IBM

International Technical Support Centers

IBM 9370 LAN
VOLUME 2 - IEEE 802.3 SUPPORT

GG24-3227-00

IBM 9370 LAN
Volume 2 - IEEE 802.3 Support

Document Number GG24-3227-0

April 1st, 1988

International Technical Support Center
Boeblingen

First Edition (April 1988)

References in this publication to IBM products, programs, or services do not imply that IBM intends to make these available in all countries in which IBM operates. Any reference to an IBM program product in this document is not intended to state or imply that only IBM's program product may be used. Any functionally equivalent program may be used instead.

> The information contained in this document has not been submitted to any formal IBM test and is distributed on an 'As Is' basis without any warranty either expressed or implied. The use of this information or the implementation of any of these techniques is a customer responsibility and depends on the customer's ability to evaluate and integrate them into the customer's operational environment. While each item may have been reviewed by IBM for accuracy in a specific situation, there is no guarantee that the same or similar results will be obtained elsewhere. Customers attempting to adapt these techniques to their own environments do so at their own risk.

Publications are not stocked at the address given below. Requests for IBM publications should be made to your IBM representative or to the IBM branch office serving your locality.

A form for reader's comments is provided at the back of this publication. If the form has been removed, comments may be addressed to IBM International Technical Support Center, Dept. 3222, Bldg. 7030-75, Schoenaicher Strasse 220, 7030 Boeblingen, West Germany. IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

ABSTRACT

This document is volume two of a series of two volumes on the 9370 LAN installation.

Volume one, "IBM 9370 LAN, Volume 1 - Token Ring Support", GG24-3240 presents our experiences installing 9370 Token-Ring Subsystem in the ITSC Raleigh, with emphasis on the practical information that readers will need to install and run their own 9370 Token-Ring environment. Though operations under SNA are emphasized, instructions for installation and operation of TSAF and SQL are also covered.

Volume two (this document), "IBM 9370 LAN, Volume 2 - 802.3 Support", GG24-3227 describes the installation and usage of the 802.3 Integrated 9370 Subsystem (Feature 6130/6035). The software which has been used to operate the IBM 9370 IEEE 802.3 Subsystem is TCP/IP V1.1. TSAF is not part of this documentation.

CSYS (62 pages)

ACKNOWLEDGEMENTS

The authors of this Bulletin are:

- Felicity Markham IBM UK
- Peter Koepp ITSC Boeblingen

Project Advisor

- Peter Koepp ITSC Boeblingen

This bulletin is the result of a residency conducted at the Boeblingen International Technical Support Center.

Thanks to the following persons for their review activities:

- S.Sutter
- H.Struck
- R.Schneck

HOW TO USE THIS PUBLICATION

The purpose of this publication is:

- to guide the installation of the IBM 9370 Information System integrated IEEE 802.3 LAN hardware and microcode. IBM 7170, IBM 8232, and S/1 as IEEE 802.3 LAN attachment controllers are NOT covered.

- to guide the installation of TCP/IP (for VM) Version 1 Release 1.1. software under VM Rel. 5.0

This document is aimed at those users who intend to use the IEEE 802.3 LAN subsystem on a IBM 9370 Information System and use it with TCP/IP (for VM) Version 1 Release 1.1.

HOW THIS BULLETIN IS ORGANIZED

This publication comprises four major sections:

Chapter 1: Introduction

This section is an introduction to the subject.

Chapter 2: Installation of 9370 IEEE 802.3 LAN subsystem

This section includes a step by step explanation to install the integrated IEEE 802.3 LAN hardware and microcode for the IBM 9370 Information System, and an introduction of some test facilities.

Chapter 3

This chapter explains how to install the TCP/IP software package under VM/SP. The complete information necessary for installation is not printed here, but this chapter is intented to point out some difficult spots in the installation procedure. The official installation publications are required.

Chapter 4

This chapter gives an overview of TCP/IP facilities, including FTP, TELNET, and SMTP, and explains how to use them. Again, this chapter does not comprise all the information, but should be regarded as additional hints and tips material to the official publications.

PREREQUISITE PUBLICATIONS

None

RELATED DOCUMENTS

- 9370 LAN -Volume 1, Token Ring Support, GA24-3240
- LAN Concepts and Positioning, GA24-3178-xx

Supplied automatically with "VM Interface Program for TCP/IP" 5798-FAL is the following machine readable material (also available from Mechanisburg).

- TCP/IP for VM, Licensed Program Specifications, GC09-1205-xx
- TCP/IP for VM, Installation and Maintenance Manual, GC09-1203-xx
- TCP/IP for VM, Command Reference, GC09-1204-xx
- TCP/IP for VM, Programmer's Manual, GC09-1206-xx

General Information about the IEEE 802.3 LAN Subsystem and information about the installation and configuration:

- 9370, Planning for Your System, GA24-4032-xx
- 9370, Introducing the System, GA24-4030-xx
- 9370, Operating Your System, SA24-4036-xx
- 9370, Using the System Programmer Functions, SA24-4037-xx

Technical Information about the interface of the IEEE 802.3 LAN subsystem:

- IEEE 802.3 LAN, Reference Manual, SA33-1590-xx

TABLE OF CONTENTS

LIST OF ILLUSTRATIONS

1.0 INTRODUCTION AND CONCEPTS

The 9370 Information System is a modular system with a new packaging technology, part of which is the connection to the IEEE 802.3 LAN network via an integrated controller and adapter.

The name ETHERNET[1] was born out of the research and development activities of the XEROX Palo Alto Research Center. They published a local area network design with the following aims in 1976:

- high datarate (10 Mbps)
- support of several hundred stations
- range of a few kilometers
- low costs
- high reliability

This first design has been picked up by a group of three companies: Digital Equipment, Intel, and XEROX (sometimes abbreviated as DIX, thus such definitions as DIX-Standard). It has been published as an improved version in 1980. This specification was the base for the Local Area Network Standardization Committee of the IEEE and has been used as the working base by the IEEE 802.3 subcommittee. Other subcommittees were working with the 802.5 Token Ring Access Method and the 802.4 Token Passing Bus Access Methodology. The IEEE 802.3 Subcommittee released the IEEE 802.3 LAN standard in 1985.

Three slightly different versions can be found in existing ETHERNET networks today.

1. ETHERNET Version 1
   This is the first ETHERNET solution. Transceivers which adhere to this concept are incompatible with IEEE 802.3.

2. ETHERNET Version 2
   This version is also known as the DIX version. The frame format is almost the same as outlined in the following figure, except that the length field is replaced with a TYPE field.

3. IEEE 802.3 LAN
   This is the version, which has been standardized by IEEE. It is also IBM's implementation of the 9370 IEEE 802.3 LAN Subsystem. The frame format has the following shape.

---

[1] ETHERNET is a trademark of XEROX Corp.

Preamble	42 bit
SDF	8 bit
Dest. Address	48 bit
Source Address	48 bit
Length	16 bit
LLC Data	min 64 bytes, max 1500 bytes
PAD	variable length
FCS	32 bit

Figure 1. MAC Frame Format

Today, the ETHERNET network is defined in IEEE 802.3 Standard, in the ECMA Standards 80, 81, and 82, and in the ISO DIS 8802/3 Standard.

Up to the announcement of the IBM 9370, the connection of a S/370 architectural machine to an IEEE 802.3 LAN network required a device called DACU (Device Attachment Control Unit, or IBM 7170). It is now simplified with the availability of an integrated pair of cards (controller and adapter) in the IBM 9370 Information System. This paper will mainly cover the aspects related to the new controller/adapter pair of cards (Feature 6130/6035) for the 9370 Information System machines, when being operated with TCP/IP under VM (5798-FAL). TSAF, being an element of VM, which also supports the 802.3 LAN Subsystem is not covered in this bulletin.

This does not imply, that the other options (IBM 7170 or IBM 8232) are not available anymore on the IBM 9370 Information System to connect to an IEEE 802.3 network. But it is a more convenient and less expensive solution to use the integrated 802.3 subsystem (feature 6130/6035).

The IEEE 802.3 LAN subsystem in the IBM 9370 Information System consists of:

- One communication Processor (Feature 6130)
- One IEEE 802.3 LAN Adapter (Feature 6035)
- The IEEE 802.3 LAN Microcode

This allows you to attach the IBM 9370 Information System to an IEEE 802.3 LAN network.

All models of the IBM 9370 Information Systems support this feature but the number of IEEE 802.3 LAN subsystems operating concurrently on one system is restricted; two for 9373, two for 9375, and twelve for 9377.

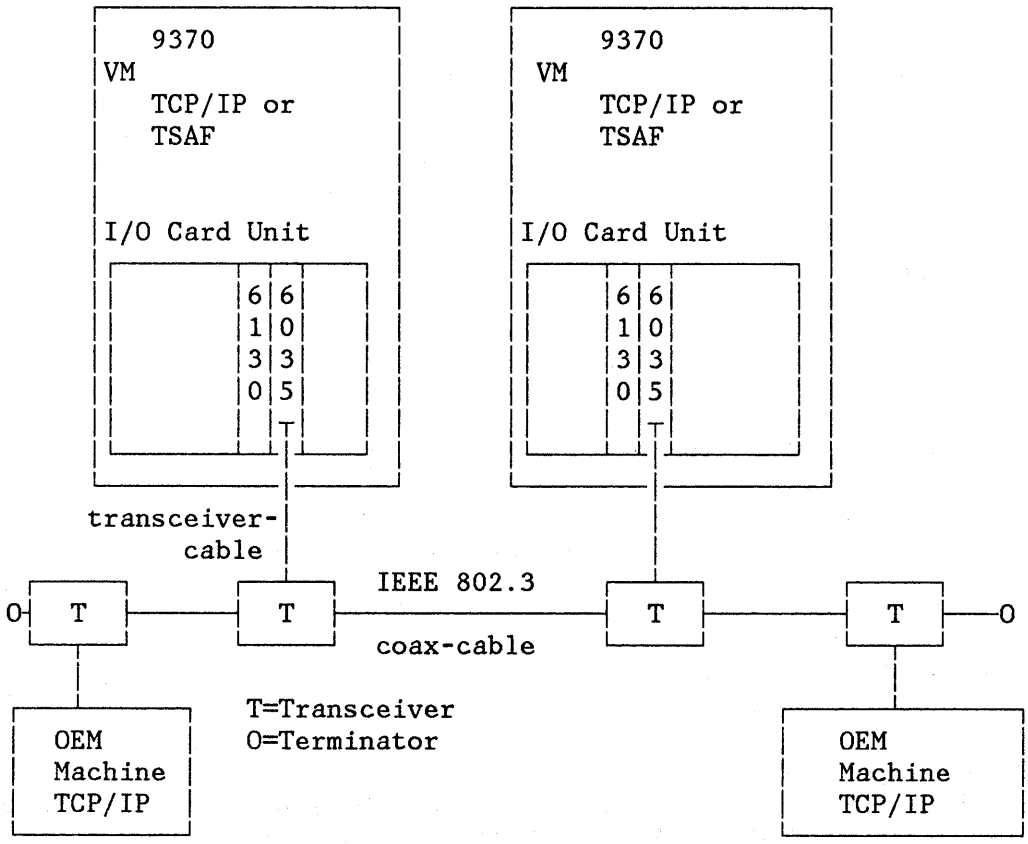

Figure 2. Schematic View of IEEE 802.3 LAN Attachment in IBM 9370 Information System

The IEEE 802.3 LAN subsystem is supported by TCP/IP Version 1, Release 1.1 under VM (5798-FAL) and TSAF which is part of VM/SP Release 5 on the IBM 9370 Information System. No support is provided by VSE and MVS.

For the connection to other systems additional equipment is required which is not available from IBM (transceiver, transceiver cable, and IEEE 802.3 LAN co-axial cable). This equipment is standardized in IEEE 802.3 and there are a number of companies which market this additional hardware. It should not cause any problems, if you validate that this additional equipment conforms to the standard.

Note: Some transceivers have switches, which allow operation in ETHERNET version 1 mode. This is not compatible with IEEE 802.3 and does not work with the IBM 9370 802.3 Subsystem.

1.1 HISTORY OF THE 9370 INTEGRATED 802.3 LAN SUBSYSTEM

The announcement of the integrated IEEE 802.3 LAN subsystem of the IBM 9370 Information System came with the IBM 9370 Information System announcement on Oct. 7th, 1986. General availability (GA) was in Dec. 1987. The hardware for the IEEE 802.3 LAN subsystem at its initial announcement was Feature 6030 (Communication Controller) and Feature 6035 (802.3 Adapter). Along with the shipping of the IEEE 802.3 LAN hardware for the IBM 9370 Information System, a new communication controller was announced (Feature 6130) in Dec.1987. All IBM 9370 Information Systems with an integrated IEEE 802.3 LAN attachment must now be equipped with communication controller feature 6130, and adapter feature 6035. Shipping of the microcode for the 802.3 Subsystem began in January and February 1988.

1.2 TCP/IP AND THE DOD ARPA

During the 1970's DARPA commissioned a great deal of research into computer networking. One of the most useful results of that work has been the TCP/IP protocols. A large number of computer vendors have implemented TCP/IP using various underlying network media. At MIT, there was even an implementation of TCP/IP which worked using slow-speed RS-232 lines. The TCP/IP protocols became also an integral element of the Berkerley UNIX version 4.2, a very popular UNIX implementation in scientific environments. The combination UNIX - TCP/IP - ETHERNET became almost a standard for workstation manufacturers.

A number of protocols belong to the TCP/IP family. They are briefly introduced in the following paragraphs. One thing you will notice is that the TCP/IP protocol family has no protocols defined for network management, such as NetView for SNA. This is probably the biggest disadvantage of TCP/IP.

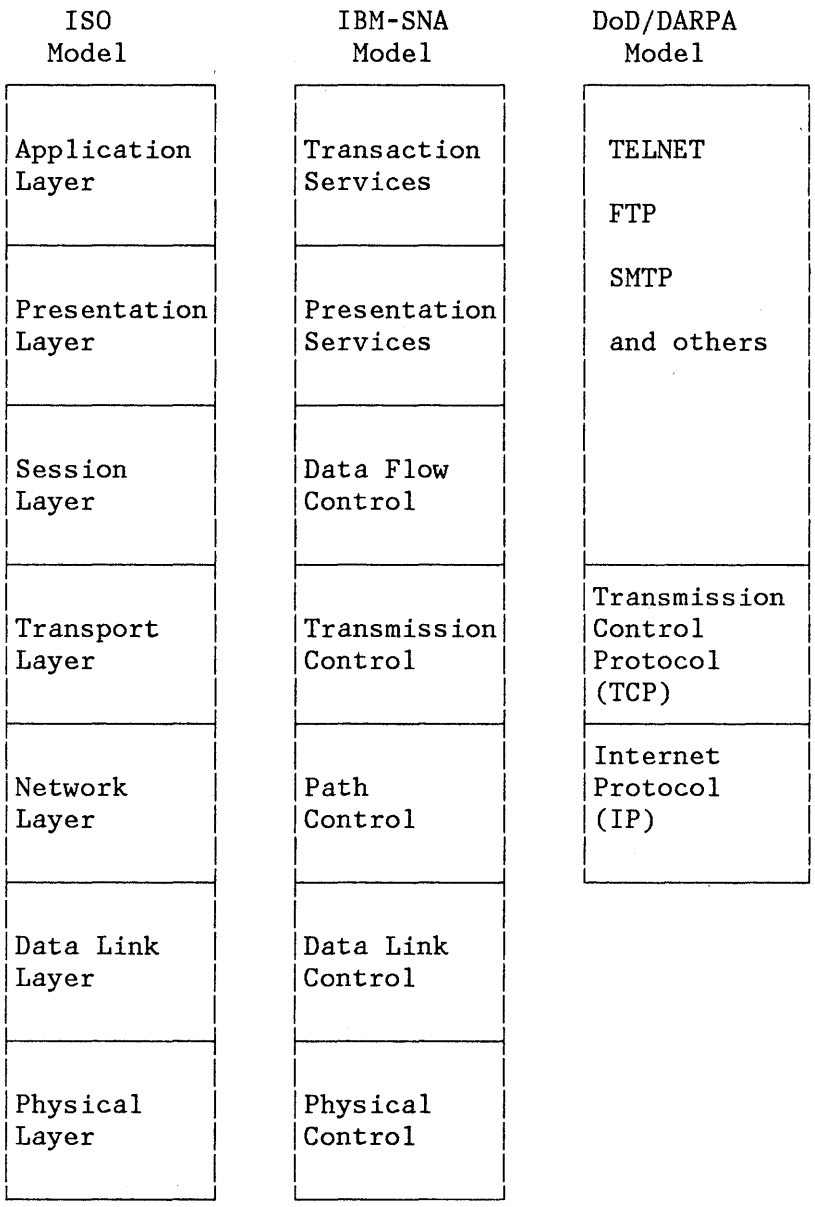

Figure 3. Schematic View of Network Models

1.2.1 IP (INTERNET PROTOCOL)

The Internet Protocol (IP) handles data packets, called datagrams, via several nodes from the sender to the receiver. It is a member of the layer 3 of the ISO/OSI reference model. No acknowledgement is returned when transmitting datagrams, the IP protocol does not ensure a safe

transmission of datagrams (see TCP). If the datagrams are too long to fit into one frame, IP fragments the datagram into several smaller ones.

1.2.2 INTERNET ADDRESSES

The internet protocol routes packets to hosts based on their "internet address". This address is always a 32-bit number and is distinct from the LAN hardware address, which is usually available in ROM on the network adapter card. IP performs a logical translation of the internet address to the Ethernet address of the destination (see also Address Resolution Protocol, ARP), or else sends the packet to another node that is better able to do so (for instance, a gateway).

Internet addresses consist of two parts; part one is a network address, part two is a local address. The IP-addresses are usually specified as four numbers separated by periods (if octal numbers are used, the field separators may be commas). For instance, a valid Internet address would be 192.9.200.1 where each field is understood to be a decimal number.

There are three classes of internet addresses, all of which result in the concatenation of a network number with a host number on that network. The only difference between the classes is that each one has a different number of bits available for the network number, and then by necessity for the host number also (since each address must be 32 bits). Class A networks are those which have the high-order bit set to '0'. The next 7 bits form the network number, and the remaining 24 bits specify the host address on that network. Very often on class A networks the host address is simply taken to be the lower 24 bits of the Ethernet address.

Class A addresses:

7 Bit for class A networks, 24 bit local address

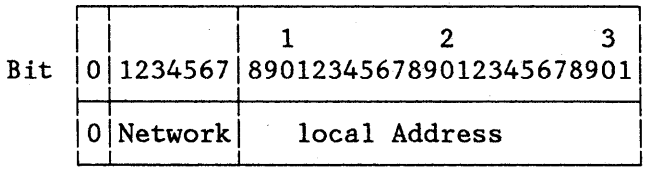

Figure 4. Class A Internet Addresses

If the two high-order bits of the Internet address are '10', the address is of class B. Then the 14 next most-significant bits form the network number (for a total of 16,384 possible networks) and the remaining 16 bits are the host address.

Class B addresses:

14 Bits for class B networks, 16s bit local address

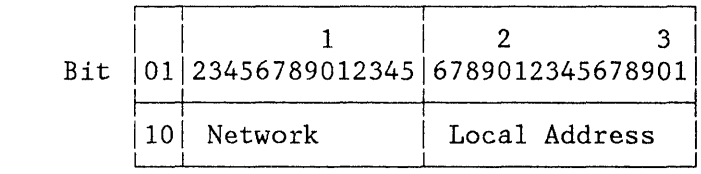

Figure 5. Class B Internet Addresses

Finally, class C addresses are those with the three high-order bits set to '110'. Class C addresses have a 21-bit network number and 8 bits remain for the host address, so that no more than 256 hosts can reside on the same class C network. Typical Ethernet installations will use class C internet addresses.

Class C addresses:

21 Bits for C networks, 8 bits local address

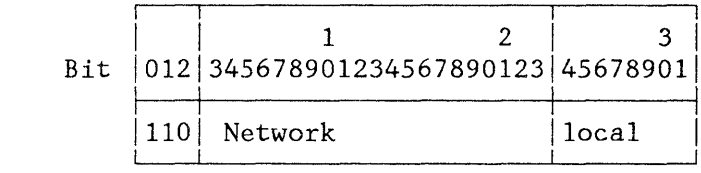

Figure 6. Class C Internet Addresses

1.2.3 TCP (TRANSPORT CONTROL PROTOCOL)

TCP ensures a reliable transmission from end to end. It can be assigned to layer 4 of the ISO/OSI reference model. TCP also solves a number of associated difficulties that might arise during the transmission of a stream of data between source and target. Among those are control of sequencing, error control, recovery, multiplexing, and connection management.

1.2.4 TELNET, FTP

Telnet and FTP are two programs usually supplied with the TCP/IP protocols and developed for use with those protocols. These programs, as do a majority of network programs, require the cooperation of programs on the source and destination computers. The destination program is usually called a "server", and the user program at the source is called its "client". Not all implementations offer clients and servers for TELNET and FTP. For example, if no server is available, the member of the network cannot be used by other participants.

1.2.5 TELNET

Telnet provides a "virtual" or "network" terminal over the TCP/IP connection. Just as with any other login, the user (client) must provide a userid and password before access to the server system is granted. After a successful login sequence, telnet users can act just as if their terminals are directly connected to the remote host.

The client telnet software usually allows the user to perform certain local operations not directly related to their current login session at the remote host, without terminating that login session. Such local operations are called "telnet commands", and to request a telnet command the user types an "escape character".

1.2.6 FTP (FILE TRANSFER PROGRAM)

The FTP program provides the capability of using a file system from several remote systems. The most important function of FTP is probably the ability to transfer files. As with telnet, the user must first provide userid and password information before access to the remote host is granted. After the login sequence, there is a number of FTP subcommands available. They can usually be listed on the screen by means of a help command. Besides copying files in either direction, the user can typically execute local commands, request session status or statistics, modify details about the presentation of file transfer information, request a listing of the files in the remote or local directories, and change the remote or local current directory.

1.2.7 ARP -- ADDRESS RESOLUTION PROTOCOL

ARP is a protocol that dynamically maps between Internet Addresses and burnt-in (or microcoded) 802.3 hardware addresses. These hardware addresses are unique for every adapter card (manufacturers agreed on

rules). ARP is not directly available to users. It allows to dynamically build mapping tables, and is an interface to the actual hardware. When a request for a mapping cannot be resolved from the cache, ARP sends the ARP request packet (broadcast) on the network requesting the address mapping. If a response is provided, a new mapping is cached.

1.2.8 UDP -- USER DATAGRAM PROTOCOL

UDP, like TCP, can be used to transmit a stream of data across the Ethernet, and uses IP services to handle the routing. Unlike TCP, however, UDP does not attempt to remedy any problems resulting from lost or damaged data. The packets are merely sent out, one by one, and the network connection is expected to be reliable enough so that the additional overhead of the TCP algorithms is not required. UDP and TCP are separate protocols, independent from each other; TCP does not depend on the existence of UDP for its operation.

1.2.9 TFTP -- TRIVIAL FILE TRANSFER PROGRAM

TFTP, in contrast to FTP, does not use the TCP protocol. It uses only UDP, and a smaller set of subcommands. TFTP does not require a login sequence, and performs file transfers without checking the access rights of users. For this reason, you will not find TFTP servers for VM.

1.2.10 SMTP -- SIMPLE MAIL TRANSFER PROTOCOL

As the name implies, SMTP is a protocol used for the transfer of electronic mail. Usually there is another user program available to allow one to edit a file and call SMTP in some convenient fashion, so that most people do not have to be familiar with the details of the protocol. There must be an SMTP server (SMTPD) on the destination site to enqueue the incoming mail. SMTP also uses the TCP/IP protocols.

1.3 TCP/IP FOR VM (5798-FAL)

Part of the software used for this project is IBM Transmission Control Protocol/Internet Protocol (TCP/IP) for VM (Program No. 5798-FAL) Version 1, Release 1.1.
TCP/IP (for VM) Release 1.0 was announced on April 21st, 1987 in the US as a PP and June 16th, 1987 in World Trade as a PO.

TCP/IP (for VM) Release 1.1 was announced in the US on December 15th, 1987, but is NOT released for World Trade so far.
TCP/IP (for VM) Release 1.1 is the first release which contains the IEEE 802.3 LAN subsystem support for the IBM 9370 Information System.

TCP/IP allows a VM user to interface with other systems that have implemented the TCP/IP protocols. A TCP/IP link enables a user to transfer files, send mail, and log on to a remote host in a network of homogeneous and heterogeneous systems. TCP/IP represents network layer three and four of the seven layer OSI/ISO reference model. Several lower levels are supported by TCP/IP for VM, which include IBM Token Ring, IEEE 802.3 LAN, ProNET [2] and DDN X.25 [3].

The actual TCP/IP protocols implemented in IBM TCP/IP for VM (5798-FAL) are:

TCP	Transmission Control Protocol (DARPA RFC 793)
IP	Internet Protocol (DARPA RFC 791)
ICMP	Internet Control Message Protocol (DARPA RFC 792)
FTP	File Transfer Protocol (DARPA RFC 959)
TELNET	TELNET protocol (DARPA RFC 854)
SMTP	Simple Mail Transfer Protocol (DARPA RFC 821)
TFTP	Trivial File Transfer Protocol (DARPA RFC 783)
UDP	User Datagram Protocol (DARPA RFC 768)
ARP	Address Resolution Protocol (DARPA RFC 826)

Some of these protocols provide the packaging and management of the data, that is, TCP, IP, ICMP and UDP. SMTP, TELNET and FTP are all protocols that are used by the CMS user. TFTP is a protocol that the CMS user would use to perform file transfer with another non-VM TCP/IP host that supported TFTP. These will be explained in more detail later in this book.

IBM's systems, which can participate in TCP/IP networks are the following:

- S/370
  This is supported with VM and TCP/IP (5798-FAL), no VSE, MVS or IX/370 support is available at this time.
  Just recently, AIX/370 has been announced (03/15/88) which includes TCP/IP support for 802.3 LANs, but will not be available before April, 1989.

- PC and PS
  This is announced as a special feature with TCP/IP for VM (5798-FAL). The PC provides client, but no server functions.

---

[2] ProNET is a Trademark of Proteon Inc.

[3] DDN X.25 is a Department of Defense X.25 Network

- 6150
  TCP/IP is part of the AIX operating system, no additional software is required.

Overview of TCP/IP for VM on the 9370 Information System

	TYPE OF ATTACHMENT				
Network Type	9370 6130/6035 802.3 LAN Ethernet	9370 6130/6034 802.5 Token Ring	9370 Channel Attached S/1	9370 Channel Attached 7170	9370 Channel Attached 8232
IEEE 802.3 LAN	yes (X)	no	no	yes	yes
802.5 Token Ring	no	yes	no	no	yes
DDN X.25 Network	no	no	yes	no	no
ProNET Network	no	no	no	yes	no

(X) This report deals only with the IEEE 802.3 LAN network in conjunction with the 9370 integrated IEEE 802.3 LAN controller/adapter (Feature 6130/6035).

Figure 7. Overview of TCP/IP Support on the IBM 9370 Information System

2.0 INSTALLATION OF 802.3 LAN ADAPTER

2.1 INSTALLATION OF CONTROLLER AND ADAPTER

Multiple IEEE 802.3 LAN subsystems per IBM 9370 Information System can be installed.

Before placing the controller and the adapter card into the 9370 I/O Unit Card, power off the system. Two adjacent slots must be used for the controller (Feature 6130) and its adapter (Feature 6035). The adapter sits to the right of the controller when seen from the back of the system.

2.2 INSTALLATION OF MICROCODE

Installing the microcode is not a very simple task and is broken down into several steps. Before you start with Step 1, power on the system. For better understanding you should have "9370 - Operating Your System, SA24-4036-02" available along with this document.

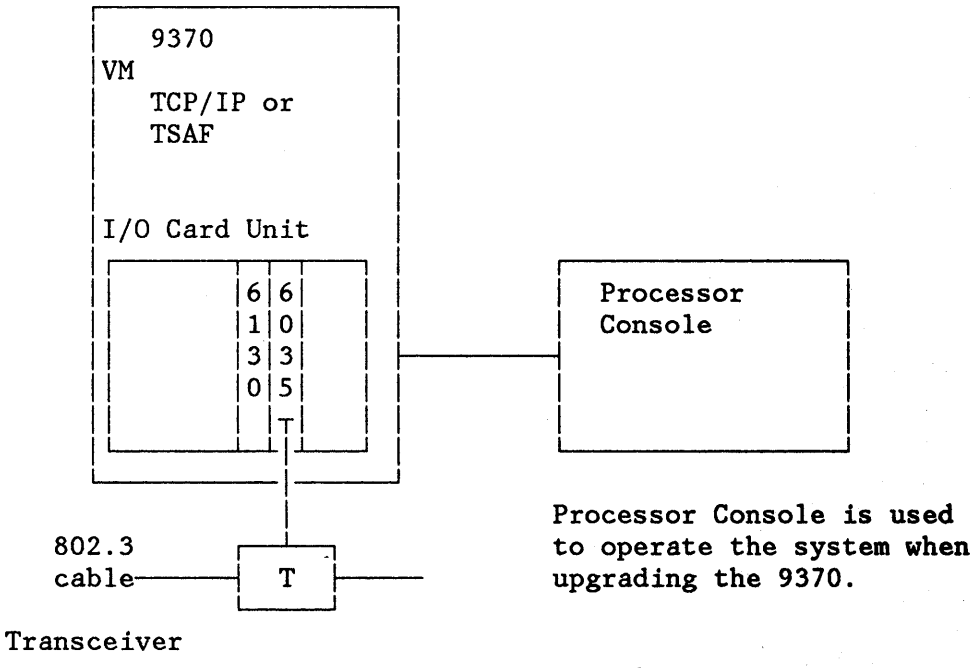

Figure 8. Installation of Microcode at 9370 Processor Console

2.2.1 STEP 1: ENTER MANUAL OPERATION AND MODE SELECTION

This Session Selection Screen is the first screen that appears when you power on the system, or when you press the Slct (Select) key.

Select option 1 (Manual Operation) to enter the User Options Screen, which is not shown here, and select option 2 (Mode Selection) before you proceed to step 2.

```
                    SESSION SELECTION SCREEN

  1  Manual Operation

  2  Work Station

  3  Remote




       Select: 1

F1=Help
```

Figure 9. Session Selection Panel

2.2.2 STEP 2: ENTER ADMINISTRATOR OPTIONS

Select option 2 to enter the administrator option menu. You may have to enter a password if customer password checking is enabled (set by customer during installation). The administrator option menu is the correct path to system upgrade functions.

```
                        MODE SELECTION

  1  General User

  2  System Administrator

  3  System Programmer

  4  Service




       Select: 2

F1=Help
```

Figure 10. Mode Selection Panel

2.2.3 STEP 3: ENTER CUSTOMER SETUP

Select option 7 to enter the Customer Setup menu which will give you the options of initial installation and system upgrade (not shown here). Select option 2 (System Upgrade).

```
                        ADMINISTRATOR OPTIONS

  1  General Information
  2  Mode Selection
  3  Program Load
  4  Enable the Time-of-Day Clock
  5  System Power off
  6  Configuration
  7  Customer Setup
  8  Problem Analysis
  9  Remote Operation



       Select: 7

F1=Help
```

Figure 11. Administrator Options Panel

2.2.4 STEP 3: PREPARE THE TOPOLOGY DISKETTE (BLUE DISKETTE)

The topology diskette is also called the "blue diskette", or "configuration diskette". It holds the configuration of your system. This is also kept in configuration records, which reside on the hard disk of the 9370 Processor Console.

Select option 1. This function writes the current internal configuration records onto a diskette, which is then your current configuration diskette. The new IEEE 802.3 LAN Subsystem must become part of your internal system configuration records. If IBM provides a new topology diskette with the delivery of the IEEE 802.3 LAN cards, then you can skip this step and continue with step 4.

Otherwise, you must write the current configuration records onto the diskette, give this diskette to the IBM representative, who must update it so that it contains the IEEE 802.3 LAN cards. In step 4, you will copy the configuration diskette (which now includes the IEEE 802.3 LAN hardware) back to the hard disk of the 9370 Processor Console.

Copying the current configuration records onto the diskette is described in more detail in "9370 - Operating Your System, SA24-4036-02", Chapter 4.

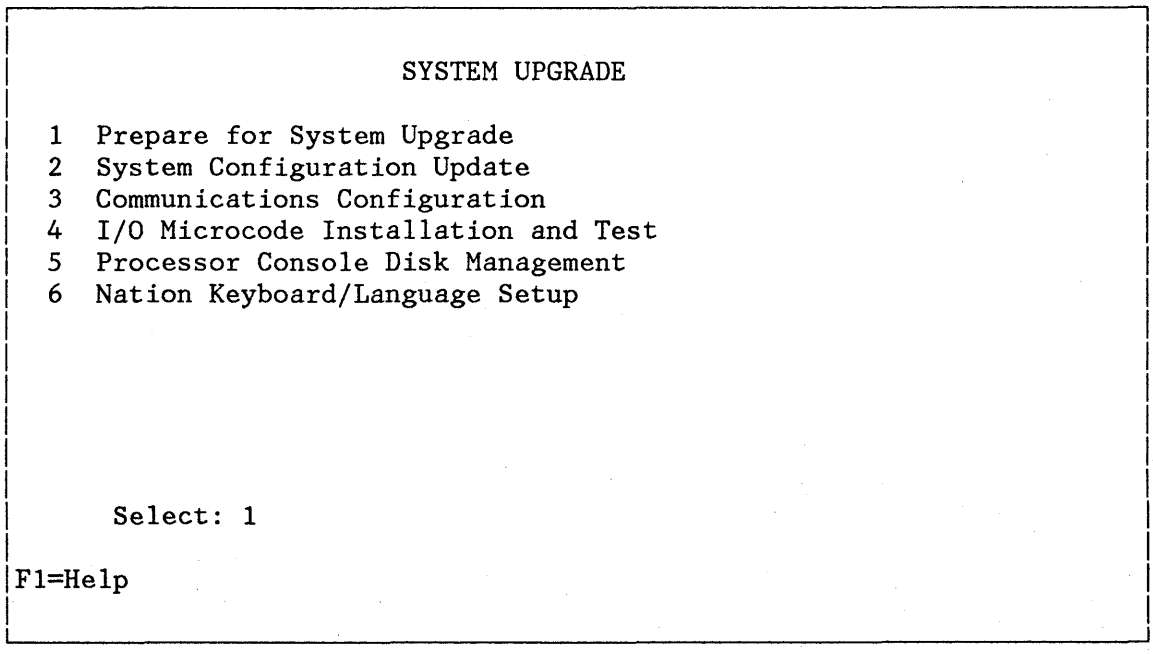

Figure 12. System Upgrade Panel

2.2.5 STEP 4: UPDATE THE CONFIGURATION RECORDS

This step copies the configuration diskette contents back to the hard disk of the 9370 Processor Console. As described in STEP 3 (Prepare the Topology diskette), your configuration diskette should now hold the new configuration information including the 802.3 LAN hardware.

To update the internal system configuration records, you should select option 2, which copies the system configuration information from the configuration diskette (topology diskette) to the system configuration records, which are located on the hard disk of the 9370 Processor Console. Use also the "9370 - Operating Your System, SA24-4036-02" manual, which describes this step in more detail.

When you have finished this step, you might want to use option 3 (Communication Configuration) to display and alter the Subsystem addresses. This function is however not provided here. The only Communication Subsystem you can display and alter from this menu (Communication Configuration) is the Telecommunication Subsystem, not the 802.3 LAN Subsystem. This will be done later, when we enter the menus as system programmer. Proceed to step 5.

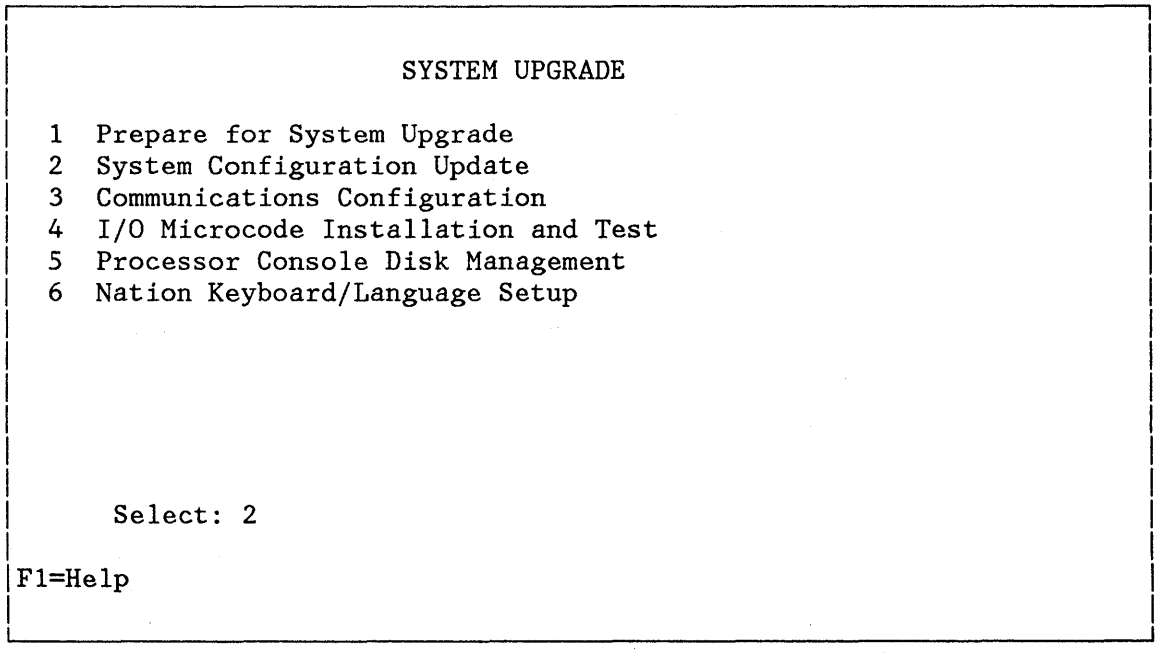

Figure 13. System Upgrade Panel

2.2.6 STEP 5: INSTALL THE IEEE 802.3 LAN MICROCODE

Select option 4. This step allows you to update the I/O controller microcode which resides on the System DASD (9332 or 9335). Since the IEEE 802.3 LAN microcode has to become part of it, you will have to load it from the diskettes. This process includes copying the microcode from the diskette to the system DASD microcode area (9332, or 9335). Use the "9370 - Operating Your System, SA24-4036-02" manual, pages 4-92 to 4-103 for a more detailed description of this step.

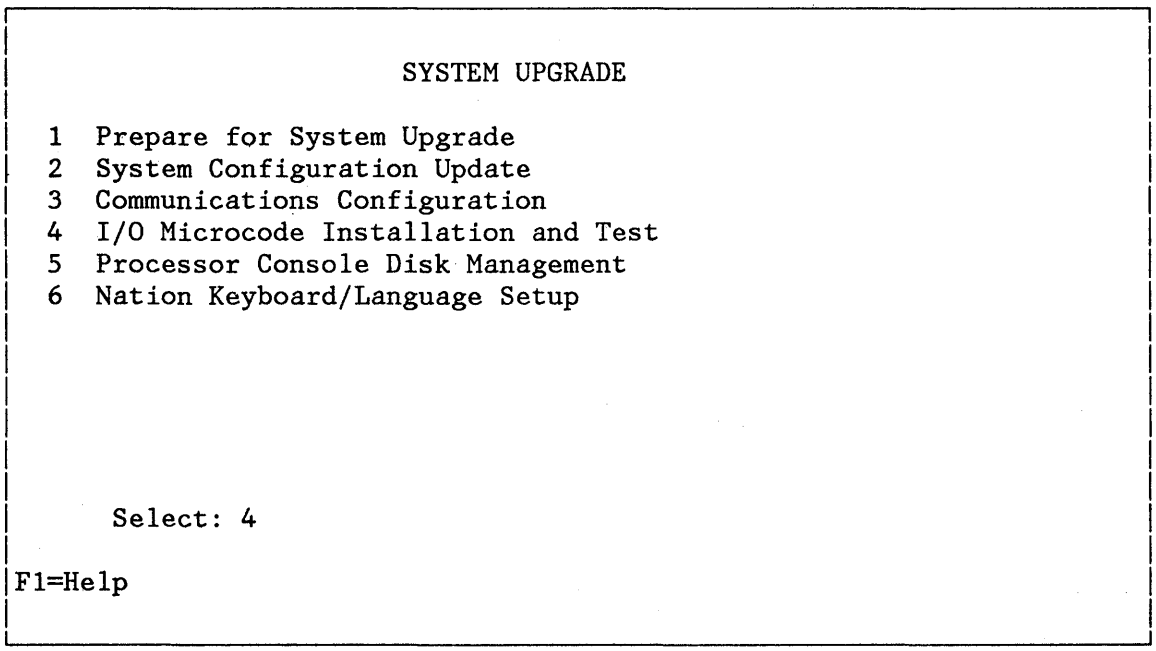

Figure 14. System Upgrade Panel

Type 1 next to the 6130-0020 line, which defines that you want to load microcode for the IEEE 802.3 LAN Subsystem. Several further screens will then lead you through the procedure to load the microcode for the IEEE 802.3 LAN Subsystem (refer to "9370 - Operating Your System, SA24-4036-02"). At the end of this procedure the microcode will be compressed and the system will reinitialize (several minutes), which means that the microcode is transferred from the hard disk of the 9370 Processor Console to the system DASD, and that the IOPs and IOAs are initialized.

```
                    I/O MICROCODE INSTALLATION AND TEST
Customer Setup

    The list shown below indicates the I/O Subsystems
    currently configured on your system.

    Indicate the I/O Subsystem for which you have microcode
    to install              1 = Yes
                            2 = No

    6030-0000 ......... 2
    6020-0000 ..........2
    6010-0000 ......... 2
    6003-0000 ..........2
    6130-0020 ..........1




          F2=MainMenu                                  F5=PrvMenu
```

Figure 15. I/O Microcode Installation Panel

2.2.7 STEP 6: BACKUP THE CURRENT CONFIGURATION

Select option 5. This will lead you to the DISK MANAGEMENT screen (not shown here), and use option 1 (Backup fixed disk). This step allows you to backup current configuration records on FUNCTIONAL1 diskette, which is needed when you want to restore the microcode to the 9370 Processor Console hard disk in case it fails.

```
                        SYSTEM UPGRADE

  1  Prepare for System Upgrade
  2  System Configuration Update
  3  Communications Configuration
  4  I/O Microcode Installation and Test
  5  Processor Console Disk Management
  6  Nation Keyboard/Language Setup




       Select: 5

F1=Help
```

Figure 16. System Upgrade Panel

2.3 CONFIGURATION DEFINITION

You have to define subchannel addresses to the IEEE 802.3 LAN Subsystem. Each CETI (Continuously Executing Transfer Interface) group requires four contiguous sub-channel addresses (range x'00' to x'F3'). They are used for the Control Port, Interrupt Port, Inbound Data Port, and the Outbound Data Port. One group of four subchannel addresses can be defined as a maximum to one IEEE 802.3 LAN Subsystem. Note, that this differs to the Token Ring Subsystem, which supports three CETI groups per subsystem.

The easiest way to do this is to enter the panels as System Programmer.

2.3.1 STEP 1: ENTER SYSTEM PROGRAMMER PANELS

After you have entered the Mode Selection screen, select option 3 to enter the System Programmer panels. A password, if set up, is required to perform this step.

```
                        MODE SELECTION

  1  General User

  2  System Administrator

  3  System Programmer

  4  Service




       Select: 3

F1=Help
```

Figure 17. Mode Selection Panel

2.3.2 STEP 2: ENTER NEXT CONFIGURATION MENU (QFI)

Select option QFI to enter the Next Configuration Menu. The NEXT I/O Configuration, which can be defined by the system programmer shows the configuration which will be active the next time you re-IML the system.

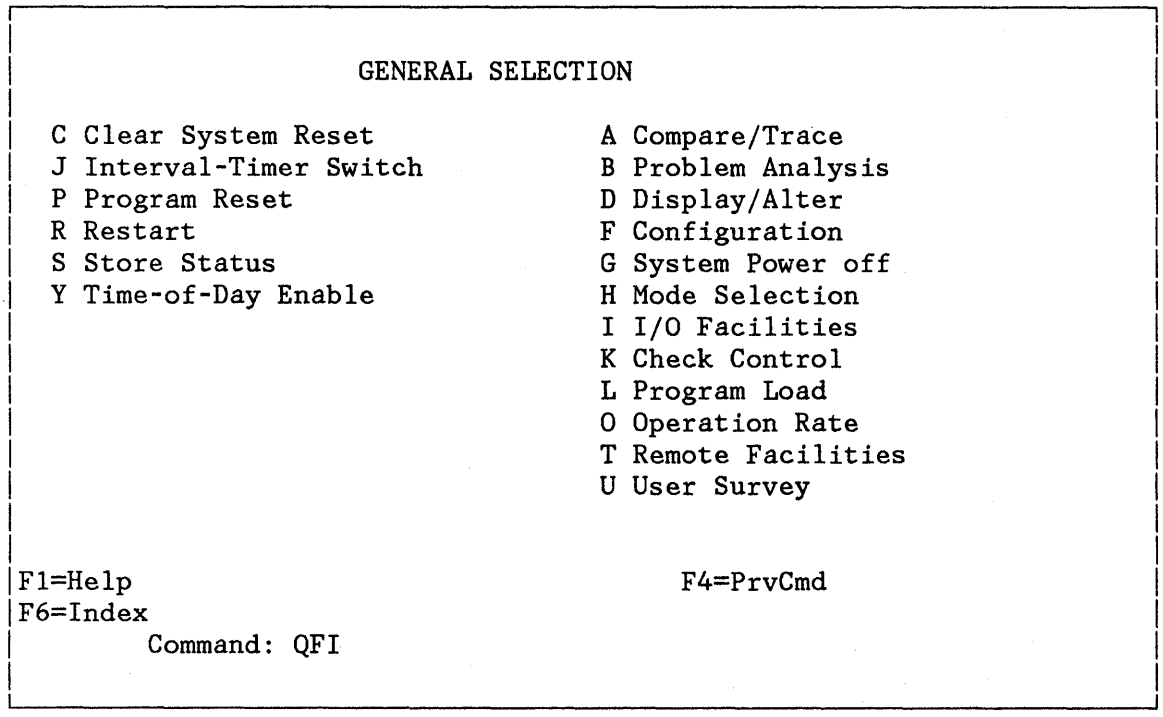

Figure 18. General Selection Panel

2.3.3 STEP 3: ENTER CHANNEL ADDRESS OF IEEE 802.3 LAN

Select the channel address of the IEEE 802.3 LAN Subsystem. You can recognize the correct channel address by looking at the I/O Feature column. The IEEE 802.3 LAN Subsystem shows the code 6130-0020. In my example it is Channel Address A.

```
Configuration                NEXT I/O

 Select an S/370 CHANNEL ADDRESS to display/alter I/O configuration

         S/370                          RACK
         CHANNEL       I/O                - UNIT
         ADDRESS       FEATURE                 - CARD

         0             6020             A  - 01A  - 18
         1             6020             A  - 01A  - 20
         5             6003             A  - 01A  - 13
         A             6130-0020        A  - 01A  - 27
         D             6010             A  - 01A  - 16


F1=Help     F2=MainMenu                      F4=PrvCmd     F5=PrvMenu
F6=Index                                                   F10=Alter
        Command: QFIA
```

Figure 19. NEXT I/O Panel

2.3.4 STEP 4: YOU MAY WANT TO CHANGE THE SUBCHANNEL ADDRESSES

Find your default subchannel address (should be 0 to 3) and decide if you want to keep them. If not, then press PF10, which allows you to change the first subchannel address. The remaining three addresses are assigned automatically in increasing order. Then press PF10 again to make the change permanent. The four sub-channel addresses have to be contiguous.

To enter a comment is optional and has no implications.

```
Configuration                        6130-0020
Next I/O                             Rack A Unit 01A  Card 27

   Enter the first four addresses

         S/370        I/O          CARD         COMMENT
         ADDRESS      FEATURE

         A00-A03      6035         28
          --                                   ---------------




F1=Help    F2=MainMenu                  F4=PrvCmd    F5=PrvMenu
F6=Index                                             F10=Alter
        Command: QFIA
```

Figure 20. NEXT I/O Panel, Display/Alter

2.3.5 STEP 5: RE-IML THE SYSTEM

The changes you make on the QFI screen will not be active until you re-IML the system. To re-IML, you may enter directly QL on the command line of the last screen and press enter.

2.4 TEST OF INSTALLATION

There are a number of diagnostic routines implemented to test the IEEE 802.3 LAN card and microcode.

Enter the QI Screen via the Service entry of the Mode Selection Panel. The service password defaults to SERVMODE, if it has not been changed by the service personnel.

2.4.1 TEST 1: LOOK AT THE DEVICE VPD

After you provide the channel address (A in my example) in the upper right corner of the QI screen, you may enter QIZ00FF and you will see a screen, which displays the vital product data (VPD) for the IEEE 802.3 LAN Subsystem. This is a method to find the burnt-in address of your IEEE 802.3 LAN Subsystem (LAN Address EEROS).

```
I/O Facility                        Device VPD Display
  Feature 6130-0020                      Channel Address: A

        Type Number          6035
        Model Number         001
        Load ID              A010 0000
        Serial Number        0000 0000
        Part Number          0000 058X 7978
        Manufacture ID       0000 0000
        LAN Address Actual   08-00-5A-A0-00-00
        LAN Address EEROS    08-00-5A-A0-00-00




          F2=MainMenu                    F4=PrvCmd    F5=PrvMenu

       Command: QIZ00FF
```

Figure 21. Display Device VPD Panel

2.4.2 TEST 2: VERIFICATION TEST

Select the Problem Analysis (QBGL) screen, and continue to select the options to reach the IEEE 802.3 LAN Subsystem tests. This is outlined in the following figures. Note the different style in making the selections, not on the Command Line but on the Select Line. On the last screen (Test Selection Panel 5), select option 1 - "Failure determination" to start the tests. A sequence of tests will be executed. They are summarized at the end of this chapter.

```
P1014                      PROBLEM ANALYSIS

  Select the Type of tests to be run and press Enter

   1 I/O Tests
   2 Other Tests




   Select: 1


F1=Help              F3=QUIT

       Command: QBGL
```

Figure 22. Test Selection Panel 1

```
P1009                    PROBLEM ANALYSIS

  Select the Type of Subsystem to be tested
  and press Enter

   1 DASD/TAPE Subsystem
   2 Communication Subsystem



   Select: 2


F1=Help              F3=QUIT                    F5=Return

       Command: QBGL
```

Figure 23. Test Selection Panel 2

```
P1012                    PROBLEM ANALYSIS

  Select the communication Subsystem to be tested
  and press Enter

   1 Telecommunication Subsystem
   2 ASCII Subsystem
   3 IBM Token Ring Subsystem
   4 IEEE 802.3 Local Area Network Subsystem



   Select: 4

F1=Help              F3=QUIT                    F5=Return

       Command: QBGL
```

Figure 24. Test Selection Panel 3

```
P3500          IEEE 802.3 LOCAL AREA NETWORK SUBSYSTEM
                      PROBLEM ANALYSIS

  Enter the S/370 Address

  Verify that this address is varied offline
  Vary online when finished

  S/370 Address . . . A00




F1=Help                F3=QUIT

       Command: QBGL
```

Figure 25. Test Selection Panel 4

```
P3520          IEEE 802.3 LOCAL AREA NETWORK SUBSYSTEM
                      PROBLEM ANALYSIS

  Select one of the following tests and press Enter

  1 Failure determination
  2 Hardware verification
  3 LAN configuration services
  4 Time domain reflectometry
  5 End


       Select: 1

F1=Help                F3=QUIT

       Command: QBGL
```

Figure 26. Test Selection Panel 5

The following is a brief description of the tests which are executed by the previously described method. You can also select single tests from this menu with the QBGZGT screen. Most meaningful for a quick check if the IEEE 802.3 LAN Subsystem is working is test 10.

1 IOA EEROS CRC Check: This test performs functional verification of the internal CRC (cyclic redundancy check) generation.

2 RAM Buffer Test: This test assures the proper operation of the RAM on the #6035 adapter card.

3 Register Addressability: This test assures the addressability of the registers on the #6035 adapter card (IOA).

4 Interrupt Test: This test assures the proper operation of the hardware that generates interrupts on the #6035 adapter card (IOA).

5 Controller Interface Test: This test assures the proper operation of the hardware that interfaces the Controller chip to the #6035 adapter card bus.

6 Internal Wrap Functional Test: This test performs functional verification of the internal wrap feature of the adapter hardware.

7 Internal CRC Functional Test: This test performs functional verification of the internal CRC (cyclic redundancy check) generation of the adapter hardware.

8 Internal Addressability Function: This test performs functional verification of the internal addressing capability of the adapter hardware. It is used to verify the address recognition circuitry of the Controller chip.

9 Operational Shared Access Test: This test performs functional verification of the circuits that implement the shared access to the adapter RAM.

10 External Wrap Functional Test: This test should be run with the card connected to the network or to the wrap connector. It performs verification of the external wrap capabilities of the adapter hardware.

11 External Functional Test: This test performs functional verification of the external transmit capability of the adapter hardware.

12 External CRC Functional Test: This test performs functional verification of the internal CRC generation circuits within the Controller chip while it is operating in the external wrap mode.

13 External Addressing Functional Test: This test performs functional verification of the external addressing capabilities of the Controller chip. It will send and receive frames using the different addressing modes of the chip.

14 Internal Disable Functional Test: This test performs functional verification of the various inhibit functions of the Controller chip.

15 Operational Buffer Error Handling Test: This tests the Controller's ability to process various error situations which may occur in the process of buffer handling.

16 Operational Error Handling Test: This tests the ability to process various error situations on the adapter card.

17 Error Detection Circuitry Test: This test assures the proper function of the error detection hardware on the adapter card.

18 Interface Error Test: This tests the Controller's ability to detect various errors which can occur when transmitting data.

It takes about 10 minutes to run all the tests. Contact the CE if the system returns Reference Codes for any of these tests.

3.1 DEFINING THE IEEE 802.3 LAN TO VM (DMKRIO)

The IEEE 802.3 LAN subsystem appears to VM as a 3088 which is just a placeholder for 64 addresses in this respect. This has the advantage that 3088 support already exists in VM/DMKRIO and no new support is required for the IEEE 802.3 LAN subsystem. Note that the entry would be different for a channel attached IBM 7170 which can also be used as an IEEE 802.3 LAN controller.

The DMKRIO entry is:

```
* these entries are for the integrated 802.3 subsystem
   RDEVICE ADDRESS=(A00,64),DEVTYPE=3088
   RCTLUNIT ADDRESS=A00,CUTYPE=3088,FEATURE=64-DEVICE
   RCHANNEL ADDRESS=A,CHTYPE=BLKMPXR
```

Figure 27. DMKRIO Entry for IEEE 802.3 LAN: This figure describes the entries required in the real I/O device description file (DMKRIO) to build the nucleus for VM.

In the example above, the start address is A00 (64 subsequent addresses are defined). CETI (Continously Executing Transfer Interface) which is used by the IEEE 802.3 LAN 9370 subsystem, uses only twelve (12) of these addresses. You may want to change the range of addresses used by the 9370 IEEE 802.3 LAN subsystem. This can be achieved using the 9370 customization panels (see "Step 4: You May Want to Change the Subchannel Addresses" on page 25).

3.2 INSTALLING TCP/IP FOR VM

This document refers to the installation of TCP/IP (for VM) Version 1, Release 1.1 using a product tape. TCP/IP will be available in VM/IS Release 5.1.

The full description of installation of TCP/IP (for VM) Version 1 Release 1.1 is in "IBM TCP/IP for VM Installation and Maintenance Manual, GC09-1203".

3.2.1 VM DIRECTORY ENTRIES

Before loading the tape, it is necessary to create VM directory entries for the virtual machines used by TCP/IP ("Appendix A. Directory Entries for TCP/IP Virtual Machines" on page 55). The virtual machines are:

TCPIP used by all the other machines, and provides the TCP/UDP/IP communication services as well as the TELNET server (prerequisite for other clients to log into this machine).

TCPMAINT used for installation and maintenance of the TCP/IP services. TCPMAINT owns minidisks 191 and 592 (user visible minidisk), which hold the code for operating TCP/IP services. Minidisks 2C0 and 5C3 are merely used for source and text decks and are not mandatory for operation of TCP/IP on the system.

SMTP handles mail to and from TCP/IP users whether originating from or destined for users on the TCP/IP or RSCS networks. SMTP owns minidisk 191, which holds the code for operating mail.

FTPSERVE provides controlled access to files by other TCP/IP users. FTPSERVE owns minidisk 191, which holds the code for the FTP server services, and which is seen as 594 H from TCPMAINT.

NAMESRV provides a network service to enable clients to name resources or objects and share this information with other objects in the network. The use of an SQL data base for maintaining the name information is optional, but if used, requires access to REXSQL and SQLDBA.

3.2.1.1 Disk Space Requirements

These machines will require disk space of approximately 50 MB. This includes source code and might be reduced to approximately 17 MB without source and text decks. Space for mail to be stored on SMTP is required in addition. All mail that SMTP handles, stays on its 191 disk until forwarded, so the size of this additional space requires careful consideration. For performance reasons, it may be advisable to define multiple FTP machines, which will also increase disk space requirements.

```
TCPMAINT
     191    3 Megabyte
     592    8 Megabyte
     2C0   14 Megabyte (optional for source/text decks)
     5C3   14 Megabyte (optional for source/text decks)

TCPIP
     191  2.4 Megabyte (593 from TCPMAINT)

FTPSERVE
     191    1 Megabyte (594 from TCPMAINT)

SMTP
     191  0.5 Megabyte (plus space for mail)
                       (595 from TCPMAINT)
NAMESRV
     191  1.5 Megabyte (596 from TCPMAINT)
```

Figure 28. Minidisk Space Requirements

3.2.2 LOAD THE FILES FROM TAPE

All the work is done from the TCPMAINT's userid, which has access to all other disks used by the five virtual machines. This is not difficult and is well explained in Chapter 3 of "IBM TCP/IP for VM Installation and Maintenance Manual, GC09-1203".

The standard tape is supplied in VMFPLC2 format. An installation EXEC and MEMO are provided in addition to the installation instructions ("IBM TCP/IP for VM Installation and Maintenance Manual, GC09-1203").

Before installion it is worthwhile reading the manual and MEMO and making a plan for the contents of the various tables and control files that will be altered during installation.

3.2.3 SOME TIPS FOR INSTALLING TCP/IP

Listed here are some changes that may not be obvious from the distributed documentation, but have been found to be helpful when installing IBM TCP/IP for VM (5798-FAL).

One problem, which has been a trap in some installations is the following: During installation, TCPMAINT wants all minidisks in write mode. To release them from this situation, all userids (TCPMAINT, TCPIP, FTPSERVE, SMTP, and NAMESRV) should be logged off after installation is completed. Then, TCPMAINT will access the minidisks in read mode.

Once TCP/IP is up and running, you may want to tailor it to meet specific requirements.

3.2.3.1 TCPIP's PROFILE EXEC File

This EXEC should be modified to reflect the addresses of the IEEE 802.3 LAN. You will have the option to automatically open an XEDIT session to make changes in this file during the installation procedure.

```
/*********************************************************************************/
/*                                                                               */
/* The PROFILE EXEC should go on TCPIP 191 minidisk                              */
/*                                                                               */
/*********************************************************************************/
  owner = 'TCPMAINT'                  /* TCP/IP system administrator  */
  "ACCESS 592 B"                      /* TCP/IP user-visible minidisk */
  "CP VARY ON A00-A03"                /* 802.3 Subsystem configured   */
  "CP ATTACH  A00-A03 *"              /* at addresses A00 to A03      */

  "CP SET QDROP TCPIP OFF USERS"      /* For improved performance     */
  "CP SET FAVOR TCPIP"
  "CP SET FAVOR TCPIP 100"

  "SET LDRTBLS 8"                     /*                              */
  "CP SPOOL CONSOLE START TO" owner   /*                              */
  "IDENTIFY"                          /*                              */

  "TCPIP"                             /*                              */

  "CP SPOOL CONSOLE STOP"             /*                              */
  "CP SPOOL CONSOLE CLOSE"            /*                              */
  EXIT
```

Figure 29. TCPIP's PROFILE EXEC

3.2.3.2 TCPIP's PROFILE TCPIP File

This file is also called the configuration file for TCP/IP and again you have the option to invoke an EXIT session during the installation procedure.

Later on, when you have a running system, you may hand over to TCPIP a new configuration file by issuing the OBEYFILE command (see also the OBEY parameter).

Comment out all DEVICE, LINK and START statements for hardware which does not exist on the 9370 being used. Also, comment out entries in the HOME and GATEWAY sections for devices not present on the system. We experienced, that if entries are left in this file which refer to network elements that are not existing, it is possible that the TCP/IP system will not start up.

If you are only using the 9370 integrated IEEE 802.3 LAN subsystem, the entries you will need for DEVICE, LINK, HOME, GATEWAY, and START are in Figure 30.

```
NOTRACE SCREEN

INFORM OPERATOR TCPMAINT
OBEY   OPERATOR TCPMAINT

DEVICE ELANS1 ELANS  A00
LINK ETH1 ETHERNET 1 ELANS1

AUTOLOG
   FTPSERVE  passwd
   SMTP      passwd

PORT
   21 TCP FTPSERVE
   23 TCP INTCLIENT
   25 TCP SMTP

HOME
* Local host's Internet addresses
   193.1.8.22     ETH1

GATEWAY
* Network First-hop link-name max-Pack-size Subn.-mask Subn.-value
* Direct routes
  193.1.8     =      ETH1     1500         0

START ELANS1
```

Figure 30. TCPIP's PROFILE TCPIP: The figure shows some of the entries in the file PROFILE TCPIP on TCPIP's 191 minidisk, which we used to operate the integrated 802.3 LAN subsystem on the 9370.

The DEFAULTNET parameter may be erased, or otherwise changed to use the IEEE 802.3 LAN.

Other parameters that may need alteration in the initial setup of TCP/IP are the passwords for autologging the TCP/IP machines, and the ids used for INFORM (user-ids to be informed in case of serious runtime problems) and OBEY (user-ids, whose requests are obeyed). The Internet addresses may require alteration to conform to the standards of the TCP/IP network that is being connected to.

There is a number of other parameters which can be specified in the PROFILE TCPIP file. These are described in "IBM TCP/IP for VM Installation and Maintenance Manual, GC09-1203", Chapter 5.

3.2.3.3 TCPIP's PROFILE CLIENT file

The file resides on TCPMAINT's 592 minidisk. This should just contain TCPIP in the third line of the file, the first two being blank. It may be modified later if required for multiple TCPIP machines or if using name-servers.

```
********** top of file **********************************************************

TCPIP
********** end of file ************************************************************
```

Figure 31. TCPIP's PROFILE CLIENT: The figure shows the file PROFILE CLIENT, which contains host information for TCP/IP client programs.

3.2.3.4 TCPMAINT'S HOSTS LOCAL File

The file HOSTS LOCAL resides on TCPMAINT's 191 minidisk. The file allows the assignation of names to Internet addresses as a name is much easier to remember than the Internet address. It will be necessary to decrease the distributed sample file, since it includes all the Internet addresses of the entire DOD network. This is too large to process with the given disk space for TCPMAINT. You probably want to code one, which reflects your TCP/IP network. For more information refer to "IBM TCP/IP for VM Installation and Maintenance Manual, GC09-1203", Chapter 4.

```
;
;
;802.3 Nets
;
HOST : 192.1.8     : DEPT01  ::::
HOST : 192.1.9     : DEPT02  ::::
;
;
;802.3 Net Segment 1
;
HOST : 192.1.8.1   : SYSTEM1 ::::
HOST : 192.1.8.2   : SYSTEM2 ::::
HOST : 192.1.8.3   : SYSTEM3 ::::
;
;802.3 Net Segment 2
;
HOST : 192.1.9.1   : SYSTEMA ::::
HOST : 192.1.9.2   : SYSTEMB ::::
HOST : 192.1.9.3   : SYSTEMC ::::
```

Figure 32. TCPMAINT's HOSTS LOCAL: The figure shows the HOSTS LOCAL file, which lists the internet addresses of all nodes participating in a sample network.

Once this is done, MAKESITE EXEC is run to create the file HOSTS ADDRINFO and HOSTS SITEINFO. These files need to reside on the user-visible mini-disk, which is generally accessed as TCPMAINT's F disk (address 592). Make sure that the output is written to this minidisk by specifying the file mode as MAKESITE, or by using the CMS COPYFILE command. Write access to the F-disk will be required.

You may also run TESTSITE to test the correctness of HOSTS SITEINFO.

3.2.3.5 SMTP's SMTP CONFIG File

This file is on the A disk (address 191) of the userid SMTP. It is intended to be a configuration file for SMTP.

Comment out the RESOLVER statement by inserting a semi-colon in column 1, unless you are using a resolver. A resolver is used when a Name Server is used.

```
;
;
PORT 25           ;port to accept incoming mail on
OWNER TCPMAINT    ;where undeliverable mail is spooled to
INACTIVE 180      ;seconds
RETRYAGE 3        ;days
RETRYINT 20       ;minutes
RESOLVER          ;use the resolver and domain name server
GATEWAY           ;accept mail from and deliver mail to RSCS hosts
RSCSDOMAIN VNET   ;pseudo domain name of the associated RSCS network
;
```

Figure 33. SMTP's Configuration File: The figure shows the SMTP CONFIG file, which holds the SMTP configuration parameters.

The configuration file (SMTP CONFIG) will be defined by a parameter in the SMTP's PROFILE EXEC. Change this parameter to the name used for the configuration file.

3.2.3.6 TCPMAINT's CMRESOL DATA File

This file is found on TCPMAINT's 592 minidisk.

The resolver obtains its configuration parameters from a file named CMRESOL sysid * (default is CMRESOL DATA *).

The NSinterAddr defines the internet address of the Name Server. Comment out the NSinterAddr statement unless you are using a Name Server.

3.2.3.7 Other Tailoring

All the hints above are intended to highlight the less obvious changes that may be needed to achieve a working TCP/IP system. However, these are only some of the steps in creating a full working system, and you must use the manual "IBM TCP/IP for VM Installation and Maintenance Manual, GC09-1203" to achieve a complete installation.

3.2.4 TESTING TCP/IP

3.2.4.1 Bringup and Verification EXEC

The first step is to bring up TCP/IP successfully. A verification EXEC is provided, V5798FAL EXEC, and documented in the manual "IBM TCP/IP for VM Installation and Maintenance Manual, GC09-1203", Chapter 3-2. The EXEC is executed automatically during installation and performs various tests on the components of the TCP/IP system.

The verification EXEC is executed from TCPMAINT, but can be called from another userid, if privilege class B and link authority to all TCP/IP minidisks (see list of minidisks in Figure 28 on page 35) is provided.

3.2.4.2 LOOPBACK - TCP/IP Installation Test without Adapter

TCP/IP for VM provides a facility called LOOPBACK which does not require any 802.3 LAN subsystem hardware at all. It is possible to test the code alone by using LOOPBACK. 'TCPIP Loopback' should work properly before proceeding to the next step.

3.2.4.3 Testing the Local LAN Attachment

One method of doing this is to communicate via the 802.3 LAN subsystem of the 9370 to yourself, using your own Internet address when sending requests. Using the local host's Internet address will cause all TCP/IP communications to be made via the LAN Subsystem and back again. If it fails, then the local host's TCPIP configuration has an error.

In the testing phase, it is easier when the ids TCPIP and TCPMAINT are logged on to terminals close to one another.

Should TCP/IP fail to come up successfully, the console log of TCPIP will generally show the reason.

4.0 OPERATIONAL CONSIDERATIONS

TCP/IP is a set of protocols that will allow communication between systems in a homogeneous or heterogeneous network (systems with different architectures). IBM TCP/IP for VM (5798-FAL) implements a number of these protocols, and offers the VM user the possibility to connect to other systems which also have a TCP/IP implementation. The major facilities are:

- FTP - File transfer between hosts
- SMTP - Mail
- TELNET - Log on to a remote host

There is also a programmer's interface for the user to call the services from his own programs.

This chapter will give you an overview of these three facilities when they are used with the 9370 integrated 802.3 LAN subsystem.

4.1 FACILITIES OF IBM TCP/IP FOR VM (5798-FAL)

4.1.1 TELNET

TELNET provides a user with the facility to log in to other hosts on the TCP/IP network. The user must satisfy the remote host's requirements for account and password information.

4.1.1.1 Using the TELNET Command

To use TELNET, the following command is used:

```
TELNET [foreignhost [portnumber]] [(LINEMODE]
```

It is possible to just enter 'TELNET' and be prompted for the input. The use of the TELNET command is fully documented in Chapter 4 of "IBM TCP/IP for VM, Command Reference, GC09-1204-00". The user may choose to run TRANSPARENT (default) or LINE mode, where TRANSPARENT mode only makes sense, if you are TELNET'ing to another VM system.

Terminal	LINEMODE?	Remote Host	3270 Data-Stream?
3270	NO (1)	VM	YES
3270	YES	VM	NO
3270	YES (2)	non-VM	NO
non-3270	YES (2)	VM	NO
non-3270	YES (2)	non-VM	NO

(1) The default
(2) LINEMODE is compulsory in this environment.

Figure 34. Transparent and Linemode: The figure shows in what instances transparent mode allows full screen operations.

Figure 34 assumes that the terminal, which issues the TELNET command, is attached to a VM TCP/IP system.

Once logged in to the remote TCP/IP host, it is possible to issue TELNET subcommands which allow the user to do various things, for example query the connection, abort output, quit the TELNET session, which are discussed in "TELNET Subcommands and PF Keys" on page 46.

Various PF keys have special meaning when using TELNET. These are:

PA1 Transparent Mode only - invokes a Telnet subcommand
PF4 PF12 Get the program's attention
PF1 PF13 Retrieve the previous line
PF2 PF14 Scroll screen half-way up
PF3 PF15 Data entered by user is zero-brightness, which may be used when entering a password

4.1.1.2 Transparent Mode

This is a special facility of IBM TCP/IP for VM (5798-FAL) to allow 3270 data streams for TELNET sessions. If the terminal that issues the TELNET in CMS command looks like a 3270 and the LINEMODE parameter is not specified, and the host that is being TELNETed to is also a VM TCP/IP host, then the terminal session will be a 3270 session, with all the full-screen facilities of the 3270.

If the user is in Transparent Mode, the screen will clear to display some information about TELNET with MORE..... at the bottom. Once the screen is cleared the VM logo of the remote VM TCP/IP host will be displayed and logon may proceed as if the user were a locally attached 3270 to that remote VM TCP/IP host.

Transparent Mode is attractive to the VM user wishing to logon to another VM TCP/IP system, as all full-screen functions will be supported, for example PROFS, XEDIT, ISPF. 3270 extended data-stream is supported but not Programmed Symbols.

In Transparent Mode, your terminal is seen as a 3270 to the remote VM TCP/IP host. A number of 3270 models are supported, the default being 3278 model 2.

```
3275 Model 2
3276 Models 2, 3 and 4
3277 Model 2
3278 Models 2, 3, 4 and 5
3279 Model 2 and 3
```

Figure 35. 3270 Terminals Supported by TELNET

In addition to being able to use full-screen facilities, it is also possible to use VM Pass-Through (via DIAL or the PASSTHRU EXEC) to access VM hosts participating in the VM network, or to DIAL VTAM to access an SNA network or to use DIAL to access a guest operating system. This is possible ONLY in Transparent Mode.

As shown in "TELNET Subcommands and PF Keys" on page 46, pressing PA1 while in Transparent Mode will not have the usual results, but will put the user in the TELNET subcommand environment. One of these subcommands is to enter the characters "PA1" and the PA1 attention will result.

The most common use of PA1 (apart from needing to get to CP) is to terminate a PASSTHRU session, where the PASSTHRU EXEC has been invoked with no parameters.

4.1.1.3 Line Mode

In Line Mode, the terminal looks like a Heath H19 terminal which is a line-mode start-stop TTY terminal. Any screen that uses TELNET from CMS and is not seen as a 3270 by VM, will be forced to use Line Mode when using TELNET. This means that output to the terminal is displayed line by line, and there are no 3270 full-screen capabilities.

PF3 or PF15 should be pressed before entering the password to prevent it being displayed on the screen.

Data is transmitted every time Enter or a PA key is pressed, except for PF keys 1, 2, 3, 4, 12, 13, 14, and 15 which all have special meanings. Any other PF key in Line Mode will allow TELNET subcommands to be entered.

If using Line Mode to a non-VM host there are some characters which may be required which are not present on a 3270 keyboard, for example, the control character. This is represented by a cent sign or a grave accent. For example, if you want to enter CTRL-P, you type ¢P instead. Other control characters are documented in the "IBM TCP/IP for VM, Command Reference, GC09-1204-00", Page 4-4.

Although it is possible to present a number of special characters when logging in to a non-VM TCP/IP host, it may not be possible to provide all the characters, or data-stream that a screen natively attached to the foreign system could provide. If this is the case, the use of the foreign system from a 3270 terminal may be limited.

4.1.1.4 TELNET Subcommands and PF Keys

To use a TELNET subcommand, press:

PA1 in Transparent Mode
Any PF key except PF1, 2, 3, 12 or 13, 14, 15 in Line Mode

The full list of subcommands is given in the "IBM TCP/IP for VM, Command Reference, GC09-1204-00" Page 4-2, but some are summarized here.

AO	Abort Output
AYT	Are You There. Query existence of the connection.
Help or ?	Receive assistance
IP	Interrupt Process
PA1	Sends a PA1 to host. See "Transparent Mode" on page 44
QUIT	Quit the TELNET session. If TELNETed to VM, your remote id will be disconnected, not logged off.
SYNCH	Clear data path to remote site apart from TELNETcommands.

4.1.1.5 Coming from a Non-VM Remote Machine

If you are using the TELNET command on a remote machine, which is not a VM TCP/IP system, and try to log into the IBM VM system, the transparent mode is not supported with VM TCP/IP. This means, that there is a severe limitation in the usage of popular VM programs, such as XEDIT, PROFS, and many others, since these programs require full screen mode.

Software companies provide additional software which claims to support a full-screen mode from non-VM hosts to VM hosts. The announcement of TCP/IP (for VM) Release 1.1 mentions that this support is provided by SIM3278/TCPIP [4], but IBM does not guarantee any of these functions with its TCP/IP (for VM) FAL-5798.

The IBM 6150 (PC/RT) with the AIX operating system is an exception. It is a non-VM TCP/IP implementation, but requires no additional software to support the full-screen mode for VM applications from the IBM 6150.

4.1.2 SIMPLE MAIL TRANSFER PROTOCOL - SMTP

A full description of this facility may be found in Chapter 6 of "IBM TCP/IP for VM, Command Reference, GC09-1204-00".

SMTP allows the transfer of mail reliably and efficiently across different environments and networks.

The SMTP implementation in VM allows a CMS user to use Note and Sendfile, or PROFS to send mail or files to users on other TCP/IP hosts.

IBM TCP/IP for VM (5798-FAL) provides modified versions of the CMS EXECs Note and Sendfile. There is also an interface for PROFS users to send mail to users on remote TCP/IP hosts. More detail about SMTP commands and the systems programmer's interface to SMTP is also documented in the "IBM TCP/IP for VM, Programmer's Manual, GC09-1206-00".

4.1.2.1 SMTP and Notes

If the Note command is used, it is possible to specify the destination address (nodeid and userid) of the TCP/IP network recipient. One copy of the note is sent to the virtual machine SMTP, which attempts to deliver it to the recipient on the TCP/IP network. The mail is delivered whenever the destination TCP/IP host becomes available. If the destination TCP/IP host is not available, SMTP (by default) attempts to deliver every 20 minutes until three days has passed, when a non-delivery note is sent to the originator. The frequency of retry (RETRYINT) and the total length of time for retries (RETRYAGE) may be set to suit the user (see SMTP CONFIG definition in "SMTP's SMTP CONFIG File" on page 39). SMTP can act as a mail gateway between the RSCS and TCP/IP networks.

---

[4] SIM3278/TCPIP is a trademark of SIMWARE Corp.

4.1.2.2 Sending Mail from PROFS to the TCP/IP Network

The PROFS user will need to know that the recipient of a note is on the TCP/IP network. The note will need to be addressed to the SMTP virtual machine, either directly, or by use of .ad or .cc., and not directly to the TCP/IP user's host name and userid. Within the note, the TCP/IP user's host and userid is placed after ".ddn" in the body of the note starting in column 1. PROFS itself does not recognise .ddn - it is the SMTP machine which reads this for the addressee information for the TCP/IP network. As PROFS does not recognise .ddn, it is considered as normal text if, for example, the FORMAT PF key is pressed. This could result in .ddn starting other than in column one, and text which is not addressed being concatenated to the end of the line.

Mail from a user arriving at PROFS via TCP/IP will be delivered to the reader by SMTP, so the sender is SMTP. If the PROFS user uses the REPLY function of PROFS, the reply will merely go to SMTP and not the true sender, so FORWARD should be used, or a new note. Similarly, acknowledgement (.ak) will only show that SMTP has processed a note and not the real recipient.

PROFS nicknames for users on TCP/IP hosts are not supported.

4.1.2.3 Sending Files with SMTP Instead of FTP

SMTP may be used to send files to a remote TCP/IP. It is however limited to text files. Transparent code will not be transferred properly, since ASCII - EBCDIC translation, blank compression and TCP/IP header imbedding are involved. One advantage of using SMTP, is that the destination TCP/IP host does not have to be reachable at the time of sending the file, and SMTP will ensure the file is sent, or otherwise advise the sender that delivery has been impossible after the RETRYAGE has expired. By contrast, to use FTP, both TCP/IP hosts must be available and the remote userid and password known.

4.1.2.4 Receiving Mail and Files from SMTP

For the VM user, mail and files which have arrived via the TCP/IP network are placed in the user's virtual reader and may be processed as usual with RDRLIST, PEEK and RECEIVE. The sender is the SMTP virtual machine.

4.1.2.5 Nicknames

The NAMES file may be used. Non-VM systems may have host names and userids that are longer than eight characters and be in mixed case. The "List of Names" may be used for such addresses.

4.1.2.6 Mail with RSCS and SMTP

The following two figures (Figure 36 on page 50, and Figure 37 on page 51) give an overview of possible mail channels between TCP/IP network users and RSCS network users.

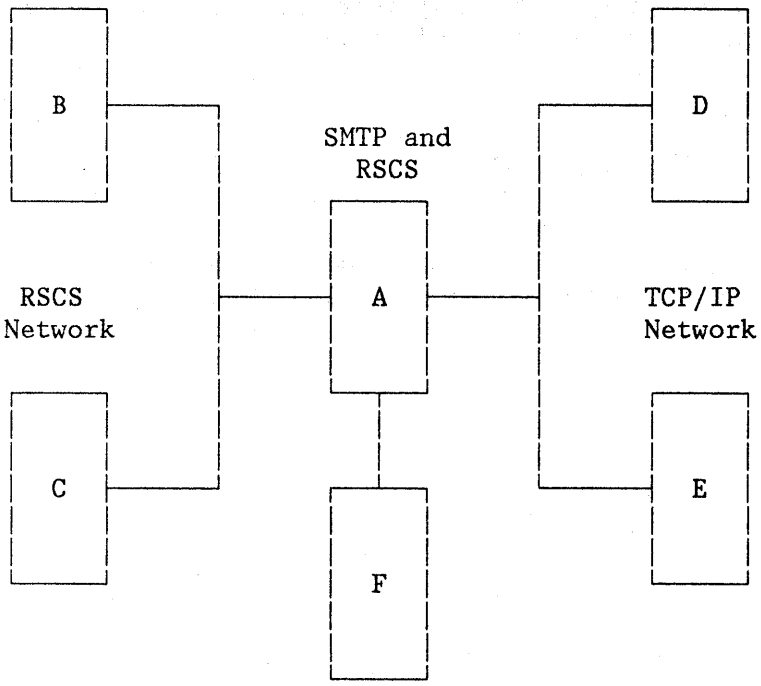

Figure 36. Example of a Mail Gateway: This figure shows a network, where the right section is a TCP/IP network and the left section is an RSCS network.

Sender's System	Receiver's System	Address to:	Transport
A	B	userB at rscsB	RSCS
PROFS A	B	rscsB(userB)	RSCS
D	A	userA@tcpA	SMTP
D	PROFS A	userA@tcpA	SMTP
PROFS user at A	D	address to SMTP .ddn tcpD(userD) in body of note	SMTP
D	B	userB%rscsB@tcpA	SMTP to RSCS
D	E	userE@tcpE No use of tcpA as a gateway	SMTP to SMTP
D	E	userE@tcpA tcpA being used as a gateway	SMTP to SMTP SMTP
A	F	userF at systemF System names are same for RSCS and TCP/IP hosts	RSCS is default
A	F	userF at tcpF userF at rscsF System names not same for RSCS and TCP/IP hosts	SMTP RSCS

Figure 37. Summary of Addressing for Electronic Mail Gateway

A to B User A and user B are members of an RSCS network. Nothing exceptional has to be considered.

A to B User A is a PROFS user, and user B is a standard CMS user. Mail is addressed following standard IBM rules.

D to A User D is located in the TCP/IP network, user A is also a member of the TCP/IP network. SMTP rules apply to forward the mail, with tcpA being the hostname of System A, as defined in a HOSTS LOCAL file.

D to A User D is located in the TCP/IP network, user A is also a member of the TCP/IP network, but is a PROFS user. User A, therefore, sees SMTP of his system as the sender of mail, and cannot use

functions such as REPLY to return to sender. Also, an acknowledgement would not return to user D.

A to D User A is a PROFS user, user D is a member of the TCP/IP network. The target address has to be defined with .ddn tcpD(userD) in the body of the note, where tcpD stands for the host site name of system D.

D to B User B is a member of the RSCS network, and user D is a member of the TCP/IP network. System A is needed to function as a gateway between these users. User D uses an address of the form user%rscsB@tcpA, where "user" is the userid of the user on system B, "rscsB" is the node name of the RSCS Host system B, and "tcpA" is the host site name (see HOSTS LOCAL) of the gateway host system A.

D to E User D and user E are members of the TCP/IP network. All rules are defined by standard forms of SMTP.

A to F User A and user F are members of the RSCS network. All rules are defined by standard forms of RSCS mail.

A to F User F is a member of the RSCS network, and user A is member of the TCP/IP network. Mail is delivered via RSCS to system A and handed to SMTP, which forwards mail to user A.

4.1.3 USE OF FILE TRANSFER PROTOCOL - FTP

FTP is fully described in Chapter 2 of the "IBM TCP/IP for VM, Command Reference, GC09-1204-00".

FTP allows the bi-directional transfer of files to any other host on the TCP/IP network that has an FTP server function. To use the function, it is necessary to provide whatever account information is required by the remote host, for example userid and password. In addition it may be necessary to give password information in order to gain access to files on the remote system. Although this appears, in many respects, like a login to the remote TCP/IP host userid, it is not. The FTP server at the remote host will access the remote TCP/IP host's file system, not the remote userid specified. The facilities available to be used at the remote host are limited to the functions of FTP, and are not the same as a terminal session.

To use FTP, the remote host needs to be available and accessible via the TCP/IP network. If files are only to be sent, Sendfile might be an alternative instead of FTP (see "Simple Mail Transfer Protocol - SMTP" on page 47) if the connection is not readily available.

The format of the FTP command is:

```
FTP [foreignhost [portnumber]] [(TRACE]
```

In general use, only the foreignhost parameter will be used. If it is not entered, then the user is prompted. In this way, host addresses longer than eight characters may be entered.

File transfer may take place between VM and VM or ASCII hosts. Both EBCDIC and ASCII are supported.

Many FTP subcommands are provided to control the FTP session such as account information, listing files, GET and PUT for files, DELETE, type of representation, mode of data, and so on.

During the use of FTP, the VM user can issue CMS commands using the CMS subcommand, which could include full-screen functions such as FILELIST. The FTP session is not full-screen, and appears as a basic CMS terminal session.

It may be possible for a terminal user to log onto the remote userid at the same time that FTP is being used. In the VM environment, the terminal user logging on to the remote userid will see that a disk to which they have access is being linked to by the FTPSERVE virtual machine, in whichever read/write mode the FTP user was able to specify. The normal restrictions will apply, for example, if the FTP user has established WRITE access to a disk that is not multi-write, the terminal user logged on to the remote id will only be allowed read access.

4.1.4 TRIVIAL FILE TRANSFER PROTOCOL - TFTP

This is a file transfer protocol that, unlike FTP requires no authentication at the remote host, that is, passwords. Using TFTP, all that is required is the knowledge of the userid and the name of any file to be copied from there.

TFTP offers little security, so is not fully implemented in IBM TCP/IP for VM (5798-FAL). The TFTP User function is provided but there is no TFTP Server Function. It is possible to use it FROM the VM TCP/IP system to another TCP/IP host (non-VM) that has a TFTP Server.

APPENDIX A. DIRECTORY ENTRIES FOR TCP/IP VIRTUAL MACHINES

A.1 TCPMAINT VIRTUAL MACHINE

```
USER TCPMAINT password 3M 4M BG
  OPTION ECMODE
  IPL CMS
  CONSOLE 009 3215
  SPOOL   00C 2540 READER *
  SPOOL   00D 2540 PUNCH  A
  SPOOL   00E 1403 A
  LINK MAINT    190 190 RR
  LINK MAINT    19E 19E RR
  LINK TCPIP    191 593 MR
  LINK FTPSERVE 191 594 MR
  LINK SMTP     191 595 MR
  LINK NAMESRV  191 596 MR
  MDISK 191 FB-512 15816    6128 OPTPK1 MR      ( 3  MB)
  MDISK 2C0 FB-512 16      28672 VMWRK1 MR      (14  MB)
  MDISK 5C3 FB-512 267608  28672 OPTPK1 MR      (14  MB)
  MDISK 592 FB-512 254692 163384 OPTPK1 MR ALL  ( 8  MB)
```

Figure 38. Definition of TCPMAINT Virtual Machine

This virtual machine is used for installing and maintaining the TCP/IP system. It has access to all TCP/IP minidisks and console listings from other TCP/IP virtual machines are transferred to this userid. Privilege class B is required for autologging the TCPIP virtual machine during the verification procedure.

To access the TCP/IP services, the users must link to the 592 minidisk. Alternatively, the content of this minidisk may be transferred to a user-visible minidisk. Minidisks TCPMAINT 2C0 and 5C3 are not required if the source code, compilation execs and text decks are not going to be unloaded from the distribution tape.

A.2 TCPIP VIRTUAL MACHINE

```
USER TCPIP password 6M 8M ABG
  OPTION ECMODE BMX MAXCONN 255 DIAG98
  IUCV ANY  PRIORITY
  IUCV *CCS PRIORITY MSGLIMIT 255
  IPL CMS
  CONSOLE 009 3215
  SPOOL   00C 2540 READER *
  SPOOL   00D 2540 PUNCH  A
  SPOOL   00E 1403 A
  LINK MAINT    190 190 RR
  LINK MAINT    19E 19E RR
  LINK TCPMAINT 592 592 RR
  MDISK 191 3380 007  4 XVMPM4 MR          (2.4 M)
```

Figure 39. Definition of TCPIP Virtual Machine

This is the main virtual machine for providing TCP/UDP/IP communication services. The Telnet server is also implemented in this virtual machine.

This virtual machine is autologged by the System Operator and it autologs the remaining service machines. Privilege class A is required for issuing the Force, Unlock and Set QDROP commands, and class B for the Autolog and Attach commands.

The Inter-User Communication Vehicle (IUCV) control statements are required for Telnet server line-mode support. The MAXCONN nn option specifies the number of concurrent IUCV connections to this virtual machine that you will allow.

The BMX option is used to specify that all TCPIP virtual machine I/O operations are to occur as block multiplexer channel operations. This allows the successful start of multiple SIOs to different devices on the same channel.

A.3 FTPSERVE VIRTUAL MACHINE

```
USER FTPSERVE password 2M 4M BG
  OPTION ECMODE ACCT
  IPL CMS
  CONSOLE 009 3215
  SPOOL   00C 2540 READER *
  SPOOL   00D 2540 PUNCH  A
  SPOOL   00E 1403 A
  LINK MAINT    190 190 RR
  LINK MAINT    19E 19E RR
  LINK TCPMAINT 592 592 RR
  MDISK 191 3380 167  2 XVMPM4 MR          ( 1 M)
```

Figure 40. Definition of FTPSERVE Virtual Machine

This is the virtual machine for the FTP server. It provides controlled access to files on the local host, and it requires the ACCT option. Privilege class B is required for issuing the Diagnose '84' command.

Multiple FTP servers may be set up to improve the system throughout. Each server requires a separate virtual machine with the above CP directory and resources (Figure 40).

A.4 SMTP VIRTUAL MACHINE

```
USER SMTP password 2M 4M BG
  OPTION ECMODE
  IPL CMS
  CONSOLE 009 3215
  SPOOL   00C 2540 READER *
  SPOOL   00D 2540 PUNCH  A
  SPOOL   00E 1403 A
  LINK MAINT    190 190 RR
  LINK MAINT    19E 19E RR
  LINK TCPMAINT 592 592 RR
  MDISK 191 3380 763 30 XVMU28 MR          (0.5 M + ?)
```

Figure 41. Definition of SMTP Virtual Machine

This is the virtual machine for both the SMTP user and server. It receives mail over a TCP network connection or from its virtual reader

and then sends it through the TCP or RSCS network, according to the mail destinations.

Mail that arrives from the virtual reader is first read onto the SMTP 191 minidisk. Mail may accumulate if it is arriving faster than it is being delivered or if some of the TCP/IP links are down. Sufficient room must be provided on the disk to accommodate the mail.

If the SMTP virtual machine is given CP privilege class B, then it will use the CP MSGNOH command to send delivery messages to local users in a more compact format. If class B is not specified, CP MSG command will be used instead.

A.5 NAMESRV VIRTUAL MACHINE

```
USER NAMESRV  password 2M 4M G
  OPTION ECMODE
  IPL CMS
  IUCV ALLOW
  CONSOLE 009 3215
  SPOOL   00C 2540 READER *
  SPOOL   00D 2540 PUNCH  A
  SPOOL   00E 1403 A
  LINK MAINT    190 190 RR
  LINK MAINT    19E 19E RR
  LINK TCPMAINT 592 592 RR
  LINK SQLDBA   295 593 RR
  LINK REXSQL   295 594 RR
  MDISK 191 3380 673  3 VMU401 MR          (1.5 M)
```

ARP: ARP stands for Address Resolution Protocol. This protocol resolves actual ETHERNET addresses by sending ARP requests on the network.

RFC: RFC stands for Request for Comment. It is documented where most of the protocols are described. They are identified by numbers.

TCP/IP: TCP/IP is the combination of TCP and IP (UDP and IP are also common). TCP/IP represent the layers 3 and 4 in the OSI/ISO seven layer reference model.

TCP: The Transmission Control Protocol (TCP) is used in the United States Advanced Research Projects Agency (ARPA) internet and any network following the Department of Defense standards. TCP provides a reliable host-to-host protocol packet switched networks. TCP assumes, that IP is the underlying protocol.

IP: The Internet Protocol (IP) is used as a basic transport mechanism to carry packets or datagrams to the next destination host. IP provides the universal addressing of hosts in the network. IP does NOT provide a reliable connection (no flow control, no retransmitting, no error control, no acknowledgements, and so on).

UDP: The User Datagram Protocol (UDP) allows transfer of datagrams. It assumes IP to be the underlying protocol. UDP is not a reliable connection.

Client: A client is any virtual machine that communicates with the VM TCP/IP program or uses it's services

Server: A server is a function that provides services for users. A server is a prerequisite, that other clients can use the functions of a host. A host can be a server and a user at the same time.

READER'S COMMENTS

Title: IBM 9370 LAN , Volume 2- IEEE 802.3 Support

You may use this form to communicate your comments about this publication, its organization or subject matter with the understanding that IBM may use or distribute whatever information you supply in any way it believes appropriate without incurring any obligation to you.

Comments:

Reply requested

Yes / No

Name : _____

Job Title : _____

Address : _____

_____

----------fold----------

IBM International Technical Support Center
Dept. 3222, Bldg. 7030-75
Schoenaicher Strasse 220
7030 Boeblingen
West Germany

----------fold----------

IBM 9370 LAN Volume 2 - IEEE 802.3 Support GG24-3227-00 PRINTED IN THE U.S.A.

GG24-3227-00