INTERNATIONAL ATOMIC ENERGY AGENCY
UNITED NATIONS EDUCATIONAL, SCIENTIFIC AND CULTURAL ORGANIZATION
INTERNATIONAL CENTRE FOR THEORETICAL PHYSICS
I.C.T.P., P.O. BOX 586, 34100 TRIESTE, ITALY, CABLE: CENTRATOM TRIESTE

H4.SMR/585-4

FIRST INTERNATIONAL SCHOOL ON COMPUTER NETWORK ANALYSIS AND MANAGEMENT

(3 - 14 December 1990)

Network Management I

Domenico Gianmarini

DIGITAL Equipment S.P.A.
Via Giambellino, 7
34127 Padova

Network Management I

Student Guide

EY-A946E-SG.0001

digital™

Educational Services

Network Management I
Student Guide

EY-A946E-SG-0001

CONTENTS

EXAMPLES

FIGURES

TABLES

About This Course

INTRODUCTION

This course description outlines the contents of the course, and suggests ways in which you can most effectively use course materials. The topics discussed in this course description are:

- Course overview
- Target audience
- Prerequisites
- Course goals
- Nongoals
- Resources
- Equipment
- Course organization
- Course map

COURSE OVERVIEW

Network Management I is designed for VMS system managers who are about to undertake the management of a DECnet network. This course is intended for the system manager who has a knowledge of system operations and a conceptual knowledge of networks, but needs to understand the management of a networking environment.

Network Management I emphasizes your role in generating the network software and overseeing network management. It also covers the tools provided by DIGITAL to help monitor, control and configure the network.

This course concentrates on managing a DECnet network from a VMS system only. It is important for you to master the basics of managing a DECnet network before learning to manage a multivendor network.

The course is organized in a series of modules. Each of these modules contains a set of learning objectives that address a single subject or a group of closely related subjects. The modules contain examples to help you master these objectives. Suggested written and laboratory exercises at the end of most modules provide practice and allow you to test your knowledge of the course topics.

The topics covered in this course include:

- An overview of network management
- DIGITAL Network Architecture (DNA)
- Installation of DECnet software on a VMS system
- Node configuration
- An overview of network access control
- An overview of monitoring and tuning
- Basic fault isolation
- Managing terminal servers

TARGET AUDIENCE

This course is intended for network managers who will be taking on the responsibility of installing DECnet-VAX software and managing a DECnet network on a VMS system.

PREREQUISITES

The following skills and knowledge are necessary for successful completion of this course:

- System management experience on a VMS system with the ability to:
  - — Install layered products on the system.
  - — Set up user authorization and accounting files on the system.
  - — Respond to user requests for operator assistance.
  - — Identify potential problems (hardware or software) by examining error log files.
  - — Monitor system activity and ensure satisfactory system performance.
- The ability to define and give examples of networking concepts and terminology.

These prerequisites may be satisfied by taking the following courses:

- VMS System Management I (Lecture/Lab)—EY-9766E
- VMS System Management (TBI)—EY-3505E
- Introduction to Data Communications (TBI with video)
  - — VHS: EY-6716-VH
  - — Umatic: EY-6716-VU

COURSE GOALS

A network manager should be able to:

- Describe the responsibilities of a network manager.
- Describe the impact of DNA on the management of a DECnet network.
- Install and start up DECnet software on a VMS system.
- Configure and checkout DECnet-VAX software.
- Use the Network Control Program (NCP) to monitor, test, and control the network.
- Identify and adjust system and DECnet parameters that affect network performance.
- Explain and use network access control to prevent unauthorized use of network capabilities.
- Install terminal server software and configure the terminal servers.

NON-GOALS

This course does not address the following topics:

- System management issues that do not relate to networks
- Hardware installation and configuration
- Operating system installation
- Installation and configuration of Ethernet server products
- Comprehensive network troubleshooting
- Comprehensive network internals
- Network design issues
- Management of a multivendor network

RESOURCES

The following resources are available to you for this course:

- The Student Workbook
- *VMS Network Control Program Manual*, (AA-LA50A-TE)
- *VMS Networking Manual*, (AA-LA48A-TE)

EQUIPMENT

To perform the exercises presented in this course, you should have accounts on two nodes running DECnet-VAX software. These nodes should be part of the same network. VMS accounts require NETMBX, OPER, TMPMBX, and SYSPRV privileges.

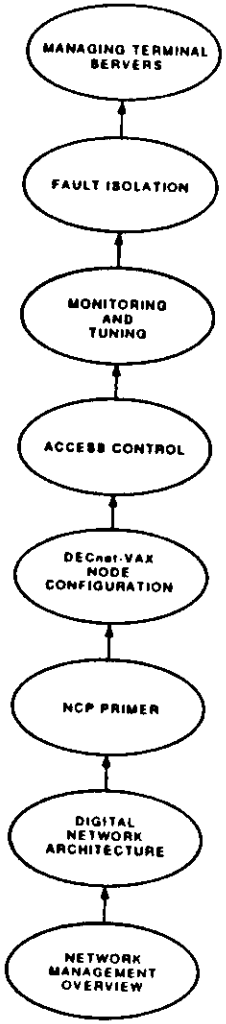
COURSE ORGANIZATION

The course material is arranged in a series of modules. Each module explains one or more of the skills needed to meet the course goals.

Each module consists of:

- An introduction, describing the purpose of the module, providing some motivation for mastering its objectives, and outlining its contents
- The objectives, stating the skills taught in the module
- A list of resources providing additional reading for the section
- The module text, including outlines, tables, figures, and examples to illustrate the topics and material covered in the module
- A summary of the topics presented in the module
- Written exercises, where appropriate, to provide practice and a way to review the skills explained in the module
- Laboratory exercises, where appropriate, to provide hands-on experience with commands and procedures presented in the module

COURSE MAP



MKV_K1600_00

MODULE 1
NETWORK MANAGEMENT OVERVIEW

INTRODUCTION

A DECnet network is a communication system comprising many individual systems that communicate with each other over various physical media. For orderly communication between these nodes, each system must follow rules and regulations for proper system configuration. It is the responsibility of the network manager to ensure that each individual system within the network meets these requirements.

This module identifies and describes the functions of network management, as well as the various roles and duties that a network manager performs. Subsequent modules of this course deal with the implementation of specific parts of network management.

This module discusses:

- The definition of network management
- The responsibilities of a network manager
- The DIGITAL hardware that a network manager must manage
- DIGITAL network management software tools

OBJECTIVES

To describe the responsibilities of a network manager accurately, a network manager should be able to:

- Describe the importance and goals of network management.
- Describe the duties and responsibilities of a network manager in the areas of administration, operation, and technical support.
- Describe the different kinds of hardware a network manager must manage.
- Identify the software tools available to help with network management.

RESOURCES

- *Guide to DECnet-VAX Networking*, (AA-LA47A-TE)
- *VMS Networking Manual*, (AA-LA48A-TE)

WHAT IS A DECnet NETWORK?

DECnet is the collective name for the family of communications products (software and hardware) that allow DIGITAL operating systems to participate in a network. A DECnet network consists of two or more computing systems linked for the purpose of exchanging information and sharing resources. Additional characteristics of a DECnet network include:

- VMS systems use DECnet-VAX software to participate in DECnet networks.
- All systems connected to a DECnet network are peers.
- Any system in the network can communicate with any other system in the network.
- Each system in the network is called a node.
- DECnet networks can vary in size from 2 nodes to over 64,000 nodes.
  - — A maximum of 1023 nodes is possible in an undivided DECnet network.
  - — Larger networks can be divided into multiple areas:

    There may be up to 63 areas.

    Each area may contain up to 1023 nodes.

    Each area operates as a subnetwork.
- DECnet networks support a variety of different network configurations including:
  - — Ethernet local area networks (LANs)
  - — Wide area networks (WANs) utilizing point-to-point, synchronous and asynchronous connections, as well as multipoint connections
  - — Communication through packet switching networks
  - — Communication with IBM SNA networks

What Can the User Do Over the Network?

DECnet software is designed to be transparent to the network user. You can carry out general user operations over the network as easily as at the local node. These operations include:

- Sending electronic mail to any user on the network
- Logging in to another network node on which you have an account
- Accessing common or public directories and databases located on any node in the network
- Manipulating files on remote nodes using several DIGITAL Command Language (DCL) commands including: TYPE, PURGE, DELETE, DIRECTORY, COPY, RENAME, SEARCH, etc.
- Running database software, such as Rdb/VMS or DBMS over the network
- Submitting jobs to remote print and batch queues

WHAT IS NETWORK MANAGEMENT?

Any network consists of two or more nodes. The nodes cooperate with each other to share resources. This cooperation entails such features as:

- Communication paths
- A system of addressing and routing
- Consistent configuration of parameters affecting communication and network performance

Network management is the process that ensures this cooperation. This process is a combination of functions performed by people (network managers) using features provided by software.

The network manager's functions are divided into three major categories:

- Administrative
- Operational
- Technical

The network management functions fall into the following three categories:

- Testing
- Controlling
- Monitoring

Three Levels of Network Management

Depending on the size of the network, the network manager's duties may consist of three levels:

1. Multinode network management
2. Area network management
3. Multiarea network management

Multinode Network Management

- Handles a network consisting of one or more nodes.
- Responsible for several systems within the network.
  - — Installation
  - — Upgrades
  - — Periodic maintenance
  - — Monitoring nodes
  - — Tuning

Area Network Management

- Handles all nodes within a given area.
- Responsible for network consistency within a given area.
- May manage other network managers.

Multiarea Network Administration

- Handles all areas within a major network.
- Responsible for coordination of:
  - — Configurations and network parameters
  - — Naming and addressing conventions
  - — Area and node managers

)UTIES AND RESPONSIBILITIES OF THE NETWORK IANAGER

letwork Administration

e network manager's administrative duties consist of:

Data collection

Network organization and planning

ıta Collection

ery network manager should maintain a set of network logs that contains specific information out the network nodes and all other network components, including:

Node information

— Node name, address, and type

— Location

— System manager

— CPU

— Native operating system

— Buffer sizes

Line and cable information

— Type of communication controller

— If point-to-point, node at the other end of the line

— Location

— Who owns them

— Whom to call to fix them

Data Collection

- Circuit data
  - — Circuit identifier
  - — Circuit cost
- Other hardware and software components
  - — Communications devices
  - — Servers
  - — Routers
  - — Location and accessibility of applications, objects, and layered products
  - — Bridges and repeaters (If Ethernet LAN)
- Management Information
  - — Current Event Log configuration
  - — Existing node configurations within the network
  - — Changes made to the network
  - — Reported problems and solutions
  - — Location of Event Log sink node
  - — Record of changes made to the system hardware and software

Network Organization and Planning

The network manager is responsible for defining and implementing procedures for:

- Distributed system coordination to deal with:
  - — Configuration guidelines
  - — Network performance
  - — Network monitoring
  - — Network security
  - — Single versus multiuser systems
  - — Heterogeneous operating systems within the network
- Coordination of DECnet Phase III and IV Nodes

Operational Functions

The following ongoing activities are used to develop standard network procedures:

- Network setup activities
  - — Implementation of security procedures
  - — Determine implementation details for:
    - Access control schemes
    - Object naming and numbering
- Periodic Activities (as needed)
  - — DECnet software installation and upgrades
  - — Addition of network users
  - — DECnet node and line startup and shutdown
  - — Tuning of the network parameters for optimal performance
  - — Supporting existing network applications
- Monthly activities
  - — Network preventative maintenance
- Daily activities
  - — On-line network data collection
  - — Local and remote network performance monitoring
  - — Down-line loading software to unattended remote nodes
  - — Maintaining awareness of network hardware state

Technical Functions

Network Troubleshooting

- Create a process for tracking and/or isolating network problems.
- Establish a contact list.
  - — Internal contacts—other system managers
  - — DIGITAL Field Service Representative
  - — DIGITAL Software Services Representative
- Establish problem documentation requirements.
  - — List of standard questions to ask when a problem is reported
  - — Hard copy documentation of on-line data required
- Establish escalation procedures consisting of:
  - — Technical support
  - — Setting problem priorities
  - — Deciding when a problem needs to be taken to a higher authority

Forecast Network Growth

Obtain the appropriate forecasting information:

- Current network utilization
- Planned upgrades for growth and performance
- Recommended network components

DIGITAL HARDWARE

A DECnet network can comprise many different types of hardware. This section describes some common hardware components.

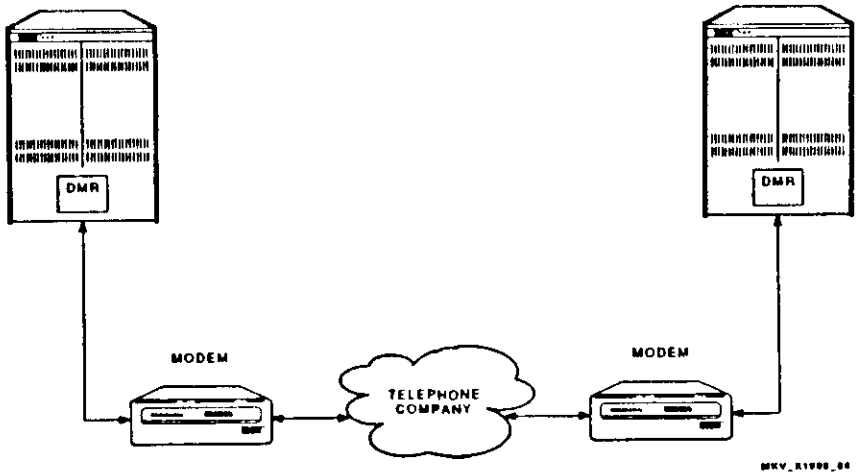
Point-to-Point Connections

A point-to-point connection uses WAN technology to link two nodes. WAN technology utilizes:

- A synchronous or asynchronous communication interface:
  - — Synchronous communication is preferred when large amounts of data must be transmitted on a continual basis.
  - — Asynchronous communication is advantageous when a temporary or low cost connection is needed.
- A modem to modulate the signal from digital to analog for transmission over the communication line and to demodulate the signal from analog to digital at the receiving end
- A communication cable, usually a telephone line

Figure 1–1 shows a simple network, consisting of two nodes joined by a point-to-point link.

Figure 1–1: A Point-to-point Connection



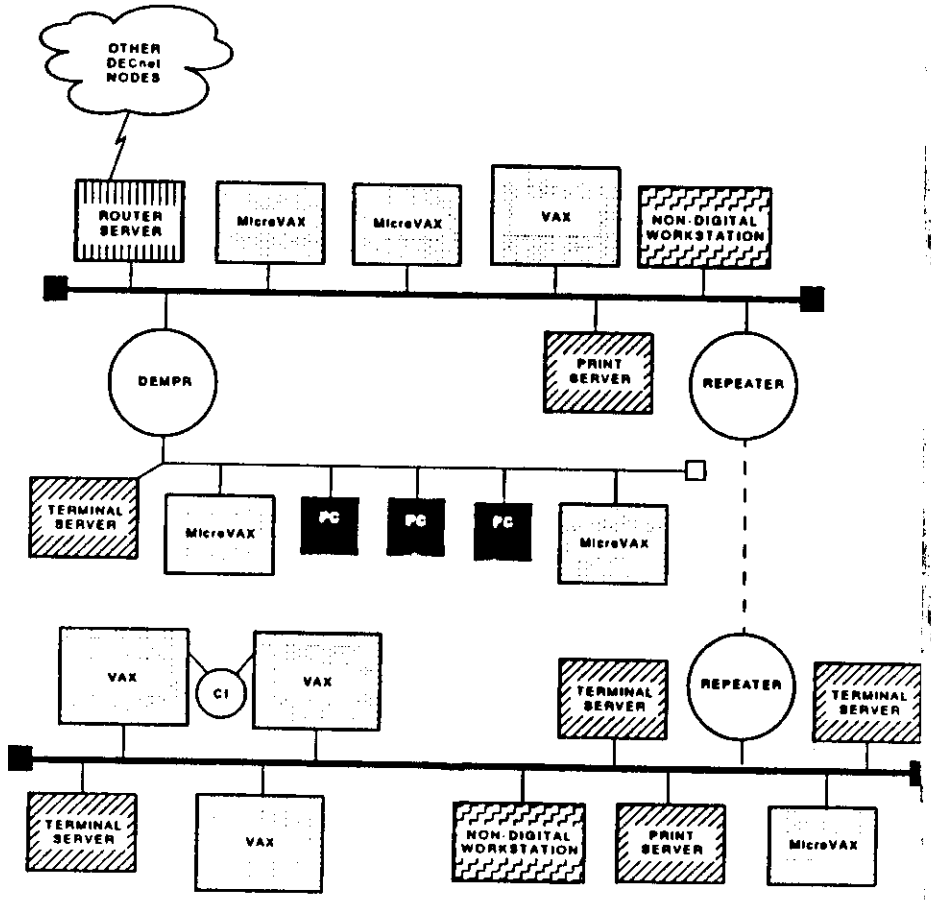
Ethernet LANs

DIGITAL uses the Ethernet protocol to implement local area networking. An Ethernet LAN acts as a hardware conduit over which the information travels.

- Ethernet LANs use CSMA/CD (carrier-sense, multiple-access with collision-detection) to regulate access to the cable.
- The longest distance between any two stations on an Ethernet LAN is 2800 meters.
- If a segment is longer than 500 meters, there must be a repeater to refresh and regenerate the signal.
  - — Local repeaters can span up to 100 meters.
  - — Remote repeaters connect two repeaters with fiber-optic cable to span up to 1000 meters.
  - — No more than two repeaters are permitted between any two stations. A remote repeater is considered one repeater.
- DECnet software can share an Ethernet cable with several other networking protocols.

Figure 1–2 shows an Ethernet LAN.

Figure 1–2: An Ethernet LAN



Servers

A server is an entity that is responsible for processing requests. The issuer of these requests is called the requestor; the sole function of the server is to process and fulfill the requests.

On an Ethernet LAN, a server is usually a special-purpose node that provides a service to the other nodes on the LAN. Figure 1–2 shows three different kinds of servers:

- Terminal servers
  - — Provide a service to both the user and the host node.
  - — Eliminate the need for terminals to be hard-wired to hosts.
  - — Allow any terminal connected to a terminal server to establish a connection with any host on the Ethernet LAN.
  - — Allow users to establish multiple simultaneous connections to the same or different hosts.

Print servers

- — Provide a printing service to the network.
- — Allow a high-speed, high-quality printer to be shared by several nodes thus distributing the expense.

Router servers

- — Provide a routing service to nodes on the Ethernet LAN.
- — Permit nodes on the Ethernet to communicate with other DECnet nodes that they are not on the Ethernet LAN.
- — Can improve the efficiency of routing on the Ethernet LAN.

Extended LANs

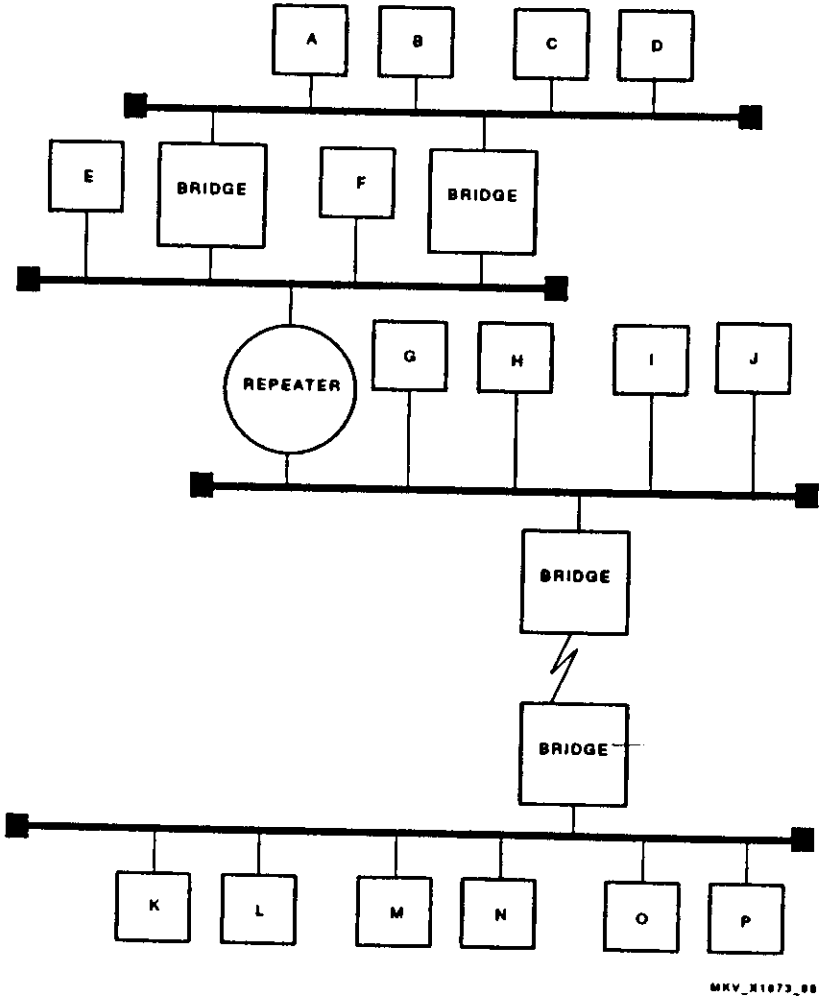
The protocol limit for Ethernet is 2800 meters between any two nodes. An extended LAN lengthens this distance without degrading the Ethernet 10 Mbits/s throughput. Extended LANs are created using bridges.

Bridges can be used to:

- Join two or more Ethernet LANs to create an extended LAN.
- Join LANs in remote locations to provide LAN capabilities where an ordinary LAN cannot reach.
  - — A remote repeater can only extend the network by 1000 meters.
  - — With fiber optic and microwave bridges, an extended LAN can span distances of up to 22,000 meters and include up to 8,000 nodes.
  - — There are bridges available that use satellite technology to span even greater distances. The throughput for a satellite bridge is limited due to propagation delays.
- Improve performance on heavily used LANs
  - — Repeaters forward all data packets, including those where the destination node is on the same segment as the source node.
  - — Bridges filter data and forward only those packets where the destination node is on a different segment than the source node.

Figure 1–3 shows an extended LAN.

Figure 1–3: An Extended LAN



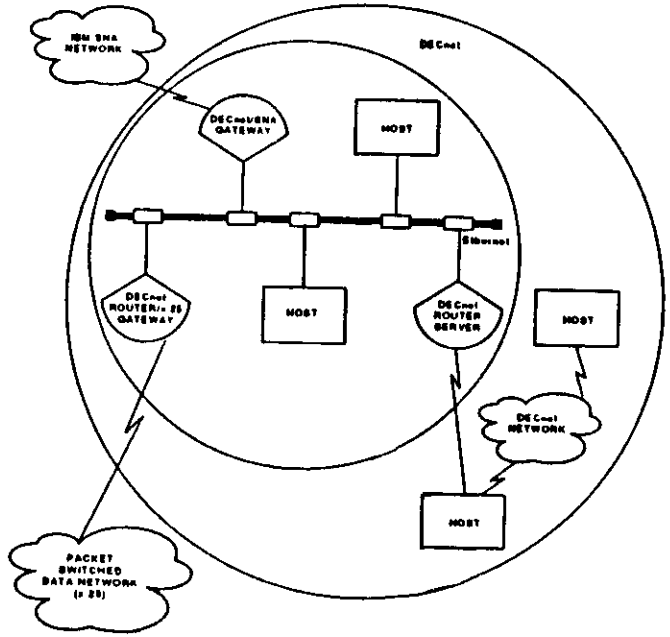
Multivendor Networks

DECnet software is flexible enough to participate in multivendor networks. To do so requ a gateway as well as special software on the VMS systems that communicate with the ot networks.

- The function of a gateway is to translate protocols between dissimilar systems.
- The DECnet/SNA Gateway allows DECnet systems on the LAN to communicate with I SNA networks.
- The DECnet Router/X.25 Gateway allows DECnet systems on the LAN to participate packet-switched data networks that use the X.25 protocol.

Figure 1–4 shows one way that DECnet software operates in a multivendor environment.

Figure 1–4: DECnet Software in a Multivendor Environment



NETWORK MANAGEMENT TOOLS

DIGITAL's collection of software network management tools includes:

- Network Control Program (NCP)
- NMCC/DECnet Monitor
- Ethernet Network Integrity Monitor (NMCC/VAX ETHERnim)
- Remote Bridge Management Software (RBMS)
- LAN Traffic Monitor (LTM)
- Terminal Server Manager (TSM)

Network Control Program (NCP)

- NCP is the main networking software tool used by a network manager.
- NCP is a user interface used to perform the following network management tasks:
  - — Configure
  - — Control
  - — Monitor
  - — Test
  - — Event logging
  - — Fault isolation
- Use NCP to display information about the network or to alter that information.

NMCC/DECnet Monitor

NMCC/DECnet Monitor is a software product that can monitor and collect information about DECnet nodes in a complex network. DECnet Monitor capabilities include:

- Addressing the problem of complex network management by collecting, analyzing, and displaying network information
- Graphically depicting the state of the network
- Maintaining a database of network information
- Looking at a large sample of data to discover trends
- Providing either standard or customized reports
- Detecting problems early, thus avoiding poor network service and lengthy downtime

NMCC/VAX ETHERnim

NMCC/VAX ETHERnim is a software product that can monitor and test nodes on the LAN. The capabilities of ETHERnim include:

- Graphically depicting the state of nodes on the LAN
- Finding nodes on the LAN
- Building a database of information about each node in the LAN
- Providing a means of testing the nodes in the LAN

Remote Bridge Management Software (RBMS)

RBMS is a software product that manages the extended LAN by controlling the LAN bridges that connect the LAN segments. Some RBMS features include:

- The ability to modify and display bridge characteristics.
- Management of the filtering of multicast and physical addresses.
- The ability to initialize the bridge via management commands.
- Maintenance of an on-line mapping of bridge ASCII names to physical addresses.
- Access to several bridges using a single command.

LAN Traffic Monitor (LTM)

LTM is a software product that can monitor the traffic statistics on an Ethernet LAN. Some LTM features include:

- The ability to generate Ethernet statistics
- The capability to display such network information as:
  - Network traffic
  - Top users
  - Utilization
  - Node lists
  - Multicast lists
  - Station traffic display

Terminal Server Manager (TSM)

TSM is a software product that gives the network manager the ability to observe and cont DIGITAL terminal servers anywhere in an extended LAN. TSM's capabilities include:

- Providing a directory database containing a terminal server name to physical address m ping
- Detecting new terminal servers and automatically adding them to the database
- Centralizing management of the terminal servers
- Improving fault management of terminal servers by providing access to status indicators a error counters

SUMMARY

Network managers control and direct various administrative, operational, and technical factors of a network for optimal network performance. Network managers can operate at various levels of responsibility, categorized in part, by the number of network nodes for which they are responsible. The progression of responsibilities ranges from the manager of a single, stand-alone system, who is responsible for the participation of one node in the network, to the manager of several nodes in a single physical location, to the manager of a regional network, to the administrator of a worldwide corporate network.

Regardless of the size of the network, the network manager's responsibilities fall into these three general categories:

- Administrative—includes data collection, network organization and planning
- Operational—includes establishment of operational guidelines and procedures, oversight of ordinary network operations
- Technical—includes fault isolation, forecasting network growth

A network manager should be familiar with the kinds of hardware that make up the network. The two basic connection types on a DECnet network are point-to-point connections for wide area transmissions, and Ethernet connections for local area networks. DECnet software is also capable of communicating over X.25 packet switching networks.

The components on an Ethernet LAN include repeaters, bridges, routers, gateways, and servers. A repeater refreshes the signal and retransmits it between different segments of the Ethernet LAN. A bridge provides a filtering service, retransmitting packets only if the destination node is not on the same segment as the source node. A router improves the efficiency of communication among nodes on the LAN and permits them to communicate with nodes that are not part of the LAN. A gateway provides protocol translation to allow DECnet nodes on the LAN to communicate with other vendors' networks. Finally, a server is an entity that processes requests for LAN users, for example, a terminal connection to an Ethernet host.

DIGITAL provides a number of tools to assist the network manager. The primary network management tool provided by DECnet software is the Network Control Program (NCP). NCP allows you to configure your node, display information about the network, monitor network performance, service remote nodes, and test the network.

DIGITAL's layered products to aid network monitoring and management include: NMCC/DECnet Monitor, NMCC/VAX ETHERnim, Remote Bridge Management Software, LAN Traffic Monitor, and Terminal Server Manager.

MODULE 2
DIGITAL NETWORK ARCHITECTURE

INTRODUCTION

A network architecture is composed of rules and functional specifications that determine how to use hardware and software when two processes need to communicate. An architecture is not a network implementation. The actual network is implemented by communications hardware and software in accordance with the rules set forth by the architecture.

The network architecture is a blueprint for the implementation of a network. Just as a blueprint for a building describes how the building is to be constructed, the architecture for a network describes how the network is to be constructed. The blueprint design must be followed for the building to be constructed as planned. Similarly, the rules specified by the network architecture must be followed for the network to operate as planned.

As a network manager, a conceptual understanding of the network architecture helps you understand the consequences of your actions. A knowledge of the terms, definitions, and concepts associated with DIGITAL Network Architecture helps to clarify the information presented in the manuals and aids comprehension of network parameters and network management activities.

OBJECTIVES

To describe the impact of DIGITAL Network Architecture on the management of a DECnet network, a network manager should be able to:

- Identify the features and functions of each layer of DNA.
- Trace the flow of information through the architectural layers.
- Define key routing terms and concepts.
- Describe the operation and module interfaces of the Network Management Layer.

RESOURCES

- *VMS Networking Manual*, (AA-LA48A-TE)
- *Digital's Networks: An Architecture with a Future*, (EY-3637E-PO)
- *DECnet DIGITAL Network Architecture (Phase IV) General Description*, (AA-N149A-TC)

DNA PHASES

There have been four phases of DNA. The features introduced in each phase are listed below:

- Phase I - 1976
  - — RSX-11M; PDP11's
  - — Program to program
  - — File transfer
  - — Sophisticated technical customer base
- Phase II - 1978
  - — All major operating systems/processors
  - — Remote file access
  - — Network management
  - — Point-to-point configurations
- Phase III - 1980
  - — Adaptive routing
  - — Network terminals
  - — Multipoint lines
  - — CCITT X.25
  - — Record access
  - — Down-line loading
- Phase IV
  - — Ethernet LANs
  - — Large networks
  - — Communications servers
  - — SNA gateway

WHAT IS A NETWORK ARCHITECTURE?

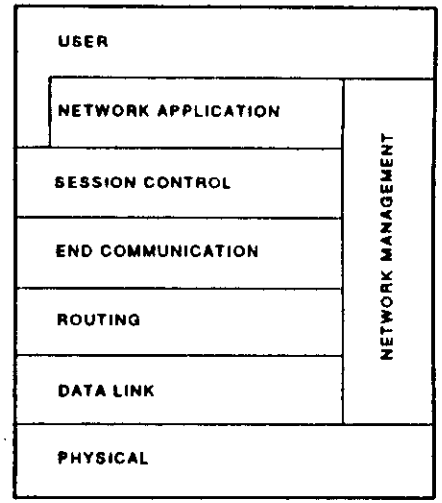
Layers

Many architectures divide network functions into logical layers:

- Modules comprising each layer perform related network operations.
- Layering keeps the network flexible and capable of being easily modified.
- Modifications cause minimal disruption to architecture as a whole.

Figure 2–1 shows the layers of DNA.

Figure 2–1: DNA Layers



MKV_X1681_85

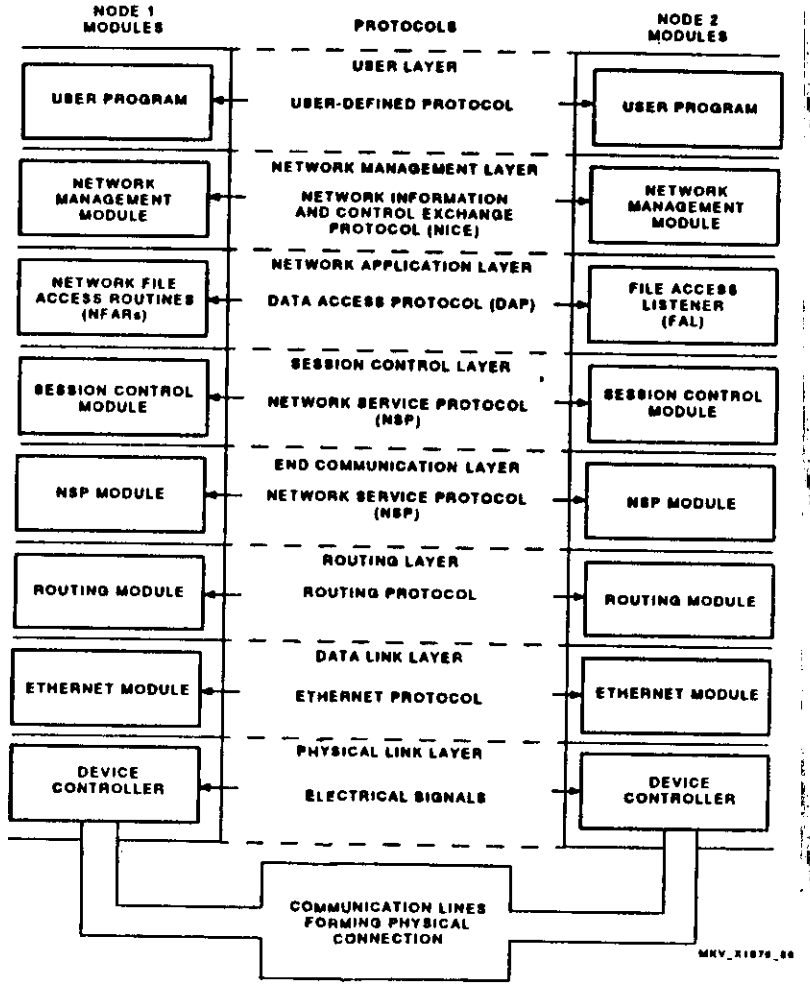
Peer Layer Protocols

Peer layer protocols operate in the following manner:

- Describe communication between equivalent layers of distinct nodes.
- Layers communicate logically but only Physical Layer communicates directly.
- Add information to data that is stripped by peer layer at receiving node.

Figure 2–2 shows some of the different protocols that operate in DNA.

Figure 2–2: DNA Protocols



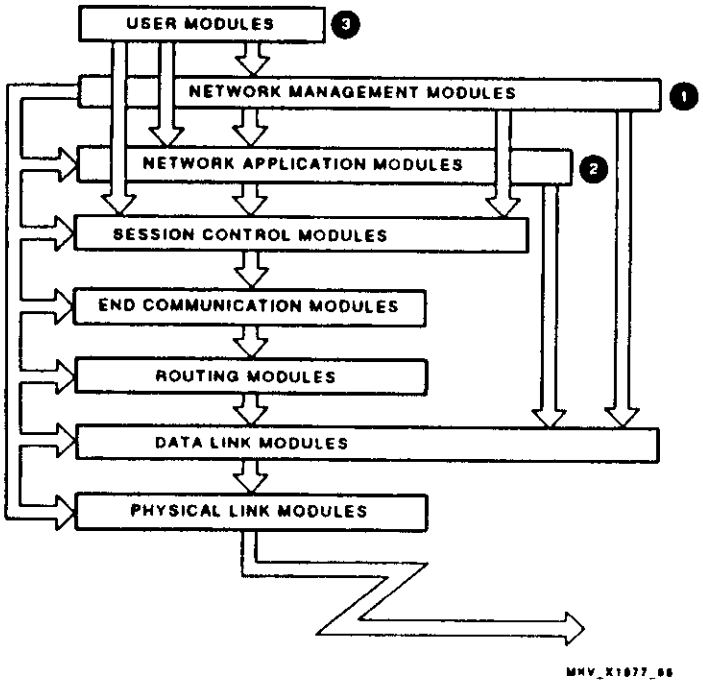
Module Interfaces

Module interfaces are responsible for the following:

- Define precise functional boundaries between the modules in adjacent layers of a single node.
- Enable layers to exchange information as data is passed through layers.

There are some other important interfaces besides those between adjacent layers. These are shown in Figure 2–3.

Figure 2–3: Module Interfaces in DNA



Problems for a Network Architecture to Overcome

A network architecture must overcome several problems. These include:

- Compensating for hardware problems, for example, noise on the communication line
- Routing messages to non-adjacent nodes
- Allowing program-to-program communication
- Controlling access to systems, applications, and files
- Converting data formats
- Providing user interface to the network

DNA LAYERS

Physical Link Layer

This layer manages the physical transmission of data over a channel. Its functions include:

- Transmission and reception
- Carrier sense on Ethernet LANs
- Collision detect on Ethernet LANs
- Interrupt handling

This layer deals with:

- EIA RS 232-C, RS 423, RS 449, etc.
- Ethernet physical layer
- CCITT X.25
- CI Bus

Data Link Layer

The Data Link Layer is responsible for the communication path between adjacent nodes. It ensures the integrity of the data transferred between these nodes and:

- Creates a communication path between adjacent nodes.
- Frames messages for transmission over the physical channel between adjacent nodes.
- Checks integrity of received messages.
- Manages use of channel resources.

Data Transparency

The Data Link Layer ensures that the physical transmission of data is transparent in the following manner:

- All information passed to the Data Link Layer is considered data.
- Layers above the data link are isolated from problems on the physical channel.
- Errors are detected, and in some cases, data is retransmitted until received correctly.

Data Link Layer Protocols

DECnet software uses three different data link protocols:

- Ethernet Data Link
  - — Operates over a LAN.
  - — Provides a best-effort delivery service.
  - — Provides link management and error detection.
- DDCMP
  - — Operates over synchronous or asynchronous lines.
  - — Ensures correct sequencing of data.
  - — Provides error control.
- X.25
  - — Follows CCITT recommendation.
  - — Defines interface between DTE and PSDN.

Routing Layer

If two nodes that are not directly connected need to communicate, there must be a means of routing information between them. The Routing Layer is responsible for forwarding packets of data to their destination. This layer:

- Provides message delivery service.
- Implements datagram service.
- Selects best path.
- Provides adaptive routing.

Node Types

There are two types of nodes in a DECnet network:

- End node:
  - — Has exactly one active circuit.
  - — Can only communicate through its adjacent node.
- Full-function (routing) node:
  - — Can have more than one active circuit.
  - — Receive and forward information addressed to other network nodes.
  - — Exchange information about network availability with other routing nodes.

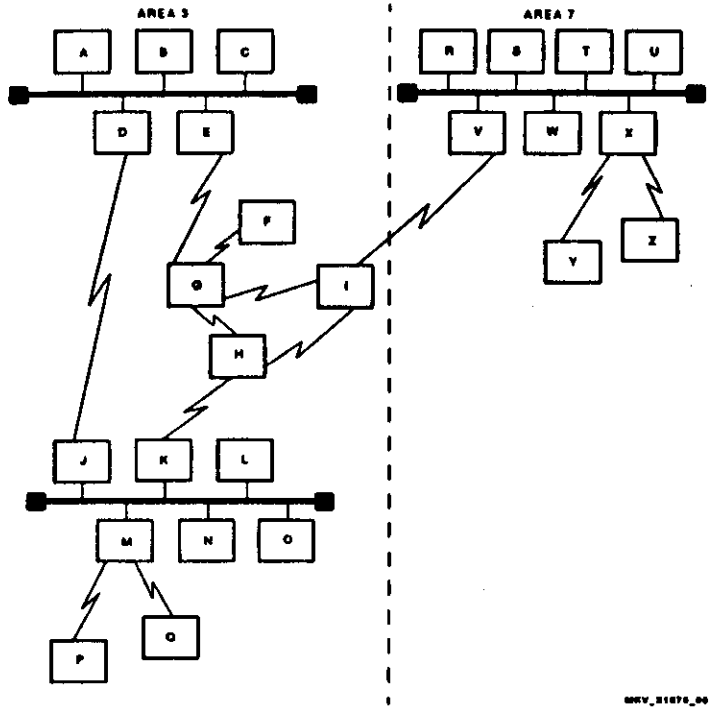
Area Routing

DECnet networks can comprise over 64,000 nodes. To make the size of the network more manageable, the network can be divided into areas.

- An area can contain up to 1023 nodes.
- A DECnet network can contain up to 63 areas.
- In a network with multiple areas, there are two types of routing nodes:
  - — Level 1 routers can route data within an area.
  - — Level 2 routers route data between areas.
- When there are two or more area routers in an area, they should form a closed loop.

Figure 2–4 shows these kinds of nodes in a DECnet network.

Figure 2–4: DECnet Node Types



Adaptive Routing

In DECnet routing, there can be more than one possible path between the source and destination nodes. With the adaptive routing provided by DECnet software:

- A routing node computes the least cost path between the source and destination nodes.
- If two paths have the same cost:
  - When equal-cost path-splitting is enabled, packets alternate between equal paths.
  - When the maximum number of path splits is 1, packets are sent along the shorter path.
- If, for any reason, the preferred path is unavailable, an alternate path is found.

Routing Layer Functions

The Routing Layer has several functions:

- Determines best path using routing database.
- Forwards incoming packets.
- Dynamically adapts to topology changes.
- Supports multiple circuit types.
- Periodically updates other routing modules.
- Manages buffers to control congestion.
- Limits number of nodes a packet can visit.
- Performs node verification.
- Monitors errors detected by the Data Link Layer.
- Maintains counters and gathers data for network management.

Routing Concepts

The concepts important in understanding routing include the following:

- Adjacency is a circuit/node pair.
- Hop is the logical distance to an adjacent node.
- Circuit Cost is a positive integer associated with using a circuit.
- Path is a possible route from the source node to the destination node.
- Visit is an intermediate node between the source node and the destination process.
- Congestion control:
  - — Handles buffer management.
  - — Prevents deadlocks.
- Packet lifetime control:
  - Loop detector
  - Node listener
  - Node talker

Routing on an Ethernet LAN

Routing on an Ethernet LAN works in the following manner:

- All nodes on an Ethernet LAN are adjacent.
- Routing nodes on an Ethernet LAN are useful for the following reasons:
  - — To allow Ethernet nodes to communicate with nodes that are not on the LAN
  - — To keep track of the availability of other nodes
- The designated router intervenes in transmissions between end nodes.
- Router-servers and other dedicated routing nodes can further enhance the performance of an Ethernet LAN by:
  - — Reducing or eliminating routing traffic on the LAN
  - — Allowing individual nodes to spend less CPU time on routing

End Communication Layer

This layer is responsible for coordinating the end-to-end communication between the source and destination nodes.

- Handles the system independent aspects of logical link communication.
- Provides process to process communication service.
- Uses Network Services Protocol (NSP).
- Creates and destroys logical links.

End Communications Layer Concepts

Some of the concepts important in understanding the End Communication Layer include:

- Logical Links
  - — Exist between cooperating tasks
  - — Transmit normal or other data
- Error Control
  - — Acknowledging messages
  - — Sequencing messages
- Flow Control
  - — Ensuring proper buffering
- Segmentation
  - — Breaking messages up into smaller pieces
- Multiplexing the Logical Link

Network Services Protocol (NSP)

The End Communication Layer uses NSP to:

- Create and destroy logical links.
- Guarantee proper sequencing of messages.
- Segment data messages.
- Reassemble segments at receiving node.
- Provide error control.
- Provide flow control.

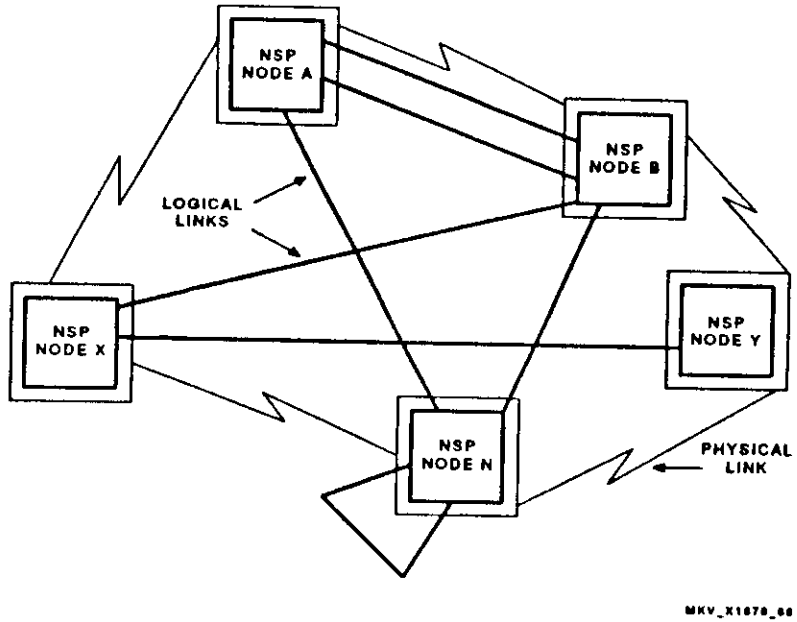
Logical Links

Logical links are created, maintained, and destroyed by the End Communication Layer upon the request of the Session Control Layer. Some characteristics of logical links include:

- Full-duplex channel between two nodes.
- Ability for users at both ends to exchange data.
- Guaranteed delivery (unless network fails).
- Several logical links can be active simultaneously over the same line.

Logical links are illustrated in Figure 2–5.

Figure 2–5: Logical Links



Cooperating Tasks

Logical links are established between cooperating tasks. Some characteristics of cooperating tasks are:

- No data is sent unless it is requested by receiving program.
- Sends and receives must be coordinated.
- Control of cooperating tasks is taken care of at the user level.

Session Control Layer

The Session Control Layer is responsible for the following functions:

- Defines the system dependent aspects of logical link communication.
- Maps node names to node addresses.
- Identifies end users.
- Activates or creates a process.
- Validates incoming connect requests.
- Verifies available access control information.

Session Control Operations

To perform its functions, the Session Control Layer:

- Requests logical link on behalf of end-users.
- Receives connect requests.
- Sends and receives logical link data.
- Disconnects or aborts logical link.
- Monitors logical link.

Requesting a Connection

When a user program requests a logical link, the Session Control Layer:

- Identifies destination node address.
- Formats connect data for End Communication Layer.
- Issues connect request to End Communication Layer.
- Starts a timer.

Receiving a Connect Request

Upon detecting a connect request from the End Communication Layer, the Session Control Layer:

- Parses connect data.
  - — Source and destination end user process names
  - — Access control information
- Validates access control information.
- Identifies, activates, or creates process for the destination end.
- Maps source node address to name.
- Delivers request for connection to end user process.

Network Application Layer

This layer provides services to the User Layer, such as remote file access and transfer, remote interactive terminal access, and gateway access to non-DIGITAL supplied modules.

- Provides generic network applications:
  - — Commonly used routines
  - — Communications services
- Allows for user-written protocols.
- The layer has several independent modules that can operate simultaneously:
  - — Data Access Protocol - remote file access
  - — Network Virtual Terminal Protocol - CTERM
  - — X.25 Gateway Access Protocol
  - — SNA Gateway Access Protocol
  - — Loopback Mirror Protocol

Data Access Protocol Functions

The Data Access Protocol (DAP) performs the following functions:

- Supports heterogeneous file systems.
- Transfers files.
- Supports deletion/renaming of remote files.
- Lists directories of remote files.
- Allows multiple transmissions over one logical link.
- Provides error recovery.

Network Management Layer

The Network Management Layer provides user access to the operational parameters and counters in the lower levels. This layer allows the network manager to:

- Perform various types and levels of network testing.
  - — Local and remote node loopback testing
  - — Circuit loopback testing
- Access network management functions at remote nodes.
- Down-line load and up-line dump remote systems.
- Examine network parameters and counters residing in the other network layers on local or remote nodes.
- Control network operations:
  - — Down-line loads
  - — Start and stop lines and circuits
  - — Monitor network performance
- Monitor significant events across the network.

Network Management Layer Components

Table 2–1 shows the components used for network management.

Table 2–1: Network Management Components

LAYER	COMPONENT	FUNCTION
User	Network Control Program	Provides user interface to network management. Allows user to manipulate network parameters.
Network Management	Network Management Access Routines	Provide generic network management functions. Communicate over logical links with Network Management Listener using the NICE protocol.
	Network Management Listener (NML)	Receives network management commands from local and remote network management access routines using the NICE protocol. Passes function requests to the local network management functions.
	Local Network Management Functions	Translate function requests into system dependent calls.
	Link Watcher	Services requests from adjacent nodes for remote load, dump and trigger functions.
	Maintenance Functions	Supports system maintenance functions such as down-line loading and up-line dumping using MOP.
	Link Service Functions	Provide a direct interface to the Data Link Layer for higher-level network management modules that need to bypass the intermediate layers.
	Event Logger	Records significant events that take place in the lower layers.
Network Application	Loopback Access Routines and Loopback Mirror	Provide a means of isolating faults and testing components between two nodes using the Loopback Mirror protocol.

Network Management Protocols

The Network Management Layer uses four protocols:

- NICE (Network Information and Control Exchange) handles most network management functions, including:
  - — Down-line load and up-line dump requests
  - — Setting parameter values
  - — Examining and zeroing counters
- Event Logger Protocol provides event related information, such as the name and address of the source node and the time the event occurred at the source node.
- Loopback Mirror Protocol handles node loopback functions.
- MOP (Maintenance Operation Protocol) communicates directly with the Data Link Layer for down-line loading, up-line dumping, and testing.

User Layer

This layer contains most user supplied functions. The interface into the network is usually transparent. The User Layer contains:

- The Network Control Program (NCP)
- MAIL
- PHONE
- SET HOST
- DCL commands for example, COPY, DIRECTORY, TYPE
- SYSMAN

DATA FLOW THROUGH THE LAYERS

Data flows across the network as follows:

1. The user process at the source node generates data.
2. User data is passed down through the source node layers. Each layer adds control information in its own header. See Figure 2–6.
   a. Network Application Layer invokes the appropriate program, which adds application specific protocol information.
   b. Session Control Layer adds access control information if it was not explicitly supplied.
   c. End Communication Layer breaks information into packets.
   d. Routing Layer:

      Adds a header containing the source and destination node addresses and the visit counter.

      Determines best path on a routing node.

   e. Data Link Layer adds:

      A header containing control information (For Ethernet nodes, this information includes the source node address and the destination address of the adjacent node.)

      Error checking CRC in trailer.
3. At the Physical Layer, the packet is transmitted to the adjacent node.
4. When it is received properly at the adjacent node, it is passed up to the Routing Layer.
5. The Routing Layer checks the destination address and forwards the packet:
   - To the End Communication Layer if the destination address matches.
   - To the next node in the path if the destination address is different.
6. The data is passed up through the destination node layers. Each layer strips off the information added by the peer layer at the source node.
7. The user process at the destination node receives the data.

This process is illustrated in Figure 2–7.

Figure 2–6: Data Flow at the Source Node

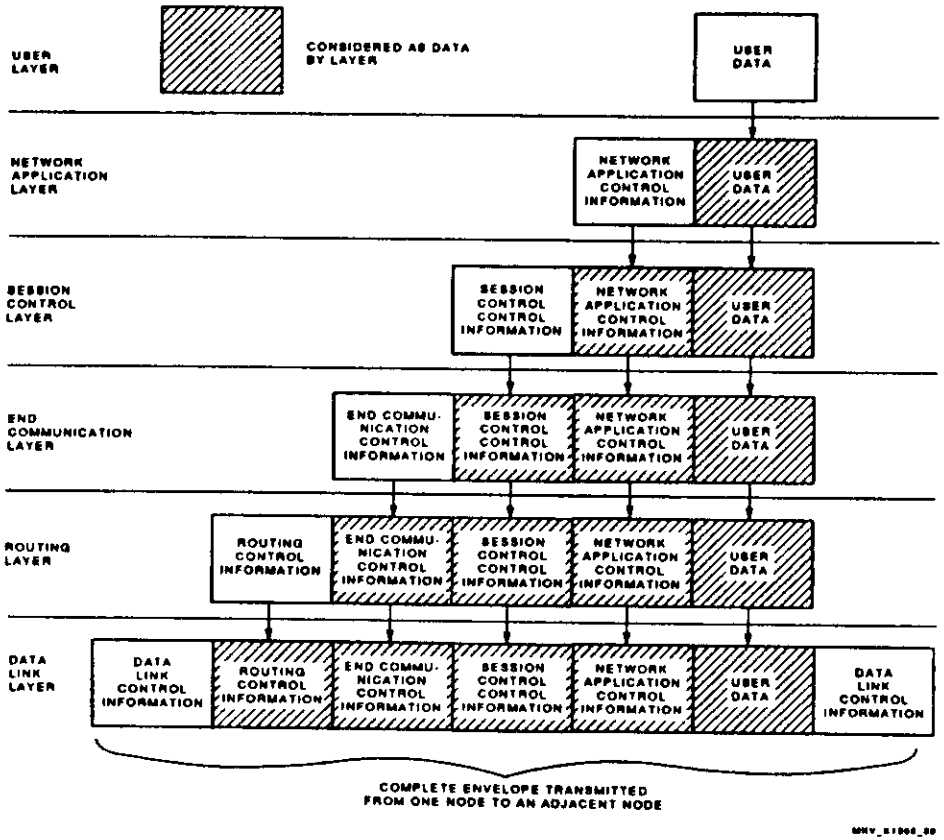
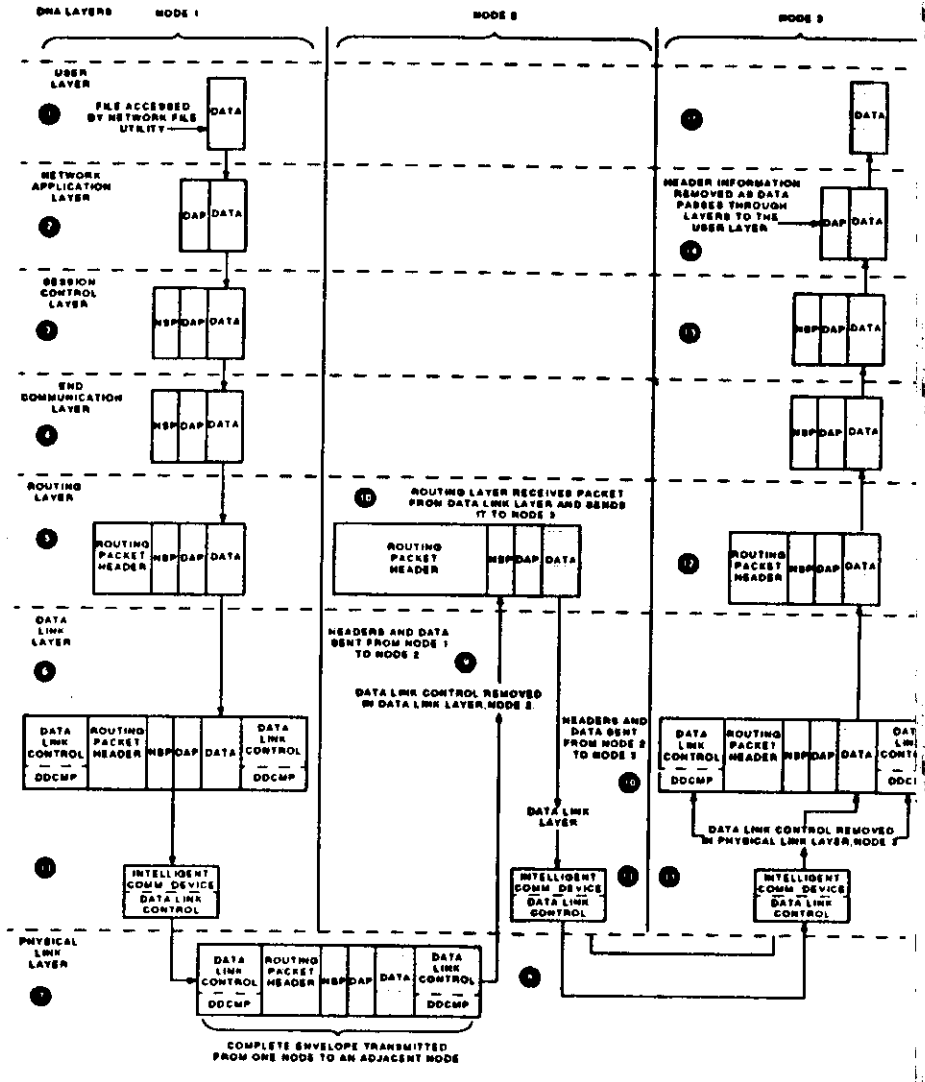


Figure 2–7: Data Flow Across the Network



SUMMARY

A network architecture is a set of rules and specifications for communication in a computer network. DIGITAL Network Architecture is made up of eight functional layers. Each layer comprises software and/or hardware modules that perform related functions. Communication between equivalent layers of separate nodes is accomplished using peer-layer protocols. Communication between different layers in the same network node is accomplished using module interfaces.

Each layer of DNA performs specific functions. A partial list of these functions appears in Table 2–2.

Table 2–2: Some Functions of DNA Layers

LAYER	FUNCTION
User	Stores user-written programs, DCL commands, and NCP.
Network Management	Performs loopback tests and down-line loading; gathers network data.
Network Application	Contains commonly used applications; provides protocol translation for communication with other vendors' networks.
Session Control	Processes logical link requests from higher layers; validates access control information.
End Communication	Establishes and maintains logical links.
Routing	Finds best path from source node to destination node.
Data Link	Oversees communication between adjacent nodes and ensures that transmission is error-free.
Physical Link	Actually transmits the data along the transmission medium.

Several other terms are introduced in this module. The following glossary reviews some of the important concepts.

Glossary

CIRCUIT:
A logical connection between protocol modules at the Data Link Layer.

CIRCUIT COST:
A positive integer value associated with using a circuit.

DESIGNATED ROUTER:
A routing node on an Ethernet LAN chosen to perform additional duties, such as informing each end node on the Ethernet LAN of the existence of other end nodes and of the identity of the Ethernet routing nodes.

END NODE:
A node that supports a single active line and cannot forward packets intended for other nodes.

HOP:
To the Routing Layer, the logical distance between two adjacent nodes in a network.

LINE (PHYSICAL LINK):
A hardware addressable communication path.

LOGICAL LINK:
A virtual circuit between two end-user processes in the same node or in separate nodes.

PACKET:
A unit of data routed from a source node to a destination node.

PATH:
A possible route for a packet from source node to destination node.

PATH COST:
The sum of the circuit costs along a path between two nodes.

PATH LENGTH:
The number of hops along a path between two nodes.

ROUTING NODE (FULL-FUNCTION NODE):
A node that has more than one connection to the network, receives and forwards information addressed to other nodes, and exchanges information about network availability with other routing nodes.

WRITTEN EXERCISES

1. What protocol is used for file transfers? At which layer does this protocol reside?
2. Which network management protocol communicates directly with the Data Link Layer, bypassing intermediate layers?
3. Which two layers are responsible for logical links? Why is it necessary to have two layers assigned to this task?
4. Peer layer protocols allow equivalent layers of remote nodes to communicate logically. Only one layer actually transmits the data. Which one?
5. Which layer is responsible for end-to-end transmissions? for transmissions between adjacent nodes?
6. How is a level 1 router different from a level 2 (area) router?
7. Place the following events in the order in which they occur when a user at the source node sends a message to a user at the destination node.

   ☐ As the message passes through the layers of the source node, each layer adds control information to it.

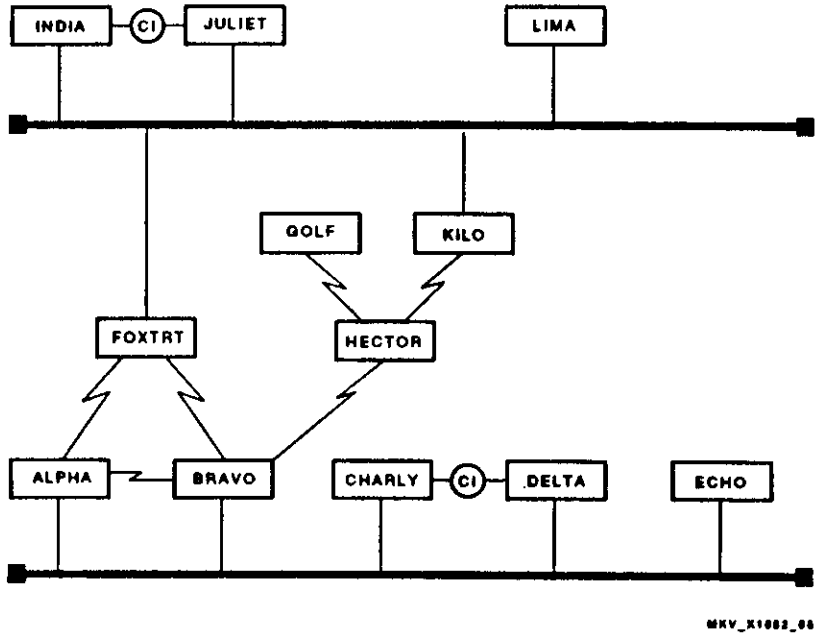
   ☐ The message is received by the network user at the destination node.

   ☐ The message is passed up through the layers of the destination node; each layer removes its control information.

   ☐ The message is transmitted in the form of electrical signals across the physical link.

   ☐ The message is passed from the user process to the highest layer of the source node (in DNA, it is the User layer).

Figure 2–8: Sample Network



MKV_X1082_88

Questions 8-11 apply to Figure 2–8. As you answer them, you need to know the following:

- Node types
  - — INDIA and BRAVO are the designated routers for the two Ethernet LANs.
  - — Any node that is shown with only one circuit is an end node. In addition, JULIET and DELTA are end nodes.
- Line types
  - — The line between ALPHA and BRAVO is an asynchronous point-to-point connection.
  - — The line between ALPHA and FOXTRT is a high-bandwidth leased line.
  - — All other point-to-point connections in the network are synchronous.
- Circuit costs
  - — The cost for all Ethernet circuits is 3.
  - — The cost for CI circuits is 10.
  - — The cost for synchronous point-to-point circuits is 8.
  - — The cost of the circuit between ALPHA and FOXTRT is 5.
  - — The cost for asynchronous point-to-point circuits is 10.

8. List all available paths between JULIET and ECHO along with their costs and lengths. How will data be routed between them?
9. The path between ECHO and ALPHA is two hops, but the path between ALPHA and ECHO is one hop. Explain this difference.
10. On node ECHO the maximum visits is set to 9, maximum hops is set to 3 and maximum cost is set to 40. If the link between BRAVO and FOXTRT becomes unavailable, several nodes will be unreachable. Which nodes and why?
11. On node BRAVO the maximum cost is set to 25. Which node is potentially unreachable and which link would need to be broken to cause this?

SOLUTIONS TO WRITTEN EXERCISES

1. **What protocol is used for file transfers? At which layer does this protocol reside?**

   The Data Access Protocol (DAP) is used for file transfers. It resides at the Network Application Layer.

2. **Which network management protocol communicates directly with the Data Link Layer, bypassing intermediate layers? Why?**

   The Maintenance Operations Protocol (MOP) communicates directly with the Data Link Layer because it is used to service nodes that are unable to use the services of higher layers.

3. **Which two layers are responsible for logical links? Why is it necessary to have two layers assigned to this task?**

   The End Communication and Session Control layers are responsible for logical links. It is necessary to have two layers perform logical link functions because some of these functions are operating-system dependent, and some are not. The Session Control Layer acts as an interface into the operating system, requesting logical links on the behalf of user and system processes. The End Communication Layer acts independently of the operating system to create and maintain the logical links.

4. **Peer layer protocols allow equivalent layers of remote nodes to communicate logically. Only one layer actually transmits the data. Which one?**

   Only the Physical Layer actually transmits data.

5. **Which layer is responsible for end-to-end transmissions? for transmissions between adjacent nodes?**

   The End Communication Layer is responsible for end-to-end transmissions. The Data Link Layer is responsible for transmissions between adjacent nodes.

6. **How is a level 1 router different from a level 2 (area) router?**

   A level 1 router can only route data within its own area. It does not store any information about the reachability of other areas. A level 2 router not only routes data within its area, but also maintains information about other parts of the network.

7. **Place the following events in the order in which they occur when a user at the source node sends a message to a user at the destination node.**

   The numbers that correspond to the boxes are: 2, 5, 4, 3, 1

8. **List all available paths between JULIET and ECHO along with their costs and lengths. How will data be routed between them?**

   All available paths are listed in Table 2–3:

Table 2–3: Solution to Exercise 8

PATH	COST	LENGTH
JULIET -> INDIA -> FOXTRT -> BRAVO -> ECHO	17	4
JULIET -> INDIA -> FOXTRT -> ALPHA -> ECHO	14	4
JULIET -> INDIA -> FOXTRT -> BRAVO -> ALPHA -> ECHO	27	5
JULIET -> INDIA -> FOXTRT -> ALPHA -> BRAVO -> ECHO	24	5
JULIET -> INDIA -> KILO -> HECTOR -> BRAVO -> ECHO	25	5
JULIET -> INDIA -> KILO -> HECTOR -> BRAVO -> ALPHA -> ECHO	35	6
JULIET -> INDIA -> FOXTRT -> BRAVO -> ECHO	24	4
JULIET -> INDIA -> FOXTRT -> ALPHA -> ECHO	21	4
JULIET -> INDIA -> FOXTRT -> BRAVO -> ALPHA -> ECHO	34	5
JULIET -> INDIA -> FOXTRT -> ALPHA -> BRAVO -> ECHO	31	5
JULIET -> INDIA -> KILO -> HECTOR -> BRAVO -> ECHO	32	5
JULIET -> INDIA -> KILO -> HECTOR -> BRAVO -> ALPHA -> ECHO	42	6

The path selected is the least cost path:

JULIET -> INDIA -> FOXTRT -> ALPHA -> ECHO.

9. **The path between ECHO and ALPHA is two hops, but the path between ALPHA and ECHO is one hop. Explain this difference.**

   ECHO is an end node, and all transmissions from ECHO must go through the designated router; therefore the path length from ECHO to ALPHA is 2. Since ALPHA is a routing node, it can communicate directly with any other node on the Ethernet; therefore the path length from ALPHA to ECHO is 1.

10. **On node ECHO the maximum visits is set to 9, maximum hops is set to 3 and maximu cost is set to 40. If the link between BRAVO and FOXTRT becomes unavailabl several nodes will be unreachable. Which nodes and why?**

    INDIA, JULIET, and LIMA will be unreachable because the path length between ECHO an each of them will be 4.

11. **On node BRAVO the maximum cost is set to 25. Which node is potentially unreachabl and which link would need to be broken to cause this?**

    If the line from BRAVO to HECTOR is unavailable, GOLF will become unreachable becaus the only available path to GOLF will be:

    BRAVO -> FOXTRT -> KILO -> HECTOR -> GOLF

    which has a cost of 27. All other nodes will still be reachable.

MODULE 3
NCP PRIMER

INTRODUCTION

The network manager uses a management tool known as the Network Control Program (NCP) to create, display, and modify component parameters in the DECnet configuration databases. NCP is used to:

- Create, display, and modify configuration database parameters.
- Monitor and test the network.

OBJECTIVES

To use NCP to monitor and control the network, a network manager should be able to:

- Identify and describe the files that make up the network configuration databases.
- Describe the use of NCP in relation to the network configuration databases.
- Use NCP commands to create, display, and modify entries in the volatile and permanent databases.
- Identify which DNA layers are affected by various DECnet parameters.
- Identify important routing and link parameters.

RESOURCES

- *Guide to DECnet-VAX Networking*, (AA-LA47A-TE)
- *VMS Network Control Program Reference Manual*, (AA-LA50A-TE)
- *VMS Networking Manual*, (AA-LA48A-TE)

DECnet CONFIGURATION DATABASES

The DECnet-VAX configuration database consists of two distinct databases:

- The permanent database
- The volatile database

Permanent Database

The permanent database is a collection of files in SYS$SYSTEM that contain the non-volatile value settings for the various NCP parameters. Features of the permanent database are:

- Resides on disk.
- Provides initial values for the volatile database.
- Can be modified by NCP.
- Modifications take effect the next time DECnet software is started up.
- SYSPRV and OPER privileges are needed to access the permanent database.

The Volatile Database

The volatile database is a memory-resident image containing current information about network management components. Features of the volatile database are:

- Allows changes to be made to a running system.
- Can be modified by NCP.
- Changes take effect immediately.
- Values are lost when system is shut down.
- OPER privilege is needed to modify the volatile database.

The Network Configuration Database

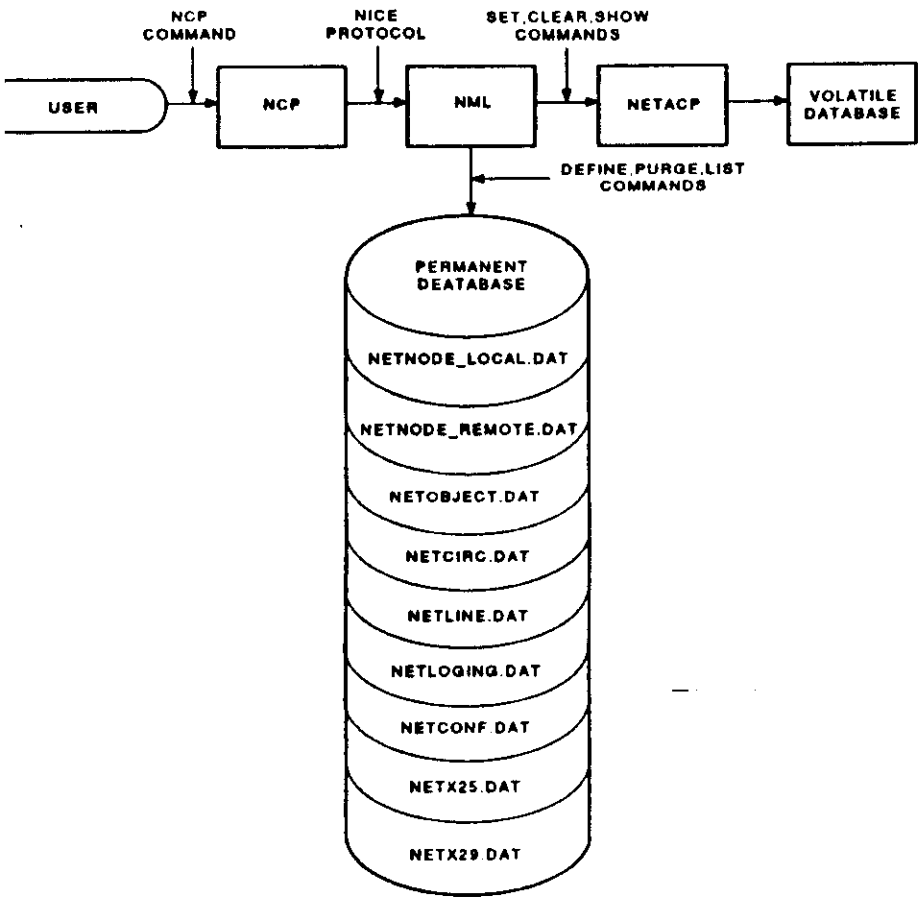
The network configuration database consists of nine files in SYS$SYSTEM.

Table 3–1: Configuration Database Files

FILENAME	DESCRIPTION
NETNODE_LOCAL.DAT	Executor node
NETNODE_REMOTE.DAT	Remote node
NETCIRC.DAT	Circuits known to the local node
NETLINE.DAT	Lines known to the local node
NETOBJECT.DAT	Objects known to the local node
NETLOGING.DAT	Event logging sinks
NETCONF.DAT	Ethernet configurator information
NETX25.DAT	X.25 database and X.25 server information
NETX29.DAT	X.29 server information

gure 3–1 shows how DECnet modules access the databases.

gure 3–1: DECnet Configuration Databases



MKV_X1001_88

NCP COMMAND OVERVIEW

Invoking and Exiting NCP

To invoke NCP:

```
$ RUN SYS$SYSTEM:NCP
NCP>
```

To exit NCP, type the word exit or press CTRL/Z:

```
NCP>EXIT
$
```

Table 3–2 shows the commands that a network manager can use to perform network management tasks:

Table 3–2: Commands that Utilize the Configuration Databases

FUNCTION	VOLATILE	PERMANENT
Create/modify parameters.	SET	DEFINE
Delete parameters.	CLEAR	PURGE
Display parameters.	SHOW	LIST
Down-line loads a node.	LOAD	
Simulates pushing the BOOT button on a remote node.	TRIGGER	
Commands a remote node to do a single command.	TELL	
Performs node and circuit testing.	LOOP	
Initializes node and circuit counters.	ZERO	

DECnet Privileges

You must be logged into a privileged account to access the permanent database or modify the volatile database. Table 3–3 lists the priviliges required for various NCP commands.

Table 3–3: Required DECnet Privileges

COMMAND(S)	PRIVILEGE(S)	REASON
SHOW	None	SHOW does not affect either database, nor does it access the permanent database.
SET, CLEAR	OPER	These commands affect the volatile database only, but must still be used with caution.
LIST	SYSPRV	The LIST command displays information from the permanent database. Only users with system privilege may access the permanent database. To display password information, BYPASS is needed as well.
DEFINE, PURGE	OPER, SYSPRV	These commands manipulate the permanent database. OPER is needed to manipulate any database; SYSPRV is needed to access the permanent database.

General NCP Command Format

All NCP commands take the same general format and consist of three parts:

- A command verb.
- A component on which the command operates.
- One or more parameters that further qualify the action to be taken on the component.

Table 3–4 divides some NCP commands into these three parts. To reconstruct the full command read across the row; for example, the first command is:

```
NCP>SHOW KNOWN OBJECT CHARACTERISTICS
```

Table 3–4: NCP Command Syntax

COMMAND	COMPONENT	PARAMETER
LIST	KNOWN OBJECT	CHARACTERISTICS
SHOW	EXECUTOR	STATUS
SHOW	ACTIVE LINKS	
SHOW	CIRCUIT UNA-0	COUNTERS
SHOW	LOGGING	
CLEAR	EXECUTOR NODE	
SET	NODE PARROT	ADDRESS 26.143
SET	EXECUTOR	NONPRIV USER DECNET PASSWOR DECNET
LOOP	CIRCUIT UNA-0	WITH ONES COUNT 40

Alternative Methods of Entering Commands

There are other ways of entering NCP commands besides typing the entire command from within NCP.

- Recall NCP commands entered earlier in the NCP session using CTRL/B or the arrow keys.
- Enter single NCP commands from DCL by preceding the command with MC NCP:

```
$ MC NCP SHOW ACTIVE LINKS
```

Using Wildcard Characters in NCP

Use wildcard characters in an NCP command line to represent NCP components by a general name, rather than specify each component individually:

The asterisk (*) is used to represent a string of characters.

The percent sign (%) is used to represent a single character.

Wildcards can represent the following component :

— Node name

— Node address

— Circuit identifier

— Line identifier

— Object name

— Events

The following rules apply to wildcard usage:

For node and object names, a wildcard can represent part or all of the name, and it may appear anywhere in the string.

If the component name is an alphanumeric string, for example, DMC-0, the wildcard character can represent either the entire name or the numeric element. The wildcard should be used alone or it should appear at the end of the component name; there should be no characters following it.

For node addresses and events, which are formatted, the wildcard should only appear after the period separating the two parts. Furthermore, it should not represent a partial number.

NOTE

These are the rules presented in the *NCP Reference Manual*. In practice, some of the commands that the manual says not to use produce the expected results. However, if you follow the rules, the commands are *certain* to produce the correct results.

Example 3–1 illustrates the correct usage of wildcard characters.

Example 3–1: Using Wildcards in NCP Command Strings

```
NCP>SHOW NODE 5* ❶

Node Volatile Summary as of 29-SEP-1988 15:40:37

    Node            State      Active  Delay   Circuit      Next node
                               Links

 5.214 (SPIDER)                                QNA-0         26.133
 6.137 (STAR)                                  QNA-0         26.133
26.25 (SPRITE)                                 QNA-0         26.133
26.130 (SWSVAX)                                QNA-0         26.133

NCP>LIST CIRCUIT * ❷

Known Circuit Permanent Summary as of 29-SEP-1988 15:40:59

   Circuit          State

  QNA-0             on
NCP>
NCP>SHOW OBJ %%L CHAR ❸

Object Volatile Characteristics as of 29-SEP-1988 15:44:19

Object = FAL

Number                    = 17
File id                   = FAL.EXE

Object = NML

Number                    = 19
File id                   = NML.EXE

Object = EVL

Number                    = 26
Process id                = 00000029

NCP>SHOW CIRCUIT QNA-% CHAR ❹

Circuit Volatile Characteristics as of 29-SEP-1988 15:44:53

Circuit = QNA-0

State                     = on
Service                   = disabled
Designated router         = 26.133
Cost                      = 4
Router priority           = 64
Hello timer               = 15
Type                      = Ethernet
Adjacent node             = 26.133
Listen timer              = 45
```

EXECUTING REMOTE COMMANDS

Most NCP commands issued on the local node are executed on that node. Occasionally, you may want to issue commands from the local node to be executed on remote nodes.

- The executor node is the node on which NCP functions are actually performed.
- To perform network management functions on remote nodes, NCP supports two commands:
  - SET EXECUTOR NODE
  - TELL

Setting an Executor Node

The SET EXECUTOR NODE command allows you to choose the node at which you want NCP commands to execute, as illustrated in Example 3–2.

Example 3–2: Setting an Executor Node

```
NCP>SHOW EXECUTOR (1)

Node Volatile Summary as of 9-SEP-1988 14:57:39

Executor node = 26.60 (LUIGI)

State                     = on
Identification            = DECnet-VAX V5.0, VMS V5.0

NCP>SET EXECUTOR NODE BOSTON (2)
NCP>SHOW EXECUTOR (3)

Node Volatile Summary as of 9-SEP-1988 14:57:55

Executor node = 2.7 (BOSTON)

State                     = on
Identification            = DECnet-VAX V5.0, VMS V5.0

NCP>CLEAR EXECUTOR NODE (4)
NCP>SHOW EXECUTOR

Node Volatile Summary as of 9-SEP-1988 14:58:34

Executor node = 26.60 (LUIGI)

State                     = on
Identification            = DECnet-VAX V5.0, VMS V5.0
```


The SHOW EXECUTOR CHARACTERISTICS command displays information about the executor node, as illustrated in Example 3–3

Example 3–3: SHOW EXECUTOR CHARACTERISTICS Command

```
NCP>SHOW EXECUTOR CHARACTERISTICS

Node Volatile Characteristics as of 9-SEP-1988 15:01:30

Executor node = 26.60  (LUIGI)

Identification            = DECnet-VAX V5.0,  VMS V5.0 (1)
Management version        = V4.0.0
Incoming timer            = 45
Outgoing timer            = 45
Incoming Proxy            = Enabled (2)
Outgoing Proxy            = Enabled (2)
NSP version               = V4.0.0
Maximum links             = 32
Delay factor              = 80
Delay weight              = 5
Inactivity timer          = 60
Retransmit factor         = 10
Routing version           = V2.0.0
Type                      = nonrouting IV (2)
Routing timer             = 600
Broadcast routing timer   = 40
Maximum address           = 1023
Maximum circuits          = 16
Maximum cost              = 1022
Maximum hops              = 15
Maximum visits            = 20
Maximum area              = 63
Max broadcast nonrouters  = 64
Max broadcast routers     = 32
Maximum path splits       = 1 (1)
Area maximum cost         = 1022
Area maximum hops         = 30
Maximum buffers           = 100
Buffer size               = 576
Nonprivileged user id     = DECNET
Nonprivileged password    = DECNET
Default access            = incoming and outgoing
Pipeline quota            = 3000
Alias Maximum Links       = 32
Path Split Policy         = Normal (1)
```

Indicating Access Control for Remote Command Execution

With the SET EXECUTOR NODE command, you can specify access control information to obtain privileged information about a remote node, as shown in Example 3–4.

Example 3–4: Using Access Control for Remote Command Execution

```
NCP>SET EXEC NODE LUIGI"SYSTEM CHOCOLATE"
NCP>DEFINE NODE VIOLET ADDRESS 55.56
NCP>SET NODE VIOLET ALL
NCP>LIST EXEC CHAR

Node Permanent Characteristics as of 29-SEP-1988 18:34:42

Executor node = 26.60 (LUIGI)

Management version       = V4.0.0
Type                     = nonrouting IV
Maximum address          = 1023
Nonprivileged user id    = DECNET
Nonprivileged password   = DECNET
```

TELL Command

The TELL command is an alternative to the SET EXECUTOR NODE command. Use the TELL command to:

- Execute only a single command at a remote node.
- Temporarily override the current executor.

Example 3–5 illustrates the use of the TELL command.

Example 3–5: Using the TELL Command

```
NCP>CLEAR EXECUTOR NODE ❶
NCP>SHOW EXECUTOR ❷

Node Volatile Summary as of 29-SEP-1988 18:53:01

Executor node = 26.60 (LUIGI)

State                    = on
Identification           = DECnet-VAX V5.0,  VMS V5.0

NCP>TELL PARROT SHOW EXEC CHAR ❸

Node Volatile Characteristics as of 29-SEP-1988 18:53:18

Executor node = 26.163 (PARROT)

Identification           = DECnet-VAX V4.7,  VMS V4.7
Management version       = V4.0.0
Incoming timer           = 45
.
.
.
Alias incoming           = Enabled
Alias maximum links      = 32
Alias node               = 26.24 (DEMON)

NCP>SHOW EXEC ❹

Node Volatile Summary as of 29-SEP-1988 18:53:26

Executor node = 26.60 (LUIGI)

State                    = on
Identification           = DECnet-VAX V5.0,  VMS V5.0
```

BUILDING THE CONFIGURATION DATABASE

This section describes how to use NCP node commands, line commands, circuit commands, and object commands to configure nodes in a DECnet network.

Node Commands

To configure an operational network at the local node:

- Set the operational state of the local node.
- Create database entries of remote nodes with which your users expect to communicate.

Setting the Operational State of Your Local Node

The operational state of a node determines the extent to which that node can participate in the network. Use the STATE parameter in conjunction with the SET EXECUTOR command to exercise control over the operational state of the local node. Table 3–5 describes the four states associated with this parameter.

Table 3–5: Operational States of Nodes

STATE	FUNCTION
OFF	Allows no new logical links to be created; terminates existing links, and stops route-through traffic.
ON	Allows new logical links to be created. The ON state is the normal operational state allowing route-through traffic.
RESTRICTED	Allows no new logical links from other nodes, yet does not inhibit route-through traffic.
SHUT	Similar to RESTRICTED. However, once all logical links are terminated, the local node goes to the OFF state.

Adding Remote Nodes to Your Configuration Database

Example 3–6 shows how to add a remote node to the configuration database.

Example 3–6: Adding a remote node

```
NCP>SHOW KNOWN NODES ❶

Known Node Volatile Summary as of  9-SEP-1988 11:23:44

Executor node = 26.60 (LUIGI)

State                     = on
Identification            = DECnet-VAX V5.0,  VMS V5.0

    Node           State      Active  Delay   Circuit     Next node
                              Links

 4.20 (FIGMEN)                                QNA-0       26.15 (CYCLPS)
24.29 (ANCHOR)                                QNA-0       26.15 (CYCLPS)
26.15 (CYCLPS)                                QNA-0       26.15 (CYCLPS)
26.24 (DEMON)                                 QNA-0       26.15 (CYCLPS)
26.25 (SPRITE)                                QNA-0       26.15 (CYCLPS)
26.49 (PILGRM)                                QNA-0       26.15 (CYCLPS)
26.61 (ENT)                    1        1     QNA-0       26.15 (CYCLPS)
26.89 (WENDI)                                 QNA-0       26.15 (CYCLPS)
26.130 (SWSVAX)                               QNA-0       26.15 (CYCLPS)
26.143 (PARROT)                               QNA-0       26.15 (CYCLPS)
26.148 (TBD3)                                 QNA-0       26.15 (CYCLPS)
26.190 (ZODIAC)                               QNA-0       26.15 (CYCLPS)
26.281 (RAPTOR)                               QNA-0       26.15 (CYCLPS)
42.240 (LESLIE)                               QNA-0       26.15 (CYCLPS)
42.398 (RDGENG)                               QNA-0       26.15 (CYCLPS)

NCP>SET NODE 3.4 NAME TOYS ❷

NCP>SHOW KNOWN NODES

Known Node Volatile Summary as of  9-SEP-1988 11:24:09

Executor node = 26.60 (LUIGI)

State                     = on
Identification            = DECnet-VAX V5.0,  VMS V5.0

    Node           State      Active  Delay   Circuit     Next node
                              Links

 3.40 (TOYS)                                  QNA-0       26.15 (CYCLPS) ❸
 4.20 (FIGMEN)                                QNA-0       26.15 (CYCLPS)
24.29 (ANCHOR)                                QNA-0       26.15 (CYCLPS)
26.15 (CYCLPS)                                QNA-0       26.15 (CYCLPS)
26.24 (DEMON)                                 QNA-0       26.15 (CYCLPS)
26.25 (SPRITE)                                QNA-0       26.15 (CYCLPS)
26.49 (PILGRM)                                QNA-0       26.15 (CYCLPS)
26.61 (ENT)                    1        1     QNA-0       26.15 (CYCLPS)
26.89 (WENDI)                                 QNA-0       26.15 (CYCLPS)
26.130 (SWSVAX)                               QNA-0       26.15 (CYCLPS)
26.143 (PARROT)                               QNA-0       26.15 (CYCLPS)
26.148 (TBD3)                                 QNA-0       26.15 (CYCLPS)
26.190 (ZODIAC)                               QNA-0       26.15 (CYCLPS)
26.281 (RAPTOR)                               QNA-0       26.15 (CYCLPS)
42.240 (LESLIE)                               QNA-0       26.15 (CYCLPS)
42.398 (RDGENG)                               QNA-0       26.15 (CYCLPS)
```

Copying Known Nodes

As new nodes are added to the network, it is the network/system manager's responsibility to create a list of remote nodes in the local database. The system manager on the newly installed node can:

Manually type a separate command for each node that needs to be defined.

Use the COPY KNOWN NODES command.

The COPY KNOWN NODES command copies the names and addresses of remote nodes from a remote database to your local node's database. Follow these steps to use the COPY KNOWN NODES command:

1. Add a node to your database that has a complete list of node definitions.

```
NCP>SET NODE 2.4 NAME COOKIE
```

2. To copy the remote node information from node nnnn, use one of the following:

```
NCP>COPY KNOWN NODES FROM nnnn USING VOLATILE
NCP>COPY KNOWN NODES FROM nnnn USING PERMANENT
NCP>COPY KNOWN NODES FROM nnnn USING PERMANENT TO BOTH
```

   For example, to copy the information to your volatile database from node COOKIE, issue the following command:

```
NCP>COPY KNOWN NODES FROM COOKIE USING VOLATILE
```

3. Use the SHOW KNOWN NODES command to ensure that the remote nodes are defined to your system.

Removing a Node from the Database

Sometimes it is necessary to remove information about a remote node from your remote node database. Use the CLEAR and PURGE commands to accomplish this.

Example 3–7 demonstrates how to remove a node from the volatile database.

Example 3–7: Removing a Node from the Database

```
NCP>SHOW NODE ZODIAC (1)

Node Volatile Summary as of 26-SEP-1988 16:28:10

    Node            State       Active  Delay   Circuit      Next node
                                Links

26.190 (ZODIAC)                                 QNA-0         26.133
NCP>
NCP>CLEAR NODE ZODIAC ALL (2)
NCP>
NCP>SHOW NODE ZODIAC (3)

Node Volatile Summary as of 26-SEP-1988 16:28:30

%NCP-W-UNRCMP, Unrecognized component , Node
```

Changing Remote Node Entries

You can change a remote node's node name or node address by first deleting the remote node from your node's database and then redefining the remote node.

If node WENDI moves to a different location on the network, you can change its address in your database by issuing the commands shown in Example 3–8.

Example 3–8: Changing a Remote Node Entry

```
NCP>SHOW NODE WENDI ❶

Node Volatile Summary as of 27-SEP-1988 10:18:00

    Node            State       Active  Delay   Circuit      Next node
                                Links

26.89 (WENDI)                               QNA-0         26.133
NCP>
NCP>CLEAR NODE WENDI ALL ❷
NCP>SET NODE 4.118 NAME WENDI ❸
NCP>SHOW NODE WENDI

Node Volatile Summary as of 27-SEP-1988 10:19:02

    Node            State       Active  Delay   Circuit      Next node
                                Links

 4.118 (WENDI)                              QNA-0         26.133 ❹
NCP>
```

Changing the Executor's Node Address

When you start up the network, the executor's node address is set in the volatile database and cannot be changed unless the system is rebooted. To change the address of the executor node:

1. Make sure the name and address you want to use are not already in use:

```
NCP>PURGE NODE 26.60 ALL
NCP>PURGE NODE LUIGI ALL
```

2. Modify the permanent database by issuing these commands:

```
NCP>DEFINE EXECUTOR ADDRESS 26.60
NCP>DEFINE EXECUTOR NAME LUIGI
```

3. Shut down the network and restart it:

```
NCP>SET EXECUTOR STATE OFF
NCP>SET EXECUTOR STATE ON
```

Line Commands

Lines are the physical data communication paths between nodes. The network manager can use NCP commands to manipulate the physical lines connected to the local node, or to add a line without reconfiguring the node.

Identifying Lines

Every line on a node must have a unique identifier. A line identifier is in the format:

dev-c[-u]

The parts of the line identifier are explained in Table 3–6.

Table 3–6: Line Identification

PART	FUNCTION
dev	Represents a communications interface device name such as UNA or DMC.
c	Represents a decimal number (0 or a positive integer) designating the device's hardware controller.
u	Represents a decimal unit or line number (0 or a positive integer) included if the device is a multiple unit line controller.

Example 3–9: Identifying Lines

```
NCP>SHOW KNOWN LINES

Known Line Volatile Summary as of  9-SEP-1988 11:39:09

   Line             State

 QNA-0              on
```

Setting the Operational State of Lines

The STATE parameter controls the operational state of lines. There are three possible line states as shown in Table 3–7.

Table 3–7: Operational State of Lines

STATE	FUNCTION
OFF	Allows no traffic over a line. The line is unavailable for network activity.
ON	Allows traffic over the line. Allows complete route-through and down-line loading operations. This is the normal operational state.
SERVICE	Reserves the line for service functions (up-line dumping, down-line loading, or line-level loopback testing.)

Use the STATE parameter in conjunction with the SET LINE command to specify the state of a line, as shown in Example 3–10.

Example 3–10: Known Line Status

```
NCP>SET LINE DMC-0 STATE ON ❶
NCP>SHOW KNOWN LINE STATUS ❷

Known Line Volatile Status as of 12-SEP-1988

   Line             State

 DMC-0              on
 DMC-1              off
 UNA-0              on
```

Displaying Line Characteristics

The configuration database contains line parameters for all physical lines connected to a node. These parameters supply information to control various aspects of a line's operation. When a line is defined, DECnet software automatically assigns default values for the parameters not specified.

Example 3–11 illustrates the SHOW KNOWN LINE CHARACTERISTICS command.

Example 3–11: SHOW KNOWN LINE CHARACTERISTICS Command

```
NCP>SHOW KNOWN LINE CHARACTERISTICS

Known Line Volatile Characteristics as of 4-OCT-1988  14:46:51

Line = QNA-0

Receive buffers          = 6 (1)
Controller               = normal (2)
Protocol                 = Ethernet (3)
Service timer            = 4000 (4)
Hardware address         = 08-00-2B-03-F7-B3 (5)
Buffer size              = 1498 (6)
```


Circuit Commands

Circuits are virtual connections between nodes. The network manager can use NCP commands to manipulate all circuits connected to the local node or to add a circuit without reconfiguring the node.

Identifying Circuits

Each circuit on a node must have a unique identifier. A circuit identifier is in the format:

dev-c or dev-c-u or dev-c.t

Table 3–8 explains the parts of the circuit identification.

Table 3–8: Circuit Identification

PART	FUNCTION
dev	Represents a communications interface device name.
c	Represents a decimal number (0 or a positive integer) designating the hardware controller for the device.
u	Represents a decimal unit or circuit number included only if there is more than one unit associated with the controller.
t	Represents a decimal number identifying a tributary on a multipoint circuit. This is a logical tributary number, not to be confused with the address used to poll the tributary.

To display the circuits connected to a node, use the SHOW KNOWN CIRCUITS command, as illustrated in Example 3–12.

Example 3–12: Showing Known Circuits

```
NCP>SHOW KNOWN CIRCUITS

Known Circuit Volatile Summary as of 12-SEP-1988 11:51:20
   Circuit          State                 Loopback      Adjacent
                                            Name      Routing Node
  QNA-0             on                                26.15 (CYCLPS)
```

Setting the Operational State of Circuits

The STATE parameter controls the operational state of circuits. Table 3–9 shows the four possible states.

Table 3–9: Operational States of Circuits

STATE	FUNCTION
OFF	Allows no traffic over a circuit. The circuit is unavailable for network activity.
ON	Allows traffic over the circuit. Allows for complete route-through and down-line loading operations. This is the normal operational state.
SERVICE	Reserves the circuit for service functions (up-line dumping, down-line loading, or line-level loopback testing). Only an Ethernet circuit allows logical link activity or route-through at the same time as service operations.
CLEARED	Applies only to X.25 circuits. The X.25 circuit does not exist in the volatile database when PSI is loaded.

Example 3–13 shows the use of the STATE parameter with the SET CIRCUIT command.

Example 3–13: Manipulating Circuit Status

```
NCP>SET CIRCUIT DMC-0 STATE ON ❶
NCP>SHOW KNOWN CIRCUIT STATUS ❷

Known Circuit Volatile Status as of 13-SEP-1988 14:10:28

 Circuit       State          Loopback      Adjacent        Block
                                Name         Node            Size

  DMC-0          on                       2.1 (BONGO)        576
  DMC-1          on                       4.13 (MANGO)       576
  UNA-0          on                       5.149 (TROPIC)    1498
```


Displaying Circuit Characteristics

The configuration database should contain circuit parameters for all circuits connected to a node. These parameters supply information used to control various aspects of a circuit's operation. When a circuit is defined, DECnet software automatically assigns default values for the parameters not specified.

Example 3–14 illustrates the SHOW KNOWN CIRCUIT CHARACTERISTICS command.

Example 3–14: Circuit Characteristics

```
NCP>SHOW KNOWN CIRCUIT CHARACTERISTICS

Known Circuit Volatile Characteristics as of 13-SEP-1988 15:15:02

Circuit = DMC-0

State                     = on ❶
Substate                  = starting ❷
Service                   = enabled ❸
Cost                      = 5 ❹
Hello timer               = 15 ❺
Verification              = disabled ❻

Circuit = UNA-0

State                     = on
Service                   = enabled
Designated router         =  2.1 (OSCAR) ❼
Cost                      = 3
Router priority           = 64 ❽
Hello timer               = 15
Type                      = Ethernet ❾
Adjacent node             =  2.1 (OSCAR) ❿
Listen timer              = 45 ⓫
```

NOTE

A network manager should *not* alter the circuit parameter values without good reason. The proper setting of circuit parameters greatly affects network performance. Changing circuit, line, and node parameter values to improve network performance is discussed in the Monitoring and Tuning module of this course.

ROUTING PARAMETERS

Routing is the network function that determines the path or route along which data (in packets) travels to its destination. Values for each of the following parameters are displayed by the SHOW EXECUTOR CHARACTERISTICS command, as Example 3–15 illustrates.

Example 3–15: Routing Parameters

```
NCP>SHOW EXEC CHAR

Node Volatile Characteristics as of  4-OCT-1988 17:41:39

Executor node = 26.148 (TBD3)

Identification            = DECnet-VAX V5.0,  VMS V5.0
Management version        = V4.0.0
Incoming timer            = 45
Outgoing timer            = 60
Incoming Proxy            = Enabled
Outgoing Proxy            = Enabled
NSP version               = V4.0.0
Maximum links             = 32
Delay factor              = 80
Delay weight              = 5
Inactivity timer          = 60
Retransmit factor         = 10
Routing version           = V2.0.0
Type                      = nonrouting IV (1)
Routing timer             = 600 (2)
Broadcast routing timer   = 180 (3)
Maximum address           = 1023 (4)
Maximum circuits          = 16 (5)
Maximum cost              = 1022 (6)
Maximum hops              = 30 (7)
Maximum visits            = 63 (8)
Maximum area              = 63 (9)
Max broadcast nonrouters  = 64 (10)
Max broadcast routers     = 32 (11)
Maximum path splits       = 1 (12)
Area maximum cost         = 1022 (13)
Area maximum hops         = 30 (14)
Maximum buffers           = 100
Buffer size               = 576
Nonprivileged user id     = DECNET
Default access            = incoming and outgoing
Pipeline quota            = 3000
Alias maximum links       = 32
Path split policy         = Normal (15)
```


The following notes refer to Example 3–15.

(1) NODE TYPES—Nonrouter versus router versus area router.

(2) ROUTING TIMER—Triggers routing update messages on a nonEthernet circuit.

(3) BROADCAST ROUTING TIMER—Triggers routing update messages on an Ethernet circuit.

(4) MAXIMUM ADDRESS—The largest address recognized by the local node.

(5) MAXIMUM CIRCUITS—The maximum number of routing circuits that the local node can use.

(6) MAXIMUM COST—Maximum cost permitted for the total path between source and destination nodes.

(7) MAXIMUM HOPS—Maximum number of hops permitted in a given path.

(8) MAXIMUM VISITS—Maximum number of nodes a packet can visit before arriving at the destination node.

(9) MAXIMUM AREA—Maximum number of areas recognized by the executor node.

(10) MAXIMUM BROADCAST NONROUTERS—Maximum number of end nodes to which the local node can be attached via its Ethernet circuits.

(11) MAXIMUM BROADCAST ROUTERS—Maximum number of routers to which the local node can be attached via its Ethernet circuits.

(12) MAXIMUM PATH SPLITS—The maximum number of equal cost paths to a given destination among which the packet load may be split.

(13) AREA MAXIMUM COST—Maximum cost of circuits on the path between level 2 routers.

(14) AREA MAXIMUM HOPS—Maximum number of hops between level 2 routers.

(15) PATH SPLIT POLICY—Indicates the policy for equal cost path splitting. NORMAL indicates that all traffic will be split over equal cost paths. INTERIM forces packets for individual network sessions to follow the same path—necessary when communicating with nodes that do not support out-of-order packet caching.

LINK PARAMETERS

A logical link is a temporary data path created between two processes. The link exists until one of the processes terminates the connection. The following parameters govern the establishment and maintenance of logical links. Values for each of these parameters are displayed by the SHOW EXECUTOR CHARACTERISTICS command, as Example 3–16 illustrates.

Example 3–16: Link Parameters

```
NCP>SHOW EXECUTOR CHARACTERISTICS

Node Volatile Characteristics as of  4-OCT-1988 17:41:47

Executor node = 26.148 (TBD3)

Identification            = DECnet-VAX V5.0,  VMS V5.0
Management version        = V4.0.0
Incoming timer            = 45 ❶
Outgoing timer            = 60 ❷
Incoming Proxy            = Enabled
Outgoing Proxy            = Enabled
NSP version               = V4.0.0
Maximum links             = 32 ❸
Delay factor              = 80 ❹
Delay weight              = 5  ❺
Inactivity timer          = 60 ❻
Retransmit factor         = 10 ❼
Routing version           = V2.0.0
Type                      = nonrouting IV
Routing timer             = 600
Broadcast routing timer   = 180
Maximum address           = 1023
Maximum circuits          = 16
Maximum cost              = 1022
Maximum hops              = 30
Maximum visits            = 63
Maximum area              = 63
Max broadcast nonrouters  = 64
Max broadcast routers     = 32
Maximum path splits       = 1
Area maximum cost         = 1022
Area maximum hops         = 30
Maximum buffers           = 100
Buffer size               = 576
Nonprivileged user id     = DECNET
Default access            = incoming and outgoing
Pipeline quota            = 3000 ❽
Alias maximum links       = 32   ❾
Path split policy         = Normal
```

The following notes refer to Example 3–16.

❶ INCOMING TIMER—Maximum duration between receipt and accept/reject of a logical link.

❷ OUTGOING TIMER—Maximum duration between request and acknowledgment of a logical link.

❸ MAXIMUM LINKS—Maximum number of active logical links.

❹ DELAY FACTOR—Time value for retransmission of network services protocol (NSP) messages.

❺ DELAY WEIGHT—Value of estimated round trip delay.

❻ INACTIVITY TIMER—Maximum duration of inactivity before a link is tested for viability.

❼ RETRANSMIT FACTOR—Number of times NSP will retransmit.

❽ PIPELINE QUOTA—Maximum number of bytes of nonpaged pool used for network transmissions.

❾ ALIAS MAXIMUM LINKS—Maximum number of links to a cluster alias.

SUMMARY

Every DECnet node has a configuration database that defines characteristics of that node and determines how it functions within the network. In DECnet-VAX implementations, this configuration database is provided within the DECnet software supplied by DIGITAL.

To provide network management flexibility, each node's database consists of two distinct databases:

- Permanent (fixed) database
- Volatile (temporary) database

The Network Control Program is a network management tool to create, display, and modify component parameters in the DECnet configuration databases. NCP is used to:

- Monitor and test the network.
- Create, display, and modify permanent and volatile database parameters for DECnet-VAX systems.

For added flexibility in network management, NCP incorporates the concept of an executor node. The executor node is the node on which NCP functions are actually performed. To perform network management functions on remote nodes, NCP supports two commands:

- SET EXECUTOR NODE
- TELL

Node, line, and circuit commands help network managers to configure a node properly in the DECnet network. The SET/DEFINE NODE command is used to add a remote node to your system's configuration database. The COPY KNOWN NODES command eliminates the need to manually add entries for remote nodes to the database. This command copies the remote node entries from another node's configuration database.

WRITTEN EXERCISES

1. Because of a serious disk failure, your system disk has to be rebuilt from a backup tape. After the rebuild is complete, you want to verify that all of the files that comprise the network configuration database have been restored properly and that the correct protection is set on them. Where should you look, and what protection mask should be set?

2. Information contained in the volatile database is dynamic while information in the permanent database is static. Based on this fact, which database is located on a disk and which is in memory?

3. You have been asked to add a new VAX to your network and the node name is to be PARIS. Describe the steps necessary to ensure that the node name and address are unique, and what command you will use to add PARIS to your permanent database?

4. Study the following example. Of the circuits shown, which are indicating that they are operating in the normal condition?

```
NCP>SHOW KNOWN CIRCUIT STATUS

Known Circuit Volatile Status as of 01-NOV-1988 12:15:23

 Circuit       State          Loopback Name    Adjacent Node      Block Size

 DMC-0         on                              1.8 (MANGO)        576
 DMC-1         off
 UNA-0         service                         2.1 (BONGO)        576
 UNA-1         on                              5.149 (BIKINI)     576
 UNA-2         cleared                         6.150 (TANGO)      576
```

5. A user has received mail from a user named SANCHEZ on the node ALPHA, but after trying to respond, received an error message indicating that there was no such account on node ALPHA. Upon investigation, you discover that the node address for node ALPHA is defined differently by three different nodes in your network. How would you rectify this situation? What steps can you take to avoid this situation altogether?

6. Node TANGO, a VAX/VMS node, has just been added to the network. Assume that you are the system/network manager on node TANGO and currently logged in to an account that has SYSPRV and OPER privileges. Write the command(s) to use, from your account on TANGO to perform each of the following operations:

   a. Add node YANKEE (address 2.10) to TANGO's permanent and volatile databases.

   b. Find the names of the remote nodes in node YANKEE's volatile database.

   c. Copy the remote node names and addresses from node YANKEE's volatile database into node TANGO's permanent and volatile databases.

   d. Delete remote node ZULU (address 2.22) from node TANGO's permanent and volatile database.

   e. Set node TANGO's operational state (in the volatile database) so that route-through traffic continues on node TANGO, and established logical links remain, but no new logical links can be created.

SOLUTIONS TO WRITTEN EXERCISES

1. **Because of a serious disk failure, your system disk has to be rebuilt from a backup tape. After the rebuild is complete, you want to verify that all of the files that comprise the network configuration database have been restored properly and that the correct protection is set on them. Where should you look, and what protection mask should be set?**

   The files should be in SYS$SYSTEM and the protection should be (S:RWED,O:RWED,G,W)

2. **Information contained in the volatile database is dynamic while information in the permanent database is static. Based on this fact, which database is located on a disk and which is in memory?**

   The volatile database is memory resident, and the permanent database is on disk.

3. **You have been asked to add a new VAX to your network and the node name is to be PARIS. Describe the steps necessary to ensure that the node name and address are unique, and what command you will use to add PARIS to your permanent database?**

   a. Find out whether the node name already exists.

      ```
      NCP>SHOW NODE PARIS
      ```

   b. Find out whether the node address already exists.

      ```
      NCP>SHOW NODE address
      ```

   c. Add the node to the permanent database.

      ```
      NCP>DEFINE NODE address NAME PARIS
      ```

4. **Study the following example. Of the circuits shown, which are indicating that they are operating in the normal condition?**

```
NCP>SHOW KNOWN CIRCUIT STATUS

Known Circuit Volatile Status as of 01-NOV-1988 12:15:23

 Circuit       State          Loopback Name   Adjacent Node          Block Size

  DMC-0        on                             1.8 (MANGO)             576
  DMC-1        off
  UNA-0        service                        2.1 (BONGO)             576
  UNA-1        on                             5.149 (BIKINI)          576
  UNA-2        cleared                        6.150 (TANGO)           576
```

   Only DMC-0 and UNA-1 are in the normal state. The ON state allows for complete route-through and downline loading operations.

5. A user has received mail from a user named SANCHEZ on the node ALPHA, but after trying to respond, received an error message indicating that there was no such account on node ALPHA. Upon investigation, you discover that the node address for node ALPHA is defined differently by three different nodes in your network. How would you rectify this situation? What steps can you take to avoid this situation altogether?

   Log in to node ALPHA directly, and issue the SHOW EXECUTOR COMMAND to determine the correct address for the node. Then log in to each of the nodes that had ALPHA erroneously defined and enter the following commands:

```
NCP>PURGE NODE ALPHA ALL
NCP>DEFINE NODE ALPHA ADDRESS correct address
NCP>SET NODE ALPHA ALL
```

   To completely avoid the situation, it is a good idea to have at least one node in your network with a complete and accurate node database. Whenever system managers add a new remote node entry to their configuration databases, the node address should be verified in the master list. Whenever a new node is added to the network, the network manager should be notified so that this master database can be updated.

6. Node TANGO, a VAX/VMS node, has just been added to the network. Assume that you are the system/network manager on node TANGO and currently logged in to an account that has SYSPRV and OPER privileges. Write the command(s) to use, from your account on TANGO to perform each of the following operations:

   a. Add node YANKEE (address 2.10) to TANGO's permanent and volatile databases.

```
NCP>DEFINE NODE 2.10 NAME YANKEE (permanent database)
NCP>SET NODE 2.10 NAME YANKEE (volatile database)
```

   b. Find the names of the remote nodes in node YANKEE's volatile database.

```
NCP>TELL YANKEE SHOW KNOWN NODES

or

NCP>SET EXECUTOR NODE YANKEE
NCP>SHOW KNOWN NODES
NCP>CLEAR EXECUTOR NODE
```

   c. Copy the remote node names (and addresses) from node YANKEE's volatile database into node TANGO's permanent and volatile databases.

```
NCP>COPY KNOWN NODES FROM YANKEE USING VOLATILE TO BOTH
```

   d. Delete remote node ZULU (address 2.22) in node TANGO's permanent and volatile database.

```
NCP>PURGE NODE ZULU ADDRESS 2.22 ALL (permanent database)
NCP>CLEAR NODE ZULU ADDRESS 2.22 ALL (volatile database)
```

   e. Set node TANGO's operational state (in the volatile database) so that route-through traffic continues on node TANGO, and established logical links remain, but no new logical links can be created.

```
NCP>SET EXECUTOR NODE STATE RESTRICTED
```

LABORATORY EXERCISES

Use NCP to find out the following:

1. What are the node addresses for all active nodes?
2. Which of the nodes in your network are end nodes?
3. Are any of the nodes area routers?
4. Which OBJECT number corresponds to the PHONE image?
5. How many active lines are connected to each node?
6. Which of the nodes are Q-BUS based?
7. How many links are active from your node now?
8. What is the value of MAXIMUM VISITS for your node?
9. Draw a map of the network with node names, node types and all lines.
10. Update your map to include the COST and HOPS from your node to any other in the network.

SOLUTIONS TO LABORATORY EXERCISES

The answers to the questions will vary depending upon the system you are using. The solution provides a set of commands to use to answer the questions. There may be additional commands that would also work.

1. **What are the node addresses for all active nodes?**

   Use the SHOW ACTIVE NODES command in NCP.

2. **Which of the nodes in your network are end nodes?**

   End nodes are also known as nonrouting nodes. To determine which nodes are nonrouters, use the SHOW EXECUTOR CHARACTERISTICS command in NCP, and examine the TYPE parameter. To find the TYPE of remote nodes, use the TELL or SET EXECUTOR NODE commands.

3. **Are any of the nodes area routers?**

   If any node in the network is an area router, its TYPE will be area. Use the same procedure you used to answer the previous question.

4. **Which OBJECT number corresponds to the PHONE image?**

   DECnet software supports process-to-process communication. The process to which a logical link is connected is called an object. There are objects associated with most network operations, including MAIL and PHONE. To display a list of all the objects defined on your node, use the SHOW KNOWN OBJECTS command in NCP. The output includes the object number for the PHONE image.

5. **How many active lines are connected to each node?**

   To determine which lines are active on each node, use the TELL command and the SHOW ACTIVE LINES command within NCP.

6. **Which of the nodes are Q-BUS based?**

   If a node is Q-BUS based, it will use a QNA, and the circuit-id will be QNA-n. Use the SHOW KNOWN CIRCUITS command, along with the TELL command to find the nodes with QNA circuits.

7. **How many links are active from your node now?**

   To determine which logical links to your node are active, use either the SHOW KNOWN LINKS CHARACTERISTICS or SHOW KNOWN LINKS STATUS command. Examine the state parameter; if the link is active, the state will be run.

8. **What is the value of MAXIMUM VISITS for your node?**

   Examine the MAXIMUM VISITS parameter in the output to the SHOW EXECUTOR CHARACTERISTICS command.

9. **Draw a map of the network with node names, node types and all lines.**

   The commands to use to build your map include: SHOW KNOWN NODES, SHOW EXECUTOR CHARACTERISTICS, SHOW KNOWN LINES, and TELL.

10. **Update your map to include the COST and HOPS from your node to any other in the network.**

    To update your map with circuit costs, use the TELL and SHOW KNOWN CIRCUIT CHARACTERISTICS commands. To determine the actual number of hops taken between your node and any other in the network, trace the path, and count the number of hops.

MODULE 4
DECNET-VAX NODE CONFIGURATION

INTRODUCTION

The Network Manager is responsible for the configuration of DECnet software on all host nodes in the network. With Version 5.0 of VMS, this involves registering the DECnet license on the system by supplying information using a Product Authorization Key (PAK) as input, and running the VMSLICENSE.COM utility.

This may be done on:

- Nodes running as part of an MI-cluster
- Single (nonclustered) nodes
- A new node in an existing network

OBJECTIVES

To configure and check out DECnet-VAX software successfully, a network manager should be able to:

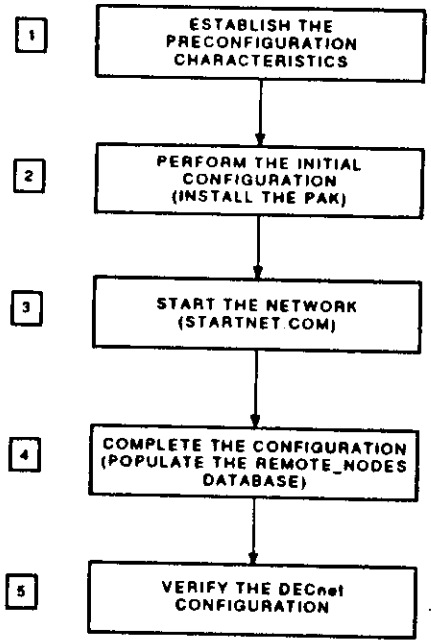
- Set up the proper conditions for configuration.
- Register the DECnet-VAX Product Authorization Key (PAK).
- Run NETCONFIG.COM to establish the initial configuration.
- Start up and shut down DECnet software.
- Run configuration checkout procedures on newly generated nodes.

RESOURCES

- *VMS License Management Utility Manual*, (AA-LA33A-TE)
- *Guide to DECnet-VAX Networking*, (AA-LA47A-TE)
- *VMS Networking Manual*, (AA-LA48A-TE)

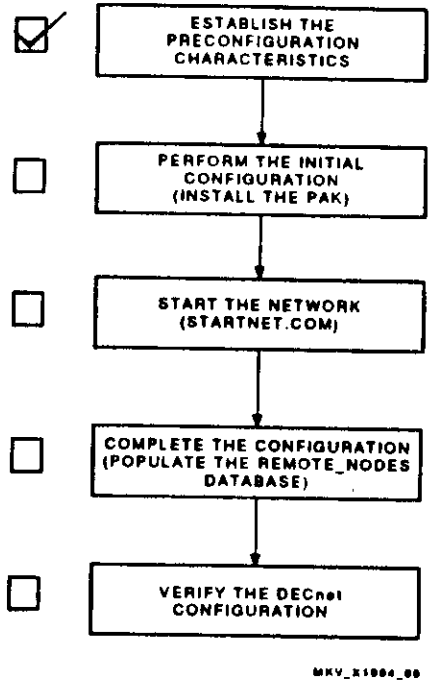
OVERVIEW: CONFIGURING DECNET-VAX

The five-step procedure for configuring DECnet-VAX is:



MKV_X1903_88

STEP 1



MKV_X1904_88

Establishing Pre-Configuration Characteristics

Before configuring the DECnet-VAX software, these characteristics must be determined:

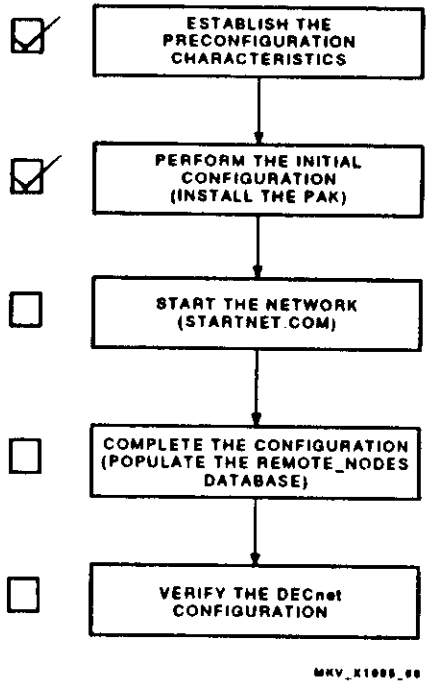
- Node name
- Node address
  - — *area . node*
- Node type
  - — End node
  - — Routing Node (level 1 or 2)
- Physical network connections
- Privileges for:
  - — Network manager
  - — Network users
  - — Application programs

Table 4–1 lists the privileges required to perform several network operations.

Table 4–1: Privileges for Various Network Operations

OPERATION	PRIVILEGE LIST
Starting the Network (STARTNET.COM)	ACNT, DETACH, CMKRNL, ALTPRI, LOG_IO, SYSNAM, NETMBX, TMPMBX, OPER, SYSPRV, WORLD
Perform task-task communication	NETMBX, TMPMBX, SYSNAM
View passwords under NCP	BYPASS
Access the permanent database	SYSPRV, OPER, NETMBX, TMPMBX

STEP 2



Performing the Initial Configuration

Installing the DECnet Product Authorization Key (PAK)

It is necessary to install the PAK before starting up DECnet software:

- Required to enable the software to operate on the network.
- Registered using the VMS License Management Facility (LMF) or the VMSLICENSE.COM utility.
- Key type based on type of license purchased:
  - — Full function PAK (for a routing node): DVNETRTG
  - — End-node PAK: DVNETEND

The licensing procedure consists of the following steps:

1. Obtain the PAK.
2. Shutdown DECnet software:

```
NCP>  SET EXECUTOR STATE SHUT
```

3. Register the PAK by entering the invoking the LICENSE utility:

```
$ @SYS$UPDATE:VMSLICENSE
```

4. Using the hardcopy PAK for input, answer the questions provided by the command procedure. Example 4–1 shows a sample PAK. Example 4–2 and Example 4–3 show a sample run of the licensing command procedure.

NOTE

Prior to VMS V5, DECnet software for MicroVMS had to be *installed* with VMSINSTAL.COM. Now, with V5, there is no longer a MicroVMS, so DECnet software comes bundled with VMS (like regular VMS for earlier versions).

Example 4–1: Sample Product Authorization Key

```
+-------------+    LICENSE SOFTWARE PRODUCT        +---------------------+
|d|i|g|i|t|a|l|    PRODUCT AUTHORIZATION KEY       | DOCUMENT ISSUE DATE |
+-------------+                                    |      1-OCT-1988     |
                                                   +---------------------+

Digital Equipment Corporation
Maynard, Ma.

+-----------------------------------+
| LICENSE ADMINISTRATION LOCATION:  |   ORDERED BY: FLINTSTONE ENTERPRISES
|                                   |               Mr. Barney Rubble
| Digital Equipment Corporation     |               32 Gravel Blvd.
| Maynard, Ma.                      |               Bedrock, Ma. 10129
|                                   |
+-----------------------------------+
*************************************************************************
 PAK ID:
                    Issuer: DEC
       Authorization Number: USA00331

 PRODUCT ID:
                Product Name: DVNETEND
                    Producer: DEC

 NUMBER OF UNITS:
             Number of units: 0

 KEY LEVEL:
                    Version: 5.0
        Product Release Date:

 KEY TERMINATION DATE:
        Key Termination Date: 31-DEC-1988

 RATING:
     Availability Table Code: E
          Activity Table Code:

 MISCELLANEOUS:
                 Key Options: MOD_UNITS
               Product Token:
                 Hardware Id:
                    Checksum: 1-DEML-LURT-NOTD-BAHT
*************************************************************************
```

Example 4–2: VMSLICENSE Command Procedure, (Sheet 1 of 2)

```
PARIS> @SYS$UPDATE:VMSLICENSE

   VMS License Management Utility Options:

       1.  Register a Product Authorization Key
       2.  Amend an existing Product Authorization Key
       3.  Exit this procedure

Select option: 1

* Do you have your Product Authorization Key? Y
                    .
                    .
                    .
    PAK ID:
* Issuer (DEC): RETURN
* Authorization Number: USA00331
    PRODUCT ID:
* Product Name: DVNETEND (1)
* Producer (DEC): RETURN
    NUMBER OF UNITS:
* Number of Units: 0
    KEY LEVEL:
* Version (vv.uu): 5.0
    KEY TERMINATION DATE:
* Key Termination Date (dd-mmm-yyyy): 31-DEC-1988
    RATING:
* Availability Table Code: E
* Activity Table Code: RETURN
    MISCELLANEOUS:
* Key Options: MOD_UNITS
* Node this authorization key is restricted to [PARIS]: RETURN (2)
* Product Token: RETURN
* Hardware ID: RETURN
* Checksum: 1-DEML-LURT-NOTD-BAHT
```

Example 4–3: VMSLICENSE Command Procedure, (Sheet 2 of 2)

```
              LMF Database: SYS$COMMON:[SYSEXE]LMFSLICENSE.LDB ❶
                    Issuer: DEC
      Authorization Number: USA00331
              Product Name: DVNETEND
                  Producer: DEC
          Number of Units: 0
                   Version: 5.0
      Product Release Date:
      Key Termination Date: 31-DEC-1988
  Availability Table Code: E
    Activity Table Code:
           Key Options: MOD_UNITS
         Product Token:
           Hardware ID:
              Checksum: 1-DEML-LURT-NOTD-BAHT

    This authorization key is restricted to: PARIS

* Is this information correct? Y ❹

    DVNETEND has been registered.

    DVNETEND has been loaded.

   VMS License Management Utility Options:

       1.  Register a Product Authorization Key
       2.  Amend an existing Product Authorization Key
       3.  Exit this procedure

Select option: 3
```


Running NETCONFIG.COM to Initialize

SYS$MANAGER:NETCONFIG.COM gives network managers an automated way of performing the minimum amount of initialization required to start a DECnet network.

After prompting for various required parameters, it builds and executes the NCP and DCL commands used to configure the DECnet-VAX node.

NETCONFIG.COM does the following:

1. Purges entries from the permanent database:
   - — Executor
   - — Lines
   - — Circuits
   - — Logging
   - — Objects
   - — Ethernet configurator
2. Automatically determines DECnet devices on the node:
   - — Ethernet
   - — CI
3. Initializes the executor permanent database.
4. Creates executor default DECnet VMS account and directory.
5. Initializes lines, circuits, and logging information.
6. Prompts to allow the commands (just built) to take effect (NETCONFIG.TMP).
7. Prompts to start the network software (STARTNET.COM).

NETCONFIG.COM does *not*:

- Save the contents of existing permanent database.
- Populate the remote node database.
- Fully populate the permanent database.
- Define CI circuits.
- Define asynchronous terminal lines/circuits.

Example 4–4 and Example 4–5 illustrate the use of NETCONFIG.COM.

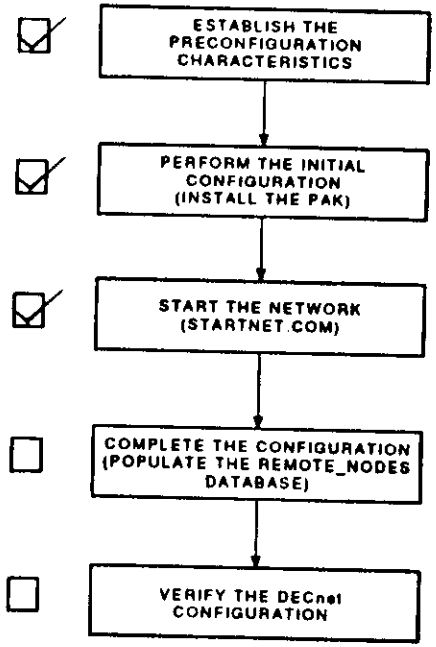
Example 4–4: NETCONFIG.COM Example for a Routing Node, (Sheet 1 of 2)

```
PARIS> @SYS$MANAGER:NETCONFIG

        DECnet-VAX network configuration procedure

This procedure will help define the parameters needed to get
DECnet running on this machine.  You will be shown the changes before
they are actually executed, in case you wish to perform them manually.

What do you want your DECnet node name to be?              : PARIS
What do you want your DECnet address to be?                : 55.4
Do you want to operate as a router?   [NO (nonrouting)]: YES
Do you want a default DECnet account?                [YES]: YES
Do you want to use the CI as a DECnet datalink?       [NO]: YES
```

Example 4–5: NETCONFIG.COM Example for a Routing Node, (Sheet 2 of 2)

```
Here are the commands necessary to set up your system:

$ RUN SYS$SYSTEM:NCP
    PURGE EXECUTOR ALL
    PURGE KNOWN LINES ALL
    PURGE KNOWN CIRCUITS ALL
    PURGE KNOWN LOGGING ALL
    PURGE KNOWN OBJECTS ALL
    PURGE MODULE CONFIGURATOR KNOWN CIRCUITS ALL
$ DEFINE/USER SYS$OUTPUT NL:
$ DEFINE/USER SYS$ERROR NL:
$ RUN SYS$SYSTEM: NCP       ! Remove existing entry, if any
    PURGE NODE 55.4 ALL
    PURGE NODE PARIS ALL
$ RUN SYS$SYSTEM: NCP
    DEFINE EXECUTOR ADDRESS 55.4 STATE ON
    DEFINE EXECUTOR NAME PARIS
    DEFINE EXECUTOR MAXIMUM ADDRESS 1023
    DEFINE EXECUTOR ROUTING TYPE ROUTING IV
    DEFINE EXECUTOR NONPRIVILEGED USER DECNET
    DEFINE EXECUTOR NONPRIVILEGED PASSWORD DECNET
$ DEFINE/USER SYSUAF SYS$SYSTEM:SYSUAF.DAT
$ RUN SYS$SYSTEM:AUTHORIZE
    ADD DECNET /OWNER="DECNET DEFAULT" -
        /PASSWORD=DECNET -
        /UIC=[376,376] /ACCOUNT=DECNET -
        /DEVICE=SYS$SYSDEVICE: /DIRECTORY=[DECNET] -
        /PRIVILEGE=(TMPMBX,NETMBX) -
        /FLAGS=(CAPTIVE) /LGICMD=NL: -
        /NOBATCH /NOINTERACTIVE
$ CREATE/DIRECTORY SYS$SYSDEVICE:[DECNET] /OWNER=[376,376]
$ RUN SYS$SYSTEM:NCP
    DEFINE LINE UNA-0 STATE ON
    DEFINE LINE CI-0 STATE ON
    DEFINE CIRCUIT UNA-0 STATE ON COST 3
    DEFINE LOGGING MONITOR STATE ON
    DEFINE LOGGING MONITOR EVENTS 0.0-9
    DEFINE LOGGING MONITOR EVENTS 2.0-1
    DEFINE LOGGING MONITOR EVENTS 4.2-13,15-16,18-19
    DEFINE LOGGING MONITOR EVENTS 5.0-18
    DEFINE LOGGING MONITOR EVENTS 128.0-4
------------------------------------------------------
Do you want these commands to be executed?        [YES]: RETURN

The changes have been made.

If you have not already registered the DECnet-VAX key, then do so now.
After the key has been registered, you should invoke the procedure
SYS$MANAGER:STARTNET.COM to start up DECnet-VAX with these changes.

(If the key is already registered) Do you want DECnet started? [YES]: RETURN
```

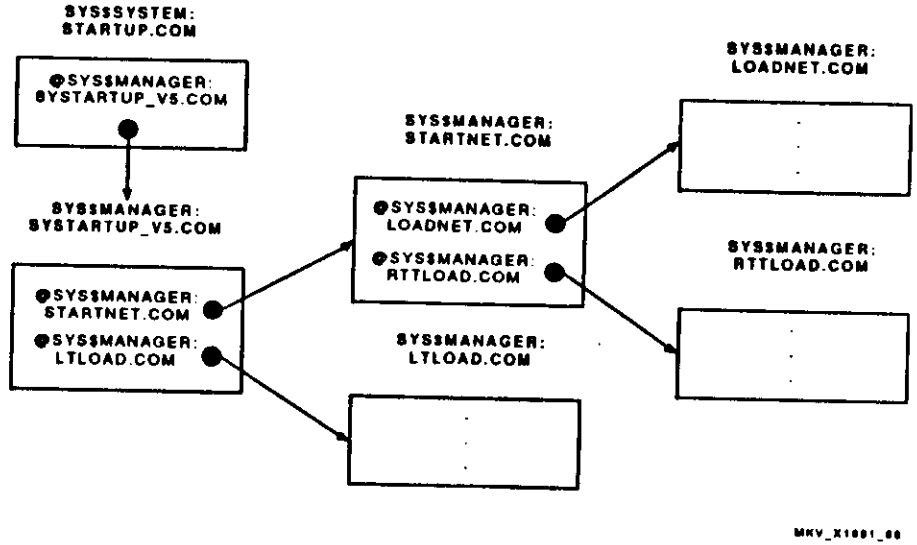
STEP 3



Starting the Network

Figure 4–1 illustrates the order of execution of various processes as a network starts.

Figure 4–1: Order of Network Startup on VMS V5.0



STARTNET.COM

STARTNET.COM performs the following tasks:

1. Checks for sufficient privileges:

   (ACNT, DETACH, CMKRNL, LOG_IO, WORLD, NETMBX, TMPMBX, SYSNAM, OPER, SYSPRV, ALTPRI)

2. Ensures that the executor permanent database is in place.

3. Compares SCSSYSTEMID, SCSNODE with executor node name and address.

4. Installs images:

   — SYS$SYSTEM:NICONFIG.EXE (privs = SYSNAM, LOG_IO)

   — SYS$SYSTEM:EVL.EXE (privs = SYSNAM, OPER, SYSPRV)

5. Executes: @SYS$MANAGER:LOADNET.COM 'P1'.

   — 'P1' defaults to NETACP if not specified.

   — Waits for NETACP to finish initialization.

6. Configures basic volatile database (from permanent):

   — SET EXECUTOR ALL

   — SET KNOWN { OBJECTS / LOGGING / PROXIES } ALL

7. Defines logicals for MOM.

8. Continues with basic configuration (permanent to volatile):

   — SET KNOWN { LINES / CIRCUITS } ALL

9. Enables module configurator circuits.

10. Executes: @SYS$MANAGER:RTTLOAD.COM (remote terminal functionality).

11. Completes basic configuration (permanent to volatile):

    — SET KNOWN NODES ALL (This can be time-consuming.)

LOADNET.COM

LOADNET.COM performs the following tasks:

1. Checks for sufficient privileges:

   (ACNT, DETACH, CMKRNL, ALTPRI)

2. Loads drivers:

   — NETDRIVER

   — NDDRIVER

3. Checks for user-override logicals:

   NETACP$ { MAXIMUM_WORKING_SET / PAGE_FILE / EXTENT / ENQUEUE_LIMIT }

RTTLOAD.COM

RTTLOAD.COM performs the following tasks:

1. Checks for sufficient privileges:

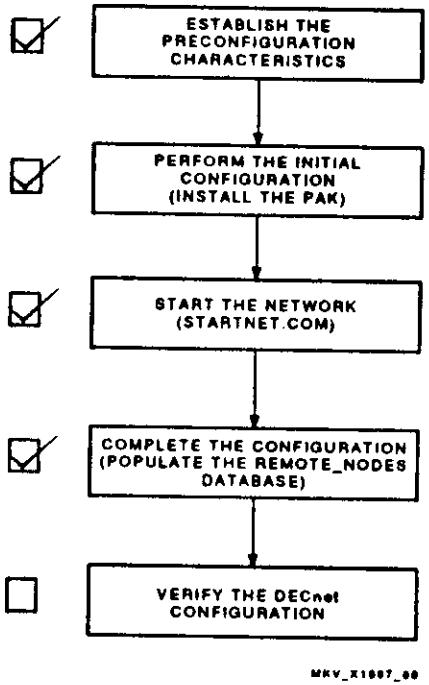
   (ACNT, DETACH, CMKRNL, LOG_IO, NETMBX, TMPMBX, SYSNAM)

2. Determines page file quota for REMACP.

3. Loads drivers:

   - RTTDRIVER
   - CTDRIVER

STEP 4



Completing the Configuration

Populating the Remote-Nodes database

Take the following steps to populate the remote-nodes database:

1. Establish a symbolic entry for an adjacent node:

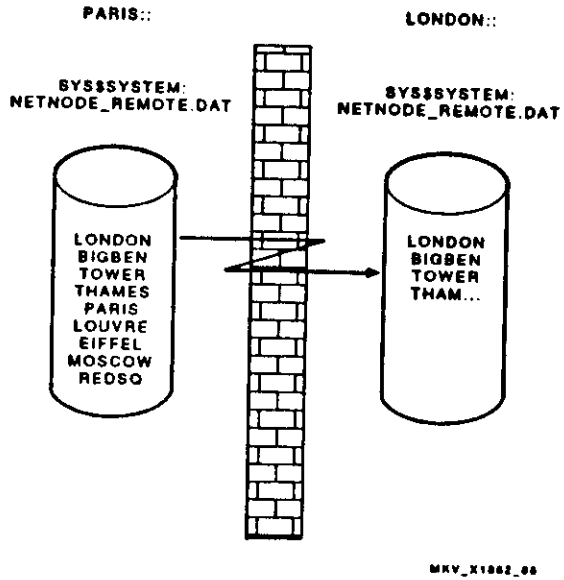
```
LONDON>  RUN SYS$SYSTEM:NCP
NCP>  SET NODE 55.4 NAME PARIS ❶
```

2. Copy the permanent remote-nodes database from the adjacent node:

```
NCP>  COPY KNOWN NODES FROM PARIS TO PERMANENT ❷
```

Figure 4–2 illustrates the transfer of information from the remote-nodes database on PARIS the remote-nodes database on LONDON.

Figure 4–2: Copying remote-node information from an adjacent node



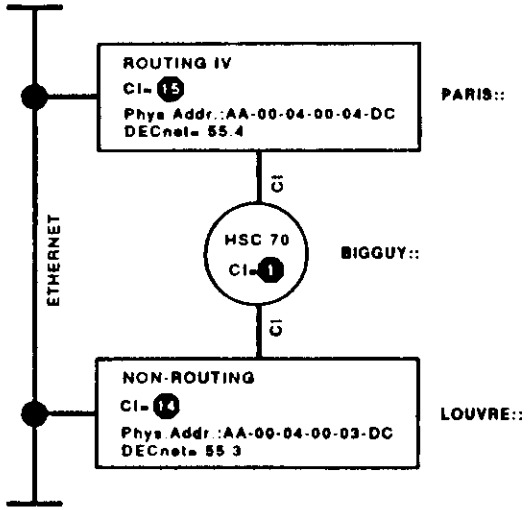
Non-Ethernet Implementations

Running DECnet Over a CI-Cluster

DECnet software can be implemented over the CI-lines of a VAXcluster, as well as over an Ethernet LAN. Usually, this is not done since operating system traffic over the CI is of a more time-critical nature than conventional Ethernet traffic.

However, if an Ethernet controller should fail, DECnet traffic can be re-routed through the CI. Figure 4–3 shows two possibilities of DECnet communications:

Figure 4–3: Sample CI-cluster network



Configuring DECnet Software Over the CI

Follow these steps to configure DECnet software over the CI:

1. Load the device driver for the CI (CNDRIVER).

   Add the following commands to SYS$MANAGER:SYCONFIG.COM:

```
$ SYSGEN :== $SYSGEN
$ SYSGEN CONNECT CNA0/NOADAPTER
```

2. Set the CI lines and circuits in the volatile database.

   Add the following commands to SYS$MANAGER:LOADNET.COM:

```
$ NCP :== $NCP
NCP> DEFINE LINE CI-0 STATE ON
NCP> DEFINE CIRCUIT CI-0.circuit-1 TRIBUTARY circuit-1 STATE ON
NCP> DEFINE CIRCUIT CI-0.circuit-2 TRIBUTARY circuit-2 STATE ON
   .
   .
   .
NCP> SET KNOWN CIRCUITS ALL
NCP> EXIT
```

   Where circuit-n can be determined through the VMS command:

```
$ SHOW CLUSTER/CONTINUOUS
```

   The circuit-n values represent the port value associated with each CI line:

The examples and figures on the next few pages illustrate the differences between running DECnet software over an Ethernet LAN and over the CI bus.

Figure 4–4: SHOW CLUSTER Display from Node PARIS

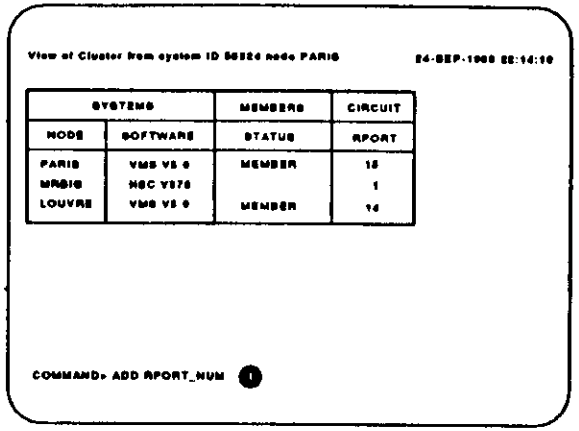
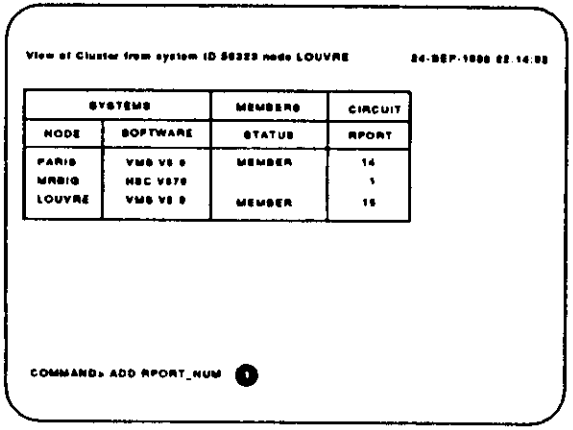


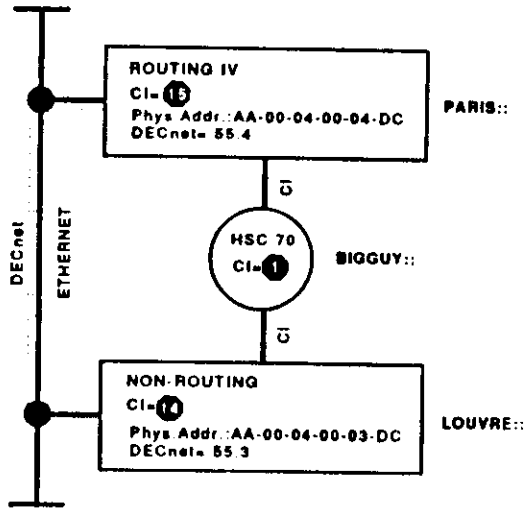
Figure 4–5: SHOW CLUSTER Display from Node LOUVRE



Example 4–6: Running DECnet over Ethernet LAN (UNA-0)

```
PARIS> SHOW NETWORK
VAX/VMS Network status for local node 55.4 PARIS on 25-SEP-1988 16:31:11.25
The next hop to the nearest area router is node 55.1 LONDON.
      Node           Links  Cost  Hops   Next Hop to Node
   55.4   PARIS        0     0     0     (Local)    -> 55.4    PARIS
                .
                .
                .
   55.35  FRANCE       0     0     0     (Local)    -> 55.4    PARIS
                .
                .
                .
   55.3   LOUVRE       0     3     1     UNA-0      -> 55.3    LOUVRE
                .
                .
                .
          Total of nnn nodes.
```

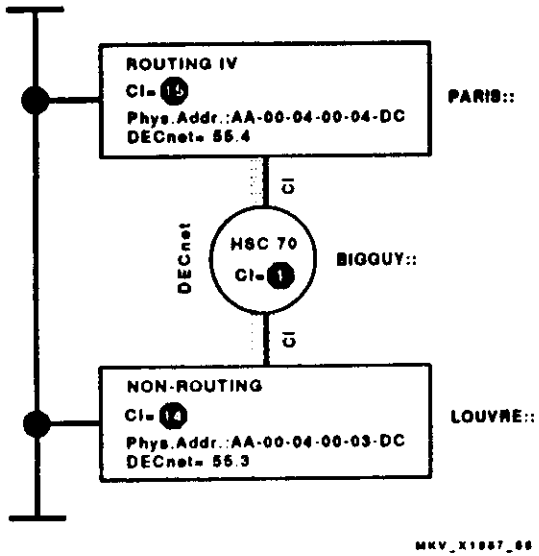
Figure 4–6: Diagram of DECnet Software over UNA-0



Example 4–7: Running DECnet Software over CI-0

```
PARIS>  SHOW NETWORK
VAX/VMS Network status for local node 55.4 PARIS on 25-SEP-1988 16:29:20.38
The next hop to the nearest area router is node 55.1 LONDON.
        Node           Links  Cost  Hops   Next Hop to Node
    55.4    PARIS        0     0     0     (Local)    -> 55.4     PARIS
              .
              .
              .
    55.35   FRANCE       0     0     0     (Local)    -> 55.4     PARIS
              .
              .
              .
    55.3    LOUVRE       1    10     1     CI-0.14    -> 55.3     LOUVRE
              .
              .
              .
              Total of nnn nodes.
```

Figure 4–7: Diagram of DECnet Software over CI-0



Running DECnet Software over Terminal Lines

STATIC Startup

To configure DECnet software to run over STATIC asynchronous lines:

1. Load the asynchronous DDCMP driver, NODRIVER, and the virtual terminal driver, TTDRIVER:

```
$ RUN SYS$SYSTEM:SYSGEN
SYSGEN> CONNECT NOA0/NOADAPTER
SYSGEN> CONNECT VTA0/NOADAPTER/DRIVER=TTDRIVER
```

2. Set the terminal line for DDCMP use:

```
$ SET TERMINAL/PROTOCOL=DDCMP/PERMANENT/NOTYPE_AHEAD/NOAUTOBAUD -
        /SPEED=9600 TTA0:
```

   OR, set the terminal line for DDCMP dial-up use:

```
$ SET TERMINAL/PROTOCOL=DDCMP/PERMANENT/NOTYPE_AHEAD/NOAUTOBAUD -
        /SPEED=1200/MODEM/NOHANGUP TTA0:
```

3. Enable the terminal line in the permanent/volatile databases:

```
NCP> DEFINE LINE TT-0-0 STATE ON RECEIVE BUFFERS 4 LINE SPEED 1200
NCP> DEFINE CIRCUIT TT-0-0 STATE ON
NCP> SET LINE TT-0-0 ALL
NCP> SET CIRCUIT TT-0-0 ALL
```

STATIC Shutdown

To terminate the connection:

1. Remove all lines from the databases:

```
NCP> SET LINE TT-0-0 STATE OFF
NCP> SET CIRCUIT TT-0-0 STATE OFF
NCP> CLEAR LINE TT-0-0 ALL
NCP> CLEAR CIRCUIT TT-0-0 ALL
```

2. Switch the line back to a terminal line (non-modem):

```
$ SET TERMINAL/PROTOCOL=NONE/PERMANENT TTA0:
```

3. Switch the line back to a terminal line (modem):

```
$ SET TERMINAL/PROTOCOL=NONE/PERMANENT/AUTOBAUD/TYPE_AHEAD TTA0:
```

Reasons for Failure of Static Asynchronous Connections

There are several reasons for the failure of static asynchronous connections:

- /MODEM and /EIGHT characteristics not set on terminal line.
- Line speeds at both ends not set to the same value.
- Parity not set to NONE on terminal line.
- Both nodes not in same DECnet area.

DYNAMIC Startup

To configure DECnet software to run over dynamic asynchronous lines:

1. Load NODRIVER, and TTDRIVER:

```
MOSCOW> RUN SYS$SYSTEM:SYSGEN
SYSGEN> CONNECT NOA0/NOADAPTER
SYSGEN> CONNECT VTA0/NOADAPTER/DRIVER=TTDRIVER
```

2. Install the shareable image DYNSWITCH:

```
MOSCOW> INSTALL :== $INSTALL/COMMAND
MOSCOW> INSTALL
INSTALL> CREATE SYS$LIBRARY:DYNSWITCH/SHARE/PROTECT/HEADER/OPEN
INSTALL> EXIT
```

3. Set the transmit and receive passwords (Circuit-level) through NCP.

   (Passwords on both systems must match.)

   On the INITIATING node (MOSCOW):

```
MOSCOW> RUN SYS$SYSTEM:NCP
NCP> SET NODE PARIS TRANSMIT PASSWORD TO_PARIS
NCP> EXIT
```

   On the TARGET node (PARIS):

```
PARIS> RUN SYS$SYSTEM:NCP
NCP> SET NODE MOSCOW RECEIVE PASSWORD FROM_PARIS
NCP> SET NODE MOSCOW INBOUND ROUTING
NCP> EXIT
```

4. Set the terminal line for DDCMP use:

```
MOSCOW> SET TERMINAL/PROTOCOL=NONE/PERMANENT/ALTYPEAHEAD/NOAUTOBAUD -
        /SPEED=1200/MODEM/NOHANGUP/DISCONNECT/HANGUP TTA0:
```

5. Connect to the remote system through the terminal emulator function of DECnet-VAX:

```
MOSCOW> SET HOST/DTE TTA0:
.
.
.
Username: enter valid username
Password: enter valid password
.
.
.
                    Welcome to node PARIS!

    Last interactive login on Saturday,  5-NOV-1988 22:11
    Last non-interactive login on Saturday,  5-NOV-1988 22:05

PARIS> SET TERMINAL/PROTOCOL=DDCMP/EIGHT/SWITCH=DECNET
%REM-S-END, control returned to node MOSCOW::
```

You are now connected using DECnet software.

DYNAMIC Shutdown

There are two ways to terminate the connection:

- Physically break the data connection (hang up).
- Clear the line/circuit entries from the volatile database by one of the following:

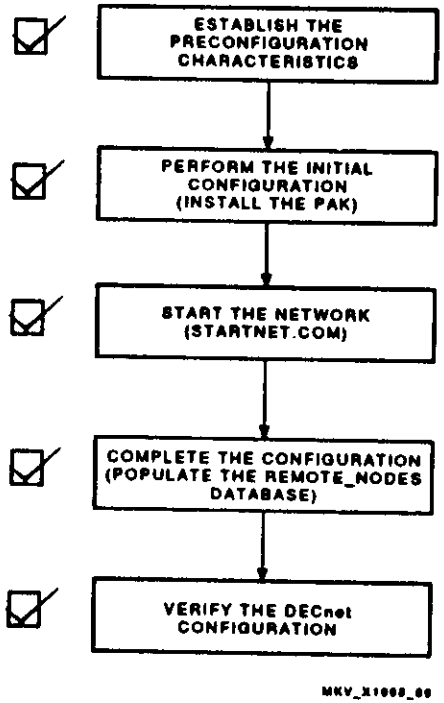
```
NCP> SET LINE TT-0-0 STATE OFF
NCP> SET CIRCUIT TT-0-0 STATE OFF
NCP> CLEAR LINE TT-0-0 ALL
NCP> CLEAR CIRCUIT TT-0-0 ALL
```

Reasons for failure of Dynamic Asynchronous Connections

There are several reasons for the failure of dynamic asynchronous connections:

- DECnet software not started on both nodes.
- Drivers not loaded (NODRIVER, TTDRIVER).
- DYNSWITCH not installed for auto-switched lines.
- Characteristic /DISCONNECT not set on terminal line.
- Both nodes not in same DECnet area.
- Routing Initialization (Circuit-level) passwords do not match.
- INBOUND ENDNODE or INBOUND ROUTING not set through NCP.

STEP 5



Verifying a Successful Configuration

After STARTNET.COM completes, the following commands can be used to verify the success of the configuration:

- DCL Commands:
  - $ SHOW SYSTEM (See Example 4–8.)
  - $ SHOW NETWORK (See Example 4–9 and Example 4–10.)
  - $ SET HOST
  - $ RUN SYS$SYSTEM:NCP
- NCP Commands:
  - SHOW EXECUTOR CHARACTERISTICS
  - SHOW NODE *nodename* STATUS
  - SHOW KNOWN CIRCUIT CHARACTERISTICS
  - SHOW KNOWN LINE CHARACTERISTICS

Example 4–8: The SHOW SYSTEM command

```
$ SHOW SYSTEM

VAX/VMS V5.0 on node HERMAN 4-NOV-1988 10:33:39.00   Uptime   17 16:43:20
  Pid    Process Name    State  Pri      I/O       CPU        Page flts Ph.Mem
20600080 NULL            COM      0        0  15 18:49:32.17         0      0
20600081 SWAPPER         HIB     16        0   0 00:13:18.48         0      0
20600085 ERRFMT          HIB      6    20965   0 00:03:53.82        68     87
20600086 CACHE_SERVER    HIB     16      346   0 00:00:01.60        58     81
20600087 CLUSTER_SERVER  HIB     10      880   0 00:02:35.66       118    286
20600088 OPCOM           LEF      9     7510   0 00:01:39.38     27308    141
20600089 JOB_CONTROL     HIB      9   122175   0 00:25:58.43       210    330
2060008A CONFIGURE       HIB      8       27   0 00:00:00.34       102    125
2060008B SYMBIONT_0001   HIB      6    61923   0 00:55:27.95    394270    512
2060008F NETACP ❶        HIB     10   117135   0 00:29:27.86     30096   1496
20600090 EVL ❷           HIB      6     3790   0 00:02:33.08    354066     41  M
20600091 REMACP ❸        HIB      8     1035   0 00:00:04.20        76     52
20600092 TRAINING        CUR      9     1057   0 00:00:00.17        36
20600E98 VAXsim_Monitor  HIB      8     3875   0 00:00:59.92       301    273
```

Notes on example 4–8:

❶ NETACP:

— Network Ancillary Control Process

(No longer stoppable with VMS v5.0; STOP/ID=8F

❷ EVL:

— Event Logger

❸ REMACP:

— Remote-terminal Ancillary Control Process

— Associated with the DECnet object CTERM (number 42)

Example 4–9: SHOW NETWORK for a routing node

```
PARIS> SHOW NETWORK

VAX/VMS Network status for local node 55.4 PARIS on 22-OCT-1988 13:34:40.98 13:3

The next hop to the nearest area router is node 55.1 LONDON.

     Node          Links    Cost     Hops    Next Hop to Node

     55.4              0       0        0     (Local)    -> 55.4
     55.1              0       3        1     UNA-0      -> 55.1
     55.2              0       3        1     UNA-0      -> 55.2
     55.3              0       3        1     UNA-0      -> 55.3

               Total of 4 nodes
```

Example 4–10: SHOW NETWORK for an end node

```
LOUVRE> SHOW NETWORK

VAX/VMS Network status for local node 55.3 LOUVRE  on 14-AUG-1988 11:33:08.03

This is a nonrouting node, and does not have any network information.
The designated router for LOUVRE is node 55.1 LONDON.
```

User Environment Test Package (UETP)

UETP performs the following functions:

- Interactive testing of network and system.
- Tests hardware and software.
- Shuts network down during test phase.
- Zeros counters.
- Uses NCP commands to create test command procedures.

The test package includes:

- Local Node Test
- Sequential Circuit Test
- Parallel Circuit Test
- Adjacent and First Hop Node Test

To Use UETP, log in to the SYSTEST account and execute:

```
$ @UETP
```

Then, make the following choices:

- Select a subset or all tests.
  - — DEVICE
  - — LOAD
  - — DECNET
  - — CLUSTER
  - — ALL
- Select the number of passes. The default is 1.
- Select long or short format. The default is long.

Example 4–11 shows a sample UETP run.

Example 4–11: UETP Example

```
        Welcome to VAX/VMS V5.0

Username: SYSTEST
Password:
        Welcome to VAX/VMS V5.0 on node LONDON

    Last interactive login on Wednesday, 28-SEP-1988 20:36


LONDON> @UETP

        Welcome to VAX/VMS UETP Version V5.0

%UETP-I-ABORTC, UETINIT00 to abort this test, type ^C
You are running on a VAXstation II/GPX CPU with 18432 pages of memory.
The system was booted from _DUA0:[SYS0.].

Run "ALL" UETP phases or a "SUBSET" [ALL]? SUBSET
You can choose one or more of the following phases:

        DEVICE, LOAD, DECNET, CLUSTER

Phase(s): DECNET
How many passes of UETP do you wish to run (1)? RETURN
Do you want Long or Short report format [Long]? RETURN
UETP starting at 28-SEP-1988 20:42:10.42 with parameters:
DECNET  phases, 1 pass, 9 loads, long report.

%UETP-I-BEGIN, UETDNET00 beginning at 28-SEP-1988 20:42:12.05
%UETP-I-BEGIN, UETDNET00_0000 beginning at 28-SEP-1988 20:42:12.59
    %UETP-I-BEGIN, EXECUTOR node testing beginning at 28-SEP-1988 20:42:18.63
    %UETP-I-ENDED, EXECUTOR node testing ended at 28-SEP-1988 20:42:37.30
    %UETP-I-BEGIN, Network sizing beginning at 28-SEP-1988 20:42:37.79
        Testing circuit QNA-0 to node 55.4 (PARIS)
    %UETP-I-ENDED, Network sizing ended at 28-SEP-1988 20:42:49.60
    %UETP-I-BEGIN, Remote circuit testing beginning at 28-SEP-1988 20:42:52.33
    %UETP-I-BEGIN, UETDNET01 beginning at 28-SEP-1988 20:42:53.29
    %UETP-I-BEGIN, QNA026133_0000 beginning at 28-SEP-1988 20:42:54.45
    %UETP-I-BEGIN, QNA026133_0001 beginning at 28-SEP-1988 20:42:55.29
    %UETP-I-ENDED, QNA026133_0000 ended at 28-SEP-1988 20:43:50.76
    %UETP-I-ENDED, QNA026133_0001 ended at 28-SEP-1988 20:43:59.65
    %UETP-I-ENDED, UETDNET01 ended at 28-SEP-1988 20:44:00.17
    %UETP-I-ENDED, Remote circuit testing ended at 28-SEP-1988 20:44:03.85
    %UETP-I-TEXT, Node  (PARIS) over QNA-0 aged packet loss = 1.
%UETP-I-ENDED, UETDNET00_0000 ended at 28-SEP-1988 20:44:18.31
%UETP-I-ENDED, UETDNET00 ended at 28-SEP-1988 20:44:18.95

 ************************************************
 *                                              *
    END OF UETP PASS 1 AT 28-SEP-1988 20:44:23.22
 *                                              *
 ************************************************


LONDON> logout
  SYSTEST       logged out at 28-SEP-1988 20:44:30.30
```


SUMMARY

Part of the Network Manager's function includes licensing DECnet software on existing host nodes. This task involves registering a Product Authorization Key (PAK). This must be done on every node that wants to use DECnet software.

With Version 5 of VMS, DECnet software now comes bundled with the operating system. It does not have to be installed with VMSINSTAL, as with Version 4 systems.

With three command files (VMSLICENSE.COM, NETCONFIG.COM, and STARTNET.COM) you can establish a VMS host node as an integral member of a DECnet network. These command files, however, depend almost exclusively on standard default values that may or may not be the best for your own environment. For example, the remote node database must be populated and SYSGEN parameters may have to be set.

WRITTEN EXERCISES

1. Rank the following procedures in the order they will be run for a first-time configuration of DECnet software.

   _____ UETP
   _____ NETCONFIG
   _____ VMSLICENSE
   _____ STARTNET
   _____ LOADNET

2. Match the descriptions with the terms. Each term may be used once, more than once, or not at all.

Description	Term
____ 1. Procedure used to automatically configure the permanent database	a. Executor b. Netconfig c. Routing Node d. End Node e. UETP
____ 2. Node that can accept and pass on data not specifically addressed to it	
____ 3. Handles data moving between areas	
____ 4. The generic name for the local node	
____ 5. Test procedure used to verify the correctness of the DECnet configuration	
____ 6. Node that can send data generated by itself or addressed to itself only	

Circle the one correct answer to each of the following.

3. Which of the following are functions of NETCONFIG.COM?

   I Registers DECnet on the node.

   II Determines DECnet devices on the node.

   III Creates a default DECnet account if desired.

   a. I and II
   b. I and III
   c. II and III
   d. I, II and III

4. Installation of the DVNETRTG kit allows you to configure the node as:

   a. An end node
   b. A routing node
   c. Both a and b

5. Which of the following commands would be used to verify that DECnet software has been configured properly?

   I $ SHOW NETWORK

   II $ SET HOST

   III $ SHOW LICENSE

   a. I and II
   b. I and III
   c. II and III
   d. I, II and III

6. Which three processes are active when DECnet software is running?

   a. NULL, SWAPPER, REMACP

   b. REMACP, NETACP, EVL

   c. NCP, NETACP, NETCONFIG

7. Which of the following commands can be used to stop DECnet software before registering the PAK?

   a. NCP SET EXECUTOR STATE STOP

   b. NCP SET EXECUTOR STATE SHUT

   c. NCP SET NODE STATE OFF

8. Which of the following commands is issued to register the PAK?

   a. @SYS$UPGRADE:VMSLICENSE

   b. @SYS$UPDATE:VMSREGISTER

   c. @SYS$UPDATE:VMSLICENSE

SOLUTIONS TO WRITTEN EXERCISES

1. Rank the following procedures in the order they will be run for a first-time configuration of DECnet software.

   __5__ UETP
   __2__ NETCONFIG
   __1__ VMSLICENSE
   __3__ STARTNET
   __4__ LOADNET

2. Match the descriptions with the terms. Each term may be used once, more than once, or not at all.

Description	Term
__b__ 1. Procedure used to automatically configure the permanent database	a. Executor b. Netconfig c. Routing Node d. End Node e. UETP
__c__ 2. Node that can accept and pass on data not specifically addressed to it	
__c__ 3. Handles data moving between areas	
__a__ 4. The generic name for the local node	
__e__ 5. Test procedure used to verify the correctness of the DECnet configuration	
__d__ 6. Node that can send data generated by itself or addressed to itself only	

The correct answers are underlined.

3. **Which of the following are functions of NETCONFIG.COM?**

   I Registers DECnet on the node.

   II Determines DECnet devices on the node.

   III Creates a default DECnet account if desired.

   a. I and II

   b. I and III

   c. II and III

   d. I, II and III

4. **Installation of the DVNETRTG kit allows you to configure the node as:**

   a. An end node

   b. A routing node

   c. Both a and b

5. **Which of the following commands would be used to verify that DECnet software has been configured properly?**

   I $ SHOW NETWORK

   II $ SET HOST

   III $ SHOW LICENSE

   a. I and II (There is a LICENSE LIST command.)

   b. I and III

   c. II and III

   d. I, II and III

6. **Which three processes are active when DECnet software is running?**

   a. NULL, SWAPPER, REMACP

   b. REMACP, NETACP, EVL

   c. NCP, NETACP, NETCONFIG

7. **Which of the following commands can be used to stop DECnet software before registering the PAK?**

   a. NCP SET EXECUTOR STATE STOP

   b. NCP SET EXECUTOR STATE SHUT

   c. NCP SET NODE STATE OFF

8. **Which of the following commands is issued to register the PAK?**

   a. @SYS$UPGRADE:VMSLICENSE

   b. @SYS$UPDATE:VMSREGISTER

   c. @SYS$UPDATE:VMSLICENSE

LABORATORY EXERCISES

Part I

For this exercise you use a VAX system on which VMS software has been installed. The system has not been configured to run as part of the network. Follow the steps presented in the module to configure your node. Your instructor will provide the following information:

- The name and address of your node.
- The node type.
- Which nodes to include in your remote node database.
- The initial physical network connections for your node.

Work as a team. Plan before you use the machine. Prepare a written list of commands, and *do not* let the person at the console take control. Everyone on the team should know why a particular action has been taken.

Part II

1. Verify the configuration using the DCL and NCP commands presented in this module.
2. Further verify the configuration using network utilities:
   - Check the PHONE and MAIL commands.
   - Manipulate files on your node as well as a remote node using explicit access control. (Include the username and password in quotation marks following the node name on the command line).
   - Make sure the default DECnet account has been set up correctly by manipulating files using default access control. (Use the null string after the node name in the command line).

'art III

'ind out from your instructor if your node requires any additional physical connections such as ;TATIC or DYNAMIC asynchronous lines. If so, follow the examples presented in the module ɔ add the additional lines and circuits necessary to make these connections functional.

Vhen you have finished adding any additional connections, verify your configuration again to nsure that everything still works properly, and that the new circuit functions properly.

MODULE 5
ACCESS CONTROL

INTRODUCTION

DECnet Access Control is the confirmation of a user's identity by checking various database (local and remote) for validity.

This module discusses the general algorithms used to accept/deny access to a DECnet-VA node through access control with examples demonstrating the use of explicit, default, and pro network log-in. This is explained with the use of a conceptual Reference Monitor Mechanism.

The creation of network processes is explained along with the log-in command procedures th can affect network accessibility.

The use of AUTHORIZE and NCP as tools used to control network access is also covered wi emphasis on enhancing the security of the default DECnet account.

OBJECTIVES

To explain and use network access control to prevent unauthorized use of network capabilitie a network manager should be able to:

- Identify the steps taken by DECnet-VAX software in network process creation.
- Identify the various network database (volatile/permanent) fields and how they affect acces control.
- Explain the methods of controlling network access from remote users and nodes.
- Set up and use network proxy accounts.
- Set up and enhance the default DECnet account using the AUTHORIZE utility.

RESOURCES

1. *Guide to VMS System Security*, (AA-LA40A-TE)
2. *VMS Networking Manual*, (AA-LA48A-TE)

THE REFERENCE MONITOR CONCEPT

Reference Monitor on a Single Node

The reference monitor concept depicts a computer system in terms of:

- **Subjects**

  Active entities that gain access to information on behalf of users.

- **Objects**

  Passive repositories of information to be protected.

- **Authorization Database**

  Defines the system security requirements by revealing which subjects can have which kinds of access to objects.

- **Audit Trail**

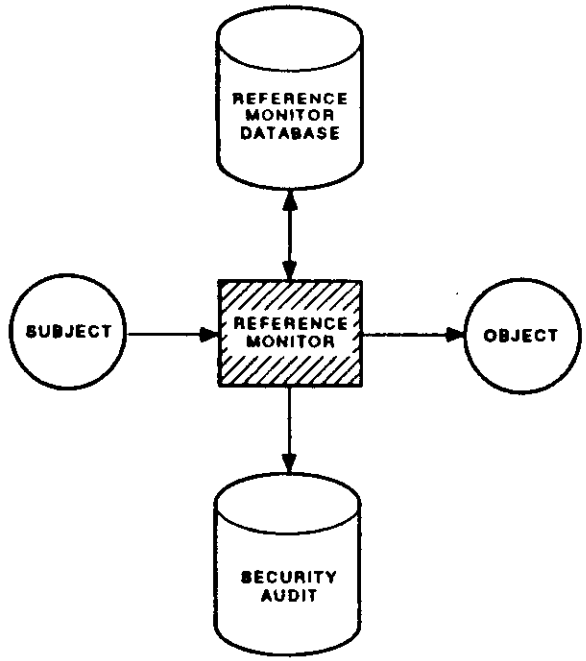
  Maintains a record of access attempts, successful or not, as required by the authorization database.

- **Reference Monitor Mechanism**

  Enforces the security rules by authorizing the creation of subjects, granting subjects access to objects according to the requirements of the database, and recording events as necessary in the audit trail.

Figure 5–1 illustrates the use of the reference monitor on a single node.

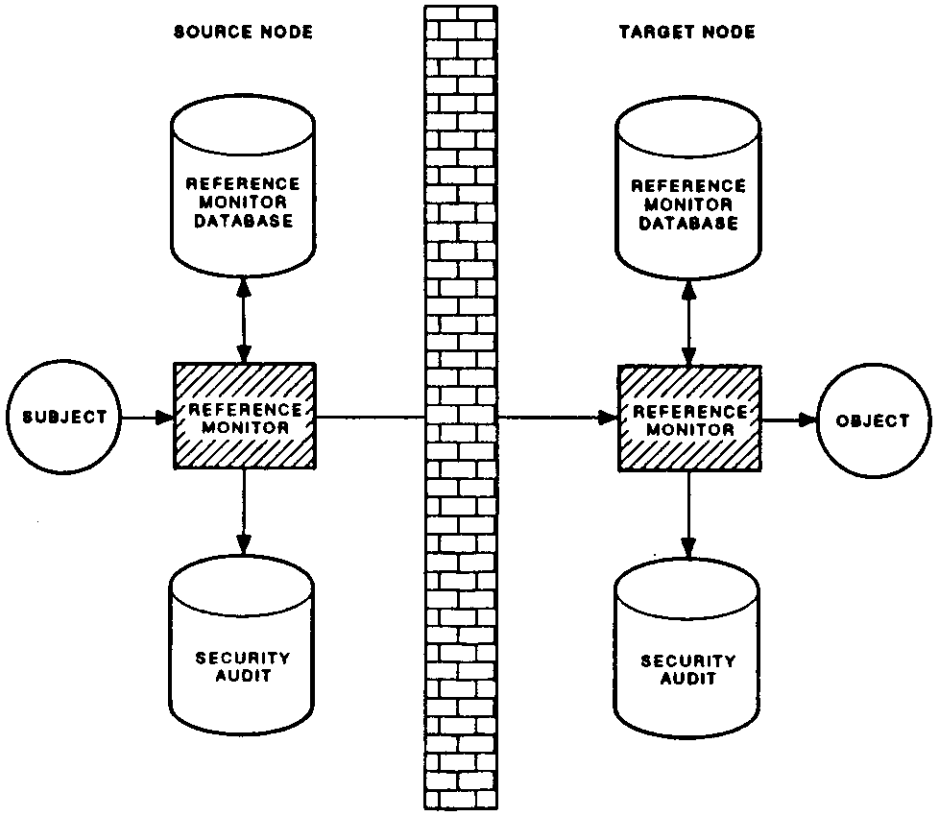
Figure 5–1: Reference Monitor on a Single Computer Node



Reference Monitor on the network

In a network, there is a subject on one node, an object on another, and a network reference monitor that grants the subject access to the object on another node. Figure 5–2 illustrates the use of the reference monitor in a network.

Figure 5–2: Reference Monitor in a Network



MAKING THE LOGICAL LINK CONNECTION

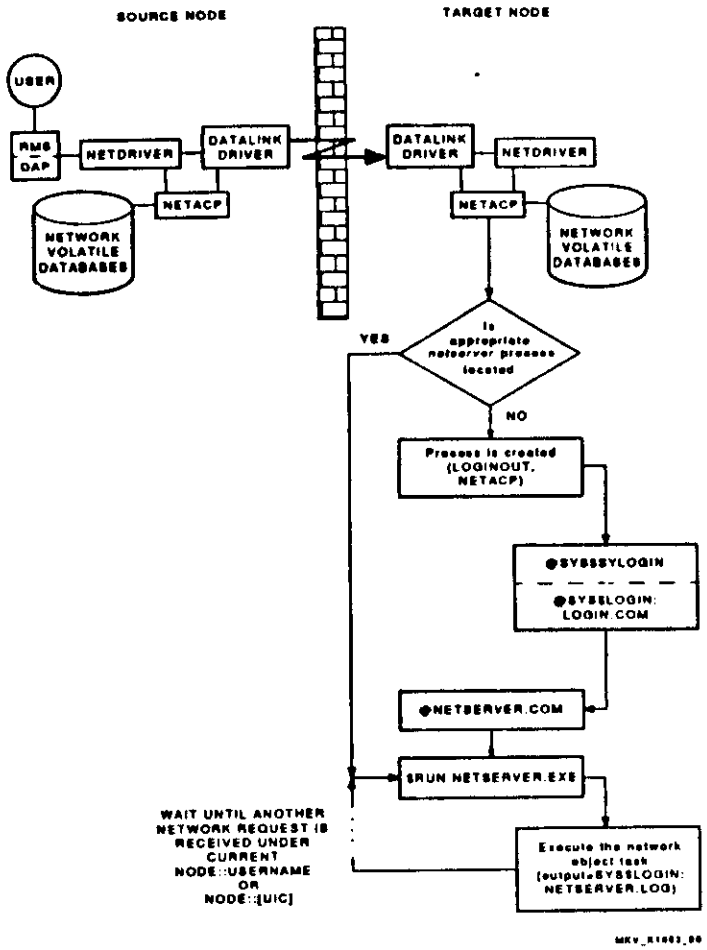
The following steps, illustrated by Figure 5–3, are executed to create a network process:

1. The application program on the initiating node sends a request to the DECnet software on the local node.
2. DECnet software on the local node sends a request to the DECnet software on the remote node (connect initiate).
3. NETACP creates a process (or uses an existing NETSERVER) to receive the connect request.
   - Access Control Information (ACI) is used in creating/using remote processes to make association between the phantom and real subject.
   - SYS$OUTPUT = SYS$LOGIN:NETSERVER.LOG
   - F$MODE() = "NETWORK"
   - Executes SYSTEM and PROCESS log-in command procedure(s).
4. NETSERVER.COM executes within the NETSERVER process and it runs NETSERVER.EXE.
5. NETSERVER.EXE invokes the program or command procedure for the requested connection.
6. The requested task runs until completion; then exits to NETSERVER.COM.
7. NETSERVER.COM runs NETSERVER.EXE again which waits, in turn, for another incoming logical link request to process.

NOTE

The following cycle runs and continues until the NETSERVER process is deleted after a specified idle time limit (NETSERVER$TIMEOUT time; default is 5 minutes).

Figure 5–3: Network Process Creation



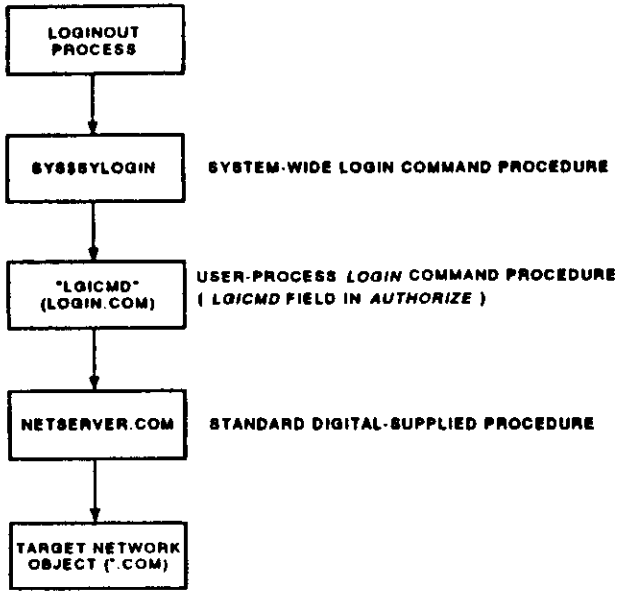
PLACES TO INSERT SPECIAL CHECKS FOR CONTROLLING ACCESS

There are two possible steps in the process creation chain that can be enhanced to further control access on a more specific basis:

- System log-in command procedure:
  - Filename is defined in the logical SYS$SYLOGIN.
  - Usually located in SYS$MANAGER:SYLOGIN.COM.
- Process log-in command procedure:
  - Filename is defined in AUTHORIZE as the LGICMD field.
  - If not defined, use SYS$LOGIN:LOGIN.COM as default.

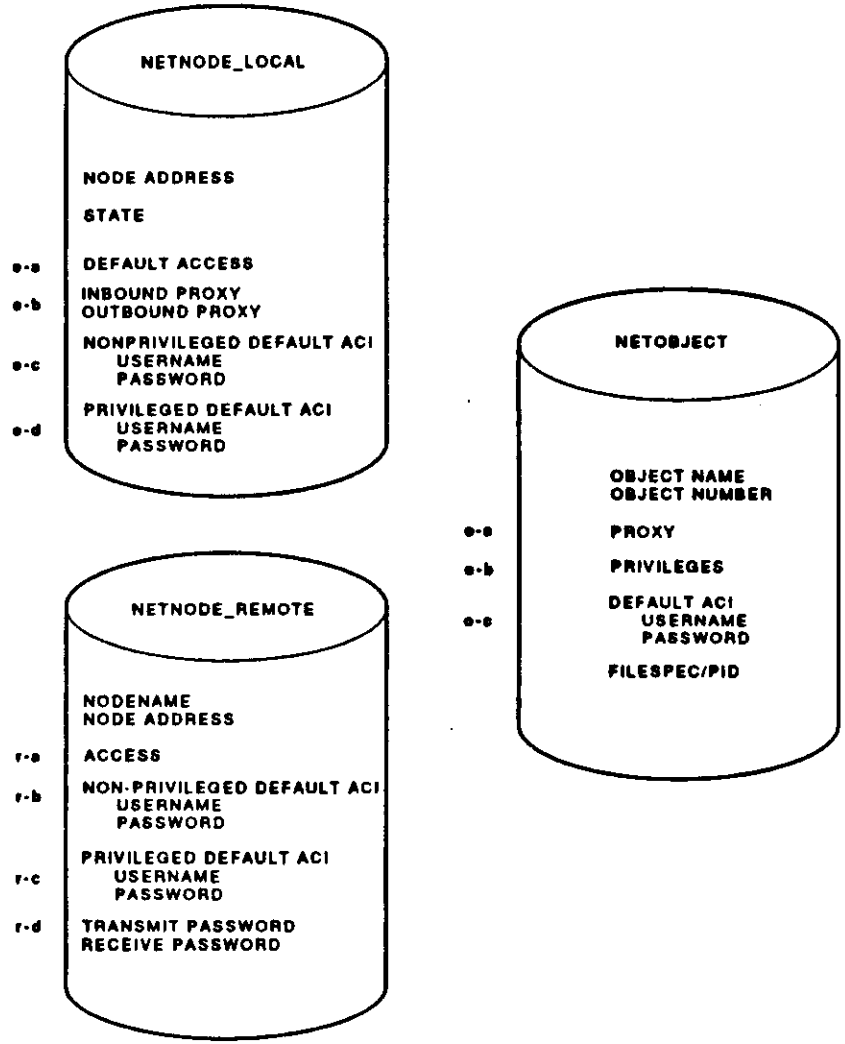
The log-in execution chain is shown in Figure 5–4.

Figure 5–4: Log-In Execution Chain



MKV_X1000_88

Figure 5–5: Key Network Databases



MKV_X1000_88

NETWORK OBJECTS

Network objects provide general-purpose network services. They are identified by object name and/or object type (number). Each object specifies a system task (image) or user task (command procedure) to execute for the inbound connect request. In addition:

- The following are examples of DIGITAL-supplied objects:
  - FAL (File Access Listener)
  - NML (Network Management Listener)
  - MAIL
  - PHONE
  - TASK (the *zero* object)
- DIGITAL-supplied objects (1-127) are automatically defined in the volatile database.
- User-written objects (0, 128-255) can be defined by the system manager in both the permanent and volatile databases:

  NCP> { SET / DEFINE } OBJECT SHOUSE NUMBER 130 FILE SHO_USE.COM

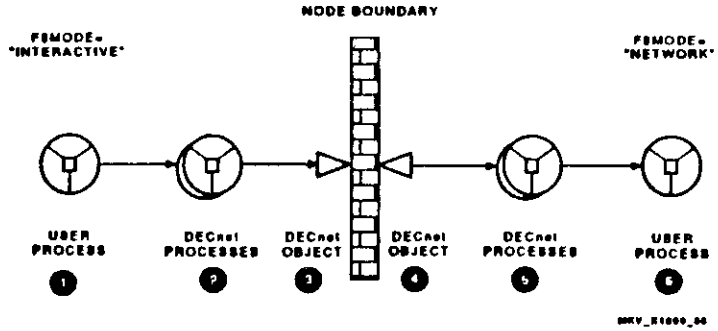
  or through non-transparent programming (at the System Service level).
- Network processes may request connections to declared objects by name or number:

```
$ TYPE LONDON::"130="
$ TYPE LONDON::"SHOUSE="
```

- Network processes may request connections to task objects by name only:

```
$ TYPE LONDON::"0=SHOSYS"
$ TYPE LONDON::"TASK=SHOSYS"
```


Figure 5–6: Intertask Communication Through DECnet Objects



The following notes refer to Figure 5–6.

❶ $ TYPE LONDON::"130="

This is the source or initiator task. It requests a DECnet link to the target task—a user-specified object identified by number (type) *130*.

❷ Local DECnet software

In VMS, it is implemented as permanent processes/drivers that are created at DECnet start-up (usually right after system startup). NETACP and NETDRIVER are two components of the DECnet software.

The following notes also refer to Figure 5–6.

❶ **PHANTOM object**

This contains information about how to access this object (what file or process is used to access the task associated with this entry point).

❹ **REAL object**

This contains the actual information (username, password, proxy, privileges) that determine network log-in characteristics.

❺ **Remote DECnet software**

Partner to local DECnet software. It performs functions in both directions: initiating and receiving connect requests.

❻ **SYS$LOGIN:SHOUSE.COM**

In this example, the target task is implemented as a DCL command procedure. It could also be implemented as an executable image (*.EXE) as are DIGITAL-supplied network objects (FAL.EXE, MAIL.EXE, ...)

DECNET-VAX ACCESS CONTROL

Overview of Access Control

Access control is exercised over all logical link connections. DECnet-VAX access control ca be divided into several different categories, implemented through various DNA layers:

- Circuit-level:
  - — Implemented at the Routing Layer.
  - — Used when a circuit between two nodes is initialized.
  - — For point-to-point connections Dynamic and Static.
- Node-level:
  - — Implemented at the Session Control Layer.
  - — Allows the ability to selectively disable access on a network on a node-by-node basis.
- System-level:
  - — Implemented at the Session Control Layer.
  - — Used to determine the VMS account to create the target network process.
  - — Broken down into three categories:

    Explicit

    Default

    Proxy

Circuit-Level Access Control

Circuit level access control verifies that a node is authorized to form a connection with another node:

- Also known as routing initialization passwords.
- Uses data stored in the remote nodes database NETNODE_REMOTE.DAT.
- Used for systems that are connected to the network with point-to-point connections (DDCMP).
- Set-up of transmit/receive passwords on the adjacent node should be the reverse of the local node:

```
NCP> { SET    } NODE nodename { TRANSMIT } { t-password }
     { DEFINE }               { RECEIVE  } { r-password }

NCP> { SET    } CIRCUIT VERIFICATION ENABLED
     { DEFINE }
```

- State changes from ON-STARTING to ON after passwords are exchanged correctly.

Node-Level Access Control

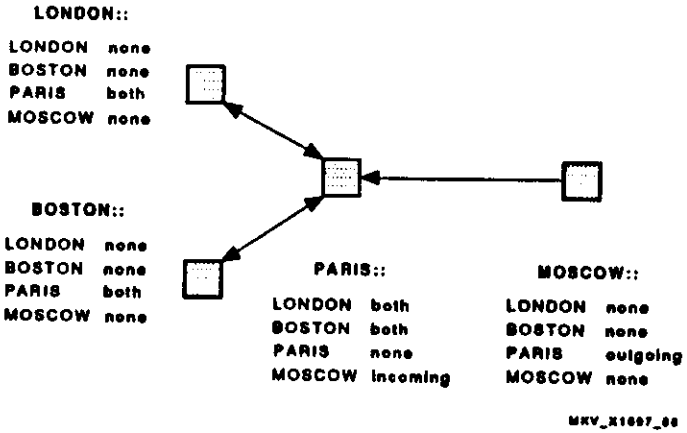
Node-level access control controls the establishment of logical links with remote nodes:

- Defined on a node-by-node basis.
- Two fields in the network database control node-level access:
  - — ACCESS (ref. [R-A]) is checked first to determine if the target node is accessible.
  - — DEFAULT ACCESS (ref. [E-A]) is checked if the access field is not explicitly defined for the remote node.

```
NCP> { SET    } { EXECUTOR DEFAULT } ACCESS { INCOMING }
     { DEFINE } { NODE nodename    }        { OUTGOING }
                                            { BOTH     }
                                            { NONE     }

NCP> { CLEAR  } { EXECUTOR DEFAULT } ACCESS
     { PURGE  } { NODE nodename    }
```

Figure 5–7 illustrates the use of node-level access control.

Figure 5–7: Controlling Node Accessibility Through ACCESS



NOTE

Processes possessing the OPER privilege will override this feature.

System-Level Access Control

System-Level ACI can be broken down into three categories:

- Explicit
  - — USERNAME, PASSWORD, and ACCOUNT fields are specified explicitly.

    (The ACCOUNT field is optional and has no meaning to a VMS system).
  - — A null string was specified ("") a special case of explicit access control.
- Proxy
  - — A new proxy feature with VMS V5 is that usernames can be specified in quotes (NODE"*remote_user*"::).
  - — Passwords are never specified or sent over the network.
  - — The target node must determine the account to use to create the network process, unless overridden by the new proxy feature in VMS V5.
- Default
  - — DECnet software uses ACI from within the volatile database to detect the need to use a default account.
  - — Nonprivileged (or privileged) ACI information can be used depending on configuration of the volatile database.
  - — Default ACI can be associated with:

    Nodes (outbound)

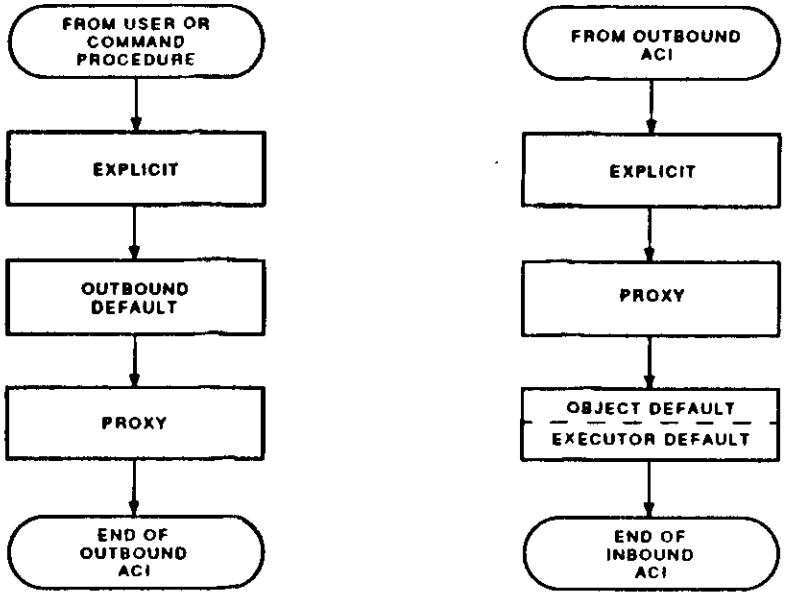
    Objects (inbound)

    Executor (inbound)

The next several pages cover the types of access control in greater depth. The section for each type begins with a flowchart, followed by examples of how to use it, followed by an explanation of the algorithm involved.

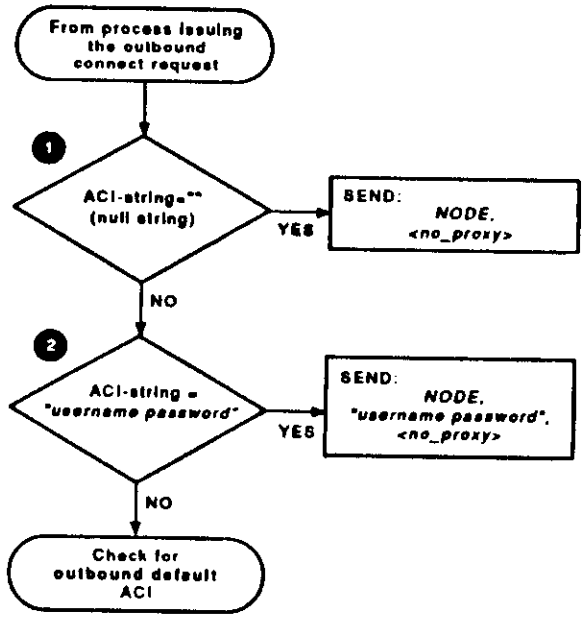
The order of evaluation for access control is outlined in Figure 5–8.

Figure 5–8: Access Control Flowchart Overview



MKV_X1854_88

Figure 5–9: Outbound Explicit Access Control Flowchart



MKV_X1855_88

Outbound Access Control

Outbound Explicit Access Control

Outbound explicit access is used whenever the initiating node supplies a literal "username password", (withing quotes) that refers to a *real* subject on the target node:

```
$ TYPE MOSCOW"Ian Fleming"::KGB$DATA:SECRET.DAT
```

Alternatively, a *null-access* string can be specified to force an inbound default:

```
$ TYPE MOSCOW""::KGB$DATA:FROM_RUSSIA.WITH_LOVE
```

The Algorithm

There are two cases of outbound explicit access:

❶ A null-string ("") was supplied instead of a specific *"username password"*.

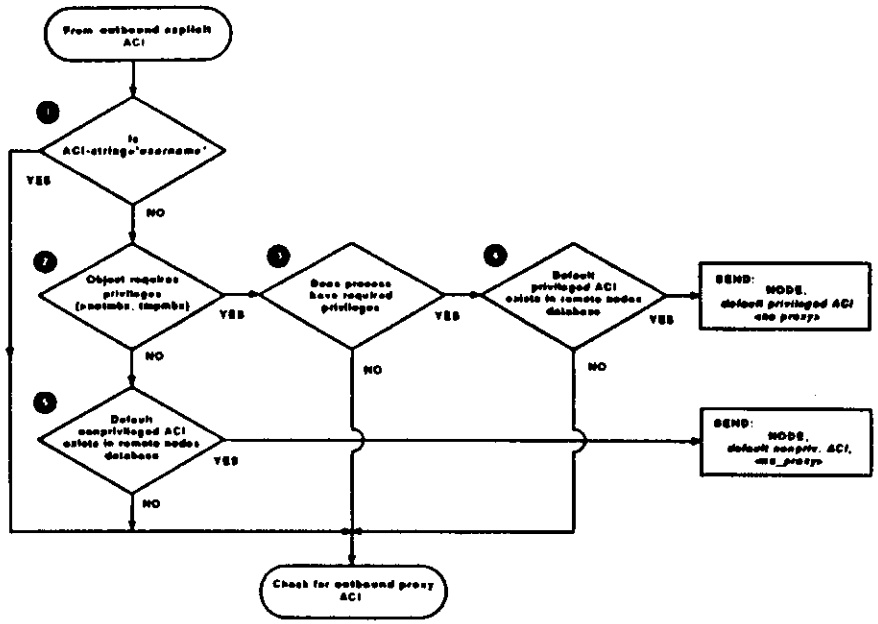
- DECnet software passes this to the target node without further case testing.

❷ *"username password"* both were specified.

- This is the simplest case; the local DECnet software sends this ACI directly to the target node's DECnet software.

If neither was satisfied, DECnet software attempts to use outbound default access.

Figure 5–10: Outbound Default Access Control Flowchart



Outbound Default Access Control

Outbound default access is used whenever outbound explicit access is not specified.

NOTE

An outbound default overrides any attempt to use proxy since default case-testing occurs before proxy (in the oubound sense).

The following example could cause an outbound default to be sent to the remote node:

```
$ TYPE MOSCOW::KGB$DATA:SECRET.DAT
```

The Algorithm

❶ If a single *"username"* (alone and in quotes) was not specified by the requesting process, then DECnet will try to use outbound default for access.

❷ The local DECnet software will check the object database to determine if the object requires privileges (beyond NETMBX and TMPMBX).

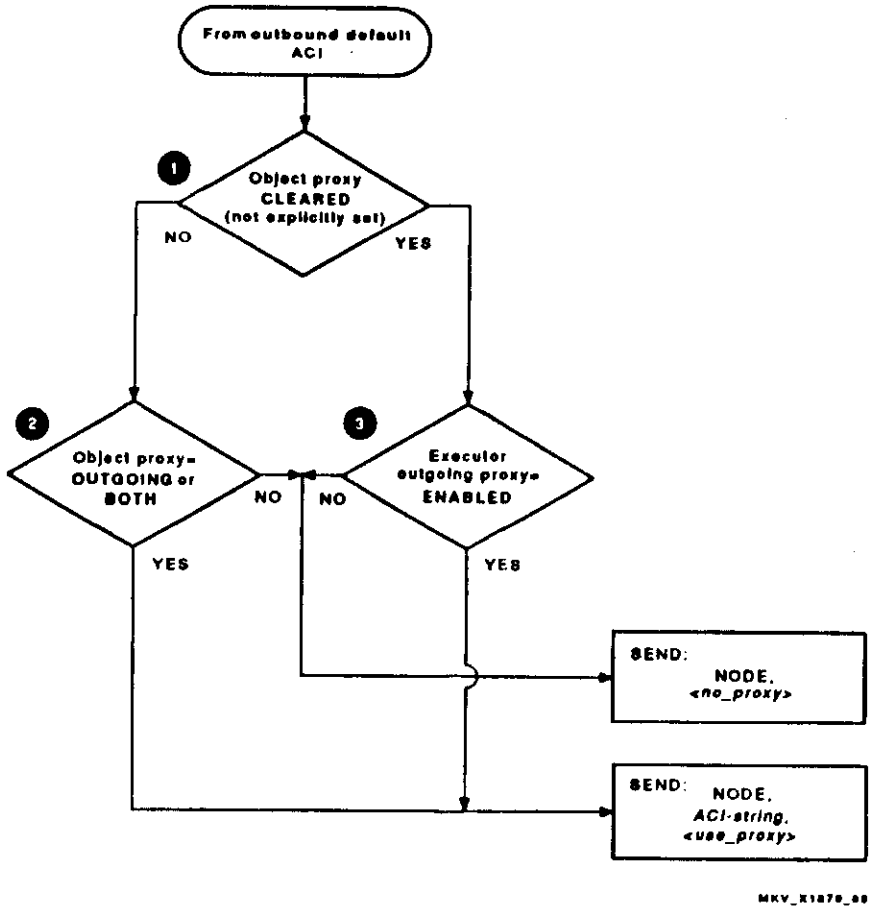
❸ If the requesting process has the required privileges, DECnet software checks its remote node database for a default privileged account (ref. [R-C]) corresponding to the desired target node (❹).

❺ The DECnet software attempts to use the default nonprivileged account (ref. [R-B]) for the target node if either is true:

- The object does not require any special privileges.
- The user DOES NOT have the required privileges (according to the Object).

If neither default privileged nor default nonprivileged accounts exist in the remote nodes database, then DECnet tries to use outbound proxy for access.

Figure 5–11: Outbound Proxy Access Control Flowchart



Outbound Proxy Access Control

Outbound proxy access is used whenever outbound explicit acess is not specified, and outbound default access is not defined (enabled) or is inappropriate.

Individual users may override outbound proxy access merely by using outbound explicit access methods. For example, neither of the following commands use outbound proxy access, even if NETPROXY.DAT and the network database fields are set up for it:

```
$ TYPE MOSCOW("Ian Fleming")::KGB$DATA:SECRET.DAT
$ TYPE MOSCOW(""):::KGB$DATA:FROM_RUSSIA.WITH_LOVE
```

The Algorithm

If the outbound explicit and outbound default tests fail, outbound proxy access is attempted.

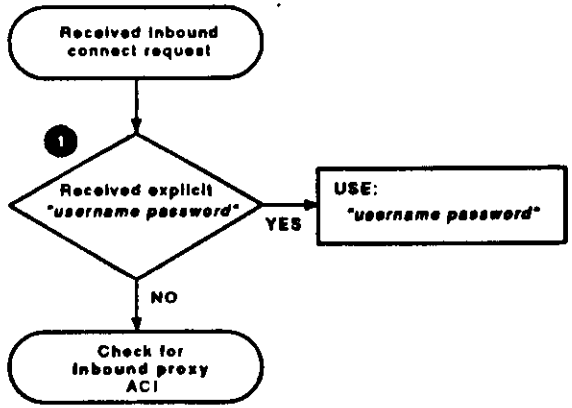
❶ If the proxy field in the object database is enabled (that is, set to a specific value, but not cleared), this parameter can be used to determine if the object will allow outbound proxy access.

❷ If this field is enabled as OUTGOING or BOTH, DECnet sends the ACI-string (as specified by the requesting process) together with a special <use_proxy> flag in its connection request.

❸ If this field is enabled, the outgoing proxy field in the executor database is checked. If this is ENABLED, the result is the same as if the object had allowed proxy (❷).

If neither the object database nor the executor database allowed outgoing proxy, DECnet software sends a special <no_proxy> flag instead of the ACI-string, as specified by the requesting process.

Figure 5–12: Inbound Explicit Access Control Flowchart



Inbound Access Control

Inbound Explicit Access Control

The DECnet software on the target (inbound) side cannot know whether it received a *"username password"* pair that was supplied by either:

- The requesting process EXPLICITLY
- The requesting DECnet software by way of an outbound default

The Algorithm

❶ If the target node received explicit ACI, it uses that to create the network process similar to when an interactive user logs into the system locally.

If both username and password were not specified, then DECnet software tries to use inbound proxy access.

Inbound Proxy Access Control

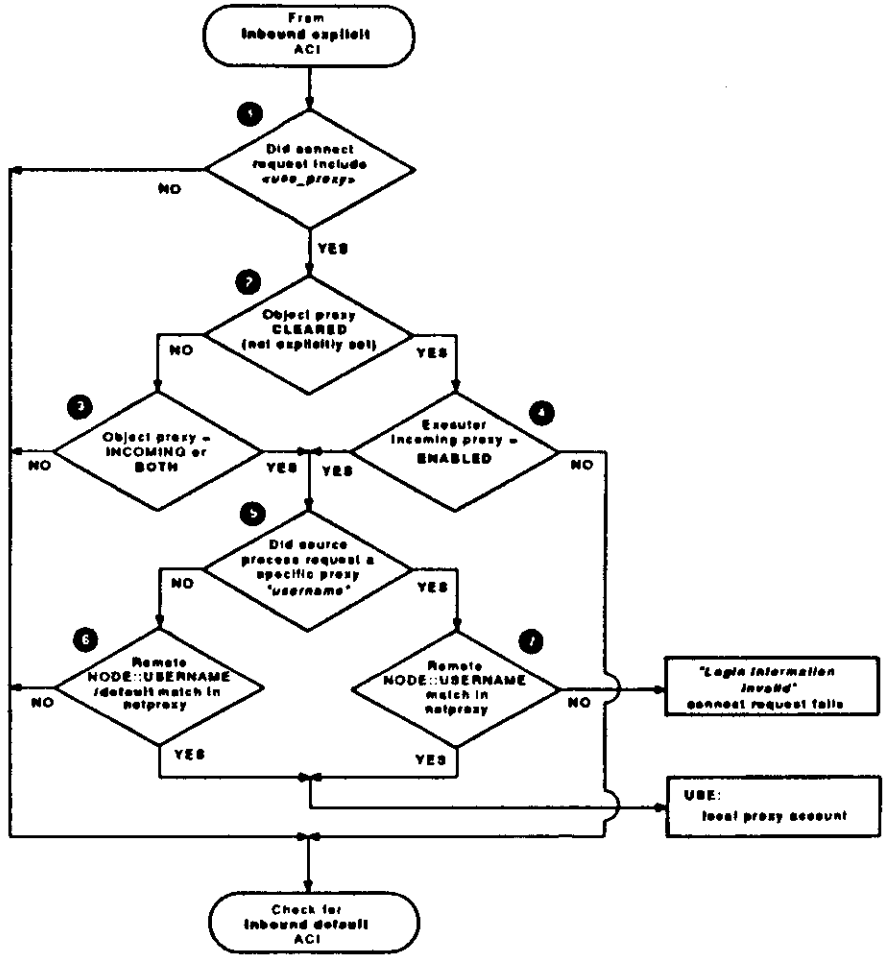
Inbound proxy has a higher priority than inbound default (occurs earlier in the inbound case-testing), so if it is possible to use proxy, inbound default is used. This is important when trying to use a default account associated with a network object.

There is a new proxy feature with VMS V5.0. Users can now designate a specific target proxy account to use for process creation. For example, this can be invoked by executing the following *DCL* command:

```
$ DIR MOSCOW"Lenin"::
```

In this case, the user is trying to map to account "Lenin" on node MOSCOW.

Figure 5–13: Inbound Proxy Access Control Flowchart



The Algorithm

❶ If the connect request did include the <use_proxy> flag in the connect request, DECnet software checks for the existence of an inbound default account.

❷ If the proxy field in the object database is enabled (that is, set to a specific value, but not cleared), this parameter can be used to determine if DECnet will allow inbound proxy access.

❸ If the proxy field in the object database is enabled as INCOMING or BOTH, inbound proxy is attempted (❺). If not, then then the executor database must be checked before a decision can be made.

❹ If the proxy field in the object database is not enabled, the incoming proxy field in the executor database is checked. If this is ENABLED, the result is the same as if the object had allowed inbound proxy access. If DISABLED, then DECnet tries to use inbound default access.

❺ With VMS V5, DECnet must check further to determine if the source process had requested a specific target proxy account to use.

❻ If a specific target proxy account was not specified, then the operation of proxy is the same as that of VMS V4.x: the remote NODE::USERNAME pair is used to find the local VMS account to use as a default inbound proxy. This can only happen if a match is found in NETPROXY.DAT with the /default qualifier.

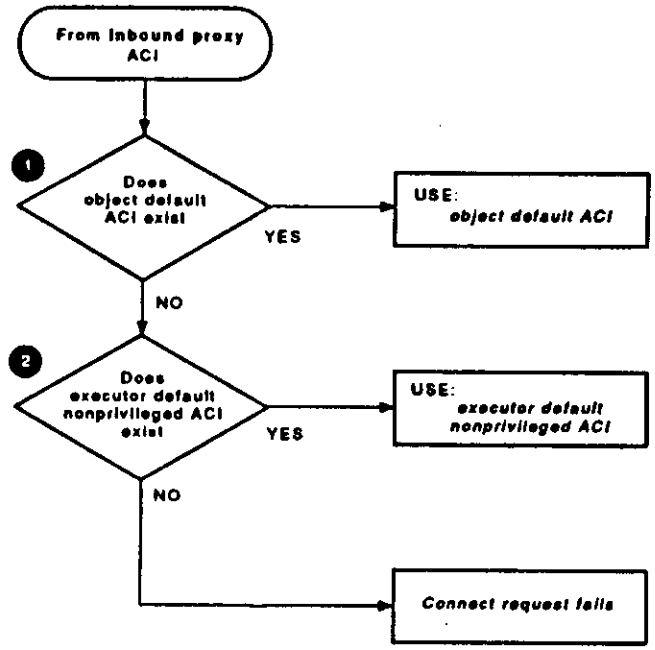
If a /default match is found, then that VMS account is used to create the network process.

If a /default match is *not* found, then DECnet tries to use inbound default access.

❼ If a specific target proxy account IS specified, then DECnet tries to locate a NODE::USERNAME match in NETPROXY.DAT that maps to the VMS account specifed by the requesting process. If a match is found, the operation is the same as in (❻).

However, if a match was *not* found, then DECnet returns an error to the requesting process indicating that the desired target proxy is invalid. This is because DECnet reasons that if the specific account cannot be used, then the account will is used as a fallback.

Figure 5–14: Inbound Default Access Control Flowchart



Inbound Default Access Control

This is the last chance to determine which account is used in creating the network process.

If the target node did not receive a *"username password"* pair, then it tries to generate a *"username password"* pair from the object or executor database on the local node.

The Algorithm

❶ DECnet checks its object database to see if an object (inbound) default account (ref. [O-C]) exists. If this account exists, it is used to create the network process.

❷ If there is no object (inbound) default account for the requested network object, then the target node's executor database is checked for the existence of a default nonprivileged (inbound) account (ref. [E-C]). If this account exists, it is used; otherwise the connection must be rejected.

Setting up Proxy Accounts

Two utilities are used to set up proxy log-ins: AUTHORIZE and NCP. Follow these steps:

1. Enable proxy access using NCP.
2. Create the NETPROXY.DAT database using AUTHORIZE.
3. Create the local proxy account using AUTHORIZE (in SYSUAF.DAT)

Using NCP to Control Proxy Access

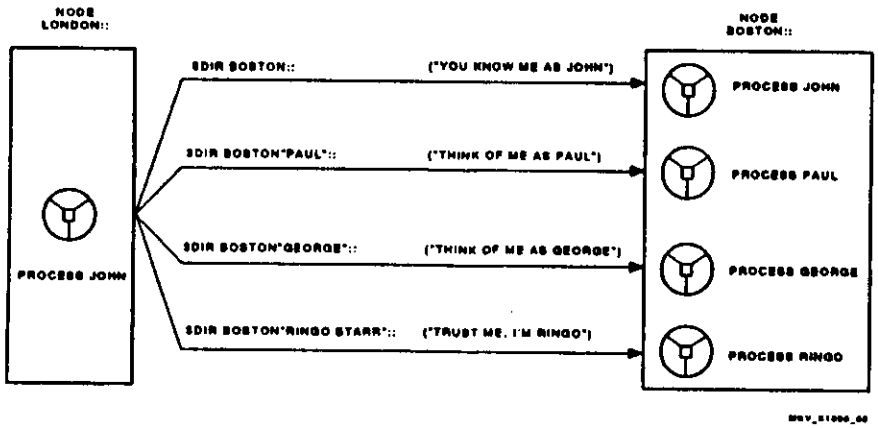
- Executor database has both inbound proxy and outbound proxy fields (ref: [E-B])
- Object database has only a single proxy parameter to control proxy access to specific objects (ref: [O-A]). This controls proxy use in both directions.

Using AUTHORIZE to Control Proxy Access

- File used by AUTHORIZE is NETPROXY.DAT (in SYS$SYSTEM).
- If this file is not already there, it must be created.
- Multiple remote users can map to one proxy account, and a single user can map to multiple local accounts (14 plus 1 default, or 15 excluding the default).
- Can establish a general access account that permits only NETWORK log-ins (using AUTHORIZE).

Figure 5–15 illustrates the use of proxy to connect to different accounts on a target node.

Figure 5–15: Using Proxy to Connect to Different Target Accounts



Object-Level Proxy Access

Permitting proxy log-in access to an object is recommended only if the proxy access serves some useful purpose.

For example, by default, MAIL is set to prevent INCOMING proxy log-in, while FAL is set to allow both INCOMING and OUTGOING proxy log-ins.

- Enable proxy access to the object in the initiator's object database to OUTGOING or BOTH.
- Enable proxy access for the object in the target node's object database to INCOMING or BOTH.

```
NCP> { SET    } OBJECT object_name PROXY { INCOMING }
     { DEFINE }                          { OUTGOING }
                                         { BOTH     }
                                         { NONE     }

NCP> { CLEAR } OBJECT object_name PROXY
     { PURGE }
```

The use of proxy on objects is illustrated in Example 5–1.

Example 5–1: Proxy on Objects

```
NCP>  SET OBJECT FAL PROXY INCOMING

NCP>  SHOW OBJECT FAL CHARACTERISTICS

Object Volatile Characteristics as of 21-SEP-1988 21:18:56

Object = FAL

Number                  = 17
File id                 = FAL.EXE
Proxy access            = incoming
```

Executor-Level Proxy Access

These network database fields specify the default that is to be used if the object proxy field is not defined (cleared) in the object database.

- Enable outgoing proxy access from the initiating node in its executor database
- Enable incoming proxy access to the target node in its executor database

NCP> { SET / DEFINE } EXECUTOR { INCOMING / OUTGOING } PROXY { ENABLED / DISABLED }

NCP> { CLEAR / PURGE } EXECUTOR { INCOMING / OUTGOING } PROXY

Example 5–2 shows the use of executor level proxy.

Example 5–2: Proxy on the Executor

```
NCP>  SET EXECUTOR INCOMING PROXY DISABLED

NCP>  SHOW EXECUTOR CHARACTERISTICS

Node Volatile Characteristics as of 21-SEP-1988 21:18:14

Executor node = 55.2 (BOSTON)

Identification            = DECnet-VAX V5.0,  VMS V5.0
Management version        = V4.0.0
Incoming timer            = 45
Outgoing timer            = 60
Incoming Proxy            = Disabled
Outgoing Proxy            = Enabled
                .
                .
                .
```

Advantages and Disadvantages of Each Access Control Method

The advantages and disadvantages of each access control method are listed on the following pages.

Explicit Access Control

- Advantages:
  - — Easy to universally restrict access, then revise access on an individual basis (user accountability).
  - — Cannot gain access by masquerading as a particular user on a particular node.
  - — No special system management tasks need be done at the target node to allow users to access files; just give out a username and password.
- Disadvantages:
  - -- Explicit *username,password* string is actually sent over the network.
  - — Passwords can be seen at a user's terminal, in command procedures, and in logical name definitions.
  - — If the destination VMS account on the target node is changed, all remote users who need to access data in that account must be notified of the new password.

Default Access Control

- OUTBOUND Disadvantages:
  - — Changes to default accounts passwords, must be propagated to all users who need to access data with that account.
  - — *usernames*, *passwords* are sent over the network if ACI is supplied by the initiating node.
  - — If defined, user cannot use proxy to that particular node.
- INBOUND Advantages:
  - — If default ACI is supplied by the target node, no passwords are sent over the network.
- INBOUND Disadvantages:
  - — Privileged users (with BYPASS) can easily read passwords with NCP.

Proxy Access Control

- Advantages:
  - — Allows a user to access a remote node without explicitly specifying access control.
  - — Provides default access to a particular account on the target node for a group of specific user(s).
  - — Removes the temptation to store passwords in command files.
  - — Since the proxy account is specified at the destination node, users may never eve know the password for their accounts on the remote node.
  - — Network database fields may inhibit either inbound or outbound proxy access on node-by-node basis (in each executor's default setting). This check is done first, thu overriding the contents of the NETPROXY.DAT file.
- Disadvantages:
  - — More susceptible to masquerade attacks.
  - — Process creation increased.

THE DEFAULT DECNET ACCOUNT(S)

The term default DECnet account usually refers to the local (inbound) nonprivileged VMS account referenced in the executor database (ref. [E-C]). If ACI cannot be derived from the requested object, the executor default is used.

The default DECnet account ID is used when:

- The initiating user did not specify explicit access.
- Proxy is not enabled (incoming and/or outgoing).

Default DECnet Account as Defined by NETCONFIG.COM

Example 5–3 shows, effectively, the commands used by NETCONFIG.COM to create the default DECnet account. This is, however, not the most secure way of creating this account.

Example 5–3: Standard Commands to Set Up the Default DECnet Account

```
$ SET DEFAULT SYS$SYSTEM
$ RUN SYS$SYSTEM:AUTHORIZE
ADD DECNET /OWNER="DECNET DEFAULT"                          -
           /PASSWORD=DECNET                                 -
           /UIC=[376,376) /ACCOUNT=DECNET                   -
           /DEVICE=SYS$SYSDEVICE: /DIRECTORY=[DECNET]       -
           /PRIVILEGE=(TMPMBX,NETMBX)                       -
           /FLAGS=(CAPTIVE) /LGICMD=NL:                     -
           /NOBATCH /NOINTERACTIVE
```


Enhancing Security Through AUTHORIZE

Normally, the default DECnet VMS account is not as secure as it can be. Below are listed various flags, switches, and other AUTHORIZE fields that can be changed:

- The DECnet account should have only TMPMBX and NETMBX for authorized (as well as default) privileges.

- The account should be in a UIC group by itself.
  - — Ensure that the DECnet group is not a SYSTEM group.
  - — Ensure the UIC group is less than the SYSGEN parameter MAXSYSGROUP.

- The following AUTHORIZE flags should be set:
  - — CAPTIVE, DISCTLY—to make the log-in command procedure inescapable.
  - — LOCKPWD—the standard password should not be changed by users.
  - — DISMAIL, DISNEWMAIL—mail is not allowed to/from the VMS account DECNET.
  - — DEFCLI—allows only the default Command Line Interpreter (DCL).
  - — DISWELCOME—no welcome message is issued on log-in.

Enhancing security through AUTHORIZE (cont.)

- The following AUTHORIZE switches should be set:
  - — NOINTERACTIVE—users are not allowed to log in interactively.
  - — NOBATCH—disallow submitting batch jobs under the DECNET account.
- LGICMD—should NOT point to the default directory, but to a real log-in command procedure (on a process-level).

Example 5–4 shows a more secure way of defining the DECNET account. It can be executed after NETCONFIG.COM is run:

Example 5–4: Commands to Enhance Security for the Default DECnet Account

```
UAF> MODIFY DECNET /UIC=[3000,1] /NOPWDLIFETIME -
                   /FLAGS=(DISCTLY,DEFCLI,LOCKPWD, DISNEWMAIL,DISMAIL,DISWELCOME) -
                   /LGICMD=SYSSMANAGER:DECNET_LOGIN.COM -
                   /NOBATCH /NOINTERACTIVE /NOLOCAL /NOREMOTE
```


Default DECnet Account SYSUAF.DAT Listing

Example 5–5 is a listing of an enhanced AUTHORIZE record for the default DECnet acco

Example 5–5: Enhanced Default DECnet Account

```
Username: DECNET                                 Owner:  DECNET DEFAULT
Account:  DECNET                                 UIC:[3000,1] ([DECNET]) ❶
CLI:      ❷ DCL                                  Tables: DCLTABLES
Default:  SYS$SYSDEVICE:[DECNET]
LGICMD: SYS$MANAGER:DECNET_LOGIN.COM ❸
Login Flags:  Disctly Defcli ❹ Lockpwd ❺ Captive Disnewmail Dismail Diswelcom
Primary days:    Mon Tue Wed Thu Fri
Secondary days:                          Sat Sun
Primary    000000000011111111112222  Secondary 000000000011111111112222
Day Hours  012345678901234567890123  Day Hours 012345678901234567890123
Network:  ##### Full access ########### Full access ❻
Batch:    -----  No access  ------              -----  No access  ------
Local:    -----  No access  ------              -----  No access  ------
Dialup:   -----  No access  ------              -----  No access  ------
Remote:   -----  No access  ------              -----  No access  ------
Expiration:            (none)    Pwdminimum:  6   Login Fails:    52
Pwdlifetime:        ❼ (none)     Pwdchange:   2-APR-1987 15:13
Last Login:            (none)  (interactive), 17-SEP-1987 08:54 (non-interactive
Maxjobs:          0  Fillm:       20  Bytlm:        8192
Maxacctjobs:      0  Shrfillm:     0  Pbytlm:          0
Maxdetach:        0  BIOlm:       10  JTquota:      1024
Prclm:            0  DIOlm:       10  WSdef:         200
Prio:             4  ASTlm:       24  WSquo:         500
Queprio:          0  TQElm:       10  WSextent:     1000
CPU:         (none)  Enqlm:       30  Pgflquo:     10000
Authorized Privileges:
   TMPMBX NETMBX ❽
Default Privileges:
   TMPMBX NETMBX ❽
```

SUMMARY

The following suggestions for enhancing the security of the default DECnet account are keyed to Example 5–5:

❶ Ensure that the DECNET account is the only account in the specified group (to guarantee world-only access to files on the system).

❷ Force the user to use the default command line interpreter.

❸ Do not put the log-in command procedure in the default directory.

❹ Lock the password from being changed.

❺ Make the account CAPTIVE.

❻ Permit only NETWORK ACCESS.

❼ Eliminate PWDLIFETIME.

❽ Do not give the nonprivileged DECnet account more than TMPMBX and NETMBX.

Other notes:

- The log-in command procedure must have execute access from the DECNET account .
- Enable disk quotas on the default disk for the DECNET account.
- Ensure the disk quota has not been exceeded by the DECNET account.
- Ensure the log file version numbers do not reach the RMS limit 32767.
- Ensure the DECNET account has write privilege to the DECNET account directory.
- Do not set up an executor default privileged DECnet account.

LABORATORY EXERCISES

PART I

For the following exercises, log in to VMS accounts SNONPRIV and SPRIV. Execute the DCL commands and note where (on the target node) the NETSERVER.LOG files will be written. This indicates which username the target network process gets associated with. Also, note any special errors or status reflected on the source node side.

OBJECT FAL

```
$ dir target::
    SNONPRIV _____
    SPRIV    _____

$ dir target"":: 
    SNONPRIV _____
    SPRIV    _____

$ dir target"TPRIV":: 
    SNONPRIV _____
    SPRIV    _____
```

OBJECT TASK

```
$ type target::"0=SHOPROX"
    SNONPRIV _____
    SPRIV    _____

$ type target"":"0=SHOPROX"
    SNONPRIV _____
    SPRIV    _____

$ type target"TPRIV"::"0=SHOPROX"
    SNONPRIV _____
    SPRIV    _____
```

OBJECT MAIL

```
$ mail login.com target::system
    SNONPRIV _____
    SPRIV    _____

$ mail login.com target"":system
    SNONPRIV _____
    SPRIV    _____

$ mail login.com target"TPRIV"::system
    SNONPRIV _____
    SPRIV    _____
```

LABORATORY EXERCISES

PART II

For the following exercise, log in to the VMS account SPRIV. Execute the following DCL command procedure (spaces for clarity only):

```
$ run sys$system:ncp
set executor node node-A
sho node node-A characteristics
sho node node-B characteristics
sho node node-C characteristics

set executor node node-B
sho node node-A characteristics
sho node node-B characteristics
sho node node-C characteristics

set executor node node-C
sho node node-A characteristics
sho node node-B characteristics
sho node node-C characteristics
$ exit
```

Replace the nodes *node-?* with your real lab nodenames.

From this data, draw a map of accessibility indicating which nodes can be accessed by which other nodes. Remember that processes with the OPER privilege will be able to override this feature, so use nonprivileged accounts (source and target) to verify your map.

SOLUTIONS TO LABORATORY EXERCISES

PART I

OBJECT FAL

```
$ dir target::
    SNONPRIV ___[DECNET]_____________________________________
    SPRIV    ___[DECNET]_____________________________________

$ dir target"":: 
    SNONPRIV ___[DECNET]_____________________________________
    SPRIV    ___[DECNET]_____________________________________

$ dir target"TPRIV"::
    SNONPRIV ___"...LOGIN FAILURE"___________________________
    SPRIV    ___"...LOGIN FAILURE"___________________________
(this is because of trying to force a proxy, when proxy is not allowed)
```

OBJECT TASK

```
$ type target::"0=SHOPROX"
    SNONPRIV ___[TNONPRIV]__(file wont exist -> VMS error)____
    SPRIV    ___[DECNET]____(file DOES exist, but USER error)_

$ type target"":"0=SHOPROX"
    SNONPRIV ___[DECNET]____(file DOES exist, but USER error)_
    SPRIV    ___[DECNET]____(file DOES exist, but USER error)_

$ type target"TPRIV"::"0=SHOPROX"
    SNONPRIV ___[TPRIV]_____(file DOES exist, works ok)_______
    SPRIV    ___[TPRIV]_____(file DOES exist, works ok)_______
(forced proxy works ok unless proxy is EXPRESSLY disallowed)
```

OBJECT MAIL

```
$ mail login.com target::system
    SNONPRIV ___[TNETMAIL]____(inbound default always works)__
    SPRIV    ___[TNETMAIL]____(inbound default always works)__

$ mail login.com target"":system
    SNONPRIV ___[TNETMAIL]____(inbound default always works)__
    SPRIV    ___[TNETMAIL]____(inbound default always works)__

$ mail login.com target"TPRIV"::system
    SNONPRIV ___[TNETMAIL]____(inbound default always works)__
    SPRIV    ___[TNETMAIL]____(inbound default always works)__
```

MODULE 6
MONITORING AND TUNING

INTRODUCTION

After DECnet key installation and node configuration have taken place, the system manager is responsible for monitoring and, if necessary, tuning the network. Various facilities exist within DECnet-VAX software to monitor the status of the network. The gathered information is then interpreted to determine whether system and network parameters are properly set, or whether changes are necessary to improve performance.

OBJECTIVES

To identify and adjust system and DECnet parameters that affect network performance, a network manager should be able to:

- Identify the system parameters affected by the installation of DECnet software.
- Use the SHOW and MONITOR commands to monitor system performance.
- Make necessary adjustments to system parameters using the SYSGEN utility.

To use NCP to monitor the network, a network manager should be able to:

- Monitor and interpret the values of node, line, and circuit counters.
- Monitor and interpret network events reported by the network event logger.

RESOURCES

- *VMS Networking Manual*, (AA-LA-50A-TE)
- *VMS Network Control Program Manual*, (AA-LA-48A-TE)

MONITORING SYSTEM ACTIVITIES

Network performance is affected by the availability of system resources.

System Parameters

DECnet software can potentially use a large amount of system resources. The network manager and the system manager must work together in adjusting the operating system parameters (SYSGEN) to provide the necessary buffer space for DECnet traffic on the node.

Table 6–1 shows the SYSGEN parameters affected by DECnet software.

Table 6–1: SYSGEN Parameters Affected by DECnet

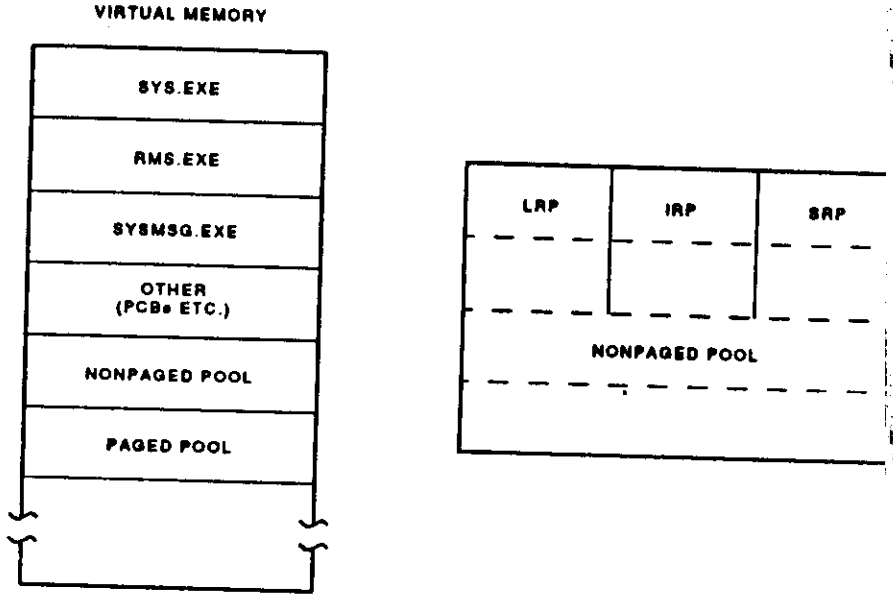
PARAMETER	FUNCTION
NPAGEDYN	Initial amount of space set aside for the nonpaged dynamic pool.
IRPCOUNT	Initial amount of space set aside for the I/O request packet pool (IRP).
LRPCOUNT	Initial amount of space set aside for the large request packet (LRP) pool.
NPAGEVIR	Size to which the nonpaged dynamic pool can be extended.
IRPCOUNTV	Size to which the I/O request packet (IRP) pool can be extended.
LRPCOUNTV	Size to which the LRP pool can be extended.
LRPSIZE	Maximum LRP size in bytes.
LRPMIN	Minimum LRP size in bytes.

Other system parameters that could have an effect on DECnet performance are:

- SRPCOUNT - Space set aside for small request packet (SRP).
- MAXBUF - Maximum size of a buffered I/O transfer.
- MAXPROCESSCNT - Sets the number of concurrent processes per system.

Figure 6–1 illustrates the allocation of the VMS pool.

Figure 6–1: VMS Pool Allocation



Monitoring Memory Resources

System performance strongly depends on the amount of physical memory the system has. For VMS to manage process and system virtual memory, it must divide available physical memory among different functions. The SHOW MEMORY command displays information about the physical memory of the system and the disk files used in the management of virtual memory.

Example 6–1 shows a sample of the SHOW MEMORY output. When the values in the free column become too small, system problems occur. Tuning the system by adjusting various system parameters may be required.

Example 6–1: SHOW MEMORY

```
$ SHOW MEMORY
            System Memory Resources on 26-SEP-1988 10:30:44.50

 Physical Memory Usage (pages):     Total       Free      In Use     Modified
  Main Memory (9.00Mb)              16432      13383        4905          144

  Slot Usage (slots):               Total       Free   Resident    Swapped
  Process Entry Slots                  28         18         10          0
  Balance Set Slots                    25         17          8          0

  Fixed-Size Pool Areas (packets):  Total       Free      In Use       Size
  Small Packet (SRP) List             437        118        319         96
  I/O Request Packet (IRP) List       270        124        146        176
  Large Packet (LRP) List              40         21         19       1648

  Dynamic Memory Usage (bytes):     Total       Free      In Use    Largest
  Nonpaged Dynamic Memory          551936      31552      520384      18096
  Paged Dynamic Memory             183296      65392      117904      64688

  Paging File Usage (pages):                    Free   Reservable      Total

  DISK$VMSRL5:[SYS0.SYSEXE]SWAPFILE.SYS         2000        2000       2000

  DISK$VMSRL5:[SYS0.SYSEXE]PAGEFILE.SYS        12631       -1906      13200

Of the physical pages in use, 3104 pages are permanently allocated to VMS.
```


DECnet Memory Requirements

Example 6–2 shows the output from the SHOW MEMORY command with the /POOL and /FULL qualifiers.

Example 6–2: SHOW MEMORY/POOL/FULL

```
$ SHOW MEMORY/POOL/FULL

            System Memory Resources on 26-SEP-1988 10:02:12.16

Small Packet (SRP) Lookaside List       Packets      Bytes      Pages
    Current Total Size                     2021     194016        379
    Initial Size (SRPCOUNT)                1007      96672        189
    Maximum Size (SRPCOUNTV)               4028     388888        756
    Free Space                              311      29856
    Space in Use                           1710     164160
    Packet Size/Upper Bound (SRPSIZE)                   96
    Lower Bound on Allocation                           32

I/O Request Packet (IRP) Lookaside List Packets      Bytes      Pages
    Current Total Size                     1024     212992        416
    Initial Size (IRPCOUNT)                 701     145808        285
    Maximum Size (IRPCOUNTV)               2804     583232       1140
    Free Space                              134      27872
    Space in Use                            890     185120
    Packet Size/Upper Bound (fixed)                     208
    Lower Bound on Allocation                            97

Large Packet (LRP) Lookaside List       Packets      Bytes      Pages
    Current Total Size                       85      55760        109
    Initial Size (LRPCOUNT)                  55      36080         71
    Maximum Size (LRPCOUNTV)                220     144320        282
    Free Space                               25      16400
    Space in Use                             60      39360
    Packet Size/Upper Bound (LRPSIZE + 80)              656
    Lower Bound on Allocation                           480

Nonpaged Dynamic Memory
    Current Size (bytes)          489472    Current Total Size (pages)      956
    Initial Size (NPAGEDYN)       413184    Initial Size (pages)            807
    Maximum Size (NPAGEVIR)      1240576    Maximum Size (pages)           2423
    Free Space (bytes)             28432    Space in Use (bytes)         461040
    Size of Largest Block          16288    Size of Smallest Block           16
    Number of Free Blocks             76    Free Blocks LEQU 32 Bytes        24

Paged Dynamic Memory
    Current Size (PAGEDYN)        288256    Current Total Size (pages)      563
    Free Space (bytes)             43392    Space in Use (bytes)         244864
    Size of Largest Block          36128    Size of Smallest Block           16
    Number of Free Blocks             65    Free Blocks LEQU 32 Bytes        26
```

Modifying Parameters

Most of the memory required by the network software is allocated from the VMS nonpaged dynamic memory pool. This pool is configured by setting the SRPCOUNT, NPAGEDYN, IRPCOUNT and LRPCOUNT system parameters. When you initially installed DECnet software on your system, the AUTOGEN Utility automatically set these four system parameters to a "best effort" value depending upon the hardware configuration of the system and the system needs.

The four parameters (SRPCOUNT, NPAGEDYN, IRPCOUNT, and LRPCOUNT) should be monitored on a regular basis to verify that the values are neither too high (waste of system resources), or too low (system used inefficiently).

The procedure for modifying a parameter is as follows:

1. Edit the MODPARAMS.DAT file in SYS$SYSTEM to set the value of the system parameter.

```
LRPCOUNT = 15  ! Increased for DECnet Traffic
```

2. Verify the changes made by running AUTOGEN with the GETDATA parameter. Then examine the resulting PARAMS.DAT file in SYS$SYSTEM to see that the changes have been made. Remember PARAMS.DAT should NOT be edited! Changes should be made only to the MODPARAMS.DAT file.

```
$ @SYS$UPDATE:AUTOGEN GETDATA
```

3. When you are satisfied with the changes made to the system parameters, run AUTOGEN to set up the system parameters with the new values.

```
$ @SYS$UPDATE:AUTOGEN GENPARAMS SETPARAMS
```

4. The last step is to run AUTOGEN to reboot your system and use the newly generated system parameter values.

```
$ @SYS$UPDATE:AUTOGEN REBOOT
```


Monitoring Active Processes

To monitor the page-faulting levels of NETACP, use the SHOW PROCESS command as sho in Example 6–3.

Example 6–3: SHOW PROCESS

```
$SHOW PROCESS/CONTIN/ID=pid (process ID of NETACP)

                  Process NETACP                    10:31:55

State             HIB             Working Set          363
Cur/base priority 12/8            Virtual Pages       1239
Current PC        7FFEDF8A        CPU time      000:00:12:10.20
Current PSL       00C00000        Direct I/O           10
Current user SP   7FFA0094        Buffered I/O         22844
PID               00000098        Page faults          203
UIC               [SYSTEM]        Event flags      E0000002
                                                   00000000
```

This display can be used to monitor the NETACP process.

Working Set Changes

If NETACP is faulting heavily, check these items:

- Working set quota size
- Process page count
- Global page count
- Working set extent

The command procedure presented in Example 6–4 checks them for you.

Example 6–4: Monitoring NETACP

```
$! In order to get the PID of the NETACP process,
$! either GROUP or WORLD privilege is required
$!
$ CONTEXT = ""
$! Loop through system process list until the PID of NETACP is located
$ GET_PID:
$ PID = F$PID(CONTEXT)
$ IF PID .EQS. "" THEN EXIT
$ IF F$EXTRACT(0,6,F$GETJPI(PID,"PRCNAM")) .NES. "NETACP" -
  THEN GOTO GET_PID
$ WORKING_SET_QUOTA = F$GETJPI(PID,"WSQUOTA")
$ SHOW SYMBOL WORKING_SET_QUOTA
$ WORKING_SET_SIZE = F$GETJPI(PID,"WSSIZE")
$ SHOW SYMBOL WORKING_SET_SIZE
$ PROCESS_PAGE_COUNT = F$GETJPI(PID,"PPGCNT")
$ SHOW SYMBOL PROCESS_PAGE_COUNT
$ GLOBAL_PAGE_COUNT = F$GETJPI(PID,"GPGCNT")
$ SHOW SYMBOL GLOBAL_PAGE_COUNT
$ WORKING_SET_EXTENT = F$GETJPI(PID,"WSEXTENT")
$ SHOW SYMBOL WORKING_SET_EXTENT
$ EXIT
```

To increase the working set quota of NETACP, define the following logical before DECnet software is started.

```
$ DEFINE/SYSTEM NETACP$MAXIMUM_WORKING_SET (new value)
```

To increase the working set extent of NETACP, define the following logical before DECnet software is started.

```
$ DEFINE/SYSTEM NETACP$EXTENT (new value)
```

NOTE

The logical definitions above only remain while the system is running, unless they are defined permanently in a system startup file (SYSLOGICALS.COM, for example).

MONITOR Utility

The VMS MONITOR Utility is a program that displays information about the use of system resources. Some of this information overlaps with the SHOW MEMORY and SHOW SYSTEM commands. MONITOR information also helps you to properly tune the operating system.

The MONITOR utility is different from any other utility that shows information because MONITOR can:

- Display one class of information after another.
- Summarize statistics over a long period of time.
- Record information in a disk file.
- Play back information it has recorded.

You can issue an individual MONITOR command at the DCL prompt, or enter the MONITOR utility and issue MONITOR commands from within the utility. Both methods display the information about classes that you select. Both methods use the same class names and qualifiers.

To enter an individual MONITOR command at the DCL prompt, type:

$ MONITOR class-name(s)/*qualifiers*

There are three classes of interest to the network manager:

- DECnet
- POOL
- SYSTEM

Example 6–5, Example 6–6, and Example 6–7 show the output from each of these classes.

Example 6–5: MONITOR DECnet

```
$ MONITOR DECNET
                              VMS Monitor Utility
                               DECNET STATISTICS
                                 on node LUIGI         From: 26-SEP-1988 10:44:03
                                   SUMMARY             To:   26-SEP-1988 10:44:33

                                  CUR         AVE         MIN         MAX

Arriving Local Packet Rate        0.00        0.33        0.00        0.66
Departing Local Packet Rate        0.99        0.43        0.00        0.99

Arriving Trans Packet Rate        0.00        0.00        0.00        0.00
Trans Congestion Loss Rate        0.00        0.00        0.00        0.00

Receiver Buff Failure Rate        0.00        0.00        0.00        0.00
LRPs Available                   28.00       28.00       24.00       30.00
```

Example 6–6: MONITOR POOL

```
$ MONITOR POOL
                              VMS Monitor Utility
                           NONPAGED POOL STATISTICS
                                 on node LUIGI         From: 26-SEP-1988 10:51:20
                                   SUMMARY             To:   26-SEP-1988 10:52:25

                                  CUR         AVE         MIN         MAX

SRPs Available                  379.00      379.00      379.00      379.00
SRPs In Use                    1429.00     1429.00     1429.00     1429.00

IRPs Available                  163.00      163.66      163.00      165.00
IRPs In Use                     723.00      722.33      721.00      723.00

LRPs Available                   42.00       42.00       42.00       42.00
LRPs In Use                      39.00       39.00       39.00       39.00

Dynamic Bytes Available       66592.00    66592.00    66592.00    66592.00
Dynamic Bytes In Use         435168.00   435168.00   435168.00   435168.00
Holes In Pool                    60.00       59.66       59.00       60.00
Largest Block                 40512.00    40512.00    40512.00    40512.00
Smallest Block                   16.00       16.00       16.00       16.00
Blocks Less or Eq 32 Bytes        5.00        5.00        5.00        5.00
```


Example 6–7: MONITOR SYSTEM

```
$ MONITOR SYSTEM

Node: ARUBA                            VMS Monitor Utility      29-SEP-1988 09:29:30
Statistic: CURRENT                      SYSTEM STATISTICS
                                                                 Process States
            + CPU Busy (87)               -+          LEF:     30        LEFO:      0
            |***********************        |          HIB:     14        HIBO:      0
CPU      0  +--------------------------+ 100          COM:      1        COMO:      0
            |********                  |          PFW:      0        Other:     1
            +--------------------------+          MWAIT:    0
            Cur Top: NETACP (32)                                Total: 46

            + Page Fault Rate (52)      -+          + Free List Size (2922)    -+
            ||************              |          |*****                     | 13K
MEMORY   0  +--------------------------+ 100   0  +--------------------------+
            |***********               |          |*************             | 500
            +--------------------------+          + Modified List Size (264) +
            Cur Top: NETACP (45)

            + Direct I/O Rate (6)       -+          + Buffered I/O Rate (23)   -+
            |**                        |          |***                       |
I/O      0  +--------------------------+ 60    0  +--------------------------+ 150
            |**                        |          |                          |
            +--------------------------+          +--------------------------+
            Cur Top: REID (5)                     Cur Top: WOZNICKI (4)
```

MONITORING NETWORK ACTIVITY

Network activity can be monitored in one of two ways:

- The NCP command SHOW/LIST
- The event logging facility and the SET LOGGING command

Monitoring the Network with NCP

The SHOW and LIST commands in NCP provide information on the following:

- EXECUTOR - The node defined to be the executor of the NCP commands.
- NODE - A computer within the network.
- CIRCUIT - A logical link between two nodes.
- LINE - A physical point-to-point connection.

The following parameters are selectable:

- CHARACTERISTICS - Lists static information.
- STATUS - Lists dynamic information.
- SUMMARY - Condensed list of CHARACTERISTICS and STATUS.
- COUNTERS - Lists all counters for the parameter.

Command keywords:

- KNOWN - Displays information about components known to the local node.
- ACTIVE - Displays information about all active components.

Monitoring Network Counters

NCP reports the contents of all counters in decimal notation. Counter content displays with an angle bracket (>) indicate that the counter has overflowed.

To reset counters for the network components, use the NCP ZERO command as follows:

```
NCP>ZERO EXECUTOR COUNTERS
NCP>ZERO KNOWN CIRCUIT COUNTERS
NCP>ZERO LINE DUP-0 COUNTERS
NCP>ZERO NODE CYCLPS COUNTERS
```

To regulate the frequency with which counters are logged and when counters are zeroed, use the NCP SET command with the COUNTER TIMER parameter as follows:

```
NCP> SET EXECUTOR COUNTER TIMER 600
NCP> SET NODE DEMON COUNTER TIMER 600
NCP> SET LINE UNA-0 COUNTER TIMER 100
NCP> SET CIRCUIT DMC-0 COUNTER TIMER 100
```

To command a remote node to execute a single command, use the NCP TELL command prefix as follows:

```
NCP>TELL BOSTON SHOW KNOWN LINES COUNTERS
```

The examples on the following pages illustrate the use of NCP monitoring commands.

Monitoring Node Counters

Example 6–8: Executor Counters

```
NCP>SHOW EXECUTOR COUNTERS

Node Counters as of 26-SEP-1988 10:44:54

Executor node = 26.60 (LUIGI)

     >65534  Seconds since last zeroed          ❶
      26008  Bytes received
      25978  Bytes sent
       1012  Messages received
       1022  Messages sent
         10  Connects received
         10  Connects sent
          0  Response timeouts
          0  Received connect resource errors
          6  Maximum logical links active
          0  Aged packet loss
          0  Node unreachable packet loss
          0  Node out-of-range packet loss     ❷
          0  Oversized packet loss
          0  Packet format error               ❸
          0  Partial routing update loss       ❹
          0  Verification reject
```

Notes on Example 6–8:

❶ 65534 is the maximum value for the seconds since zeroed parameter.

❷ If greater than 0 - May indicate that the Maximum Address value is too low.

❸ If greater than 0 - May indicate circuit problems. Check counters.

❹ If greater than 0 - May indicate that the Maximum Address value is too low.

Monitoring Circuit Counters

Example 6–9: Circuit Counters

```
NCP>SHOW KNOWN CIRCUIT COUNTERS

Known Circuit Counters as of 26-SEP-1988 10:48:11

Circuit = QNA-0

      >65534  Seconds since last zeroed
       98217  Terminating packets received
      198880  Originating packets sent
           0  Terminating congestion loss
           0  Transit packets received
           0  Transit packets sent
           0  Transit congestion loss
         102  Circuit down
           0  Initialization failure
          93  Adjacency down
        4306  Peak adjacencies
      362855  Data blocks sent
   117303487  Bytes sent
      247482  Data blocks received
    13971808  Bytes received
           0  Unrecognized frame destination
           0  User buffer unavailable
```

Monitoring Line Counters

Example 6–10: Line Counters

```
NCP>SHOW KNOWN LINE COUNTERS
Known Line Counters as of 26-SEP-1988 10:57:46
Line = QNA-0
      >65534  Seconds since last zeroed
      878564  Data blocks received
      732414  Multicast blocks received
           0  Receive failure
    46091567  Bytes received
    37794676  Multicast bytes received
           0  Data overrun
      456451  Data blocks sent
      208465  Multicast blocks sent
         217  Blocks sent, multiple collisions
         222  Blocks sent, single collision
           0  Blocks sent, initially deferred
   125767752  Bytes sent
    15053793  Multicast bytes sent
        8361  Send failure, including:
                Carrier check failed
                Short circuit
        8361  Collision detect check failure
           0  Unrecognized frame destination
           0  System buffer unavailable
           0  User buffer unavailable
```


Using Node Counters

Example 6–11: Response Timeouts

```
NCP>SHOW EXECUTOR COUNTERS
Node Counters as of 26-SEP-1988 10:44:54
Executor node = 26.60 (LUIGI)
      >65534  Seconds since last zeroed
       26008  Bytes received
       25978  Bytes sent
        1012  Messages received
        1022  Messages sent
          10  Connects received
          10  Connects sent
         323  Response timeouts
           0  Received connect resource errors
           6  Maximum logical links active
           0  Aged packet loss
           0  Node unreachable packet loss
           0  Node out-of-range packet loss
           0  Oversized packet loss
           0  Packet format error
           0  Partial routing update loss
           0  Verification reject
```

Example 6–12: Resource Errors

```
NCP>SHOW EXECUTOR COUNTERS

Node Counters as of 26-SEP-1988 10:44:54

Executor node = 26.60 (LUIGI)

      >65534  Seconds since last zeroed
       26008  Bytes received
       25978  Bytes sent
        1012  Messages received
        1022  Messages sent
          10  Connects received
          10  Connects sent
           0  Response timeouts
         212  Received connect resource errors
           6  Maximum logical links active
           0  Aged packet loss
           0  Node unreachable packet loss
           0  Node out-of-range packet loss
           0  Oversized packet loss
           0  Packet format error
           0  Partial routing update loss
           0  Verification reject
```


Using Circuit Counters

Example 6–13: Interpreting Circuit Counters

```
NCP>SHOW KNOWN CIRCUIT COUNTERS

Known Circuit Counters as of 26-SEP-1988 17:00:37

Circuit = DMC-0

       60004  Seconds since last zeroed
       28236  Terminating packets received
       56348  Originating packets sent
           0  Terminating congestion loss
       21769  Transit packets received
        3137  Transit packets sent
           0  Transit congestion loss
          48  Circuit down   <CO>(2
           0  Initialization failure
    20148464  Bytes received
    13489501  Bytes sent
      208111  Data blocks received
      189750  Data blocks sent
           0  Data errors outbound
           1  Data errors inbound, including:
                NAKs sent, header block check error
           0  Local buffer errors
          80  Remote buffer errors  <CO>(1)
           0  Local reply timeouts
           0  Remote reply timeouts

Circuit = UNA-0

       60004  Seconds since last zeroed
      110417  Terminating packets received
       76593  Originating packets sent
           0  Terminating congestion loss
        3137  Transit packets received
       21769  Transit packets sent
         304  Transit congestion loss  <CO>(3)
           0  Circuit down
           0  Initialization failure
      130353  Data blocks sent
    10917661  Bytes sent
      474384  Data blocks received
    43594335  Bytes received
           0  Unrecognized frame destination
           0  User buffer unavailable
```

Example 6–14: Excessive Multicast

```
NCP>SHOW KNOWN LINE COUNTERS

Known Line Counters as of 26-SEP-1988 10:57:46

Line = QNA-0

      >65534  Seconds since last zeroed
      878564  Data blocks received
      324949  Multicast blocks received
           0  Receive failure
    46091567  Bytes received
    37794676  Multicast bytes received
           0  Data overrun
      456451  Data blocks sent
      208465  Multicast blocks sent
         217  Blocks sent, multiple collisions
         222  Blocks sent, single collision
           0  Blocks sent, initially deferred
   125767752  Bytes sent
    15053793  Multicast bytes sent
        8361  Send failure, including:
                Carrier check failed
                Short circuit
        8361  Collision detect check failure
           0  Unrecognized frame destination
           0  System buffer unavailable
           0  User buffer unavailable
```


Example 6–15: Collision Detect Failures

```
NCP>SHOW KNOWN LINE COUNTERS

Known Line Counters as of 26-SEP-1988 10:58:50

Line = QNA-0

      >65534  Seconds since last zeroed
      878564  Data blocks received
      324949  Multicast blocks received
           0  Receive failure
    46091567  Bytes received
    37794676  Multicast bytes received
           0  Data overrun
      456451  Data blocks sent
      208465  Multicast blocks sent
         217  Blocks sent, multiple collisions
         222  Blocks sent, single collision
           0  Blocks sent, initially deferred
   125767752  Bytes sent
    15053793  Multicast bytes sent
        8361  Send failure, including:
                Carrier check failed
                Short circuit
        8361  Collision detect check failure
           0  Unrecognized frame destination
           0  System buffer unavailable
           0  User buffer unavailable
```

Event Logging

The network software logs significant events that occur during network operation, including:

- Circuit and node counter activity
- Changes in circuit, line, and node states
- Lost event reporting
- Service requests
- Passive loopback
- Routing performance and error counters
- Data transmission performance and error counters

The logging component is defined by the device or process that records the events released by the event logger. There are three types of logging components:

- Logging console - A terminal or file that receives events on the sink node in a format the user can read.
- Logging File - A user-specific file on the sink node that receives events in the standard Digital Network Architecture (DNA) binary format.
- Logging Monitor - A system or user-specified program that receives and processes DNA events.

Data may be filtered or not filtered:

- Filtering is logging only those events specified in the system's event list, which you can set using NCP.
- Events are coded as n.m, where n is the event class, and m is the event type within the event class category.

Sink Node

A sink node collects the logging information from several nodes on a network and outputs tl information to a central device (console, file, or monitor). When you define a sink node in tl logging database, the network management listener (NML) stores the executor node as addre: zero.

The logging database is transportable to other nodes.

The event list follows the EVENTS parameter. Only one class per command is allowed; howeve multiple event types per command are permitted. They must be specified in ascending order.

To enable logging of all events, type:

```
NCP>SET LOGGING MONITOR KNOWN EVENTS
NCP>SET LOGGING MONITOR STATE ON
```

To enable event logging related to circuits on a central node or network, type:

```
NCP>SET LOGGING (MONITOR,CONSOLE,FILE) EVENTS n
NCP>SET LOGGING (MONITOR,CONSOLE,FILE) SINK NODE MATCH
NCP>SET LOGGING (MONITOR,CONSOLE,FILE) STATE ON
```

To output network logging information to a special terminal, type:

```
NCP>SET LOGGING CONSOLE EVENTS 0
NCP>SET LOGGING CONSOLE NAME TTC3
NCP>SET LOGGING CONSOLE STATE ON
```

/ent Message Format

event message takes the format below. The components of an event message are described Table 6–2.

```
EVENT TYPE class.type, event-text
from node address [node-name],Occurred [dd-mm-yy]
hh:mm:ss.uu
component type component name
descriptive text
```

ble 6–2: Event Message Format

/ENT COMPONENT	DESCRIPTION
_ASS	The layer in which the event occurred.
/PE	The specific type of event for the class.
/ENT-TEXT	The text describing the event.
DDRESS	The address of the node at which the event occurred.
ODE NAME	The name of the node at which the event occurred.
D-MM-YY	The date on which the event occurred.
H:MM:SS:UU	The time at which the event occurred.
OMPONENT TYPE	The circuit, node, or line.
EXT	Information that describes the event.

xample 6–16 shows an actual event message:

xample 6–16: An Event Message

```
vent type 4.7,Circuit down - circuit fault
ccurred 26-SEP-1988 17:15:15 on node 4 (ENT)
ircuit DMC-0
ine synchronization lost
```


Table 6–3 lists the different classes of events.

Table 6–3: Event Class

EVENT CLASS	DESCRIPTION
0	Network Management Layer
1	Applications Layer
2	Session Control Layer
3	End Communication Layer
4	Routing Layer
5	Data Link Layer
6	Physical Link Layer
7-31	Reserved
32-63	RSTS system specific
64-95	RSX system specific
96-127	TOPS-20 system specific
128-159	VMS system specific
160-479	Reserved for future use

DECnet-VAX software logs events only for event classes 0,3,4,128-159. If you attempt to turn on logging for any other event, it does not log.

Event Types

The event types within the event classes 0,3,4, and 128-159 that are logged by DECnet-VAX software are as follows:

The Network Management Layer class event types are:

- 0.0 Event records lost
- 0.6 Passive loopback
- 0.7 Aborted service request

The End Communication Layer class event types are:

- 3.0 Invalid message
- 3.1 Invalid flow control

The Routing Layer class event types are:

- 4.0 Aged packet loss
- 4.1 Node unreachable packet loss
- 4.2 Node out-of-range packet loss
- 4.3 Oversized packet loss
- 4.4 Packet format error
- 4.5 Partial routing update loss
- 4.6 Verification reject
- 4.7 Circuit down, circuit fault
- 4.8 Circuit down
- 4.9 Circuit down, operator initiated
- 4.10 Circuit up
- 4.11 Initialization failure, line fault
- 4.12 Initialization failure
- 4.13 Initialization failure, operator initiated
- 4.14 Node reachability change
- 4.15 Adjacency up
- 4.16 Adjacency rejected
- 4.17 Area reachability change
- 4.18 Adjacency down
- 4.19 Adjacency down, operator initiated

The VMS system specific class events are:

- 128.1 DAP CRC error detected
- 128.2 Duplicate PHASE 2 address error
- 128.3 Process created
- 128.4 Process terminated

NOTE

Event Logger types 4.2, 4.5, 4.7, 4.8, 4.9, 4.10, and 128.1 are especially indicative of some sort of network problem. Action should be taken on them immediately.

DECnet Test Sender/DECnet Test Receiver Utility

DECnet Test Sender (DTS)/DECnet Test Receiver (DTR) are the DECnet transmitter and receiver test programs that exercise network task-to-task capabilities. DTSEND and DTRECV are the DECnet-VAX implementations of these programs.

The data test is composed of the following subtests:

- Sink Test - DTR ignores all data received during this test.
- Sequence Test - If a message is received out of sequence, DTR aborts the logical link and the test.
- Pattern Test - Data messages with a sequence number and a data pattern are sent; DTR aborts the logical link if received data does not match the sent data.
- Echo Test - DTR transmits all data messages received back to DTS during this test.

To invoke DTS and run the data test, issue the command

```
$ RUN SYS$SYSTEM:DTSEND
```

as shown in Example 6–17.

Example 6–17: DECnet Test Sender/DECnet Test Receiver Output

```
$ RUN SYS$SYSTEM:DTSEND

DTS Version xxx initiated on dd-mm-yy hh:mm:ss

-Test:  DATA/PRINT/TYPE=SEQ/SIZE=128/SECONDS=10/FLOW=MESSAGE

-DTS-S-NORMAL, normal successful completion

Test parameters:
Test duration (sec)  10
Target nodename
Line speed (baud)    1000000
Message size (bytes) 128

Summary statistics:
Total messages XMIT  788    RECV   0
Total bytes XMIT     100864
Messages per second  78
Bytes per second     10088
Line thruput (baud)  80691
%Line utilization    8.0
```


NETWORK PERFORMANCE PARAMETERS

Several network parameters affect performance on a node. They are:

- Incoming timer
- Outgoing timer
- Buffer size
- Maximum buffers
- Pipeline quota
- Circuit costs
- Maximum costs
- Maximum hops
- Maximum visits

Network Parameter Tuning Hints

Follow these guidelines in tuning your node:

- Incoming and Outgoing timer—Default is recommended unless you have a large network with many hops or slow lines.
- Buffer size—Should definitely be the same for all routing nodes.
- Maximum buffers—Default is usually sufficient, but may need to be raised if there are several high speed (56K plus) circuits or long delay links.
- Pipeline quota—High value enhances performance, but uses up nonpaged memory pool; satellite links may require an increase.
- Circuit costs—Use defaults.
- Maximum costs and Maximum hops—Network size dependent with consideration of possible failures given.
- Maximum visits—Should be two to three times maximum hops.

SUMMARY

Network performance can suffer due to the performance of a single node. Inadequate buff sizes or an under-sized pool can lead to inefficient utilization of system resources and decreas network throughput.

The network load on each system is different; therefore, system monitoring should be a routi procedure. You can use utilities and DCL commands such as MONITOR, SHOW MEMOR SHOW PROCESS and SHOW SYSTEM for monitoring system performance. If system p rameters need to be modified, then the standard procedure of running AUTOGEN should b followed.

DECnet software automatically collects certain network statistics on nodes, lines, and circuit These statistics are known as counters; for network monitoring, counters are a critical sourc of information. You can use the NCP SHOW command to display counter values to monitor th operation of the running network.

DECnet software monitors a wide range of network activities called events. Each event rep resents a significant occurrence in the network, and reporting the events may prove useful i monitoring network performance.

You can use the event logger to log all, or only certain, network events. In addition, you ca instruct the event logger to log network events at a remote console, in an event file, or sen them to an event monitor task.

When DECnet software was first brought up on your system, the major network parameters wer set with default values. Since each network is different, you may find it necessary to alter thes network parameters to improve overall network performance.

LABORATORY EXERCISES

Use the MONITOR, SHOW SYSTEM, SHOW PROCESS, and SHOW MEMORY utilities, as presented in the module, to answer the following questions.

1. Examine the NETACP process on your system.
   - What is its current priority?
   - How many times has it page faulted since the process has been active?
   - How much actual memory is it using? (HINT: No single command will provide you with this answer.)
2. Which is currently greater on your system—the arriving local packet rate or the departing local packet rate?
3. What is the average number of LRPs available to DECnet software on your system? How does this differ from the maximum?
4. Which process on your system is using the most CPU? The most memory?

Use NCP for the following exercises.

5. Since the counters were last zeroed, has your node sent or received more messages?
6. Look at the counters for a routing node in your network. Has there been more route-through traffic at that node or more local traffic?
7. As a network manager, you will want to monitor your system over time to be aware of changes that occur. You can do this manually at regularly scheduled intervals, or you can set up a command procedure to do it for you. With this in mind, write a command procedure that will do the following:
   - Write the current values of node, line, and circuit counters to a file.
   - Zero the counters.
   - Submit itself to run again in 24 hours.

   Test your command procedure by changing the interval to 5 minutes instead of 24 hours.

SOLUTIONS TO LABORATORY EXERCISES

Use the MONITOR, SHOW SYSTEM, SHOW PROCESS, and SHOW MEMORY utilities, as presented in the module, to answer the following questions.

1. Examine the NETACP process on your system.
   - What is its current priority?

     ```
     $ SHOW PROC/CONT/ID=<EMPHASIS>(pid of NETACP)
     ```

   - How many times has it page faulted since the process has been active?

     ```
     $ SHOW PROC/CONT/ID=<EMPHASIS>(pid of NETACP)
     ```

   - How much actual memory is it using? (HINT: No single command will provide you with this answer.)

     Use lexical functions to determine the process page count and the global page count, and add the two together. (See Example 6–4)
2. Which is currently greater on your system—the arriving local packet rate or the departing local packet rate?

   ```
   $ MONITOR DECNET
   ```

3. What is the average number of LRPs available to DECnet software on your system? How does this differ from the maximum?

   ```
   $ MONITOR DECNET
   ```

4. Which process on your system is using the most CPU? the most memory?

   ```
   $ MONITOR SYSTEM
   ```

Use NCP for the following exercises.

5. Since the counters were last zeroed, has your node sent or received more messages?

```
NCP> SHOW EXECUTOR COUNTERS
```

6. Look at the counters for a routing node in your network. Has there been more route-through traffic at that node or more local traffic?

```
NCP> SHOW KNOWN CIRCUIT COUNTERS
```

7. As a network manager, you will want to monitor your system over time to be aware of changes that occur. You can do this manually at regularly scheduled intervals, or you can set up a command procedure to do it for you. With this in mind, write a command procedure that will do the following:

   - Write the current values of node, line, and circuit counters to a file.
   - Zero the counters.
   - Submit itself to run again in 24 hours.

   Test your command procedure by changing the interval to 5 minutes instead of 24 hours.

```
$! ZERO_COUNTERS.COM  - will write circuit counters and executor
$!                      counters to a file in SYS$MANAGER, then
$!                      zero the counters and resubmit itself to
$!                      batch to execute again in 24 hours.
$!
$set process/priv=all
$mc ncp show executor counters to sys$manager:executor_counters.tmp
$mc ncp zero executor counters
$rename sys$manager:executor_counters.tmp counters.lis
$
$mc ncp show known circuit counters to sys$manager:circuit_counters.tmp
$mc ncp zero known circuit counters
$append sys$manager:circuit_counters.tmp counters.lis
$delete sys$manager:circuit_counters.tmp;
$
$mc ncp show known line counters to sys$manager:line_counters.tmp
$mc ncp zero known line counters
$append sys$manager:line_counters.tmp counters.lis
$delete sys$manager:line_counters.tmp;
$
$submit/noprint/after="TOMORROW+00:15" ZERO_COUNTERS.COM/queue=sys$batch
$exit
```


MODULE 7
FAULT ISOLATION

INTRODUCTION

Like a computer system, a network is prone to problems. These problems may occur in the hardware that is used for communication, in the software running on the computer systems in the network, or in the network parameters set on each system.

This module identifies some of the common network problems that occur and shows methods for determining and correcting the problems.

This module describes how to systematically isolate a hardware or software problem by starting at the User Layer of the local node, working toward the User Layer of the remote destination node, and eliminating components as the source of the problem. Some of the tools introduced in this module are node level, circuit level, and Ethernet circuit-level testing, and modem testing.

OBJECTIVES

To test the network, the network manager should be able to:

- Identify the types of problems occurring on the network.
- Select and perform loopback tests to isolate a fault to a hardware or software level from the following tests:
  - — Node-level
  - — Circuit-level
  - — File-transfer
  - — Ethernet circuit
  - — Modem

RESOURCES

- *VMS Network Control Progam Reference Manual*, (AA-LA50A-TE)
- *VMS Networking Manual*, (AA-LA48A-TE)

DECnet CONFIGURATION PROBLEMS

One way to isolate faults in the network is to eliminate the possible causes systematically. One of the most common faults leading to network failure occurs when network software is not properly configured. Common problems include:

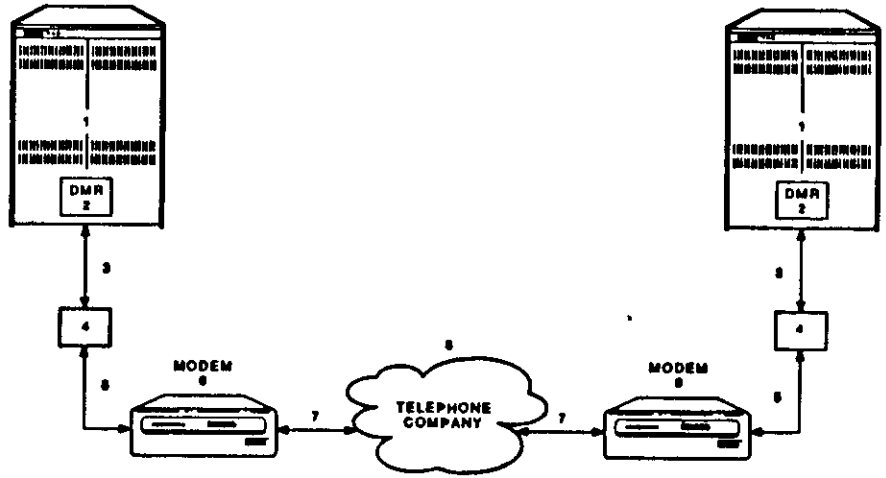
- Defined node addresses not unique
- Defined node names not unique
- Buffers too small
- Not enough system buffers
- Routing passwords incorrect
- Node numbers out of range
- Maximum visits too small
- Circuit costs improperly set
- No default DECnet account
- Invalid access control
- Insufficient resources
- Improperly set timers
- Remote node in shut state

The first step in the fault isolation process is to check that the DECnet software is properly set up.

TYPES OF FAULTS

Figure 7–1 highlights the different places where faults can occur in a point-to-point conn

Figure 7–1: Places Where Faults Can Occur



POSITION	FAULT
1	SOFTWARE PROBLEM ON NODE
2	CONTROLLER PROBLEM
3	RIBBON CABLE TO DISTRIBUTION PANEL
4	DISTRIBUTION PANEL
5	CABLE PROBLEM TO MODEM
6	MODEM PROBLEM
7	CABLE TO TELEPHONE COMPANY BLOCK
8	TELEPHONE COMPANY LINE

MKV_81000_90

SYSTEMATIC ELIMINATION

Some problems that may appear to be network faults are actually specific to the system, or even the user. When a user reports a problem using a network utility, take the steps presented in Table 7–1.

Table 7–1: Steps for Systematic Elimination of Problem Causes

	STEP	PURPOSE
1.	Check the syntax of the user's command.	Eliminates user error as the source of the problem.
2.	Check the logical names and symbols the user has defined.	Eliminates the user's environment as the source of the problem.
3.	Try to execute the utility to the local node (0::).	Ensures that the utility functions properly on the local node, eliminating the local software as the source of the problem.
4.	Try to execute the utility to a different remote node.	If successful, further eliminates the possibility of problems with the local software.
5.	Try to perform other network operations to the remote node.	Determines whether it is possible to establish any logical link to the remote node. If so, eliminates the physical connection as the source of the problem.
6.	Log in to the remote node, and try to execute the utility locally on that node.	Determines whether the object is properly configured on the remote node, eliminating the target object as the source of the problem.

If, after performing these steps, you have not found the source of the problem, or if you have determined that there is a problem establishing a logical link with the remote node, you may want to test the connection using loopback tests.

LOOPBACK TESTING STRATEGY

DECnet software provides testing routines for several types of network configurations, including Ethernet and Point-to-Point configurations.

The steps are the same for Ethernet and Point-to-Point testing:

- Local tests
- Link level tests

Table 7–2 illustrates the types of tests available:

Table 7–2: Testing Strategy Chart

STEPS FOR ETHERNET	STEPS FOR POINT-TO-POINT
Local Tests	Local Tests
Local node loopback	Local node loopback
Controller loopback	Controller loopback
Link Level Tests	Link Level Tests
Ethernet node loopback test	Controller loopback
Ethernet loop assist tests	Circuit loopback w/loopback connector
- Full assist	Local modem loopback test
- Receive assist	Remote modem loopback test
- Transmit assist	Local-to-remote loop node test (adjacent)
	Software loopback test (adjacent)
	Local-to-remote loopback test

LOCAL TESTS

Local tests examine the logical link capabilities of the local system by exchanging test data between DECnet processes on that system. Local tests are identical for Ethernet and point-to-point configurations. The tests include:

- Local-to-local loopback test - Evaluates local software using an internal logical link.
- Local-to-local loop node test - Evaluates local software and controller.

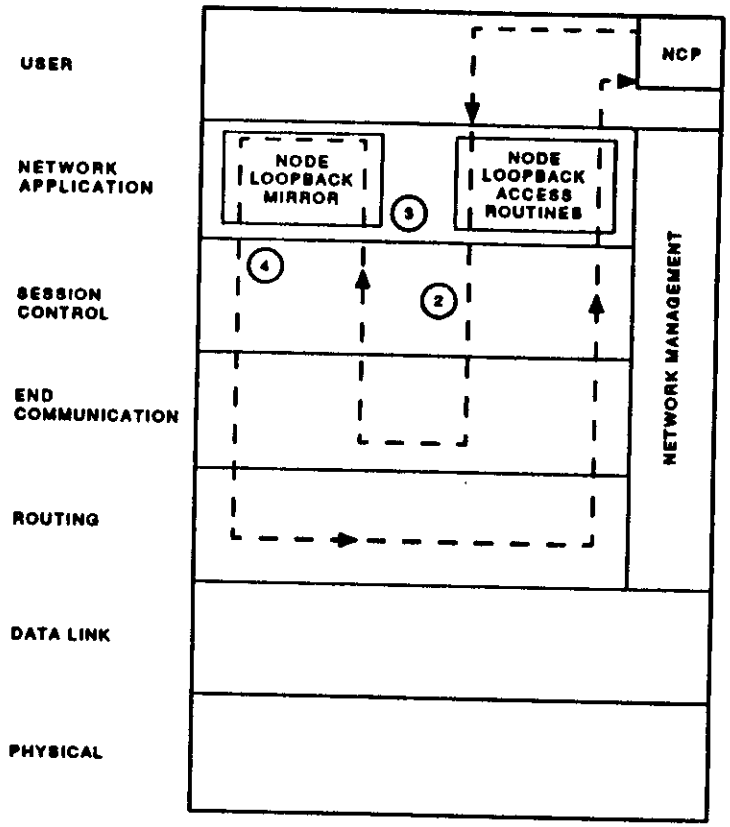
Local-to-Local Loopback Test

- The local loopback test evaluates the local DECnet software using an internal logical link path.
- It tests the ability of the local node to both initiate and accept logical link connections properly and to send and receive data.
- On a local loopback test only the local DECnet software down to the Routing Layer is tested.
- If this test fails the Event Logger messages could indicate the cause of the failure.
- The command shown in Example 7–1 is illustrated by Figure 7–2.

Example 7–1: Local-to-Local Loopback Test

```
NCP>LOOP EXECUTOR COUNT 30 LENGTH 128
```

Figure 7–2: Local-to-Local Loopback Test



Local-to-Local Loop Node Test

The local-to-local loop node test performs the following tasks:

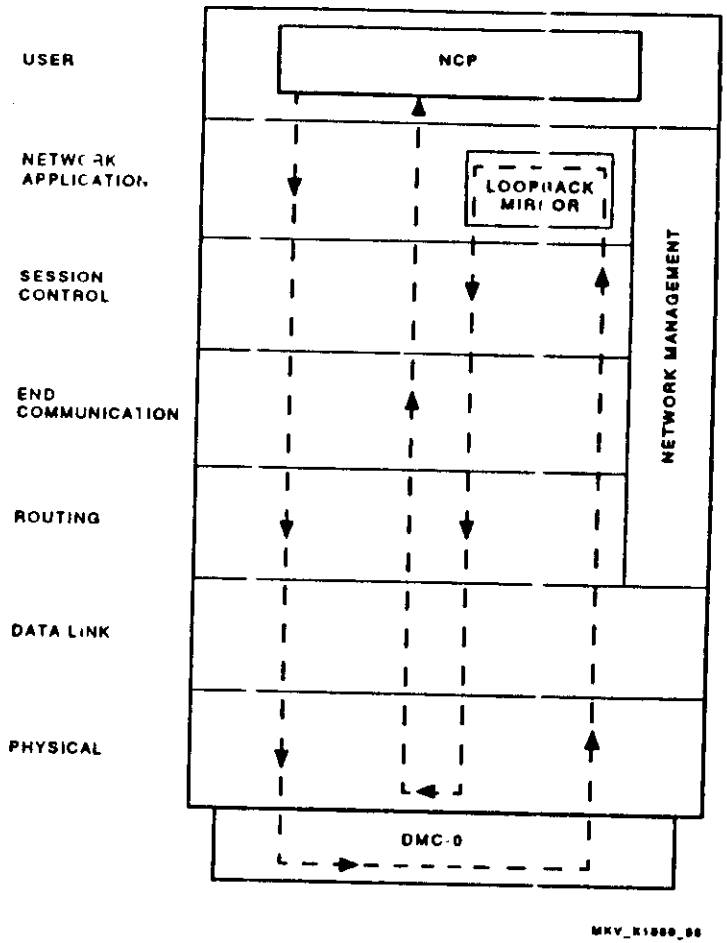
- Verifies the local Routing Layer software and the controller on the local node.
- Communications are looped internally in the communications device without any type of external loopback circuitry.
- The procedure is to turn off the line, set the controller to loopback mode and turn on the line and circuit, set up a fictitious loop node name for the given line and enter the LOOP NODE command using the loop node name.
- While this is a normal logical link, the line is unusable for all other traffic.
- If this test fails, the problem is with the controller on the local node.

The commands shown in Example 7–2 are illustrated by Figure 7–3.

Example 7–2: Local-to-Local Loop Node Test

```
NCP>SET LINE DMC-0 STATE OFF
NCP>SET LINE DMC-0 CONTROLLER LOOPBACK
NCP>SET LINE DMC-0 STATE ON
NCP>SET CIRCUIT DMC-0 STATE ON
NCP>SET NODE TESTER CIRCUIT DMC-0
NCP>LOOP NODE TESTER COUNT 10 LENGTH 32
```


Figure 7–3: Local-to-Local Loop Node Test



TESTING THE LINK

The Network Control Program (NCP) provides mechanisms for testing the link between local and remote nodes on a DECnet network. There are tests for both Ethernet and point-to-point DECnet configurations. These tests check the operation of the network between the local and remote nodes being tested.

The tests specifically for Ethernet configurations are:

- Ethernet node loopback test
- Ethernet loop assist tests with:
  - — Full assistance
  - — Receive assistance
  - — Transmit assistance

The tests for point-to-point configurations include:

- Controller loopback tests
- Circuit loopback test with loopback connector
- Local modem loopback test
- Remote modem loopback test
- Local to remote loopback test (adjacent)
- Software loopback test (adjacent)
- Local to remote loopback test

Ethernet Tests

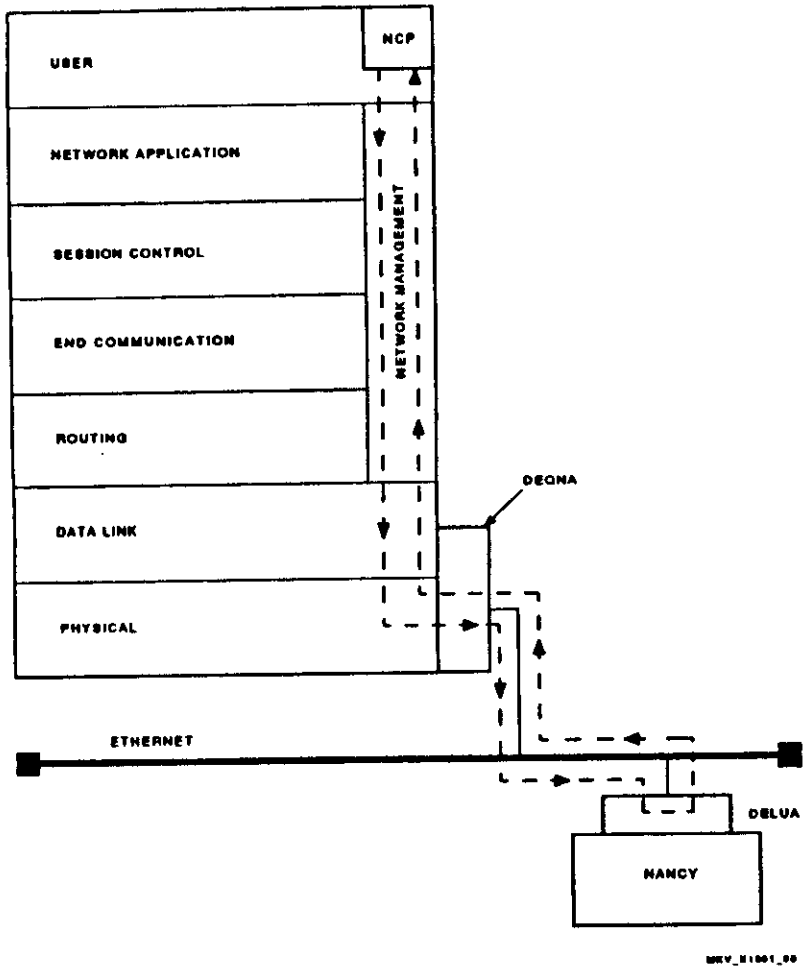
Ethernet Node Loopback Test

- The node loopback test is used for looping messages to remote systems over Ethernet LANs.
- Tests of this type allow you to determine the capability of both the local and remote controllers to send and receive messages.
- In these cases, you are required to supply the Ethernet physical address, the node name, or node address, of the node that is tested.
- The commands shown in Example 7–3 are illustrated by Figure 7–4.

Example 7–3: Ethernet Node Loopback Test

```
NCP>LOOP CIRCUIT UNA-0 PHYSICAL ADDRESS AA-01-23-45-67-89
NCP>LOOP CIRCUIT UNA-0 NODE NANCY
```

Figure 7–4: Ethernet Node Loopback Test



Loopback Assistance on the Ethernet

To perform the assistant loopback test you must provide the:

- DECnet name, address, or physical address of the assistant node
- DECnet name, address, or physical address of the destination node
- Number of times to execute the test
- Type of assistance to be provided

There are three types of assistance that can be provided:

- FULL ASSISTANCE - The node relays the test message both on the way to and back from the destination node, demonstrated by Example 7–4 and Figure 7–5.

```
NCP>LOOP CIRCUIT UNA-0 NODE xxx ASSISTANT NODE yyy
```

- RECEIVE ASSISTANCE - Your node sends the test message directly to the destination node. The assistant node relays the test message on the way back from the destination node. Use this test when you suspect that the transceiver at the destination node is transmitting a weak signal, demonstrated by Example 7–5 and Figure 7–6.

```
NCP>LOOP CIRCUIT UNA-0 NODE xxx ASSISTANT NODE yyy HELP RECEIVE
```

- TRANSMIT ASSISTANCE - The assistant node relays the test message on the way to the destination node. The test message is returned directly to your node by the destination node. Use this test when you suspect that your transceiver is transmitting a weak signal, demonstrated by Example 7–6 and Figure 7–7.

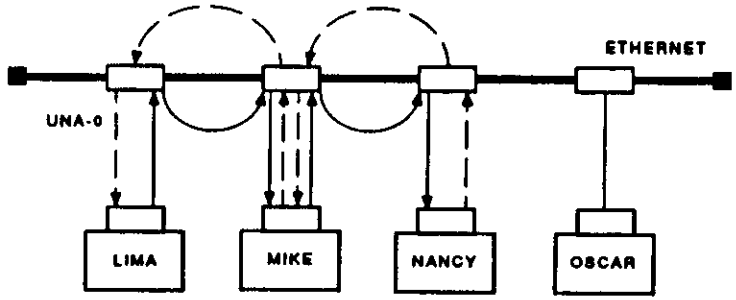
```
NCP>LOOP CIRCUIT UNA-0 NODE xxx ASSISTANT NODE yyy HELP TRANSMIT
```

Loop assist tests are useful when the node being tested cannot respond to a signal because the signal is too weak.

Example 7–4: Loopback Test Using Full Assistance

```
NCP>LOOP CIRCUIT UNA-0 NODE NANCY ASSISTANT NODE MIKE
```

Figure 7–5: Loopback Test Using Full Assistance



LEGEND

SHOWS DATA BEING LOOPED TO DESTINATION NODE.

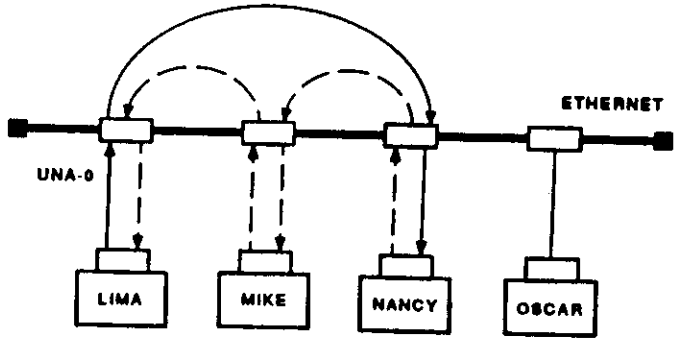
SHOWS DATA BEING LOOPED BACK TO SOURCE NODE.

MKV_X1000_88

Example 7–5: Loopback Test Using Receive Assistance

```
NCP>LOOP CIRCUIT UNA-0 NODE NANCY ASSISTANT NODE MIKE HELP RECEIVE
```

Figure 7–6: Loopback Test Using Receive Assistance



LEGEND

SHOWS DATA BEING LOOPED TO DESTINATION NODE.

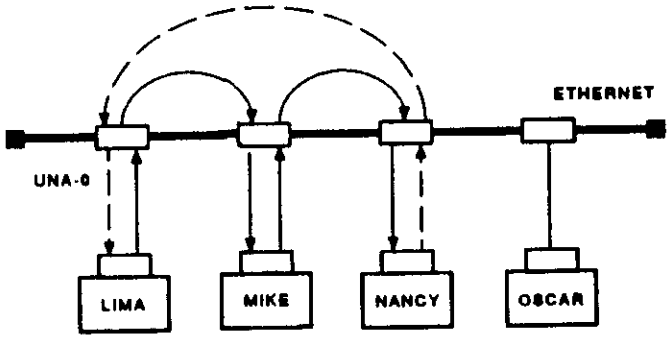
SHOWS DATA BEING LOOPED BACK TO SOURCE NODE.

MKV_X1001_88

Example 7–6: Loopback Test Using Transmit Assistance

```
NCP>LOOP CIRCUIT UNA-0 NODE NANCY ASSISTANT NODE MIKE HELP TRANSMIT
```

Figure 7–7: Loopback Test Using Transmit Assistance



LEGEND

◄——— SHOWS DATA BEING LOOPED TO DESTINATION NODE.

◄ — — SHOWS DATA BEING LOOPED BACK TO SOURCE NODE.

MKV_K1002_88

Point-to-Point Tests

Controller Loopback Test

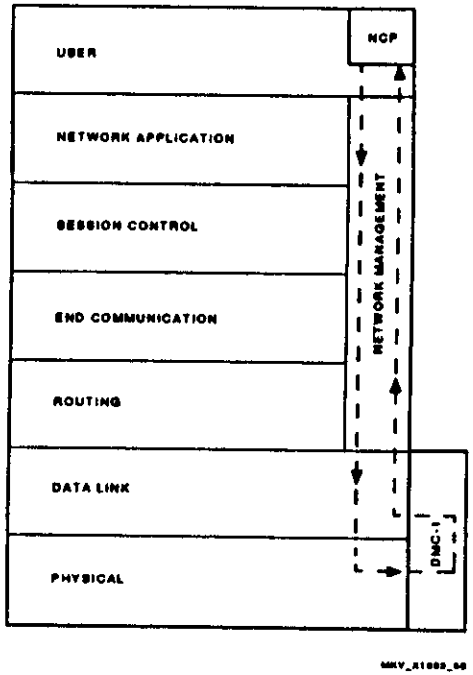
This test verifies whether or not the line up to the controller and the controller are functional.

- Use the LOOP CIRCUIT command to perform a controller loopback test of a physical line on the local node while the controller is in loopback mode.
- Test data flows from the Network Management Layer directly to the device driver.
- The commands shown in Example 7–7 are illustrated by Figure 7–8.

Example 7–7: Controller Loopback Test

```
NCP>SET LINE DMC-1 STATE OFF
NCP>SET LINE DMC-1 CONTROLLER LOOPBACK
NCP>SET LINE DMC-1 STATE ON
NCP>SET CIRCUIT DMC-1 STATE ON
NCP>LOOP CIRCUIT DMC-1 COUNT 10 LENGTH 32
```

Figure 7–8: Controller Loopback Test



Circuit Loopback Test with Loopback Connector

This test allows you to loop data through a hardware loopback connector to test whether th entire communication device and cable is functional. Cable loopback tests are conducted throug the use of NCP LOOP CIRCUIT commands. Table 7–3 lists the loopback connectors require for each device.

The commands shown in Example 7–8 are illustrated by Figure 7–9.

Example 7–8: Circuit Loopback Test Using a Loopback Connector

```
NCP>SET CIRCUIT DMC-1 SERVICE ENABLE
NCP>SET LINE DMC-1 STATE ON
NCP>LOOP CIRCUIT DMC-1
NCP>LOOP CIRCUIT DMC-1 COUNT 100 LENGTH 45
```

Figure 7–9: Circuit Loopback Test Using a Loopback Connector

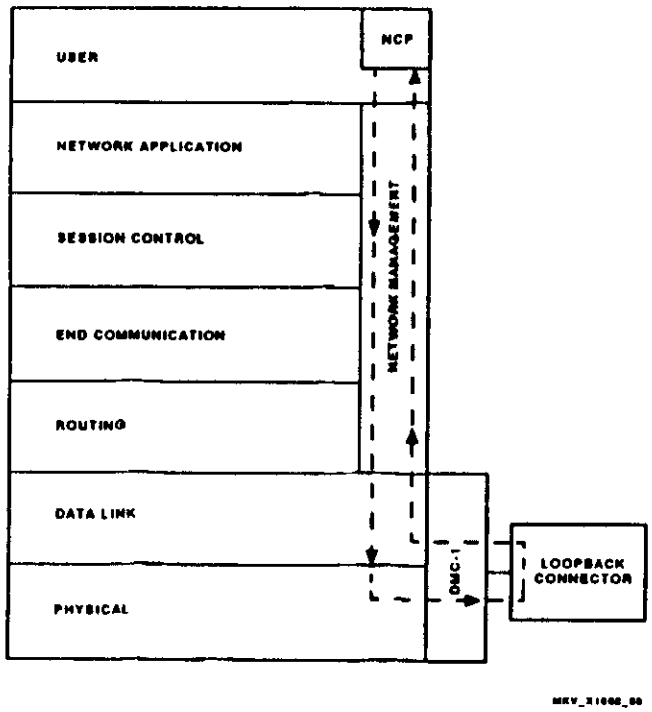


Table 7–3: Test Connectors

CONNECTORS	OPTIONS
H315	DH11, DL11, DLV11, DQ11, DU11, DUV11
H325	DJU11, DHV11, DMC11, DMP11, DMR11
	DMV11, DUP11, DV11, DZ11, DZV11
H327	DZ11
H329	DZV11
H861	DV11
H861C	DH11
H3027	DMZ32
H3028	DMZ32
H3190	DZ11
H3248	DMF32
H3249	DMF32
H3250	DMC11, DMP11, DMR11, DMV11
H3251	DMP11, DMR11, DMV11
H3254	DMP11, DMR11, DMV11
H3259	DPV11, DZ32
H3260	DPV11
H3271	DZ11, DZ11X
H3272	DZ32
H3273	DZ11X
H3274	DZ11X
H3276	DMR11
H3277	DHV11
H8568	DMR11
H8611	DH11
H8612	DZ11
M974	DH11
12-12528	DMC11

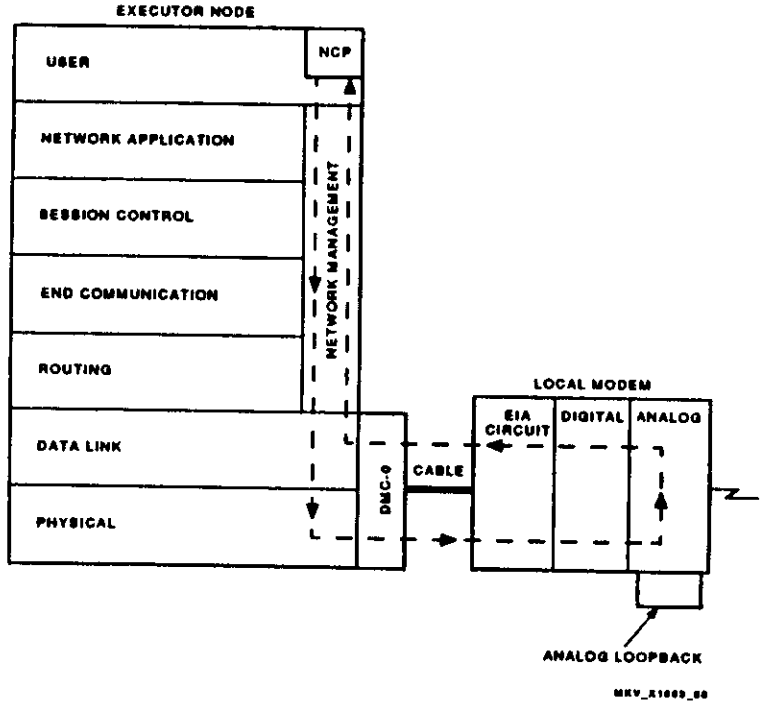
Local Modem Loopback Test

A local modem test can be performed on modems that have an analog loopback button. With this button, the data transmitted from the local node is looped around in the local modem and returned back to the local node. This loopback arrangement tests the line device, the cable, and the modem. The commands shown in Example 7–9 are illustrated by Figure 7–10.

Example 7–9: Local Modem Loopback Test

```
NCP>SET LINE DMC-0 DUPLEX FULL
NCP>SET CIRCUIT DMC-0 STATE SERVICE
NCP>LOOP CIRCUIT DMC-0 COUNT 10
```

Figure 7–10: Local Modem Loopback Test



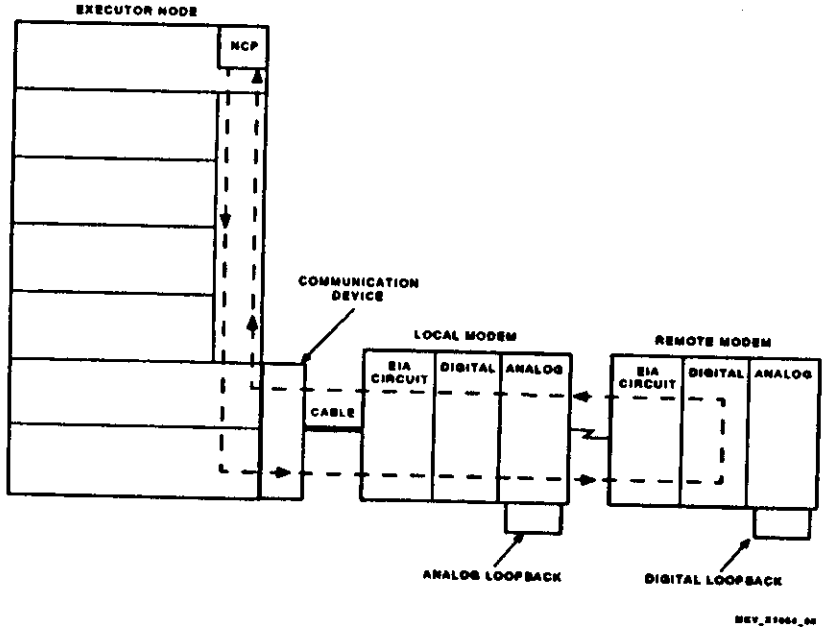
Remote Modem Loopback Test

The loopback arrangement in Figure 7-11 tests the communications device, the cable to the modem, the local modem, the telephone circuit, and the remote modem. The remote mo digitizes the data from the local modem, converts the data to analog form, and returns it t local modem. The data is then returned to the device. The commands shown in Example are illustrated by Figure 7–11.

Example 7–10: Remote Modem Loopback Test

```
NCP>SET LINE DMC-0 DUPLEX FULL
NCP>SET CIRCUIT DMC-0 STATE SERVICE
NCP>LOOP CIRCUIT DMC-0 COUNT 10
```

Figure 7–11: Remote Modem Loopback Test



Local to Remote Loop Node Test

This test verifies the logical link path over a circuit between the local node and the adjacent node:

- Looping to a test node sends test messages back to the local node mirror object through an adjacent node.
  - — The test messages are forwarded properly, as the routing header has the same address in both the source and destination fields.
  - — Any adjacent node receiving the message merely returns it.

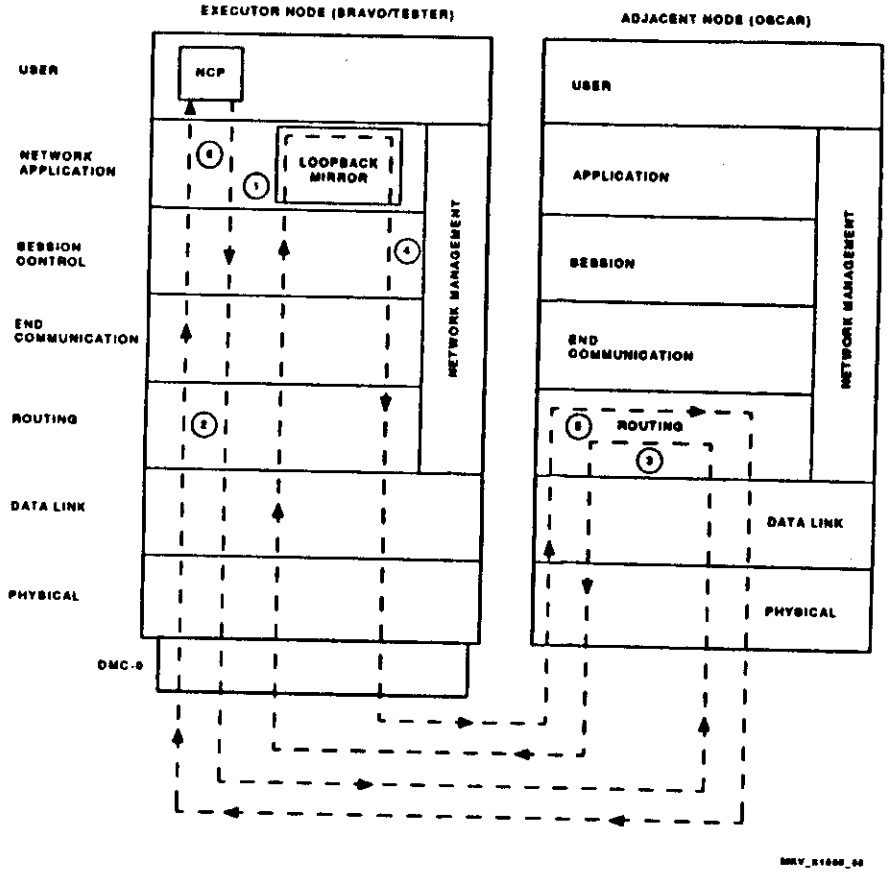
Because this actually tests the operation of the Routing Layer on the the remote adjacent node, the messages may not come back on the circuit over which it was sent.

The commands shown in Example 7–11 are illustrated by Figure 7–12.

Example 7–11: Local to Remote Loop Node Test

```
NCP>SET LINE DMC-0 STATE ON
NCP>SET NODE TESTER CIRCUIT DMC-0
NCP>SET CIRCUIT DMC-0 STATE ON
NCP>LOOP NODE TESTER COUNT n
```


Figure 7–12: Local to Remote Loop Node Test



Software Loopback Test

This test determines that the circuit is operational up to the remote circuit unit and controller:

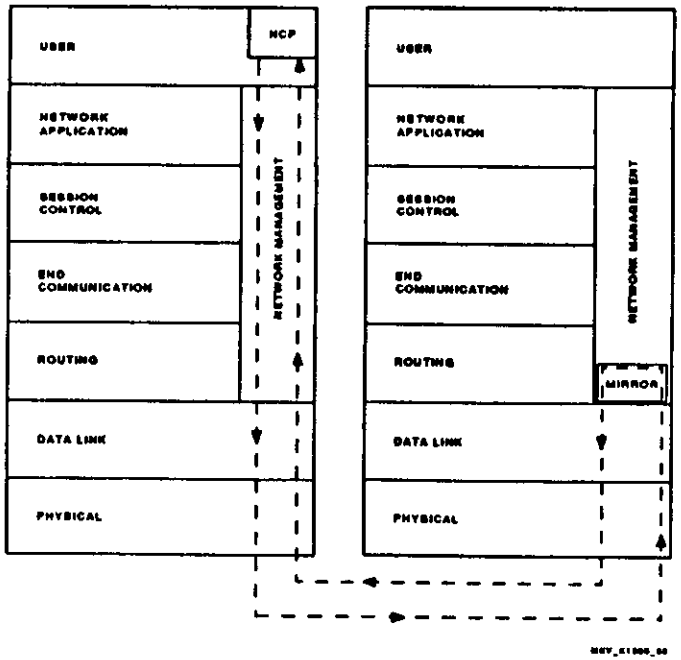
- If a circuit loopback test passes, the problem is most likely located in the network software. If the circuit loopback fails, the problem may be hardware-related.

The commands shown in Example 7–12 are illustrated by Figure 7–13.

Example 7–12: Software Loopback Test

```
NCP>SET LINE DMC-0 STATE OFF
NCP>SET LINE DMC-0 CONTROLLER NORMAL
NCP>SET LINE DMC-0 STATE ON
NCP>SET CIRCUIT DMC-0 STATE ON
NCP>LOOP CIRCUIT DMC-0 COUNT 10
```

Figure 7–13: Software Loopback Test



Local-to-Remote Loopback Test

This test verifies the logical link connection between two nodes:

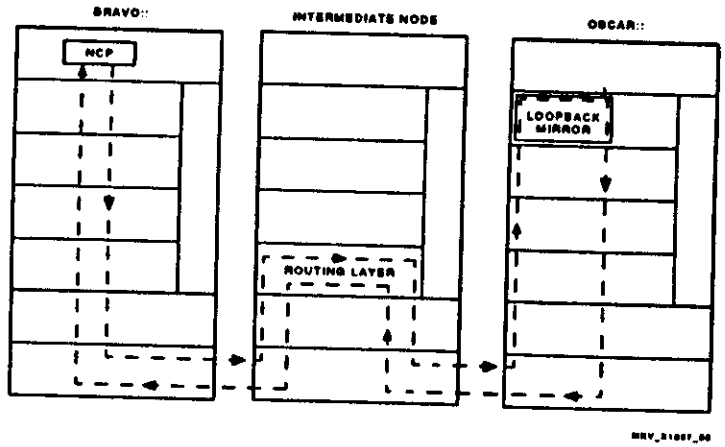
- Test data flows through intermediate nodes since the node loopback is a normal logical lin
- This test can be performed across multiple hops.

The command shown in Example 7–13 is illustrated by Figure 7–14.

Example 7–13: Local-to-Remote Loopback Test

```
NCP>LOOP NODE OSCAR COUNT 10
```

Figure 7–14: Local-to-Remote Loopback Test



SUMMARY

One of the most common faults leading to network failure occurs when network parameters are not adjusted properly. When a problem occurs on your system, check that the following network parameters are properly set:

- Node address
- Buffer size
- Maximum address
- Maximum cost
- Maximum visits
- Maximum hops
- Routing passwords

When testing a network, a test strategy should be employed. Begin testing on your own local node and test outward until the problem is isolated. In other words, test your local node's hardware and software and then work out to the remote system's hardware and software.

- Local-to-local loopback test - Evaluates local software using an internal logical link.
- Local-to-local loop node test - Evaluates local software and controller.
- Controller loopback test - Evaluates whether the line up to the controller and the controller are functional.
- Circuit loopback test with loopback connector - Loops data through a hardware connector to test the entire communication device and cable.

- Local modem loopback test - This test checks out the line device, the cable, and the modem on the local node.
- Remote modem loopback test - This test is designed to ensure that the communication device, the cable to the local modem, the local modem, the telephone circuit, and the remote modem are all working properly.
- Local-to-remote (adjacent) loop node test - Evaluates both the local node and the adjacent node's Routing and Data Link Layer software.
- Software loopback test - This test determines that the circuit is operational up to the remote circuit unit and controller.
- Local-to-remote loopback test - Evaluates ability to establish a logical link with a remote node, possibly through intermediate nodes.

When using Ethernet loopback tests, you need to obtain the Ethernet physical addresses of the remote nodes that you wish to test.

Remember that some tests are usable only on point-to-point configurations.

LABORATORY EXERCISES

For this lab, isolate the faults described by the following problem statements. As time allows, your instructor will reproduce each of the problems on your classroom systems. You will then be given a set time period to find the problem (or problems) using the tools presented throughout the week. *DO NOT FIX THE PROBLEMS WHEN YOU FIND THEM.* If you fix a problem, it won't be there for your classmates to find. When you locate a problem, write it down, along with what you would do to fix it.

You may use loopback tests; however, you should *not* execute any of the particular loopback commands that require you to put the line controller into loopback mode.

The lab reflects the material covered throughout the week. Do not limit yourself to the material in this module. There is a wide range of VMS and networking tools available to help you find the faults.

Your instructor will provide you with the names of the nodes corresponding to A, B, C, and D. You can fill in the table below for reference.

LETTER	NODE
A	
B	
C	
D	

1. **PROBLEM STATEMENT:**

   Users from other systems are unable to send MAIL to users on system A, or execute PHON commands to system A. Several users have also reported failures when they attempt to cop files to and from node A, but others have been able to copy files without trouble. Most c the users reporting problems mentioned receiving an error message about invalid log-i information at the remote node.

2. **PROBLEM STATEMENT:**

   When users attempt to access node C, they receive a message indicating that the remote node is unreachable.

3. **PROBLEM STATEMENT:**

A user with an account on system B was on vacation for a week. When she returned, she had received mail from a friend (C::JETSON). When she attempted to reply to the mail, she received an error message indicating that there was no such user on node C. When she checked with her friend by telephone, she discovered that his account on node C was, indeed, still active.

4. **PROBLEM STATEMENT:**

A user on node A reports that "PHONE is broken." He has received a couple of different error messages when he tried to contact users on remote nodes.

5. **PROBLEM STATEMENT:**

Several users have complained to you that they are able to SET HOST from other systems to node B, but they are unable to transfer files to and from node B without including their username and password on the command line.

6. **PROBLEM STATEMENT:**

Users on other nodes in the network report that sometimes when they try to execute network commands to node B, they receive error messages about insufficient system resources at the remote node. At other times, the commands execute without error. The error messages seem most frequent in the middle of the afternoon; they rarely occur at night.

MODULE 8
MANAGING TERMINAL SERVERS

INTRODUCTION

Terminal servers are part of the equipment that a network manager is directly responsible for. A network manager needs to know how to install, configure, and maintain these units. This module will present basic concepts associated with a terminal server environment.

A DECserver 200 and DECserver 500 are referenced as the primary units, although much of the information pertains to DIGITAL's terminal server family, and not one specific server.

OBJECTIVES

To manage terminal servers successfully, the network manager should be able to:

- Explain terms and concepts associated with terminal servers.
- Install terminal server software on the load host.
- Configure terminal server software characteristics.
- Configure a server port for a printer device.

RESOURCES

- *DECserver 200 Management Guide*, (AA-HL76A-TK)
- *DECserver 200 Software Installation Guide*, (AA-HL79A-TK)
- *DECserver 500 Management Guide*, (AA-HS49A-TE)
- *DECserver 500 Software Installation Guide*, (AA-HS49A-TE)

TERMS AND CONCEPTS

- Service—A software application (MAIL, PHONE) or hardware device offered on the network (printers, dial-in lines). A node is also a service.
- Session—A connection to a service. User can establish more than one session to available services.
- Port—A hardware connector on back of server where device plugs in, and software associated with it (port characteristics).
- Local Mode—User communicating with server software directly.
- Service Mode—User communicating with an available service.

Example 8–1 shows both local and service modes.

Example 8–1: Connecting to a Service

```
Local> connect ENT
local -010- Session 1 to ENT established

Welcome to node ENT!
Username:
```


Server Databases

These contain server and port characteristics, which can be modified to suit the environment.

DECserver 200 Databases

- Two databases:
  - — Permanent
  - — Operational
- Permanent database:
  - — Modified by the DEFINE command.
  - — Changes to server characteristics take effect when the server is initialized.
  - — Changes to port characteristics take effect when the:

    Server is initialized.
    User logs into a port.
- Operational database
  - — Modified by SET command.
  - — Changes to port characteristics take effect immediately.
  - — Some changes to server characteristics take effect immediately; others do not change until the server is initialized.
  - — Changes to server and port characteristics are lost when the:

    Server is shut down or initialized.
    User logs out of a port.

DECserver 500 Databases

- Three databases:
  - — Permanent
  - — Operational
  - — Log-in
- Permanent database
  - — Resides on load host.
  - — Modified using the terminal server configurator (TSC) utility.
  - — Changes take effect when server is down-line loaded.
- Operational database
  - — Resides in dynamic server memory.
  - — Modified by SET command.
  - — Changes to port characteristics take effect immediately.
  - — Some changes to server characteristics take effect immediately; others will not change until the server is initialized.
  - — Changes to server and port characteristics are lost when the:

    Server is shut down or initialized.
    User logs out of the port.
  - — User must issue the SAVE PORT command to save characteristics to the log-in database.
- Log-in database
  - — Resides in dynamic server memory.
  - — Changes remain in effect until server is down-line loaded, even if the user logs out.

LATCP and LTCOAD.COM

- LAT Control Program (LATCP)
  - — Used to display information concerning VMS LAT software.
  - — Creates/removes a local LTAn: device.
  - — Starts and stops the LAT port driver (LAT protocol).
  - — Invoked by issuing the following DCL command (CMKRNL privileges required):

```
$ RUN SYS$SYSTEM:LATCP
LCP>
```

  - — LCP commands:

    START (node) starts the LAT port driver on the specified node.
    STOP (node) stops the LAT port driver on the specified node.
    SHOW (entity) displays the LAT information specified.
    SET (entity) modifies the LAT information specified.
- The LTLOAD.COM command file
  - — Located in SYS$MANAGER.
  - — Starts LAT and configures LAT devices (LTAn:) for remote printer use.
  - — Include in SYS$MANAGER:SYSTARTUP.COM command file.

Example 8–2 shows the LTLOAD.COM default command file.

Example 8–2: LTLOAD.COM Default Command File

```
! !  Copyright (c) 1987 Digital Equipment Corporation.  All rights reserved.
! ! This command procedure starts up the LAT protocol
! ! and configures applications devices for remote printer use.
!
! RUN SYS$SYSTEM:SYSGEN
CONNECT LTA0/NOADAPTER
!
$! Invoke LATCP
!
$LCP := $LATCP ❶
!
! The following commands will set up LAT service with the default name ❷
! SYS$NODE and default ident SYS$ANNOUNCE.  The LAT service name will
! will default to the node name SYS$NODE unless you specify the name as
! the first parameter in the command line.  Additional node characteristics
! such as group codes can also be supplied as parameters.
!
$LCP SET NODE /IDENT  'P2' 'P3' 'P4' /NOLOG ❸
$LCP CREATE SERVICE /ID
$IF P1 .NES. "" THEN $LCP CREATE SERVICE 'P1' /IDENT /NOLOG
$!
$ RUN SYS$SYSTEM:LATCP
!
! Set up the applications devices that will support remote printer ❹
! access.
!
! Create the devices.
!
!CREATE PORT LTA1: /NOLOG
!CREATE PORT LTA2: /NOLOG
!
! Maps applications port(s) to a specific port(s) on the terminal ❺
! server
!
!SET PORT LTA1: /APPLICATION /NODE=SERVER_1 /PORT=LN03
!SET PORT LTA2: /APPLICATION /NODE=SERVER_2 /PORT=PORT_3
!
! Start LAT Service
!
START NODE
EXIT
```


INSTALLING SOFTWARE ON THE LOAD HOST

Installation Overview

The following tasks comprise the terminal server software installation procedure:

1. Install the software from the distribution medium to the load host.
   - — Server image file(s)
   - — DSVCONFIG command procedure
2. Run the DSVCONFIG command procedure.
3. Down-line load the server.
4. Verify that the server is down-line loaded.

The installation procedure is illustrated in Example 8–3 and Example 8–4.

Pre-installation Tasks

Perform the following tasks before installing the terminal server software.

1. Back up the system disk.
2. Make sure there is enough disk space on the load host.
3. Identify the 12-digit Ethernet hardware address of each server.
4. Assign a unique DECnet node name to each server.
5. Assign a unique DECnet address to each server.
6. Make sure the DECnet license is installed on the load host.

Example 8–3: Installing Server Software on the Load Host, (Sheet 1 of 2)

```
Username: SYSTEM
Password:
                Welcome to VMS Version 5.0

    Last interactive login on Thursday, 17-OCT-1988 06:07
    Last non-interactive login on Thursday, 17-SEP-1988 13:11

$ set def sys$update
$ @vmsinstal ds2020 mta0:

 VMS Software Product Installation Procedure V5.0

It is 17-OCT-1988 at 13:29.
Enter a question mark (?) at any time for help.

%VMSINSTAL-W-DECNET, Your DECnet network is up and running.
%VMSINSTAL-W-ACTIVE, The following processes are still active:
 Rick
* Do you want to continue anyway [NO]? y
* Are you satisfied with the backup of your system disk [YES]? y

Please mount the first volume of the set on MTA0:.
* Are you ready? y
%MOUNT-I-MOUNTED, DS2 mounted on _MTA0:
The following products will be processed:

  DS2 V2.0

 Beginning installation of DS2 V2.0 at 13:30

%VMSINSTAL-I-RESTORE, Restoring product saveset A...
%VMSINSTAL-I-RELMOVED, The products release notes have been successfully moved to SYS$HELP.
%VMSINSTAL-I-RESTORE, Restoring product saveset B...
%VMSINSTAL-I-MOVEFILES, Files will now be moved to their target directories...

Beginning installation verification procedure for DECserver 200 V2.0.

Successful creation of SYS$SYSROOT:[DECSERVER] directory

Successful installation of SYS$SYSROOT:[DECSERVER]PRO601ENG.SYS

Successful installation of SYS$SYSROOT:[DECSERVER]DSVCONFIG.COM

Successfully located SYS$SYSROOT:[DECSERVER]DSVCONFIG.DAT

Successful installation of SYS$SYSROOT:[DECSERVER]DS2_020_DEFAULTS.COM

Successful installation of SYS$SYSROOT:[DECSERVER]DS2020.RELEASE_NOTES
```


Example 8–4: Installing Server Software on the Load Host, (Sheet 2 of 2)

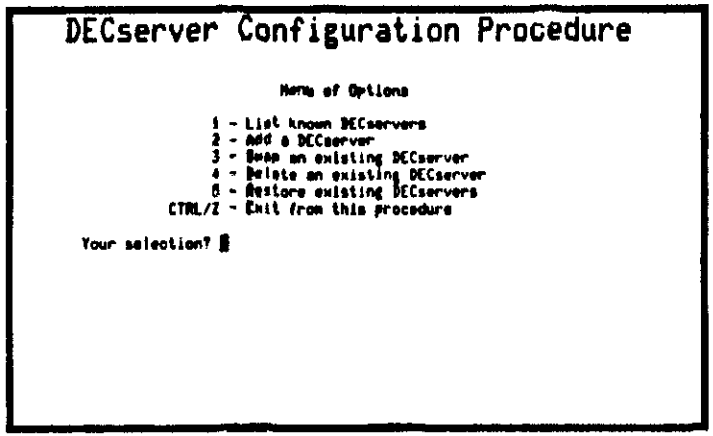
```
Your installation is now complete.  After exiting from VMSINSTAL:

1. Edit your system start-up file so that it defines the logical
   MOM$LOAD as a search string with a value equal to the current search
   string, plus the added element SYS$SYSROOT:[DECSERVER].  For example:

   DEFINE/SYSTEM/EXEC/NAME_ATTRIBUTE=NO_ALIAS/NOLOG -
   MOM$LOAD 'current-search-string',SYS$SYSROOT:[DECSERVER]

   If the current search string associated with MOM$LOAD in your
   start-up file is SYS$SYSROOT:[DECSERVER] or if you have
   already made this change for a previous installation, there
   is no need to edit this file.

   This command ensures that the location of the server image
   is defined each time the system is rebooted, necessary for
   successful down-line loading.

2. Configure the server into  your  host's database.
   Execute a command procedure  called  DSVCONFIG.COM. This
   command  procedure is in the SYS$SYSROOT:[DECSERVER] directory.
   If  you  have  already  executed  this  procedure from previous
   installations, you need to configure only any additional units.
   All previously defined units will still be configured.
 Installation of DS2 V2.0 completed at 13:31

 VMSINSTAL procedure done at 13:31
```

Configuring the Load Host's Node Database

Example 8–5: Invoking DSVCONFIG

```
$ @MOM$LOAD:DSVCONFIG

You must assign a unique DECnet node name and DECnet node
address for each new DECserver.

Press <RET> to start, or <CTRL/Z> to exit...
```

Figure 8–1: DSVCONFIG Main Menu



List known DECservers on the load host by selecting item 1 from the DSVCONFIG menu, as shown in Example 8–6.

Example 8–6: Listing Servers in the Database Using DSVCONFIG

```
      Your selection? 1

DECnet   DECnet Server Service
Address  Name   Type   Circuit  Ethernet Address   Load File   Dump File
-------  ------ -----  -------  -----------------  ----------  ----------
13.1     NACCD  DS100  QNA-0    08-00-2B-02-DF-25  PS0801ENG.SYS  PSDMPDF25.SYS
13.2     NACCD2 DS200  QNA-0    08-00-2B-07-6D-25  PRO801ENG.SYS  DS2NACCD2.DMP
13.3     NACCD3 DS200  QNA-0    08-00-2B-08-56-9C  PRO801ENG.SYS  DS2NACCD3.DMP
13.4     BED2   DS200  QNA-0    08-00-2B-06-08-DE  PRO801ENG.SYS  DS2BED2.DMP
13.5     BED1   DS200  QNA-0    08-00-2B-08-73-DD  PRO801ENG.SYS  DS2BED1.DMP

Total of 5 DECservers defined.
------------------------------
(Press RETURN for menu.)
```

Add a DECserver by selecting item 2 from the DSVCONFIG menu and answering the associated questions, as shown in Example 8–7

Example 8–7: Adding a Server Using DSVCONFIG

```
      Your selection? 2

Type a ? at any time for help on a question.
Type CTRL/Z for any question to return to menu without adding the unit.

DECserver type? ds200
DECnet node name for unit? NACCD4
DECnet node address for unit? 13.6
Ethernet address of unit? 08-00-2b-05-84-2c
DECnet Service Circuit-ID [QNA-0]?
```

Swap a DECserver by selecting item 3 from the DSVCONFIG menu and answering the associated questions as shown in Example 8–8.

Example 8–8: Swapping a Server Using DSVCONFIG

```
        Your selection? 3

Type a ? at any time for help on a question.
Type CTRL/Z for any question to return to menu without changing the unit.

What is the DECnet node name you want to swap? NACCD
DECserver at Ethernet address 08-00-2B-02-DF-25 is being
modified.

Enter the new Ethernet address and any other DECnet
characteristics you want to modify.

DECserver type [DS200]?
DECnet node name for unit [NACCD]?
Ethernet address of unit? 08-00-2b-08-7d-9a
DECnet Service Circuit-ID [QNA-0]?

%PURGE-I-FILPURG, SYS$COMMON:[DECSERVER]DSVCONFIG.DAT;7 deleted (2 blocks)
```

Delete a DECserver by selecting item 4 from the DSVCONFIG menu and answering the associated questions, as shown in Example 8–9.

Example 8–9: Deleting a Server Using DSVCONFIG

```
        Your selection? 4

(Press <CTRL-Z> to return to menu.)
Enter the DECnet node name of the server you want to delete? NACCD2

%PURGE-I-FILPURG, SYS$COMMON:[DECSERVER]DSVCONFIG.DAT;9 deleted (2 blocks)
%NCP-I-NMLRSP, listener response - Success
Remote node =   13.2 (NACCD2)
%NML-I-RECDELET, Database entry deleted
```


Load the server database into the NCP database by selecting item 5 from the DSVCONFIG menu and answering the associated questions, as shown in Example 8–10.

- Item 5 operates on two databases:
  - — Load host node database
  - — NCP database (also called DECnet load database)
- Useful when updating the local NCP database from a central, remote NCP database that does not include servers.

Example 8–10: Loading Server Database into NCP Database Using DSVCONFIG

```
        Your selection? 5

Restoring existing DECservers to host DECnet database...
```

Preparing to Down-line Load the Server

Once the server database is built, the load host should be set up to down line load the server(s) by doing the following:

1. Check the NCP Volatile database to ensure that the server is properly configured. (See Example 8–11.)
2. Check the circuit characteristics of the server's Ethernet circuit. Ensure that SERVICE is enabled. (See Example 8–12.)
3. Start the OPCOM process if it was not started by your system startup procedure. (See Example 8–13.)
4. Check to ensure that the node has event logging enabled to track down-line loading and up-line dumping events. (See Example 8–14.)

Example 8–11: Using NCP to Check Server Configuration

```
$ RUN SYS$SYSTEM:NCP
NCP> SHOW NODE NACCD3 CHAR

Node Volatile Characteristics as of  1-MAY-1988 07:10:22

Remote node =   13.200 (CYCLPS)

Service circuit              = UNA-0
Hardware address             = 08-00-2B-08-56-9C
Load file                    = SYS$COMMON:[DECSERVER]PRO801ENG.SYS
Dump file                    = SYS$COMMON:[DECSERVER]DS2LAT200.DMP
```

Example 8–12: Using NCP to Check Circuit Characteristics

```
$ RUN SYS$SYSTEM:NCP
NCP> SHOW CIRCUIT UNA-0 CHAR

Circuit Volatile Characteristics as of  1-MAY-1988 07:14:46

Circuit = UNA-0

State                        = on
Service                      = enabled
.
.
.
```

Example 8–13: Starting OPCOM

```
$ @SYS$SYSTEM:STARTUP OPCOM
```

Example 8–14: Using NCP to Enable Logging

```
$ RUN SYS$SYSTEM:NCP
NCP> SET LOGGING CONSOLE EVENT 0.3,7
NCP> SET LOGGING CONSOLE STATE ON
NCP> SET LOGGING MONITOR STATE ON
```

Down-line Loading the Server

Once the load host has been set up properly, the server can be down-line loaded using one of the following methods:

- Cycle power on the server
  - — Server sessions terminated immediately.
  - — Server executes its self-test.
  - — Down-line load request multicast to all load hosts.
  - — The first host to respond loads the server.
- The INITIALIZE command
  - — Invoked from the server to be down-line loaded.
  - — Server sessions terminated with automatic one minute delay, or time interval can be specified.
  - — Server executes its self-test.
  - — Down-line load request multicast to all load hosts.
  - — The first host to respond loads the server.
  - — Command:

```
Local> INITIALIZE
```


- The NCP TRIGGER command
  - — Server sessions terminated immediately.
  - — Down-line load request multicast to all load hosts.
  - — The first host to respond loads the server.
  - — Command:

```
NCP>TRIGGER NODE server-name
```

- The NCP LOAD command
  - — Server sessions terminated immediately.
  - — Down-line load request sent to node issuing LOAD command.
  - — The specific load host loads the server.
  - — Command:

```
NCP>LOAD NODE server-name
```

Example 8–15 and Example 8–16 show the OPCOM messages for a down-line load and an up-line dump, respectively.

Example 8–15: Sample Event Log of a Down-line Load

```
%%%%%%%%%%  OPCOM   1-MAY-1988 07:36:07.30  %%%%%%%%%%
Message from user DECNET
DECnet event 0.3, automatic line service
From node 26.143 (PARROT), ❶ 1-OCT-1988 07:36:07.01
Circuit UNA-0, ❷ Load, ❸ Requested, Node = 13.445 (NACCD4) ❹
File = MOM$LOAD:PRO801ENG, ❺ Operating system, Ethernet address = 08-00-2B-07-6D-25 ❻
```

Example 8–16: Sample Event Log of an Up-line Dump

```
%%%%%%%%%%  OPCOM   1-MAY-1988 07:43:02.52  %%%%%%%%%%
Message from user DECNET
DECnet event 0.3, automatic line service
From node 26.143 (PARROT), ❶ 1-OCT-1988 07:43:02.47
Circuit UNA-0, ❷ Dump, ❸ Requested, Node = 13.445 (NACCD4) ❹
File = SYS$COMMON:[DECSERVER]DS2LAT200.DMP, ❺ Ethernet address = 08-00-2B-07-6D-25 ❻
```

The following notes identify the parts of the OPCOM messages shown in Example 8–15 and Example 8–16.

❶ DECnet address and node name of node receiving the request for the activity.

❷ Circuit used for the activity.

❸ Type of activity.

❹ DECnet address and node name of node requesting the activity.

❺ File used for the activity.

❻ Ethernet address of the node requesting the activity.

Verifying the Down-line Load

To verify the down-line load:

1. Log in to the server. (See Example 8–17.)
2. Test the port using the TEST PORT command. (See Example 8–18.)

Example 8–17: Logging into the Server

```
# <password>
DECserver 200 Terminal Server V2.0 (BL29) - LAT V5.1
Please type HELP if you need assistance
Enter username> SYSTEM
Local>
```

Example 8–18: Testing the Port

```
Local> Test Port Count 3
 !"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklno
!"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklnop
"#$%&'()*+,-./0123456789:;<=>?@ABCDEFGHIJKLMNOPQRSTUVWXYZ[\]^_`abcdefghijklnopq
Local>
```

CONFIGURING THE SERVER

Remote Console Facility(R.C.F.)

- Allows a terminal on any DECnet node to issue local commands to a server.
- Requires only DECnet software.

Example 8–19 illustrates the use of R.C.F.

Example 8–19: Establishing a Connection with R.C.F.

```
$ RUN SYS$SYSTEM:NCP
NCP> CONNECT NODE LAT501

Console connected (press CTRL/D when finished)

DECserver 500 Terminal Server V1.1.1 - LAT V5.1

Please type HELP if you need assistance

Enter username> Carl Derone
Local>
```

NOTE

There can be only one console carrier connection active to a given server at a time.

Terminal Server Configurator (TSC)

Used to configure the permanent database for the DECserver 500. TSC should be run load host that has DECnet started. The load host should also have write access to the s image files. Example 8–20 and Example 8–21 illustrate the use of TSC.

Example 8–20: Invoking TSC on the DECserver 500

```
$ SET DEFAULT SYS$SYSROOT:[DECSERVER]
$ RUN DS5CFG
```

TSC accepts:

- Individual server commands
- Command procedure containing server commands

Example 8–21: Using TSC

```
$ SET DEFAULT SYS$SYSROOT:[DECSERVER]
$ RUN DS5CFG

  Terminal Server Configurator - V2.0
  Server Image:PRISMTSV.SYS

  DECserver 500, V1.01.01 (Database V8).
  (No date/time of last change available.)

  TSC>@CONFIG_PRISM.COM
       .
       .
       .

  TSC>EXIT
```

TSC and Terminal Server User Commands

Table 8–1: TSC and Terminal Server User Commands

TSC COMMANDS	TERMINAL SERVER USER COMMANDS
SET or DEFINE	SET
SHOW or LIST	SHOW
CLEAR or PURGE	CLEAR

TSC specific commands:

```
TSC>DEFINE SERVER BACKUP HOSTS ALIEN,IMP
TSC>DEFINE SERVER LINE FREQUENCY 60
TSC>DEFINE SERVER MAINTENANCE PASSWORD FA07
```


Server Management Commands

Setting Server Characteristics

The SET/DEFINE SERVER commands modify these characteristics:

- Server identification

```
Local>SET SERVER NAME Prism
Local>SET SERVER IDENTIFICATION "Newton's Lab"
```

- Network features

```
Local> SET SERVER SERVICE GROUPS 5,15 ENABLED
Local> SET SERVER CIRCUIT TIMER 70
Local> SET SERVER RETRANSMIT LIMIT 10
Local> SET SERVER KEEPALIVE TIMER 12
Local> SET SERVER NODE LIMIT 60
Local> SET SERVER MULTICAST TIMER 60
```

- Port's local access mode

```
Local>SET SERVER SESSION LIMIT 4
Local>SET SERVER BROADCAST ENABLED
Local>SET SERVER LOCK ENABLED
Local>SET SERVER INACTIVITY TIMER 15
```

- Server passwords

```
Local>SET SERVER PRIVILEGED PASSWORD
New password>
Verification>
Local>SET SERVER LOGIN PASSWORD
New password>
Verification>
```

Use the SHOW command to check the settings of the port and the server, as illustrated in Example 8–22 and Example 8–23.

Example 8–22: Displaying Port Settings (DECserver 200)

```
Local> Show Port

Port 1:  RICK (1)

Character Size:           8 (2)   Input Speed:        4800
Flow Control:           XON           Output Speed:       4800
Parity:                None

Access:                Local          Local Switch:       None
Backwards Switch:       None          Name:             PORT_1
Break:                 Local          Session Limit:         4
Forwards Switch:        None          Type:               Ansi (3)

Preferred Service: None

Authorized Groups:   0
 Current   Groups:   0

Enabled Characteristics:

Autobaud, (4) Autoprompt,  Broadcast,  Input Flow Control,  Loss Notification,
Message Codes,  Output Flow Control,  Verification (5)

Local>
```

Example 8–23: Displaying Server Settings (DECserver 200)

```
Local> Show Server

DECserver 200 V2.0 BL29     LAT V5.1   ROM BL20    Uptime:  19 22:46:04 (6)

Address:   08-00-2B-09-45-03   Name:   FPO32 (7)      Number:      0

Identification: (8)

Circuit Timer:           80          Password Limit:          3
Console Port:             1          Queue Limit:            24
Inactivity Timer:        30          Retransmit Limit:        8
Keepalive Timer:         20          Session Limit:          20 (9)
Multicast Timer:         30          Software:        PROBO1ENG (10)
Node Limit:             100

Service Groups:   0

Enabled Characteristics:

Announcements,  Broadcast,  Dump,  Lock
```


Setting Port Characteristics

SET/DEFINE PORT modifies these port characteristics:

- Port access

```
Local>SET PORT 3 ACCESS LOCAL
Local>SET PORT 4 ACCESS REMOTE
```

- Port session control

```
Local>SET PORT 8 FORWARD SWITCH CTRL/F
Local>SET PORT 8 PREFERRED SERVICE DEMON
Local>SET PORT 8 DEDICATED SERVICE NONE
```

- Physical port features

```
Local>SET PORT 8 FLOW CONTROL XON
Local>SET PORT 8 PARITY NONE
Local>SET PORT 8 CHARACTER SIZE 8
Local>SET PORT 8 AUTOBAUD ENABLED
Local>SET PORT 8 MODEM DISABLED
```

- Port management

```
Local>SET PORT 8 AUTHORIZED GROUPS ALL ENABLED
Local>SET PORT 8 SESSION LIMIT 4
Local>SET PORT 8 USERNAME "Robert Preston"
Local>SET PORT 8 PASSWORD DISABLED
Local>SET PORT 8 SECURITY DISABLED
```

- Port display control

```
Local>SET PORT 8 BROADCAST ENABLED
Local>SET PORT 8 VERIFICATION ENABLED
Local>SET PORT 8 TYPE ANSI
```

Saving Port Characteristics (DS500)

```
Local> SAVE PORT 10 CHARACTERISTICS
Local> LOGOUT PORT 10
Local> SAVE PORT ALL CHARACTERISTICS
Local> LOGOUT PORT ALL
```

Verifying Locally Defined Services

```
Local> SHOW SERVICES

Name                 Status      Identification

LUIGI                Available   MicroVMS System
PARROT               Available   11/785 System


TSC>LIST SERVICES

List of services defined for local system:

Name              Identification

UVMS              MicroVMS System


Local>SHOW NODE PRISM

Node: PRISM                              Address: AA-00-04-00-35-04
LAT Protocol:  V5.1                      Data Link Frame Size:  1500

Identification: The Refraction Connection

Node Groups:  0,27,50

Service Name         Status      Rating  Identification

UVMS                 Reachable       81  MicroVMS System
```


SETTING UP A PRINTER PORT

Server ports can be configured to support printer devices as well as terminals.

To set up a remote printer as an available service on the network, do the following:

1. Run LTLOAD.COM (See Example 8–24) which:
   - — Creates applications ports on a service node.
   - — Maps applications ports to server ports.
2. Run REMOTE_PRINT.COM (See Example 8–25, Example 8–26, and Example 8–27) which:
   - — Limits access for the applications port to the LATSYM print symbiont.
   - — Issues queue manager commands.
3. Set up printer port characteristics.

Example 8–24: LTLOAD.COM (Create and Map Applications Ports)

```
$ !  Copyright (c) 1987 Digital Equipment Corporation.  All rights reserved.
$ ! This command procedure starts up the LAT protocol
$ ! and configures applications devices for remote printer use.
   .
   .
   .
$ RUN SYS$SYSTEM:LATCP
!
! Set up the applications devices that will support remote printer
! access.
!
! Create the devices.
!
!CREATE PORT LTA1: /NOLOG  ❶
!CREATE PORT LTA2: /NOLOG
!
! Maps applications port(s) to a specific port(s) on the terminal
! server
!
!SET PORT LTA1: /APPLICATION /NODE=SERVER_1 /PORT=LN03  ❷
!SET PORT LTA2: /APPLICATION /NODE=SERVER-2 /PORT=PORT_3
!
! Start LAT Service
!
START NODE
EXIT
```


Example 8–25: REMOTE_PRINT.COM Default Command File

```
$ ! This command procedure sets up the local characteristics of the
$ ! applications devices for remote printers and sets up the print
$ ! queues for these remote printers.  These devices should have been
$ ! set up previously by the LTLOAD.COM command file.  NOTE: The queue
$ ! manager must be running before executing this file.
$ !
$ ! o Replace the strings formA and formA_number with the name and number
$ !   of the form you set up, or remove all references to them if you do
$ !   not set up a form.
$ ! o Replace the device types LQP02 and LA100 with the actual device
$ !   types for your remote printers.
$ ! o Replace the strings LQ$PRINT, and LA$PRINT, with the actual names
$ !   you choose for queues associated with remote printers.
$ !
$ ! Set up local characteristics for the applications devices.
$ !
$ ! SET TERMINAL LTA1: /PERM /DEVICE=LQP02 /WIDTH=80 /PAGE=60 -
                      /LOWERCASE /NOBROADCAST
$ ! SET TERMINAL LTA2: /PERM /DEVICE=LA100 /WIDTH=132 /PAGE=66 /NOBROAD
$ !
$ ! Set the protection on the devices so that only the symbiont can access
$ ! them.
$ !
$ ! SET PROTECTION=(S:RWLP,O,G,W) /DEVICE LTA1:
$ ! SET PROTECTION=(S:RWLP,O,G,W) /DEVICE LTA2:
$ !
$ ! Set the devices spooled.
$ !
$ ! SET DEVICE LTA1: /SPOOLED=(LQ$PRINT,SYS$SYSDEVICE:)
$ ! SET DEVICE LTA2: /SPOOLED=(LA$PRINT,SYS$SYSDEVICE:)
$ !
$ ! Define a form to use with the remote printers.  Be sure to use a
$ ! form number that has not already been used.
$ !
$ !  DEFINE/FORM formA formA_number /WIDTH=80 /STOCK=DEFAULT /TRUNCATE
$ !
$ ! Initialize the remote printer queues.
$ ! The following assumes that the queue manager has been started.
$ !
$ ! INITIALIZE/QUEUE /START /PROCESSOR=LATSYM /FORM=formA -
  !           /RETAIN=ERROR /DEFAULT=(NOBURST,FLAG=ONE,NOTRAILER) -
  !           /RECORD_BLOCKING LQ$PRINT /ON=LTA1:
$ ! INITIALIZE/QUEUE /START /PROCESSOR=LATSYM /RETAIN=ERROR -
  !  /DEFAULT=(NOBURST,FLAG=ONE,NOTRAILER) /RECORD_BLOCKING -
  !  LA$PRINT /ON=LTA2:
$
```

Example 8–26: COMMON_REMOTE_PRINT.COM Default Command File, (Sheet 1 of 2)

```
$! This is a template cluster common command procedure which sets up
$! characteristics and queues for remote printers.
$!
$! This file assumes that two nodes in the cluster access the remote
$! devices, and that ONLY those nodes call this file.
$!
$! o Replace the strings nodeA and nodeB with the actual names for your
$!   cluster nodes which access the remote devices.
$! o Replace the strings formA and formA_number with the name and number
$!   of the form you set up, or remove all references to them if you do
$!   not set up a form.
$! o Replace the device types LQP02 and LA100 with the actual device type
$!   for your remote devices.
$! o Replace the strings LQ$PRINT, LA$PRINT, SYS$LQPRINT and
$!   TERMINAL$PRINT with the actual names for your queues to the
$!   remote devices.
$!
$! Compute the name of the executing node
$!
$ NODE = F$GETSYI("NODENAME")
$!
$ nodeA_START = "/NOSTART"
$ nodeB_START = "/NOSTART"
$!
$! Redefine one of the previous symbols.
$!
$ 'NODE'_START = "/START"
$!
$! Set up local characteristics for the applications devices.
$!
$! This procedure assumes that the remote devices have been mapped to the
$! same LTAx: device on each node that accesses them.
$!
$ SET TERMINAL LTA1: /PERM /DEVICE=LQP02 /WIDTH=80 /PAGE=60
                     /LOWERCASE /NOBROADCAST
$ SET TERMINAL LTA2: /PERM /DEVICE=LA100 /NOBROADCAST
$!
$! Set the protection on the devices so that only the symbiont can access
$! them.
$!
$ SET PROTECTION=(S:RWLP,O,G,W) /DEVICE LTA1:
$ SET PROTECTION=(S:RWLP,O,G,W) /DEVICE LTA2:
```

Example 8–27: COMMON_REMOTE_PRINT.COM Default Command File, (Sheet 2 of 2)

```
$!
$! Set the devices spooled.
$!
$ SET DEVICE LTA1: /SPOOLED=('NODE'$LQPRINT,SYS$SYSDEVICE)
$ SET DEVICE LTA2: /SPOOLED=('NODE'$LAPRINT,SYS$SYSDEVICE)
$!
$! Define a form to use with the remote printers.  Be sure to use a
$! form number that has not already been used.
$!
$ DEFINE/FORM formA formA_number /WIDTH=80 /STOCK=DEFAULT /TRUNCATE
$!
$! Initialize the remote printer queues.
$! The following assumes that the queue manager has been started.
$!
$ INITIALIZE/QUEUE /PROCESSOR=LATSYM /FORM=formA /RETAIN=ERROR -
  /DEFAULT=(NOBURST,FLAG=ONE,NOTRAILER) /RECORD_BLOCKING -
  /ON=nodeA::LTA1: 'nodeA_START' nodeA$LQPRINT
$ INITIALIZE/QUEUE /PROCESSOR=LATSYM /RETAIN=ERROR -
  /DEFAULT=(NOBURST,FLAG=ONE,NOTRAILER) /RECORD_BLOCKING -
  /ON=nodeA::LTA2: 'nodeA_START' nodeA$LAPRINT
$!
$ INITIALIZE/QUEUE /PROCESSOR=LATSYM /FORM=formA /RETAIN=ERROR -
  /DEFAULT=(NOBURST,FLAG=ONE,NOTRAILER) /RECORD_BLOCKING -
  /ON=nodeB::LTA1: 'nodeB_START' nodeB$LQPRINT
$ INITIALIZE/QUEUE /PROCESSOR=LATSYM /RETAIN=ERROR -
  /DEFAULT=(NOBURST,FLAG=ONE,NOTRAILER) /RECORD_BLOCKING -
  /ON=nodeB::LTA2: 'nodeB_START' nodeB$LAPRINT
$!
$! Initialize the cluster wide generic queues.
$!
$! A generic queue with one printer.
$!
$ INITIALIZE/QUEUE /START /GENERIC=(nodeA$LQPRINT,nodeB$LQPRINT) -
  SYS$LQPRINT
$!
$! A generic queue with two printers.
$!
$ INITIALIZE/QUEUE /START /GENERIC=(nodeA$LQPRINT,nodeA$LAPRINT, -
  nodeB$LQPRINT, nodeB$LAPRINT) TERMINAL$PRINT
```

Port characteristics must be modified from their default settings in order to support printer devices. Example 8–28 is a port configured for host-initiated requests.

Example 8–28: Printer Port Configuration

```
Port 2:

Character Size:            8          Input Speed:        4800
Flow Control:            XON          Output Speed:       4800
Parity:                 None          Modem Control:   Disabled

Access:                Remote          Local Switch:       None
Backwards Switch:        None          Name:             LN03_4
Break:                Disabled         Session Limit:         1
Forwards Switch:         None          Type:               Hard

Preferred Service: None

Authorized Groups:    0
(Current)  Groups:    0

Enabled Characteristics:

DSRlogout,  Inactivity Logout,  Input Flow Control,  Output Flow Control,
Verification
```

Table 8–2 lists required values that must be changed from the default settings:

Table 8–2: Required Characteristics to Change for a Printer Port

CHARACTERISTIC	SETTING
ACCESS	REMOTE
AUTOBAUD	DISABLED
BREAK	DISABLED
DSRLOGOUT	ENABLED
INACTIVITY LOGOUT	ENABLED
NAME	port name

SUMMARY

- The DECserver 200 has two databases:
  - — Permanent
  - — Operational
- The DECserver 500 has three databases:
  - — Permanent
  - — Operational
  - — Log-in
- There are a variety of different server types, although the user interface is basically the same.
- The server software is installed on service nodes, also called load hosts, and down-line loaded to the terminal server upon initialization.
- Port characteristics can be viewed and modified by the user in nonprivileged mode.
- Server characteristics can be modified in privileged mode.
- Services available to the server can be listed, and connections established to them.
- Selected ports on the server can be tested.
- Multiple sessions to different services can be maintained, and the user can switch between them without termination.
- On-line help can be accessed in local mode.
- Terminal server ports can be configured to support printer devices. There are several configurations well documented in the Management Guide for the server you are using. (Port configuration section).

MODULE 9
TEST

TEST

Select the letter corresponding to the option that best answers each of the following questions, and mark the answer on the answer sheet provided. There is only one correct answer for each question.

1. **What commands are used to bring up DECnet software on a VMS system?**

   a. @SYSGEN and @STARTNET.COM

   b. @NETCONFIG.COM and @NETGEN

   c. @NETCONFIG.COM and @STARTNET.COM

   d. @SYSGEN and @NETGEN

2. **Which of the following tests should be run after DECnet software is installed on a VMS system to verify that the installation did not have an adverse effect on the operating system?**

   a. NTEST

   b. STARTNET

   c. NETINS

   d. UETP

3. **Which of the following NCP commands manipulates the volatile database?**

   a. PURGE

   b. DEFINE

   c. LIST

   d. CLEAR

4. Which of the following commands creates a new entry in the permanent database on a DECnet-VAX node?

   a. SET NODE ROGER ADDRESS 2.4

   b. SET NODE 2.4 NAME ROGER

   c. DEFINE NODE 2.4 NAME ROGER

   d. DEFINE ADDRESS 2.4 NAME ROGER

5. Which NCP command allows all current network activity to complete while disallowing any new activity to take place?

   a. SET EXECUTOR STATE RESTRICTED

   b. SET EXECUTOR STATE OFF

   c. SET EXECUTOR STATE CLOSED

   d. SET EXECUTOR STATE SHUT

6. Which of the following AUTHORIZE commands sets up a PROXY entry so that user JOHNSON on node ALPHA can access the STUDENT account on node BRAVO?

   a. ADD/PROXY ALPHA::JOHNSON STUDENT

   b. ADD/PROXY BRAVO::STUDENT JOHNSON

   c. ADD/PROXY STUDENT ALPHA::JOHNSON

   d. ADD/PROXY JOHNSON BRAVO::STUDENT

7. Which NCP command should be issued to find the circuit cost for circuit DMC-2 on remote node FOXTRT?

   a. TELL FOXTRT SHOW CIRCUIT DMC-2 COUNTERS

   b. TELL FOXTRT SHOW EXECUTOR CHARACTERISTICS

   c. TELL FOXTRT SHOW CIRCUIT DMC-2 CHARACTERISTICS

   d. TELL FOXTRT SHOW CIRCUIT DMC-2 COST

8. Which NCP command identifies a node's physical Ethernet address?

   a. SHOW LINE UNA-0 CHARACTERISTICS

   b. SHOW EXECUTOR STATUS

   c. SHOW CIRCUIT UNA-0 STATUS

   d. SHOW EXECUTOR CHARACTERISTICS

9. Which DCL command displays (on one screen) several important classes of information about the local node's performance?

   a. MONITOR SYSTEM

   b. MONITOR SCS

   c. MONITOR STATES

   d. MONITOR ALL_CLASSES

10. Which of the following specifies when permanent database parameter values take effect?

    a. As soon as they are changed within NCP

    b. When the network is restarted

    c. After a timeout interval

    d. When the user exits out of NCP

11. Which circuit should low circuit costs be assigned to?

    a. Low bandwidth circuit

    b. High bandwidth circuit

    c. Circuit with multiple connections

    d. None of the above

12. An error in which of the following network parameters would cause a file to arrive at an incorrect node?

    a. Buffer size

    b. Maximum visits

    c. Maximum hops

    d. Node address

13. Which counter indicates inadequate buffer allocation?

    a. Transit congestion loss

    b. Data errors outbound

    c. Remote reply timeouts

    d. Initialization failure

14. Which of the following items are affected by circuit costs?

    I Traffic patterns

    II Circuit state

    III Node congestion

    a. I and II

    b. I and III

    c. II and III

    d. I, II, and III

15. Which NCP command allows this command to execute properly?

    NCP> LOOP CIRCUIT UNA-0 NODE ECHO

    a. SET CIRCUIT UNA-0 STATE OFF SERVICE DISABLED

    b. SET CIRCUIT UNA-0 STATE ON SERVICE DISABLED

    c. SET CIRCUIT UNA-0 STATE OFF SERVICE ENABLED

    d. SET CIRCUIT UNA-0 STATE ON SERVICE ENABLED

16. Which of the following NCP commands would you issue from node DELTA to verify the operation of the local node's DECnet software?

    a. LOOP EXECUTOR COUNT 10

    b. LOOP CIRCUIT UNA-1 COUNT 10

    c. LOOP NODE COUNT 10

    d. LOOP NODE DELTA COUNT 10

17. What is the node that collects logging information from other network nodes known as?

    a. Event logger

    b. Sink node

    c. End node

    d. Target node

18. When a user is communicating directly with the terminal server software user interface, the port is said to be in which of the following modes?

    a. Session mode

    b. Service mode

    c. Local mode

    d. Dedicated mode

19. Of the following methods to downline load a terminal server, which are initiated by (or at) the server?

    a. Cycling power on the server and issuing the INITIALIZE command

    b. Issuing the INITIALIZE command and issuing the NCP LOAD command

    c. Issuing the NCP TRIGGER command and issuing the NCP LOAD command

    d. Cycling power on the server

20. Which type of loopback test uses normal logical links for transmission?

    a. Circuit loopback

    b. Controller loopback

    c. Line loopback

    d. Node loopback

21. Which of the following actions can a network manager take to enhance security for the default DECnet account?

    I Set the LOCKPWD AUTHORIZE flag for the DECnet account.

    II Place the DECnet account in a UIC group by itself.

    III Point the AUTHORIZE qualifier LGICMD to a file that does not reside in the DECnet log-in directory.

    a. I and II

    b. I and III

    c. II and III

    d. I, II and III

22. Of the following NCP commands which one would allow outgoing access to but prevent incoming access from remote node HECTOR?

    a. SET EXECUTOR HECTOR DEFAULT ACCESS OUTGOING

    b. SET NODE HECTOR ACCESS NOINCOMING

    c. SET NODE HECTOR ACCESS OUTGOING

    d. SET NODE HECTOR ACCESS NONE

23. Which of the following is the correct order of system-level access checking during network process creation?

    a. EXPLICIT, DEFAULT, PROXY

    b. DEFAULT, PROXY, EXPLICIT

    c. EXPLICIT, PROXY, DEFAULT

    d. PROXY, EXPLICIT, DEFAULT

24. Loopback testing can be used to isolate faults in which of the following?

    I User Layer software

    II Logical links

    III Modems

    a. I and II

    b. I and III

    c. II and III

    d. I, II and III

25. All of the following Ethernet devices forward packets to other parts of the network. Which one is a store and forward device that forwards only those packets destined for a node located on a remote segment?

    a. Bridge

    b. Gateway

    c. Repeater

    d. Router

26. Which two DNA Layers are responsible for logical links?

    a. End Communication and Session Control

    b. Routing and Network Application

    c. Routing and Session Control

    d. End Communication and Network Application

27. Which of the following statements regarding Ethernet LANs are correct?

    I Several protocols can run over an Ethernet LAN simultaneously.

    II With the addition of repeaters, the Ethernet LAN can be extended up to 22,000 meters.

    III According to the specification, the maximum distance allowed between two nodes is 2800 meters.

    a. I and II

    b. I and III

    c. II and III

    d. I, II, and III

28. Which Data Link protocol provides a best-effort delivery service, leaving error recovery to higher layers?

    a. DDCMP

    b. Ethernet

    c. X.25

    d. All of the above

29. Which of the following statements accurately represent routing on an Ethernet LAN?

    I If there are too many routers on an Ethernet LAN, the number of collisions increases and the efficiency decreases.

    II The router with the highest priority, the designated router, intervenes in transmissions between end nodes.

    III If the Ethernet LAN is an independent network with no wide area connections, it is not necessary to have any routers.

    a. I and II

    b. I and III

    c. II and III

    d. I, II, and III

30. When outbound proxy ACI is attempted, which of the following databases are checked for the value of the proxy parameter?

    a. NETOBJECT

    b. NETNODE_LOCAL

    c. NETOBJECT then NETNODE_LOCAL

    d. NETNODE_LOCAL then NETNODE_REMOTE

31. On a non-clustered node, what two command procedures are executed to configure a printer port on a terminal server?

    a. DSVCONFIG.COM and REMOTE_PRINT.COM

    b. SYSTARTUP.COM and LTLOAD.COM

    c. SYSTARTNET.COM and REMOTE_PRINT.COM

    d. LTLOAD.COM and REMOTE_PRINT.COM

32. Which of the following command procedures is usually used to set up the initial permanent database for DECnet software?

    a. SYS$SYSTEM:STARTNET.COM

    b. SYS$SYSTEM:NETCONFIG.COM

    c. SYS$MANAGER:NICONFIG.COM

    d. SYS$MANAGER:NETCONFIG.COM

33. Which of the following parameters (on the remote node) might need tuning if you consistently receive the message: Insufficient resources at remote node.

    I Maximum links

    II Executor buffer size

    III Incoming and outgoing timers

    a. I and II

    b. I and III

    c. II and III

    d. I, II, and III

ANSWERS

The correct answer for each question is underlined.

1. What commands are used to bring up DECnet software on a VMS system?

    a. @SYSGEN and @STARTNET.COM

    b. @NETCONFIG.COM and @NETGEN

    c. @NETCONFIG.COM and @STARTNET.COM

    d. @SYSGEN and @NETGEN

2. Which of the following tests should be run after DECnet software is installed on a system to verify that the installation did not have an adverse effect on the opera system?

    a. NTEST

    b. STARTNET

    c. NETINS

    d. UETP

3. Which of the following NCP commands manipulates the volatile database?

    a. PURGE

    b. DEFINE

    c. LIST

    d. CLEAR

4. **Which of the following commands creates a new entry in the permanent database on a DECnet-VAX node?**

   a. SET NODE ROGER ADDRESS 2.4

   b. SET NODE 2.4 NAME ROGER

   c. DEFINE NODE 2.4 NAME ROGER

   d. DEFINE ADDRESS 2.4 NAME ROGER

5. **Which NCP command allows all current network activity to complete while disallowing any new activity to take place?**

   a. SET EXECUTOR STATE RESTRICTED

   b. SET EXECUTOR STATE OFF

   c. SET EXECUTOR STATE CLOSED

   d. SET EXECUTOR STATE SHUT

6. **Which of the following AUTHORIZE commands sets up a PROXY entry so that user JOHNSON on node ALPHA can access the STUDENT account on node BRAVO?**

   a. ADD/PROXY ALPHA::JOHNSON STUDENT

   b. ADD/PROXY BRAVO::STUDENT JOHNSON

   c. ADD/PROXY STUDENT ALPHA::JOHNSON

   d. ADD/PROXY JOHNSON BRAVO::STUDENT

7. **Which NCP command should be issued to find the circuit cost for circuit DMC-2 on remote node FOXTRT?**

   a. TELL FOXTRT SHOW CIRCUIT DMC-2 COUNTERS

   b. TELL FOXTRT SHOW EXECUTOR CHARACTERISTICS

   c. TELL FOXTRT SHOW CIRCUIT DMC-2 CHARACTERISTICS

   d. TELL FOXTRT SHOW CIRCUIT DMC-2 COST

8. **Which NCP command identifies a node's physical Ethernet address?**

   a. SHOW LINE UNA-0 CHARACTERISTICS

   b. SHOW EXECUTOR STATUS

   c. SHOW CIRCUIT UNA-0 STATUS

   d. SHOW EXECUTOR CHARACTERISTICS

9. **Which DCL command displays (on one screen) several important classes of information about the local node's performance?**

   a. MONITOR SYSTEM

   b. MONITOR SCS

   c. MONITOR STATES

   d. MONITOR ALL_CLASSES

10. **Which of the following specifies when permanent database parameter values take effect?**

    a. As soon as they are changed within NCP

    b. When the network is restarted

    c. After a timeout interval

    d. When the user exits out of NCP

11. **Which circuit should low circuit costs be assigned to?**

    a. Low bandwidth circuit

    b. High bandwidth circuit

    c. Circuit with multiple connections

    d. None of the above

12. An error in which of the following network parameters would cause a file to arrive at an incorrect node?

    a. Buffer size

    b. Maximum visits

    c. Maximum hops

    d. Node address

13. Which counter indicates inadaquate buffer allocation?

    a. Transit congestion loss

    b. Data errors outbound

    c. Remote reply timeouts

    d. Initialization failure

14. Which of the following items are affected by circuit costs?

    I Traffic patterns

    II Circuit state

    III Node congestion

    a. I and II

    b. I and III

    c. II and III

    d. I, II, and III

15. Which NCP command allows this command to execute properly?

    NCP> LOOP CIRCUIT UNA-0 NODE ECHO

    a. SET CIRCUIT UNA-0 STATE OFF SERVICE DISABLED

    b. SET CIRCUIT UNA-0 STATE ON SERVICE DISABLED

    c. SET CIRCUIT UNA-0 STATE OFF SERVICE ENABLED

    d. SET CIRCUIT UNA-0 STATE ON SERVICE ENABLED

16. Which of the following NCP commands would you issue from node DELTA to verify the operation of the local node's DECnet software?

    a. LOOP EXECUTOR COUNT 10

    b. LOOP CIRCUIT UNA-1 COUNT 10

    c. LOOP NODE COUNT 10

    d. LOOP NODE DELTA COUNT 10

17. What is the node that collects logging information from other network nodes known as?

    a. Event logger

    b. Sink Node

    c. End Node

    d. Target Node

18. When a user is communicating directly with the terminal server software user interface, the port is said to be in which of the following modes?

    a. Session mode

    b. Service mode

    c. Local mode

    d. Dedicated mode

19. Of the following methods to downline load a terminal server, which are initiated by (or at) the server?

    a. Cycling power on the server and issuing the INITIALIZE command

    b. Issuing the INITIALIZE command and issuing the NCP LOAD command

    c. Issuing the NCP TRIGGER command and issuing the NCP LOAD command

    d. Cycling power on the server

20. Which type of loopback test uses normal logical links for transmission?

    a. Circuit loopback

    b. Controller loopback

    c. Line loopback

    d. Node loopback

21. Which of the following actions can a network manager take to enhance security for the default DECnet account?

    I Set the LOCKPWD AUTHORIZE flag for the DECnet account

    II Place the DECnet account in a UIC group by itself

    III Point the AUTHORIZE qualifier LGICMD to a file that does not reside in the DECnet log-in directory

    a. I and II

    b. I and III

    c. II and III

    d. I, II and III

22. Of the following NCP commands which one would allow outgoing access to but prevent incoming access from remote node HECTOR?

    a. SET EXECUTOR HECTOR DEFAULT ACCESS OUTGOING

    b. SET NODE HECTOR ACCESS NOINCOMING

    c. SET NODE HECTOR ACCESS OUTGOING

    d. SET NODE HECTOR ACCESS NONE

23. Which of the following is the correct order of system-level access checking during network process creation?

    a. EXPLICIT, DEFAULT, PROXY

    b. DEFAULT, PROXY, EXPLICIT

    c. EXPLICIT, PROXY, DEFAULT

    d. PROXY, EXPLICIT, DEFAULT

24. Loopback testing can be used to isolate faults in which of the following?

    I User Layer software

    II Logical links

    III Modems

    a. I and II

    b. I and III

    c. II and III

    d. I, II and III

25. All of the following Ethernet devices forward packets to other parts of the network. Which one is a store and forward device that forwards only those packets destined for a node located on a remote segment?

    a. Bridge

    b. Gateway

    c. Repeater

    d. Router

26. Which two DNA Layers are responsible for logical links?

    a. End Communication and Session Control

    b. Routing and Network Application

    c. Routing and Session Control

    d. End Communication and Network Application

27. Which of the following statements regarding Ethernet LANs are correct?

    I Several protocols can run over an Ethernet LAN simultaneously.

    II With the addition of repeaters, the Ethernet LAN can be extended up to 22,000 meters.

    III According to the specification, the maximum distance allowed between two nodes is 2800 meters.

    a. I and II

    b. I and III

    c. II and III

    d. I, II, and III

28. Which Data Link protocol provides a best-effort delivery service, leaving error recovery to higher layers?

    a. DDCMP

    b. Ethernet

    c. X.25

    d. All of the above

29. Which of the following statements accurately represent routing on an Ethernet LAN?

    I If there are too many routers on an Ethernet LAN, the number of collisions increases and the efficiency decreases.

    II The router with the highest priority, the designated router, intervenes in transmissions between end nodes.

    III If the Ethernet LAN is an independent network with no wide area connections, it is not necessary to have any routers.

    a. I and II

    b. I and III

    c. II and III

    d. I, II, and III

30. When outbound proxy ACI is attempted, which of the following databases are checked for the value of the proxy parameter?

    a. NETOBJECT

    b. NETNODE_LOCAL

    c. NETOBJECT then NETNODE_LOCAL

    d. NETNODE_LOCAL then NETNODE_REMOTE

31. **On a non-clustered node, what two command procedures are executed to configure a printer port on a terminal server?**

    a. DSVCONFIG.COM and REMOTE_PRINT.COM

    b. SYSTARTUP.COM and LTLOAD.COM

    c. SYSTARTNET.COM and REMOTE_PRINT.COM

    d. LTLOAD.COM and REMOTE_PRINT.COM

32. **Which of the following command procedures is usually used to set up the initial permanent database for DECnet software?**

    a. SYS$SYSTEM:STARTNET.COM

    b. SYS$SYSTEM:NETCONFIG.COM

    c. SYS$MANAGER:NICONFIG.COM

    d. SYS$MANAGER:NETCONFIG.COM

33. **Which of the following parameters (on the remote node) might need tuning if you consistently receive the message: Insufficient resources at remote node.**

    I Maximum links

    II Executor buffer size

    III Incoming and outgoing timers

    a. I and II

    b. I and III

    c. II and III

    d. I, II, and III

APPENDIX A
NETWORK SITE GUIDE

Example A–1: Node Log

Node Name_____ Node Address_____

System Manager_____ Telephone_____

Node Type_____ Location_____

System Type_____ Base Software_____

Device Type_____ DECnet Version_____

If Remote Load - Designated Load Host_____

Layered Products Installed_____

Access Control Method_____

Circuits ID --	Comm. Cont. -----	Speed -----	Trans. Type ----------	Protocol --------	Cost ----

Example A–2: Third Party Vendor Contact List

Product Name ------------	Vendor ------	Service Contact ---------------	Telephone ---------

Example A–3: Problem Log

Problem Number_____

Date Problem Reported_____ Reported By_____

Problem Description_____

_____

_____

_____

_____

Changes Made Prior to the Appearance of the Problem?_____

_____

_____

_____

_____

_____

Hardware_____ Software_____

_____ _____

_____ _____

Resolution Date_____

Problem Resolution_____

_____

_____

_____

Example A–4: NCP Update Form

Node Name_____

Date	Parameter	Old Value	New Value	Comments
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____
_____	_____	_____	_____	_____