mv.ENTERPRISE

Online User Reference Manual, Chapter 9

Release 4.0
August 1997

This edition of the mv.ENTERPRISE manual set is to be used with all mv.ENTERPRISE systems operating under release 4.0 or higher. This electronic document combines the four hard copy volumes into a single file to be viewed with Adobe's Acrobat Reader, 3.01 or later. Content is identical between online and hard copy editions of this manual set.

It is the policy of PICK Systems, Inc. to improve products as new technology, components, software and firmware become available. PICK Systems, therefore, reserves the right to change specifications without prior notice.

Part Numbers:	This online document combines the hard copy manuals with these part numbers: 84-00014A01 84-00014A02 84-00014A03 84-00014A04
Software Release:	4.0
Document Release:	AA

Note that PICK Systems appreciates receiving suggestions and comments on its publications. Comments may be sent to the publisher:

PICK Systems, Inc.
1691 Brwoning
Irvine, CA 9606
Tel (800) 367-7425
E-mail: documentation@picksys.com
ATTN: Manager, Technical Publications

This page intentionally left blank.

Chapter 9 Table of Contents

Summary of mv.ENTERPRISE/ODA Commands

Chapter 9: Open Data Architecture (ODA)

Introduction to Open Data Architecture

The Open Data Architecture (ODA) provides a standard mechanism for handling remote data sources as if they were local multivalue files. mv.ENTERPRISE/ODA is licensed as a separate product. Please contact PICK Systems Sales for additional information regarding this product.

The high-level interface is through *Remote Q-pointers* which indicate the host name and some identifier of the data in the remote environment.

Open Data Architecture uses the specified host information to access one of several low-level drivers which opens a direct channel into the remote environment. All standard mv.ENTERPRISE file system calls are translated into a limited number of internal commands which all low-level drivers understand and can translate into the appropriate operation in their respective environments. The drivers included in the mv.ENTERPRISE/ODA interface:

1. mv.ENTERPRISE remote file driver. Provides access to remote mv.ENTERPRISE files. The remote mv.ENTERPRISE machine may be a different mv.ENTERPRISE virtual on the same hardware, or an mv.ENTERPRISE virtual on a remote system accessible over a TCP/IP network.
2. UNIX file driver. Provides access to UNIX files. Special files (devices, pipes, etc.) can also be specified with some restrictions.
3. Spooler driver. Provides access to spooler jobs as if they were standard files.

This page intentionally left blank.

Section 1: mv.ENTERPRISE/ODA Installation

Installation Overview

An overview of the installation process is followed by detailed instructions. Before installing, have your mv.ENTERPRISE/ODA license key available. The installation process involves:

1. Installing the mv.ENTERPRISE/ODA configuration control record.
2. Restoring the ODA.ADMIN account.
3. Installing the ODA monitor.
4. Installing mv.ENTERPRISE/ODA from the Network Administrator.
5. Setting up the network.

Before you Install

1. Read through all sections of the mv.ENTERPRISE/ODA Installation section carefully before proceeding. If you have any questions or problems, call PICK Systems, Inc. at (800) 367-7425 for prompt attention.
2. Review the “Network Administration” topic for a detailed description of using the NETWORK-SETUP utility program, menu navigation, and detailed descriptions and definitions.
3. It is necessary to acquire the mv.ENTERPRISE/ODA configuration control record from PICK Systems Customer Support. This record is unique to your machine and contains the maximum number of mv.ENTERPRISE/ODA server processes you are licensed for and allowed to run at one time. Without the configuration control record, the installation cannot be completed.
4. Add the mv.ENTERPRISE/ODA configuration control record to the /usr/config/config.pick file. The mv.ENTERPRISE/ODA configuration control record *must* be the second line in this file, following the mv.ENTERPRISE configuration control record.

Installation Instructions

Using mv.ENTERPRISE/ODA requires the *pickoda* monitor and the ODA.ADMIN account. Both of these are located on the mv.ENTERPRISE/ODA release tape. Installation of mv.ENTERPRISE/ODA requires a SHUTDOWN of the mv.ENTERPRISE virtual machine.

1. Perform a SHUTDOWN of all processes from mv.ENTERPRISE by typing **SHUTDOWN**.
2. Load the mv.ENTERPRISE/ODA tape into the tape drive.
3. Change directories to the mv.ENTERPRISE directory. Load the UNIX tar section by entering the command:

   tape device_name

   where: ***tape device_name*** represents the tape drive from which mv.ENTERPRISE is being loaded.

   Use this command to install the program:

Program	Description
pickoda	mv.ENTERPRISE/ODA monitor program.

4. Save a copy of the current mv.ENTERPRISE monitor program (prodpick).
5. Replace the existing mv.ENTERPRISE monitor program with the mv.ENTERPRISE/ODA monitor program.
6. Restart mv.ENTERPRISE.
7. If upgrading, DELETE/RENAME the old ODA.ADMIN account before proceeding. If not upgrading, proceed to the next step.

8. Log on to the SYSPROG account and restore the ODA.ADMIN account. At TCL, type:

   T-ATT 0
   T-REW
   T-FWD
   ACCOUNT-RESTORE ODA.ADMIN

This completes the ODA.ADMIN installation procedure. Each execution of the *prodpick* monitor now has the capability to use mv.ENTERPRISE/ODA. Continue the mv.ENTERPRISE/ODA installation process by executing the remaining steps.

9. Log to the ODA.ADMIN account.

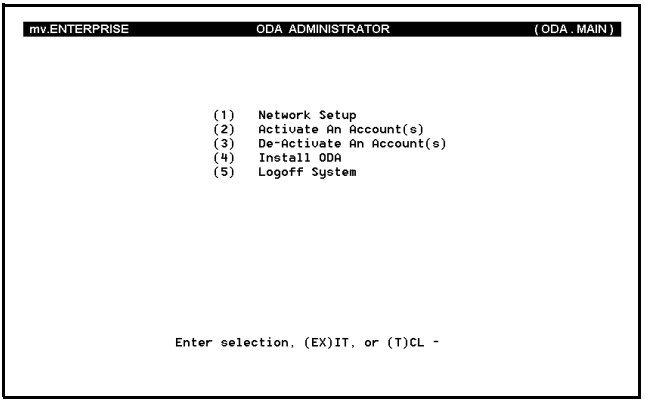

Figure 9-1: mv.ENTERPRISE/ODA Administrator menu.

10. Install mv.ENTERPRISE/ODA.

    From the ODA Administrator menu, select option 4, **Install ODA**. When installation is complete, the screen displays INSTALL PROCEDURE COMPLETE.

11. Setup the network.

    From the ODA Administrator menu, select option 1, **Network-Setup.**

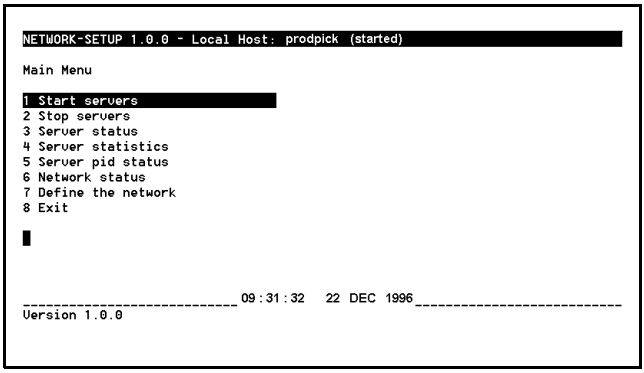

Figure 9-2: NETWORK-SETUP Main menu.

Refer to the “Network Administration” topic for a detailed explanation of each menu item.

12. To set up the network, it must first be defined.

- Select option 7, **Define the network**.
- Select option 3, **Define local host** to configure the local network hosts. If creating a server, define the local host. Selecting this option displays the Host Setup Data Entry Screen:

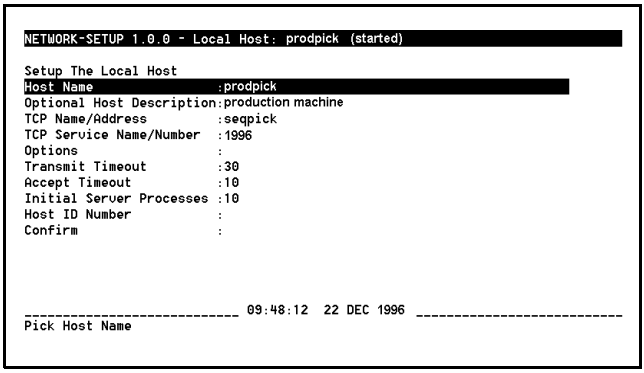

Figure 9-3: Host Setup Data Entry screen.

Refer to Figure 9-13 and the accompanying input field definitions to determine your optimum setup. Upon confirmation, the Network Definition Menu displays.

✓NOTE Clients do not require local hosts.

- Select option 4, **Define remote host** to setup the remote hosts configuration items. The local host setup and remote host setup contain the same information, except that the local host has the additional options number of servers and accept timeout values, which are not applicable when defining remote hosts. Upon confirmation, a listing of existing host items displays. (Refer to Figure 9-14.)
- Select option 1, **New host**. Refer to Figure 9-13 and the accompanying input field definitions to determine your optimum setup. Upon confirmation the Network Definition Menu displays.
- Select option 8, **Exit** to return to the ODA Administrator Menu.
- Select option 2, **Activate An Account(s)**. This option adds to the account the ability to execute remote commands using the REMX command and to define remote files using SET-RFILE.

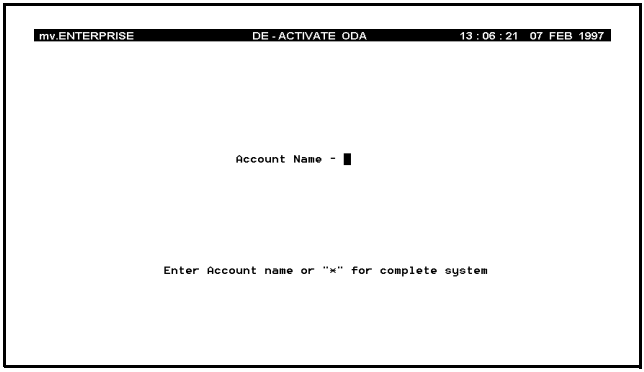

Figure 9-4: Activate ODA screen.

At the prompt, enter the Account name, or type ***** to activate the complete system.

13. From the NETWORK-SETUP menu, select option 1, **Start servers** then select option 3, **Server stats** to display all started servers.

✓NOTE This step is for mv.ENTERPRISE/ODA servers only with a local host defined. To have mv.ENTERPRISE/ODA reinitialized each time the system boots, place the following line in your USER-COLDSTART Proc:

```
NETWORK-SETUP start
```

The mv.ENTERPRISE/ODA installation is complete.

This page intentionally left blank.

Section 2: Network Administration

Network Administration

Prior to accessing files on a remote MultiValue machine, the remote machine must be configured and initialized as an mv.ENTERPRISE/ODA server. These functions are performed using ODA Administrator.

ODA Administrator

To access the ODA Administrator log to the ODA.ADMIN account by typing:

ODA.ADMIN

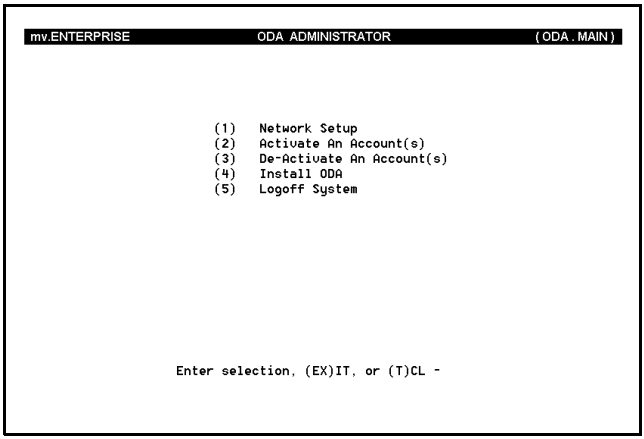

Figure 9-5: ODA Administrator.

- Option 1, Network Setup, configures and initializes an mv.ENTERPRISE/ODA server.
- Option 2, Activate an Account(s), adds the ability to execute remote commands and define remote files.
- Option 3, De-Activate An Account(s), removes the ability to execute remote commands and define remote files from the account.

- Option 4, Install ODA, installs the necessary system pointers and activates SYSPROG.
- Option 5, Logoff System, returns you to the Logon screen.

NETWORK-SETUP Utility

To run the NETWORK-SETUP utility program, select option 1, **Network Setup**. The NETWORK-SETUP Menu displays:

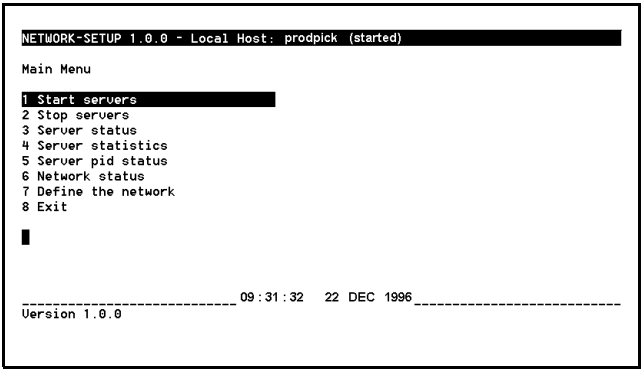

Figure 9-6: NETWORK-SETUP Menu.

Use these keystrokes to navigate through the menus and setup screens:

ENTER	Validate the highlighted choice.
number	Select the corresponding choice.
CTRL+N	Move cursor down.
CTRL+B	Move cursor up.
CTRL+X (Cancel)	Applicable only when input is requested.
ESC (Quit)	Return to previous menu, or back to TCL.
Q (Quit)	Return to previous menu.
X (Exit)	Exit to TCL.

When the cursor is moved to a new field, a short help comment is displayed in the message area.

The screens are divided in two sections:

- The menu/screen section where menu/screen text is displayed.
- The message section, where results, messages or help are displayed.

An explanation of the NETWORK-SETUP menu options:

1. Start network servers.

   Starts up all local network servers. Before running this command, it is necessary to define the network using the Define local hosts and Define remote host options and declare a local host. The server status is automatically displayed after network servers are started.

2. Stop network servers.

   Stops all local network servers.

CAUTION! Stopping network servers will prevent access to this machine by remote clients.

3. Server status.

   Displays the status of all phantom servers.

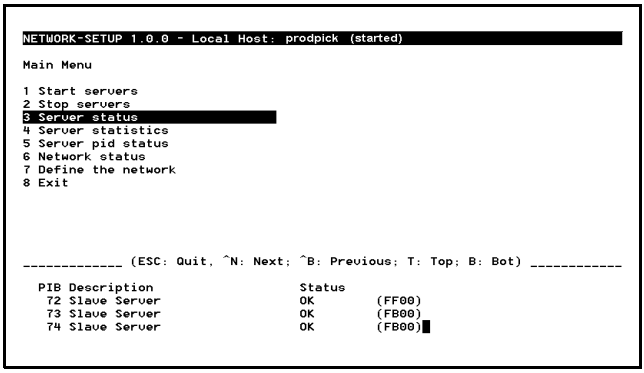

Figure 9-7: Server Status sample display.

4. Server statistics.

Displays transaction statistics for all local server processes, such as reads and writes per second.

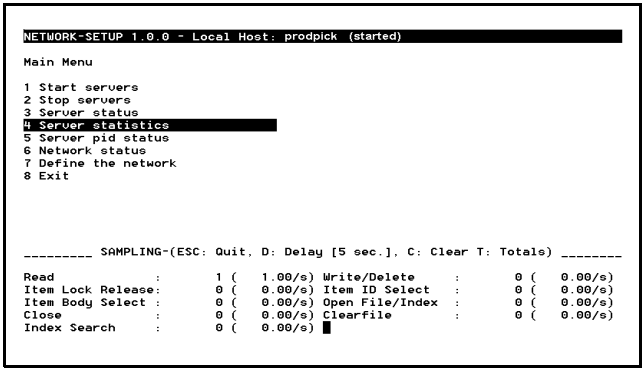

Figure 9-8: Server Statistics sample display.

5. Server pid status.

Displays a UNIX ps listing of all server processes.

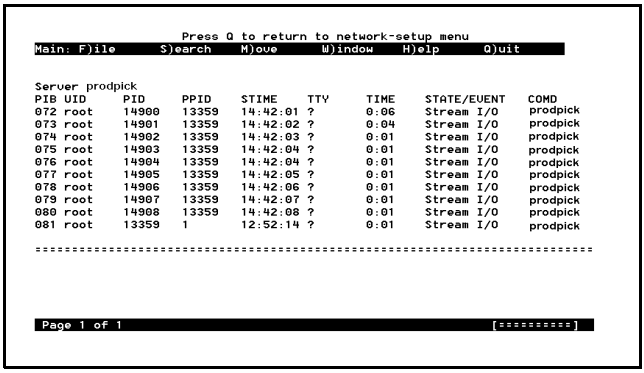

Figure 9-9: Server pid Status sample display.

6. Network status.

   Displays all lines referencing remote files.

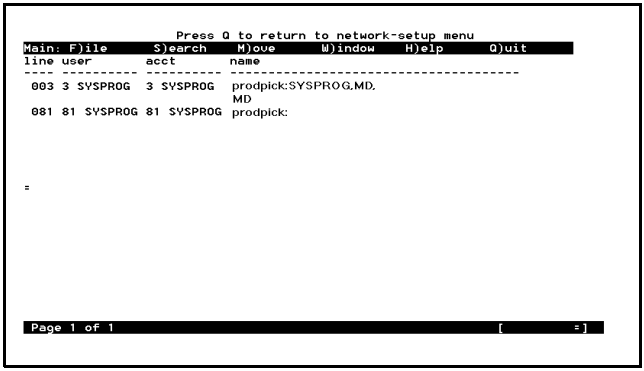

Figure 9-10: Network Status sample display.

7. Define the network.

   Displays the network definition menu in Figure 9-11. Each option is described below.

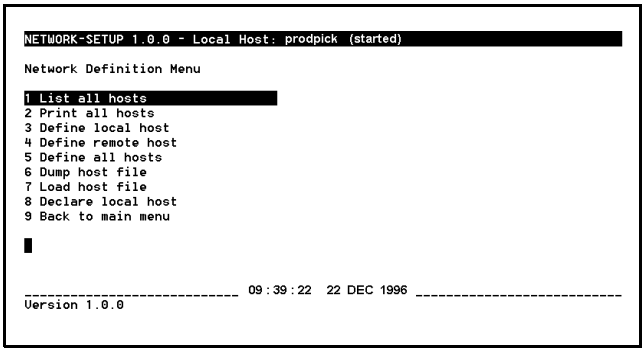

Figure 9-11: Network Definition menu display.

1. List all hosts.

   Displays a listing of all defined hosts.

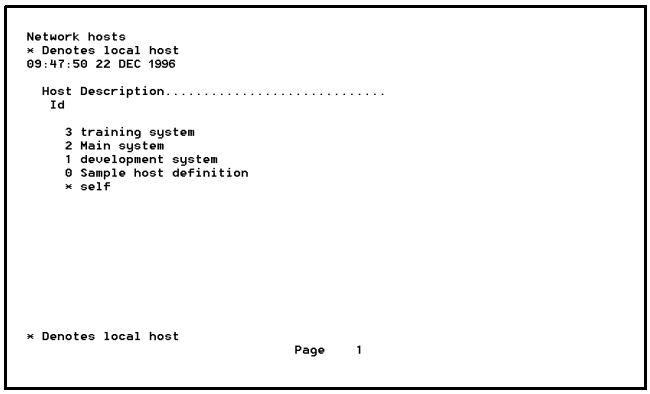

Figure 9-12: Listing of Defined Hosts

2. Print all hosts.

   Lists all hosts to the spooler.

3. Define local host.

   Configures the local network hosts. (If you are defining the entire network use option 9. Define all hosts.) Selecting this option displays the following screen:

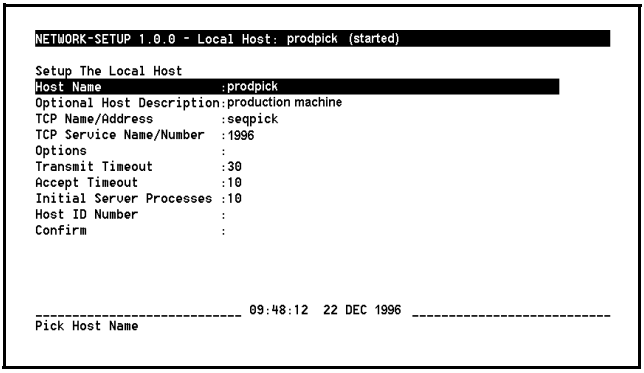

Figure 9-13: Host Setup Data Entry screen.

The following input fields are requested from the Host Setup Data Entry screen:

Host Name This is the item-ID of this host item, which is used in the Remote Q-pointer to reference files on this host. Any alphanumeric string may be entered. This field defaults to the name of the UNIX machine if no local host is defined.

For most situations, a value between 1 and 10 will provide a good balance between too many TCP connections in TIMEWAIT state and too few server processes. Note that the server process remains bound to its client when it holds item locks for that client, regardless of the Accept timeout value.

Host Description An optional description of the host. The physical description of the machine or a description of its location or the name and number of its system administrator could be helpful here.

TCP Name/ Address The TCP Name/Address where the mv.ENTERPRISE machine exists. For the server, this should be the local UNIX host name. There must be an entry for this name in the /etc/hosts file.

TCP Service Name/Number The TCP port number or service name. It is recommended that port numbers in the range 1041 through 1073 *not* be used in order to prevent interference with mv.ENTERPRISE ethernet tape operations.

✓**NOTE** Ports already in use may be verified by checking the /etc/services file.

Options These are driver-specific options. May be left blank in the simplest case.

Transmit timeout Time (in seconds) allowed for each remote operation. After this time, the client assumes the server is down and follows the error path. This value should be increased when the server is slow and *no response* errors are randomly encountered.

Accept timeout Time (in seconds) during which a server process remains bound to a client when no operations are performed. A setting of 0 (zero) disconnects after every operation and is not recommended.

Initial Server Processes Number of phantom server processes that are started when the network is started. The network must be shutdown and restarted for this value to take effect.

Host ID Number The host ID number is a number assigned to this host, which uniquely identifies this host on the network. The host ID is used when record locks are set on a remote host to identify the owner of the lock.

✓**NOTE** The host IDs must be assigned on each *client* host using the Define Local Host option from the NETWORK-SETUP utility. It is the responsibility of the system administrator to ensure that a valid, unique ID is assigned to each host.

The host ID number is used to differentiate between different virtual machines on the same UNIX host. If there is one mv.ENTERPRISE virtual on each UNIX machine, this number is not needed. If there are multiple mv.ENTERPRISE virtual machines on a UNIX host, select small numbers (less than 128) for each virtual machine on that host.

Confirm (y/n/q) Type **Y** to confirm the host information, **N** to continue editing the host item, **Q** to quit and abandon all modifications.

4. Define remote host.

   Sets up the remote hosts configuration items and displays a listing of existing host items. The local host item and remote host items contain the same information, except that the local host has the options Number of servers and Accept timeout values, which are not applicable when defining remote hosts.

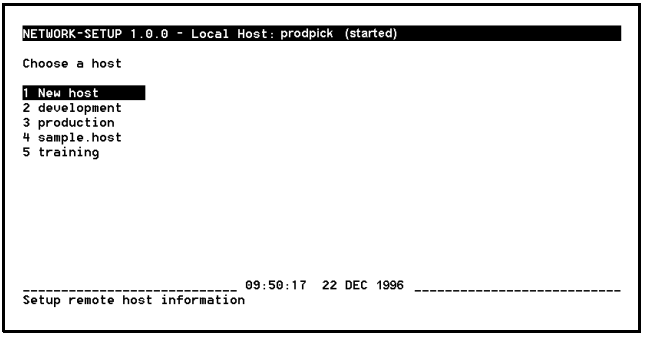

Figure 9-14: Host Listing.

To enter a new host item, select 1 (New host) and press ENTER. To modify an existing host item, select the number displayed to the left of the host name and press ENTER. A sample screen:

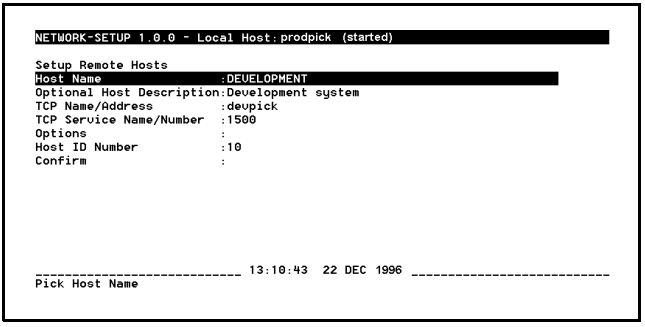

Figure 9-15: Remote Host Screen.

5. Define all hosts.

   Configure all hosts on a MultiValue network. Use this option to configure an entire MultiValue network from one station. This option, when combined with the next three, allows the network administrator to enter configuration data for all hosts, both this local one and all remotes, then dump the information to tape. That tape is then loaded on each separate MultiValue virtual machine. See menu option 7 for details on each prompt.

6. Dump host file.

   Writes the hosts file using the T-DUMP verb. Enter the tape drive number to use at the prompt.

7. Load host file.

   Loads the hosts file using the T-LOAD verb. Enter the tape drive number to use at the prompt.

8. Declare local host.

   Presents a list of hosts. After network host items have been entered, the system must be told which host item describes the local MultiValue virtual machine. Select the host that describes this machine. The phantom servers use the selected host information at startup to establish the communication link to this machine.

9. Back to main menu.

   Returns to the NETWORK-SETUP main menu (displayed in Figure 9-16).

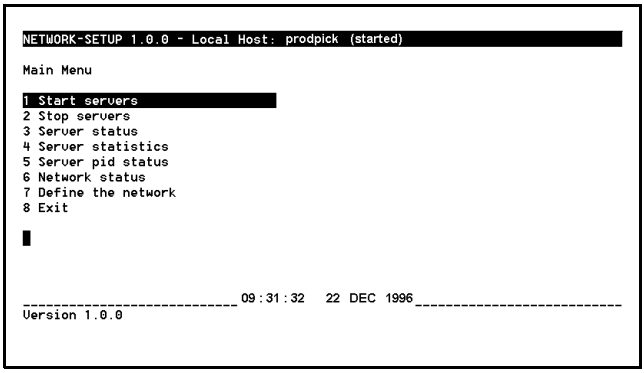

Figure 9-16: Main Menu.

10. Exit.

Exits to the ODA Administrator.

Nonmenu Operations of NETWORK-SETUP Utility

It is possible to perform some operations from TCL by specifying a command after NETWORK-SETUP at the TCL line. This functionality is useful for performing some commands in Procs and Paragraphs or through the BASIC EXECUTE statement.

Format

NETWORK-SETUP command

where: ***command*** is one of the following network commands, executable from TCL:

start	Start local server processes. (Main Menu option 1.)
stop	Stop all local server processes. (Main Menu option 2.)
status	Display status information for all local server processes. (Main Menu option 3.)
statistics	Display transaction statistics for all local server processes. (Main Menu option 4.)

Network TCL Commands

These commands perform operations from the TCL prompt. Some are also available as menu options.

NETPS

Displays a UNIX ps listing of all server processes. (NETWORK-SETUP main menu option 5)

Format

NETPS

NETWORK-STATUS

Displays remote files opened by a line.

Format

NETWORK-STATUS [*|ports] {(options}

where: ***lports*** is a line number that you can specify as one line number, a list of line numbers, a range of line numbers, or all line numbers as follows:

n,m	Displays information for line n and line m.
n-m	Displays information for lines n through m, inclusive.
n,m-o	Displays information for lines n and m through o, inclusive.
*	Displays information for all lines.

where: ***options*** are:

a	Displays all file descriptors in workspace, even closed ones.
r	Displays information for all drivers, default is the remote mv.ENTERPRISE file driver.
v	Displays internal fields - output can change between releases.

START-NETWORK

Starts all local network servers.

Format

START-NETWORK

STOP-NETWORK

Stops all local network servers.

Format

STOP-NETWORK

Section 3: mv.ENTERPRISE/ODA Operations

mv.ENTERPRISE Remote File Driver

The mv.ENTERPRISE remote file driver provides access to remote mv.ENTERPRISE files. The remote mv.ENTERPRISE machine may be a different mv.ENTERPRISE virtual on the same hardware, or an mv.ENTERPRISE virtual on a remote system accessible over a TCP/IP network.

Remote files are referenced through *Remote Q-pointers*.

mv.ENTERPRISE Remote Q-pointer

Format

001 QR
002 Account-name
003 File-name
004 Host-name

Attribute 1 Must contain the letters QR. This identifies the Master Dictionary entry as a remote Q-pointer.

Attribute 2 Name of the account on the remote machine.

Attribute 3 Name of the file in the remote account.

Attribute 4 Name of the host. This is the item- ID of the host definition item in the HOSTS file.

For each remote host, there must be an item set up in the HOSTS file. This item defines the name and the network address of the remote host. This item is added to the HOSTS file, using the network setup utility to define local and remote hosts.

Example

This remote Q-pointer references the BP file in the SOURCE account on a machine identified as DEVELOPMENT:

DEVELOPMENT.BP
001 QR
002 SOURCE
003 BP
004 DEVELOPMENT

The corresponding entry in the HOSTS file for the DEVELOPMENT machine is:

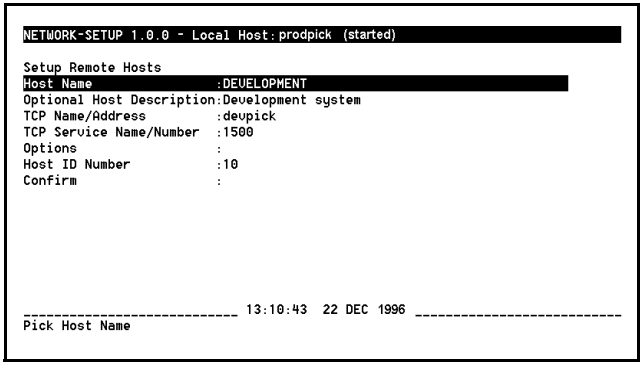

Figure 9-17: Remote Hosts Setup screen.

✓NOTE If the HOSTS file is resized, you must reinstall mv.ENTERPRISE/ODA.

The network host address consists of a UNIX local host name as defined in the /etc/hosts file and either a service name as defined in /etc/services or a TCP port number.

Access to remote files is provided through server processes running as phantom jobs on the remote system. The servers accept client connections, receive client database requests and transmit back the resultant data.

The server process will remain connected to a client for as long as there is activity from the client. If the client becomes idle for a user

definable period, the server will disconnect from the client and becomes available to service other clients.

There must be one server process per concurrent client. If there are no servers available when a client connection request is made, the client will wait for a server to become available or until the timeout period is reached, in which case the request is denied and the process returns an appropriate error message.

✓NOTE If there are record locks set on the remote machine by a client, the server becomes bound to that client until all record locks set by that client are released.

The number of server processes is defined by the system administrator using the NETWORK-SETUP utility when the server system is initially configured.

Depending on the size of the system, number of available phantom lines and the number of anticipated concurrent clients, the system can be configured to have several hundred server processes.

The server processes continue running until they are shutdown using NETWORK-SETUP or until the entire mv.ENTERPRISE machine is shutdown.

✓NOTE Warmstop/warmstart procedures are not supported on mv.ENTERPRISE/ODA clients or server machines on releases prior to release 1.0.8. If it is necessary to warmstop/warmstart, all ODA clients and servers must be SHUTDOWN before proceeding.

Use of the ON ERROR Clause with Remote Files

It is recommended that mv.ENTERPRISE BASIC programs accessing remote files use the ON ERROR clause where ever possible to report and recover from possible network errors. The ON

ERROR clause is supported on all mv.ENTERPRISE BASIC statements that can reference remote files.

If the ON ERROR clause is present and a fatal error is encountered, the statements in the ON ERROR clause are executed. The STATUS( ) function can be used to return the error number from the failed operation. Based on the error returned, the appropriate action can be taken.

If the ON ERROR clause is not used and a fatal error is encountered while performing input or output to a remote file, the program will abort to the mv.ENTERPRISE BASIC run-time debugger.

The following error numbers are returned after a failed remote file operation:

STATUS( ) Error Code	Description
3053	Specified operation not supported with the selected driver.
3054	File error.
3055	Illegal command.
3056	Server did not respond. (Increase timeout value.)
3057	Invalid file.
3058	Invalid driver number.
3059	Groups exhausted on sequential operation.
3060	Unable to allocate file descriptor at the driver level.
3061	Permission denied.
3062	Invalid TCP service name / port number.
3063	Invalid TCP host name.

Table 9-1: STATUS( ) Error Codes.

STATUS( ) Error Code	Description
3064	Protocol not found.
3065	Socket not found.
3066	Unable to bind socket to port.
3067	Unable to set passive status.
3068	Unable to connect. (Increase timeout value.)
3069	Disconnected from server. (Automatic reconnect.)
3070	Transmission error.
3071	Transmission was interrupted.
3072	Data corruption/GFE encountered on remote system.
3073	Illegal host number specified for record lock operation.
3074	You do not own object you are attempting to access. Operation failed.

Table 9-1: STATUS( ) Error Codes.

UNIX File Driver

Through the UNIX file driver, UNIX files can be accessed as if they were mv.ENTERPRISE items.

This section describes the format of the UNIX Q-pointer, the file structure and access rules.

Conventions

Since the mv.ENTERPRISE file system structure is fundamentally different from the UNIX file system, a few conventions have to be made to map an object from one file system to the other.

- An mv.ENTERPRISE item is mapped onto a UNIX file.
- By default, the mv.ENTERPRISE attribute marks are converted to newline characters (decimal 10). This option can be optionally disabled.
- By default, if a UNIX file contains the mv.ENTERPRISE system delimiters, they are converted in a sequence of two characters, DLE (decimal 16) followed by a displayable character.

UNIX	mv.ENTERPRISE
SM	DLE _
AM	DLE ^
VM	DLE]
SVM	DLE \
DLE	DLE DLE

- UNIX text files are generally terminated by a new-line character, while mv.ENTERPRISE items do not have a trailing attribute mark. By default, the terminating new-line (which would be converted to an attribute mark) is stripped when the item is read into mv.ENTERPRISE and re-appended when that item is again exported to UNIX. This provides a comfortable interface for text items, but it will write an additional new-line when writing binary items. Therefore, this default mechanism must be disabled using UNIX driver option A when modifying binary text.
- Optionally, a section of white-space preceding a block of alpha-numeric text which aligns to a tab-stop can be replaced by the appropriate number of tab characters. This process is reversed if the item is transferred to UNIX.
- An mv.ENTERPRISE file is mapped onto one or more UNIX directories. The main data level of the file is mapped to a directory which has the same name. The dictionary of the file is a subdirectory called .DICT. Other data levels are mapped onto subdirectories of the .DICT directory, prefixed with a period. The dictionary is optional and required only if data is actually stored in the dictionary. If the dictionary is missing, the file system will open it, but an error will be returned (no item, on a read and file write protected on a write) if the application actually tries to access items in it.

For example, consider the mv.ENTERPRISE file bp, with its directory and two data levels bp:

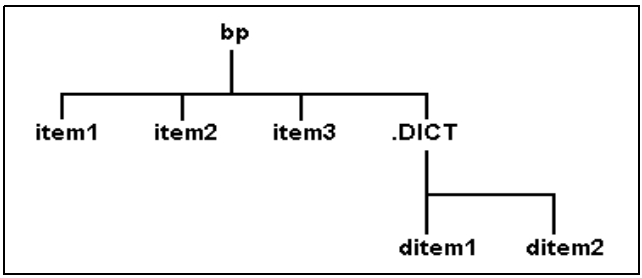

Figure 9-18: File, Directory and Data levels.

This seemingly complex structure aims at making the most common case (flat file) as simple as possible and to make commands.

UNIX Q-pointer

Format

```
001  QR
002
003
004  UNIX-host:directory{]options}
```

Attribute 1 must contain the letters QR. This identifies the item as a remote Q-pointer. Attribute 2 and 3 are null. Attribute 4 contains a UNIX host name, a UNIX path and optional driver flags.

UNIX-host:	Name of the *remote* host in the HOSTS file. UNIX hosts are identified by a 1 in attribute 1 of the host item. Several host entries can be created to use different options attached to the host. The : (colon) is used as a separator.
directory	Name of the UNIX directory onto which the main data level of the file is mapped. This directory can be any valid directory name (local directory, mounted UNIX removable medium, NFS directory). Special files (devices, pipes, etc...) can also be specified with some restrictions.
options	An alphanumeric string which controls the behavior of the UNIX file driver. Spaces can be inserted in the option string for readability. The options are separated from the directory by a value mark. The following options are available:
t n	Converts white spaces preceding text aligned to a tab-stop into a series of tabs. By default, no conversion occurs. Note that this conversion option may modify the data (especially binary items) and is therefore only suggested for text files.

A	Specifies that an extra attribute mark always be added when UNIX files are moved into mv.ENTERPRISE and that attribute mark always be removed when that item is placed back in UNIX. This option is absolutely necessary when copying between different files. Without this, nontextual items may have an extra new-line appended to them when added to the final UNIX destination.
c	Specifies the target is a special character file. This option imposes some restrictions (see the “UNIX Special Files” topic).

UNIX files can also be referenced directly without having to create a remote Q-pointer first. If the specified file cannot be located on the mv.ENTERPRISE machine and the file name begins with a /, then the name is assumed to refer to a UNIX directory. In this case the default host *UNIX* is used as the remote UNIX host.

UNIX Item-ID

The UNIX driver items are stored in the HOSTS file. The item format for a UNIX driver is:

```
itemid  unix-host-name

001   1
002
003   options
```

Attribute 1 must contain a 1. This identifies the item as a UNIX driver. Attribute 2 is null. Attribute 3 contains the driver options (see options listed in the “UNIX Q-pointer” topic).

UNIX Special Files

It is possible to specify a special character file (pipe, device) as the UNIX directory, by using the c option in the Q-pointer. However, there are restrictions:

- Special files cannot have a dictionary or their data levels.

- Only OPEN, READ, WRITE and CLOSE operations are permitted. DELETE is ignored. Sequential access (for example, LIST) returns no items present message.
- When writing, there is no guarantee that the data is written as one block. This is especially important on pipes which the notion of atomic write is critical.
- When reading, the device must be able to report the size of the data using the UNIX system call fstat( ). For example, a pipe may appear empty (size 0) at one point, and then contain data. The application must be prepared to handle empty items.

Examples

1. Create a UNIX Q-pointer to an mv.ENTERPRISE BASIC program file located on UNIX:

```
     UNIX.BP
001  QR
002
003
004  unix:/home/dev/bp]t4
```

   Use the default conversion with tab expansion.

2. Create a Q-pointer to /usr/spool/uucppublic/readme:

```
      UUCP.TEMP
001   QR
002
003
004   unix:/usr/spool/uucppublic/readme
```

3. Report on files in a uucp directory using ACCESS:

```
LIST /usr/spool/uucppublic/readme TOTAL *A9999
```

4. Use mv.ENTERPRISE BASIC to access a UNIX file:

```
001  OPEN '/users/bob' TO FILE ELSE STOP 201,'/users/bob'
002  SELECT FILE
003  10 READNEXT ID ELSE STOP
004  READ ITEM FROM FILE,ID THEN
005  PRINT ID,ITEM
006  END
007  GO 10
```

This page intentionally left blank.

Section 4: mv.ENTERPRISE TCL Commands

These commands are specific to mv.ENTERPRISE.

CLEAR-RECLOCKS Command

The CLEAR-RECLOCKS command clears record locks.

Format

CLEAR-RECLOCKS hostid/hostname/**ALL/LOCAL** {line-number{filebase}}

Parameter(s)

hostid	Numeric host identification number.
hostname	Item-ID of host definition item in 'HOSTS' file.
ALL	Specifies all hosts.
LOCAL	Specifies the local machine.
line-number	Line number of the record lock owner.
filebase	Specifies only locks for the specified filebase (in hexidecimal) are to be released.

If no line number is specified, all record locks for the specified host will be released.

CAUTION! Inappropriate use of the CLEAR-RECLOCKS verb will violate multiuser lock protocols and may damage your database. This verb is intended solely for use by qualfied individuals who understand and accept the risks associated with it.

REMOTE-CACHE Command

The REMOTE-CACHE command increases the performance of updates over a network by sending groups of updates.

Normally, each update made on a remote file is sent immediately to the remote site. Because of limitations in network throughput, this action can introduce delays in batch update applications. To alleviate this issue, batch updates can be cached and sent in groups. Caching significantly improves performance to almost the same point as a series of local updates. Use REMOTE-CACHE to turn update caching on and off, and/or to flush the cache.

Format

REMOTE-CACHE remotefilename {number.of.updates}

Parameter(s)

remotefilename	Name of the remote file.
number. of.updates	Number of updates. If no amount is specified, the default is 32.

To turn off update caching and to flush the cache type:

```
REMOTE-CACHE remotefilename 0
```

The REMOTE-CACHE command only affects updates from the current line to the selected file and remains active until the line is logged off.

When using cached updates be aware of the following limitations:

- Caching will not take place for binary items.
- Caching will not take place if any remote locks are held.
- The actual modification to the remote machine does not take place until one of the following events occur:

  1. The maximum number of updates fill the cache.

2. An item is read from the remote file.
3. The process requests terminal input.
4. The process performs a TCL level push operation, either interactively using the break key or with the BASIC EXECUTE statement.
5. A BASIC SELECT statement is executed on the remote file.
6. A BASIC SLEEP statement is executed when sleep time is more than one second.
7. The process returns to TCL.
8. The process logs off or is logged off by another line.
9. To take advantage of caching when using the COPY command the O overwrite option must be used.

REMX Command

The REMX command executes a TCL command on a remote system and returns the results, including error messages, command output and any active select list.

Format

REMX {[remx_options]}

REMX {[remx_options]} hostname command {(command-options}

REMX {[remx_options]} hostname:accountname{,password} command {(command-options}

Parameter(s)

remx_options	Effect the behavior of the REMX command itself. These *must* be enclosed in square brackets ([ ]). Currently, the only available option is S, which requests that the returned command output be suppressed.
hostname:	Name of the remote host to execute the specified command on. Must be previously defined in the local HOSTS file and have one or more active mv.ENTERPRISE/ODA server processes running. The : (colon) is used as a separator. (Refer to ”NETWORK-SETUP Utility.”)
accountname	Name of the account on the remote host in which the specified command should be executed. If not specified, defaults to the account the remote server was started on (usually ODA.ADMIN).
password	Password for the specified account, if required.
command	A single-line TCL command followed by any desired command-line options. (Refer to Figure 9-19.)

The REMX command may conceptually be thought of as similar to a BASIC EXECUTE statement, in that it executes a TCL-level command and then returns the results to the process that issued the REMX. As with EXECUTE, these results can include the actual screen output from the command (similar to EXECUTE 's CAPTURING clause), any error message numbers produced during the command's execution (EXECUTE's RETURNING clause), and the contents of any active select list produced by the command.

REMX has two main forms: interactive and command-line. The interactive form is entered by entering REMX alone at TCL; this begins a dialogue which prompts the user for each of the required REMX parameters. The interactive form allows multiple remote commands to be submitted at one time, with each sequentially executed by the remote system. At the end of the execution of the last command, the screen output from all commands is displayed on the screen of the process that issued the REMX. If the final command produced an active select list, this list is transferred to the local system and becomes the active select list for the issuing process.

The command-line form of REMX functions identically to the interactive form, except that only one command can be issued at a time. (This command may, of course, reference a Proc or BASIC program on the remote system which itself performs many commands.)

```
:REMX
Hostname: ARCHIVEPICK
Accountname{,password} (<cr> for default
account):  OLD-ORDER
Command: SELECT ORD.DETAIL WITH SKU “A34-1222”
Command: RUN ARCHIVE.BP SALES.ANAL.RPT
Command:
```

Figure 9-19: Interactive REMX.

Refer to Figure 9-19. Two commands are issued for sequential execution on the remote system ARCHIVEPICK. The first performs a file SELECT, and the second command processes the items from this active list. No list is returned to the calling process because the list generated by the SELECT will not be active at the end of the execution of the SALES.ANAL.RPT program. The Command: prompt displays continuously, until a carriage return is entered at the prompt.

```
REMX [S] DEVPICK:MAIN,XYZZY SELECT PRODUCT
WITH SKU “JDR412]”
```

Figure 9-20: Command-line REMX.

Refer to Figure 9-20. A SELECT command is issued to system DEVPICK for execution 6 on account MAIN (account password XYZZY). The REMX option [S] specifies that the screen output from this command, if any, is not to be returned to the local system. Any active select list produced by the execution of this SELECT on the remote system will be returned to the local system and become the currently active select list. If no items are found on the PRODUCT file meeting the specified SELECT criteria, no list will be returned, and error message 401 will be issued—just as if the SELECT command had been executed on the local system.

✓NOTE

- Input cannot be *stacked* on the local system to satisfy terminal input statements issued by the remote process. Any request for terminal input will terminate the remote command immediately.
- The pseudo-LOGTO process performed by the server process to execute the remote command on the specified account does not update the remote system's ACC file. This means that the command REMX host:accountname WHO will always return ODA.ADMIN, not accountname, as its output.
- File access and update permissions in effect during the execution of the remote command will be those of the account the command is being executed on, not those of the local client process that issued the REMX command.
- The server process executing the remote command will be bound to the local client for the entire duration of the command's execution. This will reduce the ODA requests during that time, possibly leading to reduced mv.ENTERPRISE/ODA performance if not enough ODA data transfer requests. To prevent this, the remote command can be executed on the remote machine as a phantom process by preceding it with the Z or ZH commands. This will free up both the client and the server system immediately after the phantom job request is submitted (but will of course not permit capturing of screen output or the direct return of an active select list).
- As with a BASIC EXECUTE statement, a UNIX-level command can be executed, but the output from the command cannot be captured or return.

```
:REMX SYSTEMB SHrm -f /edi/tmp/*
```

Figure 9-21: REMX executing a UNIX command.

```
:REMX ANCHORAGE1 COPY USERS 'MADGE' (T)
```

Figure 9-22: REMX with options.

```
:REMX MEGASYSTEM ZH BIG.NASTY.BATCH.PROCESS
```

Figure 9-23: REMX issuing a remote command as a phantom process.

Error Messages

Error messages specific to REMX you may receive are:

3001	Remote execute failed!
3002	Specified account name or password was rejected; remote execute failed.
30XX	Other normal mv.ENTERPRISE/ODA errors.

SET-RFILE Command

The SET-RFILE command sets up one or more Q-pointer items in the user's account, pointing to one or more files of a remote account.

Format

SET-RFILE accountname filename hostname {synonym} {(**O**}
SET-RFILE accountname **MD** hostname {synonym} {(**O**}
SET-RFILE accountname * hostname {(**O**}

Parameter(s)

accountname	Name of the account on the remote host in which the specified filename(s) or MD is defined.
filename	Name of the file to be accessed.
MD	The account MD may be specified.
*	Used to also create Q-pointer items for all files in the remote account. These will be created using the same filenames as on the remote account.
hostname	Name of a remote host as defined in ODA.ADMIN. (Refer to the "NETWORK-SETUP Utility" topic.)
synonym	The optional synonym name may be included if only one file name (not '*') is specified. If omitted, the synonym item QRFILE is used and updated.
O	The optional (O may be used to force existing items to be overwritten, although any existing file definition items will not be updated.

Example

```
SET-RFILE EDSACCOUNT EDSFILE EDSHOST
EDSNEW (O
```

Section 5: Summary of mv.ENTERPRISE/ODA Commands

Summary of mv.ENTERPRISE/ODA Commands

The following is a summary of the mv.ENTERPRISE/ODA commands described in this chapter:

CLEAR-RECLOCKS hostid/hostname/ALL {line-number}

NETPS

NETWORK-SETUP command

NETWORK-STATUS [*|ports] {(options}

ODA.ADMIN

REMOTE-CACHE remotefilename {number.of.updates}
REMOTE-CACHE remotefilename 0

REMX {[remx_options]}
REMX {[remx_options]} hostname command {(command-options}
REMX {[remx_options]} hostname:accountname{,password} command {(command-options}

SET-RFILE accountname filename hostname {synonym} {(O}
SET-RFILE accountname MD hostname {synonym} {(O}
SET-RFILE accountname * hostname {(O}

START-NETWORK

STOP-NETWORK

This page intentionally left blank.