Additional copies of this manual may be obtained from:

Technical Publications, M/S DV2/292
Integrated Systems Operation—South
Intel Corporation
2402 W. Beardsley Road
Phoenix, Arizona 85027

Other Intel literature may be obtained from:

Literature Department
Intel Corporation
3065 Bowers Avenue
Santa Clara, CA 95051

The information in this document is subject to change without notice.

Intel Corporation makes no warranty of any kind with regard to this material, including, but not limited to, the implied warranties to merchantability and fitness for a particular purpose. Intel Corporation assumes no responsibility for any errors that may appear in this document. Intel Corporation makes no commitment to update nor to keep current the information contained in this document.

Intel Corporation assumes no responsibility for the use of any circuitry other than circuitry embodied in an Intel product. No other circuit patent licenses are implied.

Intel software products are copyrighted by and shall remain the property of Intel Corporation. Use, duplication or disclosure is subject to restrictions stated in Intel's software license, or as defined in ASPR 7-104.9(a)(9).

No part of this document may be copied or reproduced in any form or by any means without the prior written consent of Intel Corporation.

The following are trademarks of Intel Corporation and its affiliates and may be used only to describe Intel products:

<table>
<thead>
<tr>
<th>Trademark</th>
<th>Vendor</th>
</tr>
</thead>
<tbody>
<tr>
<td>AEDIT</td>
<td>iDIS</td>
</tr>
<tr>
<td>BITBUS</td>
<td>iLBX</td>
</tr>
<tr>
<td>BXP</td>
<td>iMDX</td>
</tr>
<tr>
<td>COMMputer</td>
<td>iMMX</td>
</tr>
<tr>
<td>CREDIT</td>
<td>Intel</td>
</tr>
<tr>
<td>Data Pipeline</td>
<td>intellinet</td>
</tr>
<tr>
<td>Genis</td>
<td>intelBOS</td>
</tr>
<tr>
<td>IS</td>
<td>iMXX</td>
</tr>
<tr>
<td>iATC</td>
<td>Intelligent</td>
</tr>
<tr>
<td>iICE</td>
<td>iBOS</td>
</tr>
<tr>
<td>iCS</td>
<td>Intelligent</td>
</tr>
<tr>
<td>iDBP</td>
<td>IntelBOS</td>
</tr>
</tbody>
</table>

and the combination of ICE, iCS, iRMX, iSBC, iSBX, or MCS and a numerical suffix.
<table>
<thead>
<tr>
<th>REV.</th>
<th>REVISION HISTORY</th>
<th>DATE</th>
</tr>
</thead>
<tbody>
<tr>
<td>-001</td>
<td>Original issue</td>
<td>03/85</td>
</tr>
</tbody>
</table>
This manual addresses the installation and configuration of XENIX Networking Software on the 286/380 and the 286/310 systems. Users of this manual should be familiar with the Xenix operating system and local area networks (LANs). The instructions provided in this manual assume that the ETHERNET* has been properly installed, and that each system being placed on the network is currently running Xenix Release 3.0 operating system. Do not perform this procedure until that environment has been created.

This manual does not describe how to use the network to access files, printers, or other resources. For instructions on using the network, refer to the Xenix Networking Software Users Guide, Order Number 135147.

Briefly, the manual consists of the following:

- Chapter 1—“Introduction,” contains an overview of Xenix Networking Software.
- Chapter 2—“Hardware Installation,” is a brief set of procedures for the installation of network hardware on system 286/310s and 286/380s.
- Chapter 3—“Planning the Network,” defines the basic network entities and describes the information needed prior to configuring the network.
- Chapter 4—“Installation & Configuration,” provides a step by step network software installation procedure.
- Chapter 5—“Defining Users and Groups,” is a guide for creating network user and group definition files.
- Appendix A—“iSXM 552S Jumper Configuration,” is an illustration showing the locations of required jumpers on the Ethernet Communication Board.

*ETHERNET is a Trademark of Xerox Corporation
Contents

CHAPTER 1
INTRODUCTION
Product Definition ..................................................... 1-1
OpenNET Product Family ........................................ 1-1
OpenNET Network Model ........................................ 1-1
Xenix Networking Software Operating Environment .......... 1-2
Xenix Networking Software Services ............................. 1-2
Xenix Networking Software Administration ..................... 1-3
Xenix Networking Software Installation ........................ 1-4

CHAPTER 2
HARDWARE INSTALLATION
Introduction ............................................................... 2-1
Required Hardware ................................................... 2-1
iSXM 552S Installation in the System 310 ...................... 2-1
iSXM 552S Installation in the System 380 ...................... 2-3

CHAPTER 3
PLANNING THE NETWORK
Introduction ............................................................... 3-1
Nodes ........................................................................ 3-1
Users ........................................................................ 3-1
Groups ........................................................................ 3-2
Special Network Files ................................................ 3-2
Self Definition File .................................................... 3-2
Consumer Definition File (/net/cdf) ............................... 3-2
Nameserver Database (/net/data) .................................. 3-2

CHAPTER 4
INSTALLATION AND CONFIGURATION
Introduction ................................................................ 4-1
Installation Procedure ............................................... 4-1
Configuration Procedure ............................................ 4-2
  mksel ................................................................. 4-2
  mkcon ................................................................. 4-2
  mkns ................................................................. 4-3
Enabling the Network ................................................. 4-4

CHAPTER 5
DEFINING USERS AND GROUPS
Introduction ................................................................ 5-1
New Installation ......................................................... 5-1
Existing XENIX Systems ............................................. 5-2
  Invoking mguser ................................................... 5-2
  Invoking chuid ..................................................... 5-4
  Invoking chmem .................................................... 5-5
  Invoking mggrup ................................................... 5-5
  Invoking chgid ..................................................... 5-7
Completing the Process ............................................... 5-7

APPENDIX A
iSXM 552S JUMPER CONFIGURATION

Tables

<table>
<thead>
<tr>
<th>TABLE</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>1-1</td>
<td>ISO Open System Interconnect Model</td>
<td>1-2</td>
</tr>
</tbody>
</table>
## Figures

<table>
<thead>
<tr>
<th>FIGURE</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>2-1</td>
<td>System 310 Hardware</td>
<td>2-2</td>
</tr>
<tr>
<td>2-2</td>
<td>System 380 Installation</td>
<td>2-4</td>
</tr>
<tr>
<td>3-1</td>
<td>Example Three-Node Virtual Circuit</td>
<td>3-4</td>
</tr>
<tr>
<td></td>
<td>Connection</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FIGURE</th>
<th>TITLE</th>
<th>PAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>3-2</td>
<td>Example Configuration Files for Three-Node Network (Consumer Based Validation)</td>
<td>3-5</td>
</tr>
<tr>
<td>3-3</td>
<td>Example Configuration Files for Three-Node Network (Server Based Validation on node &quot;cash&quot;)</td>
<td>3-6</td>
</tr>
</tbody>
</table>
1.1 Product Definition

XENIX Networking Software is the XENIX implementation of the layer 5-7 OpenNET services and protocols. It provides network services with a high degree of user interface transparency. The combination of XENIX Networking Software, iNA961 transport software and the iSX552 Ethernet interface board provide a full, seven layer OpenNET networking package for XENIX systems that offers high performance and extensive interconnectability. XENIX Networking Software will function with other lower layer solutions.

1.2 OpenNET Product Family

The OpenNET product family incorporates a set of system and component level LAN products covering all seven layers of the ISO Open System Interconnect (OSI) model, and the protocols on which they are based. OpenNET protocols are, wherever possible, established industry standards for each function. Therefore OpenNET products can interconnect and interoperate not only with each other, but with the most popular networking products from other vendors. OpenNET networks provide a high level of interoperability between heterogeneous systems (MS-DOS1, PC-DOS and iRMX86 versions are being developed), thus users can tailor their networks to meet their specific needs by incorporating any combination of the capabilities of these diverse systems.

The OpenNET application layer protocols implemented by XENIX Networking Software are those adopted by Microsoft and IBM for their microcomputer networking products. XENIX Networking Software is therefore compatible with, and will interoperate with, Microsoft's MS-NET for MS-DOS and IBM's PC-NET at the application layer (assuming the availability of compatible lower layer hardware and software). In addition a compatible version of iRMX Networking Software is being developed.

The services provided by XENIX Networking Software Release 1.0 are Network File Sharing and inter-application communication.

1.3 OpenNET Network Model

OpenNET conforms to the ISO (International Standards Organization) reference model for Open System Interconnection. The following table illustrates the layering of this model and the OpenNET use of it.

1XENIX and MS-DOS are trademarks of Microsoft Corp.
Table 1-1. ISO Open System Interconnect Model

<table>
<thead>
<tr>
<th>Layer</th>
<th>Service</th>
<th>OpenNET</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application</td>
<td>End User Services</td>
<td>PC-NET File Access</td>
</tr>
<tr>
<td>Presentation</td>
<td>Data Transformation</td>
<td>null</td>
</tr>
<tr>
<td>Session</td>
<td>Logical Connections</td>
<td>standard interface</td>
</tr>
<tr>
<td>Transport</td>
<td>Virtual Circuit Support</td>
<td>ISO DP8073 (Class 4)</td>
</tr>
<tr>
<td>Network</td>
<td>Message Routing</td>
<td>null</td>
</tr>
<tr>
<td>Data Link</td>
<td>Byte Stream Transfer</td>
<td>IEEE 802.3 (Ethernet)</td>
</tr>
<tr>
<td>Physical</td>
<td>Physical Connection</td>
<td>Ethernet</td>
</tr>
</tbody>
</table>

A node using XENIX Networking Software can interoperate with both XENIX and MS-DOS systems on the network. They are connected by Ethernet in a typical bus topology—all systems have direct access to all other systems. Each system is identified by a unique 48-bit address which is used by the Data Link layer when connecting to other systems.

1.4 XENIX Networking Software Operating Environment

XENIX Networking Software requires an Intel 286/310 or 286/380 system with at least 512K of RAM, 15MB of disk storage and an iSXM 552 Ethernet controller. XENIX 286 Release 3.0 with update 1 (or a later release) must be installed.

1.5 XENIX Networking Software Services

At the Application layer XENIX Networking Software provides Network File Access. This service allows any user in the network to have access to any file in the network. Such accesses are "transparent", i.e., remote files are accessed in exactly the same fashion as local files, a user application need not be aware of the location of a file being accessed.

To provide network unique names that are consistent throughout the network the file hierarchy has been extended "upwards" through the addition of a "network root" to the file name space, and the name of the system containing the file is included in the pathname. The presence of the network root is indicated by commencing the pathname with "//". A full network pathname thus has the form:

```
//network_node/local_path/file_name<cr>
```

The treatment of pathnames not commencing with the network root identifier is unchanged, i.e., a single "/" indicates the local root, no initial delimiter indicates a reference relative to the current directory.

To access a remote file a user simply references it. Because network file access is transparent there are no special "network file" commands or system calls. The user may reference a remote file in any context that a local file may be referenced. For example, to list the directory "/etc" on the machine "test", the user enters the following command:

```
ls //test/etc<cr>
```

To then display the file "/etc/passwd" on node "test", he may enter the following command:

```
mores //test/etc/passwd<cr>
```
Similarly file protection and sharing are transparent. The owner of a file may allow or prevent accesses by network users in the same manner that permissions are granted to local users. Concurrent sharing of network files is permitted and the standard XENIX Locking primitives may be used to synchronize accesses. As with standalone XENIX it is the users' responsibility to use these primitives correctly.

The XENIX Networking Software session layer provides XENIX application developers with a logical connection capability. This facility allows users to establish connections between any pair of cooperating applications in the network. Once established these connections may be used to exchange any data that the applications desire.

1.6 XENIX Networking Software Administration

There are two major aspects to the management of an OpenNET network—control of the network configuration and control of the network users.

The network configuration is managed through a service called the “Nameserver.” This service maintains a database containing the physical configuration of the network and the capabilities of each participating system. The database is replicated at each node in the network. Tools are provided for maintaining this database and for retrieving data from it. It is the user's responsibility to ensure that the nameserver database accurately reflects the configuration and capabilities of his network.

XENIX Networking Software provides a “single system” view of the network to its users. The entire network appears to each user as a single large system with a single integrated file system. The fact that the network's processing capabilities and file system are physically distributed is invisible to the normal end-user.

In keeping with this view of the network each network will support a single community of users, i.e., each network user has a single identity (name and user ID) in the network and can login to any system in the network using that identity (provided that node allows his access), much as a user of a large timesharing system may login from any connected terminal.

All nodes keep a local copy of the user definitions so that they may continue to operate should they be removed from the network. User identities may be validated by either the consumer node or the server node. When the consumer node performs the validation, the user need only login to that consumer node to gain access to all server nodes that accept its validations. In these cases the server will validate the consumer node to ensure that it is a node whose user validations it accepts. When the server node validates users, the users must explicitly “login” to each such server node they wish to access.

There will be a master copy of the user definition (/etc/passwd) file and group definition file (/etc/group) that will reflect all changes to these definitions. If the system containing the master copy permits remote superusers to write to them, the XENIX Networking Software utilities will allow the master to be updated from any node. Otherwise all updates must be made at the node containing the master copy. It is the user's responsibility to ensure that the local copy on each node is updated from this master copy.
1.7 XENIX Networking Software Installation

The remaining chapters of this manual provide instructions for installing XENIX Networking Software and the networking hardware necessary to support it. In addition, the XENIX Networking Software User's Guide, order number 135147 provides a complete reference to the installation and administration networking utilities.

This manual covers the following subjects:

- Installation of the networking hardware (the iSX552 Ethernet Controller).
- Planning the network, installing XENIX Networking Software and building the required configuration files.
- Establishing the user and group definition files for the network users.
2.1 Introduction

This chapter describes the installation of the hardware necessary for an operational Ethernet. There are two sections: instructions on installing hardware in a system 310 and similar instructions for the system 380. Additional information for performing the system 310 and system 380 installations are provided in the iNA 961 Programmer's Reference Manual.

When the network hardware has been installed, refer to the iMDDX Test Reference Manual to run the supplemental level diagnostics. Execute the MD552 diagnostic test suite in both the single station and two station modes. Repeat the two station test until all systems have communicated. This allows complete confidence in the communication hardware before performing the XENIX Networking Software Installation.

2.2 Required Hardware

The following board and cable are the only internal hardware requirements for the 286/380 and 286/310 systems.

iSX M 552S Ethernet Communication Board
Internal Ethernet Transciever Cable

The iSX M 552S Ethernet Communication board comes strapped for installation with Xenix. The jumpers for this environment are illustrated in Appendix A.

2.3 iSX M 552S Installation in the System 310

The following instructions are provided to guide the user through the installation of the internal hardware on the System 310. Perform these procedures on every System 310 that will be a part of the network.

1. Power down the system and remove the AC power cord from the power source.
2. Remove the four screws securing the System 310 back panel to the chassis (refer to Figure 2-1).
3. Remove all cables connected from the 310 to the back panel. Record the connections and cable orientation for re-installation.
4. Remove the card retainers located on either side of the card cage by loosening the two screws, then lifting up and away from the system chassis.
5. Install the iSX M 552S board into slots four or five of the system cardcage. Ensure that the board is well seated by pushing firmly on the card ejectors.

NOTE
Because initial versions of the iSX M 552 have an attached adapter board, the iSX M 552S requires the space of two slots.
Figure 2-1. System 310 Hardware
6. Replace the card retainers as removed in step 4 of this procedure.
7. Connect the plastic connector end of the internal transceiver cable to connector J1 on the iSXM 552S board.
8. Connect the other end of the internal transceiver cable to the J1 knockout on the 310 back panel. Use the medium panel adapter plate supplied with the transceiver cable kit.
9. Reconnect all cables to the back panel as removed in step 3 of this procedure.
10. Replace the back panel on the system and secure with four screws.
11. Plug the system in to AC power and power on the system.
12. Verify that during the power up diagnostics the Ethernet Communication Subsystem test passes.
13. Verify that when XENIX is booted the node's Ethernet address is displayed. This will have the form:

\[ 00AA0000xxxx \]

### 2.5 iSXM 552S Installation in the System 380

The following instructions are provided to guide the user through the installation of the internal hardware on the system 380. Perform these procedures on every system 380 that will be a part of the Opennet network.

1. Power down the system and remove the AC power cord from the power source.
2. Turn the four quarter turn screws and remove top cover from system (see Figure 2-2).
3. Insert the iSXM 552S board into slot 4 or 5 of the system cardcage. Push firmly on the card ejector tabs to ensure that the board seats.
4. Connect the plastic end of the internal transceiver cable to the J1 connector of the iSXM 552S board.
5. Connect the other end of the internal transceiver cable to an available port on the back panel of the system. It may require the use of an adapter plate supplied with the hardware kit. (See Figure 2-2.)
6. Replace the top cover on the system and tighten the four quarter turn screws to secure.
7. Plug the power cord in and power up the system.
8. Verify that the power diagnostic test for the Ethernet communication subsystem passes.
9. Verify that when XENIX is booted the node's Ethernet address is displayed. This will have the form:

\[ 00AA0000xxxx \]
Figure 2-2. System 380 Installation
CHAPTER 3
PLANNING THE NETWORK

3.1 Introduction

The network is made up of four basic entities: nodes (systems), users, groups, and special network files. Each of these plays an important role in the network’s configuration. Before you begin planning and configuring your network, an understanding of these basic entities is essential. This chapter provides an overview of these basic concepts, a brief summary of how the network functions, and a checklist of those items which should be determined prior to configuring the network.

3.2 Nodes

A node is an individual system on the network. Each node must be assigned a unique logical name and an associated password. In addition to its logical name, each node has an Ethernet address which is normally found on the communications board. This address will be displayed at system boot time and should be recorded so that it can be referenced later when executing some of the configuration utilities.

The node name and the password may each contain up to 12 characters consisting of all ASCII printable characters except ‘/’, ‘\’, ‘*’, ‘;’, ‘:’, ‘!’, and ‘l’. The node name must contain at least three characters. The password must contain at least five characters.

The node name and password must be available locally and to those servers that will allow the node to access their services as a consumer. They are available in the local file /net/self established by the mkself utility. The node name and password are presented to the server via a login protocol. The server validates them against its local /net/cdf file. The /net/cdf file is established by the mkcon utility. Mkself and mkcon are discussed in Chapter 4.

3.3 Users

Network users are the people who make use of network resources and services. They are defined in a user definition file known as /etc/passwd. There is a master copy of /etc/passwd and each node on the network holds a copy of the file. This master copy must reside on a XENIX server node which is accessible from all other XENIX nodes. The master copy may have any name the network administrator chooses to assign to it; the local copies of the file must be known as /etc/passwd.

When building a network out of existing XENIX systems or adding an existing system to a network, it is necessary to make certain that there is no duplication in user definitions. Each user must have a unique login name and a unique user ID. The mguser utility is provided to identify any duplication in user definitions. If duplications are found they must be resolved by the network administrator. Additional information on /etc/passwd and resolving duplications is found in Chapter 5.
3.4 Groups

Network users may be divided into groups, with each group being defined in a group definition file known as /etc/group. There is a master copy of /etc/group with each node holding a local copy of the file. The master copy should reside on a server node which is accessible from all other XENIX nodes. Each group must have a unique definition within the network. The master copy may have any name the network administrator chooses to assign to it; the local copies of the file must be known as /etc/group.

When building a network out of existing XENIX systems or adding an existing system to a network, it is necessary to make certain that there is no duplication in group definitions. Each group's name and group ID must be unique. The mggroup utility is provided to identify any duplication in group names and group IDs. If duplications are found they must be resolved by the network administrator. Additional information on /etc/group and the resolution of duplicate entries is found in Chapter 5.

3.5 Special Network Files

Three special files (/net/self, /net/cdf, and /net/data) must be established for use by the XENIX Networking Software.

3.5.1 Self Definition File (/net/self)

This file defines a XENIX node. It contains the node's name, password, physical address, and the full network pathnames of the master copies of the other administration files. Each node has a unique Self Definition File.

3.5.2 Consumer Definition File (/net/cdf)

This file exists only at server nodes. It contains a list of consumer nodes whose user validations the server will accept. The entry for each consumer node contains the consumers name, a password, and a list of allowed services. It is used to validate the consumers identity and requested service when it connects to the server. Each server node has a unique Consumer Definition File.

3.5.3 Nameserver Database (/net/data)

This file defines the topology of the network. It contains an entry for every process that can communicate on the network (including the file consumer and server processes). These entries contain the logical name of the process, its physical address and its operating system type. The database is used to translate process names into physical addresses when connections between processes are established. The database is replicated at every node. One copy is designated the "master" copy and XENIX Networking Software ensures that all updates to the database are made to this copy. The master copy must then be copied to all other nodes by the superuser.
3.6 User Validation

XENIX Networking Software supports two schemes of user validation, consumer based and server based. The two schemes are compatible and may coexist on the same network. To illustrate these concepts, a sample network is used. This network consists of three nodes which have been assigned the names "books", "cash", and "folks" as illustrated in Figure 3-1. Each process begins with a request for services initiated by one node (a consumer) to another node that is to provide the services (a server).

3.6.1 Consumer Based Validation

With consumer based user validation, the server node validates the consumer node in much the same way as "login" validates a user. The server checks the node name and password supplied by the consumer node against the entries in the server's /net/cdf file to verify that the request is coming from an authorized consumer node. The consuming process obtains its node name and password from its local /net/self file, so it is essential that the information placed in the consumer's /net/self file is consistent with the information placed in the server's /net/cdf file. Once the consumer has been validated, a logical connection is established between the server process and the consumer process. This logical connection is referred to as a virtual circuit (VC), and is represented as an arrow in Figure 3-1.

Note that VCs can be established between any consumer and server in the sample network. Once the server finds a valid entry for the consumer node in its /net/cdf file, the consumer node performs all user validation; any user of the consumer node then has access to the server with no further validation by the server node.

Figure 3-2 provides a summary of the content found in each node's /net/self and /net/cdf file for the sample network with consumer based validation. An example of the nameserver database file, /net/data, is also included. This file would be the same at all nodes.

3.6.2 Server Based Validation

An alternative view of the network is one in which not all users from a node (or set of nodes) can access another node in the network. Perhaps the users defined on system "cash" are not permitted ready access to resources on node "folks", i.e., the server on "folks" does not accept user validations performed by the node "cash".

The /net/cdf file on "folks" would not contain an entry for the consumer node "cash". This would force a user from node "cash" to login to the server node via the "net use" command so that the server process could validate the user who is requesting the services. (The net use command is discussed in detail in the XENIX Networking Software User's Guide.)

Figure 3-3 provides a summary of the content found in each node's /net/self and /net/cdf file for our sample network with server based validation for node "cash". An example of the nameserver database file, /net/data, is also included. This file would be the same at all nodes.
Figure 3-1. Example Three-Node Virtual Circuit Connection
### "books"

<table>
<thead>
<tr>
<th>/net/self</th>
<th>/net/cdf</th>
</tr>
</thead>
<tbody>
<tr>
<td>books:secret</td>
<td>folks:xykgrsx:1</td>
</tr>
<tr>
<td>0x81000a0000000100aa0002b46000000</td>
<td>cash:xykgrsx:1</td>
</tr>
<tr>
<td>0x80000a0000000100aa0002b46000000</td>
<td>/folks/etc/passwd</td>
</tr>
<tr>
<td></td>
<td>/folks/etc/group</td>
</tr>
<tr>
<td></td>
<td>/folks/net/data.master</td>
</tr>
</tbody>
</table>

### "cash"

<table>
<thead>
<tr>
<th>/net/self</th>
<th>/net/cdf</th>
</tr>
</thead>
<tbody>
<tr>
<td>cash:money</td>
<td>folks:yzzstavk:1</td>
</tr>
<tr>
<td>0x81000a0000000100aa0002db4000000</td>
<td>books:yzzstavk:1</td>
</tr>
<tr>
<td>0x80000a0000000100aa0002db4000000</td>
<td>/folks/etc/passwd</td>
</tr>
<tr>
<td></td>
<td>/folks/etc/group</td>
</tr>
<tr>
<td></td>
<td>/folks/net/data.master</td>
</tr>
</tbody>
</table>

### "folks"

<table>
<thead>
<tr>
<th>/net/self</th>
<th>net/cdf</th>
</tr>
</thead>
<tbody>
<tr>
<td>folks:message</td>
<td>books:vckxzy:1</td>
</tr>
<tr>
<td>0x81000a0000000100aa0002cbo000000</td>
<td>cash:vckxzy:1</td>
</tr>
<tr>
<td>0x80000a0000000100aa0002cbo000000</td>
<td>/folks/etc/passwd</td>
</tr>
<tr>
<td></td>
<td>/folks/etc/group</td>
</tr>
<tr>
<td></td>
<td>/folks/net/data.master</td>
</tr>
</tbody>
</table>

### sample

/net/data replicated at each node

- folks/nfs:TYPE=XENIX:ADDRESS=0x80000a0000000100aa0002cbo000000;
- folks/nfc:TYPE=XENIX:ADDRESS=0x81000a0000000100aa0002cbo000000;
- books/nfs:TYPE=XENIX:ADDRESS=0x80000a0000000100aa0002b46000000;
- books/nfc:TYPE=XENIX:ADDRESS=0x81000a0000000100aa0002b46000000;
- cash/nfs:TYPE=XENIX:ADDRESS=0x80000a0000000100aa0002db4000000;
- cash/nfc:TYPE=XENIX:ADDRESS=0x81000a0000000100aa0002db4000000;

---

**Figure 3-2. Example Configuration Files for Three-Node Network**

*(Consumer Based Validation)*
### 'books'

<table>
<thead>
<tr>
<th>/net/self</th>
<th>/net/cdf</th>
</tr>
</thead>
<tbody>
<tr>
<td>books:secret 0X81000A00000000100AA00002B4G000000 0X80000A00000000100AA00002B4G000000 //folks/etc/passwd //folks/etc/group //folks/net/data.master</td>
<td>folks:xlkfsf:1</td>
</tr>
</tbody>
</table>

### 'cash'

<table>
<thead>
<tr>
<th>/net/self</th>
<th>/net/cdf</th>
</tr>
</thead>
<tbody>
<tr>
<td>cash:money 0X81000A00000000100AA00002B4G000000 0X80000A00000000100AA00002B4G000000 //folks/etc/passwd //folks/etc/group //folks/net/data.master</td>
<td>folks:xclvwkl:1 books:xcvddk:1</td>
</tr>
</tbody>
</table>

### 'folks'

<table>
<thead>
<tr>
<th>/net/self</th>
<th>/net/cdf</th>
</tr>
</thead>
<tbody>
<tr>
<td>folks:message 0X81000A00000000100AA00002B4G000000 0X80000A00000000100AA00002B4G000000 //folks/etc/passwd //folks/etc/group //folks/net/data.master</td>
<td>books:qwoe:1</td>
</tr>
</tbody>
</table>

### sample

/net/data replicated at each node


---

Figure 3-3. Example Configuration Files for Three-Node Network (Server Based Validation on node "cash").

3-6
For a user on "cash" to connect to "folks" the user must be defined in the /etc/passwd file on "folks". The user definition should be consistent with that found in the /etc/passwd file on "cash". If the user ID and group ID are not the same in both entries, those utilities and functions which make use of these values may behave in an inconsistent manner.

Note that unless the node(s) containing the master copies of the /etc/passwd, /etc/group and /net/data ("folks" in the example) allow remote users to login as superuser, it will not be possible to modify users, groups or node definitions from remote nodes when server based user authentication is used. Such updates would have to be performed at the node containing the master files. They must then be copied to the other nodes on the network.

In addition to the "net use" interface, this approach introduces one other non-transparent aspect to the user interface. When a file with the SETUID or SETGID attribute is executed and accesses a server, the server will not honor the change in user ID or group ID. It will continue to execute all accesses on behalf of the original logged in user. This restriction is necessary, for allowing the identity of the accessor to change without validation against the server's /etc/passwd file would violate the basic purpose of this approach.

3.7 Checklist of Required Information

In preparation for configuring the network, the network administrator must determine the following information:

- logical name for each node (3 to 12 alphanumeric characters). Node names must not conflict with the first level XENIX directory names—etc, bin, lib, usr, sys, net, calendar, etc.
- password for each node (5 to 12 alphanumeric characters)
- Ethernet address for each node (should be noted at boot time)
- nodes which will be servers
- nodes which will be consumers
- consumers whose user validations will be accepted by each server
- name of node to host master copy of the user definition file (/etc/passwd)
- full pathname of master copy of the user definition file (/etc/passwd)
- name of node to host master copy of the group definition file (/etc/group)
- full pathname of master copy of the group definition file (/etc/group)
- name of node to host master copy of the nameserver database (/net/data)
- full pathname of master copy of nameserver database file (/net/data)
- users to be defined on the network
- procedure for resolving any inconsistencies in existing user definitions (the mguser, chuid and chmem commands are provided to assist with this task)
- groups which will be defined on the network
- procedure for resolving any duplication in existing group definitions (the mgroup and chgid utilities are provided to assist with this task)
4.1 Introduction

The following installation procedure installs the software from diskette to Winchester disk. This procedure must be performed at every network node. It is recommended that the node's file system and the OpenNET diskettes be backed up before performing software installation.

4.2 Installation Procedure

1. Boot the system in maintenance mode. Run "fsck -y" until the system is clean. If the message "File system was modified" appears after the fsck has completed, run fsck again until the message no longer appears.

2. If XENIX 286 Release 3.0 Update 1 has not been installed, install it now.

3. If you are running a 310-40 or a 380, mount the usr partition.

4. Enter the following command:
   
   sh /etc/instlxnet <cr>

5. Read the instructions that appear on the screen. Prompts will be provided to take you through the sequence of steps needed to install the software.

6. Once the OpenNET software has been installed, you will be prompted to insert the iNA961 diskette so that it may be loaded on to the system. The iNA961 software must be located in the file /net/ina961. (If you choose not to load iNA961 at this time, be certain that you DO load it before issuing an 'nfc on' or 'nfs on' command or using the session layer in any way.)

7. You will be prompted to indicate whether or not a new kernel is to be generated at this time. Enter a 'yes' response unless you wish to change some of the network parameters used in building the kernel. The default kernel which will be built assumes the presence of a 544 serial I/O board and is adequate for most network configurations. Special configurations may require a change to the default parameters used in this kernel. Refer to the XENIX Networking Software User's Guide for information on modifying the kernel.

8. If you entered a 'no' response in step 6, make the desired modifications, and upon completion enter the following:
   
   cd /sys/cfg<cr>
   make<cr>

   Then generate the new kernel by entering the following:
   
   cd /sys/conf<cr>
   make<cr>

   The new kernel is located in /sys/conf/xenix and should be moved to /xenix.

9. If you answered yes in step 6, you will be asked if the new kernel should be moved to /xenix. A 'no' response places the new kernel in /xenix.net.

10. Shut the system down and reboot from the new kernel.

    If you gave a 'yes' response in step 8, reboot from /xenix.

    If you gave a 'no' response in step 8, reboot from /xenix.net.
When you reboot from the new kernel, record the Ethernet address which is displayed. It is needed when executing some of the configuration utilities in the next phase of the installation/configuration procedure.

4.3 Configuration Procedure

The next step is to establish the three network files /net/self, /net/cdf, and the master nameserver database (/net/data) via the utilities mkself, mkcon, and mkns, respectively. At this time you will need the information identified in the checklist found at the end of the chapter on Planning the Network. It is recommended that the systems remain in maintenance mode during this process.

4.3.1 mkself

For each node in the network perform the following:

1. Enter: `mkself (cr)`

2. You will be prompted to enter each of the following pieces of information:
   - machine name: enter the node name for this node (example: cash)
   - machine password: enter the password for this node (example: money)
   - ETHERNET address: enter (cr) to automatically enter the address of the installed iSXM552 board.
   - port ID for consumer process: enter (cr) for XENIX default
   - port ID for server process: enter (cr) for XENIX default
   - full pathname of master /etc/passwd: enter full network path for master passwd file (example: //folks/etc/passwd)
   - full pathname of master /etc/group: enter full network path for master group file (example: //folks/etc/group)
   - full pathname of master nameserver database: enter full network path for master database (example://folks/net/data)

3. A summary of the data you entered will appear on the screen and you will have an opportunity to change and data that was entered incorrectly. If all the data is correct, enter 'n' to the prompt and the /net/self file will be established.

4.3.2 mkcon

For each server node in the network perform the following:

1. For EACH consumer node which is to have access to this server enter the following command:
   
   `mkcon -c consumer name consumer password 1 (cr)`

   (example session: mkcon -c books secret 1
    mkcon -c cash money 1)
NOTE

"\*" for the consumer name means all consumer names, "\*" for
the password means no password checking.

2. If you make a mistake in an entry, remove the entry by entering the following
command:

```
rmcon -c node name of incorrect entry node password
of incorrect entry<cr>
```

You may then re-issue the command in step 1 to make the correct entry.

3. Make an entry for each consumer to be served by this server.

4.3.3 mkns

Mksel must have been executed on the node to contain the master nameserver
database (/net/data) before performing this step. Mkns will create the master
copy of /net/data.

1. At the node which is to contain the master nameserver database enter

```
mkhs<cr>
```

2. At the “Service requested” prompt enter: addname<cr>

3. The next prompt is for the entity name

```
node name/process name<cr>
```

where node name is the name assigned to a node on the network

process name is either nfs (XENIX server) or nfc (XENIX consumer)

(example: folks/nfs)

4. You are then prompted for the entity type

```
XENIX<cr> for a XENIX node
MSDOS<cr> for MS-DOS nodes
RMX<cr> for RMX nodes
```

5. The system will ask if you want to enter address information now, enter 'y'

When prompted for the port ID of the process,

```
8100 if the process name was nfc on XENIX node
```

```
8000 if the process name was nfs on a XENIX node
```

```
1111 for MSDOS nodes
```

6. You are then prompted for the ETHERNET address. Enter the address you

recorded for the node you specified in step 3.

NOTE

For an MS-DOS system, the ETHERNET address can be obtained
by inspecting the Ungermann Bass card. It will contain a label with
a five digit decimal number. Convert this number to a four digit hexa-
decimal value and form an address of the following format:

00DD00xxxx00, where xxxx is the four digit hexadecimal value.

7. You will now be back at the “Service requested” prompt. Repeat the above
procedure for each process which is to be defined in the nameserver database.
(If a node is both a server and consumer, the addname function must be per-
formed twice for that node.) For a description of the mkns functions see the
XENIX Networking Software User’s Guide.
4.3.4 Enabling the Network

1. Activate the server process on all nodes.
   At every node enter: `nfs on<cr>`

2. At the node containing the master /net/data file, activate the consumer.
   Enter: `nfc on<cr>`

3. From the node containing the master copy of /net/data, copy it to each node
   on the network by entering:
   `cp /net/data //node/name/net/data<cr>`
   Repeat this step for each node on the network.

4. Activate the consumer process at each node which is to be a consumer by
   entering:
   `nfc on<cr>`
   at each consumer node.

5. The network is now functional. You may test the operation of your network
   by going to a node and giving a command which is to access resources on a
   different node.
   Example: `lc // <remote node name>/etc`

The user and group definitions must now be established before the network
is ready for use. Proceed to Chapter 5 for instructions on how to establish the
user and group definition files.
5.1 Introduction

The procedure to be followed in establishing the network /etc/passwd and /etc/group files depends on whether it is a new installation (i.e., no /etc/passwd or /etc/group files exist) or you are installing XENIX Networking Software on XENIX nodes that already have established these files. This chapter describes both procedures.

5.2 New Installation

Before you can establish the /etc/passwd file and /etc/group file it is necessary to have a list of the users you wish to define on the network, along with the names of the groups you wish to assign them to. Mkuser will build the appropriate entry in both the /etc/passwd file and in the /etc/group file. You may abort this utility without affecting any files by either pressing the BREAK key at any time prior to confirmation of the entries, or by entering 'q' or 'quit' in response to a prompt.

1. At the node which is to contain the master copy of /etc/passwd and /etc/group enter: mkuser

2. You will be prompted for the following information:
   - login name (of new user you are adding)
   - group to which new user is being assigned
   - new user's password
   - type of shell the new user requires
   - comments

   You will also be prompted for the node name on which the new user's default home directory is to be located. The prompt for this node name is:

   Enter machine name:

3. Nothing is updated on the system until you confirm the correctness of your responses. You will be prompted for this confirmation once all other prompts have been answered.

4. When you have finished defining the users on your network, enter the following commands to copy the network user and group definition files to all nodes on the network:

   cp /etc/passwd //target node/etc/passwd
   cp /etc/group //target node/etc/group

   Repeat these commands until each node on the network has received a copy of the passwd and group file.

5. Terminate the server process at those nodes which are NOT intended to be server nodes by entering:

   nfs off

5-1
This completes the installation and configuration procedure. At this point the network is fully operational and all nodes may be placed in multi-user mode. For additional information, refer to the XENIX Networking Software User's Guide.

5.3 Existing XENIX Systems

Since existing XENIX systems already have an /etc/passwd file and an /etc/group file established, it is necessary to combine all the passwd files into one consistent /etc/passwd file, and combine all the group files into one consistent /etc/group file. This is accomplished via the utilities mguser and mggroup. These utilities take existing passwd or group files as input and build two files: a merged file containing those entries which did not create inconsistencies, and an error file containing any entries which would cause duplicate names or IDs. You will need to examine the error file(s) and make the corrections necessary to resolve the inconsistencies. If a user's name, group name, UID or GID changes as a result of any inconsistency keep a record of those which have changed, noting both the previous values and the new values, as well as the node on which the user or group originally resided. This information will be needed later as input to the utilities chuid, chgid, and chmem.

NOTE

The order in which these utilities are invoked is important. Mguser must be invoked first. It is repeatedly invoked until all inconsistencies are found. If inconsistencies are found the utilities chuid and chmem are invoked. Then the utility mggroup is invoked. As with mguser, mggroup must be repeatedly invoked until all inconsistencies are found. Following this, the utility chgid is invoked if there were changes made in the assignment of group IDs.

5.3.1 Invoking mguser

1. To invoke the mguser utility enter: mguser

2. The first two prompts are:
   
   Enter new password filename:
      enter <cr> to create the default password file /tmp/passwd
   
   Enter error filename:
      enter <cr> to create the default error file /tmp/pwdup

3. The next set of prompts are:

   Enter filename:
      Enter the full network pathname of the passwd file you wish to use as the basis for your network passwd file. (The entries in this first file will automatically be placed in the network passwd file.)

   Enter machine name:
      Enter the name of the node on which the users in the above passwd file reside.

   This set of prompts will be repeated up to 10 times. Enter each node's passwd file name and the associated machine name until all files being merged have been entered (or the limit of 10 is reached, whichever comes first). When they have all been entered, respond with <cr> in response to the “Enter filename” prompt.
4. If the message "Error file /tmp/pwdup written" appears, then duplicate user
definition entries were found. Additional steps must be taken to resolve
the conflicting entries. If the message did not appear, each user and user ID en­
countered was unique and you may proceed to step 10.

5. Using an editor, examine the file /tmp/pwdup. You will see pairs of entries. The
entry preceded by 'A' was added to the /tmp/passwd file, while the entry
preceded by 'X' was not.

The following user names are special system user IDs and should remain local
users only. Delete any entry pairs having the following user names:

- root
- cron
- bin
- uucp
- sys
- asg
- sysinfo
- network
- demo
- who

6. Any remaining entry pairs in /tmp/pwdup represent conflicting entries which
must be resolved.

For each entry pair, compare the user name and the user ID of the 'X' entry
to that of the 'A' entry. These two entries have either identical user names
and/or user ID numbers. To resolve the inconsistency you must either make
the 'X' entry a new user on the network (see step a), or make the two users
from the 'X' entry and the 'A' entry the same user (see step b).

a. Record the user name, the user ID (found in the third field of the record),
and the machine name of the 'X' entry.

If the user name is identical in both entries, change the one in the 'X'
entry to a user name not already being used.

If the user ID is identical in both entries, change the one in the 'X' entry
to a value not already being used.

(You may wish to examine /tmp/passwd to see what names and values
are in use).

Record the new user name and/or new ID value beside the old values
which you have already recorded.

Delete the 'A' entry for this pair and the blank line which follows it.

On the 'X' entry of this pair, delete the 'X', the last semicolon, and every­
thing to the right of the last semicolon.

For example, the X-A pair:

```
xuser joe:xhuqprldxzi:301:110:Joe \ 
Smith@cash:/usr/joe;cash: /cash/etc/passwd
Auserx:tqhdwxpve:301:121:Sam Sludge \ 
@folks:/usr/joe;folks:/folks/etc/passwd
```

might result in the following single entry:

```
userjoe:xhuqprldoi:350:110:Joe Smith \ 
@cash:/usr/joe
```

b. If the user name is different in the two entries, record the old user name
(from the 'X' entry) and the new user name (from the 'A' entry).

If the user ID is different in the two entries, record the old user ID (from
the 'X' entry) and the new user ID (from the 'A' entry).

Record the node name of the machine on which the old user name/ID
resides.

Delete the 'X' and 'A' entry pair for this user and the blank line which
follows it.
7. You are now ready to merge this edited version of the /tmp/pwdup file with the network password file which was created in /tmp/passwd.

Enter the following commands:

```
mv /tmp/passwd /tmp/passnet
mv /tmp/pwdup /tmp/dupnet
```

8. To execute mguser again, enter `mguser`

Respond to the prompts as follows:

1. **Enter new password filename:**
   - `enter` to create the default password file /tmp/passwd

2. **Enter error filename:**
   - `enter` to create the default error file /tmp/pwdup

3. **Enter filename:**
   - `enter /tmp/passnet`

4. **Enter machine name:**
   - `enter name of node from which you are working`

5. **Enter filename:**
   - `enter` (cr)

9. If the message “Error file /tmp/pwdup written” appears it means that there are still inconsistencies within the user definitions you have provided.

   Return to step 5 and repeat the process in steps 5 through 9.

10. If more than 10 systems are in the network, repeat steps 1 through 9 to merge those remaining password files with the data in the new network password file, /tmp/passwd.

### 5.3.2 Invoking chuid

If conflicts in the user ID values were found in step 6 (above), the chuid utility may be invoked to correct the user ID information on those files owned by the user whose ID was changed (the ‘X’ entry). If no conflicts in user ID values were identified, proceed to the chmem utility.

1. If you have only a few users whose ID value was changed, you may invoke chuid via a command line of the following format:

   ```
   chuid olduserID newuserID //node name on which olduserID resides
   ```

   Repeat the above command for each user whose ID value was changed.

2. If there are several users whose user ID was changed, proceed as follows.

   Using an editor, create a file which contains an entry (one per line) for each user whose ID value was changed. Each entry must have the following format:

   ```
   olduserID newuserID //node name on which olduserID resides
   ```

   After all the needed entries have been placed in the file, enter:

   ```
   chuid name of file you created
   ```
5.3.3 Invoking chmem

If conflicts in user names were identified during mguser, the chmem utility must
be invoked to update the appropriate group file. If no conflicts in user names were
identified, proceed to the mggroup utility.

1. If you have only a few users whose user name was changed, go to the node
where the user resides and enter the following:

```
chmem old user name new user name
```

Repeat this step for each user whose user name was changed.

2. If there are several users whose user name was changed, RESIDING AT THE
SAME NODE, proceed as follows.

At the node where these users reside, create a file which contains an entry
(one per line) for each user whose user name was changed. Each entry must
have the following format:

```
old user name new user name
```

After all the needed entries FOR THIS NODE have been placed in the file,
enter:

```
chmem name of file you created
```

Repeat this step for each node on which user names were changed.

5.3.4 Invoking mggroup

1. To invoke the mggroup utility enter:

```
mggroup
```

2. The first two prompts are:

```
Enter new group filename:
```
enter [cr] to create the default group file /tmp/group

```
Enter error filename:
```
enter [cr] to create the default error file /tmp/grpdup

3. The next set of prompts is:

```
Enter filename:
```
Enter the full network pathname of the group file you wish to use as the basis
for your network group file. (The entries in this first file will automatically
be placed in the network group file.)

```
Enter machine name:
```
Enter the name of the node on which the groups in the above group file reside.
This set of prompts will be repeated up to 10 times. Enter each node's group
file name and the associated machine name until all files being merged have
been entered (or the limit of 10 is reached, whichever comes first). When they
have all been entered, respond with <cr> in response to the “Enter file-
name:’” prompt.

4. If the message “Error file /tmp/grpdup” appears then duplicate group defi-
nition entries were found. Additional steps must be taken to resolve the con-
flicting entries. If the message did not appear, each group and group ID
encountered was unique and you may proceed to step 10.

5. Using an editor, examine the file /tmp/grpdup. You will see pairs of entries.
The entry preceded by 'A' was added to the /tmp/group file, while the entry
preceded by 'X' was not.
The following group names are special system group IDs and should remain local. Delete any entry pairs having the following group names:

- root
- cron
- bin
- uucp
- sys
- asg
- sysinfo
- network
- demo
- who

6. Any remaining entry pairs in /tmp/grpdup represent conflicting entries which must be resolved.

For each entry pair, compare the group name and the group ID of the 'X' entry to that of the 'A' entry. These two entries have either identical group names and/or group ID numbers. To resolve the inconsistency you must either make the 'X' entry a new group on the network (see step a), or make the group members from the 'X' entry part of the 'A' entry group (see step b).

a. Record the group name, the group ID (found in the third field of the record), and the machine name of the 'X' entry.

   If the group name is identical in both entries, change the one in the 'X' entry to a group name not already being used.

   If the group ID is identical in both entries, change the one in the 'X' entry to a value not already being used.

   (You may wish to examine /tmp/group to see what names and values are in use).

   Record the new group name and/or new ID value beside the old values which you have already recorded.

   Delete the 'A' entry for this pair and the blank line which follows it.

   On the 'X' entry of this pair, delete the 'X', the last semicolon, and everything to the right of the last semicolon.

   For example, the X-A pair:

   Xproja::125:tom,dick,harry;cash://cash/etc/group
   Afms::125:paul

   might result in the following single entry:

   proja::134:tom,dick,harry

b. Record all the group member names in the 'X' entry which are to be placed in the list of group members for the 'A' entry. Also record the group name, group ID, and machine name from the 'X' entry.

   Delete the 'X' and 'A' entry pair for this group and the blank line which follows it.

   Using an editor, examine the /tmp/group file which was just created. Find the entry for the 'A' group and add the additional members to the list of members in this entry.

7. You are now ready to merge this edited version of the /tmp/grpdup file with the network group file which was created in /tmp/group.

   enter the following commands:

   ```
   mv /tmp/group /tmp/groupnet
   mv /tmp/grpdup /tmp/netdup
   ```
8. To execute mggroup again, enter `mggroup<cr>`

   Respond to the prompts as follows:

   **Enter new group filename:**
   enter `<cr>` to create the default group file `/tmp/group`

   **Enter error filename:**
   enter `<cr>` to create the default error file `/tmp/grpdup`

   **Enter filename:**
   enter `/tmp/groupnet<cr>`

   **Enter machine name:**
   enter `name of node from which you are working<cr>`

   **Enter filename:**
   enter `<cr>`

9. If the message “Error file /tmp/grpdup written” appears it means that there are still inconsistencies within the group definitions you have provided.

   Return to step 5 and repeat the process in steps 5 through 9.

10. If more than 10 systems are in the network, repeat steps 1 through 9 to merge those remaining group files with the data in the new network group file, `/tmp/group`.

### 5.3.5 Invoking chgid

If conflicts in the group ID values were found in step 6 (above), the chgid utility must be invoked to correct the group ID information on those files owned by the group whose ID was changed (the ‘X’ entry). If no conflicts in group ID values were identified, proceed to the section entitled “Completing the Process”.

1. If you have only a few groups whose ID value was changed, you may invoke chgid via a command line of the following format:

   ```
   chgid oldgroupID newgroupID //node name on which oldgroupID resides<cr>
   ```

   Repeat the above command for each group whose ID value was changed.

2. If there are several groups whose group ID was changed, proceed as follows.

   Using an editor, create a file which contains an entry (one per line) for each group whose group ID was changed. Each entry must have the following format:

   ```
   oldgroupID newgroupID //node name on which oldgroupID resides/
   ```

   After all the needed entries have been placed in the file, enter:

   ```
   chgid name of file you created<cr>
   ```

### 5.3.6 Completing the Process

1. Verify the correctness of the user and group definitions found in `/tmp/passwd` and `/tmp/group`.
2. From the node on which these files reside, copy the files to all nodes on the network:

```
cp /tmp/passwd //target node/ /etc/passwd
```

```
cp /tmp/group //target node/ /etc/group
```

Repeat these commands until every node on the network has a copy of the network passwd and group file.

Be sure to copy /tmp/passwd and /tmp/group to the /etc/passwd and /etc/group file on the node you are logged in on.

3. Terminate the server process at those nodes which will not be server nodes by entering:

```
nfs off
```

This completes the installation and configuration procedure. At this point the network is fully operational and the nodes may be placed in multi-user mode. For additional information on the use and administration of the network, refer to the *XENIX Networking Software User's Guide*. 
### iSBC 552 Jumper Configuration List

<table>
<thead>
<tr>
<th>E1-E2</th>
<th>E72-E57</th>
</tr>
</thead>
<tbody>
<tr>
<td>E5-E6</td>
<td>E74-E59</td>
</tr>
<tr>
<td>E7-E8</td>
<td>E76-E51</td>
</tr>
<tr>
<td>E11-E12</td>
<td>E77-E62</td>
</tr>
<tr>
<td>E13-E14</td>
<td>E78-E63</td>
</tr>
<tr>
<td>E17-E18</td>
<td>E79-E64</td>
</tr>
<tr>
<td>E19-E20</td>
<td>E81-E66</td>
</tr>
<tr>
<td>E23-E24</td>
<td>E82-E67</td>
</tr>
<tr>
<td>E25-E26</td>
<td>E83-E68</td>
</tr>
<tr>
<td>E28-E29</td>
<td>E84-E69</td>
</tr>
<tr>
<td>E30-E31</td>
<td>E85-E66</td>
</tr>
<tr>
<td>E34-E35</td>
<td>E88-E89</td>
</tr>
<tr>
<td>E37-E38</td>
<td>E95-E96</td>
</tr>
<tr>
<td>E41-E55</td>
<td>E98-E99</td>
</tr>
<tr>
<td>E44-E58</td>
<td>E91-E92</td>
</tr>
<tr>
<td>E46-E60</td>
<td>E105-E110</td>
</tr>
<tr>
<td>E50-E65</td>
<td>E119-E127</td>
</tr>
<tr>
<td>E71-E56</td>
<td>E120-E128</td>
</tr>
</tbody>
</table>

### Diagram

![Diagram of the iSXM 552S Jumper Configuration](image)
REQUEST FOR READER'S COMMENTS

Intel's Technical Publications Departments attempt to provide publications that meet the needs of all Intel product users. This form lets you participate directly in the publication process. Your comments will help us correct and improve our publications. Please take a few minutes to respond.

Please restrict your comments to the usability, accuracy, readability, organization, and completeness of this publication. If you have any comments on the product that this publication describes, please contact your Intel representative. If you wish to order publications, contact the Intel Literature Department (see page ii of this manual).

1. Please describe any errors you found in this publication (include page number).

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

2. Does the publication cover the information you expected or required? Please make suggestions for improvement.

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

3. Is this the right type of publication for your needs? Is it at the right level? What other types of publications are needed?

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

4. Did you have any difficulty understanding descriptions or wording? Where?

________________________________________________________________________
________________________________________________________________________
________________________________________________________________________

5. Please rate this publication on a scale of 1 to 5 (5 being the best rating.)

---------------------------------  ---------------------------------
NAME       DATE

TITLE

COMPANY NAME/DEPARTMENT

ADDRESS

CITY       STATE       ZIP CODE       (COUNTRY)

Please check here if you require a written reply.  

WE'D LIKE YOUR COMMENTS ... 

This document is one of a series describing Intel products. Your comments on the back of this form will help us produce better manuals. Each reply will be carefully reviewed by the responsible person. All comments and suggestions become the property of Intel Corporation.

BUSINESS REPLY MAIL
FIRST CLASS PERMIT NO. 1040 SANTA CLARA, CA
POSTAGE WILL BE PAID BY ADDRESSEE

Intel Corporation
Attn: Technical Publications M/S DV2-291
2402 West Beardsley Road
Phoenix, Arizona 85027