DNSMG0.WS4   (= "DR Net System Manager's Guide", foreword)

DR Net
System Manager's Guide

First Edition: April 1984

(Retyped by Emmanuel ROCHE.)

Foreword

DR Net is a network operating system that enables use of remote disk drives,
list devices, and queues. It is designed for use with computers running
Concurrent CP/M and CP/M-86. DR Net requires no modifications to these
resident operating systems, or to the application software. When you integrate
DR Net with CP/M-86, the computer can function as a network requester node.
When you integrate DR Net with Concurrent CP/M, the computer can function as a
network requester, server, or as a homogeneous node which provides requester
and server functions simultaneously.

How to use this manual

The "DR Net System Manager's Guide" is written for the person responsible for
installing and maintaining a network of computers. DR Net can be implemented
upon a wide variety of computers, for an extensive range of network
controllers and network topologies. However, this manual cannot discuss all
the configurations possible with DR Net. Consequently, it serves as a general
guide to network installation and maintenance.

Your system implementer provides specific information regarding the
installation and maintenance of the DR Net network. We refer to this person
throughout this manual as the original equipment manufacturer (OEM). This is
the person or company who developed an integrated package from a computer, the
Concurrent CP/M or CP/M-86 operating system, a network controller, and DR Net.
When there are discrepancies between documentation provided by your OEM and
this DR Net manual, The OEM information supercedes the information provided
herein.

This manual describes the DR Net features, options, and operating
characteristics from a system management perspective. The presentation is as
follows

    - Section 1 describes the different types of DR Net nodes, the internal
      resource maps that provide remote replacements for local disk drives,
      printers, and queues, and the DR Net options that affect your network
      configurations.

    - Section 2 describes DR Net system generation, and offers some

suggestion to help with DR Net installation and network setup.

- Section 3 provides guidelines for maintaining your network, lists and
  describes DR Net error messages and CP/M error messages, and offers
  advice on how to recover from errors, and locate problems.

- Appendix A lists and describes the GENNET, GENRQR, and ADDNET error
  messages.

- Appendix B contains configuration forms to help you plan and keep
  track of your network.

Before using this manual, you should understand CP/M-86 or Concurrent CP/M
nomenclature and operating procedures. This assumes familiarity with the
concepts and use of virtual consoles and command conventions, and options. It
also assumes that you have read the "DR Net User's Guide".

Conventions used in this manual

In all commands illustrations and example, "A>" represents the system prompt.
Drive A is used as the current drive. However, this does not preclude the use
of other drives.

All commands are shown in UPPERCASE. Command tails are shown in lowercase. For
example,

    LOGON {nodename}

Both of these conventions are used for clarity. Both the command and the
command tail can be entered in uppercase or lowercase. If the command tail is
enclosed in curly brackets ("{" and "}"), as above, the tail is optional.

In this manual, computer output is shown in colored type. User input is shown
in boldface, colored type.

Each DR Net node has a unique, hexadecimal ID number. Two colons ("::") always
follow the ID number, and are considered part of the number. For example,
"00::" and "AE::" are valid node ID numbers.

"Resident operating system" refers to the computer's implementation of
Concurrent CP/M or CP/M-86, not to the DR Net implementation.

"Application program" refers to any program that the user can invoke. This
includes all DR Net and CP/M utilities, as well as data processing programs
such as a general ledger, word processing, and spreadsheet software.

"OEM" (for Original Equipment Manufacturer) is used throughout this manual as
a reference to the manufacturer who customized DR Net for your use.

"Attach the network" can be interpreted to mean "load the network". Although
this is not a truly accurate word replacement, use of the system is not
compromised by the difference.

"Resource map" is synonymous with term "device map" used in the "User's Guide".

This manual references many of the DR Net utilities. Familiarity with them is assumed. For descriptions of DR Net utilities, see the "User's Guide".

Table of Contents

EOF

DNSMG1.WS4   (= "DR Net System Manager's Guide", section 1)

DR Net
System Manager's Guide

First Edition: April 1984

(Retyped by Emmanuel ROCHE.)

Section 1: What is DR Net?

DR Net is a network operating system that enables computers to communicate
with other computers, permitting shared access to disk drives, list devices,
and queues. DR Net is a program, and is not the physical network hardware or
the transaction protocol responsible for moving data from one computer to
another. DR Net is the interface that allows application programs to access
the remote disk drives, list devices, and queues through the network hardware.
Figure 1-1 illustrates the concept of DR Net and its role in networked
computer systems.

```
   Computer      Hardware            Hardware
    System       Resources           Resources
 +-------------+                    +-------------+
 | Resident  |--> Console      Console <--| Resident  |
 | Operating |--> Disk Drive    Disk Drive <--| Operating |
 | System    |--> Printer        Printer <--| System    |
+-+-------------+                    +-------------+-+
|| DR Net   |--> Network <-> Physical <-> Network <--| DR Net  ||
+-+-------------+  Controller  Network  Controller +-------------+-+
|| Application |                    | Application ||
|| Programs  |                    | Programs  ||
| +-------------+                    +-------------+ |
+---------------------------- DR Net traps ----------------------------+
                and routes system
              calls from applications.
```
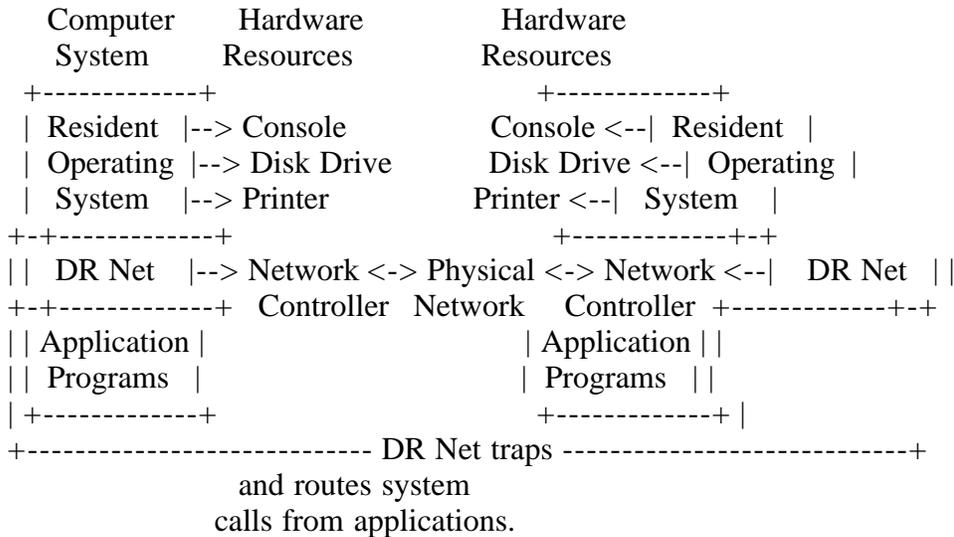
     Figure 1-1. Computer environment with DR Net

DR Net operates on a resource swapping basis. This means that operators use
local resouces, both real and virtual, as references to access an equivalent
remote resource. DR Net automatically replaces the local resource with the
remote equivalent resource according to the entries in an internal table
called the resource map. Computer resources that can be swapped under DR Net
are disk drives, list devices, and queues.

Every networked computer has its own resource map. This table allows a
separate map entry for 16 drives, 16 list devices, and 16 queues. Each entry
in the table consists of three fields. The first indicates whether the
associated resource is local or networked. The second indicates   the

replacement resource. The third indicates the node number where the replacement resource is located. The second and third fields are applicable only when the first field indicates the resource is networked.

DR Net conducts transactions between networked computers on a system call basis. System calls are the standard set of CP/M-86 and Concurrent CP/M functions called by utilities and data processing software to use computer facilities. When an application makes a system call, DR Net traps the call and determines if it accesses a remote resource. If it does, a network message is sent to the node designated in the resource map where the function is executed, and the response returned.

DR Net is not involved with application program operation until the program makes a system call. In addition, DR Net only becomes involved when the system call references a remote disk drive, list device, or queue. Otherwise, all system calls are executed by the resident operating system.

Although unnecessary, most DR Net implementations use a controller to send and receive messages over the physical network. A network controller functions like a disk controller in that, just as a disk controller is used by an operating system to access a disk drive, a network controller is used by DR Net to access the network lines.

Network controllers are available in a variety of forms, and can use different data transfer protocols to network computers. For example, many popular, bus-oriented computers have a plug-compatible, printed circuit board. In turn, different boards are available for the same computer, which provide different transfer protocols, such as Ethernet or ARCNET for moving messages between nodes.

The distinction between a network's hardware and software, though real, is not significant to the user. Your OEM has implemented DR Net for a specific computer system and network controller; consequently, it always has the same user interface. However, you should understand the distinction between the hardware and software if you must physically connect one computer to another and conduct troubleshooting procedures. For specific information on your network controller or other computer hardware, contact your OEM.

1.1 Network node types

Every networked computer must have DR Net installed. DR Net provides the following three types of network nodes:

    - requester-only
    - server-only
    - simultaneous requester/server

Computer systems with the Concurrent CP/M operating systems can be configured for any of the three node types. Computers running the CP/M-86 operating system can function as requesters only.

1.1.1 Requester nodes

A DR Net requester is any node that attempts to access resources on remote
network nodes. The requester node has access to its own printers, disk drives,
and queues, as well as to resources on remote nodes when the network is
attached. When the network is not attached, only the local resources are
available.

The DR Net requester function can be thought of as a system call screener. As
application programs make standard system calls to access a disk drive, print
a character, and so forth, DR Net screens the calls, and sends those that
reference a mapped resource to the appropriate server. System calls that
reference local resources are passed to the resident operating system for
execution. Figure 1-2 illustrates the DR Net call screening process in a
requester node.

```
                    +------------+
                    | Resident |
                    | Operating |
                    | System   |
                    |     /\  |
              +--+--||---||---+
              | | ||  ||---|-- Calls to local
              | | ||  || |    resources.
              | | ||  || |
              | | ||/---------- Return value
        DR net <--+ | ||\----------  from server.
              | | ||  || |
              | | || +----+----> Resource map screen
       Return values --|--|--|| |....| |
       from system    | | || |....|----\ Calls to mapped
       call to        | | || |....|----/  resources.
       application    | | || +----+ |
              | | ||  /\  |
                +--+--||---||---+
                 | \/ ||  |
                 |      ||------> System calls
                |Application |     from applications.
                | Program  |
                +------------+
```
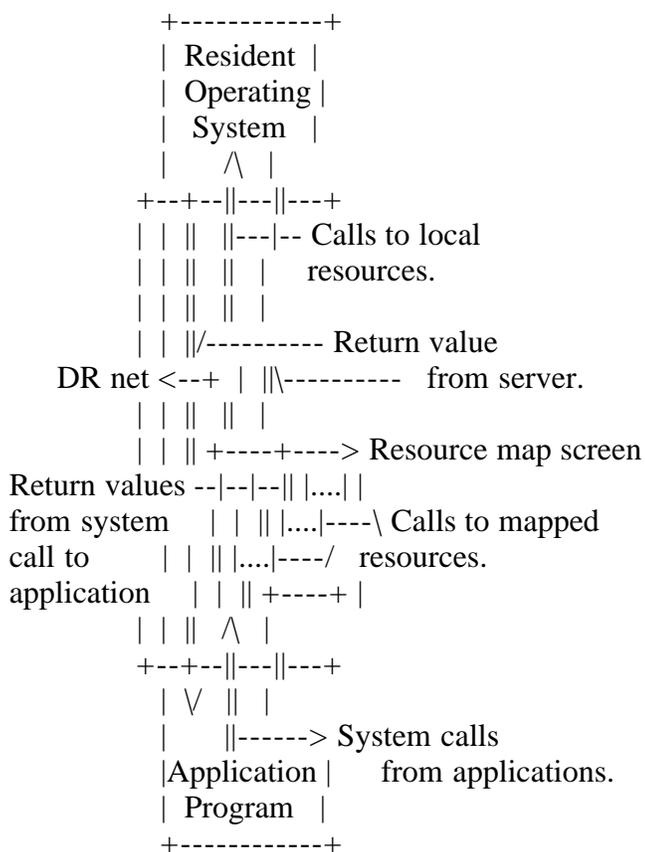
   Figure 1-2. DR Net requester

After the call has been executed on the server, DR Net recives the information
from the server, and returns it to the calling program. The entire network
transaction is transparent to the calling application and the operator, so
that existing utilities and applications require no modifications to run in
the DR Net environment.

In Concurrent CP/M requesters, users attach DR Net with NETON.CMD. In CP/M-86
requesters, users attach DR Net with NETLDR.CMD. Attaching provides a virtual
console or a computer system with a network environment consisting of a
resource map and a blank log-on table. The resource map, as mentioned earlier,

is an internal table referenced by DR Net to map disk drives, list devices, and queues to servers. The log-on table is another internal table that contains a list of all servers logged on.

Note: In Concurrent CP/M systems, NETON only attaches the current virtual console. If the user switches consoles, NETON must be invoked again to attach the network. The previous virtual console remains attached, so that, when the user switches back to it, he or she need not run NETON again. This feature, combined with the ability to change resource map entries, allows you to have different network environment on each virtual console.

After invoking NETON, the user must log-on servers with the LOGON.CMD utility before they can be accessed. Each server is logged on individually by its node number or, if name service has been installed, by its node name. Each requester has a default server. For convenience, DR Net logs on the default server when the LOGON command is invoked without a node specification. After LOGON has been run, the designated server's resources can be accessed using local resources as references.

Servers are logged off one at a time with the LOGOFF.CMD utility. Alternatively, users on nodes with the Concurrent CP/M operating system can log off all servers, and detach from the network, with the NETOFF.CMD. CP/M-86 requesters can only use LOGOFF to log off servers. To detach the network from a CP/M-86 requester, the computer must be reset. Subsequently, the network is no longer attached, and only local resources are available. To use the network again, the operator must first invoke NETON or NETLDR, and then use LOGON to log on the servers.

In Concurrent CP/M requesters, NETON attaches the network to processes, rather than the entire node. (This is why virtual consoles must be attached individually.) The first process attached on each virtual console is the terminal message process which interprets all user commands. When application programs are invoked, they are automatically attached and become, along with the terminal message process, requester processes.

There is a limit to the number of requester processes that can be attached simultaneously. The limit is set when you create the computer's DR Net system image. To avoid specifying too few requester processes, add up the number of applications on each virtual console that you project will be using the network concurrently. For example, a SUBMIT routine that invokes a single program requires three requester processes: one for the terminal message process, one for SUBMIT, and one for the application.

Because CP/M-86 does not support concurrent programs, only one process is attached to the network in CP/M-86 requesters.

1.1.2 Server nodes

Server nodes service requests from requester nodes. As soon as the operating system is loaded, the node is available to function as a network server. There is no equivalent to the NETON utility for DR Net server nodes.

Every requester has a default server. The single default server can be shared
by all requesters, groups of requesters can have different default servers, or
each requester can have a different default server. The default server is
distinguished, because it is the node accessed by the DR Net LOGON, LOGOFF,
and NET.CMD utilities when a node number or name is not entered by the user.
The default server is also where the data file that provides DR Net's name
service is recorded. (See Section 1.3.5 for a description of DR Net's name
service.)

DR Net server nodes are full-service computers with the Concurrent CP/M
operating system. Consequently, a server-only node can be used as a stand-
alone system. Operators have access to all of the system's facilities. Because
servers require no operator supervision or intervention, server systems do not
require a console. In addition, DR Net allows you to specify private drives
that are withheld from access by remote requesters.

The DR Net server functions as a process manager that creates, signals, and
terminates shadow processes according to messages received from requesters. A
shadow process is a requester process's representative whose purpose is to
present the requester's system calls to the server's operating system. For
example, when a system call is received to read a record from a disk file, the
shadow process makes the system call to its operating system on behalf of
requester. The shadow process also sends the response back to the requester.
Figure 1-3 illustrates the relationship of shadow processes to requester
processes.

```
                   +-------------+
                   | Resident  | System calls to and
         Requester   | Operating | return values from
          Nodes    |  System   | resident operating
                   | ∧ ∧ ∧ ∧ <---- system.
          R1 <--+  +-||-||-||-||-+--+
                | | |∨ ∨ ∨ ∨| |
          R2 <--+ | S1 S2 S3 S4 <----- Shadow Processes
                | |∧ ∧ ∧ ∧| +--> DR Net
                | | || || || || | |
          R3 <--+--+-++-++-++-++ | |
     Network      | +-------------+--+
     Connection -->| | Application |
                | | Programs  |
          R4 <--+ |(not directly|
                 |involved with|
                 |   shadow   |
                 | processes) |
                 +-------------+
```
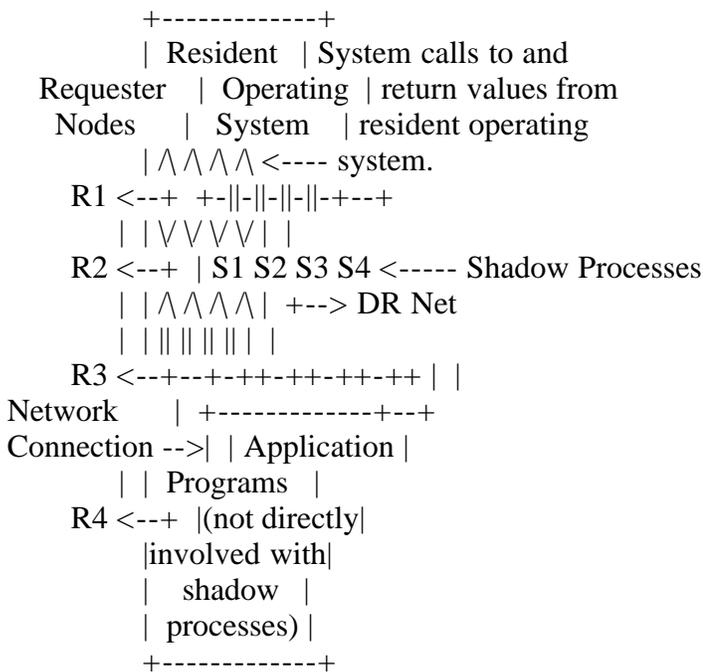
      Figure 1-3. DR Net server shadow processes

Shadow processes are created when the server receives a log-on message with
the proper password. The shadow process idles until signaled that a message
has been received from its requester process. The shadow process is terminated
when the requester process logs off or goes inactive for a long time, or when
a failure in the network connection occurs.

The number of shadow processes that can be created in a DR Net server is set during DR Net system generation. Because it is possible to specify too small a number, determine each server's requirements by adding up the number of requester processes you would like the server to be able to support at one time.

1.1.3 Requester/server nodes

Computers based on Concurrent CP/M can be configured as simultaneous requester and server nodes. A requester/server node provides all functions of a requester node, and all the functions of a server node. You can attach to the network, log on servers, and make requests of all other servers. You can also detach from the network, and use only the local resources. While all this is going on, the server function can be servicing requests from other nodes without the intervention of the operator.

1.2 Resource mapping

The resource map is a table that contains individual entries for local disk drives A through P, local printers 0 through 15, and up to 16 local queue. Each entry indicates the following:

    - whether the resource is local, or contains a map entry
    - the replacement drive name, list number, or queue name
    - the server ID number where the replacement resource is located

When it traps a system call, DR Net uses the resource map to determine if the resource referenced in the system call is local or remote. Figure 1-4 illustrates this function.

```
     Requester node  Resources       Resources      Server nodes
     -------------- ---------       ---------       ------------
    Console--Computer--Drive A Drive B...Drive A Drive B--SERVER
           :                      :    |
           +......Drive C.....................+     |
           :                             |
    Virtual    :            +.........Printer 0-------+
    Devices    :         :                |
           +......Drive D....:.........+          |
           :          :    |         |
           :          :    Drive A Drive B--PRINT
           +......Printer 0..+             |
           :                         |
           +......Printer 1............Printer 0-------+
```

    See Figure 1-5 for NETSTAT display of this configuration.
    (There are three nodes: SERVER, PRINT, and the computer on the left.)
    Note that queues are not illustrated.
    Network connections: ---
    Virtual connections: ...

Figure 1-4. Sample resource map

1.2.1 Displaying the current resource map

The NETSTAT.CMD utility displays a virtual console's current resource map.
Figure 1-5 is a sample of a NETSTAT display.

```
       ------------------------------------------------------
       Network Status Utility           For Node 06::
       ------------------------------------------------------
       Device Type  Local = Remote  on  Node  Logged On?
       -----------  -----   ------      ---- ----------
       Disks :     B      A       SERVER   YES
                   C      B       SERVER   YES
                   D      A        PRINT    YES
       Printers:   0      0        SERVER   YES
                   1      0      PRINT    NO
       Queues:    MXSPL  MXSPL     PRINT    NO
                  SPLIN  SPLIN     PRINT   NO
                  SPLOUT SPLOUT    PRINT   NO
       ------------------------------------------------------
                    Node     Name
                    ----     ----
       Servers Logged on:    00::     SERVER
       ------------------------------------------------------
```

Figure 1-5. NETSTAT display

In the NETSTAT display, the local column contains the list of all disks,
printers, and queues for which there is a map entry. The "Remote" column
contains the name or number of the remote replacement for each local resource.
The "Node" column indicates the server from which the replacement is
available. To use this table, read the information from the column as follows:
"I use local (drive, printer, or queue) to access remote (drive, printer, or
queue) on node (number or name)."

Notice that the NETSTAT display also indicates if you are logged on to a
resource's server. In addition, the lower portion of the display contains a
list of all servers currently logged on. Server node names are shown in Figure
1-5. These are only displayed if the name service is available. Otherwise, the
server node numbers are shown.

1.2.2 Default resource map

Every requester node has a default resource map. The default resource map is
created from prompts in the DR Net system generation utilities. When a
requester node attaches the network, its initial environment is defined by the
default resource map.

Users can change default map assignments with the DR Net NET.CMD and LOCAL.CMD
utilities. Applications that use special DR Net system calls can also change a
resource map under program control, without the operator's knowledge. However,
when NETOFF is run, or the computer is reset, all modifications are erased.
The next time you attach DR Net, the network environment is defined by the
default resource map.

1.3 Network planning

Before you install DR Net, plan your network by determining the following:

        - the configuration of requester, server, and requester/server nodes
        - the default server for each requester node
        - the resource map for each requester node
        - the server passwords
        - the DR Net name service
        - your application software

Each item in this list is significant to network implementation. Careful
planning can reduce operator confusion, maximize system efficiency, and
prevent time-consuming adjustments. Appendix B contains forms to help you plan
and configure your network.

1.3.1 Network configuration

DR Net allows you to configure a network of requesters and servers in three
basic ways. The configuration you select impacts on your choice of default
servers, passwords, and resource maps.

Note: Do not confuse the network configuration with the network topology.
Network topology refers to the internal transfer mechanism that moves messages
from one computer to another, and prevents message collisions on the physical
network lines. This is transparent to the user, and independent of the
configuration of requester and server nodes.

Figure 1-6 illustrates three basic types of network configurations supported
by DR Net. Other configurations are possible. The configuration you adopt can
combine up to 255 computers in any combination of requesters and servers, and
can be modified as data processing needs change.
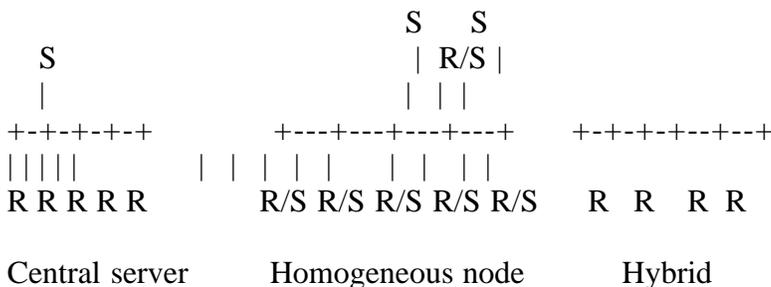

```
                             S    S
      S                      | R/S |
      |                      | | |
    +-+-+-+-+         +---+---+---+---+      +-+-+-+--+--+--+
    |||||            |  |  |  |  |      |  |  |  |
    R R R R R         R/S R/S R/S R/S R/S     R   R   R R

    Central server      Homogeneous node        Hybrid

    R = requester
```

S = server
R/S = combination requester/server

Figure 1-6. Fundamental network configurations

Central server configuration

The central server configuration is appropriate when you want a group of
small, limited-resource computers to share access to a computer with
expensive, high-performance resources (for example, a hard disk or high-speed
printer). Besides sharing physical resources, this configuration is also
suitable in applications where requesters require common access to a data
base. An example of a central server configuration would be an order
processing system consisting of independent stations to enter orders, and a
server with a hard disk to file the orders.

Homogeneous node configuration

In this configuration, each node serves both requester and server functions.
This alternative is suitable for installations where each computer has
sufficient facilities to run its applications, but intercomputer communication
is required for the occasional exchange of data. An example of a homogeneous
node configuration would be a community of users, each with a full-function
personal computer, that send electronic mail over the network, and share
files.

Hybrid configuration

Hybrid networks combine the features of the sentral server and homogeneous
node configurations.

1.3.2 Default server

Remember that each node has a single default server. The default server of a
requester node is determined during system generation from a prompt in the
system genration program. The default ID value of the default server is 00::.
However, any other value, up to and including FE::, can be entered.

The default is significant to the DR Net name service used by the LOGON,
LOGOFF, NETSTAT, and NAMESMOD utilities. DR Net's name service allows you to
use node names, rather than node numbers to specify a node. In order to
provide this feature, these utilities reference a file, named "NAMSVR.DAT", in
user area 0 on the system drive of their node's default server. This file
contains the name assigned to each node ID number.

The default server is also significant in that it is the server assumed when

the operator does not specify a node in the LOGON, LOGOFF, and NET command lines.

Note that a requester can be its own default server. This provides name service immediately after the network is attached, but before the user logs on to any servers. However, you should exercise care when you map resources and use the network utilities. For example, the LOGON utility logs on the default server if no other server is specified in the command line. If you attempt to log on yourself, many implementations of DR Net display an error message.

1.3.3 Default resource map

The default resource map for each requester is defined during DR Net system generation. It defines the user's initial environment of local and remote disk drives, list devices, and queues when the network is attached. When you create the default resource map, consider the following:

   - Any disk drive or list device can be mapped. For example, local drive
     P on a two drive system with logical drives A and B can be mapped to a
     remote drive A. However, make sure that the remote device exists. If
     the same drive P is mapped to drive K when there is no drive K, file
     system errors are returned to the requester when it references drive
     P.

   - It is sometimes convenient to create a single resource map for all
     nodes. (This is especially true in central server and some hybrid
     configurations.) When you create the map, make sure that a requester
     has no virtual devices mapped to itself.

Attempting to access such devices results in a DR Net physical transmission error.

   - You can map queues for a requester based on CP/M-86. However,
     application programs can only use the queues when they are mapped to a
     server, and the network is attached. If the queue is not mapped, or
     the network is not attached, a local file system error results.

   - Under no circumstances should any of the Concurrent CP/M system queues
     be mapped across the network. Examples of such queues are:

          Mxdisk
          Mxload
          VOUTQxx
          VINQxx
          DIR
          ABORT

     Mapping any of these queues has unpredictable, but usually
     catastrophic, results.

The DR Net system generation utility allows you to specify private drives for each server node. A requester cannot access a private drive on a server. If a

requester attempts to access a remote drive that has been marked private, a
file system error results.

1.3.4 Network passwords

DR Net allows you to incorporate password protection to control access to a
server. The password is entered in response to a prompt in the DR Net system
generation utility. Because the same system generation program is also used to
create requester and requester/server nodes, the following rules apply to the
password entered:

   - In requester nodes, the password you enter becomes the default
     password sent with each LOGON command. When a password is specified in
     the command line, the user entry overrides the default password.

   - In server nodes, the password entered is the password that must be
     matched by every log on message to gain access to that server.

   - In combination requester/server nodes, the password entered is the
     password that must be matched by remote requesters, and the default
     password sent with each LOGON command.

1.3.5 Network name service

When DR Net's name service is implemented, each requester and server node can
be referred to by a unique name, as well as by an ID number. The name service
is available to all requester nodes.

Name service is installed and maintained by the DR Net NAMESMOD.CMD utility.
This program creates a file named "NAMSVR.DAT", which contains all the node
number and name assignments. When a requester node attaches the network, DR
Net looks to user area 0 of the system drive on the node's default server for
the "NAMSVR.DAT" file. For this reason, it is advisable to make sure that the
system drive of the default server is a hard disk or, at least, is a disk that
will not be removed in day to day operation.

When name service is implemented, users can display the name assignments for
each network server and requester node recorded, and use these assignments to
log on servers. If name service is not installed, users enter the ID number to
specify server nodes.

1.3.6 Application software

When planning your network configuration and the resource map for each
requester node, consider your application software. For example, the central
server configuration shown in Figure 1-6 is well suited to an installation
where users share a common application, data base, or printer. This
configuration also connotes that users have little to do with each other, as

far as sharing resources. Instead, each uses the central server.

Because attaching the network, logging on servers, and using apparently non-existent devices are new concepts that are potentially confusing to users, you might want to create SUBMIT files to configure the resource map, and load different applications. For example, a SUBMIT file could be created for each application that contains a NETON command, all of the required LOGON commands (one for each server is required), perhaps NET or LOCAL commands, or both if changes to the resource map are necessary, and finally the command to load the application. The "User's Guide" contains some examples of SUBMIT routines.

Keep in mind a few other things regarding your software and its impact on the network. Some multiprocess applications may have different processes resident on different nodes, and use networked queues to communicate with one another. The Print Spooler System is an example of an application that uses queues for this purpose. When this is the case, the queues used should be mapped in the default resource map, or users should be provided with a SUBMIT file to perform the mapping before the program is run.

One last note about your application software: DR Net allows a requester to load an application over the network. That is, the program file need not be on a local drive. This can result in savings in overall storage, and in better control of changes and upgradings of the application. Before implementing this option, refer to any licenses pertaining to the program in question, to make sure that you are not violating your contract by running the same copy of the software on several different computers.

EOF

DNSMG2.WS4   (= "DR Net System Manager's Guide", section 2)

DR Net
System Manager's Guide

First Edition: April 1984

(Retyped by Emmanuel ROCHE.)

Section 2: Network installation

Network installation can be classified into four distinct phases:

   1. Configure and connect the hardware. This includes installation of the
      CP/M-86 or Concurrent CP/M operating systems for the computer.

   2. Generate the DR Net network operating system for each node, and
      incorporate it with the local operating system. This implements the
      physical network topology on an operating system level.

   3. Perform a simple system testing, using the default resource map to
      confirm that each requester is connected to the intended servers. Use
      the standard DR Net utilities at this time to alter the resource map,
      and test non-default connections.

   4. Install the DR Net name server.

This section explains as much as possible the procedures required in each
step. We qualify the descriptions, because it is beyond the scope of this
manual to address every possible network configuration, network controller,
and DR Net implementation. For example, it is certainly feasible, and in many
cases likely, for an OEM to provide a preconfigured computer with the
operating system and network controller installed. Before proceeding, be sure
to review any and all documentation provided by your OEM to determine what
installation tasks have been performed by the OEM, and which are your
responsibility.

2.1 Network hardware installation

Refer to the instructions provided by your system implementer to install the
network controller, and to connect the computer to the network. This section
is provided only as a summary of the system requirements for each DR Net node
type.

2.1.1 Hardware requirements

DR Net allows up to 255 computers to be networked. All computers must have, at
least, one disk drive. This is necessary to store the resident operating
system and, in CP/M-86 requesters only, to store the DR Net system image file.
All requester nodes must have a console, but this is optional for server-only
nodes.

If the network controller has not been installed, do so at this time. Again,
refer to the OEM's instructions to install the components. Once the controller
has been installed, connect the computer to the network.

2.1.2 Software requirements

The host operating system is assumed to have been successfully installed. DR
Net requires no special memory configuration of the host operating system.
However, some DR Net implementations for systems based on Concurrent CP/M may
require that you specify more flags than the default number selected by the
GENCCPM.CMD program. A safe strategy is to run GENCCPM with your standard
responses, except when the program prompt asks for the number of flags. For
this value, add one to the total number of requester and shadow processes that
will run on this machine to your standard response.

2.2 DR Net system generation

Important: A DR Net option allows an OEM to write a self-initialization
routine that can set any of the parameters described below. When you use this
option, some of your responses to the system generation program prompts may be
irrelevant, as the initialization routine overrides then when DR Net is
loaded. Determine beforehand from the documentation rpvided by your OEM which
prompts are significant.

The DR Net network operating system is assembled from several files by a
system generation program. Tables 2-1 and 2-2 list the DR Net files required
for nodes based on Concurrent CP/M or CP/M-86, respectively.

Table 2-1. DR Net files for nodes based on Concurrent CP/M

Format: File name
     Description

R.CMD
A generalized, compact model, loader program.

GENNET.CMD
The loader program invoked to run CPGENNET.CMD.

CPGENNET.CMD
The primary system generation program for computers based on Concurrent CP/M.
CPGENNET displays a series of prompts, and combines the values input with the
DR Net invariant file and customized NIOS.CMD to produce a DRNET.CMD system
image file.

ADDNET.CMD
The loader program invoked by the user to run CPADDNET.CMD.

CPADDNET.CMD
The secondary system generation program for computers based on Concurrent
CP/M. CPADDNET combines the DRNET.CMD file with the computer's Concurrent CP/M
system image file to create a CCPM.SYS with DR Net installed.

CCPM.SYS
The Concurrent CP/M system image for your computer.

NIOS.CMD
The custom interface for your system and network controller provided by your
OEM.

RNET.CMD
The DR Net invariant file from which a Concurrent CP/M requester-only node is
created.

SNET.CMD
The DR Net invariant file from which a Concurrent CP/M server-only node is
created.

RSNET.CMD
The DR Net source file from which a Concurrent CP/M simultaneous
requester/server is created.

Table 2. DR Net files for nodes based on CP/M-86

Format: File name
        Description

R.CMD
A generalized compact model loader.

GENRQR.CMD
The loader program invoked to run CPGENRQR.CMD.

CPGENRQR.CMD
The sole DR Net system generation program for nodes based on CP/M-86. CPGENRQR
displays a series of prompts, and incorporates the responses with the
invariant RNET.CMD file and the customized NIOS.CMD to produce a DRNET.CMD
file.

RNET.CMD
This is the DR Net invariant file from which a CP/M-86 requester is created.

NIOS.CMD
The custom interface for your system and network controller provided by your
OEM.

Important: Although it has the same name, the RNET.CMD source file used to make a Concurrent CP/M requester is not the same as the RNET.CMD source file used to make a CP/M-86 requester. The two are not interchangeable. Take precautions to ensure that they do not get mixed up. Similarly, the DRNET.CMD file created by GENNET and GENRQR programs are different, and must not be confused. The same precaution may or may not be true for your NIOS.CMD file. In some cases, the same NIOS can be used for computer based on CP/M-86 or Concurrent CP/M.

DR Net system generation and installation is a two step procedure for Concurrent CP/M systems:

    1. Invoke GENNET, and answer the CPGENNET prompts.
    2. Invoke ADDNET.

The first step takes your responses to the CPGENNET prompts to build the DRNET.CMD from the NIOS.CMD and RNET.CMD, SNET.CMD, or RSNET.CMD files. The second step, running ADDNET, merges the DRNET.CMD file with your Concurrent CP/M system image. This leaves the file CCPM.SYS on the disk, which contains the Concurrent CP/M and DR Net system images.

For a node based on CP/M-86, DR Net is not installed with the host operating system. Instead, the values entered in response to the CPGENRQR prompts are used to build the DRNET.CMD file. This file is then loaded by the NETLDR utility.

Figures 2-1 and 2-2 below list the complete set of CPGENNET and CPGENRQR prompts, respectively. Each prompt is explained following the figures. Use these descriptions and all information provided by your system implementer to determine your answers before invoking GENNET or GENRQR. We also strongly recommend completing a Configuration Form (see Appendix B) for each network node before running either system generation utility.

When you have accumulated your answers to the prompts, and filled out the Configuration Forms, you are ready to run the program. Each is invoked by entering GENNET or GENRQR; there are no command line options to either program. Both GENNET and GENRQR can be run under either Concurrent CP/M or CP/M-86, and automatically chain R.CMD and CPGENNET or CPGENRQR.

Note: The square bracketed ("[" and "]") numbers shown on the left side of Figures 2-1 and 2-2 are not displayed. They are included for reference purposes only. In Figure 2-2, several prompts appear to be missing. This is because the prompts displayed by CPGENRQR are a subset of the CPGENNET prompts. The descriptions provided apply to both programs. Also note that these programs interpret all numeric input as hexadecimal values.

    Please answer the following questions. All numbers are in
    hexadecimal unless preceded by a pound (#) sign. Defaults
    are in parentheses.

[1]   What is this machine's physical node ID?   :
[2]   How many shadow processes can run on this machine?   (10):
[3]   How many processes can run as network requesters?   (0C):

[4]   How many copies of the Requester Configuration Table?   (08):
[5]   How many input Line Driver Control Blocks (LDCBs)?   (01):
[6]   How many output Line Driver Control Blocks (LDCBs)?   (01):
[7]   What is the first flag available for use by DR Net?   (20):
[8]   What is the maximum message buffer size?   (10B):
[9]   What is the length of any end-to-end message header?   (00):
[10]   What is the length of any end-to-end message trailer?   (00):
[11]   How big should the message buffer pool be?   (2000):
[12]   How many seconds until a transaction timeout?   (06):
[13]   Network server password (8 characters limit)   (PASSWORD):
[14]   What server should be your default server?   (00):

[15]   Note: Flags nn through nn must be used only by the network.

[16]   Is all of the information above correct?   (Y/N):

[17]   What disks do you want mapped across the network initially?
        (Use a carriage return when you are through mapping.)

        Local Disk Drive (A: through P:)?   :
[18]   Remote Disk Drive (A: through P:)?   :
[19]   Server node ID of the remote disk drive?   :

[20]   List all drives you want protected from network access
        (Use a carriage return when you are through mapping.)
        List a private drive   :

[21]   What printers do you want mapped across the network initially?
        (Use a carriage return when you are through mapping.)

        Local Printer Number (0 through F)?   :
[22]   Remote Printer Number (0 through F)?   :
[23]   Server node ID of remote printer?   :

[24]   What queues do you want mapped across the network?
        (Use a carriage return when you are through mapping.)

        Local Queue Name (8 characters or less)?   :
[25]   Remote Queue Name (8 characters or less)?   :
[26]   Server node ID of the remote queue?   :

[27]   Are all of the mappings above correct?   (Y/N):

        Building DRNET.CMD ...
        Network System Generation Complete

        Figure 2-1. CPGENNET prompts

        Please answer the following questions. All numbers are in
        hexadecimal unless preceded by a pound (#) sign. Defaults
        are in parentheses.

[1]   What is this machine's physical node ID?   :

[5]   How many input Line Driver Control Blocks (LDCBs)?   (01):
[6]   How many output Line Driver Control Blocks (LDCBs)?   (01):
[8]   What is the maximum message buffer size?   (10B):
[9]   What is the length of any end-to-end message header?   (00):
[10]   What is the length of any end-to-end message trailer?   (00):
[11]   How big should the message buffer pool be?   (2000):
[13]   Network server password (8 characters limit)   (PASSWORD):
[14]   What server should be your default server?   (00):

[16]   Is all of the information above correct?   (Y/N):

[17]   What disks do you want mapped across the network initially?
        (Use a carriage return when you are through mapping.)

        Local Disk Drive (A: through P:)?   :
[18]   Remote Disk Drive (A: through P:)?   :
[19]   Server node ID of the remote disk drive?   :

[21]   What printers do you want mapped across the network initially?
        (Use a carriage return when you are through mapping.)

        Local Printer Number (0 through F)?   :
[22]   Remote Printer Number (0 through F)?   :
[23]   Server node ID of remote printer?   :

[24]   What queues do you want mapped across the network?
        (Use a carriage return when you are through mapping.)

        Local Queue Name (8 characters or less)?   :
[25]   Remote Queue Name (8 characters or less)?   :
[26]   Server node ID of the remote queue?   :

[27]   Are all of the mappings above correct?   (Y/N):

        Building DRNET.CMD ...
        Network System Generation Complete

        Figure 2-2. CPGENRQR prompts

The CPGENNET and CPGENRQR prompts can be classified under three general
headings.

   1) Network Parameters
      The responses to these prompts depend on your system implementer's DR
      Net   design. The values entered must agree with the   internal
      characteristics of DR Net's interface with the network controller.
      Many of these responses are the same for each node on the network.

   2) Node-dependent Parameters
      Your responses to these prompts set values that are unique to the
      node, and identify its relationship to the network.

   3) Resource Map Values

Your responses to these prompts set the node's default resource map of disk drives, list devices, and queues.

The prompt descriptions below are organized according to these general headings. Table 2-3 lists the prompt numbers for your reference.

Table 2-3. CPGENNET and CPGENRQR prompts listed by class

Network Parameters	Node-dependent Parameters	Resource Map Values
4 though 12	1	17 through 27
	2	
	3	
	13	
	14	

Note: Appendix A describes the error messages that can display during DR Net system generation.

2.2.1 Network parameters

Table 2-4 lists the network parameter prompts with the default values. The default values are intended only as guidelines. There are no descriptions for the prompts themselves. However, should your system implementer have provided you with the appropriate responses, we recommend writing them in at this time. All values shown below are hexadecimal, and all numeric values entered are interpreted as hexadecimal by CPGENNET and CPGENRQR.

Do not be alarmed if you have not been provided with responses to these prompts. Your OEM has the option to install a routine in DR Net that sets these values when the network operating system is loaded.

Table 2-4. Network parameters and their default values

Network parameter prompt	Default
How many copies of the Requester Configuration Table?	(08)
How many input Line Driver Control Blocks (LDCBs)?	(01)
How many output Line Driver Control Blocks (LDCBs)?	(01)
What is the first flag available for use by DR Net?	(20)
What is the maximum message buffer size?	(10B)
What is the length of any end-to-end message header?	(00)
What is the length of any end-to-end message trailer?	(00)
How big should the message buffer pool be?	(2000)
How many seconds until a transaction timeout?	(06)

2.2 Node-dependent parameters

This subsection lists and describes each node-dependent prompt. Default values

provided by CPGENNET or CPGENRQR appear in parenthesis ("(" and ")") at the
end of the prompt.

Table 2-5. Node-dependent parameter prompts

Format: Prompt
    Explanation

[1]   What is this machine's physical node ID?
Enter the node's unique hex ID number in response to this prompt. Any value
from 00 through FE is valid. Nodes need not be numbered sequentially. No two
nodes should have the same number.

[2]   How many shadow processes can run on this machine? (10)
This prompt determines whether or not the node functions as a server on the
network. Notice that the question does not ask how many requesters can be
using this node at one time. Rather, it asks for the number of shadow
processes for which it should reserve internal space. The difference is
important, because one requester can have multiple concurrent processes logged
on to the same server at the same time.

The default allows up to 16 separate requester processes to be logged on to
this server simultaneously. When this maximum is reached, that server cannot
support another requester until a logged on requester logs off.

[3]   How many processes can run as network requesters? (0C)
This prompt determines whether or not the node functions as a requester on the
network. Notice that this question has nothing to do with the number of
servers this node can talk to at any one time. Instead, the number specifies
how many local processes can be attached to the network at any one time.

Each application that uses a remote disk or printer is a requester process.
The default value allows 12 separate requester processes to be logged on to as
many as 16 different servers each. This is enough processes for SUBMIT
routines to be running concurrently on four virtual consoles.

[13]   Network server password (8 characters limit) (PASSWORD)
In a requester node, the value entered in response to this prompt is used by
the LOGON utility when no password is entered by the operator. In a server
node, this value is compared against the password in a requester's log on
message before access is permitted. In a requester/server, this value serves
both purposes. Upper- or lowercase letters can be used when entering the
password, however, all characters are translated to uppercase by the program.

[14]   What server should be your default server? (00)
This hex value indicates a requester node's default server. (It has no meaning
in server-only nodes.) The default server has significance in two areas.
First, the default server is where the NAMSVR.DAT file is stored. Second, this
is the node assumed by DR Net should the user omit a server ID number from a
command line. For user convenience, the default server should be the server
used most frequently.

Unless you enter another number, the node with ID number 00 is selected as the
default server.

[15]   Note: Flags nn through nn must be used only by the network.
This statement indicates the range of flags reserved for exclusive use by DR
Net, where "nn" represents the actual flag numbers. This is not a prompt.
Unless you know how many flags, and which ones are required by your Concurrent
CP/M, this statement is meaningless. However, if this information is available
to you, confirm that none of the flags used by DR Net are used by Concurrent
CP/M. If collisions are apparent, contact your OEM.

[16]   Is all of the information above correct? (Y/N)
A "N" response returns you to the first prompt. All previous entries are
ignored. Only a "Y" response allows you to proceed. Note that upper- and
lowercase "N" and "Y" are accepted.

2.2.3 Default resource map values

In a requester node, your entries in response to the following prompts set the
node's default resource map. In a server only node, all prompts are irrelevant
(any entries are ignored), except for number 20 below.

Up to 16 entries can be made for each resouce. For each entry, three prompts
are displayed to elicit the local resource, the remote resource, and the
server number. After the response to the last prompt in the series has been
answered, you are returned to the first prompt in the series. To exit each
cycle, enter a carriage return in response to the first prompt.

The lone exception to this pattern is prompt 20. When you specify a private
drive, the same prompt is displayed again. Enter a carriage return to exit
this prompt too.

Table 2-6. Default resource map prompts

Format: Prompt
      Explanation

[17]   What disks do you want mapped across the network initially?
      (Use a carriage return when you are through mapping.)

      Local Disk Drive (A: through P:)?

Enter the logical name of a local drive to which you wish to refer to when
accessing a networked disk drive. This could be a local drive name for which
you have a physical drive (drive B for example), or a virtual drive. In either
case, all references to that drive will be trapped and sent to the drive
specified in the next two prompts.

[18]   Remote Disk Drive (A: through P:)?
Enter the logical name of the disk drive that you want to replace the local
drive specified in the previous prompt.

[19]   Server node ID of the remote disk drive?
Enter the node ID number of the server with the replacement drive. Node names

cannot be used; only the ID numbers are valid.

[20]   List all drives you want protected from network access
       (Use a carriage return when you are through mapping.)
       List a private drive (A: through P:)

Drive names entered in response to this prompt are protected from access by
requesters. After each entry, the prompt is redisplayed asking for another.
Attempts by a requesters to access a drive marked as private return a file
system select error.

[21]   What printers do you want mapped across the network initially?
       (Use a carriage return when you are through mapping.)

       Local Printer Number (0 through F)?

Local printers, like drives, are mapped individually to a specific, remote
list device. In response to this prompt, enter the physical list device number
of the local printer you wish to refer to when accessing the networked
printer. Any hexadecimal value from 0 through F is valid.

[22]   Remote Printer Number (0 through F)?

Enter the physical list device number of the replacement printer. Any
hexadecimal value from 0 through F is valid.

[23]   Server node ID of remote printer?
Enter the node ID number of the server to which the replacement printer is
attached.

[24]   What queues do you want mapped across the network?
       (Use a carriage return when you are through mapping.)

       Local Queue Name (8 characters or less)?

A local queue can also be mapped to a remote queue. In response to this
prompt, enter the name of the local queue you wish to refer to when accessing
the remote queue. Be sure to use the proper case for each letter, and observe
the 8 characters limit. (Queues are upper- and lowercase sensitive. For
example, DR Net will not recognize local queue MXSPL if it is entered as
mxspl.)

[25]   Remote Queue Name (8 characters or less)?
Enter the name of the replacement queue, being careful to match the case of
each character. The name need not be the same as the local queue name entered
above. Again, there is an 8 character limit, and ou must match the case of
each letter.

[26]   Server node ID of the remote queue?
Enter the hex ID number of the server node where the replacement queue is
located.

[27]   Are all of the mappings above correct? (Y/N)
The last prompt allows you to reconsider your entries. A "N" response returns

you to the first drive mapping prompt. Otherwise, a "Y" response proceeds with
the building of the DRNET.CMD file. This prompt accepts either upper- or
lowercase responses.

CPGENNET and CPGENRQR construct the DR Net DRNET.CMD system image file after
the last prompt. After the DR Net system image for a node based on CP/M-86 is
generated, you are done. The DRNET.CMD file created can be transferred to your
network boot disk. (Be sure to provide the NETLDR utility on the diskette as
well.)

DR Net system generation is not complete at this point for Concurrent CP/M-
based nodes. ADDNET program must be invoked to complete system generation.

2.2.4 ADDNET

ADDNET is run after GENNET to merge the newly created DRNET.CMD file with your
Concurrent CP/M system image file. Like GENNET, ADDNET automatically chains to
R.CMD and CPADDNET. When ADDNET is complete, the CCPM.SYS file recorded on the
disk has DR Net installed.

ADDNET has a single command line option that specifies the name of the source
file of your Concurrent CP/M system image.

If you enter

        A>ADDNET

the program assumes that your Concurrent CP/M system image is in the standard
CCPM.SYS file. In the process of creating a new CCPM.SYS, the source file is
consumed and disappears. There is no way to recover your original CCPM.SYS
file when this ADDNET option is selected.

If you enter

        A>ADDNET filename.typ

the program reads the Concurrent CP/M system image from the file specified.
This option is useful to preserve your original Concurrent CP/M system image.
Before using this ADDNET in this form, PIP a duplicate of your CCPM.SYS to a
different file name. Use this new file in the ADDNET command line.

Both forms of ADDNET automatically chains to R.CMD and CPADDNET.CMD. While the
new system image is being created, the following messages are displayed:

        Reading in system image
        Reading in network system image
        Writing completed system to CCPM.SYS

        Addition of network to system image is complete

Note that systems based on Concurrent CP/M do not need to have the DRNET.CMD
file present on the system disk. CPADDNET integrates the DR Net system image

directly with the Concurrent CP/M system image. Appendix A lists and discuss
ADDNET error messages.

2.3 Configuration testing

After DR Net and the network communication lines have been installed, a series
of tests should be performed with the DR Net utilities to confirma that your
CPGENNET and CPGENRQR entries were correct. The utilities used in this test
are not special programs written specifically for test purposes; these are the
same programs an operator uses in day to day operation of the computer. This
test procedure is not intended to replace any others. If others were provided
with your system, the following procedure should be the last test performed.

Before starting with the test, load the operating system on each node, and
have your Configuration Forms for the nodes handy. We assume that your current
disk has the DR Net utilities listed in Table 2-7 on it. Other utilities used
below are any utility that displays a drive directory (DIR, SDIR, or DIRS),
PRINTER, and PIP. It would also prove useful to have a short file available to
print on remote servers.

Table 2-7. DR Net user utilities

Format: File name
      Description

NETLDR.CMD
Loads DRNET.CMD file, and hence the DR Net system image, for a node based on
CP/M-86. This file is not needed for Concurrent CP/M computers.

NETON.CMD
Attaches DR Net in a node based on Concurrent CP/M. This file is not needed
for CP/M-86 computers.

NETOFF.CMD
Detaches DR Net in a node based on Concurrent CP/M. This file is not needed
for CP/M-86 computers.

LOGON.CMD
Logs on a server.

LOGOFF.CMD
Logs off a server.

NETSTAT.CMD
Displays the network status.

NET.CMD
Maps a local resource to a server.

LOCAL.CMD
Unmaps a local resource.

For test purposes only, you should create a file on the destination drives in
each server that reveals immediately from a directory listing which server you
have accessed. For example, the file SERV00, SERV01, and SERVPR could be used
to indicate the default server (00::), server node 01::, and the print server,
respectively.

Repeat the following sequence of commands at each requester node. All commands
or command forms shown below are terminated by a carriage return.

  1. For Concurrent CP/M requesters, enter

        A>NETON

     to attach the console to the network. For CP/M-86 requesters, enter

        A>NETLDR

     to load DR Net and attach the network.

  2. Enter

        A>NETSTAT

     to display the node's default resource map. Confirm that the node
     number in the display is correct for that node, and that your
     configuration of local to remote resources is correct. If anything is
     wrong, the DR Net system generation utility must be run again to make
     corrections.

  3. Enter a LOGON command for each server listed in the NETSTAT display's
     "Node" column. For the default server, use the command form

        LOGON ;password

     where "password" is the 8 character or less actual password required
     by the default server. For all other servers, you must specify the
     node explicitly. Until you have installed the name service, the only
     LOGON command form supported is

        LOGON nn::;password

     where "nn" is the server node's ID number, and "password" is the 8
     character or less actual password required by that node.

  4. Display the directory for each local drive listed by NETSTAT. Notice
     that the drive label shown in the display indicates the local drive
     name, rather than the remote name. Confirm that this is the intended
     remote drive.

  5. If you have one or more remote printers, use the command form

        PIP LST:=filename

to print your test file. Use the PRINTER utility to change the current
list printer, if necessary, and repeat this test for each remote
printer. Confirm that the listing was made by the intended printer.

This concludes the configuration test. However, if your application requires
that the user make changes to the default resource map, confirm that these
connections are in place as well. To map a local disk drive or printer to a
server, you can use the NET command in the form

        NET <local resource> = <remote resource><server>

where "local resource" is the requester's drive name, list device, or queue
name; "remote resource" is the remote drive name, list device number, or queue
name, and "server" is the remote node ID number.

To remove the map of a local device, use the LOCAL command in the form

        LOCAL <local resource>

where "local resource" is the requester's drive name, list device number, r
queue name.

Note that there is no way to confirm queue mappings with the DR Net utilties.
The only way to test the remote access to queues is with the application for
which they were installed.

2.4 Installing name service

DR Net's name service allows nodes to be referenced by name, rather than ID
number. It is also provided so that a directory of servers and requesters can
be maintained. The use of node names is significant to the LOGON, LOGOFF, NET,
NETSTAT, and NAMES utilities only. All of these programs reference the node's
NAMSVR.DAT file when a node name rather than a number is found in the command
line, when network status is retrieved, or when the name server directory is
requested.

There are four things to keep in mind about name service when designing your
facility.

   - You can have as many NAMSVR.DAT files as you want. However, each
     requester only looks to its default server's system drive to find this
     file. Consequently, requesters sharing the same default server must
     also share the same NAMSVR.DAT file.

   - The contents of the NAMSVR.DAT are completely up to you. DR Net does
     not care about your name and ID number assignments, or crosscheck your
     entries to confirm that they are accurate.

   - You need not list all servers and requesters in NAMSVR.DAT. This means
     that you can hide servers and other requesters from a requesters by
     not listing them in NAMSVR.DAT.

- The names in one NAMSVR.DAT file need not be the same as the names in
     another NAMSVR.DAT file.

Two utilities are pertinent to the name serveice installation and use:

   - NAMESMOD.CMD is used to create and modify the NAMSVR.DAT file.
   - NAMES.CMD displays the contents of the NAMSVR.DAT file.

2.4.1 NAMESMOD description

Before you run NAMESMOD, the node you are working at must be attached to the
network, and you must log on the server for with the NAMSVR.DAT file is to be
created. To invoke the utility, enter the command

     A>NAMESMOD

NAMESMOD has no command line options. Figure 2-3 illustrates the different
prompts displayed by this utility. There is nothing special about the sequence
of commands shown. However, you must invoke the SET option to create the
NAMSVR.DAT file before ADD can be used to make entries.

Note: NAMESMOD is the only utility that can be used to create the NAMSVR.DAT
file. Never use a word processor or edito to create or make changes to
NAMSVR.DAT. In addition, NAMSVR.DAT must always have the SYS and RW file
attributes. We recommend backing up NAMSVR.DAT after it has been created.

The square bracketed ("[" and "]") numbers in the leftmost column of Figure 2-
3 are for reference purposes only. They do not appear when NAMESMOD is run. In
addition, the term "User" refers to a requester node. Finally, user entries
are shown in UPPERCASE and boldface.

     A>NAMESMOD
[1]   On what node is the name server you wish to modify?
       Modifying the name server on node nn::

[2]   Enter Option: ADD, DELete, DISplay or SETup > SET
[3]   Password protection for update privileges? Y/N Y
[4]   Enter Password>
       Name server file 'NAMSVR.DAT' has been created

[5]   Enter Option: ADD, DELete, DISplay or SETup > ADD

[6]   ADD: Name   > SERVER
[7]   Node ID   > 99
[8]   Type (User/Server) > S
[9]   Really add the entry (Y/N) > Y
       Entry added to name server

[10]   Enter Option: ADD, DELete, DISplay, or SETup > DEL

[11]   DELETE: Name   > JOE
[12]   Type (User/Server) > U

[13]   Really delete the entry (Y/N) > Y
        Entry deleted from name server

[14]   Enter Option: ADD, DELete, DISplay, or SETup >

        Figure 2-3. NAMESMOD setup, add, and detele dialogues

Table 2-8 contains the descriptions for the prompts in Fugure 2-3. The numbers
in the table correspond to the square bracketed ("[" and "]") numbers in the
figure. All responses shown in the figure and the table are fictitious. In
addition, all entries can be made in either upper- or lowercase. However, all
entries are translated to uppercase by NAMESMOD. When you run NAMESMOD,
terminate each response with a carriage return.

Table 2-8. NAMESMOD prompt descriptions

Format: Number and prompt
        Description

[1]   On what node is the name server you wish to modify?
        Modifying the name server on node nn::

The first NAMESMOD prompt asks for the node ID number of the server whose
NAMSVR.DAT file you are going to create or modify. Entering a carriage return
selects your node's default server. However, any other logged on server can be
selected by entering the node's ID number. A leading 0 and the trailing double
colons ("::") need not be entered to specify a server. Regardless of the
server node selected, the NAMSVR.DAT file is written, or assumed to be present
on that computer's system drive, user area 0.

[2]   Enter Option: ADD, DELete, DISplay or SETup > SET

This is the NAMESMOD option prompt. Each option is selected by entering the
three initial letters of each option. To create a NAMSVR.DAT file, enter SET.

[3]   Password protection for update privileges? Y/N > Y

This option is only available if you have enabled directory labels on the
server's system drive. If so, you can specify a password to prevent
unauthorized access to NAMSVR.DAT. Access is only protected for write purposes
only. Answer with a "Y" and the next prompt is displayed. Enter an "N" and
NAMESMOD creates NAMSVR.DAT without password protection, displays the comment

        Name server file 'NAMSVR.DAT' has been created

and returns the NAMESMOD option prompt.

[4]   Enter Password>

NAMESMOD displays this prompt only if you have answered "Y" to the previous
prompt. The password entered is recorded and used in the same manner as if you
had used the Concurrent CP/M SET command to password protect NAMSVR.DAT. See
the "Concurrent CP/M User's Guide" for an explanation of the SET command. The

password entered can be 8 characters or less. All entries are translated into uppercase. After the password has been entered, NAMESMOD displays the following comment:

     Name server file 'NAMSVR.DAT' has been created

This, in turn, is followed by the NAMESMOD option prompt.

Note: If the Concurrent CP/M INITDIR utility has not been run to extend the directory space on the current server's disk, the password entered here is ignored. To re-iterate, you must have enabled directory labels to password protection with NAMSVR.DAT.

[5]   Enter Option: ADD, DELete, DISplay or SETup > ADD

Until ADD is invoked, a new NAMSVR.DAT file is blank. There are no default name assingments. Select the ADD option to make your original assignments, and subsequently to incorporate name assignments in NAMSVR.DAT for new network nodes.

[6]   ADD: Name   > SERVER

This is the first of the four sequential prompts required to make a single NAMSVR.DAT entry. Enter the unique name of the node. The name can be 8 characters or less, and consist of any combination of letters, numbers, and special characters. However, the name cannot be the same as another node's in the same NAMSVR.DAT file. All lowercase characters entered are translated to uppercase.

After you have cycled through the sequence of four prompts, NAMESMOD returns to this prompt. You can make another entry at this point, or exit the ADD option by entering a carriage return.

[7]   Node ID   > 99

Enter the hexadecimal ID number of the node. Note that you can have more than one name referring to the same node number.

[8]   Type (User/Server) > S

Node names are recorded and displayed according to their network function -- server or user (requester). Enter an "S" or a "U" to classify this entry. Note that a combination requester and server node must be ADDed twice, to register it in the two categories.

[9]   Really add the entry (Y/N) > Y
        Entry added to name server

NAMESMOD gives you a chance to reconsider your entries. If you enter "Y", the name-to-number assignment is recorded in NAMSVR.DAT, and the comment shown above is displayed. If you enter "N", the assignment is not recorded, and the following comment is displayed:

     Entry no added to name server

Whether you enter a "Y" or a "N", NAMESMOD returns you to the initial ADD
prompt.

[10]   Enter Option: ADD, DELete, DISplay, or SETup > DEL

To delete an entry from the NAMSVR.DAT file, enter DEL from the NAMESMOD
command prompt. This initiates a sequence of three prompts.

[11]   DELETE: Name   > JOE

The first prompt in the delete sequence asks for the node name. The name can
be entered in upper- or lowercase.

After the entire sequence has been completed, NAMESMOD returns you to this
prompt. Enter a carriage return to exit, or another node name to continue.

[12]   Type (User/Server) > U

Enter the network function type of the entry to be deleted. DEL only removes
the listing for the function specified. For example, if you have a node
classified in both server and user categories, and enter "U", NAMESMOD only
erases the entry from the user category.

[13]   Really delete the entry (Y/N) > Y
        Entry deleted from name server

Before NAMESMOD erases the entry, it asks for confirmation. If you enter "Y",
the name-to-number assignment is erased, and the comment shown above is
displayed. If you enter "N", the assignment remains intact, and the following
comment is shown.

        Entry not deleted from name server

In both cases, you are returned to the first prompt in the series.

[14]   Enter Option: ADD, DELete, DISplay, or SETup >

Exit NAMESMOD any time the option prompt is displayed by entering a carriage
return. To view your current entries, enter "DIS". The resulting display is
the same as that provided by the NAMES.CMD utility.

2.4.2 NAMESMOD error messages

Table 2-7 lists the error messages you can encounter running NAMESMOD, and
explains their meaning.

Table 2-9. NAMESMOD error messages

Format: Message
        Meaning

Unable to find 'NAMSVR.DAT' on the node.
NAMESMOD did not find a NAMSVR.DAT file on the system drive of the node you
specified in response to the first program prompt. Invoke NAMESMOD again, and
use the SET option to create NAMSVR.DAT on that node.

Cannot make sense out of that option
NAMESMOD did not recognize the three characters you entered in response to the
option prompt.

Cannot make sense out of that node designation
NAMESMOD did not recognize the node number you specified. Node IDs are limited
to the hexadecimal values 00 through FE.

You must first logon to that server
The server node number you specified in response to the first NAMESMOD prompt
is not logged on. Before invoking NAMESMOD again, use the LOGON program to log
on that server.

A name service file already exists on the node
You invoked the SET option, but the file NAMSVR.DAT already exists on the
specified server's system drive.

An entry of that name and type already exists.
The name you entered from the ADD prompt already appears for that type in the
NAMSVR.DAT file. Although the same name can appear in both user and server
catagories, it cannot be used twice within a category.

Note: The restriction preventing duplicate node names does not apply to node
numbers. The ID number can appear twice within a type, as long as the names
are different.

Network error
A network error occurred while NAMESMOD was writing to, or reading from, the
NAMSVR.DAT file.

File system error
A file system error occurred while NAMESMOD was writing to, or reading from,
the NAMSVR.DAT file.

EOF

DNSMG3.WS4   (= "DR Net System Manager's Guide", section 3)

DR Net
System Manager's Guide

First Edition: April 1984

(Retyped by Emmanuel ROCHE.)

Section 3: Network maintenance

The ongoing network maintenance can be categorized in two ways. First, the
system manager must respond to failures of the network. Second, changes to the
network configuration are occasionally necessary.

Network failures are most likely results of equipment failure and operator
misunderstanding. However, there is the possibility that a change to a node's
DR Net system image file can solve a specific problem. DR Net's error
messages, though few, indicate the full range of network problems that can be
encountered. Section 3.1 below describes the error messages and what they
mean.

Configuration in the network context applies not only to the arrangement of
server and requesters, but to the configuration of application software and
data files as well. For example, a central server configuration connotes that
all operator's share a central resource such as a hard disk or large data
base. In this configuration, all operators could be sharing the same program
as well, invoking them from the central server.

Depending on the network configuration, making a change can have little
effect, or far reaching repercussions. Section 3.2 points out the implications
to DR Net when modifications to the configuration are made.

3.1 Trouble locating

This section assumes that you have debugged your network's configuration of
requesters and servers, and that the system has been successfully in use. When
this is true, failures can arise from the following three sources:

      - operator misunderstanding
      - operating system failures on the requester or server systems
      - failures of the network

3.1.1 Operator errors

The most common operator error is to neglect to attach or log on before using

the network. In addition, failure to comprehend the concepts of device mapping and virtual consoles can lead to misunderstandings. When the operator fails to invoke NETON or NETLDR before using one of the network utilities, the following message is displayed:

    You are not attached to the Network
    Please run NETON for a Concurrent CP/M requester
        or run NETLDR for a CP/M-86 requester

When an operator attempts to use a remote resource before the network is attached, a file system error results. For example, an attempt to PIP a file to a virtual drive, that does not exist until the operator attaches, results in the message

    ERROR: OPEN FILE INVALID DISK SELECT - d:

where "d:" is the virtual drive name. An attempt to PIP to a list device that is not available until the network is attached results in the message

    ERROR: INVALID DESTINATION

Should the operator attempts to get a directory of a non-existent drive, the error message is as follows:

    CP/M error on d: Invalid Drive
    BDOS Function = 17 File = ????????.???

All of these are standard CP/M operating system error messages completely independent of the DR Net network.

If the operator has run NETON or NETLDR, but failed to log on the intended server, the error messages are the same, unless the operator is referencing a mapped resource. For example, when an operator attempts to PIP a file to drive M when only drives B, C, and D are mapped, the error message would be

    ERROR: OPEN FILE INVALID DISK SELECT - M:

However, when the operator attempts to PIP to a drive that has a map entry, but that server is not logged on, a network error message is displayed. The same is true for local and mapped list devices.

The solution to all of these problems is to attach the network with NETON or NETLDR, and log on servers with LOGON.

3.1.2 Local and remote file system errors

File system errors are all errors related to the writing and reading of files. Examples of file system errors are a bad sector, a full directory, a misspelled file name, an invalid file reference, an attempt to write to a read/only disk, an invalid file password specification, and so forth.

When the network is attached, and servers are logged on, remote file system

errors are reported differently than local file system errors. The display format of a local file system error is as follows:

    CP/M error on d:, message
    BDOS Function = n File = filename.typ

The variables in this display are drive name "d:"; the error "message"; the BDOS function number "n"; and the file name "filename.typ".

When a file system error occurs on a server, DR Net returns an abbreviated error display message as follows.

    Network Error: message

The specific error "message" is the same as displayed by local errors. For a complete accounting of the errors, and their meaning, see the user's guide provided for the node's resident operating system.

Local and remote file system errors do not affect a requester's relationship with the server or the network. After the error has occurred, the network is still attached, and the server is still logged on.

Error recovery from remote file system errors is the same as for local file system errors. Refer to the user's guide for the offending node's operating system for error recovery suggestions and procedures.

3.1.3 DR Net errors

The DR Net network error messages appear as follows:

    Network Error: Server Not Logged On
    Network Error: Physical Transmission Error
    Network Error: Requester Error

The messages indicate failures of the server, requester, and the physical connection between a requester and a server, respectively. Note that these messages only cover network problems. A different set of messages are displayed when errors occur during the use of the DR Net utilities. These messages are described in the utility descriptions in the "User's Guide".

Table 3-1. DR Net error messages

Format: Message
    Description

Network Error: Server Not Logged On
This message means that the server designated in the most recent disk drive, list device, or queue reference was not logged on. The solution is to log on the server with the LOGON utility. This error does not change the node's network status. That is, the network remains attached, and all logged on servers remain logged on.

Network Error: Physical Transmission Error
This message means that the network connection between a requester and server
has broken down. Although this message is displayed when a requester attempts
to access a server that has crashed, it is far more likely to result from a
break down in the physical connection between the requester and the server.
The biggest problem when this occurs is to locate where the connection is
severed.

Note: Do not assume that the server has crashed when this message is
displayed. Accordingly, do not automatically reset the server to fix the
problem. If the server is not at fault, a reset terminates all shadow
processes for requesters that are still logged on.

When this message appears, perform the following checks to locate the problem:

   - Attempt to access another server from the requester. Failure to access
     other servers indicates that the problem is in the requester's
     interface to the network. Success in accessing other servers should
     tend to indicate that the problem is at the server.

   - Attempt to access the problem server from another requester. If this
     proves successful, the original requester is probably at fault. If
     this proves unsuccessful, try accessing other servers from the same
     requester. If other servers are accessible, it would implicate the
     server's network interface.

   - Use the server as a stand-alone computer or as a requester. If the
     problem server is also a requester, attach the network, and try to
     access another server. Otherwise, run any program from the server's
     console. If the program does not run, a server crash can be assumed.
     If the system can be used to run a program locally or over the
     network, you can eliminate server crash as a possibility.

Note: Although a system reset may provide an apparent cure when a server crash
is the problem, you should find the reason for the crash, to prevent future
occurrences. Also, note that the crash of a local program running on a server-
only node brings down the DR Net processes as well.

Network Error: Requester Error
A requester error only occurs when a program attempts to create a requester
process after the limit of requester processes has been reached. (Recall that
each requester node can support a maximum number of attached processes. This
value is set when the DR Net system image is generated.) No other attached
processes are affected when this error occurs.

The remedy for this error condition is to limit the number of concurrent
attached processes the operator can network at one time. If this proves a
burden, the system generation program can be run again to specify more
requester processes. Note that the amount of system memory can limit the
number of requester and server processes the node can support. If your OEM
specified a limit, consult with them to confirm that this limit can be safely
exceeded.

3.1.4 DR Net error response modes

There are three response modes that determine how the host operating system
and network operating system respond to errors. The response modes listed here
are not selected by the operator. They are options implemented by the software
developer from within the program. You should be aware of the modes, because
they determine your system's response to local and remote file system errors
and the three network errors.

   - Display and Abort
    The error message is output to the associated virtual console, the
    calling program is aborted, and the system prompt is returned to the
    screen.

   - Display and Return
    The error message is output to the associated virtual console, and the
    error code is returned to the program. When the software developer
    selects this option, the error recovery routine is included in the
    application program.

   - Return
    This option only returns the error code to the program. No message is
    output to the associated virtual console. When this option is
    implemented, the software developer has incorporated the error
    recovery routine into the program.

3.2 Configuration modifications

When you add a node, delete a node, or make changes to the apllication
programs available to users, it can have implications in the following areas:

   - Network configuration
    Before installing a new node, plan its default server, default
    password, location on the system, resource maps, and so forth. In many
    respects, this differs very little from the installation of a node
    when the network is first set up. When removing a node, consider the
    impact upon resource maps, default servers, passwords, and names
    service. A requester node typically has littel impact when it is
    removed. However, removing a server can have profound and extensive
    repercussions. For example, you must run the DR Net system generation
    program again for each requester affected when a default server is
    removed.

   - Names service
    The new or former node should be added or deleted from the NAMSVR.DAT
    file with the NAMESMOD utility. If a server is removed, determine if
    it is a requester's default server. If so, a new default server should
    be selected, so that names service can be restored.

   - Shadow processes

Adding a new node may require an increase in the number of shadow
processes available from any given server. For example, a new
requester node in which virtual consoles are used concurrently can
require the use of as many as two or three shadow processes per
console. This is especially true if SUBMIT routines are used on each
virtual console to load the applications.

- The NIOS
  In some networks, there may be a limit to the number of nodes that can
  be serviced. Before adding a node, confirm with your OEM that the
  network can accomodate the increase.

- Application software
  Consideration should be given to the applications that will be
  available on a new node. For example, to conserve disk space, it might
  be desirable to have a new requester access its default server to load
  all application programs, but use local resources for data storage.
  Alternatively, both program and data files can be accessed from the
  default or a secondary server. A change of software on a server
  affects every requester who uses that program.

- Records
  Be sure to update your records and configuration forms when changes
  are made.

EOF

DNSMG4.WS4   (= "DR Net System Manager's Guide", appendixes)

DR Net
System Manager's Guide

First Edition: April 1984

(Retyped by Emmanuel ROCHE.)

Appendixes

Appendix A: System generation error messages

This appendix lists and describes the error messages that can be displayed by
the GENNET, GENRQR, and ADDNET utilities. There are two general types of error
messages. The first type is characterized by the immediate display of the
message after the offending value has been entered. This class is further
distinguished in that the prompt is redisplayed immediately, to solicit the
entry of another value. All messages preceded by numbers below are errors of
this type. The number references the prompt number in Figure 2-1 and 2-2.

The other type of error message occurs after a series of related prompts, and
indicates a more profound configuration problem. When this occurs, GENNET and
GENRQR return you to the first prompt in the series, and require you to re-
enter each value. This second type of error is preceded by an asterisk ("*"),
rather than a number in the list below.

Table A-1. GENNET and GENRQR prompt-phase error messages

Format: Number and Message
     Explanation

Invalid number.
No specific prompt is associated with this error message. It is displayed
whenever an illegal number, such as 0FMh, is entered. This message is not
displayed, however, if a valid number is displayed that is out of the range
allowed for that parameter.

1. Please specify a node ID in the range 00 - FE.
The node ID number entered was FFh or greater. Re-enter the node number with a
value in the given range.

2. Can't have more than 83 shadow processes.
More than 53h shadow processes were requested. Re-enter the parameter with a
value less than or equal to 53h.

3. Can't have more than 90 requester processes.
More than 5Ah requester processes were specified. Re-enter the parameter with
a value less than or equal to 5Ah.

4. Can't have more than 149 local RCTs.
More than 95h copies of the requester Configuration Table were ordered. Re-enter the parameter with a value less than or equal to 95h.

5. Can't have more than 16 input line drivers.
More than 10h input Line Driver Control Blocks were specified. Re-enter the parameter with less than or equal to 10h.

6. Can't have more then 16 output line drivers.
More than 10h output Line Driver Control Blocks were specified. Re-enter the parameter with less than or equal to 10h.

* Parameters given need more than 64K of static storage.
The memory needs required to support the number of requester and shadow processes, or Requester Configuration Tables, and of input and output line drivers, exceed 64 KB. One or more of these values will have to be reduced. Consult your OEM for assistance if this message occurs repeatedly.

7. Flags must be in the range 00 - FF.
The first flag entered was out of the range shown. Re-enter the parameter, and specify a beginning flag number within the range.

* Too many flags are required to run this configuration.
To allocate a flag to each requester and shadow processe specified requires a flag number in excess of FF. To correct this situation, enter a lower beginning flag number, or specify fewer requester and/or shadow processes.

11. Can't have a buffer pool larger than 64K.
The message buffer pool specified was greater than 0FFFFh. Re-enter the parameter with a number equal to or below this value.

* Buffer pool isn't big enough to guarantee no deadlocks.
GENNET uses a minimum value formula to determine if the lessage buffer pool specified is large enough to prevent deadlocks. A deadlock is a situation where there are no message buffers available and a process is waiting to receive a message, so that it can deallocate a message buffer. After this prompt is displayed, you are returned to the first program prompt. The solution is to specify a larger message buffer pool.

14. Passwords should be 8 characters or less.
The password entered was in excess of 8 characters. Re-ebter the password, and observe the 8 character limit.

15. Node IDs must be in the range 00 -FE.
The hex node ID number specified was FF or greater. Re-enter the parameter with a value in the range shown.

16. Please type yes (Y) or no (N).
This prompt, and the last one, respond to an upper- or lowercase "Y" or "N" only. Any other response results in this error message.

17. Disk drives should be in the range A: through P:.
This error message can also result from an errant entry to prompts 18 and 20.

It indicates that the entry was outside the given range. Re-enter the value,
and be sure to use the logical drive name, rather than a number. Colons (":")
are not necessary.

21. List devices must be in the range 0 - F to be networked.
This message indicates that the entry was a number outside the range shown.
Re-enter the value with a number within the range.

24. Queue names should be 8 characters or less.
The queue name entered was in excess of 8 characters. Re-enter the name, and
observe the 8 character limit. This message can also result from prompt 25.

The following error messages only result after the message

        Building DRNET.CMD ...

is displayed. They indicate the nature of any problem encountered during
DRNET.CMD generation.

Table A-2. GENNET and GENRQR file system error messages

Format: Message
        Explanation

Can't open network or NIOS input file.
GENNET cannot find or open either the RNET.CMD, SNET.CMD, RSNET.CMD, or
NIOS.CMD file. Confirm that these files are on the current disk, and ensure
that there is nothing to prevent them from being opened.

Can't allocate space to build the output file.
GENNET has run out of memory. The utility will have to be run in a system with
a smaller operating system, or with more memory.

Can't create the DRNET.CMD output file.
There is something preventing the file DRNET.CMD from being written to the
disk. Corroborate that the drive is not set to read only, that the write
protect notch is covered, and that there is enough space in the directory and
the disk. (The length of DRNET.CMD can be projected by adding your NIOS.CMD to
the appropriate DR Net invariant file.)

Error reading one of the input files.
A file system error was encountered while reading RNET.CMD, SNET.CMD,
RSNET.CMD, or NIOS.CMD. Replace any files that have been corrupted.

Unexpected error writing the DRNET.CMD output file.
A file system error was encountered while writing the DRNET.CMD file. Verify
that the disk is formatted correctly, and that the disk is formatted
correctly, and that it has enough space and room in the directory.

Table A-3 shows the ADDNET error messages:

Table A-3. ADDNET error messages

Format: Message
　　　Explanation

ADDNET has already been run on this system file.
This indicates that the CCPM.SYS file provided to ADDNET was previously merged
with the DRNET.CMD.

Can't create output CCPM.SYS file.
This indicates that the destination disk, or the original CCPM.SYS, was set to
read only, or that there was no space left in the directory to create a new
CCPM.SYS file.

Can't open an input system file.
ADDnet could not open the CCPM.SYS file or the file specified in the ADDNET
command line. Confirm that the file is present on the current disk, and that
there are no restrictions preventing ADDNET from opening it.

Can't open the network input file DRNET.CMD.
ADDNET could not open or find the DRNET.CMD DR Net system image file. Confirm
that the DRNET.CMD file is present on the current disk, and that there is
nothing preventing ADDNET from opening it.

Encountered an error reading input file.
This indicates that an unrecoverable file system error occurred while reading
either the CCPM.SYS or DRNET.CMD file. Determine which file is corrupted, and
replace it.

Encountered an error writing CCPM.SYS.
This indicates a disk full condition, or a unrecoverable file system error
occurred. Confirm that there is more room on the disk than the total of your
CCPM.SYS and DRNET.CMD files.

Not enough memory to add the network to the system.
This message indicates that there is not enough memory for ADDNET to run and
merge the two system files. ADDNET requires a total of the following amounts
of memory to complete:

　　　- 31 KB of memory for the ADDNET program
　　　- memory to accomodate the entire CCPM.SYS file
　　　- memory to accomodate the entire DRNET.CMD file
　　　- 5 KB to 10 KB for overhead

Appendix B: Configuration forms

The DR Net configuration forms are provided to help you install and maintain a
network of computers. We recommend completing a form for each requester and
server node before running GENNET, and updating the forms as changes are made.
We also waive the copyright restrictions against copying these forms. You
should always keep one form of each type blank, so that copies can be made
after the initial set are made.

There are two configuration forms: one for the requester function, and one for the server function. Normally, a single form is sufficient for a requester or server node. Occasionally, a server may require two server forms when it services a lot of requesters. For requester/server nodes, both a requester and server form should be completed.

Complete the form for each node before performing DR Net system generation. This will help you to prevent erroneous entries, and assist you in projecting the node dependent variables for each computer.

After the network is installed, be sure to keep the forms up-to-date with any changes that have been made. As the system manager position is passed from one person to another, the record and history of the network can prove an invaluable tool to expedite the transition.

B.1 Requester form instructions

Figure B-1 is a sample requester form that has been filled in with fictitious values. The instructions that follow reference this figure.

                    REQUESTER

5A	HENRY	AA	OK	8
Node #	Node Name	Default Server #	Password	# Requester Processes

SYSTEM DESCRIPTION   Resident Operating System: Concurrent CP/M

Virtual Consoles	Applications	Local Drives	Local Printers	Local Queues	Other
4	1) GL.CMD	A	--	MXd	192 KB
	2) SC2.CMD	B			
	3) WS4.CMD (SUB)				

MAPPED RESOURCES

| | Drives | | | Printers | | | Queues | |
Local	Remote	Server	Local	Remote	Server	Local	Remote	Server
1) C	A	AA	0	0	AA	--	--	--
D	C	AA						
2) C	A	AA	0	0	AA	MXd	MXd	AA
D	C	AA						
3)*E	A	01	0	1	02	--	--	--
F	B	02						

* = Requires Net ro remap printer -- Handled by WS4.SUB

NETWORK PARAMETER VALUES

Copies Requester Configuration Table _4____
Input Line Driver Control Blocks _1____
Output Line Driver Control Blocks _1____
DR Net's first flag _60___; total flags _60___ - _67___
Maximum logical message buffer size _112__ (hex)
Length of end-to-end message header _4____
Length of end-to-end message trailer _3____
Size of message buffer pool _A00__ (hex)
Seconds to transaction time-out _6____

CONFIGURATION MAP

List of
Servers

AA___(default)
01___
02___
_____
_____


```
        Letter printer 02:: <-----------+------+
                            | 5A:: | GL (General Ledger)
        Word processor 01:: <-----------+------+ SC2 (Spreadsheet)
                                |
        Line printer <--+           |
                +----- AA:: <------+
        Hard disk <-----+
```
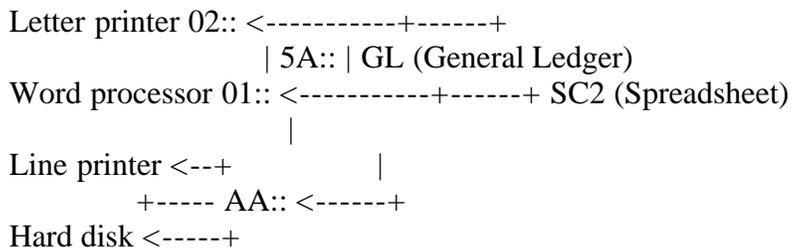
        Figure B-1. Sample requester form

1. Node dependent information

Fill in the general information, such as the node ID number, name, default
server number, and so forth along the top of the form. The last item in that
category, "# Requester Processes", should be filled in at this time if you
know it. (For example, if the installation instructions from your OEM say:
"Configure each node with nn requester processes", where "nn" is a specific
number.) If the number is not apparent, do not fill in this category until the
applications column is completed.

2. System description

Begin these entries by writing in the resident operating system. Next, fill in the columns with the system components and the applications for which the node will be used. In Figure B-1, the computer has two drives (A and B), 4 virtual consoles, and no local printers.

The "Applications" column lists the programs the user will be running. Notice that each application is numbered. This is for cross-reference to the mapped resources. Also, not that SUB is appended to the third item, to indicate that the program is invoked from a SUBMIT file.

Note: The number of applications gives you an approximation of the number of requester processes required. In this case, eight requester processes have been specified, because it is likely on this node that the general ledger, spreadsheet, and word processor programs will be run concurrently. Each requires two processes (remember: one process is always required for the console itself). WS4.CMD requires three, however, because it is invoked from SUBMIT, which requires a requester process of its own.

In the queue column, you should list those queues that are meagingful to you. For example, you can list all queues used by all software, or just those queues that are mapped over the network. In Figure B-1, the second option was selected.

The "Other" column is used to indicate how much random access memory (RAM) is in the computer. Other things that might deserve mention are a modem, a color monitor, and so forth.

3. Mapped resources

You can list the mapped resources in any fashion meaningful to your system. In Figure B-1, the mapping is done by application. The asterisk ("*") is applied to the third application because local printer 0 must be remapped to server 02:: from server AA::. As the footnote states, the change is made by invoking the SUBMIT utility with a reference to the file WS4.SUB.

4. Network parameter values

These values correspond to the Network Parameters described in Section 2.2.1. As mentioned in that section, you will have to get these values from your OEM. Those shown in Figure B-1 are fictitious, but appropriate given all other node characteristics.

5. Configuration map

Use this space to illustrate the node's relationship to its servers and other nodes. Any distinguishing characteristics, such as the node's physical location and unique features, should also be listed.

B.2 Server form instructions

Figure B-2 is a sample server form that has been filled in with fictitious
values. The instructions that follow reference this figure.

                      SERVER

AA   DEFAULT   OK   YES   2D hex
------ --------------   -------- ---------   ---------
Node #   Node Name   Password Someone's   # Shadow
                         Default?   Processes

SYSTEM DESCRIPTION

Virtual   Local   Local   Local
Consoles Applications   Drives Printers   Queues Other
-------- ------------   ------   --------   ------ -----
4   GL.CMD (A, C)   A (system) 0 (line)   MXd
       SC2.CMD (A, C)   B (private) 1 (dot)
                   C (hard disk)

NETWORKED RESOURCES

         Drives   Printers
  A   B   C   0   1
---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----
  5A   --   5A   5A   --
  5B   5B   5B
  59   51
  44

             Queues
  MXd
-------- -------- -------- -------- -------- --------
  5A (SC2)
  5B (SC2)

NETWORK PARAMETER VALUES

Number of Input Line Driver Control Blocks _1____
Number of Output Line Driver Control Blocks _1____
DR Net's first flag _60___; total flags _60___ - _7F___
Maximum logical message buffer sier _112__(hex)
Length of end-to-end message header _4____
Length of end-to-end message trailer _3____
Size of message buffer pool _2000_(hex)

CONFIGURATION MAP

```
   +------+
   | AA:: |
   +------+
    |||||
    ||||+----> 5A::
    |||+-----> 5B::
    ||+------> 59::
    |+-------> 51::
    +--------> 44::
```

   Figure B-2. Sample server form

1. Node dependent information

Fill in the specific about the node, such as its ID number, node name, and the
password required to access it. Also, indicate with a "yes" or "no" whether
this node is a requester's default server. This is pertinent to the DR Net
name service. Finally, indicate the number of shadow processes. If this value
is not provided by your OEM, it can be arrived at by adding up the number of
requester processes you determine will require simultaneous access to the
server. Notice that this number is always entered under GENNET as a
hexadecimal number.

2. System description

Use these columns to list the computer's resources. Virtual console are an
item because the node can be used as standalone computer. (Of course, it can
also be requester/server too.) Under each column, you should list all
information about each resource pertinent to the network. For example, in the
"Applications" column, the disks referenced by each program are included; in
the Local Drives columns, the system drive, a private drive, and the data file
drive are designated; and, in the Local Printers column, the type of printer
is shown.

The Local Queues column can be used for all server queues, or just those that
are accessed by remote requesters. In Figure B-2, only the networked queue is
shown.

Use the "Other" column to register distinguishing features that are relevant
to the netork.

3. Networked resources

Allocate each column to a specific drive, printe, or queue, and list the
requesters that are going to use it. In this case, node ID numbers are used,
rather than node names. If more space is needed, use more than one column per

resource, or use a second form.

4. Network parameter values

These values correspond to the Network Parameters described in Section 2.2.1.
As mentioned in that section, you will have to get these values from your OEM.
Those values shown in Figure B-2 are fictitious, but appropriate given all
other node characteristics.

5. Configuration map

Use this space to illustrate the node's relationship to its requesters. Any
distinguishing characteristics, such as each node's physical location and
unique features, should also be listed.

EOF

DNSMGRQR.WS4   (= DR Net System Manager's Guide, Requester form)

DR Net REQUESTER configuration form

(Retyped by Emmanuel ROCHE.)

                  REQUESTER

_____ _____ _____ _____ _____
Node #   Node Name   Default   Password   # Requester
                 Server #   Processes

SYSTEM DESCRIPTION   Resident Operating System: _____

Virtual   Local   Local   Local
Consoles Applications   Drives Printers   Queues Other
-------- ------------   ------ --------   ------ -----

MAPPED RESOURCES

    Drives   Printers   Queues
Local Remote Server Local Remote Server Local Remote Server
----- ------ ------ ----- ------ ------ ----- ------ ------

NETWORK PARAMETER VALUES

Copies Requester Configuration Table _____
Input Line Driver Control Blocks _____
Output Line Driver Control Blocks _____
DR Net's first flag _____; total flags _____ - _____
Maximum logical message buffer sier _____
Length of end-to-end message header _____
Length of end-to-end message trailer _____
Size of message buffer pool _____
Seconds to transaction time-out _____

CONFIGURATION MAP

List of
Servers

_____(default)

_____

_____

_____

_____

EOF

DNSMGRQR.WS4   (= DR Net System Manager's Guide, Server form)

DR Net SERVER configuration form

(Retyped by Emmanuel ROCHE.)

            SERVER

_____ _____   _____ _____   _____
Node #   Node Name   Password Someone's   # Shadow
                        Default?   Processes

SYSTEM DESCRIPTION

Virtual   Local   Local   Local
Consoles Applications   Drives Printers   Queues Other
-------- ------------   ------ --------   ------ -----

NETWORKED RESOURCES

        Drives   Printers

---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ---- ----

              Queues

-------- -------- -------- -------- -------- --------

NETWORK PARAMETER VALUES

Number of Input Line Driver Control Blocks _____
Number of Output Line Driver Control Blocks _____
DR Net's first flag _____; total flags _____ - _____
Maximum logical message buffer sier _____

Length of end-to-end message header _____
Length of end-to-end message trailer _____
Size of message buffer pool _____

CONFIGURATION MAP

List of
Servers

_____(default)
_____
_____
_____
_____

EOF