if it is to be accessed as a node during plan activity. Any use of the server as a file 'repository' is simply done by design in the implementation of user written plans.

NFM non-client node

The NFM non-client refers to any node that is defined to the NFM server but is not running the NFM client software. These nodes rely on a different mechanism to facilitate file transfer and program execution (but not necessarily both). An example would be an FTP or HTTP(S) site, which could be an Internet site, where the NFM client could not be installed. The available NFM functionality to such nodes will vary based on their type. For example, the NFM file browsing capability also works with an FTP type node but not an NVDM node. An NVDM node has the capability of executing a program but an FTP node does not.

Additionally, during a file transfer between a source and target node, at least one of the two nodes must be an NFM client node. In order to transfer between two non-clients sites, it would be necessary to pull files from the source site to an NFM client and then separately push the files to the target site.

NFM user interface

This is the JAVA-based user interface for the NFM system. This program communicates directly to the NFM server to perform and monitor NFM system activities. Any number of users can be logged on simultaneously to the NFM system. The user interface stores no control or configuration information on the local computer. It acts only as a graphics terminal into the NFM system. There are two different methods of the browser interface. Both methods can be used interchangeably within the system. The methods for configuring an NFM user interface:

Browser interface This option requires the JAVA classes to be packaged on a web server. This allows access to the NFM user interface from any standard web browser that can access the web server on the network. The primary disadvantage to this method is an initial delay involved in downloading the JAVA applets the first time for any given computer accessing the system, after which time the JAVA applets should remain cached in local storage. The web server must be installed on the system running the FM Server.

Stand-alone interface This option requires running JAVA Jar file directly or installing a Windows stand-alone program on the computer that will access the user interface. This has the advantage that it will load faster, but it also means that it has to be installed on the computer before accessing the NFM User Interface. If there is more than one NFM Server, this method allows the user to connect to any one of them.

The initial screen looks different between these two methods, but once logged onto the browser a new window is opened and the two methods are virtually identical.

Communications between Components

With the exception of the NFM non-client nodes, all components of the NFM system communicate with one another via TCP/IP sockets. The server, client, and user interface may all be running on different computers, or all on the same computer. If the NFM server is communicating with an NFM client running on the same computer, it is not even aware of it (it is simply on a loopback socket). Likewise, if the user interface is running on a computer that is also enabled as an NFM client node, they are not aware of one another. This provides great flexibility in the implementation and load balancing requirements of the system.

Requirements

Software

The following section shows the supported platforms for each of the NFM components along with version requirements and optional software information.

NFM Server

The NFM server is currently supported on the following operating systems:

- IBM® AIX® *for* IBM® pSeries (32-bit/64-bit)
- Linux® *for* IBM® pSeries (64-bit), Intel®/AMD® (32-bit/64-bit)
- Windows® 2003/2008/XP/Vista/Windows 7 and 8 *for* Intel®/AMD®

Other requirements:

- If the user interface will operate using a web server, this must be done on the NFM server computer and will require the installation of an optional http package.
- TPS®/SNA Primary must be installed for use with NVDM type nodes.

NFM Client

The NFM client is currently supported on the following operating systems:

- IBM® AIX® *for* IBM® pSeries (32-bit/64-bit)
- Linux® *for* IBM pSeries (64-bit), Intel®/AMD® (32-bit/64-bit),
- IBM® OS390 *for* IBM® zSeries
- IBM® 4690
- IBM® AS/400 iSeries
- SUN® Solaris *for* Sparc (32 / 64-bit)
- Windows® 2003/2008/XP/Vista/Windows 7 and 8 *for* Intel®/AMD®
- SCO® OpenServer 5
- JAVA OS
- Apple® OS X *for* MAC, iOS iPad and iPhone
- Android (any device) Version 2.2 through 4.4

NFM non-client

There are currently two types of NFM non-clients, the necessary hardware and software will vary based on the individual computer types but basically include:

- Any computer that can serve as a standard FTP(S)/HTTP(S) server. This can include Internet sites.
- Any computer that can serve as an NVDM downstream node (or catcher).

NFM user interface

The NFM user interface operates from a browser, JAVA Jar file, or from a stand-alone Windows application. The following software is necessary on a system that has TCP/IP access to the NFM server computer:

- If running from a browser, any browser that supports JAVA version 1.4 or higher should work but a Windows system running Internet Explorer 4.01 or higher is recommended.
- The JAVA Jar file or a stand-alone Windows application can be installed on any Windows system Windows XP or greater.

Hardware

An adapter card may be required for the connection from the RISC System/6000 to the other nodes. The type of adapter is determined by your connection requirements and communication software requirements.

Configuration interface

The user interface has the general look and feel of a browser session. After initially logging on, a pull-down menu at the top of the screen gives you full access to the entire system. The pull-down menu is always present along with the current screen title and current time of day. Most of the configuration screens exist under the Management pull-down menu (nodes, models, etc.). Most configuration items have two screens, summary and detail. The summary screen provides a list of all items of that type. The detail screen allows viewing or configuring any one item.

Configuration database

All configurable items reside in the NFM database located on the NFM server computer. The process of configuration adds or updates these records through the NFM user interface. These components include the following:

- Users
- Models
- Nodes
- Node groups
- Filesets
- Plans

Opening screen The initial logging onto the system will vary slightly between using the browser versus the stand-alone user interface.

Stand-alone option After starting the stand-alone NFM user interface program an initial screen will prompt the user for the following information:

User name This is the name of an existing user record that identifies an individual to the NFM system. This name will identify certain attributes and permissions for this user during this session with NFM. See “Users” later in this chapter for more information.

Password The password assigned to this user.

NFM server This field represents the TCP/IP host name or address of the computer running the NFM server software.

Browser option The browser should go to a predefined URL that represents the NFM HTML page that exists on the NFM server machine. The LOGIN procedure is then identical to the above procedure for the stand-alone except that the user will not be required to enter an NFM Server field, but rather will access the NFM server residing on the web server computer.

Users

The NFM system maintains its own set of user configurations that control access to the various NFM activities. A user must sign on the NFM system with a password. Individual permissions are maintained that control the users abilities to read/modify different components of the NFM system. There is also the ability to independently restrict users from reading from, or writing to specific nodes.

Nodes

A node configuration defines a network entity that can be specified for NFM activity. It contains parameters that are unique to each node, like the communications name (IP address, phone #, etc.). The parameters that define a node are stored in two places. While the node configuration contains node specific information, the Model configuration contains parameters that are likely to be duplicated among several nodes. The node configuration combined with its designated model provides the NFM system with all the necessary information for communicating with the node.

There is also a mechanism by which user specified information can be stored on a per node basis (environment variables).

Models

The model configuration defines node parameters that are likely to be duplicated on several nodes. A model specifies the operating system, file transfer method and whether or not the node is running the NFM client software. If any of this information differs between nodes, it will be necessary to create an additional model for each combination of these parameters as needed.

Environment variables can also be defined on a per model basis.

Node groups

Node group configuration is a simple list of nodes used to enable actions to be taken on a group of nodes simultaneously. Node groups are also used to specify read and write access for given users. A group may contain any combination of nodes and may contain other groups. Nodes may belong to any number of groups.

Node group activity

Working with node groups within a plan involves some special consideration. The following section describes the characteristics of each type of function with regards to node groups.

File transfers

The Unique files flag that can be checked in a fileset definition controls the behavior of transferring to and from node groups. There are four different scenarios:

Copying from a node to a node (unique on/off)

Unique flag has no effect - files are simply copied. File names are unchanged unless the rename field is specified.

Copying from a node to a node group (unique off)

Each node in the group will receive an identical copy of each file. File names are unchanged unless the rename field is specified.

Copying from a node to a node group (unique on)

The source node contains a separate (and unique) copy of each file destined for each node in the group.

Copying from a node group to a node (unique on)

The unique flag must be specified to allow for copying from a group to a node.

File deletion

Only the target node/group is taken into consideration while deleting files. If the target is a node group, the files will be deleted on each node in the group.

Program execution

The target node/group specifies on which node(s) the program will execute. The source node/group may be used to specify multiple instances of a program's execution in the following way. If the source specifies a node group and the target specifies a node, separate instances of a program will be started (on the target node) for each node in the group. In this case, the reserved environment variable *NFM_NODE* may be specified in the program string. For each instance of execution, the actual node name will be substituted allowing the program to uniquely perform the activity related to its specific instance.

Running another plan

The function allows plans to run other plans as if they were functions. The source and target node/group fields are used to enter default nodes just as if they were entered in the plan scheduler. The plan would be run immediately in the ready state. The return code from the plan would become the return code of this function.

Filesets

A fileset configuration in its simplest form is a list of files. A fileset must be defined for any files that are to be manipulated by the NFM system. These files can be data files or directory entries. A source and target name may be specified in the event the files that are being copied need to be renamed or need to be copied into a different directory on the target node. This list can be created by manually typing in the entries or by using the browse facility that allows you to copy the names of the files directly from a directory display of files on any NFM client node.

A fileset may also include wildcard designators to more conveniently specify a larger list of files or files whose names may change on a regular basis. The name may also include an environment variable to specify different file names based on the node or nodes associated with the files.

Plans

With a general understanding of the base components of NFM, we can now look at plans where everything comes together. A plan contains the instructions for performing various activities amongst various nodes defined to the NFM system. Users can create plans to control any combination of the following functions:

- Copying files or directories between nodes.
- Deleting files or directories on nodes.
- Executing system programs or user applications on nodes (executables can be scripts, bat files, etc.).

Functions in a plan are grouped together into phases. Any number of phases may be created, each containing any number of functions. Functions within a phase are always run sequentially, phases however, may be specified to run sequentially or simultaneously or some combination of the two. Various control mechanisms allow for phases to be conditionally run based on the success or failure of other phases. Other controlling parameters effect how and if error recovery is performed when errors occur.

Plan execution flow

Overview

Execution flow within a plan can be controlled by several options. This can most easily be described by first understanding the default behavior of phases, functions, and node group considerations.

Default execution flow

Phases within a plan run sequentially by default. Each one must finish before the next one begins. Functions within a phase always run sequentially. For two functions to run at the same time they must be in separate phases. In most instances, when a function deals with a node group, multiple tasks (one for each node) perform the function at the same time, except as noted in the above section. The function cannot complete until each task is finished. The exception to this is when the next function in the phase is also working with the same node group and no termination logic for the current function is in effect. In this case, the individual task may continue into the next function. This allows for speeding up a plan by not having to wait on a slow node.

Terminating phases

Functions may specify a termination threshold. If the return code from the function is greater than or equal to a specified value, no other functions within the phase will execute. This may be specified explicitly for each function or may be specified in the phase as the default for each function. If specified in the phase, it will override the default value specified in the phase.

Phase logic

Several alternatives for running phases simultaneously exist. Phases may specify a dependent phase that they run after or run with. In addition, whether or not the phase runs may be specified based on the return code from the previous phase. This behavior is examined in more detail with a description of each option and some examples.

Run phase after phase

A phase specifies that it will run after another if the return code allows for it. Consider the example:

Phase2 runs after Phase1 finishes with return code greater than 4.
Phase3 runs after Phase1 finishes with return code less than or equal to 4.

This allows for a simple if, then, else logic. Phase1 will run, and then either Phase2 or Phase3 will run depending on the return code.

Run phase with phase

Phases may run simultaneously by specifying more than one to run after another or to specify running with another phase. Phases may also specify running after multiple phases complete. This is best described by the example:

Phase2 runs after Phase1 finishes with return code less than 8.
Phase3 runs after Phase1 finishes with return code less than 8.

Effect:

Phase2 and Phase3 run simultaneously after Phase 1 finishes. They are completely independent from one another.

Errors/Helpdesk alerts

Most of the conditional logic is controlled through the use of a return code. Return codes in this context; indicate the severity level of an error that can occur. The higher the return code, the more severe the error with zero being considered successful (no error). A return code is associated with each function in a plan as well as each phase.

The return code of a phase is set to the highest (or most severe) return code of any function within that phase. Likewise, a return code is associated with an entire run of a

plan that is set to the highest phases return code within the plan. This ‘filtering up’ of the highest return codes allows for an operator to know with a glance whether or not errors have occurred.

Scheduling/Monitoring/Auditing

User Interface The user interface has the general look and feel of a browser session. After initially logging on, a pull-down menu at the top of the screen gives you full access to the entire system. The pull-down menu is always present along with the current screen title and current time of day. The scheduling screens exist under the Scheduling pull-down menu.

Components

Plan Scheduler The Plan Scheduler screen may be accessed from the Operations menu. This screen will allow you to schedule one or more ‘instances’ of a plan to actually run.

Plan Monitor This screen shows the current status of an individual plan instance. This screen always displays the instance ID; plan name and current status, along with the plan’s scheduled start time.

The Plan Monitor screen is not directly accessible from the pull down menu but is reached in one of two ways. Once a plan is submitted from the plan scheduler, the user may click on the monitor button to go directly to this screen and display that plan instance. Otherwise, any user may go to the Plan Activity screen, where all submitted plans are listed, and double click on an entry to bring it up on the Plan Monitor screen.

Plan Activity The Plan Activity screen may be accessed from the Scheduling drop down menu. This screen is essentially the summary screen for all plan instances. Various information about each instance is listed along with its current state and return code (if finished). Double clicking on an entry at any time, will transfer control to the Plan Monitor screen for the selected plan instance. Like the Plan Monitor screen, this screen automatically refreshes itself to display changing plan information.

Day schedule The Day Schedule screen may be accessed from the Scheduling drop down menu. This screen maintains custom calendars that tailor the exact days to run plans that are to be automatically repeated. Once created, the schedule is specified in the Day Schedule field on the plan scheduler to associate it with a given plan.

Hour schedule The Hour Schedule screen may be accessed from the Scheduling drop down menu. This screen maintains custom schedulers like the day schedule but for use on an hourly basis instead. Once created, the schedule is specified in the Hour Schedule field on the plan scheduler to associate it with a given plan.

Audit trail Audit messages may be created for certain NFM activities occurring on the network. The level of audit messages, which are created, is configurable on a per-plan basis through the Plan configuration interface. At the lowest audit level, an audit message is created when a Plan instance runs, completes, and when error conditions occur. The Audit trail screen is used to view and filter audit messages. Audit records may be searched for specific text, and filtered by dates, plan names, filesets, nodes, and instance IDs. Once an audit message has been read, the record is marked as such in the audit list, using state images.

Plan Scheduler

Once a plan is created, it can now be scheduled to actually run. The process of scheduling a plan involves first checking the plan for any configuration errors and then creating what is called an 'instance' of the plan which gets a unique ID assigned to it (this allows for multiple instances of the same plan). The plan is scheduled to run at a particular time and date.

A plan may be scheduled to automatically reoccur at predefined intervals. Through the use of a customized calendar and hour table, even more control over scheduling is possible. For example, a plan could be submitted to run once an hour between 9:00 a.m. and 5:00 p.m. but only Monday through Friday and not on Holidays.

Plan Monitoring

Once scheduled, a monitoring screen allows a user to watch the status of a particular plan instance. The user will see either a countdown, a plan in progress, or a plan's finished status along with any errors that occurred. There are also controls that can be accessed from the monitoring screens that allow an operator to hold, release, or exclude individual nodes from plan activity.

It should also be noted that the plan monitoring can be done by anyone logged in through the NFM user interface, not just by the operator who scheduled the plan.

Plan Activity

The Plan Activity screen is essentially the summary screen for all plan instances. Various information about each instance is listed along with its current state and return code. Double clicking on an entry at any time, will transfer control to the Plan Monitor screen for the selected plan instance. Like the Plan Monitor screen, this screen automatically refreshes (user defined number of seconds) itself to display changing plan information.

Auditing/Error logging

NFM provides detailed logging capabilities in the form of audit trail records. Audit records are generated during a plan's execution and may include errors or just be informational. These records include the plan name, instance ID, operation, status, time, and date. The amount of information recorded into audits during a plan's execution may be optionally set to different levels. This can range from recording only errors to a detailed list of exactly what files went where and when.

While primarily used to record plan activity, audit records also reflect maintenance activity and system access (who deleted these nodes?, when did this person log on?, etc.).

Live Graph / Historical Statistics

Graph

NFM provides a reporting mechanism that offers detailed statistics about its own bandwidth usage. This can be used to analyze network usage and aid in tuning the bandwidth control mechanisms. A performance graph is available through the GUI that can view real time statistics as they are occurring, or view historical data. Also the statistics information can be exported in a batch fashion to simple text files, where it would be available for outside applications.

Additional features

Local/Remote Command Line Interface

The NFM Command line interface is a low-level programmatic access to the NFM server. This feature allows users to automatically perform tasks from applications. The NFM command provides a command line interface for most tasks that can be performed through the GUI user interface. Users can execute NFM functions within applications to distribute files, update configurations, extract audit information and interface with third party schedulers.

Examples of subcommands:

browsedir	Get a directory list from an NFM client node.
callplan	Run a plan immediately, wait for it to complete before returning.
holdjobnode	Changes the state of a node with regard to the submitted plan specified.
getfileset	Returns the contents of a fileset.
getjobstatus	Retrieve the status of a submitted plan ID.

Streaming File Transfers

A streaming file transfer allows a file to be transferred as it is being written to by another application or command. Once a streaming file transfer starts, it will copy whatever portion of the file that exists to the target node, check the file every # seconds, and continue copying any new data appended to the file until such time as the transfer is terminated.

Encryption

A method of coding and decoding data to secure the information during transfers utilizing the Twofish algorithm

Compression

A method of coding data to decrease the amount of data transmitted during transfers.

IP Multicasting

IP Multicasting is a feature of the Internet Protocol Standards. This feature is implemented in TPS®/NFM so that when a fileset is transferred from a single source client to a large group of target clients, the IP `multicast` protocol can provide dramatically increased performance.

Bandwidth Management

NFM provides two primary mechanisms that enable the user to control the amount of data NFM attempts to transfer at any given moment. These consist of limiting the number of active nodes and data pacing or throttling.

Maximum Active Nodes	- By System and by groups
Pacing	- Block size and request/acknowledgment interval timing

Bandwidth Performance Monitoring

NFM provides a reporting mechanism that offers detailed statistics about its own bandwidth usage. This can be used to analyze network usage and aid in tuning the bandwidth mechanisms. The reporting is available by two methods. A performance graph is available through a graphical user interface that can view real time statistics, as they are occurring or view historical data. Also the statistics information can be exported in several formats so that other reporting applications can utilize the data.

4690 Client Support

The Client for 4690 will support NFM services on the IBM 4690 POS Controller operating system Version 2 Release 3 or higher. The TPS[®]/NFM client executes as a background subsystem on the 4690 controller and communicates when necessary with the Server using TCP/IP services.

Mainframe Client Support

The Client for OS/390 will support NFM services on the IBM OS/390 mainframes running OS/390 MVS V2R5 or higher. The client exists as a basic load module that can be started interactively or run unattended as a OS/390 background task. The NFM client runs as a POSIX compliant application and uses the native OS/390 TCP/IP subsystem to communicate with the TPS[®]/NFM server on a server host machine.

Quick functions

NFM quick functions enable users to perform simple operations on demand (non-scheduled). The following types of operations are available:

- Quick Transfer** User can perform a simple file transfer (one file) from a source node to a target node.
- Quick Execute** User can execute a non-interactive command on a target node (similar to the execute function within a plan).
- Quick Plan** User can run a pre-defined plan.

The quick functions, in addition to offering a simplified way for users to perform certain tasks, also allows for a class of users to be created that can benefit from the services of NFM while being completely restricted as to which resources they may access. Users can be restricted to any combination of the above types of functions as well as being restricted to certain nodes, and even certain directories of certain nodes, based on their user ID (this is fully explained under Configuration, later in this chapter).

Users performing the quick transfer and execute type functions, can enter the appropriate parameters for the operation, selecting nodes from pop-up lists and file descriptions from browse menus, or typing both in manually. Once these parameters are set, the entire operation may be saved under a user-selected name, to simplify performing the same operation in the future by being able to simply select the name from a menu.

Import/Export Database Files

A stand-alone program that allows the NFM database files to be exported *to* and imported *from* text files. This feature allows configuration files to be built automatically from applications. It also allows log files within the NFM system to be exported to applications for reformatting and reporting purposes.

Environment Variables

The NFM environment variables provide information to commands that are executed in plan functions. There are two types of environment variables available, user configured and NFM provided. The user's configured variables consist of those variables configured on the model

TPS®/NetWork File Manager

and node definitions that correspond to the target node. The NFM provided environment variables are automatically generated during a plans execution. Example of these variables:

NFMPLAN	Current plan name.
NFMPLNID	Current plan instance ID number.
NFMSSNODE	Current source node name.

Environment variables can be used in two different ways. Variables can be referenced in the execute string directly in the plan, in the form \$(VARIABLE). In this case, the substitution is done on the NFM server prior to the command being sent to the client node. All environment variables are also passed down to the NFM client and are available in local context as real operating system environment variables.

Multiple Servers / Shared Database Support

NFM will now support multiple NFM servers sharing a common database. This allows the customer all the obvious benefits of having several servers (including workload distribution, connectivity considerations, etc.) while providing a single virtual server image, allowing administrators to view and maintain configuration across servers from a single login session.

Enhanced FTP and FTPS client support

NFM clients now directly support the FTP client protocol (this support was only available batch calls to an existing FTP client program previously). This offers enhanced performance, better error handling, and in some cases eliminates the need to install third party software, especially for secure FTP support.

FTP and FTPS server support

NFM clients will now act as FTP and secure FTP servers. This support includes the ability to do user authentication with NFM usernames and passwords, and also audits transfers automatically to the NFM server. Existing FTP clients (outside of NFM) can be used with this support.

Radius Authentication

Support for Radius authentication has been added.

Enhanced NFM proxy support

The NFM proxy program may now be installed on a separate computer from the NFM server. This allows the NFM clients to be able to connect to the NFM server (for remote command line interface, FTP server support, and Watchfile support) without having to open up an incoming port on the NFM server.

Watchfiles

NFM may now be configured to watch for specific files to appear on a given set of nodes, and then automatically perform file transfers (or other plan activity) once this occurs. This functionality may be configured centrally on the NFM server or configured locally at the NFM nodes.

Function Retry

A plan function will now allow an automatic retry upon failure. This can be specified with a retry count and retry interval. This feature looks similar to the connection retry count and interval already available in the node or model definition, however these are only for connection failures. The new retry will take place on any function that has a return code of 4 or higher. The function retry will not occur for a connection failure, if the connection retry was active.

Change Only file transfers

NFM now allows enabling file transfers to detect the differences between the source and target files, and only send the changes across, potentially offering increased performance.

File Synchronization

NFM now allows a synchronization function within a plan. This allows a group of files, on any number of nodes, to be synchronized. Based on a set of rules, files are copied as needed between the nodes involved so that they each end up with the same files. Synchronized deletes are available as well. File comparisons may be done by size, time stamp, checksum, or any combination of these attributes.

AS/400 Support

An NFM client is now available for AS/400 computers.

Separate Append Function

An append operation may now be performed as its own function (versus a transfer with an append). This allows for some enhanced processing including:

- Concatenating files already at a location.
- Continuing a transfer and append even if some files are not present.
- Performing a retry on the previously mentioned operation to get missing files.

Recursive wildcard specification

NFM now allows a double asterisks wildcard expression that may be used to automatically scan a complete directory tree for a file match (recursive search).

User Password Rules

Configurable user password rules now available in NFM. These consist primarily of minimum complexity requirements imposed upon the creation of passwords by end users. It also includes the ability to disable and/or delete users, following password expiration, periods of inactivity or guessing attacks. (Refer to the manual, chapter 4, “CONFIGURATION / System Settings / AUTH tab / NFM” for a detailed description).

Node Password Rules

Node password rules (similar to user password rules described above). Minimum password requirements are available as well as the expiration of passwords. (Refer to the manual, chapter 4 “CONFIGURATION / System Settings / Node Passwords tab” for a detailed description).

Node Improved Configuration Auditing

Auditing of configuration changes is now much more comprehensive, including showing field level details of almost all changes and also including the old and new values for each field.

Data Import/Export Changes

Data export feature now offers the option to generate comma separated fields or CSV fields, as opposed to the traditional format of NAME=”VALUE”. A header field is also generated to show field tag names. (Refer to the manual, chapter 8 “Tools / NFM Command Line Interface / Subcommands / exportc” for a detailed description).

HTTP Enhancements:

File transfers with HTTP servers:

NFM will now support HTTP type file transfers and other file activity to computers running an HTTP server (like Apache or Internet Information Server). This may be done with computers that cannot otherwise run an NFM client or where a customer simply prefers to implement a pure HTTP solution. This is very similar to NFM’s support for FTP servers.

NFM native file transfers over HTTP protocols.

NFM will now support file transfers between NFM clients using the HTTP protocol. The native NFM messaging is, in this case, imbedded (or tunneled) over an existing HTTP connection. This is useful in an environment that allows for the NFM clients to be installed but requires that only the HTTP protocol and ports are used for communications.

NFM client provides HTTP server functionality

The NFM client is now capable of functioning as an HTTP server (in addition to its standard duties). This allows certain HTTP type operations to be performed without having to install an additional HTTP server. It also allows certain additional functionality such as performing NFM auditing when HTTP uploads or downloads are initiated by individuals using browsers for example (this is similar to the NFM client built in FTP server support).

NFM iPad/iPhone Client

The iOS Client App can be used to perform standard client operations via the NFM Server. Since iOS on the iPad employs a user-based interface without real service type programs, the Client must be activated by the user and remain the active application while it is in use. While on other OSs, the Client required no user interaction, on iOS, the user is an integral part of the system. The NFM Server can download and upload files available to other applications and files from other applications available to the NFM Client.

NFM Android Client

Remote Monitoring and Quick Transfer

Installed as a separate app, a Remote User Interface allows monitoring and configuration viewing on the NFM Server through a series of screens optimized for the Android. The app also allows file system browsing of remote NFM nodes and initiating file transfers to and from the Android device.

Summary

TPS®/NetWork File Manager is a cost-effective, powerful data distribution program to aid in the expansion of your e-commerce initiatives. As part of your overall Network Management, NFM provides a way to disseminate vital information throughout your globally connected enterprise with its support for multiple open system platforms and protocols. The necessity for collecting

and distributing information among various legacy applications and systems is becoming increasingly important. NFM can greatly assist you in this endeavor by decreasing associated costs for moving this data and by increasing your effectiveness in communicating not only internally, but also with your customers and partners.