XEROX

Network Administration Library
Guide to System Administration Activities

Version 5/88
610E09020

Changes are periodically made to this document. Changes, technical inaccuracies, and typographic errors will be corrected in subsequent editions.

The content of this book is based on the Services 11.0 Release.

A Customer Comment Form is provided in this Network Administration Library. If this form has been removed, address comments to:

Xerox Corporation
Attn: Product Education (N1-12)
701 S. Aviation Blvd.
El Segundo, California 90245

Warning: As to equipment manufactured prior to October 1, 1983, such equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instructions manual, may cause interference to radio communications. As permitted by regulation, it had not been tested for compliance with the limits for Class A compliance with the limits for Class A computing devices pursuant to Subpart J of part 15 of FCC rules, which are designed to provide reasonable protection against such interference. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

As to equipment manufactured after October 1, 1983, such equipment complies with the requirements in Part 15 of FCC Rules for Class A computing devices. Such equipment generates, uses, and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC Rules, which are designed to provide reasonable protection against such interference when operated in a commercial environment. Operation of this equipment in a residential area is likely to cause interference, in which case the user, at his own expense, will be required to take whatever measures may be required to correct the interference.

Table of contents

List of figures

List of tables

Preface

Purpose

The *Guide to System Administration Activities* describes all that you need to know to set up and maintain your network services. For each service, this book provides the following information:

- An overview of how the hardware and software works
- A list of the depedencies and limitations
- Your duties as System Administrator
- Guidelines for setting up the service
- Guidelines for maintaining the service
- Instructions for filling out the service-related worksheet

Intended audience

This book is intended for System Administrators who are responsible for starting up and keeping the network services running efficiently.

1. Introduction

The *Guide to System Administration Activities* contains all the information you need to know before you can perform the installation, set up, and maintenance procedures for the services on the Xerox network. Read this book carefully. It tells you how to plan for installation, setup, and maintenance.

An important part of the *Guide to System Administration Activities* are the worksheets for each service. Use the information in the guide to fill out the worksheets before you begin any service operations. The worksheets help to organize your network information, keep an up-to-date log of your services and server performance, and perform your System Administration duties.

System Administrator duties

The System Administrator has responsibility for network management. Duties include:

- Installing and setting up your services
- Adding new services or servers
- Performing regularly scheduled backups for particular services
- Maintaining your services by deleting services from servers, adding new users, expanding databases, and so on
- Troubleshooting your network as necessary

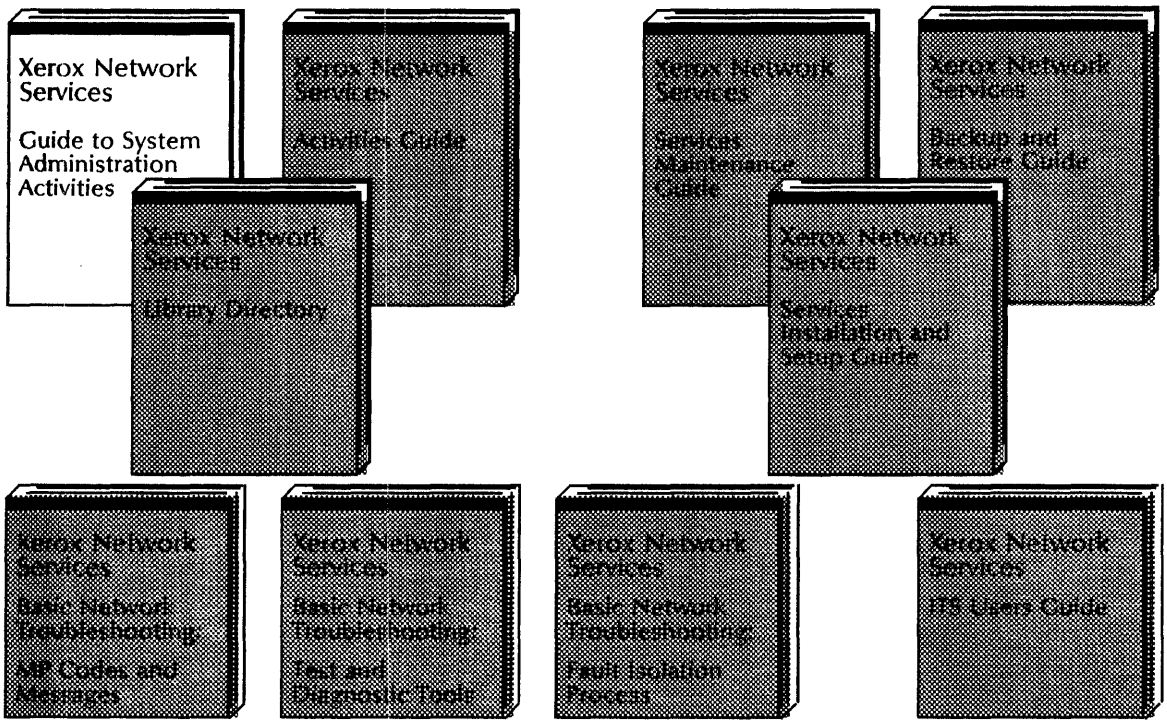
These duties can be regularly scheduled (backup) or unscheduled (renaming a service). Use this book to understand the particular tasks you need to be doing, and the steps and parameters involved. With this understanding, you can plan your activities.

See the *Backup and Restore Guide* and *Basic Network Troubleshooting* for specific information and procedures for backup, restore, and troubleshooting activities.

Network Administration Library organization

The *Guide to System Administration Activities* is one of the books that make up the Network Administration Library (Figure 1-1).

Figure 1-1. **Network Administration Library organization**



Reference books

These books contain information on network planning, network growth, and services.

- *Guide to System Administration Activities* - Helps you, the System Administrator, organize and control your installation, setup, and maintenance activities. This book is required reading for successful network administration.
- *Activities Guide* - A blank folder for storing your completed worksheets, and Remote System Administration logs.
- *Library Directory* - Contains the cumulative index for the Network Administration Library, a summary of services commands, a summary of services procedures, and a glossary.

Procedural books

These books contain complete procedures for the installation, setup, maintenance, backup, restore, and troubleshooting activities associated with each service.

- *Services Installation and Setup Guide* - Helps you install and set up your services.
- *Services Maintenance Guide* - Contains step-by-step procedures for routine and nonroutine maintenance tasks associated with your services.
- *Backup and Restore Guide* - Contains step-by-step procedures for your backup and restore tasks.
- *Basic Network Troubleshooting* - Contains step-by-step procedures and task-related information that help you identify, locate, describe, or solve a network services problem; or

prepare to contact service or the System Customer Support Center. *Basic Network Troubleshooting* is composed of these three inter-related books:

- *MP Codes and Messages* - Lists the problem messages and maintenance panel codes that are displayed on your maintenance panel or server terminal. This book includes remedial steps for each code or message, and may direct you to one of the other books in the *Basic Network Troubleshooting* set.
- *Fault Isolation Process* - Contains trouble isolation steps and remedial actions as directed from *MP Codes and Messages.*
- *Test and Diagnostic Tools* - Contains diagnostic tests and recovery procedures as directed from *Fault Isolation Process* and *MP Codes and Messages.*

How to use this book

Because each service is unique, each chapter in this guide has a slightly different organization. The Services System Software chapter, for example, contains a section about general services software conventions. However, most chapters include the following sections, when applicable.

Contents

Each chapter in this book is organized for ease of use. Before you begin to use the procedures in this book, familiarize yourself with the contents of a typical service chapter.

Service description

The chapter introduction briefly describes the service, how it works.

System Administrator duties and responsibilities

This section lists the general duties that should concern you as the System Administrator when working with the particular service. For each service, the duties include filling out worksheets for service-specific information, installing the service, setting it up, and ensuring that the service is properly maintained as necessary.

Planning for installation

This section discusses configuration information that you need to decide before installing your service. It also reviews the hardware and software requirements, service dependencies and limitations, and filling out the worksheet.

Planning for setup

This section discusses the parameters and other information you need to know and decide upon before you set up your service.

As you read the discussions about service setup, record the information you need on the worksheets. The worksheets will serve as aids when you begin the actual installation and setup.

Planning for maintenance

Some services have activities that you should perform regularly, such as monitoring your database size. This section explains the parameters you need to consider when setting up a schedule for these activities.

However, most of the procedures you perform as System Administrator are unscheduled activities. For example, these procedures include renaming a service or adding mailboxes for new users. This section tells you why to perform a procedure, when, and how to do it most efficiently.

Worksheets

The worksheets you use for each service are included at the end of each chapter. Follow the detailed instructions in each chapter to fill out the worksheets before you begin to work with any service. When properly filled out, these worksheets contain information you need to know as you set up and configure your services.

Make copies of each worksheet. When the services are up and running, keep the filled-out copies in the *Activities Guide* near your server. The worksheets serve as a reference for the information you used to configure your services, in case you need to enter it again. As server information changes, use Remote System Administration to make copies of the server and service-related information for your records. For more information about Remote System Administration, see Chapter 2, Network Overview.

Documentation conventions

The books in the Network Administration Library use these conventions to help you recognize information.

⇐|	This symbol means "press RETURN." When you see it after a procedural step, press the RETURN key on the terminal keyboard.
BREAK	Words appearing in all capital letters represent the keys or switches on your equipment.
<service name>	Words appearing in angled brackets represent system-supplied information.

WARNING: Warnings appear immediately before any action that may cause physical harm to you or your equipment. Make sure you understand the warning before you perform the step.

CAUTION: Cautions appear immediately before any action that may destroy the data stored on your network. Make sure you understand the potential impact of the action before you perform it.

Notes are helpful hints that help you perform a task or understand the text.

This symbol means that you can perform the procedure from a workstation using Remote System Administration (RSA). If you need to record any information while performing the procedure, you can use the RSA Make Document (or Make Screen) feature.

2. Network overview

This chapter is a basic introduction to your network. It briefly describes:

- The devices that can reside on the network, and how they communicate
- The services available to you and your site, including communication options
- Network management, including your major duties as a System Administrator
- Network hardware requirements and options
- Remote System Administration capabilities and use

Network devices and communication

The Xerox local area network is based on a coaxial cable, or other medium called Ethernet. This industry-standard network transmits information at high speeds, while providing a flexible, low-cost connection between workstations and shared servers. A server supplies a service, such as filing or printing, to network users.

Workstations and servers need not reside in the same building or the same city. The Xerox Network System (XNS) supports the interconnection of networks in different locations to create a single internetwork. On an internetwork, all elements attached to any of the interconnected networks can communicate with each other.

Your organization may have a single Ethernet network or multiple interconnected Ethernet networks forming an internetwork. As System Administrator, you are responsible for maintaining all the servers connected to your local Ethernet network and for supporting all the people using workstations at your site. If your Ethernet network is part of an internetwork, System Administrators at other sites are responsible for the servers and workstations users on their Ethernet networks.

Your Ethernet network may also support users of personal computers or terminals that are not physically connected to it. These users may be traveling, working at home, or working in small branch offices. They can connect their non-networked devices to modems to establish temporary, dial-up sessions with some of the network services.

For the most part, the network services work on their own to integrate your site and provide your organization with a variety of shared resources and means for sharing information. As System Administrator, you also install, set up, and ensure day-to-day operation of the services running on your servers.

Servers

A server is a device connected to the Ethernet that supplies a service to network users. "Server" refers to the hardware; "service" refers to the software providing a particular shared resource. Many workstations can use and share the services running on a single server.

Each installation of a Xerox Network System includes at least one Xerox server dedicated to the support of one or more services. Some servers are configured to support just one service, especially a high-volume service such as printing. Other servers can support many functions. Certain workstations can function as servers, given the right software and peripheral hardware.

For descriptions of the individual services, see "Network services" later in this chapter.

Workstations

Your network can include any combination of these workstations:

- The 6085 Professional Computer System and the 8010 Information Processing System are powerful, versatile workstations. These workstations provide easy-to-use graphic interfaces that allow switching among multiple tasks. They support document preparation and illustration, electronic mailing, terminal emulation, Remote System Administration, electronic spreadsheets, and many other activities.
- The Xerox 6060 series of personal computers (PCs) and the 850/860 Information Processing System support document preparation; electronic mailing, filing, and printing; and terminal emulation.
- The 820-II Personal Computer is a CP/M-based microcomputer that can be used as a network workstation. This workstation supports electronic mailing, filing, and printing, as well as other network capabilities.
- The IBM PC is a DOS-based microcomputer that can be used as a network workstation when equipped with an Ethernet interface board. The IBM PC supports electronic mailing, filing, and printing, as well as terminal emulation.
- The DEC VT100 and VT52 terminals can be used for filing, printing, and other tasks if the VAX has XNS/DEC VAX software configured and running.

Each type of workstation features different hardware, operating systems, and application software. Nonetheless, users at any workstation can efficiently share and exchange information regardless of geographic location.

Workstations and personal computers connected to the network retain their independence, reliable operation, and unique applications. Access to network services helps extend the power of these devices.

Relationship between servers and workstations

The server's central processing unit, memory, and other computing resources are independent from those of the

workstations. Peak server use has no effect on workstation performance.

A problem at the server affects only the services running there; workstations used for other activities are unaffected.

Servers and services are continuously available for processing requests from workstations and remote dial-in users. Workstations prepare and send requests from users initiating activities that require action from one or more network services. To the user, this sequence of network communications seems automatic and instantaneous.

Workstation users can take advantage of network resources and information exchange without memorizing complex pathnames, command sequences, naming schemes, and procedures. The communication software resident on all networked servers and workstations simplifies network tasks for these users.

Non-networked devices and compatibility services

Your network can also include other types of computing devices that are not directly compatible with the Xerox Network System. The Xerox Network System is designed to accept information from these computing resources, thus creating an open network. Your organization can use both Xerox network architecture and other systems that provide applications and programming environments.

To support the open network, Xerox has developed a family of compatibility services. Compatibility services act as gateways between networked and non-networked mainframe and personal computers.

These services perform terminal emulation, document transfer, and network access functions. Information originating on non-networked devices can be moved to and from the Xerox Network System.

Xerox Network System communication

Xerox Network System protocols specify the conventions and formats for communication between devices. Servers and workstations that use these protocols are called network citizens. Devices not directly compatible with these protocols are called non-citizens.

Communication is not limited to data transfer. Communication also defines the specific activities that services carry out for their clients.

The term client refers to the workstation or compatible service directing a user's request to a service. When many services work together to complete an operation, services are clients of each other. Compatibility services can also be clients.

The automatic client-to-service and service-to-service communication that characterizes the Xerox Network System enables users to work independently and efficiently. The network architecture that defines communication conventions for workstation and services, along with the services themselves, forms the backbone for integrating all devices and sites on the network.

Network services

A network service is the software that makes a shared resource available to network citizens. A printer or a large filing system is an example of a primary resource. A directory or a mail service is an example of a support resource.

There are three groups of services:

- **Basic services** are the fundamental network services. They enable you to run your server, and to mail, file, and print information.
- **Communication services** support communication in the internetwork, between networks, and between networked and non-networked devices.
- **Utilities services** monitor network activity and provide information for network management and troubleshooting.

The following sections briefly describe the services software that can run on your servers. For more detailed information, see the service-specific chapters in this book.

Basic services

Basic services are fundamental to the operation of single-server networks, multiple-server, and interconnecting networks.

Services System Software

The Services System Software is required software that runs your server. It includes the operating system for the server and the software that supports the services. The Services System Software supports installation, configuration, and operation of multiple services on a server. It also contains the communication software the services use to access other services on the same or a different server.

You must install Services System Software on all servers, regardless of their function.

Clearinghouse Service

The Clearinghouse Service joins the Services System Software in providing a foundation for the other network services. The Clearinghouse contains information about the network community including users, servers, services, and service-managed resources. You name all these network entities and register them in the Clearinghouse, creating a system-wide network directory.

All services find the information they need, such as a mailbox location or file drawer location, through the Clearinghouse. The Clearinghouse also authenticates users when they access the network, providing network security.

The Clearinghouse Service requires a File Service for backing up its database. The two services need not reside on the same server, but should be on the same network.

You do not need to install a Clearinghouse Service on every server, but every network must have access to a Clearinghouse. As your network grows, you can easily add more Clearinghouses. The multiple Clearinghouses automatically share information among themselves, forming a single system of accurate information about all network resources.

Mail Service

The Mail Service is an electronic post office enabling quick communication between network users. Users can send plain text messages or complex documents including graphics to any users registered in the Clearinghouse Service.

The Mail Service requires a File Service for backing up its database. The two services need not reside on the same server, but should be on the same network.

The External Mail Gateway option of the Mail Service enables users to transmit to and receive messages from a remote network community. With this option, two separate networks can exchange information without using the more costly Internetwork Routing Service circuits.

File Service

The File Service acts as a centralized storage and organization service for files. It lets users store files, documents, and folders produced at any networked workstation or non-networked personal computer. The documents need not be in any particular internal format; format conversion software is available on some networked workstations and at the Interactive Terminal Service.

The File Service supports access controls so you can restrict file access. The File Service is used to back up the Clearinghouse Service, the Services System Software profile, the Mail Service, the Librarian Service, and the Server Monitor Service.

PC File Service

The PC File Service lets networked PC users access files on a network File Service. The PC File Service affords a direct network connection for PCs and workstations. The PC must be running XC20 applications software. The File Service must be on the same server as the PC File Service to allow XNS users access to the PC files and directories stored on the File Service.

Print Service

The Print Service enables users to print documents and folders at any printer on the network. The Print Service supports several printing options, among them electronic and facsimile printers that can produce text integrated with graphics, equations, and multiple-fonts.

Communication services

Network communication services enable users, servers, and services on the internetwork and users of incompatible

computers to share information and resources. The communication services support communication between:

- Local area networks that are not alike
- A local area network and an internetwork
- A local area network and a standalone computer or terminal

All communication gateways have at least two characteristics in common. First, they implement at least two different communication protocols and/or operating system architectures. Second, they perform some sort of protocol conversion.

Protocol conversion may mean accepting information from an IBM network (IBM communication protocol) and converting it to information that a Xerox network understands (Xerox communication protocol). Communication services are complex because some protocol conversions are the sole domain of one service, while other conversions require cooperation between service and workstation software.

A communication gateway includes these components:

- An 8000 or 8090 server
- One or more RS232C ports
- Any modems needed to make a physical connection
- The communication service software
- The workstation software

SNA Mail Relay

The SNA Mail Relay is a group of software products that provide electronic mail exchange between Xerox network system users and IBM SNA distribution services users running DISOSS.

External Communication Service

The External Communication Service (ECS) supports information exchange between Xerox Network System devices and non-Xerox devices. It enables network workstations to access mainframe computers through terminal emulation, and can translate non-Xerox protocols into Xerox protocols.

Two software options are available for the ECS:

- **Asynchronous Communication Protocol** works with the ECS to support sessions in which the workstation emulates a VT100 or standard TTY-compatible terminal. With this emulation protocol on the server and emulation software on the workstation, workstation users can interact with remote hosts. The remote host can be any device attached to a VT100 or TTY-compatible terminal using ASCII Asynchronous protocols.

  The Asynchronous Communication Protocol also enables the ECS to support incoming ASCII asynchronous calls from personal computers or VT100 and TTY-compatible terminals.

- **3270 Communication Protocol** works with the ECS to support emulation of IBM 3270 Binary Synchronous Communication (BSC) and IBM 3270 System Network Architecture (SNA) communication. With this emulation protocol on the server

and emulation software on the workstation, workstation users can interact with IBM mainframe computers.

Internetwork Routing Service

The Internetwork Routing Service (IRS) connects Ethernets to create an internetwork. You must install an IRS on each internetwork being connected.

Two software options are available for the IRS:

- **X.25 Communication Protocol** interconnects Ethernets over leased-line links through a public data network.
- **Clusternet Communication** provides remote workstation users access to network services through a dial-up session.

Interactive Terminal Service

The Interactive Terminal Service enables users of remote personal computers and TTY-compatible terminals to access the network Mail Service, File Service, and Print Service. The Interactive Terminal Service requires support from the External Communication Service with the Asynchronous Communication Protocol option.

Remote Batch Service

The Remote Batch Service (RBS) provides document interchange and file transfer capability among devices using or emulating the IBM 3270 Binary Synchronous (BSC) protocol. The IBM 2770, 2780, and 3780 remote batch terminals use this protocol; other data processing and word processing devices emulate it.

The RBS uses the File Service to store documents to be transmitted as well as documents received from the remote devices.

850/860 Gateway Service

The 850/860 Gateway Service enables standalone 850/860 Information Processing Systems to access the network Mail Service to send and receive documents.

Utilities services

Utilities services let you monitor servers and communication on a network or internetwork. They also enable you to use diagnostics and other utility files over the network.

Server Monitor Service

The Server Monitor Service regularly monitors the availability of one or more servers on the network or internetwork. It keeps a history of server performance and notifies you of any server failures.

The Server Monitor Service requires a File Service for backing up its database. It also requires a Mail Service to send notifications.

Communications Monitoring Service

The Communications Monitoring Service can monitor all the communication services and the Mail Service. The resulting data, stored in a log file on the server, indicates communication service performance and supports troubleshooting.

Boot Service

The Boot Service provides two utilities: the installation utility lets you load network software over the network (called etherbooting); the diagnostics utility lets you access programs to analyze hardware problems. It functions as a remote server, constantly checking the Ethernet for file requests. The Boot Service responds to these requests by sending the required utility files from its database to the requesting device.

Librarian Service

The Librarian Service enables you to set up and maintain a database of network resource information that many users can access simultaneously. For example, the Librarian Service can store information about documents and note when a document is being edited. A user accessing the Librarian Service database can thus discover the current state of the document.

A word about configuring servers and services

Your Xerox Systems Analyst and others at your site have planned which services will run on your server or servers. When planning your network or internetwork configuration, your Systems Analyst considered the following:

- Placement of Clearinghouse Services and replication of domains
- Placement of Mail Services
- Placement of multiple services on a single server
- Coresidency requirements for the External Communication Service and the Internetwork Routing Service
- Coresidency limitations because of local communications port dependencies
- Interservice dependencies

When one service cannot perform a particular function without the help of another service, the first service has a dependency on the other service. Most interservice dependencies require that a certain service reside on a server in the network or on a connected network.

For example, the Mail Service, Interactive Terminal Service, Remote Batch Service, and Server Monitor Service, all have dependencies on the File Service. The File Service must be present somewhere on the internetwork.

When both a service and the service on which it depends reside on the same network, performance and reliability improve. However, such coresidency is rarely required.

Network management

To provide network services to users, you as System Administrator install and maintain the network. Most larger networks require a full-time System Administrator and an assistant who helps maintain the network. The size of the network, the number of users, the services on the network, and the volume of user activity determine your System Administrator duties and schedule.

As you read the service-specific chapters in this book, you will find a section in each chapter that lists your duties. Make sure you develop a schedule for fulfilling your duties that will keep your network functioning and responsive.

In general, your duties fall into four main areas:

- Filling out worksheets
- Establishing naming conventions
- Installing, initializing, and setting up server and services software
- Maintaining and troubleshooting your network

You can perform most procedures at the server, or by using Remote System Administration at your workstation. See "Remote System Administration" later in this chapter.

Filling out worksheets

Each service-specific chapter in this book contains one or more worksheets for that service. You fill out these worksheets before you install, initialize, and set up your software. The values and names you record on the worksheets are required by the software during installation, initialization, and setup. You find all the information you need to know for filling out each worksheet in each service-specific chapter in this book

Among the information you need to know to fill out the worksheets are:

- Ethernet network numbers
- Organization, domain, server and, service names and passwords
- Service database sizes
- Communication port data and characteristics

The worksheets will also come in handy as you maintain your network, change setup information, or add new information on the network. Keep a clean copy of each worksheet in your *Activities Guide* for reference.

Establishing naming conventions

During initialization and setup, you supply names for all the "objects" in your network community. Developing naming conventions that suit your organization is a creative and important activity. Users specify these names to access network resources.

Select names that are clear and unique, and that will be meaningful over time. Names should be easy to remember and easy to type.

To simplify the task of creating new names as the network grows, establish themes for each object type and start a naming tradition. For example, your File Services can have college and university names, such as Yale or USC. Your Print Services can have planetary names, such as Jupiter or Pluto.

Although you can rename most servers and services, try to minimize renaming. You must notify 6085/8010 workstation users when you rename network objects, so the users can retrieve new icons for the objects. Until all users comply, there may be some confusion.

Installing, initializing, and setting up server and services software

After you fill out the worksheets, review the Services System Software chapter in this book. It explains general operating techniques and discusses the Services Executive, which is your primary administration tool.

Then work with your Systems Analyst to install the server and services software and respond to your server's first-time initialization prompts. The Services System Software chapter in the *Services Installation and Setup Guide* provides step-by-step instructions to guide you through this activity.

Next, perform first-time initialization of each service that you installed. Initialization includes naming the service, ensuring that it registers with the Clearinghouse, and providing any additional information required. The first time you run a service, it prompts you for all the initialization information it needs. This information is explained in the service-specific chapters in this book, while the step-by-step procedures are in the service-specific chapter in the *Services Installation and Setup Guide*.

Finally, after running the services for the first time, set them up or configure them. This activity differs for each service. For example, configuring the Mail Service includes creating mailboxes for each user, specifying when the External Mail Gateway is to call other External Mail Gateways, and specifying the phone number the service is to use. The service-specific chapters in this book and the *Services Installation and Setup Guide* help you with these activities.

Maintaining your network

After you install and set up your network resources, you maintain your network as necessary to keep the network operating smoothly.

Performing backup

Backup is a critical aspect of network maintenance. Taking the time to perform regular backups can save you hours of effort and service downtime when data is damaged or lost. The *Backup and Restore Guide* provides information and step-by-step procedures for backing up your server profile, primary and secondary services volumes, Clearinghouse database and domains, and the databases for the Mail Service, Server Monitor Service, and Librarian Service.

Reconfiguring servers and services

As your network grows and your resource needs change, you may need to move services to different servers, add users to Clearinghouse domains, and install new services. For general maintenance procedures for network reconfiguration, see the Services System Software chapter in the *Services Maintenance Guide*. For specific procedures for each service, see the service-specific chapter in the *Services Maintenance Guide*.

Xerox releases new versions of server and services software to improve and extend network performance. The Services System Software chapter in the *Services Installation and Setup Guide*, together with the upgrade kit that accompanies each release, helps you upgrade your servers to new software versions.

Monitoring server and services

Certain services have statistics-gathering functions that enable you to see at a glance how a service is performing. Use the service-specific statistics capabilities to keep an eye on server performance, plan database expansions, and support troubleshooting activities.

Troubleshooting your network

After you install and set up your network resources, you may need to troubleshoot your network to keep it operating smoothly.

Tips and procedures for resolving problems are contained in the three *Basic Network Troubleshooting* books. Book 1 contains maintenance panel codes and service messages. Book 2 provides techniques for isolating network problems. Book 3 contains diagnostic and test procedures you can use to define and resolve problems.

These books are designed to help you identify and locate a network services problem, clearly solve the problem, or prepare to contact Service or the Systems Customer Support Center. This process consists of three phases: identification, level one solution, and level two solution.

The identification phase focuses on identifying and locating a problem and describing it clearly. Identify the problem using problem messages, maintenance panel codes, and task non-performance indicators.

You can research each of these indicators in one or more of the *Basic Network Troubleshooting* books. Problem messages and maintenance panel codes can be researched in *MP Codes and Messages*. Task non-performance indicators can be researched in *Fault Isolation Process*.

Once you have researched the indicators, solutions are available in all three troubleshooting books. *MP Codes and Messages* directs you to specific, level one clearing actions, or further steps in the *Fault Isolation Process*. If the level one solutions do not fix the problem, you are directed to level two solutions in *Fault Isolation Process*, and *Test and Diagnostic Tools*.

Problem Report Form

Use the Problem Report Form to record any problem indicators such as messages, maintenance panel codes, or task non-performance details. The Problem Report Form helps you keep track of your troubleshooting activities, and serves as a record for Xerox personnel, should their assistance be required. The Problem Report Form is at the end of this chapter. Be sure to make a copy of the form before you fill it out.

① Use section ① on the Problem Report Form to enter caller-related information. Fill this section out before you call the Systems Customer Support Center, to have it ready for the Xerox Customer Support Representative. Be sure to enter the Assigned SCSC log number that the Xerox Customer Support Representative will give you when you call in your problem report.

② Use section ② on the Problem Report Form to enter the details about your server. You will need this information when you talk to the Systems Customer Support Center. You can obtain most of this information from the Services Installation Worksheet. You filled out this worksheet in the Services System Software chapter of the *Guide to System Administration Activities*.

③ Use section ③ on the Problem Report Form to describe the network or services problem you are experiencing. You will need this information when you talk to the Systems Customer Support Center.

④ Use section ④ on the Problem Report Form to list the maintenance panel codes, server messages, and task non-performance indicators that may have occurred in conjunction with the problem. You will need this information when you talk to the Systems Customer Support Center.

⑤ Use section ⑤ on the Problem Report Form to record the tests or diagnostics you performed while attempting to isolate, research, or fix the problem. Be sure to note the test indicators in the "Results" section. You will need this information when you talk to the Systems Customer Support Center.

⑥ Use section ⑥ on the Problem Report Form to record the final solution to your problem. Be as specific as possible. This becomes a permanent record of your network's performance and may provide valuable clues for future troubleshooting.

Store your completed Problem Report Forms in the *Activities Guide*.

Network hardware

A suitable operating environment for network services depends on an appropriate hardware configuration. At a minimum, your network needs:

- An 8000 or 8090 server housing the computer and peripherals
- One rigid disk drive with at least 10 Mb capacity
- 512 Kb of real memory
- An attached terminal and keyboard
- A floppy disk drive or cartridge tape drive

Both the 8000 and the 8090 servers run services release versions 11.0 and earlier.

SNA Access and some Print Service configurations require more server memory. Also, performance may suffer with some configurations if you use the 512 Kb server memory size configuration. When configuring your server, keep in mind that 512 Kb of memory is a minimum, any service will perform better on a server with 768 Kb of memory or more.

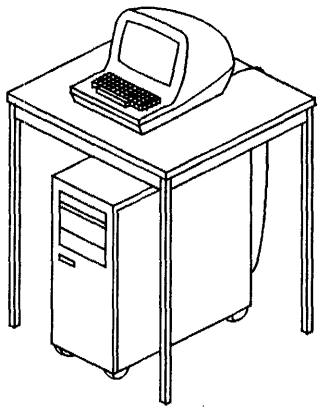
8000 server

The 8000 server supports floppy disks and removable disk drives. It has these components:

- An 8-inch floppy disk drive located within the server unit (1.2 Mb).
- One or more rigid disk drives (fixed or removable disk). The drive options are:
  - A 10 Mb drive, contained within the server unit
  - A 29 Mb drive, this drive is still supported, but no longer sold
  - A 42 Mb drive, contained within the server unit
  - An 80 Mb (T80) removable disk drive, housed in a separate, connected unit; can be configured with up to four drives; called multiple-drive servers
  - A 300 Mb (T300) removable disk drive, housed in a separate, connected unit; can be configured with up to four drives; called multiple-drive servers
- A terminal and keyboard
- An RS232C port connection for communication or attaching printers

Figure 2-1 shows an 8000 server and display terminal.

Fig. 2-1. **8000 server and display terminal**



8090 server

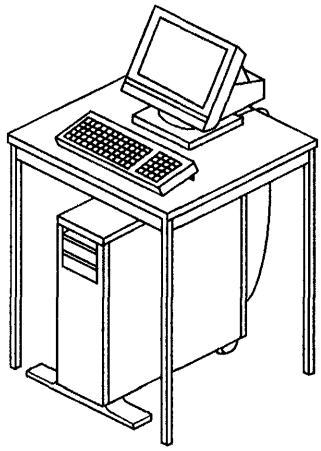
The 8090 server supports cartridge tapes instead of floppy disks and high-capacity cartridge tapes instead of removable disk drives. The 8090 server has these components:

- A central server unit (1.1 Mb, expandable to 1.6 or 3.6 Mb)
- A $5\frac{1}{4}$-inch cartridge tape drive within the server (20 or 80 Mb)
- An input/output (I/O) processor within the server (8085) with 24 Kb RAM and 8 Kb ROM
- A $5\frac{1}{2}$-inch high-capacity disk drive, separate from the server unit (310 Mb)
- A high-capacity tape drive, separate from the server unit (120 Mb)
- A terminal and keyboard
- A high-capacity peripheral connection to the high-capacity disk drive
- An RS232C/RS366 port for communication or attaching printers

The 8090 server supports up to seven high-capacity connections without a laser printer attached, and up to four connections with a laser printer attached.

Figure 2-2 shows an 8090 server and display terminal.

Fig. 2-2. **8090 server and display terminal**



Communication hardware

If you are connecting networks or setting up communication between Xerox and non-Xerox equipment, your configuration needs the appropriate communication hardware.

RS232C Communication Kit

The RS232C Communication Kit provides a single port that is installed on your 8000 or 8090 server. Your server needs this option to support the Telecopier 495-1 printing option of the Print Service or a service that communicates with remote devices using a modem. The 3270 Communication Protocol (IBM 3270 BSC emulation option) of the External Communication Service, the Remote Batch Service, the External Mail Gateway, Internetwork Routing Service, Interactive Terminal Service, and the Gateway Service require the RS232C Communication Kit.

The kit consists of a board and an RS232C connector. When you use the RS232C port to drive a facsimile printer, a ribbon cable connects the port to the printer. When you use the RS232C port for communication, the port is connected to a modem.

Communication Interface Unit

The Communication Interface Unit (CIU) provides four or eight ports in a one-board or two-board configuration, respectively. These additional RS232C ports support one or more External Communication Service options as well as the Internetwork Routing Service.

The CIU is separate from the server and has its own Ethernet transceiver and drop cable. The External Communication Service

manages the CIU ports, and provides the commands you use to set up these additional ports.

Multiport Option Kit

The Multiport Option Kit provides five ports installed on your 8000 or 8090 server. The Multiport Option Kit can control four RS232C ports, one RS366 port for autodialing, and an Ethernet interface on a server. Use the Multiport Option Kit when you are running asynchronous or bisynchronous communication protocols.

The kit consists of a board, RS232C connectors, and supporting software. You install the software from floppy disk or cartridge tape when you install all services on your server.

Modems

If your server is to support a communication service, use a modem to connect a port to the phone or phone jack. The modem transforms computer digital signals to the analog signals used over phone lines, and vice versa.

Remote System Administration

You can perform your administrative tasks at the server running the service. However, when you do not have convenient access to the server, you can use the Remote System Administration (RSA) facility of the network system.

RSA capabilities

Remote System Administration lets you access a server from a 6085/8010 workstation. If you have the Asynchronous Communication Protocol option of the External Communication Service (ECS), you can configure one or more ECS ports to receive incoming asynchronous calls that are answered by the "Greeter." Then you can perform remote administration from your home personal computer.

When you use Remote System Administration, you have access to all the functions available to you at the server terminal. In addition, Remote System Administration enables you to capture the entire session in a document for your records.

You cannot use Remote System Administration for procedures that involve:

- Booting the server
- Installing floppy disks or cartridge tapes
- Performing activities at one of the server's initialization interrupt points (after booting)

If you have more than one server, you can open one remote administration (emulation) window for each server.

Make Document and Make Screen features

The Make Document feature creates a document containing everything that has appeared in the remote administration window since you began your session or last selected Make Document. Use this feature to save a log of your setup activities, service statistics, or any other information.

When you use the Make Document feature, a document appears on your desktop. The document has the emulator's name and a time stamp. You can work with RSA documents as you would any other 6085/8010 document. You may want to rename them, and then store them in a file drawer dedicated to remote system administration information, or save hard copies of them in your *Activities Guide*.

Later, you can use the information in these documents to configure a service on a different server or to modify an existing configuration. You save time by following the sequence of commands you used on a previous occasion. You can also copy text from the document to the remote administration window, saving keystrokes and minimizing errors.

Use the Make Screen feature to save what you see in the remote administration window. This feature is most useful for statistics or status reports that indicate server use or reliability.

For complete information on Remote System Administration, see the Workstation Administration chapter in the *Workstation Administration and System Resources* volume of the VP Series Reference and Procedures Library.

Using remote System Administration

To use Remote System Administration, follow the steps below.

Prerequisites

- If you will be using RSA from a remote personal computer, ensure that the Asynchronous Communication Protocol software is loaded and running in the loader icon.
- Ensure that the Remote System Administration software is loaded and running in the loader icon.
- Ensure that a port icon and a TTY icon are on your desktop.
- Ensure that the Remote Executive option in your server profile is greater than zero. See the "Changing the server profile" section in the Services System Software chapter of the *Guide to System Administration Activities* for information about the server profile.

Step-by-step

1. Copy the Network Management Terminal Emulator TTY icon to your desktop.
2. Open the Network Management Terminal Emulator TTY icon, and then the port icon.
3. Copy the port icon representing the server you want to your desktop.
4. Open the port icon.
5. Select [Start] on the TTY options sheet to begin communication with the server and open a remote administration (emulation) window.
6. Select a location inside the window and begin your session.
7. Perform the System Administration functions just as you would at the server.
8. If the VP Document Editor is running, you can make a copy of all or some of your session. Select [Make Document] or [Make Screen] from the emulation window.

If you use the Make Screen feature, you capture only what is displayed on the screen.

9. When the session is complete, log off the server.
10. Type **Quit** and press RETURN.
11. Select [Close] from the emulation window header.

References

For complete information on Remote System Administration, see the Workstation Administration chapter in the *Workstation*

Administration and System Resources volume of the VP Series Reference and Procedures Library.

For information about loading workstation applications software, see the *ViewPoint* volume of the VP Series Reference and Procedures Library.

For information about TTY emulation, see the VP Terminal Emulations chapter in the *Host Interfaces* volume of the VP Series Reference and Procedures Library.

3. Services System Software

This chapter helps you prepare for installation, setup, and maintenance of the Services System Software. This information supports the procedures you perform from an 8000 or 8090 server.

Description

Each installation of the Xerox Network System includes at least one Xerox 8000 or 8090 server. The Services System Software installed on the 8000/8090 server enables it to act as a server. A server supports one or more of the Xerox Network Services.

How the software works

The Services System Software is part of the Standard Services Software package. This package contains Pilot (the operating system) and server software consisting of software programs that function as an intermediate layer between the operating system and the network services.

Pilot operating system

Pilot is the basic operating system for the 8000/8090 server. It contains the communications software necessary to send and receive information between the server and workstations.

Pilot also enables the server to support many activities at once. Because of this capability and the large server memory, one server can support all the services that a small organization needs.

Pilot manages server memory, files, and network communication. In general, Pilot:

- Allocates disk space to a service as needed and ensures efficient use of available disk space
- Supplies needed memory for large programs and applications
- Enables network services and workstation applications to use Xerox Standard protocols for transmitting and receiving information anywhere on the internetwork

Server software

The server software consists of the programs that function as an intermediate layer between the Pilot operating system and the network services. Required for the operation of all network services, these programs enhance performance and convenience for the services they serve. Server software includes the Services Executive, remote executives, backstop software, services options control, multilingual support software, and online diagnostics.

Services Executive
The Services Executive is used for installing services, and for setting up, maintaining, and troubleshooting the server and services. You, the System Administrator, are the primary user of the Services Executive.

The Services Executive coordinates your input to the services. The executive invokes the service interface you request, making available the service commands for setup and maintenance. It also displays service prompts and messages.

The executive gives access to commands based on whether you are a System Administrator or a user with more limited access. Users with limited access have access only to the commands they need to view the current status of the server or the services that reside on the server.

As System Administrator, you can establish, change, and maintain your server configuration. Administrative commands allow extensive, but not necessarily exclusive, control over all resources on a server.

Not all System Administrators can gain administrative access to all commands at all servers in an internetwork. Each server requires that a logged-on user be enabled with administrative access to the server domain before gaining access to all administrative commands. The server domain is a generally named geographic grouping within the network, over which you are responsible as System Administrator. Not all logged-on users can enable themselves.

Each server uses its own domain name, provided by the System Administrator during server initialization and saved permanently in the server profile, to determine if the user qualifies as a Domain Administrator. See the Clearinghouse Service chapter in this book for information on Domain Administrators and domains.

Remote executives
The Services System Software can support multiple concurrent executive interfaces to a single server. The software always provides one executive at the server's local terminal. You can establish additional, remote executives, from the 6085/8010 workstation, or from dial-up asynchronous personal computers or terminals. Thus you can perform most of your administrative tasks at your desk or from an off-site location.

Interaction with the remote executive is identical to interaction with the local executive. To maintain server security, the same security considerations that prevail at the local executive are enforced at the remote executive.

You can also disallow remote executives altogether, or allow them only at the 6085/8010 workstation. The latter approach enables users to check the status of print jobs or other services without leaving their workstations.

Backstop software
The backstop software automatically recovers the server from power failures and other problems that cause server failure. The backstop software captures the state of the system before the failure, logs the errors that caused the failure, and boots (or restarts) the system software. All active services running before

the failure are loaded into memory and run with the previous configurations.

As System Administrator, you can specify which services installed on a server are activated. These services are added to the active services list, applied each time you or the backstop software boots the server.

Services options control

After the server is booted, the system software determines which services you have purchased for use on that server. If you have not yet configured the server for services, the Services Executive prompts you to enter a configuration password. You get this password from the Xerox Software Control Center.

The system software also enables you to change the options you have set. Each time you change the options, you must supply a new password obtained from the Xerox Software Control Center.

Multilingual support software

The Services System Software includes a mapping capability for supporting keyboard input and service message output in several languages. Each server is purchased with one of the language packages. Message files, which translate server and service messages, are available for each language option.

Online diagnostics

The Services System Software includes a number of status messages, commands, and tests that aid troubleshooting. Many of the tests examine the server floppy and cartridge tape drives, communication hardware, or network function.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Understanding the Services Executive characteristics and conventions as described next in this chapter.
- Completing and maintaining the Services System Software worksheets at the end of this chapter.
- Installing the Services System Software and services software as described in the Server Software Installation chapter of the *Services Installation and Setup Guide*.
- Maintaining the Services System Software as described in the Services System Software chapter of the *Services Maintenance Guide*.
  - Regularly monitoring the disk volume.
- Regularly performing backup as described in the Services System Software chapter of the *Backup and Restore Guide*.
- Notifying users of any change or disruption in the service.
- Upgrading hardware and software as required.
- Troubleshooting the service as described in *Basic Network Troubleshooting*.

You can perform most Services System Software procedures from a workstation using Remote System Administration (RSA).

Characteristics and conventions

Read this section to familiarize yourself with the conventions of the Services Executive. Understanding these conventions before you begin working with the executive will make your job much easier.

Starting a Services Executive session

When you start an Executive session, using the **Logon** command, you are prompted for your name and password. The server checks to see that your name is registered in a Clearinghouse domain and that your password is correct. This process is called "authentication."

If the authentication succeeds, you are granted logged-on status, with access to commands that allow you to affect resources (such as file drawers or services) that you "own" or to which you have access. For example, you can change your password, change the access controls on your file drawers, or add people to user groups you administer.

As System Administrator, you should have Domain Administrator status for one or more Clearinghouse domains. This access allows you to use special commands that maintain the servers on your network. As System Administrator, you need access to the Clearinghouse domain or domains containing your site's resources and user information.

When you access System Administrator commands using the **Enable** command, the server first checks to see if you are an administrator of the server's Clearinghouse domain. When you are enabled, you can access more commands than are available to ordinary users.

Use your logged-on, non-enabled status when you are making changes to your own user entries. Do not enable yourself every time you log on. If you do, you risk accidentally issuing a command that affects other users of your server or services.

Executive prompt summary

A prompt indicates that the Services Executive is ready for your input. Prompts always appear at the left side of your screen. The executive displays one of two prompts:

- The > prompt appears when no user is logged on and the executive is awaiting input. This prompt also appears when a user is logged on and has not enabled special administrative privileges.
- The ! prompt appears when a user is logged on and has enabled special administrative privileges.

Logged-on and enabled status

The Services Executive uses the logged-on status to determine which commands to make available. These terms for logged-on status are used throughout the Network Administration Library:

Any user Any user who has not logged on.

Logged-on user A user who has issued the **Logon** command and has been successfully authenticated as a member of any Clearinghouse domain.

Enabled user A logged-on user who has successfully issued the **Enable** command as a result of having administrative access to the server's domain.

Using commands

In general, commands contain a verb and an object separated by a space. The verb portion of a command conveys the type of action (for example, **Add**, **Change**, or **Delete**), and the object specifies what is to be affected (for example, **Drawer**, **User,** or **Mailbox**). Some objects are identified by multiple words separated by spaces. Two typical commands are **List Services** and **Show Logged On User**.

You can learn the executive commands quickly, because many of the services use the same verbs to operate on objects. After you are familiar with these commonly used verbs, you need only learn the objects in the different services.

The exceptions to the normal verb/object command form are those commands which affect logged-on status, such as **Logon**, **Logoff**, **Enable**, and **Disable**. The object of these commands is always the user entering them.

Command input

After you type a command, pressing RETURN begins the operation. Often more input is needed to direct the operation. You may need to specify the fully qualified (three-part) name of an object, select an item from an option list or menu, confirm an option, or enter text or a numeric value.

Correcting mistakes

At an 8000 server, if you make a mistake while typing a command or responding to a prompt, you can:

- Delete one character at a time by holding down the CTRL key and simultaneously pressing H, or by holding down the SHIFT key and simultaneously pressing RUB.
- Delete a full word by simultaneously pressing CTRL and W.
- Delete a full line by simultaneously pressing CTRL and X.

If you type a command and press RETURN, then decide you do not want to complete the command, hold down the CTRL key and simultaneously press C. This key sequence cancels the command and returns the current Executive prompt. You can use the BREAK key to stop floppy disk commands.

At an 8090 server, if you make a mistake while typing a command or responding to a prompt, you can:

- Delete one character by holding down the CTRL key and simultaneously pressing H, by pressing the DEL key or the left arrow key.
- Delete a full line by simultaneously pressing the CTRL and the DEL LINE keys on the numeric keypad.

Automatic completion of command input

To help you enter commands, the Services Executive can complete words within a command or complete the entire command. After you type enough characters to identify the word or command uniquely, pressing the space bar causes the complete word or command to appear on the screen. Pressing RETURN starts the operation.

For example, if you type "Del" and press the space bar, the Executive completes the word "Delete." You can then type the initial characters of the object you want to delete, press the space bar again, and then press RETURN.

If a verb can affect only one object, you need not specify the object at all. After you type enough characters to identify the verb uniquely and then press RETURN, the Executive completes the command and begins the operation.

Context for using commands

The Services Executive provides different contexts for accessing commands to manage your network.

Server context The server context lets you access the commands for the different services.

Test context The test context lets you access test commands.

The server and test contexts are available within a service context, and even when the server has no services--as long as the server software has been booted and initialized.

Service context Because a server can support several services at one time, the executive provides a context for each service that is running. Each context has a name and an acronym (the initials of the service name) corresponding to the service.

For example, suppose your server has the Clearinghouse Service, Print Service, and File Service installed. You can switch among five different contexts: server, test, Clearinghouse Service, Print Service, and File Service.

When you need to work in a particular service and use one of its commands, you must first set the executive context to correspond to that service by supplying the name of the service you want. An acronym for that context now precedes the > or ! prompt. For example, PS> or PS! identifies the Print Service context, and MS> or MS! identifies the Mail Service context. Using the **Reset Context** command returns you to the server context.

If you try to enter a command that is not available in the context you are in, the Executive cannot process the command. The

Executive displays a question mark after your input to indicate it does not recognize the command. The server commands are available in every context.

Command types

The commands you can use are grouped into three types: server commands, test commands, and service commands.

Server commands
Regardless of the services installed and running on a server, a set of commands exists that establishes and manipulates the server's configuration. Server commands enable you to:

- Install, run, stop, and restart services
- Set software options
- View the current server configuration
- Change your logged-on status
- Manipulate the services volume
- Change or view the server profile
- Recover from file system inconsistencies
- View reports generated by the recovery software
- Remove services from the server

See the Services System Software chapters in the *Services Installation and Setup Guide*, the *Services Maintenance Guide*, and the *Backup and Restore Guide* for more information on server commands.

Test commands
Test commands run diagnostic tests of server hardware components. Most of these commands are accessible after you boot the server and complete initialization. You access test commands in the test context. The test context is just like a service context; it gives you access to a set of test commands. See *Basic Network Troubleshooting* for more information on test commands.

Service commands
Service commands are specific to a service and available only within the context of that service. You can use service commands after you install and run one or more services on a server.

See the *Services Installation and Setup Guide*, the *Services Maintenance Guide*, and the *Backup and Restore Guide* for more information on the service commands.

Server and service states

Service and server states limit the availability of commands within a context. You can perform some operations only while the service or server is in a particular state.

For example, the Print Service cannot be printing when you are installing fonts. For this reason, the **Install From Floppy** and **Install Fonts and Test Patterns** commands are not available when the Print Service is started. However, you can stop the Print Service and then use these commands.

Most server states depend on the server startup process. By selecting a non-normal startup after the boot process finishes, you can interrupt server initialization and gain access to server commands that alter the initialization parameters, that dictate server startup.

Many server commands are available at one or more interrupt points as well as after server initialization is complete. Other commands do not function in all these states.

Some commands, when used before the server completes initialization, affect the server configuration immediately. These same commands, when used after initialization is complete, affect the server only after a subsequent boot and initialization.

These terms for server states are used throughout the Network Administration Library:

Interrupt points Three interrupt points that are available during non-normal initialization of the server. For more information, see "Running a service manually" under "Planning for maintenance" later in this chapter.

After initialization is complete The point at which most commands are available. If you select an interrupt point, initialization finishes after you type **Proceed**. For normal server startup, initialization finishes when the > prompt appears.

Open/Closed/Online Various states of server volumes. The collection of files contained on each disk is called a volume. The volume state determines which commands are available for manipulating the volume. Every server has a primary volume; servers configured with additional drives can have up to four volumes.

For more information about interrupt points and the commands available after the server is in these partially initialized states, see "Unscheduled activities" later in this chapter.

Using help features

You do not need to memorize all the Executive or service commands. You can learn which commands are available in the current context and state by typing **?** at the Executive prompt. The Executive displays all the verbs of the currently available commands, and the first word of each available context.

The Executive first lists the verbs that apply to the current context and then those that apply to the currently available server commands.

When you know which verb you need, you can learn which objects the verb can take by typing the verb and **?**. Once again, if the current context is other than the server context, the Executive first lists the valid objects for the specific context and then valid objects for the server commands.

Suppose you are not logged on, but the server has completed initialization and the server context is set. You see the following display when you enter **?** at the > prompt:

The Executive displays three verbs and the first words of the available contexts. In this case, the External Communication Service, Gateway Service, and Interactive Terminal Service have all been installed and run on the server.

```
>?
    List, Logon, Show, External, Gateway, Interactive,
    Internetwork
```

Now suppose you log on and set the context to the Internetwork Routing Service. You enter **?** and see the following display:

```
IRS>?
    List, Show

    Enable, List, Logoff, Reset, Show, External, Gateway,
    Interactive
```

To determine which objects you can use with the verb "list," you enter **List?**. The following display appears:

```
IRS>List?
    List Circuits, Routes, X25 Network

    List Executives, Services, Volumes
```

You can use six commands beginning with the verb "list" when you are logged on and in the Internetwork Routing Service context. These commands are:

List Circuits
List Routes
List X25 Network

List Executives
List Services
List Volumes

Remember, if you do not see the verb or object you want, you may need to change the current context, or the state of the server or service. Enter **Enable** to change your logged-on status, and request help again by entering **?**. If the command you want is still not displayed, stop or start the service, change the context, or reboot the server and take a non-normal startup.

Using the wildcard to name multiple objects

You can use the wildcard symbol (*) for several purposes: to list or display many objects of a particular type, add members to a user group in the Clearinghouse database, or establish access controls at the File Service.

For example, you may want to list all files in the working directory, all objects in a Clearinghouse domain, or all domains in an organization.

You can use the wildcard symbol (*) in place of some or all of the characters in a file name, or in place of one or more parts of a fully qualified name. The three parts of a fully qualified name are the local name, domain name, and organization name.

For example, the **List Print Services** command prompts for the three-part name of the Print Services to be listed. The response:

***:domain name:organization name**

causes all Print Services in the specified domain to be listed.

You cannot use the wildcard to specify a domain or organization; for example, User:*:Organization, or User:Domain:*.

Here are other examples of wildcard use. In this case, the user has typed the **List Files** command. The prompt is "File List:*":

Pattern	Result
*	Lists all files
*.bcd	Lists all files whose names end with ".bcd"
Server*	Lists all files whose names start with "Server"
S*Profile	Lists all files whose names start with "S" and end with "Profile," regardless of the characters in between.

Specific contexts limit the use of wildcards. The service-specific chapters in the *Services Installation and Setup Guide* and the *Services Maintenance Guide* explain any limits, as well as recommended uses of the wildcard symbol for that context.

Specifying pathnames

Many operations at the Services Executive or Interactive Terminal Service request pathnames. Pathnames are pointers to the location of a specific object. For example, you use a pathname to indicate the file drawer in which the Server Monitor Service stores its logs. A pathname takes the form:

(File Service name:Domain name:Organization name) File drawer name/directory or file name

You must type the parentheses and the slashes. You can truncate the pathname after the file drawer name, or have any number of directories nested in the file drawer. The last element in a pathname is always the name of the directory or file being specified.

Here are some examples of various pathnames:

File Service specifier:

(Tundra:Dallas:Acme)

File drawer specifier:

(Tundra:Dallas:Acme)Maindrawer

Directory specifier:

(Tundra:Dallas:Acme)Maindrawer/Maindir/Subdir

File specifier:

(Tundra:Dallas:Acme)Maindrawer/Maindir/Subdir/Afile

Interpreting Executive messages

A server or a service may periodically inform you about an activity that is in progress or completed. A server or a service also displays error messages when an operation you started could not be completed.

The Executive can display two types of messages, depending on the activity that causes the message. If a message relates to a background activity, (that is, an activity either not directly related to your current input or performed while no one is present), the Executive prefaces the message with an acronym indicating which software element is responsible for the message. If a message relates directly to your current activity, the acronym does not appear.

For example, suppose your server is running the Clearinghouse Service, Mail Service, and File Service. If a Mail Service activity generates a message while you are working in the File Service, the initials "MS:" appear before the message. If you are in the Mail Service context, the message appears without "MS:"

Terminating Services Executive sessions

If you are logged on at the server terminal, typing **Logoff** terminates your session. Always log off when you leave the terminal so that other users cannot take advantage of your System Administrator access rights; these users could start activities that interfere with the current server configuration or violate the security of your network resources.

If you initiated your Executive session from a remote location, using the **Quit Connection** command ends the session by terminating the connection and automatically logging you off. If you established the session by dialing into the External Communication Service Greeter, the **Quit Connection** command returns you to the Greeter.

Planning for installation

The Server Software Installation chapter in the *Services Installation and Setup Guide* contains the procedures for installing your Services System Software. This section explains the hardware, software, and other requirements for installation.

You must read this section carefully to install your services correctly. The section covers three installation scenarios:

- Installing server and services software on a server connected to an existing network. An existing network includes at least one other server running a Clearinghouse Service. This scenario is called non-Genesis installation.
- Installing server and services software on the first or only server on a network. This server must run at least one Clearinghouse Service. This scenario is called Genesis Clearinghouse Service installation.
- Installing server and services software on a server to be connected to another network using an Internetwork Routing Service link. The other network contains the Clearinghouse Service in which all local network clients are registered. This scenario is called Genesis Internetwork Routing Service installation.

Do not use the information in this section or the associated procedures to install additional services on an existing server. See "Planning for maintenance" later in this chapter and the Services System Software chapter of the *Services Maintenance Guide* for the correct procedure.

Hardware requirements

The Services System Software operates on an 8000 or 8090 server attached to a server console. If you are planning to use the Multiport Option Kit, have a Xerox technician install it.

Software requirements

The required software for an 8000 server exists on a set of floppy disks. For an 8090 server, the software resides on a cartridge tape.

8000 server floppy disks

If your server has a 10, 29, or 42 Mb fixed disk, you need this set of floppy disks:

- Services System Software # 1 (10, 29, 42 Mb Disks)
- Services System Software # 2 (10, 29, 42 Mb Disks)
- Services System Software # 3 (10, 29, 42 Mb Disks)

If your server has an 80 or 300 Mb fixed disk, you need this set of floppy disks:

- Services System Software # 1 (80, 300 Mb Disks)
- Services System Software # 2 (80, 300 Mb Disks)
- Services System Software # 3 (80, 300 Mb Disks)

You also need the floppy disks with the software for your services options. The titles of the available floppy disks are:

- Boot Service
- Clearinghouse Service, External Communication Service, and Server Monitor Service
- Communications Monitoring Service
- 850/860 Gateway Service
- File Service
- Interactive Terminal Service
- Internetwork Routing Service
- Mail Service
- Multiport Option
- PC File Service
- Print Service
- Remote Batch Service

If you are installing Print Service, have ready the disks containing your Print Service fonts. Here is the complete list of font floppy disks (DPI means dots per inch):

- Xerox Required Fonts (300 DPI)
- Xerox Classic Fonts (300 DPI)
- Xerox Printwheel Fonts (300 DPI - #1 and #2)
- Xerox Math Classic Fonts (300 DPI - #1 and #2)
- Xerox Modern Fonts (300 DPI - #1, #2, #3, and #4)
- Xerox XC1K Modern Fonts (300 DPI) - #1 through #14. These floppy disks contain all the Japanese Modern Fonts (also called extended language fonts).
- Xerox XC1K Classic Fonts (300 DPI) - #1 through #14. These floppy disks contain all the Japanese Classic Fonts (also called extended language fonts).
- Xerox Required Fonts (200 DPI)
- Xerox Classic Fonts (200 DPI)
- Xerox Printwheel Fonts (200 DPI)
- Xerox Math Classic Fonts (200 DPI) - #1 and #2
- Xerox Modern Fonts (200 DPI) - #1 and #2

Please refer to the Print Service chapter in this book for important information you need for determining the fonts you need, the disk space required, and the installation order.

8090 server cartridge tapes

You need this cartridge tape for Services System Software and services installation:

- XC80 Services System Software and Network Services for the 8090 Server

Print Service fonts are on these cartridge tapes:

- Xerox Network Printer Fonts 5.4 - 300 DPI. This tape contains all the 300 DPI Xerox fonts, except the extended language fonts; it includes:
  - Xerox Required Fonts
  - Xerox Classic Fonts
  - Xerox Printwheel Fonts
  - Xerox Math Classic Fonts
  - Xerox Modern Fonts

  - PC Emulation Fonts
  - Helvetica ™ Fonts 5.4 300 DPI
  - Arabic Safiir Fonts
- Xerox Extended Language Fonts 5.4 - 300 DPI. This tape contains the Japanese Classic and Japanese Modern fonts.

Please refer to the Print Service chapter in this book for important information you need for determining the fonts you need, the disk space required, and the font installation order.

Services System Software worksheets

Use the Services Installation Worksheet to record server-related and service-related information. Use the Services Options Worksheet to identify the software options to enable for the server. For your convenience, these worksheets are at the end of this chapter.

If you are preparing for a Genesis Internetwork Routing Service installation, also complete the Internetwork Routing Service Worksheet. This worksheet is at the end of the Internetwork Routing Service chapter of this book.

If you are preparing for a Genesis Internetwork Routing Service installation that will use a Communication Interface Unit, also complete section 2 of the External Communication Service Worksheet. This worksheet is at the end of the External Communication Service chapter of this book.

If you are installing software on more than one server, make a copy of each worksheet needed for each server. Retain the originals worksheets for future use, and store the completed worksheets in your *Activities Guide*.

Using the worksheets

Before you bring up the server and install the software, complete all worksheets. It is important that you fill out the worksheets accurately and update them whenever changes occur. The completed worksheets save you time as you perform installation, setup, and maintenance procedures. They also serve as an information source for new System Administrators unfamiliar with your network configuration.

Filling out the worksheets

As you read the rest of this chapter, you are directed to make entries on the worksheets. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① on the Services Installation Worksheet for information about the server and the services installed on the server. Use section ② for information about the first Clearinghouse Service on the network.

On the Services Options Worksheet, specify the service options and printer fonts installed on the network server.

General preparation

Prepare for installation by completing the following tasks. A Genesis installation requires additional preparation. See the next section, "Genesis installation preparation."

Reading requirements

- Read this chapter. Become familiar with the basic server operating conventions described in "Characteristics and conventions" earlier in this chapter.
- Read the Clearinghouse Service chapter in this book. Pay special attention to the section on naming conventions.
- Read the Internetwork Routing Service chapter in this book, if you are using the Internetwork Routing Service to connect to another network.
- Read the External Communication Service chapter in this book, if you are planning to use a Communication Interface Unit for your Internetwork Routing Service link.

Server names

Choose fully qualified names for the servers you plan to install. Note that the domain and organization portions of the names should be the same for the server and all services.

You can use up to 40 characters for the server name. Do not use commas, parentheses, asterisks, or pound signs (#) in a server name.

Filling in the worksheet:

① Record the name of your server, its domain and organization on the Services Installation Worksheet.

Also record the type of other services you plan to install on the server, whether they will be activated, the number of disk pages they require, and their names and descriptions. Your Xerox Systems Analyst should have this information.

Server disk partition

You must partition a disk before the server can use it to support services. Partitioning the rigid disk divides the disk space into three storage areas: two for the system software you will install, and one for services software.

CAUTION: Partitioning erases all data on a disk. Partition the server disk only when installing the server for the first time. If you ever need to reload software, do not partition the disk again unless your Xerox Systems Analyst advises you to do so. Partitioning takes from 3 to 20 minutes, depending on the size of the disk.

Disk packs

If your server has removable disk packs (T80 and T300 disk drive options), format each disk pack you plan to use on the server.

Use the T80 and T300 format software contained on the diagnostic floppy disk.

Time and zone

If you are installing the first server on the network, or if your server was turned off, you must set the server time and date. Otherwise, you must set the time zone and confirm the current server time and date.

Set the time zone for the geographical area where you are installing the server. The time zone values are:

-5 for Eastern Standard Time
-6 for Central Standard Time
-7 for Mountain Standard Time
-8 for Pacific Standard Time
+0 for the United Kingdom
+1 for Western Europe (excluding the United Kingdom)

The default time zone is -8.

You must also set the correct Daylight Saving Time values. These values indicate on which days of the year Daylight Saving Time begins and ends. The default values are **98** and **305** for states in the United States and Canada using Daylight Saving Time.

These values are also valid:

0 and **0** for parts of the United States not using Daylight Saving Time (parts of Illinois and Arizona)

91 and **303** for the United Kingdom

91 and **274** for Western Europe (excluding the United Kingdom)

Filling out the worksheet:

① Enter the values for the time zone and for Daylight Saving Time for your area on the Services Installation Worksheet.

Genesis installation preparation

Installing software on the first server on an Ethernet network is called a Genesis installation. In a Genesis installation, the server cannot verify at the Clearinghouse that you have administrative access to its domain. Either that domain does not exist, or it exists at a remote site.

Normally, the server must have verification before making its administrative commands available to you. A Genesis installation gives you temporary access to a limited set of commands so you can install the first server at your site and make the Clearinghouse domain available to your site.

For an 8090 high capacity server, obtain an extra high capacity cartridge tape to create a diagnostic tape.

Each type of Genesis installation requires different preparation.

System software startup

When you start the server for the first time after installing the Services System Software, the server creates a new user file

system. The server detects that no software options have been set and halts initialization until you enter the necessary passwords.

Network number and server name

If you are installing the first server on a new network, this server cannot obtain your network number from any other server. You must enter the network number you obtained from your Xerox Systems Analyst. Otherwise, the new server can obtain the network number from another server on your network. You simply see a message with that number.

You must also enter a fully qualified server name and a server description. This critical step establishes future protection for the server. Enter the name carefully, noting the spelling, spacing, and case you have used.

CAUTION: For a Genesis installation, the organization portion of the name must match exactly the format you specified when you obtained your organization password.

Filling out the worksheet:

① Enter the network number, fully qualified server name, and server description on the Services Installation Worksheet.

Services selection

Installing software for an 8000 server requires floppy disks. Installing software for an 8090 server requires one cartridge tape containing all the system and services software. See "Software requirements" earlier in this chapter for floppy disk and tape names.

Services installation includes two steps. First, you copy from floppy disk or cartridge tape to the server's primary services volume all files necessary to run a service. You must have enabled that service for use on the server. Then, you activate each service you need on the server.

Activated services

Activating a service adds it to the Active Services list. When the server is restarted, the service is run automatically. Generally, you want all services installed on a server to be run automatically (activated) each time the server completes initialization. This way, if a system failure occurs, the recovery software can re-establish the previous working configuration of the server.

Filling out the worksheet:

① and ② Check off the services in Services Group I and II you want to enable on the Software Options Worksheet. Fill in the software serial numbers as they are displayed when you are at this step in the installation procedures.

Call the Xerox Software Control Center to obtain a password for each product group for which you are setting options. Be prepared to name the software options you want to enable.

Multiport Option Kit

If you are installing the Multiport Option Kit, install it now, just like a service. Numerous server displays list the Multiport Option Kit as if it were a service, until you next boot the server.

The server and server software are designed to run multiple services at the same time on a single server. However, some services cannot run at the same time on a server.

For example, the External Mail Gateway option, 850/860 Gateway Service, IBM 3270 BSC Terminal Emulation, Facsimile Print Service, and Remote Batch Service all require use of the RS232C port on the server. Thus, only one of these options or services can run at a time on a server. Do not activate more than one of these services at the same time.

Other service combinations may not be advisable because they increase response time to user requests. See the service-specific chapter in this book for more information. If you have further questions, contact your Xerox representative.

Filling out the worksheet:

① Indicate on the Services Installation Worksheet whether or not the services you enabled are activated.

Genesis Clearinghouse Service preparation

Date and time

Be prepared to enter the exact date and time during the installation process.

Processor, network, and serial number

Contact your Xerox Systems Analyst for these numbers.

Organization and domain names

If you are installing the first server on an internetwork, you need to create a new organization and domain.

First, you choose a name for the organization. Then you obtain a password from the Xerox Software Control Center that lets you introduce the new organization. The Center issues a password that applies only to the spelling, spacing, and case you specify for the organization name. For example, the names "Acme" and "ACME" would have different passwords. You cannot easily change the organization name after you create it.

After you choose the organization name and obtain the password, choose the name for the first domain. You will need the organization and domain names during installation.

Clearinghouse Service

For a Genesis Clearinghouse Service installation, you must run the new Clearinghouse Service. You initialize the Clearinghouse database and add a domain and organization. You then add yourself as the first user of the new domain with complete access to the domain and organization. Finally, you add a user group, and yourself as a user.

When naming, do not use characters such as commas, parentheses, asterisks, or pound signs (#).

Filling out the worksheet:

② On the Services Installation Worksheet, record a name and description for the first Clearinghouse Service on the network. Also enter your name and password as the first user, your alias, and the name of your home File Service where your desktop can be stored. Then add the name of the first user group, of which you are the first member.

Genesis Internetwork Routing Service preparation

Date and time Be prepared to enter the exact date and time during the installation process.

Processor, network, and serial number Contact your Xerox Systems Analyst for these numbers.

Services For a Genesis Internetwork Routing Service installation, you must run the Internetwork Routing Service and configure a circuit. To establish an Internetwork Routing Service link using a Communication Interface Unit, you must also run the External Communication Service, register a Communication Interface Unit, and configure a circuit.

Running a service includes initializing it and providing its name and description. If you run the External Communication Service, you must later assign ports to it.

You can configure one of four types of circuits:

- X.25 switched virtual circuit (SVC)
- Auto-dialed
- Manually dialed
- Dedicated

If an X.25 network will be your Internetwork Routing Service link, you must configure an X.25 network.

Remote System Administrator Contact the System Administrator at the site with which you will interconnect. Arrange for administrative access to the domain in which you will register your site's servers, services, users, user groups, and so on.

If your internetwork community decides that your site should use a new domain (and, perhaps, a new organization), have the System Administrator at the remote site create the necessary domain or domain and organization. The remote System Administrator must then grant you Administrative access to the new domain and organization. See the Clearinghouse Service chapter in this book for more information.

Filling out the worksheet:

① Record the network number on the Services Installation Worksheet. Also note whether you are installing the External Communication Service as well as the Internetwork Routing Service in the "Services installed" section.

See the Internetwork Routing Service and External Communication Service chapters in this book for information on filling out those worksheets. These chapters also help you determine the correct configuration information.

Planning for setup

After you install the software for all the services to be run on the server, you initialize each service. You supply service-specific information during this process.

Refer to the appropriate chapter in this book for each service you install. Read that chapter carefully to prepare for setting up the service before you perform the setup procedures. Refer to the *Services Installation and Setup Guide* for complete setup procedures.

Planning for maintenance

After you install the Services System Software, you are responsible for maintaining it. This section provides guidelines for monitoring your services volume, working with the server, and performing the most common maintenance procedures. See the Services System Software chapter in the *Services Maintenance Guide* for complete maintenance procedures. You perform certain maintenance activities for the Services System Software on a scheduled basis. You perform other maintenance activities on an unscheduled basis.

Scheduled maintenance

Scheduled maintenance activities keep your Services System Software running smoothly and efficiently. These activities are:

- Monitoring the services volume to ensure you have enough disk space for user files.
- Saving the backstop log so you can monitor your server's performance. The log may also help in troubleshooting operations. (See *Basic Network Troubleshooting* for more information.)
- Backing up the server profile so you always have a current record of this valuable information. (See the *Backup and Restore Guide* for complete information.)

Unscheduled maintenance

Many unscheduled maintenance activities apply to all the services that the system software runs. These operations are:

- Server operations, including booting the server, turning server power on and off, changing the server profile, and managing volumes.
- Installing new services from floppy disk or cartridge tape. You also install a service when you move it from one server to another. Remember to expunge the service before installing it elsewhere.
- Running a service, bringing it to a fully operational state.
- Stopping a service, to keep it running but not responding to external requests.
- Starting a service so it begins responding to external requests. This operation reverses the stop procedure, or explicitly starts the service after a service-specific failure.
- Expunging a service, which removes it from the server, deletes any files created during or after installation, and removes any Clearinghouse entries associated with the service. This operation retains files required by another installed service.
- Activating a service by adding it to the Active Services list. The service is run automatically the next time you boot the server.
- Deactivating a service by removing it from the Active Services list. The service is not run automatically the next time you boot the server.
- Showing (displaying) the details about a specific object.
- Listing names and other information about specified objects.

Other procedures associated with the Services System Software are not generic.

Monitoring your services volume

You must ensure that your services volume never becomes more than 98 percent full. Generally, if the services volume is nearly full, a message to that effect appears each time you try an operation requiring more disk space.

Effects of a full volume

If your services volume does become full, service performance degrades and users experience slow response times; in some cases, the services may become inoperative.

For example, if you cannot expand your Mail Service database because your services volume is full, the mail queue fills up. The result is slow performance, delayed Clearinghouse Service updates, and no room to add mailboxes to the service.

A File Service on a too-full services volume cannot store more backup copies or hold new file drawers. You may be unable to complete a scavenge, a file recovery procedure, on a volume that is nearly full.

Related procedure: Monitoring your services volume

Disk space recovery

When your services volume uses more than 95 percent of disk space, act as soon as possible to recover disk space. You have two options--moving or deleting information. Consider which option is better for your server or network.

For example, you can move one of the services to a new server. If you have another File Service on your network, you can move file drawers from the full volume to the other File Service. If you have another Mail Service on your network, you can move mailboxes from the full volume to the other Mail Service. (Also tell users with unretrieved mail messages to retrieve their mail.)

You can also delete files that are not in use. Before you do, ensure you do not delete a file that one of your services needs.

Related procedure: Moving a service to another server

Booting the server

Many service-related procedures require you to boot (or restart) the server. You may boot from a floppy disk on an 8000 server, from a cartridge tape on an 8090 server, or from the Ethernet to run a utility program not on your server's primary volume. Such utilities install the server software and run disk diagnostics.

CAUTION: If your server is running and services are started, you must stop all services before you boot the server.

Boot switches

During the boot procedure, you release the ALT B (Alternate B for 8090 servers) switch when the maintenance panel displays a certain number. The number displayed when you release ALT B starts a particular type of boot process. The boot switch numbers and types of boot process are listed below.

Boot switch	Boot process type
0000	Drive 0 diagnostic boot for disk-drive attached processors
0001	Drive 1 nondiagnostic boot for disk-drive attached processors
0002	Cartridge tape/floppy disk nondiagnostic boot
0003	Ethernet nondiagnostic boot
0004	Ethernet diagnostic utility boot
0005	Cartridge tape/floppy disk diagnostic boot
0006	Ethernet boot of experimental microcode or software
0007	8090 large capacity drive 2 diagnostic boot
0008	8090 large capacity drive 3 diagnostic boot
0009	8090 large capacity drive 4 diagnostic boot
0010	Cartridge tape retension, floppy disk drive head-cleaning function
0011	8090 high capacity drive 5 diagnostic boot
0012	8090 high capacity drive 6 diagnostic boot
0013	8090 high capacity drive 7 diagnostic boot

Each procedure that requires you to boot the server indicates the required boot number. Most procedures require you to boot the server from 0001. If you pass the correct boot switch number, the sequence continues to cycle back to 0001.

Normal versus non-normal startup

Booting from the primary volume (boot switches 0000 and 0001) runs the Services System Software. The server displays the Services Executive banner and indicates the restart reason as a "User Restart." (The server also displays this message after a power failure, because it cannot distinguish the restart reason. Other restart reasons are displayed as applicable) The server then prompts you to select a normal or non-normal startup, waiting until you respond.

Normal startup

The server initializes itself during an automatic or user-specified normal startup. During initialization, the server verifies its Clearinghouse Service registration, prepares to support the specified number of remote Executives, and applies other configuration information from the server profile. Finally, the server runs all services on the Active Services list.

Non-normal startup

A non-normal server startup enables you to access commands that affect your server's configuration.

The Services Executive is unavailable from remote locations until initialization is complete. Remain at the server terminal to ensure that normal startup results in a successful initialization, or to

answer prompts and give commands in the case of non-normal startup.

If the server fails during normal operation, the backstop software automatically reboots the server and displays the message "System restart" after logging the error in the backstop log. The server then waits 60 seconds while displaying the "Normal startup" prompt. If the server receives no user input during this time, the server assumes a normal startup and begins initialization.

Because initialization can occur automatically after a system error, the server can re-establish its former working configuration without your intervention. However, you may need to re-establish the working configuration of some services. For example, you may have to configure to autostart one or more circuits for an Internetwork Routing Service.

Related procedures: Booting the server, Running a service manually

Controlling server power

The services on a network are more effective if servers remain powered up at night. The Clearinghouse Service and Mail Service work through the night to verify the accuracy of Clearinghouse database entries and to deliver mail. The special operation (called propagation) that the Clearinghouse Service performs to verify its database occurs only in the middle of the night. If you power down your server every evening, this operation never occurs automatically.

If your organization has several interconnected networks spanning a large geographic area, particularly multiple time zones, it is particularly important for your servers to remain powered up through the night.

CAUTION: Stop all services before you power your server down for any reason.

If you power up the server and immediately boot it, the boot takes longer. The disk drive must warm up, and diagnostics must be run.

Related procedure: Powering the server up or down

Changing the server profile

After you configure a server, the server information such as the server name and terminal types is kept in the server profile. The profile saves you from re-entering all the configuration information each time you boot the server. The profile is divided into sections, one for each service and one for the server itself.

Each service maintains and interprets the entries in its section. Do not edit the service-specific sections of the profile.

The server section of the profile is the only section that may require editing. Since the process can be time-consuming, keep the profile backed up at all times; see the Services System Software chapter in the *Backup and Restore Guide*. If you change the server profile after initialization is complete, the new values do not take effect until the next time you boot the server.

The Clearinghouse no longer allows System Administrators to specify whether clients can look up passwords. The field does not appear in the server profile.

You can change this information in the server profile:

Server version The software version running on the server.

Network number The number of the local network to which the server is connected. This number is set during initialization; any change takes effect only after a reboot. The number is also registered in the Clearinghouse.

Server name The fully qualified name of the server. The name is also registered in the Clearinghouse. When you log on, the domain and organization of the server are used as defaults.

Server name changes take effect at the next boot. You must manually delete the old server name from the Clearinghouse.

CAUTION: Changing the domain name of the server can affect your ability to access System Administrator commands at that server. Do not change the domain name of the server unless you first create a Clearinghouse domain matching the new domain name and give yourself Domain Administrator status for it.

Server description Descriptive information about the server, such as its location, owner, purpose, or the services it is running. The description is also registered in the Clearinghouse.

Active service The services run during initialization. Changes do not take effect on the current boot unless you make them at the second interrupt point.

CAUTION: If you deactivate your Mail Service or Clearinghouse Service and then reboot the server, do not leave either service in a stopped state for an extended period of time.

Number of remote execs The maximum allowed number of remote Executive connections to the server. Any change does not abort existing connections.

Local terminal type The terminal type used for the local terminal. The local terminal type must be ASCII.

Remote terminal type The terminal type used for remote connections. The remote terminal type must be ASCII.

Related procedures: Changing the server profile, Showing the server profile

Managing volumes

You can create secondary volumes on a multi-drive server for use as a remote or backup storage area.

The partitioning operation that is a part of this procedure destroys data on the disk. Prepare as a secondary volume only a formatted and blank, removable or fixed AMS 315 disk that has never been used. Opening server volumes at server startup may take from 10 to 40 seconds on an 8000 server, and from 1 to 6 minutes on an 8090 server.

After you bring the new volume online, create file drawers on it so other users can access it. See the File Service chapter in this book for more information.

You may occasionally need to change the name of a volume. The volume whose name you are changing must be open. Note that you cannot use the comma, left or right parentheses, asterisk, or pound sign (#) in any volume name.

Users on 6085/8010 workstations must copy a new file server icon to their desktops after a volume name change.

Related procedures: Changing the volume name, Creating a services volume on a secondary drive, Replacing a disk pack

Running a service manually

At times you may run one or more services manually. For example, you may want to run a service that was not on the Active Services list at the time initialization was completed, or you may want to run a service before the server completes initialization.

You may also want to run a service so you can specify non-normal startup and change the service configuration. For example, during non-normal startup you can:

- Expand the size of the Clearinghouse database
- Prevent the File Service from automatically opening or placing online auxiliary volumes, so you can scavenge one of them
- Expand the size of the Mail Service database
- Restore or repair the Mail Service database
- Initialize a new Mail Service database
- Change the type of printer (printing option) that the Print Service uses
- Prevent the Internetwork Routing Service from automatically starting its circuits so you can reconfigure them
- Change the size of the Interactive Terminal Service workspace or number of users

Interrupt points

During a non-normal server startup (initialization), you must select one or more interrupt points:

1 Interrupt before opening the primary volume

2 Interrupt before processing the server profile

3 Interrupt before running services

You decide which interrupt point to select based on the activity you need to perform.

At the first interrupt point, a few administrative commands are available to you. You cannot log on or enable, but the commands you need to scavenge or copy the primary volume or to examine the backstop log are available. At the second and third interrupt points, you must log on and enable to access

administrative commands, unless your server enters Genesis Mode, described below.

Not all server commands are available at all interrupt points. Service contexts are generally not available, because their corresponding services have not been run yet. If you do run a service at the third interrupt point, its context becomes available after the service initializes.

Interrupt point activities

Table 3-1 lists activities you perform during non-normal server startup option. The table specifies the appropriate interrupt point for each activity.

Table 3-1. **Interrupt point activities**

Activity	Interrupt point
Scavenging the server's primary volume	1
Scavenging a secondary volume on a multiple-drive server	3
Copying the primary volume to an attached disk	1
Examining the backstop log when the volume cannot be opened	1
Installing one or more new services	3
Upgrading the server with new services options software	3
Explicitly running the Clearinghouse Service or Mail Service to change the database size	3
Changing the initialization values for a service	3
Expunging a service	3
Changing software options	2
Changing server profile values	2
Deleting or restoring the server profile from a remote File Service	2
Activating or deactivating one or more services	2, 3

After you complete activities at an interrupt point, you can continue to the next interrupt point you selected or proceed with server initialization.

Should your server enter Genesis Mode, do not leave it unattended until you finish your activities. If you leave it unattended, any user who can physically access the server can use the administrative commands.

Related procedure: Running a service manually

Genesis Mode

When you select the third interrupt point, your server may enter Genesis Mode. The server enters this mode automatically when it determines that no Clearinghouse Service is available that serves its domain.

Genesis Mode makes available a limited set of administrative commands, even though you cannot enable special administrative functions. These commands enable you to perform certain administrative tasks, such as installing the first server on an Ethernet network, installing new services, running one or more services manually, and activating or deactivating existing services.

After the first server is installed, Genesis Mode should never occur at servers on multi-server networks. If it does, an error condition is preventing the initializing server from accessing the Clearinghouse Service for its domain. Check the Clearinghouse Service to ensure it is running properly. Also check the Ethernet cable connection.

Genesis Mode is a normal occurrence on single-server networks. In this case, the only instance of the Clearinghouse domain resides on the server being initialized. That domain is not accessible until the Clearinghouse Service is run, initialization is finished and the services in the Active Services list are run. An exception occurs when you run the Clearinghouse Service at the third interrupt point.

Starting and stopping services

Before you boot or power down your server, always stop all services. Otherwise, you risk interrupting client sessions. For example, if you boot a server running the File Service without stopping the File Service first, you might interrupt a user's filing session and leave your services volume in an inconsistent state.

The system prompts you whether to stop the service immediately. If you specify more than one service to be stopped, the system issues this prompt for each service.

An immediate stop terminates all activity on the service. If you indicate that you do not want to stop a service immediately, the server prevents any new sessions and stops the service after all current activity ends.

Some services have special considerations you should keep in mind when stopping the service. For example, a Clearinghouse Service co-resident with a Mail Service relies on the Mail system to keep its database consistent. If you stop the co-resident Mail Service for a long time, the Clearinghouse becomes inconsistent with the rest of the Clearinghouse system.

If you reboot the server after deactivating the Mail Service, a co-resident Clearinghouse creates its own "invisible" Mail Service that uses the same database as the previous Mail Service. If you then scavenge the previous Mail database, you will lose the database.

Related procedure: Starting and stopping services

The Mail Service cannot stop completely while processing its pending queue. You may notice a delay of an hour or more between the time the Mail Service indicates it is stopping, and the time the Mail Service reports it has stopped. Do not interrupt the server during the delay. Wait until the "Mail Service is stopped" message appears.

CAUTION: Stopping the Mail Service makes most Mail Service operations unavailable to network clients. Mail cannot be posted or forwarded, and users cannot retrieve mail. Mail backs up on other Mail Services, which have increased responsibility for accepting posted messages, repeated forwarding attempts, and returned messages.

The Server Monitor Service has its own commands for starting and stopping. See the Server Monitor Service chapter in this book.

Expunging a service

As your network grows and your user needs change, you may add servers to your network and move services from one server to another. You move a service by expunging it from one server and installing it on another.

Expunging a service removes it from a server, freeing server resources for use by the remaining services. This operation deletes the local database files for the expunged service, as well as any files not shared by another service.

CAUTION: The following services have special procedures you must perform either before or instead of expunging the service. See the service-specific chapters in this book for more information.

- Mail Service
- External Mail Gateway Service
- File Service
- External Communication Service
- 850/860 Gateway Service

Related procedures: Expunging a service, Moving a service to another server

Listing information

You can list several types of information about the server.

Executives You can list information about the Services Executive and each remote executive in use on the server. This information includes the logged-on users, their enabled status, the host address, the date and time the Executive was created, and the last Executive activity.

Files You can list the names of the files in the server's working directory, along with the date and time they were installed.

Services By listing services, you can see which services are installed and activated on the server. The displayed information includes the server name, network number, and processor number; a list of

installed services; and a list of activated services. The fully qualified name and status (started or stopped) of each service also appear.

RS232C ports You can list the configuration information for all the ports configured on your server. This information includes port names and descriptions, types of ports, and line speeds. See the External Communication Service, Internetwork Routing Service, Remote Batch Service, and Interactive Terminal Service chapters in this book for more information about port configurations.

Related procedures: Listing executives, Listing files, Listing RS232C port information, Listing services

4. Clearinghouse Service

This chapter helps you prepare for installation, setup, and maintenance of the Clearinghouse Service (CHS). This information supports the procedures you perform from an 8000 or 8090 server.

Service description

The Clearinghouse Service helps provide the foundation for other network services. It keeps track of information about users, the network services, and other resources within one or more domains. It forms a network community, enabling servers and workstations to access needed resources. The Clearinghouse also authenticates users when they access the network, providing access security.

The collection of information stored in the Clearinghouse Service is called the Clearinghouse database. The database holds information about users, services, and other network objects such as printers and file drawers.

As the network grows, you can easily add more Clearinghouses to support it. Multiple Clearinghouses make up one entity, called the Clearinghouse system, and automatically communicate with each other to maintain accurate information about all the resources on the network.

The Clearinghouse provides:

- Database access - Workstations and services can request information on a particular object or a list of all objects in a particular category.
- Database update - When any database receives new information, all Clearinghouses on the internetwork or a single network update each other automatically.
- User authentication - Vital resources such as file drawers are accessible only after the Clearinghouse validates the user's access rights.
- Reliability - Domain duplication (replication) ensures the continuous availability of the Clearinghouse database in the event of a hardware or software failure.
- Expandability - Few restrictions apply to the number of Clearinghouses, or the number of domains allowed on a network. Your network can grow as your organization grows.

How the software works

Each Clearinghouse maintains a database composed of the organization and one or more domains. Usually a domain covers a particular geographic location. No user or object can be

registered more than once in a domain. An organization can divide the resources of a network into multiple domains.

Objects are registered in each domain. Objects are logical (non-physical) or physical entities managed by the server or the services it supports. Logical objects are file drawers, Clearinghouse domains, Clearinghouse domain entries, services volumes, and mailboxes. Physical objects are printers, ports, disk drives, processors, and server terminals.

Lookup service

Any Clearinghouse in an organization can answer any request for information, or direct the request to the Clearinghouse with the right information.

The Clearinghouse stores the address of each object, and links the object to a user-assigned (mnemonic) name. If the user wants to use a printer, the user can simply specify the printer's user-assigned name. The workstation then interacts with the Clearinghouse to determine the correct network address for the printer.

Other distributed systems often require the user to know the address or pathname of a remote object, and to supply it before the user can access that object. In the Xerox Network System, the user need provide only the name of the needed object, or the name of the person to receive mail. The workstation automatically determines the address of the network object or user by communicating with the Clearinghouse. The communications software automatically handles routing the request or sending mail.

The workstation or service ability to look up information in the Clearinghouse database is like the service provided by the white pages in the telephone book. The Clearinghouse Service also offers a lookup service similar to the yellow pages of a telephone directory. A user unsure of the exact name of a co-worker or a needed object can request a listing of objects of a certain type registered in the Clearinghouse.

Clearinghouse security

Security reduces the risk of unauthorized access that could jeopardize the configuration or the integrity of the data on your server. The Clearinghouse provides five levels of security.

System Administrator

As System Administrator, you:

- Oversee network resources at a site
- Answer user questions
- Train assistant System Administrators
- Install, set up, maintain, and troubleshoot the server and services software.

Your Xerox Systems Analyst and the Network Administration Library help you perform these activities. As System Administrator, you may also assume Organization Administrator or Domain Administrator status.

Organization Administrator

As Organization Administrator, you:

- Create new domains
- Delete the last copy of a domain from an organization
- Add users to the organization access list

Domain Administrator

As Domain Administrator, you:

- Change server operating parameters
- Set up and maintain your services
- Expunge services
- Add new users, user groups, and mailboxes to the domain
- Give other people domain access
- Control access to file drawers
- Change software options and add new services
- Copy domains

With Domain Administrator status, you can issue Clearinghouse Service commands that introduce, modify, or delete Clearinghouse entries in your domain. This status gives you access to any administrative commands on all servers registered in your domain.

Objects

The Clearinghouse Service, in conjunction with the File Service, enables you to grant administrative status over specific objects to users who do not have domain or organization access. For example, you might set up a file drawer and let one user control access for the drawer.

Logical objects are protected by software mechanisms (object-level access controls). To protect physical objects, you restrict physical access to them.

Server security

You can restrict physical access to the server by keeping it in a locked location. The Services System Software protects the server configuration by allowing only a Domain Administrator to have access to special administrative commands. This access requires the Clearinghouse Service to authenticate the System Administrator's name and password, and then apply access controls to that user.

Authentication

The Clearinghouse must authenticate a user before the user can gain access to a network workstation, server terminal, emulation port, or any service or resource that can be accessed from remote dial-in devices. Authentication occurs when the user logs on and provides the correct password. The software accepting the user's name and password interacts with the authentication capability in the Clearinghouse database to verify the user's identity.

The Clearinghouse may check the credentials of the user again if the user tries to access a restricted object. A restricted object is accessible to only a subset of authenticated users.

Password suppression

Passwords entered at any workstation or server are "suppressed." The characters that make up the password are not displayed as

you type them. Instead, special characters (usually asterisks) appear on the screen.

Relationship with other services

The Clearinghouse Service works with all the services on the network. Each service must make its location known to the Clearinghouse, so that the Clearinghouse can pass on that information to requesting users.

Some objects, such as services, automatically register and verify themselves and their associated resources in the Clearinghouse database when you first initialize the service. The automatic registration and verification occur each time you restart the service. Other objects, such as users, user groups, and group members, are not registered automatically with the Clearinghouse. You must register these objects manually. Considerations for registering these objects are in "Preparing for setup" later in this chapter.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the Clearinghouse Service worksheets located at the end of this chapter.
- Installing the Clearinghouse Service software as described in the Server Software Installation chapter of the *Services Installation and Setup Guide*.
- Setting up the Clearinghouse Service as described in the Clearinghouse Service chapter of the *Services Installation and Setup Guide*.
- Maintaining the Clearinghouse Service as described in the Clearinghouse Service chapter of the *Services Maintenance Guide*.
  - Maintaining system security by following Clearinghouse Service conventions described earlier in this chapter.
  - Regularly replicating domains.
  - Monitoring and expanding the Clearinghouse database.
  - Manually updating Clearinghouse Services not connected by 24-hour continuous links.
- Regularly performing backup using the Clearinghouse Service procedures of the *Backup and Restore Guide*.
- Notifying users of any change or disruption in the Clearinghouse Service.
- Upgrading hardware and software as required.
- Troubleshooting the service as described in the *Basic Network Troubleshooting*.

You can perform most Clearinghouse Service procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter in the *Services Installation and Setup Guide* contains the procedures for installing your Clearinghouse Service software. This section explains hardware, software, and other requirements for installation of a second or subsequent Clearinghouse on the network.

You install the first Clearinghouse when you install the Services System Software. Follow the steps in the Server Software Installation chapter in the *Services Installation and Setup Guide* if you are installing the first Clearinghouse on the network. These steps require you to install Clearinghouse software, add a domain, add yourself as a user, and give yourself certain access rights. This information should already be filled out on the Services Installation Worksheet.

CAUTION: Do not upgrade a Clearinghouse running software version 5.0, 6.0, or 7.0 directly to version 10.0. Upgrade first to version 8.0, then to version 10.0.

Hardware requirements

The Clearinghouse Service runs on an 8000 or 8090 server. When determining your server size, consider the amount of disk space the Clearinghouse Service, its growing database, and coresident services will consume, as well as the volume of Clearinghouse Service network users.

Software requirements

The Clearinghouse Service requires these program files:

- ClearinghouseSDF.bcd
- CHSAnnouncer.bcd
- ClearingHouseService.messages
- DistSVCConfig.bcd

When determining disk pages to allocate for a new Clearinghouse, keep these guidelines in mind:

- Allow 50 disk pages for the Clearinghouse Service software.
- Allow at least 2000 disk pages for one Clearinghouse database.
- If the Clearinghouse has more than one domain, add 300 disk pages for each domain.

Dependencies and limitations

The Clearinghouse Service has these dependencies and limitations:

- For small installations with a single Clearinghouse Service, domain replication is not possible. A File Service is necessary to manually back up and restore the Clearinghouse database.

- The Clearinghouse depends on the Mail Service to propagate updates if both services are coresident. The Clearinghouse must verify that the Mail Service is always running. Be alert to Clearinghouse messages indicating that a Mail Service is not started. Prompt action can ensure consistency of the local and remote Clearinghouse databases.
- For multiple internetworks, the Clearinghouse depends on the External Communication Service and the Internetwork Routing Service for communication.
- Up-to-date databases depend on consistent domain replication and the arrangement of replicated databases among the Clearinghouses. See "Replication" under "Planning for setup" later in this chapter.
- A Remote Batch Service should not be coresident with the Clearinghouse Service.
- A Clearinghouse Service domain is limited to approximately 200 to 300 users and their associated resources.
- The Clearinghouse database size can only be increased, not decreased.
- Do not operate the Clearinghouse Service while it is unplugged from the Ethernet. This action may disrupt the consistency of the Clearinghouse database, and may destroy or make unusable a domain or organization for 30 days.

Clearinghouse Service worksheets

Use the Clearinghouse Service Worksheet to record server-related and service-related data. Use the Clearinghouse User Directory Worksheet and the Clearinghouse Group Member Directory Worksheet to record information for the Clearinghouse Service database. The worksheets are at the end of this chapter.

Fill out separate copies of the worksheets for each Clearinghouse Service for which you have System Administrator responsibility. Make copies of the User Directory Worksheet and the Group Member Directory Worksheet to use as your Clearinghouse database expands. Retain the original worksheets for future use, and store the completed worksheets in the *Activities Guide*.

Using the worksheets

Before you install the software and set up a Clearinghouse Service, complete all three worksheets. It is important that you fill out the worksheets accurately and update them whenever changes occur.

The completed worksheets save you time as you perform the setup and maintenance procedures. They also serve as an information source for new System Administrators unfamiliar with your network configuration.

Filling out the worksheets

As you read the rest of this chapter, you are directed to make entries on the worksheets.

Use section ① on the Clearinghouse Service Worksheet for information about the server and the services installed on the

server. Copy this information from the Services Installation Worksheet you filled out while reading the Services System Software chapter of this book.

Use sections ② and ③ to record domain and organization information for the Clearinghouse.

Use the Clearinghouse User Directory Worksheet to record the name, password, description, home File Service and alias for each user you register in the Clearinghouse database.

Use the Clearinghouse Group Directory Worksheet to record the names and access privileges of the members in the user groups in the Clearinghouse database.

Planning for setup

After you install the Clearinghouse Service, initialize it by naming the service and making it accessible to network users. When initialization is complete, you can add or replicate a domain, add users, add user groups, and establish access rights. See the Clearinghouse Service chapter of the *Services Installation and Setup Guide* for complete setup procedures.

Naming conventions

As System Administrator, you assign names to network objects and register them in the Clearinghouse database. These naming conventions apply to all objects, including users.

Types of names

Clearinghouse Service name

During initialization, you name and describe the Clearinghouse Service. You did this for the first Clearinghouse Service when you first installed and set up your services on your network. If you are adding a second or subsequent Clearinghouse Service, you need to create a new, unique name for each Clearinghouse Service you set up.

Filling out the worksheet:

① On the Clearinghouse Service Worksheet, fill in the name and description of the Clearinghouse Service.

Fully qualified (three-part) name

Every network object has a name. The Clearinghouse Service requires that all network objects have three-part, or "fully qualified," names. The parts are the local name of the object or user, a domain name, and an organization name, in this format:

Name:Domain:Organization

For example, the fully qualified name for Thomas J. Taylor might be:

Thomas J. Taylor:Chicago:Xerox

With each fully qualified name, the Clearinghouse associates a unique set of properties that define the object with that name. For example, the Clearinghouse may associate a user name not only with the user's password, but also with a File Service and a Mail Service, enabling the user to access these objects easily. You can obtain the property information associated with a name at any Clearinghouse Service.

Local name

The local, or distinguished, name is the name of the object or user, and must be unique within the domain. A distinguished name for a user typically consists of a first name, middle initial, and last name, such as Thomas J. Taylor. A distinguished name for a service might indicate the service function or location, such as "Printer1."

Domain name

The domain name represents a geographical grouping such as a building or city; for example, "Chicago." All objects within a

domain have the same domain name. Every domain name must be unique within the organization.

Organization name

The organization name is typically the company name, such as "Xerox." An organization is the name given to the whole network community. A network community consists of the elements that communicate on the same network or on another network within the internetwork owned and managed by the company. Very large internetworks can have more than one organization name.

Shortcuts for naming

For your convenience, you can use two shortcuts to avoid using fully qualified names.

Defaults

If you are using a remote network with the same organization name as yours, you can omit the organization name. For example:

Thomas J. Taylor:Chicago

If you are entering information from the network for your organization and domain, you can omit the organization and domain names and use the local name alone. For example:

Thomas J. Taylor

Aliases

The Clearinghouse Service supports the use of aliases for quicker log-on to workstations and for quicker mailing. You specify multiple aliases when you add users to the Clearinghouse. Use an alias instead of a local name.

For example, the local name "Thomas J. Taylor" might have the alias "TTaylor." Like local names, each alias must be unique.

Naming guidelines

Keep these guidelines in mind as you create names to be registered in the Clearinghouse:

- Names can contain uppercase, lowercase, or mixed-case letters.
- Names can contain spaces.
- Names may not contain asterisks, colons, or characters not accessible through the default keyboard. This includes the neutral double quote, apostrophe, backslash, circumflex, accent grave, vertical bar, and tilde.
- The local name can be up to 40 characters long. The domain name can be up to 20 characters long. The organization name can be up to 20 characters long.
- The Clearinghouse Service rejects duplicate names for objects to be registered in the same domain.
- Avoid using first names as local names or aliases for users. This practice invites future problems with duplicate names. Similarly, do not use a generic name for an object, such as "Printer" for a printer.

- Apply geographically significant names to domains. Domain names must remain meaningful for the lifetime of your network. Avoid naming domains for departments of the organization, such as "Accounting" or "Finance." Also, avoid acronyms corresponding to current organizational structures.
- All internetwork network sites should establish unique organization names. Unique names make possible mail exchange between separate internetworks or future interconnection of internetworks. The Xerox Software Control Center must approve all organization names.

Users

The Clearinghouse Service registers information about network users. Only registered users can use the services available on the network. Check the spelling of user names, and discuss passwords and aliases with each user.

User information guidelines

Keep in mind these items when deciding on user information.

- Make sure that no two users have the same user name. If they do, use abbreviations or add initials to distinguish between users.
- Encourage users to select passwords they will easily remember. To prevent other users from guessing passwords, recommend passwords of six to eight characters. The maximum password length is 40 characters. It is recommended that you not keep a record of user passwords, or if you do, keep it in a secure place.
- For user description, include office numbers, telephone numbers, and job functions. The maximum length for a user description is 100 characters.
- Assign the Home File Service on which the user will store his or her 6085/8010 desktop.

Filling out the worksheet:

On the Clearinghouse User Directory Worksheet, fill in the user name, password, description, Home File Service, and alias.

User access controls

You perform most Clearinghouse Service security tasks. However, authorized users can access the Clearinghouse to change their own passwords or their membership in groups.

By administering access controls, you grant users the right to change limited information in the Clearinghouse database. Two kinds of access rights to Clearinghouse data are available:

- Administrative access - Enables users to change any information on any object at a specified security level within the Clearinghouse database: organization, domain, or group.
- Self access - Enables users to add themselves to, or remove themselves from, user groups.

All users added to the Clearinghouse database have access rights to change their own password. Users may want to change their passwords for personal security.

Types of access controls include:

Access to organizations

A user with administrative access to an organization is an Organization Administrator. As an Organization Administrator, you can create domains in the organization as well as change access controls for the organization. Only you can delete the last copy of a domain in the organization.

The Xerox Software Control Center issues organization-specific passwords to control and authorize the creation of organizations.

Access to domains

A user with administrative access to a domain is a Domain Administrator. Domain Administrator status lets you create and delete entries in the domain. It also lets you copy (replicate) a domain among multiple Clearinghouse Services, delete copies of the domain, and change the access controls for the domain. An Organization Administrator automatically has administrative access to the domain.

Access to users

Users have administrative access to their own passwords so they can modify their passwords.

A Domain Administrator has administrative access to all user entries in the domain. A Domain Administrator can modify the fields of the user entry (description, password, home File Service, aliases) and change user mailboxes (Mail Service).

Access to user groups

Both administrative access and self-access controls protect user groups. Administrative access permits the addition or deletion of members in the group and the setting of group access controls. Administrative access to a domain does not guarantee administrative access to all user groups in the domain.

The Domain Administrator has implicit administrative access while creating groups. After the Domain Administrator sets explicit administrative access to a group, all implicit rights are canceled. The Domain Administrator who wants to retain administrative access to a group must explicitly assign administrative rights to himself or herself, or make no explicit assignments.

A user with administrative access to a group is a Group Administrator. A Group Administrator can add and delete group members. A Group Administrator also controls the privileges associated with self access; see "User groups" next in this chapter for more information.

Access to services and other entries

Administrative access controls protect domain entries (other than users and user groups). The self-registration of services creates a variety of entries in the Clearinghouse Service. The administrator invoking the self-registration must have administrative access to the containing domain. Thereafter, administrative access to the domain gives administrative access to the entries themselves. The Domain Administrator can change and delete entries using the appropriate service-specific commands.

You cannot change the access controls on service and other entries in a domain.

Filling out the worksheet:

① On the Group Member Directory Worksheet, indicate whether each member has administrative access and self access rights.

② On the Clearinghouse Service Worksheet, record the name of the Domain Administrator and the access privileges.

③ On the Clearinghouse Service Worksheet, record the name of the Organization Administrator and the access privileges.

User groups

You can register a collection of users as a user group in the Clearinghouse Service. The existence of a group enables users to specify all group members by one group name, eliminating the need to enter individual user names. This practice is especially handy for mailing--the user can specify a group name for mail distribution instead of individual user names.

Membership in a group

The members of a group can include individual users, other groups, and patterns.

Users Add an individual user as a member by specifying the user's name or alias. The members of a group may be registered in the same domain as the group itself, or they can be registered in another domain or organization.

To ensure accurate results when you list group members, do not use aliases when adding users to the group.

If you are a Group Administrator attempting to add yourself to your group's membership list, you must have self-access privilegeS, or the operation will fail.

Groups Add one group as a member of another group by specifying its name. All members of the added group are then considered members of the new group.

To ensure accurate listings of group members, do not use an alias to add a smaller group to a larger group.

Patterns Add a pattern as a member of a group by specifying a name containing one or more asterisks. In a pattern, the Clearinghouse treats the asterisk as a wildcard that matches any user name, domain, or organization. For example:

- The pattern "*" indicates all users in the default domain.
- The pattern "*:Chicago:Acme" indicates all users in the domain "Chicago:Acme."
- The pattern "*:*:Acme" indicates all users in the organization "Acme."
- The pattern "*:*:*" indicates all users in the internetwork.

The patterns that you can add to groups are restricted. You can choose not to specify the local name, or the local and domain names, or all three parts of the fully qualified name. Other combinations are invalid.

Here are some examples of valid and invalid patterns:

Valid patterns	Invalid patterns
*:Chicago:Acme	*Smith:Chicago:Acme
::Acme	Smith:*:Acme
::*	*:Chicago:*

For convenience, group membership should consist of only one pattern and be named according to the pattern. A group named "All Chicago" could contain the pattern "*:Chicago:Acme," representing all users in the domain and organization "Chicago:Acme."

A convention for setting up groups is to follow a hierarchical structure as in an organization chart. It is easier to maintain a hierarchical set of groups than an equivalent number of unstructured groups.

For example, suppose your Customer Support Division contains a Training Department and a Service Department. You can create two groups, "Training" and "Service," and add the appropriate individuals as members of each group.

To represent the division, you create a third group named "Customer Support" and add the "Training" and "Service" groups as members. Later, if you delete a member from the "Training" group, that member is automatically removed from the "Customer Support" group.

Group access controls

Each user group has one or more Group Administrators who can change the membership and access controls of the group. The Group Administrator also controls the privileges associated with self access. Group access controls have three categories:

- *Open group* - Self access allows users to join or leave the group at will.
- *Closed group* - Self access allows members to leave the group but prevents non-members from joining. Only a Group Administrator can add new members.
- *Controlled group* - Self access does not exist. Members join and leave the group only by action of the Group Administrator.

Group use guidelines

Use groups to simplify mailing, file drawer access control, or both.

- *Mail groups* - Groups used as mail distribution lists can contain patterns. You can choose not to specify the local name only. For example:

Valid pattern	Invalid patterns
*:Chicago:Acme	*:*:Acme
	::*

- *Access control groups* - When you define access control for a group, the group can contain users, other groups, or patterns. Generally, use only closed and controlled groups as access control groups.

NOTE

The time the Clearinghouse needs to determine whether a name is a valid group member increases with the number of names in the group. Unacceptable access- checking times may result when a group contains 100 individual names. Try to use patterns to represent large numbers of individuals. Do not use heavily nested groups, that is, groups containing groups containing groups, for frequently used access control groups.

To create groups for both mail distribution and access control, combine these guidelines.

Filling out the worksheet:

On the Clearinghouse Group Member Directory Worksheet, fill in the group name, description, Group Administrator, and member names. Also fill in the access privileges for each group member.

Replication of domains

The Clearinghouse Services on an internetwork actively cooperate to form a unified Clearinghouse system. You can increase the reliability, availability, and efficiency of your Clearinghouse system by replicating your domain within one or more additional Clearinghouse Services.

Domain replication duplicates a domain on multiple servers. Replication provides:

- A reliable database despite inadvertent damage to any copy of the domain information
- Readily available domain information despite server or communication failures
- Efficient access to the database despite geographically dispersed users

Replication also eliminates the need for manual backup of the database. If a Clearinghouse Service database is lost, you can rebuild it by re-initializing the Clearinghouse Service and then copying back all the domains that resided there.

In very small installations, the Clearinghouse may reside on a single server. In these cases, you must perform manual backup and restoration of the database on a File Service. (See the Clearinghouse Service chapter in the *Backup and Restore Guide* for complete details.)

When to create a new domain

Create a new domain when no appropriate domain exists. For example, you create a new domain when you install the first Ethernet network at a site, or when you connect a new Ethernet to its parent company.

See the "Planning for maintenance" section later in this chapter for more information.

When to add a copy of a domain

Increased reliability, availability, and efficiency are factors that may influence your decision to replicate domains.

To increase reliability
Many user, group, and machine entries for a domain may change each day. Suppose the disk on the only Clearinghouse server in the internetwork fails. Re-entering all the changes that occurred between the time of the last backup and the time of the failure would be time-consuming. A replicated domain saves you that time.

To increase availability
Many network resources are unavailable when all Clearinghouse Services for a domain are unavailable. Replicating a domain within many Clearinghouse Services increases availability of the domain.

However, replicating a domain also increases both the amount of disk space devoted to the Clearinghouse system and the amount of work the system must perform to answer user queries and still maintain consistency of the distributed database. For these reasons, you must balance availability needs with making the best use of available resources.

To increase efficiency
Users experience long delays accessing a domain that does not reside on their local Ethernet. Replication helps to eliminate this delay.

Configuration guidelines

You need to select an appropriate configuration of replicated domains at each Clearinghouse Service. Here are some guidelines to help you decide when to replicate a domain:

- Each Ethernet network should have an attached Clearinghouse Service containing its local domain.
- Each domain must exist on at least two Clearinghouse Services to provide reliability and availability in case of server malfunction. For example, if your organization has only one Ethernet network and multiple servers, install two Clearinghouse Services and replicate your domain to the second Clearinghouse Service. If your network is connected to other networks, replicate your local domains to one or more Clearinghouse Services on the other Ethernet networks.
- Heavily used remote domains should be replicated near the site of their usage. If a particular remote domain is popular among local users, place a copy of that domain on the local Clearinghouse Service.
- Monitor the global configuration of the entire Clearinghouse database, and check the distribution of the various replicated domains. In general, replicate a domain on two to five Clearinghouse Services.

NOTE

If a domain does not exist on at least two Clearinghouse Services, the Clearinghouse response time may be slow. Over-replication (on more than five Clearinghouse Services) consumes excessive amounts of server disk space and increases the overhead of update propagation.

You can replicate a domain as long as at least one Clearinghouse Service serves that domain.

Procedural considerations

Be aware of these considerations for replicating domains:

- You must have access to the server's domain and the domain to be replicated.
- The destination Clearinghouse Service must contain sufficient space before you replicate your domain.
- If you plan to replicate a Clearinghouse domain from a different network to your network, initialize the Internetwork Routing Service before you replicate the domain. Request the Domain Administrator from the other network to give you temporary Domain Administrator access to the domain to replicate. If the domain to be replicated is in a different organization, you must also have temporary Organization Administrator access to the source organization.

A special case exists when a new network is added to an existing internet. The new network requires its own Clearinghouse. Initializing this Clearinghouse includes adding domains to it, in particular, the domain that will function as the local domain for the new network.

The recommended procedure in this case is to request the System Administrator of the existing Clearinghouse which you are replicating to set up the domain and register you as the System Administrator for the new network. You can add the domain to the new Clearinghouse when the new network has been linked to the internet and the new Clearinghouse installed.

When a new domain is replicated, its information propagates to all Clearinghouses for the organization.

NOTE

Avoid replicating a domain from a Clearinghouse running one version of software to a Clearinghouse running a different version of software. The databases remain inconsistent and may cause other difficulties.

Filling out the worksheet:

② On your Clearinghouse Service Worksheet, record the size of your domain and the name of the Clearinghouse (domain:organization) to which you are replicating the domain.

Planning for maintenance

After you install and set up the Clearinghouse Service, you are responsible for maintaining it properly. You perform maintenance as needed; there are no scheduled duties.

See the Clearinghouse Service chapter in the *Services Maintenance Guide* for the complete maintenance procedures.

Changing user information

Your System Administrator duties for users include adding new users as your organization expands, changing existing user information, and deleting users who are no longer working on the network.

User name

To change a user's registered name (for example, to reflect a change in marital status), first give the user a new identity, without removing the old identity.

The name identifies the user's group membership, file drawer, mailbox, and desktop. While the old and the new identities exist, change all occurrences of the old name to the new name.

- If the user is in a group, remove the old name and add the new name to all groups.
- Change the old name to the new name in access lists to the file drawers in which the user has explicit access. (See the File Service chapter in the *Services Maintenance Guide*.)
- If the user has a mailbox, tell the user to read all mail. Then delete the user's current mailbox from the Mail Service and add a new mailbox with the new name. Inform users on the network of the new name so they can address electronic mail properly. (See the Mail Service chapter in the *Services Maintenance Guide*.)
- Ask users of 6085/8010 workstations to store all documents, record files, and folders that are to be saved by moving them to the File Service or copying them to floppy disks. Retrieve these items after the name change.

Related procedure: Changing a user's registered name

Password

You may want to have users regularly change their passwords to maintain system security. Only a Domain Administrator or the user can change the password.

Related procedure: Changing a user's password

Home File Service

If you change a user's home File Service, tell the user to move his or her desktop to a workstation and leave it there until the Clearinghouse Service change has been completed and all

Clearinghouse Services serving the domain have noted the change (up to one week later for large internetworks).

Related procedure: Changing user information

Changing user groups

As a System Administrator, you may also be required to add new user groups or to delete groups. In addition, you may need to perform the following tasks.

Assigning group membership

Adding or deleting users to or from groups requires administrative access to the group, or self access if the user is adding or deleting himself or herself. Users can change their own group membership when you give them self access. Letting users control their passwords and group membership can help free your time for other System Administration duties.

You can explicitly name users, user groups, or patterns as new group members. Use a fully qualified name when deleting a user from a group.

Related procedures: Adding user groups and members, Deleting a member from a group

Controlling group access

Explicitly delegating administrative access to a group immediately revokes the implicit access of the System Administrator. After explicit delegation, any user with administrative access can grant or revoke the administrative access of any other user. Trying to grant administrative and self access in the same command fails unless the System Administrator has explicit administrative access.

Domain Administrators always retain the power to delete any user group, whether or not they have administrative access to it.

Related procedure: Changing group access

Showing object information

You can list or show information about these objects, depending on your configuration.

Aliases	Mail Services
Boot Services	Members
Communication Interface Units	Print Services
Communication Monitoring Services	Organizations
Domains	Remote Batch Services
External Communication Services	RS232C Ports
File Services	Servers
Gateway Services	Users
IBM 3270 Hosts	User Groups
Interactive Terminal Services	Workstations

You cannot list or show information about these services or products: Adobe Service, Librarian Service, SNA Mail Relay, SNA Access, or Foreign Gateway Assistant.

You can delete any object registered manually in the Clearinghouse database to partially remove a service, but you cannot remove all objects in an effort to remove a service. Instead, expunge a service to automatically delete all entries associated with it. See "Expunging a Clearinghouse" at the end of this chapter.

Related procedure: Showing objects registered in a domain

Maintaining domains

As a System Administrator, you need to assign administrative access privileges to each domain, compare databases to maintain consistency, and determine when to add new or delete unused domains.

Domain access

You can give a user administrative access to a domain. You can also define an administrative user group in the domain and give the group administrative access. Any member you add to the group automatically receives this administrative access.

Related procedure: Changing domain access

Domain consistency

Xerox Network System services are designed to take advantage of continuous internetwork links and continuous operation of all servers. All objects on the internetwork (servers, services, and workstations) depend on the Clearinghouse Service for up-to-date information about network resources.

When multiple Clearinghouse Services exist in an internetwork, each must be able to provide accurate and up-to-date information to its network clients. All Clearinghouses in an internet communicate to ensure consistency of the Clearinghouse databases.

When a new Clearinghouse is added to the internetwork, it notifies all Clearinghouses of its name and the domains it serves. Additionally, Clearinghouses serving the same domain as other Clearinghouses automatically send update messages to each other when changes to the domain occur.

To ensure that all Clearinghouses are consistent and have received all necessary update messages, each Clearinghouse Service performs an automatic consistency check between 12:00 midnight and 6:00 a.m. local time. Internetworks that depend on transient links (links that are not up 24 hours a day) may not receive these automatic consistency checks.

Inconsistencies sometimes result from interrupted server operation. If you notice inconsistencies lasting longer than 24 hours, you can manually correct them by comparing databases between domains. Also see "Comparing Clearinghouse databases" later in this chapter.

Compare databases with the nearest Clearinghouse Service containing a copy of the affected domain. Comparing databases does not change the domain replication configuration among the Clearinghouse Services involved. Instead, it compares the various copies of each replicated domain, and reconciles any differences.

Related procedure: Correcting domain inconsistency

New domains

Under these circumstances, you may need to create a new Clearinghouse domain:

- When you create the first domain in your internetwork. Use the special Genesis procedure described in the Server Software Installation chapter in the *Services Installation and Setup Guide*.
- When a new network is about to join your internetwork through the Internetwork Routing Service.

You can use one of two ways to create a domain in normal operation:

- If the new network is to share your domain, you need only make the remote System Administrator a Domain Administrator of your existing domain.
- If the new network is to have a new domain of its own, you must create the new domain on your Clearinghouse Service. You must be an Organization Administrator to create a new domain.

Use the correct spelling and capitalization for new domain and organization names; these names are difficult to correct later.

When you add a domain, a message may appear warning you that the database is full. You must immediately boot the server and expand the Clearinghouse Service database. The Clearinghouse Service adds the new domain as soon as the database has been expanded. See "Expanding the database" later in this chapter.

Related procedures: Adding a copy of a domain (replicating), Creating domains

Old domains

If a domain or copy of a domain no longer needs to reside on your Clearinghouse Service, you can delete it from the Clearinghouse Service databases. You must have Domain Administrator status to delete a domain.

Delete a domain to:

- Rearrange the replication pattern of the domain (remove one or more replications of the domain). Usually, the local System Administrator determines that the copy on the local Clearinghouse Service is no longer needed.

  You must have administrative access to the domain of the server and the domain you are deleting.
- Eliminate the domain altogether. You must delete the domain on all Clearinghouse Services holding the domain. If the domain to be deleted is the last domain in a network, the system tries to delete the organization. You must have

administrative access to the organization to delete an organization. When you delete the last copy of a domain, you cannot create a domain or organization with the same name for approximately one month.

To delete the last domain in a network, you must be an Organization Administrator and logged on to the Clearinghouse Service that has the last copy of the domain you are deleting.

CAUTION: Never delete a domain unless you know it is replicated elsewhere, or is no longer needed in your internetwork.

Related procedure: Deleting a domain

Maintaining organizations

You must have administrative access to the organization to grant or revoke organization administrative access to other users.

Related procedure: Changing organization access

Registering Print Services

Normally, services are self-registering; you do not need to manually register them in the Clearinghouse database. The exceptions are the Print Services. Register the Print Services on your network with the Clearinghouse.

Related procedure: Enabling manual registration

Expanding the database

If your Clearinghouse domain expands, or if you add new replicated domains to your local database, you may need to expand the Clearinghouse database. Always allow about 25 percent free space at all times to allow for a safety margin, and accommodate copies of additional domains.

Expand the database if:

- The database is full from gradual expansion of existing domains. Provide a reasonable number of free disk pages, based on the amount of further anticipated growth.
- You are about to add a new copy of a replicated domain to an already-full database.

The Clearinghouse database is always sized in multiples of six disk pages. Numbers are rounded down automatically.

Related procedure: Expanding the Clearinghouse database

Comparing Clearinghouse databases

Some network communities do not keep their Internetwork Routing Service links continually interconnected between Ethernet sites. In some cases, servers are powered down each night, as well as on weekends and holiday periods; or are connected by manually-dialed telephone lines. You must manually update Clearinghouses across these types of

internetwork links to maintain the consistency of Clearinghouse databases. See "Maintaining domains" earlier in this chapter.

Comparing databases does not change the domain replication configuration among the Clearinghouse Services involved. Instead, it compares the various copies of replicated domains, and reconciles any differences.

Perform manual consistency checks by comparing databases every other day at internetworks that use manually-dialed telephone lines or have servers that are powered down at night.

Also compare databases when one of these conditions exists:

- A Clearinghouse Service has been down for more than a day.
- You have just established an Internetwork Routing Service link joining internetworks. The first time you perform a comparison in this case, you must enter the network address instead of the Clearinghouse name during the procedure.
- The network addresses of two Clearinghouses change simultaneously when multiple servers containing Clearinghouse services are moved to new Ethernets, or when multiple servers containing Clearinghouse services receive new processor IDs.

  In this rare circumstance, do not bring the Clearinghouse services with the new addresses online until you compare each with a Clearinghouse that has not either been moved or had its processor ID changed. If all Clearinghouses on an entire internetwork have been moved, pick one and use it as the target for a compare operation.

You need to decide which Clearinghouses to compare so that domains served on opposite sides of manually-dialed telephone lines are consistent, and so that all Clearinghouses separated by dial-up links obtain a consistent view of other Clearinghouses on the internetwork. Each Clearinghouse must know the addresses of the other Clearinghouses and the domains they serve. It does not matter which of the two Clearinghouses involved in a database comparison operation is the initiator or the target of the operation.

Databases are compared in background, so all Clearinghouse Services can serve their network clients while the operation is running. System Administrators must coordinate the operation to ensure the necessary links are connected, and the appropriate target Clearinghouses are selected. After comparison, leave the links connected for an additional 15 minutes to allow all resulting update messages to propagate to those Clearinghouses on the internet that were not directly involved in the operation.

Domain inconsistencies sometimes result from slow update propagation. Never manually update multiple copies of a domain by adding or changing the same piece of information in each Clearinghouse Service that serves the domain. This process cancels any updates already processed. For example, if you think a user entry has been lost, and you add it again, the user's mailbox location is canceled. You then have to add the mailbox again before the new user can receive mail.

Related procedures: Correcting domain inconsistency, Manually updating Clearinghouses connected by dial-up links

Example Clearinghouse comparisons

The following figures show different internetwork configurations and explain the database comparison operations for each.

Figure 4-1 shows an internetwork with two networks connected by a dial-up Internetwork Routing Service link. Domain A is served on both sides of the link. Domain B is served only at Network 1. A single database comparison operation, performed every other day between CHS X and CHS Y, will take care of all necessary consistency checks.

Figure 4-1. **Internetwork with two networks**

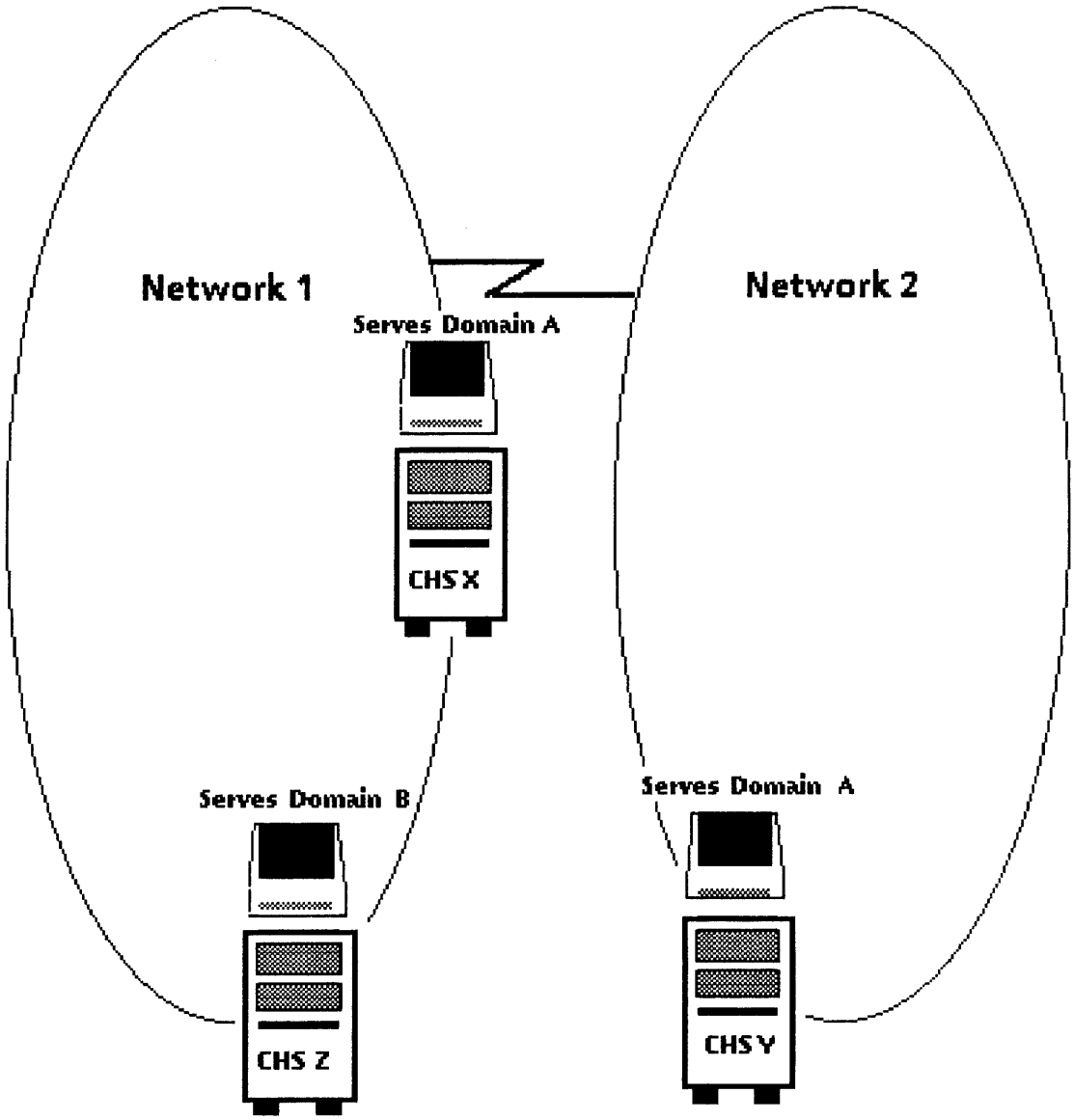


Figure 4-2 shows an internetwork with three networks interconnected only by Internetwork Routing Service links. Domains A and B are served at all sites, and Domain C is served at sites 2 and 3. Use the following schedule for comparing databases for this configuration:

On Monday, compare CHS W with CHS Z.
On Monday, compare CHS X with CHS Y.

On Wednesday, compare CHS X with CHS Z.
On Wednesday, compare CHS X with CHS Y.

Continue to alternate between these two sets of operations every other day. Because domains A and B are served at all three sites, they are compared between CHS W and CHS Z on one day, and between CHS X and CHS Z two days later. This way, all instances of the domains are regularly included in a database comparison.

Figure 4-2. **Internetwork with three networks**

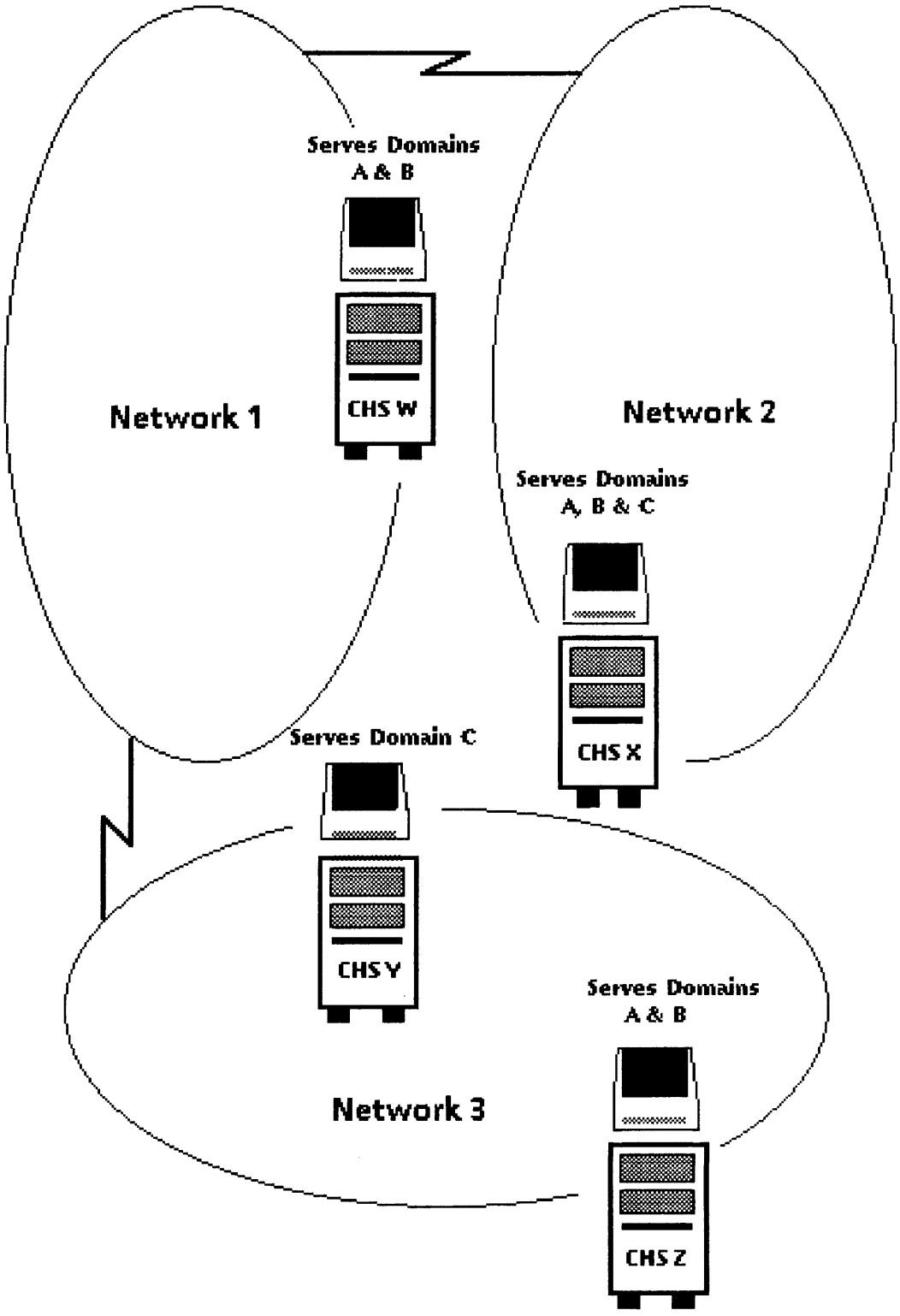
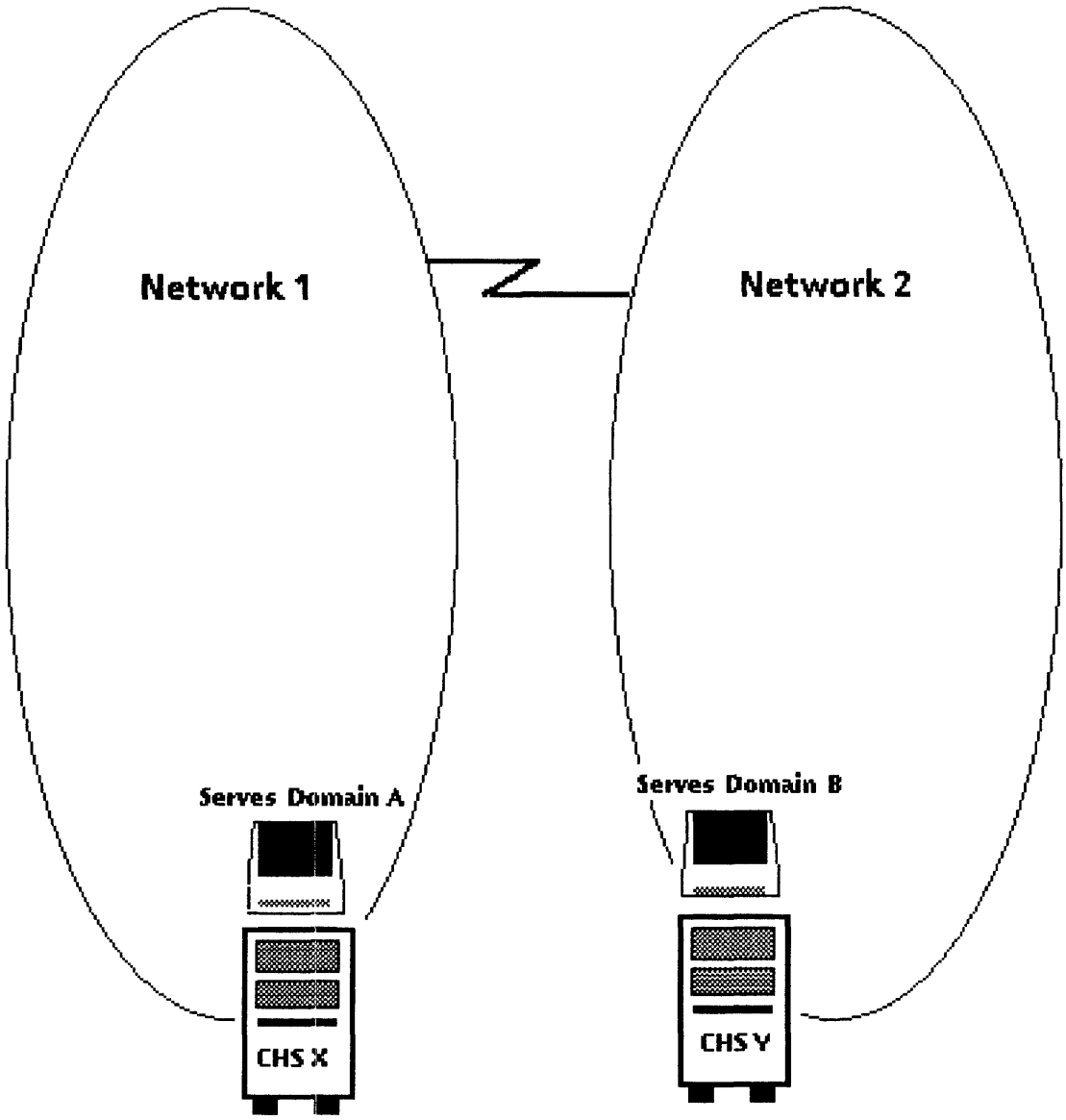


Figure 4-3 shows an internetwork with two Ethernet networks that are interconnected by an Internetwork Routing Service link. Although no domain is served on both sides of the internetwork link, the System Administrator should perform one database comparison operation between any two Clearinghouses that are on opposite sides of the link. This comparison ensures that all Clearinghouses on the same internetwork are kept up-to-date on the addresses of the other Clearinghouses and domains they serve.

Figure 4-3. **Internetwork with two networks, no common domain**



You also can ensure consistency between internets connected via internetwork links by:

- Establishing continuous internetwork links using leased or X.25 lines.
- Establishing your transient links at least every day between midnight and 6 a.m. If your internetwork spans different time zones, you may not be able to ensure that all necessary links are up during this period in the local time zones. If your internetwork community spans time zones, elect one of the other two options, or depend on manually comparing databases.
- Permanently decommissioning some or all of the links and replacing them with an External Mail Gateway.

Merging internetworks

Combine your internetwork with another to form one large internetwork by establishing a link between a pair of Internetwork Routing Services (one on each internetwork). The Clearinghouse software merges the Clearinghouse databases of the two internetworks into one database.

Merging internetworks creates a permanent connection. Do not try to merge internetworks temporarily, because you cannot divide the merged database back into two separate databases. Note the following considerations:

- Merging two separate networks places a heavy burden on all Clearinghouses in both networks. Before attempting a merge, consult your Xerox Systems Analyst.
- Maintain and routinely check all communication links, because all Clearinghouse services must keep each other informed about changes to the distributed databases. See the Internetwork Routing Service chapter of this book for guidelines on monitoring the links.
- Do not merge internetworks as a substitute for Clearinghouse replication.
- Merge internetworks only during off-peak hours. The Domain Administrator of each domain must perform this procedure. The Domain Administrators should be in contact by telephone to ensure that the merge is done simultaneously.
- Do not merge two internetworks that have domain names in common.

Contact the System Administrator of the other network, and exchange network addresses. After the Internetwork Routing Service link is established, begin merging the two Clearinghouse Service databases.

Related procedure: Merging internetworks

Expunging a Clearinghouse

Erasing the Clearinghouse database recovers server disk space and removes the Clearinghouse database from the Clearinghouse system.

Expunge the Clearinghouse if you are moving a Clearinghouse Service to another server. Be sure to replicate the domains

contained in the Clearinghouse database to another server before you remove the Clearinghouse Service.

Also expunge Clearinghouses to remove unwanted Clearinghouse Services. If you try to individually delete the objects in a Clearinghouse Service without doing an expunge, you will have problems with the Mail and Clearinghouse systems.

Before you expunge a Clearinghouse Service from a server housing a Mail Service, list all files and ensure that the file "MailServiceSDF.bcd" is on the disk. If the file is on the disk, then continue with the expunge operation. If it is not, reinstall the Mail Service before you expunge the Clearinghouse.

Occasionally a server may crash during an expunge. The server can recover automatically, and will resume the expunge operation. In very large networks (more than 50 Clearinghouses), this second expunge attempt can take up to two hours.

After a Clearinghouse Service is expunged, do not reuse the name of that service for 30 days. If you reuse the old Clearinghouse name too soon, the server will crash.

If a Clearinghouse database is damaged or erased, do not expunge and reinstall the Clearinghouse Service. This procedure causes unnecessary global database updates for the new Clearinghouse name. See the *Backup and Restore Guide* for information on and procedures for recovering a damaged or lost database.

Related procedure: Removing the Clearinghouse Service from a server

5. Mail Service

This chapter helps you prepare for installation, setup, and maintenance of the Mail Service (MS) and its External Mail Gateway (EMG) option. The information supports the procedures you perform from an 8000 or 8090 server.

Service description

Using the Mail Service, network users in geographically dispersed locations can send messages and documents in a fast, convenient, and reliable way.

The Mail Service delivers messages almost instantaneously, whether the recipient is a user in the next office or in another city. Not only can all workstation users on a network communicate through electronic mail, but messages originating from geographically dispersed networks can also be exchanged across the internetwork over the External Mail Gateway or the Internetwork Routing Service.

In addition, users on terminals and workstations not on the internetwork can exchange mail messages with each other or with users on internetwork workstations over phone lines using compatibility services (see the 850/860 Gateway Service and Interactive Terminal Service chapters in this book). The Mail Service is directly accessible to all Xerox Network System workstations and to many non-networked, non-Xerox compatible devices that can dial up the appropriate compatibility service.

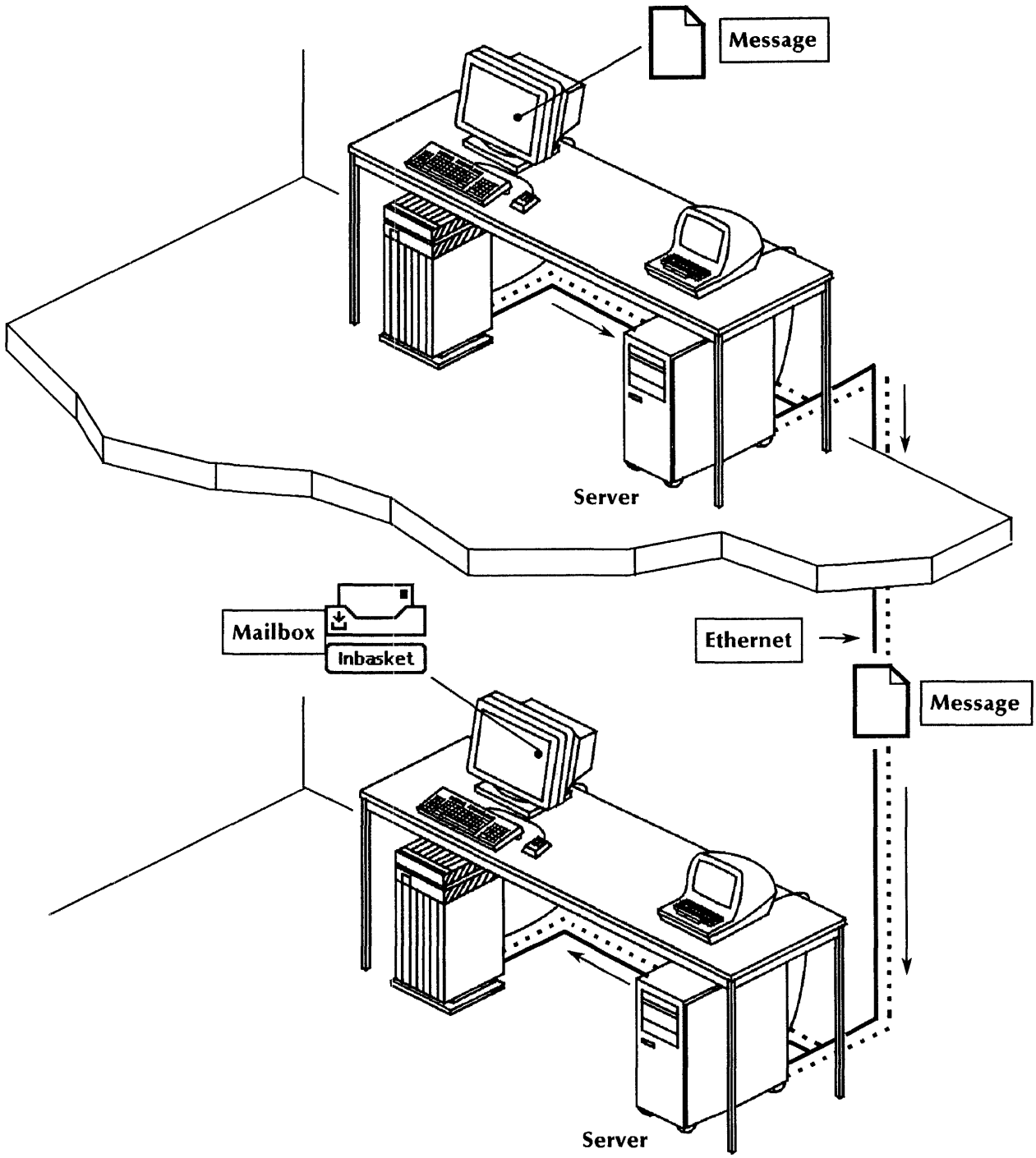
Mail Service features

An important feature of the Mail Service is its ability to handle information in a wide variety of formats. The Mail Service accepts information from personal computers, the 860 Information Processing System, and the 8010 and 6085 workstations. Documents with complex graphics created at a 6085 or 8010 workstation can be transmitted to remote locations, retrieved by users, and printed at a Print Service in minutes.

Another feature of the Mail Service is its ability to expand its database as the need arises. Users can be added to the existing service, and new services can be added to support growth.

Figure 5-1 illustrates the message transfer process between two 6085 workstations on an internetwork.

Figure 5-1. **Simple message transfer between two 6085 workstations**



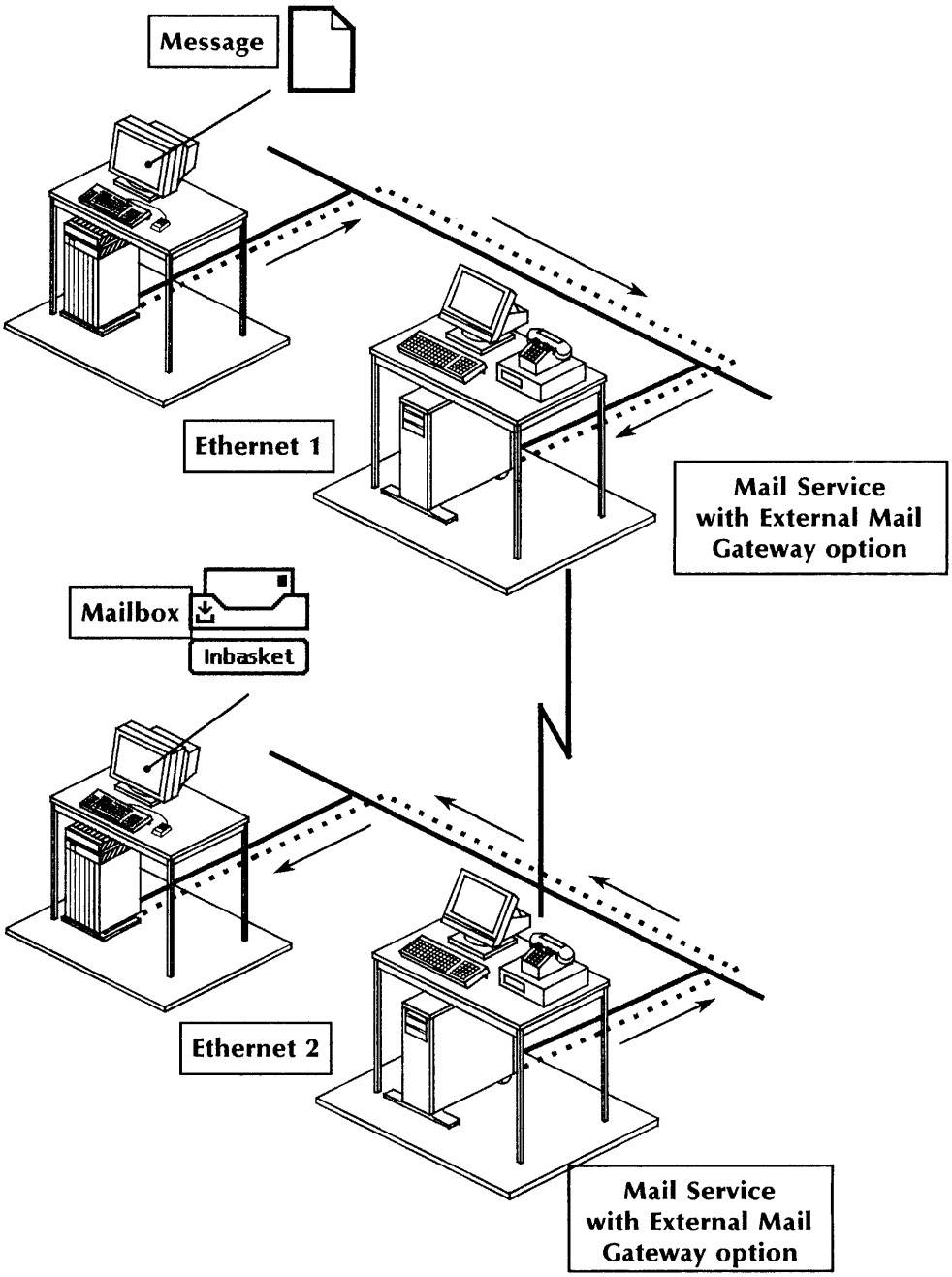
External Mail Gateway option

The External Mail Gateway option of the Mail Service allows mail exchange between internetworks, without merging the internetworks. Users on one internetwork can send mail

messages and receive them from the other internetwork, but cannot access other services there.

Figure 5-2 illustrates mail exchange between two internetworks using mail gateways.

Figure 5-2. **Message transfer between two internetworks using an External Mail Gateway options**



How the software works

Multiple mail services on the internetwork form a unified mail system. Each Mail Service can accept mail, hold mail for pickup, and forward mail to the recipient's Mail Service.

When a user sends a mail message, the workstation software locates the Mail Services of the message recipients. The software then selects the closest Mail Service, usually the local one, and uses it to send the message. Message processing begins with examination of the recipient list.

Recipient lists

The recipient list determines who receives the mail message. The list contains the names of individual users and/or names of distribution lists.

A distribution list includes all members of a user group registered in the Clearinghouse. All registered users can send mail to any existing distribution list.

To determine who is on a distribution list, the Mail Service interacts with the Clearinghouse Service. If the recipient list includes several distribution lists containing duplicate names, the Mail Service sends the message only once to each recipient.

After identifying the individual recipients, the Mail Service begins distributing the message. Local recipients (recipients with mailboxes on the distributing Mail Service) receive a copy of the message in their mailbox. To reach remote recipients (recipients with mailboxes on another Mail Service), the Mail Service forwards the message to the recipient's local Mail Service, which then places the message in the mailbox.

User mailboxes

The Mail Service requires a separate mailbox for each user. By holding mail in a mailbox, the Mail Service allows users to read their mail at their convenience from any workstation or terminal with Mail Service access.

Non-delivery notifications

If a message waits longer than two working days in a Mail Service's pending queue, or if a message is addressed to an unknown or invalid recipient, the Mail Service tries to return the message to the sender. The same conditions that prevent message delivery may prevent its return. In this case, the Mail Service holds the message and tries to return it at regular intervals.

If the Mail Service cannot return the message within two days, it deletes the message contents to protect the privacy of the sender and the recipient. The Mail Service then tries for two days to return the message heading (the subject, recipient list, and other information that helps the sender identify the message). If these return attempts fail, the Mail Service places the message heading in the local Postmaster mailbox.

External Mail Gateway operation

An External Mail Gateway establishes autodialed phone connections for transmitting mail from one Mail Service to another. Each Mail Gateway serves as the incoming connection point for a set of local domains, and as the outgoing connection

point, it can serve an unlimited number of foreign domains. For each foreign domain, however, only one Mail Service can serve as the outbound gateway.

When a user sends a message to another internetwork, the Mail Service places it in a special queue that the External Mail Gateway periodically polls. When the Mail Gateway finds a message, it tries to establish a phone connection with the Mail Gateway in which the recipients are registered. After making the connection, the Mail Service transmits the message and places it in the recipient's mailbox.

So that the Mail Gateway can establish connections when phone rates are lower, you determine its polling and delivery schedules. A gateway makes autodialed connections every 15 minutes during its calling interval when mail is waiting for delivery. You can specify multiple calling intervals, if necessary.

User interaction

All Xerox Network System compatible workstations, as well as devices with access to the internetwork through the 850/860 Gateway Service or the Interactive Terminal Service, can communicate with the Mail Service. They include the 6085 Professional Computer System, 8010 Information System, 850 and 860 Information Processing Systems, 820-II and IBM Personal Computers, and other devices. Because each system requires different instructions for accessing the Mail Service, consult the appropriate instruction manual for more information.

The following sections describe how users send and receive mail on the 6085 and the 860.

Using the Mail Service from a 6085 workstation

On a 6085 workstation, the Inbasket and Outbasket icons simplify sending and receiving mail notes, documents, folders, record files, and spreadsheets.

Mail notes are plain text messages without graphics. Any type of workstation or computer accessing the Mail Service can receive the mail note format. To send a mail note, the user copies or moves the Mail Note icon to the Outbasket icon and fills in the address information.

Users can mail documents containing graphics, or folders of such documents, in the same way as a mail note. However, to be retrieved at a workstation other than a 6085 or 8010, a document must be converted before it is sent. Although some formatting may be lost because of limitations at the receiving workstation, content is preserved.

When mail is received in a 6085 workstation user mailbox, a letter icon appears in the Inbasket icon. The letter icon remains visible until the user opens the Inbasket and retrieves the mail. After retrieving the mail, the user can view, forward, answer, or delete it.

Using the Mail Service from an 860 system

Users of an 860 Information Processing System can send plain text messages or enhanced documents containing graphics. The

860 system provides mail forms for sending plain text messages. Mail forms do not need to be converted to other formats to be read at different devices. To send a mail form, the user activates the Mail Service, fills in a mail form, and requests that it be sent.

When sending enhanced documents, the user attaches a mail form to the document. If a document is sent to a 6085 or 8010 workstation, the mail form may be read but the document must be converted to the proper format (using the converter icon) before it can be read. The conversion software enables the recipient to display the document at the workstation with most of the formatting preserved.

The 860 system has no visible indicator that mail has arrived in the user mailbox. The user must activate the Mail Service and display the mailbox contents. The user can then select a message to be read, answered, forwarded, or deleted.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the Mail Service Worksheet located at the end of this chapter. Fill out a separate worksheet for each Mail Service for which you have System Administrator responisbility.
- Installing the Mail Service software (and enabling the External Mail Gateway option, if required) as described in the Server Software Installation chapter of the *Services Installation and Setup Guide*.
- Setting up user mailboxes and the Postmaster mailbox as described in the Mail Service chapter of the *Services Installation and Setup Guide*.
- Setting up RS232C port parameters and inbound/outbound External Mail Gateway information as described in the Mail Service chapter of the *Services Installation and Setup Guide*.
- Maintaining your Mail Service as described in the Mail Service chapter of the *Services Maintenance Guide*.
- Setting backup parameters and performing backup procedures on a regular basis, as described in the Mail Service chapter of the *Backup and Restore Guide*.
- Upgrading software and hardware as required.
- Notifying users of any change or disruption in the service.
- Troubleshooting the service as described in the *Basic Network Troubleshooting*.

You can perform most Mail Service procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter in the *Services Installation and Setup Guide* contains the procedures for installing the Mail Service software and, if required, enabling the External Mail Gateway option. This section explains hardware, software, and other requirements for installation.

Hardware requirements

The Mail Service operates on an 8000 or 8090 server and requires no unique hardware. The External Mail Gateway option requires the RS232C Communication Kit; a 1200 to 2400 baud full-duplex modem; an autodialer; and a phone line.

Software requirements

The Mail Service requires Services System Software and these Mail Service program files:

- MailSDF.bcd
- MailStubConfig.bcd
- X25Config.bcd
- RS232CCommon.bcd
- MSStarter.bcd
- DistSvcConfig.bck
- CommunicationServicesArea.messages
- MailService.messages
- MailGateway.messages

If you are using an 8000 server, use services release version 10.4. If you are using an 8090 server, use services release version 10.5.

Allow 1,164 disk pages for the Mail Service program files.

Dependencies and limitations

The Mail Service cannot initialize a new database larger than 65,534 pages. You cannot reduce the size of an existing Mail Service database.

The Mail Service needs the Clearinghouse Service to provide address information for mail delivery. The Clearinghouse Service may be co-resident with a Mail Service.

Mail system availability improves if the Mail Service and the Internetwork Routing Service are not coresident. Also, avoid installing a Print Service, an External Communication Service, or any communication protocols on the same server as the Mail Service.

The Mail Service uses the File Service for backing up its database. Install the File Service and the Mail Service on different servers to

avoid time-consuming recovery of the Mail Service database in the event of server disk problems.

Mail Service Worksheet

Use the Mail Service Worksheet to record server-related information that helps you perform procedures. For your convenience, the Mail Service Worksheet is at the end of this chapter.

Make a copy of the Mail Service worksheet. Retain the original Worksheet for future use, and store the completed worksheet in your *Activities Guide*.

Using the worksheet

Before you install the software on a server and set up your Mail Service, complete the Mail Service worksheet. It is important that you fill out the worksheet accurately and update it whenever changes occur. The completed worksheet saves you time as you perform your procedural duties. It also serves as an information source for new System Administrators unfamiliar with your network configuration.

Filling out the worksheet

As you read the rest of this chapter, you are directed to make entries on the Mail Service Worksheet. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and the services installed on the server. Copy this information from the Services Installation Worksheet. If you need more information, see the Services System Software chapter in this book.

Use section ② for recording the disk page requirement for the Mail Service database. Use section ④ for recording information about the Postmaster mailbox.

If you have the External Mail Gateway option, use section ③ for RS232C port information. Use sections ⑤ and ⑥ to define inbound and outbound gateway characteristics.

Planning for setup

After you install the Mail Service, you initialize it. If you enabled the External Mail Gateway option, you also enter modem information as part of the Mail Service initialization. You then add the Postmaster and user mailboxes for the Mail Service, and the domain information for the External Mail Gateway.

See the Mail Service chapter of the *Services Installation and Setup Guide* for complete setup procedures.

Service name and description

When you name the Mail Service, use a name different from all other names in the domain. The fully qualified Mail Service name takes the form:

Mail Service name:domain:organization

The domain and organization must be the same as the domain and organization of the server. For example, if the server name is Tuscon:Home Office:Acme Company, then the Mail Service name might be First Class:Home Office:Acme Company. To avoid possible errors, enter only the local name when you name the Mail Service during initialization. This lets the domain and organization default to that of the server.

This naming convention gives the System Administrator for the server domain access to System Administrator commands for the Mail Service. These commands are available only when you are enabled.

You can use up to 40 characters for the Mail Service name. Do not use commas, parentheses, asterisks, or pound signs in a service name.

A Mail Service description is optional. It may be the location of the server, or any other information. The description can be up to 100 characters.

Related procedure: Initializing the Mail Service

Filling out the worksheet

① Record the service name and description for the Mail Service.

Record the type of other services installed on the server, whether they are activated, the number of disk pages they require, and the name and descriptions.

Mail Service database

The size of the Mail Service database depends on the number of user mailboxes and the amount of service use you expect. You can increase the size of an existing database, but you cannot reduce its size. Estimate that each mailbox will require 100 disk pages, but underestimate the number of mailboxes you will add.

Related procedure: Initializing the Mail Service

Filling out the worksheet

② Record the number of users and multiply it by 100 to determine the total disk pages for the Mail Service database.

External Mail Gateway option

If you are using the External Mail Gateway option, you initialize the RS232C port by entering the phone line speed and the phone number for the local gateway. The type of modem determines the line speed. The phone number is part of the inbound/outbound gateway information determined in the "Assigning External Mail Gateway domains" section, next.

This phone number should be the same number listed for the inbound gateway in section ⑤ of the worksheet. Include the area code if the foreign domain is outside your local area. Do not use hyphens or parentheses to separate the numbers.

Related procedure: Initializing the Mail Service

Filling out the worksheet

③ Indicate the line speed of the modem attached to the RS232C port.

Record the phone number that foreign gateways dial to forward mail to an incoming gateway.

Assign External Mail Gateway domains

Each External Mail Gateway serves as a connection point for both incoming and outgoing mail. In these two roles, it is called an inbound gateway and an outbound gateway, respectively.

Mail is routed between internetworks on the basis of the recipient's domain. A specified Mail Gateway thus serves as the outbound gateway for sending mail to foreign (on other Xerox networks) domains, and as the inbound gateway for receiving mail for local domains. Only one gateway can serve as the outbound gateway for each foreign domain.

The System Administrators for all networks collaborate to assign domains for the External Mail Gateway Mail Services.

Assign inbound Mail Gateways - For all Mail Gateways, the System Administrators in an internetwork decide which gateway (and associated domains) receives incoming mail from users in foreign domains. The inbound gateway should be on the Mail Service geographically closest to the user mailboxes in the domain.

Generate an inbound list - For each inbound gateways in the internetwork, the System Administrators list the phone number, gographic location and local domain(s). Only domains on this list can be registered as foreign domains for outbound gateways.

Exchange inbound lists - The System Administrators whose networks are sending and receiving mail exchange the list of inbound gateways.

Assign outbound Gateways - Each System Administrator uses the list to decide (for each inbound gateway receiving mail from users in foreign domains), which of his or her gateways serves as the outbound gateway. A System Administrator should select as an outbound gateway the inbound gateway geographically closest to the foreign domains.

Add foreign gateways and domains - Each System Administrator establishes the outbound gateway for the specified foreign domains. The System Administrator must add each foreign domain to receive mail to an outbound gateway, but a different foreign domain in the same internetwork can be connected to a different outbound gateway.

Related procedure: Enabling outbound mail transmission

Filling out the worksheet

The worksheet accommodates information for one gateway and associated domains. If you have more than one gateway, make an additional copy of the worksheet for each gateway.

⑤ **Phone number** - Record the phone number of the inbound gateway. This is the phone number used by foreign gateways to forward mail to a local inbound gateway. Include the area code if the foreign gateways are outside your area. Do not use hyphens or parentheses to separate the numbers.

Location - Record the geographic location of the inbound gateway. If you are supporting more than one gateway within the same city, include the department location.

Domain name - Record the local domain(s). These are the domains receiving mail from users in foreign domains. Include the organization name for each domain. Domains excluded from the inbound list will not be registered with any outbound gateway, and will not be able to send or receive mail from other Xerox networks.

⑥ For each inbound gateway that also serves as an outbound gateway for sending mail to recipients in foreign domains, fill in outbound gateway information. You should select the inbound gateway geographically closest to the users in the foreign domains.

Phone number – Record the phone number of the outbound gateway for the foreign gateway. This is the same phone number for the inbound gateway listed in section ⑤, that serves as the outbound gateway for sending mail to recipients in foreign domains.

Start time - Record the start time of the calling interval. The calling interval specifies a period of time during which the local gateway dials up the foreign gateway. Calling intervals control only outbound mail transfer. Inbound mail arrives by means of the phone connections that the outbound gateway in the foreign internetwork establishes. Enter the number in the HH:MM format. For example, if the start time is 4:30 pm, you enter 16:30. Set the start time at an hour when the phone rates are less expensive.

Length - Record the length of the calling interval. The calling interval length specifies the number of hours or minutes the local gateway can dial up the foreign gateway beginning at the start time. Enter the number in the HH:MM format using the 24-hour

clock. For example, if you want the local gateway to send mail over 10 hours and 45 minutes, enter 10:45. Within the length of the calling interval, autodial connections are made every 15 minutes if mail is waiting for delivery.

Name - Record the name of the foreign domain(s). This is the name of the foreign domain(s) receiving mail from users in local domains. Include the organization name for each domain.

Phone number - Record the phone number of the outbound gateway. This is the same phone number for the inbound gateway listed in section ⑤, that serves as the outbound gateway for sending mail to recipients in foreign domains.

Setting up Postmaster and user mailboxes

The Postmaster mailbox receives notification whenever the Mail Service cannot deliver a message. Before you add the Postmaster mailbox at the Mail Service server, you must register the entry with the Clearinghouse Service.

You determine a unique name for the Postmaster mailbox for each Mail Service. Enter the name in the following format and fill in the service name where it is shown in italics:

Postmaster of *Mail Service name*:*Mail Service* domain:*Mail Service* organization.

You can use up to 40 characters for the local name. If Postmaster of *Mail Service name* is longer than 40 characters, only the first 40 characters are used.

You also create a mailbox for each Mail Service user. The users must already be registered in the Clearinghouse Service database. Establish the user mailbox at the mail server closest to the user workshtation.

Use the Clearinghouse Service User Directory Worksheet to enter the user name or alias for each mailbox.

Related procedures: Creating mailboxes, Creating a Postmaster mailbox

Filling out the worksheet

④ Record the fully qualified name of the Postmaster mailbox for the Mail Service.

Indicate whether the fully-qualified name of the Postmaster mailbox is registered with the Clearinghouse Service. If it is not, see the Clearinghouse Service chapter in this book for information on registering users.

Planning for maintenance

After you install and set up the Mail Service, you are responsible for maintaining it. You perform maintenance as needed; there are no scheduled duties.

Use the information in "Planning for setup" in conjunction with the information here to further your understanding of Mail Service maintenance. See the Mail Service chapter in the *Services Maintenance Guide* for the complete maintenance procedures.

Monitoring the Mail Service database

Carefully monitor each Mail Service database to ensure that it is less than 95 percent full, and that it never exceeds 65,535 disk pages. If the database is full, the Mail Service cannot receive mail and you cannot repair the database (see *Basic Network Troubleshooting*). If the database remains full for two working days, messages destined for the Mail Service are returned to the sender.

The **Show Usage** command allows you to see the number of operations the Mail Service has been requested to perform. The *totals* column tells you how many operations have been requested, and the *rejected* column tells you how many operations could not be performed because the Mail Service was too busy.

The **Show Status** command shows the size of the queues for posting mail. A large number of messages on the input queue means that messages are being posted at the server faster than they can be processed and delivered. This can occur with a coresident Clearinghouse Service. It may also indicate that the server is overloaded and the Mail Service should be moved to another location.

One full Mail Service database can slow mail delivery throughout the internetwork. Mail destined for another Mail Service often waits behind mail destined for the Mail Service with the full database, because other Mail Services continue to deliver mail to that Mail Service.

As a Mail Service database becomes full, you can expand the size of the database. If you need a database larger than 65,535 disk pages, install a new Mail Service on a different server, and then move some of the mailboxes to the new Mail Service.

Related procedures: Monitoring Mail Service activity, Expanding the Mail Service database

Monitor undelivered mail

When a user sends a mail message to a distribution list including one or more invalid users, the Mail Service deposits a "Bad Group Member" notification in the Postmaster mailbox. The Mail Service returns the message to the sender only if a recipient was removed from the network after the message was sent, or if the message crossed a mail gateway on its way to the invalid recipient.

Regularly access the Postmaster mailbox by logging on as the Postmaster and retrieving mail in the usual way. By reviewing the notifications in the Postmaster mailbox, you can be aware of problems preventing mail delivery.

Related procedure: Monitoring user activity

Maintaining user mailboxes

You may need to create new mailboxes or delete existing mailboxes. You may also need to move mailboxes from one Mail Service to another.

Generally, a mailbox and its contents are transferred quickly to a new location. Occasionally, however, it may take up to two days to transfer the contents or to inform all Clearinghouse Services of the change in the mailbox location. Do not delete the mailbox from the old location. This mailbox is deleted automatically when the contents have been moved.

During the moving process, some mail messages may appear to be lost. Some messages may be directed to the old mailbox and some to the new one, depending on which Clearinghouse Service the Mail Service contacts for the mailbox address. Eventually, all messages will be forwarded to the new mailbox.

Related procedures: Moving mailboxes, Removing a mailbox

Displaying mailbox storage space

You can display the number of messages and the amount of storage space used in each mailbox. Keep in mind that the number of messages in a mailbox does not indicate how much space the mailbox occupies in the database. For example, 99 two-page messages take up much less space than a single 1000-page message.

The sum of all mailbox sizes may be larger than the database size. This situation indicates multiple recipients are sharing one copy of a message, but their mailboxes all claim storage. All recipients of a shared message must delete it to remove it from the database.

Related procedure: Monitoring user activity

Change the Mail Service location

Occasionally, you may need to move a Mail Service from one server to another because of a hardware deficiency, or coresidency problems. To move a Mail Service, install a Mail Service with a new name, move the mailboxes to it, and then expunge the original Mail Service.

After installing the new Mail Service, wait two days before moving the mailboxes. This delay allows the new Mail Service entry to propagate to all Clearinghouse Services serving the new Mail Service domain. If you add mailboxes before propagation occurs, mail sent to those mailboxex may be returned with the message "No Such Recipient."

Do not expunge the old Mail Service until you have added all mailboxes. Otherwise, you will lose mailboxes and their

contents. List the mailboxes at the Mail Service you are expunging to make sure they have all been forwarded.

Related procedure: Moving the Mail Service

Deleting a Mail Service from a server

To prepare for expunging a Mail Service, move all mailboxes you want to remain active to another Mail Service. Do not move the Postmaster mailbox. The Mail Service to which you are moving the mailboxes already has its own Postmaster. Delete the Postmaster entry from the Clearinghouse Service.

You must ensure that all messages are forwarded to another Mail Service before you expunge the Mail Service. Note the number of messages in each mailbox before you begin to add the mailboxes to another Mail Service. It is also a good idea to tell users to retrieve their mail. Ensure that all mailboxes have been forwarded on the Mail Service you are expunging. If no mailboxes are listed, all the mailboxes have been forwarded, and you can shut down the Mail Service. You must shut down the Mail Service before you remove it.

When you shut down the Mail Service, any mail in transit is forwarded to a Mail Service you specify. A dot is displayed for each forwarded message so you can track the progress of the operation. If the specified Mail Service becomes unavailable or fills up during the transfer, you name another Mail Service to which messages can be forwarded.

If the Mail Service has the External Mail Gateway option, it returns to the sender any undelivered mail destined for foreign domains. In addition, move to another Mail Gateway the foreign mail gateways and domains that still need to be served before you delete this Mail Service.

Related procedures: Removing the Mail Service, Moving a Mail Service

Results of expunging a Mail Service

You can expunge the mail Service after it shuts down. You must confirm that you want to expunge any Mail Service still containing mailboxes. Occasionally, the Mail Service does not remove itself from the Clearinghouse Service during the expunge. You can list the Mail Services at each Clearinghouse Service serving the expunged Mail Service domain to check for this error.

If the expunged Mail Service name still appears at a Clearinghouse Service, delete that Mail Service name. The deletion propagates to other Clearinghouse Services serving the same domain.

If you expunge the Mail Service from a server with a coresident Clearinghouse, reboot the server before running the Clearinghouse Service. See the Services System Software chapter in this book for more information.

Stopping the Mail Service

Stopping the Mail Service is necessary to reboot the server, expunge a mail gateway, or run diagnostic tests on the RS232C port. If a Mail Service is part of a distributed Mail and

Clearinghouse system, stop the Mail Service only when absolutely necessary.

See the *Basic Network Troubleshooting* book for information on stopping the Mail Service.

Related procedures: Expanding the Mail Service database, Moving the Mail Service, Removing the Mail Service

Cancel non-normal startup

Some procedures are accessible only through the Mail Service non-normal startup, such as expanding the Mail Service database. To reverse your decision to apply a non-normal startup, reboot the server.

Related procedures: Expanding the Mail Service database, Moving the Mail Service, Removing the Mail Service

Monitoring External Mail Gateway activity

You can list the local mail gateways and/or domains accessible from a Mail Service with the External Mail Gateway option. Only foreign gateway and domain information for the local mail gateway is displayed. The information displayed does not include the foreign gateways or domains accessible or served by other Mail Gateway options on other Mail Services in the internetwork.

You can list calling intervals and mail transfer statistics for a specified foreign gateway, and show the state of the gateway's queue for outgoing mail. You can also show RS232C port information to isolate problems found with gateway mail transfer.

Related procedure: *Monitoring foreign gateway and domain activity*

Changing External Mail Gateway information

You can update the calling intervals and change foreign gateway phone numbers. Typically, a foreign gateway will have a single calling interval assigned, although multiple intervals may be assigned.

CAUTION: If a Mail Service calling interval starts at midnight, do not add another calling interval that starts before midnight and ends after midnight. Otherwise, the server housing the Mail Service locks up.

Deleting a mail gateway

You delete a mail gateway by disabling the External Mail Gateway option, expunging the mail gateway, and rebooting the server. The mail gateway message file remains in the working directory. Do not delete this file; the Mail Service cannot load and run without it.

Occasionally, the mail gateway is not completely removed. In this case, mail destined for a foreign domain formerly served by the expunged gateway may be returned. You may also be unable to configure a different mail gateway to serve a foreign domain formerly served by the expunged gateway. To recover, enable

the External Mail gateway option again, reconfigure it with the same set of foreign domains, and expunge it.

Related procedures: Deleting a foreign gateway, Deleting the Mail Gateway option

Modifying foreign gateways and domains

You can change or move established gateway configurations. If the existing External Mail Gateway is local (on a single Mail Service), you can change phone numbers and calling intervals.

If the existing External Mail Gateway is global (spanning multiple Mail Services), reassign inbound/outbound gateway roles among the various Mail Services (for example, when a new External Mail Gateway is added to an existing internetwork). You also can move a gateway by adding the gateway and its associated domains at the new mail gateway, then deleting them from the old mail gateway.

Obtain the list of inbound gateways from the System Administrator of the foreign internetwork you are reconfiguring.

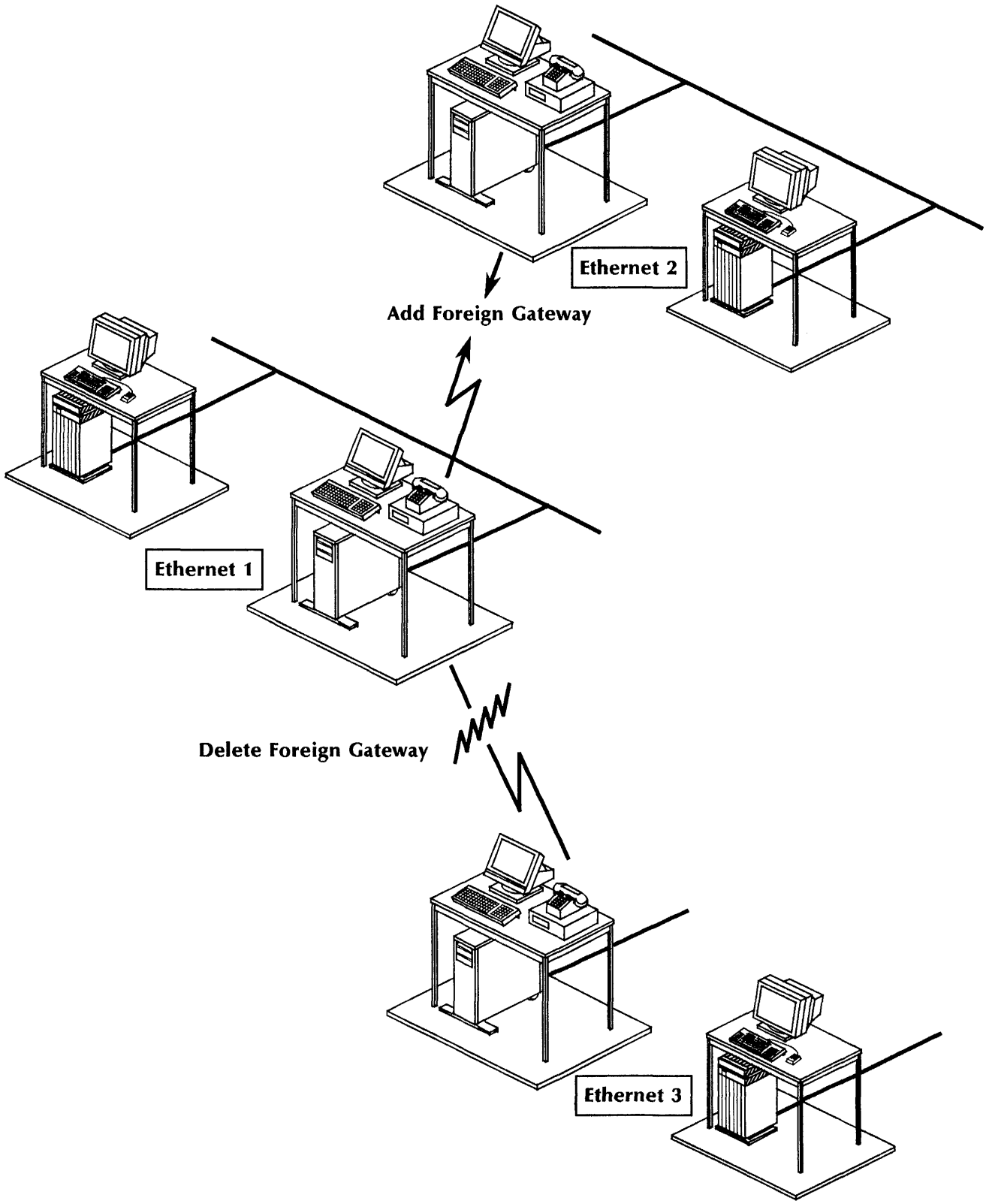
CAUTION: Do not delete a foreign domain or a foreign gateway as long as mail is in the gateway queue. Otherwise, a server problem may result.

If you delete a foreign domain shortly after you add it, you may see the message "Unexpected problem with Clearinghouse." The information about the new foreign domain has not propagated to all Clearinghouse Services. Try to delete the foreign domain later.

Related procedures: Changing a foreign gateway phone number, Changing a local gateway's line speed or phone number, Moving a foreing domain, Moving a foreing gateway, Updating foreign gateway calling intervals

Figure 5-3 illustrates a mail gateway reconfiguration where a gateway is added and another gateway is deleted.

Figure 5-3. **Adding an External Mail Gateway at a new location and deleting the gateway from the old location**



6. Print Service

This chapter helps you prepare for installation, setup, and maintenance of the Print Service. This information supports the procedures you perform from an 8000 or an 8090 server using these software versions:

- 11.0 - This chapter supports the procedures you perform for an 8040 Series Electronic Printer or a Laser CP Electronic Printer. You can run 11.0 software on an 8000 or an 8090 server.
- 10.0 through 10.3 - This chapter supports the procedures you perform for a Telecopier 495-1 Printer or a Formatting Print Service. You can run 10.0, 10.2, or 10.3 software on an 8000 server only.

Unless otherwise labeled, the information in this chapter applies to all software versions. Be sure you use the appropriate information for your software version.

Service description

The Print Service provides printing capabilities to all Xerox Network Systems workstations. It enables network users to obtain paper versions of what they create on their workstations. The Print Service supports electronic printing, facsimile transmission, and document conversion and forwarding.

Printing options

The Print Service supports three attached printing options and the Formatting Print Service. No local hardware is associated with the Formatting Print Service, because output is forwarded to a different networked Print Service.

8040 Series Electronic Printer

The 8040 Series Electronic Printer produces quick-turnaround, high-quality 300 DPI (dots per inch) output. It can print a variety of font styles as well as graphic illustrations. The 8040 Series Electronic Printer comes in two versions: Build 1 (B1) and Build 2 (B2).

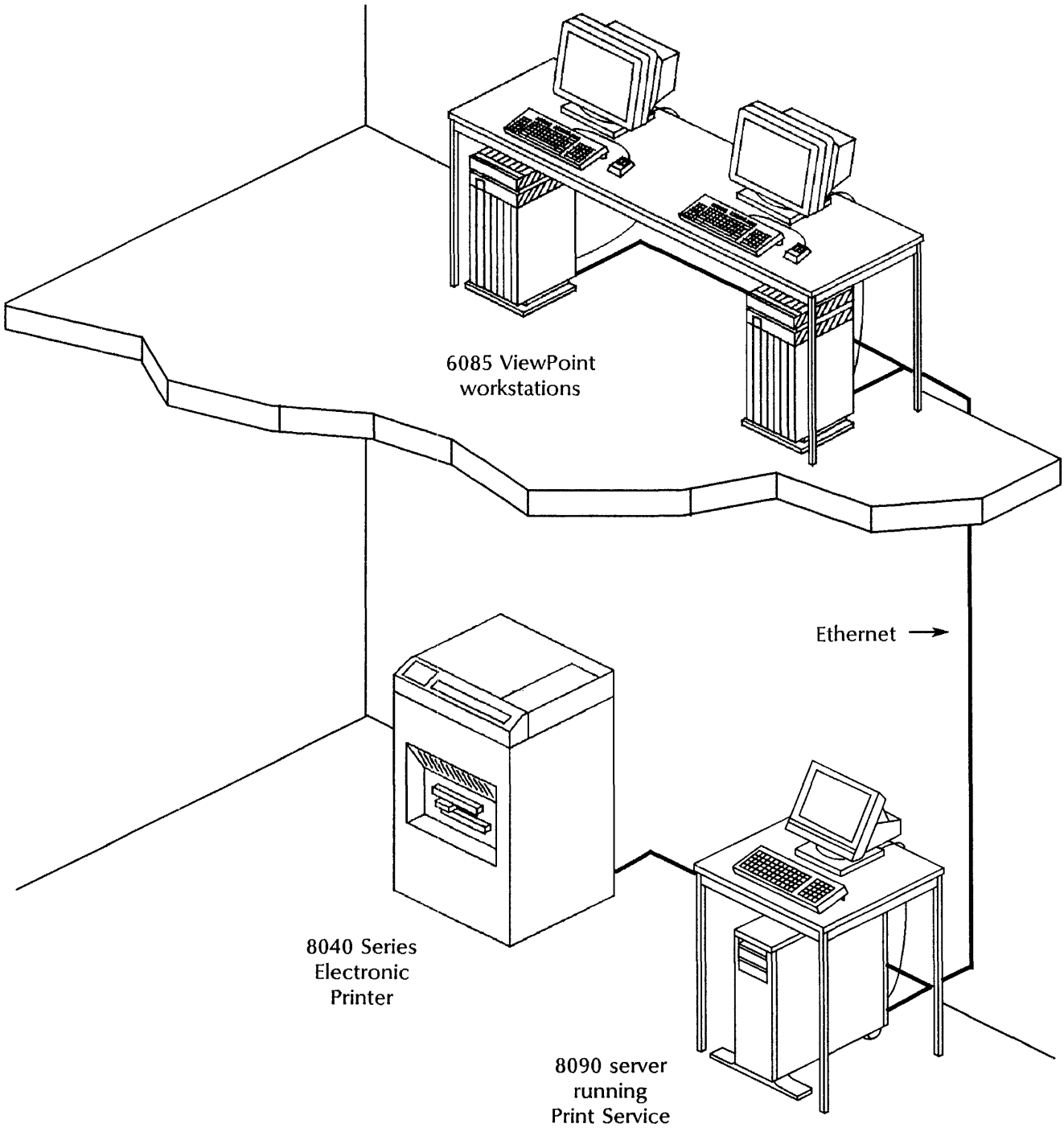
B1 printer The B1 printer has an output tray that holds up to 250 sheets. It delivers printed sheets face up and prints a document from the last page to the first page.

B2 printer The B2 printer has a drum-shaped output stacker and a tray that holds up to 500 sheets. It delivers printed sheets face down and prints a document from the first page to the last page. The B2 printer provides an offset stacking capability. It can also enter low-power mode during low-use periods.

An audible alarm kit is available for B2 printers. The alarm buzzes when the printer needs attention. The volume control for the buzzer is located behind the front printer panel near the top, and is marked with a bell symbol. The B2 printer may require logic upgrades before Xerox service personnel can install the alarm kit.

Figure 6-1 shows an 8040 Series Electronic Printer on an Ethernet network.

Figure 6-1. **8040 Series Electronic Printer, 8090 server, and workstations on an Ethernet network**

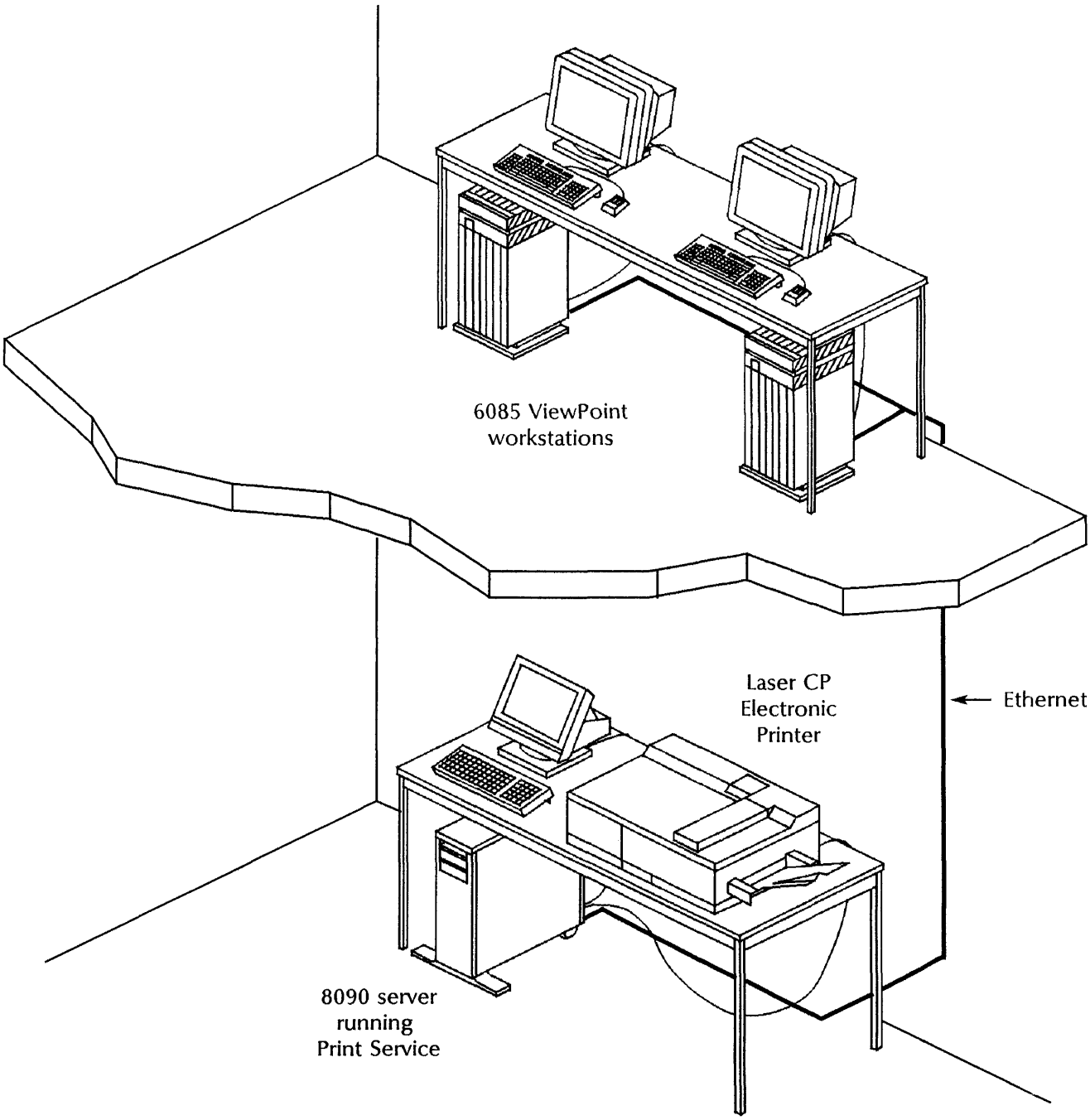


Laser CP Electronic Printer

The Laser CP Electronic Printer is a desktop printer that produces quick-turnaround, high-quality 300 DPI (dots per inch) output. It can print a variety of font styles as well as graphic illustrations. Optionally, the printer can perform photocopying.

Figure 6-2 shows a Laser CP Electronic Printer on an Ethernet network.

Figure 6-2. **Laser CP Electronic Printer, 8090 server, and workstations on an Ethernet network**

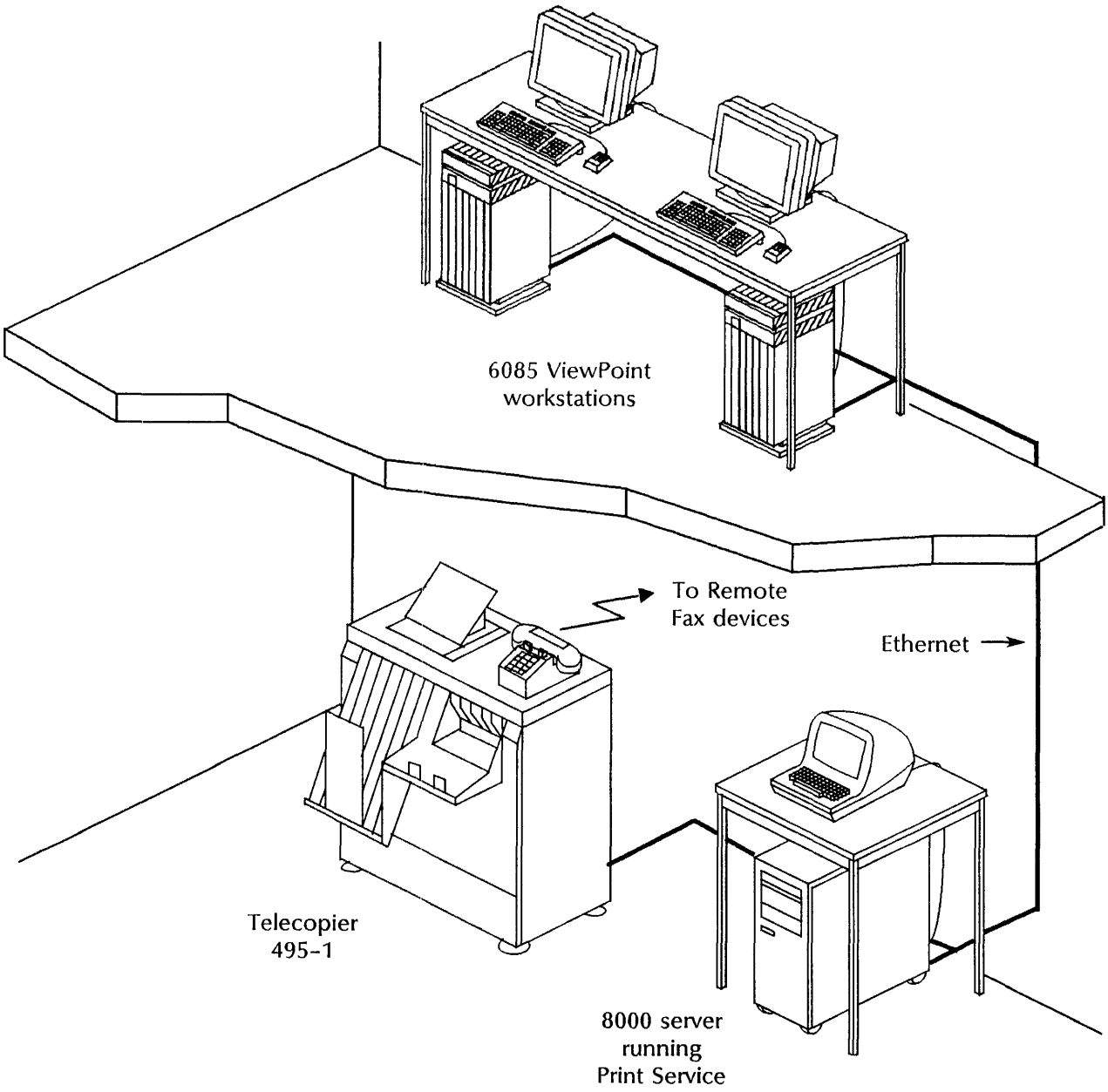


Telecopier 495-1 Printer (versions 10.0 through 10.3 only)

The Telecopier 495-1 Printer is a facsimile (FAX) device used for transmitting documents automatically to any group 1, 2, or 3 compatible remote facsimile devices. The documents can contain a variety of font styles and graphic illustrations. The Telecopier 495-1 can transmit to as many as 10 remote facsimile devices over telephone lines, as well as provide local printing. It uses the local RS232C communications port.

Figure 6-3 shows a Telecopier 495-1 Printer on an Ethernet network.

Figure 6-3. **Telecopier 495-1 Facsimile Device, 8000 server, and workstations on an Ethernet network**

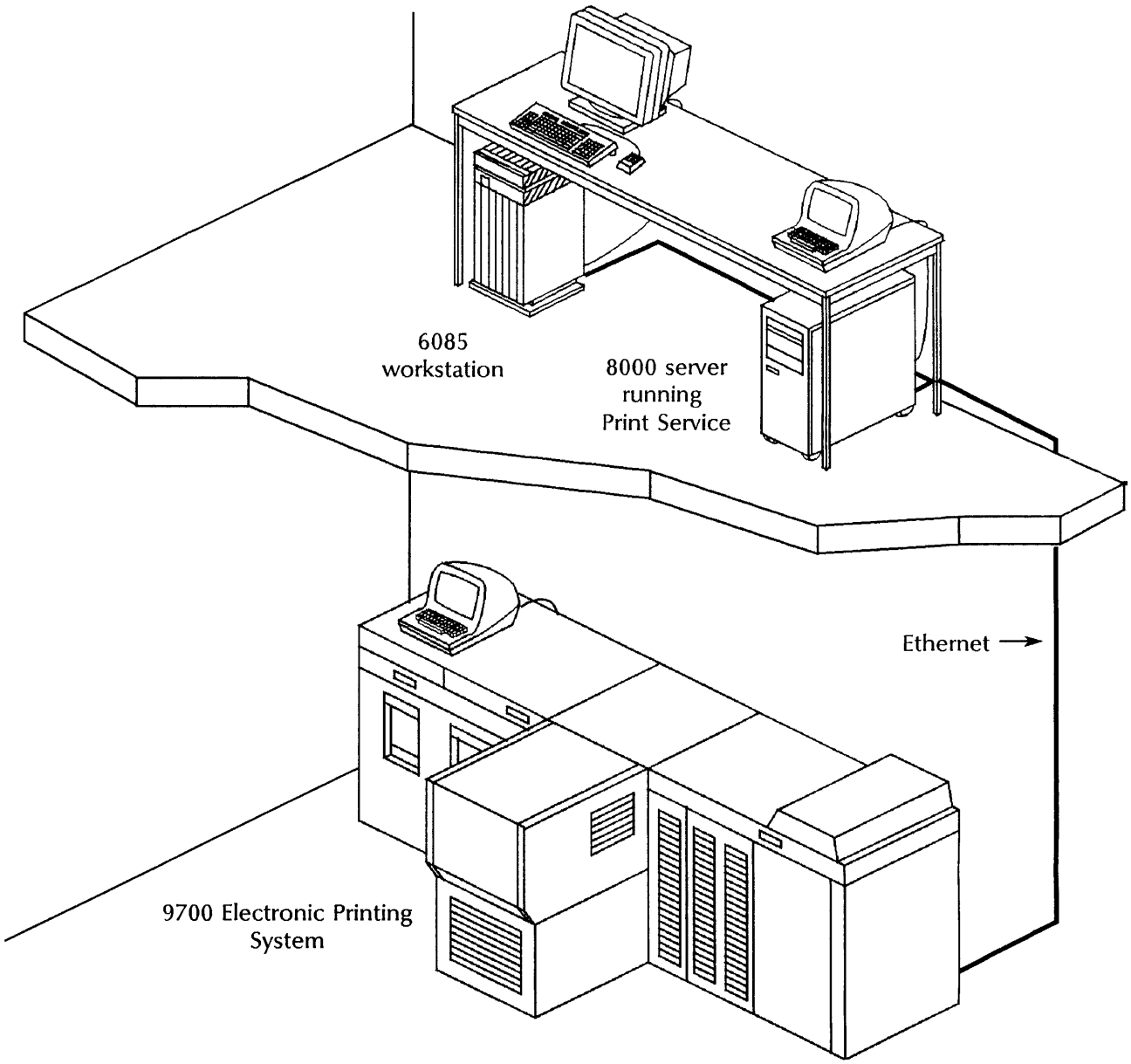


Formatting Print Service (versions 10.0 through 10.3 only)

The Formatting Print Service is a network service that converts 6085 or 8010 ViewPoint documents and forwards them for printing. The printer specified to receive and print the documents is called the Target Print Service. The Formatting Print Service is designed to support a 4050, 8700, or 9700 Electronic Printing System as the Target Print Service. However, it can support any networked printer that accepts the Interpress page description language. The documents can contain complex graphics, including illustrations with non-vertical, non-horizontal, and curved lines, shapes, and shadings.

Figure 6-4 shows a Target Print Service (9700 Electronic Printing System) on an Ethernet network.

Figure 6-4. **9700 Electronic Printing System, 8000 server, and workstation on an Ethernet network**



How the software works

When you send a document to a printer, the workstation converts the document into an Interpress master. An Interpress master is a file written to the Xerox Interpress standard. It describes the desired appearance of a page that has been composed by some other process. The workstation then transmits the Interpress master to the Print Service along with properties and options specifying the document name, user name, and creation date. The Print Service interprets the master and directs the printer during the printing process. This process involves queuing, and either formatting and printing at an attached printing device, or formatting and forwarding to the Target Print Service.

Queuing

Queuing is the process of accepting and storing documents by the Print Service. The print queue tracks the status of documents throughout processing for as many as 39 documents. Documents are queued in the order received.

Formatting and printing

During formatting, the Print Service with an attached printing device uses the Interpress master to create an internal description of the document. The formatter proceeds through the master, page by page, building the internal description of the image (text and graphics). When a requested font is not loaded on the Print Service, the formatter substitutes the specified default font (Modern or Classic).

The Print Service then converts the internal description into the actual page image in real-time, as the printer transfers the image to the paper. After the document is printed, the Print Service deletes the Interpress master.

Formatting and forwarding (versions 10.0 through 10.3 only)

The Formatting Print Service converts Interpress masters (containing text and graphics) into interleaved Interpress masters. Graphics in the original Interpress master are converted into compressed graphic images, one for each page containing graphics. The Formatting Print Service then forwards the interleaved Interpress masters to the Target Print Service.

When a document forwarded by the Formatting Print Service is printed, all text within the text frames (including overlaid text frames) is printed, regardless of the document's appearance at the workstation. For overlaid text frames, the Formatting Print Service loses the information that specifies which text frame is on top. To avoid this problem, remove all underlying text frames before sending a document to the Formatting Print Service.

Do not send Interpress masters created by an 860 or an 820-II workstation to the Formatting Print Service. The Formatting Print Service does not support Interpress masters generated by 860 workstations with sequence insert file references and aborts such printing requests.

Complex and slow page printing features (version 11.0 only)

The Print Service has two features that support printing of complex documents: complex printing and slow page printing. When you enable complex printing, slow page printing is required and enabled automatically; however, you may enable slow page printing separately. If either feature cannot be enabled, you see a message stating the reason.

Complex printing increases the amount of working space allocated by the formatter and allows better use of the real memory resources available. This additional disk space is reserved whether or not a complex page is printing. Slow page printing allows more time to process a page with complex graphics and corrects image gaps before printing a page.

Image gaps occur when image generation is slower than the printer during the printing of extremely complex images or graphics. Image gaps are blank strips running vertically on pages from the 8040 Series Electronic Printer and horizontally across pages from the Laser CP Electronic Printer.

"Planning for setup" contains additional information on these Print Service features.

Relationship with other services

The Clearinghouse Service automatically registers the Print Service during initialization.

The Internetwork Routing Service enables communication between workstations and Print Services located on different networks on the internet.

The Interactive Terminal Service supports printing of Xerox Memorywriter, plain text, and Interpress documents.

Versions 10.0 through 10.3 only:

The Clearinghouse Service lets you manually register these printers:

- 4050, 8700, and 9700 Electronic Printing Systems connected to the network and designated as a Target Print Service for the Formatting Print Service.
- Any networked printer that accepts the Interpress page description language and is designated as a Target Print Service for the Formatting Print Service.

See the "Enabling manual registration" procedure in the Clearinghouse Service chapter of the *Services Maintenance Guide* for more information. Also, see the documentation accompanying your printer.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the Print Service Worksheet and the Print Service Activity Log located at the end of this chapter.
- Installing the Print Service software as described in the Server Software Installation chapter in the *Services Installation and Setup Guide*.
- Setting up the Print Service as described in the Print Service chapter of the *Services Installation and Setup Guide*.
- Ensuring that the printer contains paper, has the proper level of dry imager, and is free from paper jams. For more information, see the quick-reference cards, machine labels, or instruction manual accompanying your printer.
- Maintaining the Print Service as described in the Print Service chapter of the *Services Maintenance Guide*.
- Notifying users of any change or disruption in the service, as when:
  - New fonts are installed or old fonts are deleted
  - Service is interrupted for a long time
  - Heavy workloads require excessive use of a printer
- Upgrading the software and hardware as required.
- Troubleshooting the service as described in *Basic Network Troubleshooting*.

You can perform most Print Service procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter in the *Services Installation and Setup Guide* contains the procedures for installing your Print Service software. This section explains software, hardware, and other requirements to help you prepare for installation.

Hardware requirements

The Print Service operates on an 8000 or an 8090 server. When the Print Service is configured to support an attached printing device, the necessary printer hardware must be connected to the server. You can connect only one printer at a time to a server.

The cable from the 8040 Series Electronic Printer or the Laser CP Electronic Printer attaches to the receptacle labeled "LSEP" on the back of the server.

The cable from the Telecopier 495-1 Printer attaches to the RS232C port on the back of the server.

Printer specifications

Table 6-1 shows printer specifications for the attached printing options.

Table 6-1. **Printer specifications**

Feature	8040 Series	Laser CP	Telecopier 495-1 (10.0 - 10.3 only)
Printer type	Plain paper xerographic laser printer	Plain paper xerographic laser printer	Thermal transfer device for local printing or remote transmission
Volume per month	15,000 pages	5,000 pages	500 pages (local printing)
Maximum speed	12 pg/min	10 pg/min	Grp 1: 1 pg/6 min Grp 2: 1 pg/2 min Grp 3: 1 pg/< min
Resolution	300 dots per inch	300 dots per inch	200 dots per inch (local printing)
Paper trays	Two	One	None
Paper type	Single sheets 8.5" x 11" 8.5" x 14" A4 (metric letter)	Single sheets 8.5" x 11" 8.5" x 14" A4 (metric letter)	Treated paper roll 8.5" or 210 mm wide
Paper capacity	500 input 500 output	250 input 100 output	100 meter roll input
Location	Floor	Desktop	Floor

Safety instructions for printers

"Warning -- This equipment generates, uses, and can radiate radio frequency energy and if not installed and used in accordance with the instruction manual, may cause interference to radio communications. It has been tested and found to comply with the limits for a Class A computing device pursuant to Subpart J of Part 15 of FCC rules, which are designed to provide reasonable protection against such interference. Operation of this equipment in a residential area is likely to cause interference, in which case the user at his own expense will be required to correct the interference."

Xerox has designed and tested your printer and supplies to meet strict safety requirements. These requirements include safety agency examination and approval, and compliance with established environmental standards. Pay attention to the following warnings to ensure the continued safe operation of your equipment.

WARNING: Improper connection of the printer grounding conductor can result in risk of electrical shock.

- ALWAYS connect the printer to a properly grounded power source receptacle. If in doubt, have the receptacle checked by a qualified electrician.
- ALWAYS use materials and supplies specifically designated for your printer. Use of non-approved materials may result in poor performance and can create a hazardous situation.
- ALWAYS place the printer on a solid support surface, with adequate strength for the weight of the machine.
- ALWAYS exercise care when moving or relocating the printer. See the instructions accompanying your equipment.
- NEVER use a ground adapter plug to connect the printer to a power source receptacle that lacks a ground connection terminal.
- NEVER attempt any maintenance function that is not specifically described in the material provided.
- NEVER remove any covers or guards that are fastened with screws. No operator-serviceable areas exist behind these covers.
- NEVER override or "cheat" electrical or mechanical interlock devices.
- NEVER use supplies or cleaning materials for other than their intended purpose. Keep all such materials out of the reach of children.
- NEVER operate the printer if it is producing unusual noises or odors. Disconnect the power cord from the power source receptacle and call your local Xerox office to correct the problem.

Software requirements

The Print Service requires software files, message files, print queue data, profile entries, fonts, test patterns, and reserved virtual memory.

Fonts

The Print Service needs a minimum set of font files to operate and print test patterns. You purchased these files with the Print Service software. They are contained on the "Xerox Network Printer Fonts ..." cartridge tape and the "Xerox Required Fonts ..." floppy disk:

- Xerox.Graphics.Newvec
- Xerox.XC1-1-1.Modern
- Xerox.XC1-1-1.Terminal
- Xerox.XC1-1-1.Terminal.Bold
- Xerox.Diagnostic.Bits
- Xerox.Diagostic.XeroxBook

It is recommended that you install the larger set of Modern or Math Classic fonts so the Print Service has a default substitution font. That way, the Print Service can substitute the Modern or Classic font if a requested font is not installed. If you plan to install the larger set of Modern or Terminal fonts, you do not need to install the Modern or Terminal fonts listed above.

Table 6-2 shows the compatible Xerox fonts for each printing option. If the Print Service is a new installation, follow the sequence in Table 6-2 when you load fonts. The Print Service will not let you load fonts that are not compatible with your printing option.

Table 6-2. **Compatible Xerox fonts**

Font Family	8040 Series	Laser CP	Telecopier 495-1[1]	FPS[1]
Xerox Required Fonts (300 DPI)	X	X		X[3]
Xerox Basic Classic Fonts (300 DPI)	X[2]	X[2]		
Xerox Printwheel Fonts (300DPI)	X	X		
Xerox Math Classic Fonts (300 DPI)	X	X		
Xerox Modern Fonts (300 DPI)	X	X		
Xerox Required Fonts (200 DPI)			X	
Xerox Basic Classic Fonts (200 DPI)			X[2]	
Xerox Printwheel Fonts (200DPI)			X	
Xerox Math Classic Fonts (200 DPI)			X	
Xerox Modern Fonts (200 DPI)			X	

[1]Versions 10.0 through 10.3 only

[2]The Print Service does not need the Basic Classic Fonts if you install the Math Classic Fonts; Math Classic files overwrite Basic Classic files.

[3]Only two font files are required: Xerox.Graphics.Newvec and Xerox.XC1-1-1.Modern.

Extended language fonts:

Extended language fonts are available only in Modern and Classic fonts for Japanese and Chinese. To load both Modern and Classic extended language fonts, the server must have at least 80 Mb of available disk space. The server must have at least 42 Mb if you are loading only one of these fonts.

If you load regular fonts and extended language fonts on the same Print Service, delete the duplicate regular fonts (Xerox.XC1-1-1.Modern and Xerox.XC1-1-1.Classic).

Test patterns

Test patterns are Interpress masters required for testing the Print Service. You use test patterns to check or adjust printer alignment. Xerox service personnel use them as aids in troubleshooting the service and judging the print quality. You load test patterns after you install and initialize the software. The Print Service will not let you load test patterns that are not compatible with your printing option.

Table 6-3 shows the required test patterns for each printing option and how they are used.

Table 6-3. **Printing options and required test patterns**

Test Pattern/Purpose	8040 Series	Laser CP	Telecopier 495-1[1]	FPS[1]
AlignmentPattern.interpress - used to check the alignment of images on paper	X			
LaserCPAlignmentPattern.interpress - used to check the alignment of images on paper		X		
CAM.interpress - used to check Print Service operation	X	X	X	X
LightDusting.interpress -used by Xerox service personnel to check copy quality	X	X		
GreyDusting.interpress - used to diagnose a printer, cable, or server problem by running the image test; used by Xerox service personnel to check copy quality	X	X		
DarkDusting.interpress - used by Xerox service personnel to check copy quality	X			

[1]Versions 10.0 through 10.3 only

Disk space requirements

Table 6-4 shows the approximate disk pages required for the Print Service program files. Table 6-5 shows the approximate disk pages required for fonts and test patterns. Combine the totals from both tables for the total disk pages the Print Service requires to function optimally. These disk page requirements may vary slightly.

Table 6-4. **Disk pages required for Print Service program files**

File Type	Disk Pages
Software files	700
Message files	55
Miscellaneous internal files	105
Virtual memory working space reserved by the formatter when the Print Service is run	6,000[1]
Space for queued documents	3,000[2]
TOTAL DISK SPACE FOR STANDARD PRINT SERVICE	9,860
Page buffer reserved for slow page printing when the Print Service is run	2,700[3]
TOTAL DISK SPACE FOR PRINT SERVICE WITH SLOW PAGE PRINTING ENABLED	12,560[3]
Additional virtual memory working space needed for complex printing (reserved by formatter when the Print Service is run)	6,000[1,3]
TOTAL DISK SPACE FOR PRINT SERVICE WITH COMPLEX PRINTING ENABLED	18,560[3]

[1]The formatter requires 6,000 pages to handle the widest variety of typical documents; 12,000 pages in complex printing mode to handle the widest variety of all documents (version 11.0 only). The Print Service will run with fewer available pages; however the more restricted the working space is, the more documents will be unprintable. The Print Service will not run with fewer than 800 available pages on the volume.

This requirement does not apply to 8000 servers with 10 Mb disk drives. These servers allocate the formatter working space from the System volume rather than the default Services volume. Complex printing cannot be enabled on a 10 Mb server.

[2]A minimum of 3,000 available disk pages is recommended for storing queued documents. The actual number of pages used will vary, depending on whether the documents are very large or very small. If you save only a small amount of available space for queued documents, then users will be able to queue only a limited number of documents at one time.

[3]Version 11.0 only

Table 6-5. **Disk pages required for printer fonts and test patterns (1 of 2)**

Font Family	Font/Test Pattern Name	Font Sizes									Font Styles				Disk Pages	
		6	8	10	12	14	18	24	30	36	R	B	I	BI	300 DPI	200 DPI[1]
Xerox Required Fonts (includes test patterns)	CAM.interpress														5	5
	AlignmentPattern.interpress														86	
	LightDusting.interpress														1	
	DarkDusting.interpress														1	
	GreyDusting.interpress														1	
	Xerox.Graphics.Newvec														133	133
	Xerox.Diagnostic.Bits														9	
	Xerox.Diagnostic.XeroxBook														25	
	Modern				X						X				90	63
	Terminal		X		X						X	X			344	240
	Total														695	441
Xerox Modern Fonts	Modern	X	X	X	X	X	X	X	X	X	X				1,988	1,129
		X	X	X	X	X	X	X	X	X		X			1,605	946
		X	X	X	X	X	X	X	X	X			X		1,561	911
		X	X	X	X	X	X	X	X	X				X	1,644	960
	Total														6,798	3,946
Xerox Classic Fonts	Classic		X	X	X						X	X	X		508	344
Xerox Math Classic Fonts	Classic	X	X	X	X	X	X	X			X				1,253	772
		X	X	X	X	X	X	X				X			1,179	726
		X	X	X	X	X	X	X					X		844	545
	Classic Thin (Limited font set. Also includes sizes 16, 20, and 26.)								X		X	X			101	84
	Total														3,377	2,127
Helvetica 300™ Fonts	Helvetica (Also available in sizes 7, 9, and 11)	X	X	X	X	X	X	X			X	X			1,987	-
		X	X	X	X	X	X	X					X	X	2,073	-
	Total														4,060	-

NOTE: R = regular typeface; B = bold; I = italic; BI = bold italic; DPI = dots per inch.
[1]Versions 10.0 through 10.3 only

Table 6-5. **Disk pages required for printer fonts and test patterns (2 of 2)**

Font Family	Font Name	Font Sizes								Font Styles				Disk Pages	
		6	8	10	12	14	18	24	30 36	R	B	I	BI	300 DPI	200 DPI[1]
Xerox Printwheel Fonts	BoldPS			X						X	X	X	X	282	193
	BoldPS FigureSize			X						X	X	X	X	8	8
	Elite			X						X	X			128	84
	LetterGothic			X						X	X			151	101
	Master			X						X	X			128	90
	OcrA (12 point, 10 pitch)				X					X				38	23
	OcrB (12 point, 10 pitch)				X					X				34	21
	Pica				X					X	X			126	89
	PSBold (BoldPS)			X						X	X	X	X	282	193
	PSBold FigureSize			X						X	X	X	X	8	8
	Scientific			X	X					X	X			131	93
	Scientific Thin (16 and 18 point)						X			X	X			32	28
	Spokesman				X					X	X			171	121
	Titan			X	X					X	X			257	181
	Titan			X								X	X	125	88
	Trend (TrendPS)			X						X	X			144	102
	TrendFigureSize			X						X	X			4	4
	TrendPS			X						X	X			144	102
	TrendPS FigureSize			X						X	X			4	4
	Trojan				X					X	X			154	105
	Vintage			X	X					X	X			294	202
	Total													2,645	1,841
Xerox Japanese Modern Fonts	Modern (Chinese available only in 12 point)		X	X	X	X	X			X				29,836	-
Xerox Japanese Classic Fonts	Classic (Chinese available only in 12 point)		X	X	X	X	X			X				29,098	-
Xerox PC Emulation Fonts	PC Terminal				X					X	X			205	118
Xerox Arabic Safiir Fonts	Modern				X		X	X		X				1,090	-

NOTE: R = regular typeface; B = bold; I = italic; BI = bold italic; DPI = dots per inch.
[1]Versions 10.0 through 10.3 only

Dependencies and limitations

The Print Service and each printing option have certain dependencies and limitations.

Print Service limitations

- The Print Service and the Multiport Option cannot reside on the same server because each one must reserve the same portion of memory.
- Only one printing option at a time can run on the server.
- The print queue limit is 39 documents, unless the available disk space cannot accommodate 39 documents.
- Documents are printed in the order received.

8040 Series Electronic Printer and Laser CP Electronic Printer

- Fonts at 300 DPI (dots per inch) resolution are required, including the Xerox.Graphics.Newvec and Xerox.XC1-1-1.Modern font files.
- (Version 11.0 only) If the Print Service is configured with the complex printing feature enabled, the server must have at least 1.5 Mb of memory, 23-bit (extended) virtual memory, and at least a 25 Mb (8090 server) or a 29 Mb (8000 server) disk. To handle the widest variety of documents and allow more fonts, at least an 85 Mb (8090 server) or a 42 Mb (8000 server) disk is recommended. If the server has less than 3.6 Mb of memory, it must be configured for Print Service only.
- (Version 11.0 only) If the Print Service is configured with the slow page printing feature enabled, the server must have at least 1.5 Mb of memory and at least a 25 Mb (8090 server) or a 29 Mb (8000 server) disk. If the server has less than 3.6 Mb of memory, it must be configured for Print Service only.
- If the Print Service is added to a server with any other service, the server must have at least 768 Kb of memory and at least an 85 Mb (8090 server) or a 29 Mb (8000 server) disk.
- A server supporting the extended language fonts requires a minimum of 768 Kb of memory. An 8090 server requires at least an 85 Mb rigid disk drive to support either Japanese Modern or Japanese Classic fonts, or both. An 8000 server requires at least a 42 Mb rigid disk drive to support either Japanese Modern or Japanese Classic fonts; at least 80 Mb to support both. (Chinese fonts are incorporated into the Japanese font sets.)

Telecopier 495-1 Printer (versions 10.0 through 10.3 only)

- Fonts at 200 DPI (dots per inch) resolution are required, including the Xerox.Graphics.Newvec and Xerox.XC1-1-1.Modern font files.
- If a Telecopier 495-1 is added to a server with any other service, the server must have at least 768 Kb of memory.

- The Telecopier 495-1 cannot reside on the same server with another service that needs to use the local port.

Formatting Print Service (versions 10.0 through 10.3 only)

- The server must have at least 512 Kb of memory.
- Fonts at 300 DPI (dots per inch) resolution are required including the Xerox.Graphics.Newvec and Xerox.XC1-1-1/Modern font files.
- The Formatting Print Service can be associated with only one Target Print Service at a time.

Print Service Worksheet and Activity Log

Use the Print Service Worksheet to record server-related and service-related information, and information about your printing option and installed fonts. Use the Print Service Activity Log to track printer activity. The worksheet and the activity log are located at the end of this chapter.

Fill out a separate copy of the worksheet for each Print Service for which you have System Administrator responsibility. Store the completed worksheets in your *Activities Guide*. Maintain a copy of the activity log with each printer for which you have System Administrator responsibility. Retain the original worksheet and activity log for future use.

Using the worksheet and activity log

Before you install the software and set up your Print Service, complete the Print Service Worksheet. It is important that you fill out the Print Service Worksheet accurately and update it whenever changes occur. The completed worksheet saves you time as you perform the setup and maintenance procedures. It also serves as an information source for new System Administrators unfamiliar with your configuration.

Make an entry on the Print Service Activity Log any time major printer activity occurs. The log entries provide an easy way to monitor printer failures, excessive error codes, and other conditions requiring System Administrator assistance or printer repair.

Filling out the worksheet

As you read the rest of this chapter, you are directed to make entries on the Print Service Worksheet. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and the services installed on that server. Copy this information from the Services Installation Worksheet you filled out while reading the Services System Software chapter of this book.

Use sections ② through ⑤ to describe specific printing options. Use the appropriate section for your printing option.

Use section ⑥ to keep track of font families installed on the Print Service.

Planning for setup

After you install the Print Service, you must initialize it and install fonts and test patterns. Initialization begins when you specify the printing option, then name and describe the Print Service. See the Print Service chapter in the *Services Installation and Setup Guide* for complete procedures.

Versions 10.0 through 10.3 only:

If your printing option is a Telecopier 495-1, initialization also requires that you specify the paper width and the transmission resolution supported. Then you set the operational parameters, set the internal clock, and check server-to-printer communication.

If your printing option is the Formatting Print Service, you must specify the Target Print Service to receive and print the documents.

Common Print Service information

The information described in this section helps you set up the Print Service and applies to all printing options.

Print Service name and description

When you name the Print Service, use a name different from all other names in the domain. The fully qualified Print Service name takes the form:

Print Service name:Domain:Organization

The domain and organization must be the same as the domain and organization of the server. For example, if the server name is Dallas:Home Office:ABC Company, then the Print Service name might be Daily Planet:Home Office:ABC Company. To avoid possible errors, enter only the local name when you name the Print Service. This approach lets the domain and organization default to those of the server.

This naming convention gives the System Administrator for the server domain access to System Administrator commands for the Print Service. These commands are available only when you are enabled.

Some procedures request an optional Print Service description. The description may be the location of the printer (Printer in Room 386), a department name (Printer in Contracts), the name of the assigned System Administrator (Jane Miller's Printer), or any other descriptive information.

Related procedures: Initializing the 8040 Series Electronic Printer, the Laser CP Electronic Printer, or the Formatting Print Service; Initializing the Telecopier 495-1 Printer

Filling out the worksheet:

① Record the name and description of the Print Service.

Complex and slow page printing features (version 11.0 only)

The complex printing feature lets you print documents with more complex graphics, large numbers of graphics, or large bitmap images (e.g., scanned images). When you try to print a document but receive a banner sheet with the message "plate too complicated; large image plus many fonts" or "plate too complicated; too much font space," enable the complex printing feature and resend the document.

Complex documents take more time to format than simple documents. Depending on the number of complex pages in your document, formatting can take as long as 30 minutes. Even though more time is required to format a complex document, your system is operating normally as long as it responds to your commands. If you type **List Documents** periodically at the server, you will see the complex document being formatted for a long period of time.

The complex printing feature requires these resources:

- At least 1.5 Mb of real memory
- 23-bit (extended) virtual memory (VM)
- At least 17,700 available disk pages when the Print Service is run (8,700 more than the standard Print Service)

You can enable complex printing with only 12,000 available disk pages; however, the Print Service needs 17,700 available disk pages to function at the optimum level.

When you print a document that contains image gaps, enable the slow page printing feature and resend those pages containing the image gaps.

The slow page printing feature requires these resources when enabled separately:

- At least 1.5 Mb of real memory
- At least 11,700 available disk pages when the Print Service is run (2,700 more than the standard Print Service)

You can enable slow page printing with only 5,000 available disk pages; however, the Print Service needs 11,700 available disk pages to function at the optimum level.

See "Software requirements" earlier in this chapter for more disk space information.

CAUTION: Do not enable complex printing or slow page printing on multi-function servers with less than 3.6 Mb of real memory.

Related procedures: Initializing the 8040 Series Electronic Printer, the Laser CP Electronic Printer, or the Formatting Print Service; Changing the printing option

Filling out the worksheet:

② or ③ Use the appropriate section for your printing option and circle whether you will enable complex page printing or slow page printing.

Fonts

You must install fonts on your Print Service before it can process a job. Normally, you install fonts after initializing your Print Service, when you obtain new fonts, or when Xerox releases new versions of fonts. When you install fonts, you may specify that the files be loaded automatically using the default settings. The default settings load new, newer, or larger files; they do not load the same, older, or smaller files. These terms have the following meanings:

New - The named file does not exist on the server.

Newer - The named file on the installation medium has a newer creation date than the file on the server.

Larger - (Version 11.0 only) The named file on the installation medium is larger than the file on the server. Normally, you install the larger file, whether it is newer or older.

Same or Same Version - The named file on the installation medium has the same creation date as the file on the server.

Older - The named file on the installation medium has an older creation date than the file on the server.

Smaller - (Version 11.0 only) The named file on the installation medium is smaller than the file on the server.

Larger and smaller apply only to the Modern and Classic font families, which have large and small versions of font files.

Load the new, newer, and larger fonts that are compatible with your printing option. Then, as you determine which fonts you do not need, you can delete them to increase disk space.

When you load fonts from multiple floppy disks, you are prompted to insert the next floppy disk at the appropriate time. If you insert a floppy disk out of sequence, you see a message indicating that the disk is inserted in the incorrect order or does not have the requested file.

See "Planning for installation" earlier in this chapter for the compatible fonts, the sequence of installation, and disk space requirements.

Related procedure: Loading fonts and test patterns onto the Print Service

Fonts available on cartridge tape

You load font files onto the 8090 server from the following cartridge tapes:

- Xerox Network Printer Fonts 11.0 (300 DPI) - This tape contains all the 300 DPI (dots per inch) fonts (except the extended language fonts), including:
  - Xerox Required Fonts
  - Xerox Modern Fonts
  - Xerox Classic Fonts
  - Xerox Math Classic Fonts
  - Xerox Printwheel Fonts

- PC Emulation Fonts
- Helvetica 300™ Fonts
- Arabic Safiir Fonts

- Xerox Extended Language Fonts 11.0 (300 DPI) - This tape contains the Japanese Classic and Japanese Modern fonts.

Fonts available on floppy disks

You load font files onto the 8000 server from the following floppy disks:

- Xerox Required Fonts (300 DPI); Network Services 11.0
- Xerox Modern Fonts (300 DPI) - #1, #2, #3, and #4
- Xerox Classic Fonts (300 DPI)
- Xerox Math Classic Fonts (300 DPI) - #1 and #2
- Xerox Printwheel Fonts (300 DPI) - #1 and #2
- PC Emulation Fonts
- Helvetica 300™ Fonts (300 DPI)
- Arabic Safiir Fonts
- Xerox XC1K Modern Fonts (300 DPI) - #1 through #14. These floppy disks contain all the Japanese Modern Fonts (also called extended language fonts).
- Xerox XC1K Classic Fonts (300 DPI) - #1 through #14. These floppy disks contain all the Japanese Classic Fonts (also called extended language fonts).

Versions 10.0 through 10.3 only:

- Xerox Required Fonts (200 DPI)
- Xerox Modern Fonts (200 DPI) - #1 and #2
- Xerox Classic Fonts (200 DPI)
- Xerox Math Classic Fonts (200 DPI) - #1 and #2
- Xerox Printwheel Fonts (200 DPI)

Filling out the worksheet:

⑥ Check off the fonts you will load on the Print Service.

8040 Series Electronic Printer information

The 8040 Series Electronic Printer requires you to specify whether you have a B1 or B2 printer.

- The B1 printer has an output tray that holds 250 sheets. It delivers printed sheets face up.
- The B2 printer has a distinctive drum-shaped output stacker and a tray that holds 500 sheets. It delivers printed sheets face down.

See "Service description" earlier in this chapter for more information.

Related procedures: Initializing the 8040 Series Electronic Printer, the Laser CP Electronic Printer, or the Formatting Print Service; Changing the printing option

Filling out the worksheet:

② Circle whether you have a B1 or B2 printer.

Telecopier 495-1 Printer information (versions 10.0 through 10.3 only)

When you set up the Telecopier 495-1 Printer, you must specify a transmission resolution. You have two options:

- Standard mode transmits to group 1 or group 2 machines (machines other than Xerox Telecopier 495, 295, or 7000 models). Standard mode also permits faster transmission to another Telecopier 495-1 printer.
- Fine mode transmits to group 3 machines (other Xerox Telecopier 495, 295, or 7000 models) at maximum resolution (highest quality). Fine mode results in higher phone costs than standard mode.

Groups 1, 2, and 3 are standard terms used to describe the general capability and compatibility of a facsimile device. Group 1 is slower than group 2, which is slower than group 3.

Related procedure: Initializing the Telecopier 495-1 Printer

Filling out the worksheet:

④ Circle the transmission resolution your telecopier will support.

Formatting Print Service information (versions 10.0 through 10.3 only)

When you set up the Formatting Print Service, you must specify a Target Print Service to receive and print your documents. That Target Print Service must already be connected to the network and registered in the Clearinghouse.

The Formatting Print Service may reject print requests if it does not have the correct Target Print Service paper handling properties. Paper handling properties include paper size, stapling, and two-sided printing.

If the Target Print Service is not available when you first specify it, paper handling properties are set to these default values:

Paper size - letter size only

Stapling - not available

Two-sided copy - not available

Because the default properties may not be correct for the Target Print Service, you must update the paper handling properties.

You can update status and paper handling properties at any time. They are updated automatically when you specify the Target Print Service or when you reboot the server and restart the Print Service.

Related procedure: Setting the Target Print Service

Filling out the worksheet:

⑤ Record the fully qualified Target Print Service name that is registered in the Clearinghouse.

⑤ Record the network address of the Clearinghouse where the Target Print Service is registered.

Planning for maintenance

After you install and set up the Print Service, you are responsible for maintaining it. You perform maintenance as needed; there are no scheduled duties.

See the Print Service chapter in the *Services Maintenance Guide* for complete maintenance procedures.

Common Print Service information

The information described in this section helps you plan for Print Service maintenance and applies to all printing options.

Canceling a document (version 11.0 only)

An enabled System Administrator may cancel printing of a specific document sent to the Print Service or all documents in the Print Service queue. A logged on user may cancel his or her own documents only. The user's fully qualified name must be specified as the sender name with the print request. For example, if a user logs on at a server as Mary C. Wright, the user can only cancel documents sent to the printer by Mary C. Wright. If the user logs on at the server using an alias, the Print Service validates his or her fully qualified name at the Clearinghouse Service.

ViewPoint workstations automatically supply the fully qualified sender name with each print request. Some network workstations do not supply this information and the user must ensure that his or her fully qualified name is sent with the print request. Xerox Development Environment users must specify their fully qualified names in the PrintedBy field in the Hardcopy section of their user.cm. For example:

```
[Hardcopy]
PrintedBy: "Mathew H. Bell:Home Office:ABC Company"
```

Related procedures: Canceling a specific document sent to the Print Service, Canceling all documents sent to the Print Service

Canceling a document (versions 10.0 through 10.3 only)

An enabled System Administrator can cancel printing of documents in these categories:

Formatting document - The document being formatted

Printing document - The document being printed (Telecopier 495-1 only)

Forwarding document - The document being forwarded (Formatting Print Service only)

Documents being processed - All documents being processed (the document being formatted, documents already formatted, and the document being printed or forwarded)

Queued documents - All documents awaiting processing

All documents - All documents

List the documents first to determine the status of the document you want to cancel.

Related procedure: Canceling a document sent to the Print Service

Complex and slow page printing features (version 11.0 only)

This information is the same as for setup. See "Complex and slow page printing features" under "Planning for setup" earlier in this chapter.

Related procedure: Printing documents with complex pages

Default substitution font (version 11.0 only)

The default substitution font is the font that the Print Service substitutes when you request a font that is not installed or a character that is not available in that font. The Print Service automatically specifies the Modern font as the default substitution font when the service is installed.

You may change the default substitution font to specify Classic. If you normally use serif fonts in your documents, then specify Classic as the default font. A serif font has short lines stemming from and at an angle to the upper and lower ends of the strokes of each letter. If you normally use sans serif fonts, then specify Modern. A sans serif font does not have lines stemming from each letter.

Related procedure: Changing the default substitution font

Listing documents

You can list the documents received by the Print Service to check the position of a document in the queue or the status of all documents. For up to 39 documents, the listing shows the sender, the document status, and the document name. The listing also shows the number of pages, if the document is being or has been formatted.

(Versions 10.0 through 10.3 only) If your printing option is a Telecopier 495-1, the document listing includes the status for each job destination (Transmit Status). For local printing, the destination is identified as "local." For a remote transmission, the destination is identified by the first 22 characters of the telephone number that the user supplied. The listing shows the date and time that processing was completed for each destination, and the elapsed telephone time for remote transmissions.

Documents are listed in the order they were added to the queue, from the most recent to the earliest addition. You can list documents in these categories:

Documents being processed - Lists documents being processed

All uncompleted documents - Lists all documents awaiting processing as well as those documents being processed

Completed documents - Lists all completed documents

All documents - Lists all documents

The default is all uncompleted documents.

Related procedure: Checking the status of documents received by the Print Service

Print Service status

You can display the Print Service status to monitor the operational status of the printer. The display shows the following information:

- Whether the service is started or stopped
- The person who started printing and queuing
- The date the service was installed and the times rebooted
- The date last rebooted
- The date statistics were last reset
- The date of the last activity
- The queue disk pages allocated
- The font directory disk pages allocated
- The default substitution font (version 11.0 only)
- The printing option supported
- The printer status
- Whether the complex printing and slow page printing features are enabled, disabled, or unavailable (version 11.0 only)

If the server does not have the required resources to support either of these features, the status is unavailable.

- The paper handling options

Each statistic is displayed including a count since the last reboot (current count) and a count since statistics were last reset (cumulative count). Statistics and their meanings are:

- Documents being processed - The number of documents printed successfully by the Print Service
- Documents canceled - The number of documents that users canceled or the Print Service aborted (version 11.0 only)
- Documents aborted - The number of documents that users canceled or the Print Service aborted (versions 10.0 through 10.3 only)
- Queue failures - The number of documents that could not be queued (usually documents too big to fit on the server disk, or for which the requested paper size was not available)
- Test pattern requests - The number of test patterns printed
- Recovery retry requests - The number of documents found in progress and retried after a server reboot
- Docs purged at recovery - The number of documents found in progress and aborted after a server reboot

Documents found in progress after a server reboot are generally retried once. If found in progress after a second server reboot, they are aborted. Such handling prevents a problem document from repeatedly crashing the Print Service.

You can reset to zero the current count and cumulative count for each statistic displayed.

Related procedure: Showing Print Service status

Renaming the Print Service

You can change the name of the Print Service at any time. Changing the name deletes the old name from the Clearinghouse Service database and adds the new name to the database. See "Print Service name and description" under "Planning for setup" earlier in this chapter.

Related procedure: Renaming the Print Service

8040 Series Electronic Printer information

The additional information in this section helps you plan for 8040 Series Electronic Printer maintenance.

Paper handling options

You can change the paper handling options if the default settings do not meet your requirements. If you change the options for a special print job, be sure to return them to their original settings when that job has been completed. You have these paper handling options:

- **Paper size** - Lets you select one of these paper sizes for the top tray and the bottom tray:
  - 8.5" x 11"
  - 8.5" x 14"
  - A4

  The default setting is 8.5" x 11" for both trays.

If you use an incorrect paper size, print requests may be rejected or printed on the wrong paper size.

- **Feed** - Controls which paper tray feeds the printer, operating in conjunction with the paper size selected. You have two options:
  - From bottom, banner from top - Feeds the banner sheet of a job from the top tray, and all other pages from the bottom tray. A banner sheet, also known as a banner page, precedes the first page of a document, if you set parameters for banner sheet printing. If both trays use the same paper size, you can separate jobs by loading colored paper into the top tray for banner sheets.
  - From bottom or top - Lets the Print Service print longer without adding paper. When one tray is empty, the other tray starts feeding the printer.

If both trays are the same paper size and the feed option is set from bottom or top, the paper will feed from the bottom tray first. When the bottom tray is empty, the message "C-4: Please check paper tray" displays. Three to five seconds later, the system notices that it can feed from the top tray, resumes printing, and displays a normal status.

If both trays use the same paper size, the default setting is from bottom or top. If the trays use different paper sizes, the default setting is as appropriate; paper feeds from the tray containing the paper size needed.

- **Banner -** Controls printing of banner sheets. You have three options:

  - Per copy - Prints a banner sheet for every copy of a document.
  - Per set of copies - Prints a banner sheet for every job request.
  - Suppressed - Prints no banner sheet.

  The default setting prints a banner sheet for every job request.

  A banner sheet identifies who sent the document to the Print Service and the document name. The workstation supplies the sender name, document name, and time created. If any of these are not supplied, they will not appear on the banner sheet. The Print Service supplies the time of printing, the number of sheets (pages) and copies printed, and the name of the printer.

  If the Print Service encounters warnings or errors when formatting the document, the banner sheet includes a message with the warning or error. There are two types of banner sheet messages:

  - Appearance warning messages try to describe the problem and usually indicate an appearance error. Only the first appearance warning is printed on the banner sheet. Additional warnings are indicated by "...and <number> more."
  - Error messages indicate problems that prevent printing of part or all of a document. Some errors indicate that the limitations of the Print Service have been exceeded, others that the document is malformed.

  Here is an example of the information you see on a banner sheet:

  For Jackson:Home Office:CCCB

  Important Memo

  Created 11-Mar-87 14:03:22

  Printed 11-Mar-87 14:04:52

  5 Sheet(s), 4 Copies.

  Xerox Print Service 10.5 on Concord

  Appearance Warning: font 'Modern' substituted for 'Classic'

  Appearance Error (page 2): image off paper at (8.62,8.60) inches, (21.99,21.93) cm...and 8 more.

  Banner messages are in the "Problem messages" chapter of *MP Codes and Messages* in *Basic Network Troubleshooting*.

- **Stacking** - Controls the output stacking alignment on B2 printers only. You have three options:
  - Aligned - Stacks the document aligned with other documents.
  - Each copy offset - Stacks each copy of a document offset.
  - Each set of copies offset - Stacks each print job offset.

  The default setting stacks each print job offset.

Related procedure: Changing paper handling options

Filling out the worksheet:

② Record the default settings for paper size, feed, banner, and stacking; these are the current settings. Be sure to update the worksheet if you change them.

Laser CP Electronic Printer information

The Laser CP Electronic Printer maintenance enables you to control when banner sheets are printed. You have three options:

- Per copy - Prints a banner sheet for every copy of a document.
- Per set of copies - Prints a banner sheet for every job request.
- Suppressed - Prints no banner sheet.

See the preceding section for a sample banner sheet.

Related procedure: Changing the banner option

Telecopier 495-1 Printer information (versions 10.0 through 10.3 only)

The additional information in this section helps you plan for Telecopier 495-1 Printer maintenance.

Paper handling and transmission options

Telecopier 495-1 Printer maintenance enables you to change the paper handling and transmission options. You have three options:

- **Transmission retries** - Controls the handling of transmission retries after an unsuccessful attempt to transmit to a remote facsimile device. There are two types of failed transmissions:
  - No telephone connection is made; the document transmit status is "Busy" or "No answer."
  - A telephone connection is made but an error occurs during transmission; the document transmit status is "Transmit error" or "Local FAX failure."

  For each type of failed transmission, you specify the number and frequency of transmission retries:
  - Retries in case of no connection (0..100)
  - Retry interval in minutes (1..100)
  - Retries in case of transmit error (0..100)
  - Retry interval in minutes (1..100)

The maximum number of retries is 100. The maximum retry interval, which is the number of minutes between each transmission attempt, is 100. Retries may be delayed if another document is being printed or transmitted.

For transmissions that failed because no connection was made, the default setting allows six retries at five-minute intervals. For transmissions that failed because of error, the default setting allows three retries at two-minute intervals.

Retries caused by transmit errors are more costly than retries necessary because phone contact was never made.

- **Banner** - Controls when banner sheets are printed, both locally and remotely. See "Paper handling options," under "8040 Series Electronic Printer information," earlier in this chapter, for more information and a sample banner sheet.
- **Multiple copies** - Controls the printing of multiple document copies, both locally and remotely. You have two options for local and remote printing:
  - Allowed - Permits printing of multiple copies.
  - Suppressed - Does not permit printing of multiple copies (helps control phone costs when sending to a remote printer).

  For local printing, the default setting allows multiple copies. For remote transmissions, the default setting suppresses multiple copies.

Related procedure: Changing paper handling and transmission options

Filling out the worksheet:

④ Record the default settings for transmission retry values, banner, and multiple copies; these are the current settings. Be sure to update the worksheet if you change them.

Formatting Print Service information (versions 10.0 through 10.3 only)

Formatting Print Service maintenance enables you to specify a different Target Print Service to receive and print your document. For more information, see "Formatting Print Service" under "Planning for setup" earlier in this chapter.

Related procedures: Changing the Target Print Service, Updating paper handling options

7. File Service

This chapter helps you prepare for installation, setup, and maintenance of the File Service. This information supports the procedures you perform from an 8000 or 8090 server.

Service description

A network consists of many distributed and interconnected workstations. The File Service provides an efficient and convenient means for consolidating and sharing data files produced at any networked workstation. Personal computers can access the File Service through the Interactive Terminal Service.

How the software works

The File Service lets you store and retrieve files created on all types of workstations and personal computers. You can make these files available to other users by copying the files to a File Service.

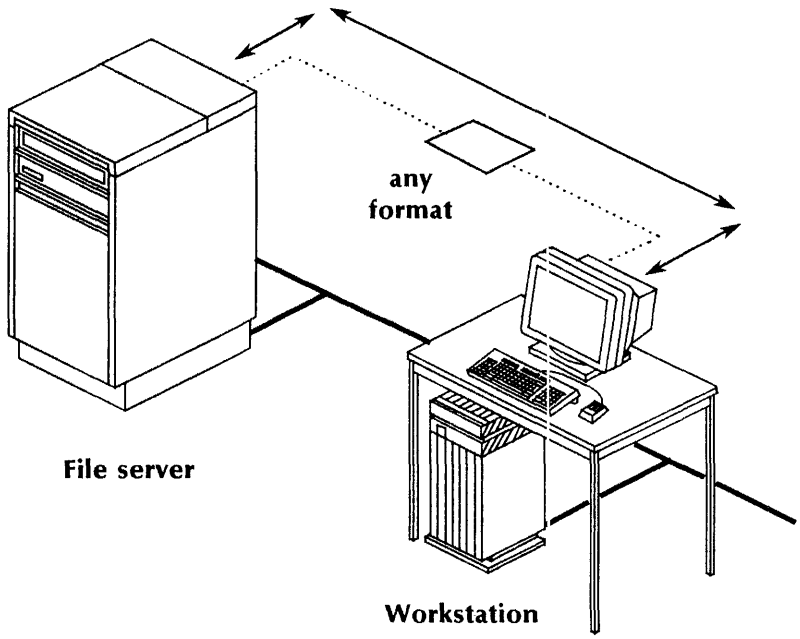
You can also access and retrieve a file created at a different type of workstation using format conversion software available on some networked workstations and through the Interactive Terminal Service. To retrieve a document that is in ASCII format from a non-ASCII device, you first convert the document to the format of the non-ASCII device.

File Service requests

When you initiate a request for File Service activity, the workstation software contacts the File Service and establishes a connection. The information is transmitted over the Ethernet (and through Internetwork Routing Services, if the File Service is on a different network) to the File Service.

Figure 7-1 shows transmitting a document between a workstation and a file server.

Figure 7-1. **Transmitting a document between a workstation and a file server**



Users frequently use the File Service to store backup copies of files from their workstations, to store infrequently used files and increase workstation disk space, to share files with other network users, and to archive files. The File Service can also store users' desktops, enabling a user to log on at any 6085 or 8010 workstation on the network and retrieve the desktop.

Multiple workstations can connect simultaneously with the File Service, increasing the accessibility of the files. File Service performance and ability to fulfill requests depend on these variables:

- The amount of memory on the server where the File Service resides
- The number of simultaneous operations requested by users
- The number of other active services residing on the server with the File Service
- The current level of use of coresident services

File drawers and folders

The File Service stores information in directories (containers) called file drawers and folders. A file drawer contains all the folders and files at the next lower level. This second level can contain more folders or files, as can the third and fourth levels. The hierarchy can include as many levels of folders as you need.

File Service states

The File Service has two states: started and stopped. File Service volumes also have two states: online and offline. The state of the File Service is independent of the state of its volumes. If the File Service is started, a volume must be online to be available to network users. If the File Service is stopped, none of its volumes is available to network users, even if the volume is online. When you stop a File Service, it remains in the stopping state until all connections are terminated.

Relationship with other services

The File Service supports these services and functions:

- The Clearinghouse Service uses the File Service to back up the Clearinghouse database when there is only one Clearinghouse Service in the network.
- The Mail Service uses the File Service for backup and restore functions.
- The Services System Software uses the File Service to back up and restore the server profile file.
- The Boot Service uses the File Service to store the installation utility, which allows users to install workstation software over the network.
- The Interactive Terminal Service must access one or more File Services to support its clients.
- The Remote Batch Service requires that the File Service be on the internetwork. Network workstation users direct Remote Batch Service jobs to a File Service; the Remote Batch Service directs completed jobs to a File Service.
- The Server Monitor Service uses a file drawer on the File Service to back up and restore its database.
- The Librarian Service uses a file drawer on the File Service to back up and restore its database.
- The SNA Mail Relay Service uses a file drawer on the File Service to back up and restore its database.
- The PC File Service enables PC users to share (access, store, and retrieve) the File Service directories, file drawers, and files.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the File Service Worksheet and the File Drawer Worksheet located at the end of this chapter
- Installing the File Service software as described in the Server Software Installation chapter of the *Services Installation and Setup Guide*
- Setting up the File Service as described in the File Service chapter of the *Services Installation and Setup Guide*
- Maintaining the File Service as described in the File Service chapter of the *Services Maintenance Guide*
  - Monitoring the disk space of File Service volumes
  - Monitoring the disk space and use of file drawers
  - Monitoring the desktops stored on the File Service
  - Monitoring File Service activity
- Notifying users of any change or disruption in the service, for example:
  - When service is interrupted for a substantial period of time
  - When File Service volumes or file drawers become too full
- Performing backup procedures regularly as described in the File Service chapter of the *Backup and Restore Guide*
- Upgrading hardware and software as required
- Troubleshooting the service as described in *Basic Network Troubleshooting*

You can perform most File Service procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter in the *Services Installation and Setup Guide* contains the procedures for installing the File Service software. This section explains hardware, software, and other requirements to prepare you for installation.

Hardware requirements

The File Service operates on an 8000 or 8090 server attached to a server console. The server may be a single-drive or a multiple-drive server. The disk drive is the physical device that contains a rigid disk or a removable disk pack. See "File Service volumes" later in this chapter for more information.

As you determine your hardware requirements, consider the amount of space the File Service and coresident services will require, the amount of space the backup function will require, and the use of the File Service by network users.

Software requirements

The File Service requires these program files:

- FileSDF.bcd
- FileServiceConfig.bcd
- FileService.messages
- FSCommonConfig.bcd
- FSCommon.messages

Allow about 275 disk pages for the File Service program files.

When you install File Service software on a multiple-drive server, you must install it on the primary volume. You may then install the software on a secondary volume as well. When you upgrade the software, be sure you install the new software on the primary volume and all secondary volumes containing the File Service software.

CAUTION: If you replace a primary volume with a secondary volume running an older software version, the File Service detects that the software is not compatible and requests a scavenge. If you run the scavenge, it changes the new data to the old format with unpredictable results.

Dependencies and limitations

The File Service has these dependencies and limitations:

- The File Service relies on the Clearinghouse Service to register file drawer users and authenticate access rights.
- The File Service's automatic backup facility is required in multiple File Service configurations. The facility automatically backs up one or more File Service volumes to different File

Services at scheduled intervals. See the File Service chapter in the *Backup and Restore Guide* for more information.

- The File Service can support up to 15 connections. If other services are installed and running on the server, the maximum is 15 connections for all services.
- If both 80 and 300 Mb drives are attached to an 8000 server, the 300 Mb drive must be used as the primary drive.
- When you use the File Service to back up the database of another service, the two services should not coreside.
- Stop all coresident communication services before formatting a cartridge tape. Stop all coresident communication services that use the server's local RS232C port before a backup, restore, copy container, or restore container operation using floppy disk or cartridge tape. You do not need to stop services if you are using the CIU or Multiport Option Kit.

File Service worksheets

Use the File Service Worksheet to record server-related and service-related information. Use the File Drawer Worksheet to record the size of the file drawer and the users' access rights. The worksheets are at the end of this chapter.

If you have several single-drive servers, fill out a separate copy of the File Service Worksheet for each File Service for which you have System Administrator responsibility. If you have a multiple-drive server, record the data for all File Service volumes on the same worksheet. Fill out a separate copy of the File Drawer Worksheet for each file drawer you create. Retain the original worksheets for future use, and store the completed worksheets in your *Activities Guide*.

Using the worksheets

Before you install the software and set up your File Service, complete both worksheets. It is important that you fill out the worksheets accurately and update them whenever changes occur. The completed worksheets save you time as you perform the setup and maintenance procedures. They also serve as an information source for new System Administrators unfamiliar with your network configuration.

Filling out the worksheets

As you read the rest of this chapter, you are directed to make entries on the File Service Worksheet and the File Drawer Worksheet. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① of the File Service Worksheet for information about the server and the services installed on the server. Copy this information from the Services Installation Worksheet you filled out while reading the Services System Software chapter of this book. Use section ② for information about the primary and secondary File Service volumes. Use sections ① and ② of the File Drawer Worksheet to record information about each file drawer on the volume.

Planning for setup

After you install the File Service software, you must initialize the primary volume of the File Service. If you have a multiple-drive server, you then initialize each secondary volume separately.

Initializing a primary volume includes naming and describing the File Service and bringing the volume online. Initializing a secondary volume includes naming the volume and bringing the volume online. When you bring a volume online, the volume registers in the Clearinghouse and becomes accessible to network users. When initialization is complete, you create file drawers.

This section helps you prepare for the setup procedures. See the File Service chapter in the *Services Installation and Setup Guide* for complete procedures.

File Service volumes

The disk drive provides the storage capacity for the File Service. The collection of files contained on each disk is called a volume. You can partition each disk drive connected to a server into a volume and then initialize the volume to contain a file system managed by the File Service.

The File Service can manage up to four volumes on an 8000 server; seven volumes on an 8090 server. These volumes can be accessed at the same time. Each volume is registered in the Clearinghouse as a File Service. You give users file storage and retrieval capability by adding file drawers to the volume.

Single-drive servers

A single-drive server has only one volume, the primary volume. You make the files on a volume accessible to network users by bringing the volume online.

An 8090 single-drive server may have a 25 Mb or an 85 Mb fixed drive. An 8000 single-drive server may have a 10 Mb, 29 Mb, or a 42 Mb fixed drive.

Filling out the worksheet:

① Record on the File Service Worksheet if you have a single-drive server.

② Record the disk size of the primary volume on the File Service Worksheet.

Multiple-drive servers

On a multiple-drive server, the volume in drive 1 is a special volume called the primary volume; this volume stores the software for each service. This drive has the name "Primary::", but you rename it during initialization. Multiple-drive servers have additional drives known as secondary drives; the volumes contained therein are secondary volumes.

The File Service may use multiple disk packs for storing files on a multiple-drive server. You can remove the disk packs from the server and load them on a different server.

An 8090 multiple-drive server may have up to seven drives. This may be any combination of 310 Mb fixed disk drives or high-capacity cartridge tape drives (about 100 Mb), not to exceed four high-capacity cartridge tape drives per server. An 8000 multiple-drive server may have any combination of up to four 80 Mb or 300 Mb drives.

Filling out the worksheet:

① Record on the File Service Worksheet if you have a multiple-drive server.

② Record on the File Service Worksheet the disk size of each secondary volume.

Volume states

A volume can be open or closed; when open, it can be either online or offline. When a volume is open and offline, the files it contains are available only for local System Administrator operations. If the volume is open and online, the files it contains are available to all network users.

When a volume is closed, the files it contains are not available to local or remote users. You can also unload removable disk packs when the volume is closed. You cannot close a primary volume, because it must be available to local users at all times.

File Service names and descriptions

When you name the File Service, use a name different from all other names in the domain. If you have a multiple-drive server, each File Service volume is considered a separate File Service and must have a different local name. The fully qualified File Service name takes the form:

File Service name:Domain:Organization

The domain and organization must be the same as the domain and organization of the server. For example, if the server name is Universal:Headquarters:XYZ Company, then the File Service name might be Los Angeles:Headquarters:XYZ Company. This naming convention gives the enabled System Administrator for the server domain access to all File Service commands.

To avoid possible errors, enter only the local name when you name the File Service. This approach lets the domain and organization default to those of the server. Do not use commas (,), parentheses (), asterisks (*), or pound signs (#) in the volume name.

Some procedures request an optional File Service description. Providing a description helps to identify the location or the users of the File Service. The description may be the location of the server where the File Service resides (Room 211), a department name (Public Relations), or any other descriptive information.

Related Procedures: Initializing the primary volume, Initializing secondary volumes

Filling out the worksheet

② If you have a single-drive server, record the name and description of the File Service on the File Service Worksheet.

If you have a multiple-drive server, record the name and description of the primary volume and the name of each secondary volume.

File drawer hierarchy

The File Service organizes files hierarchically. Each level of the hierarchy contains the folders and files that are descendants of the preceding level. A major file drawer at the top level of the file organization contains all the file drawers, folders, and files at the second level. These folders and files can contain additional levels of subdirectories or documents.

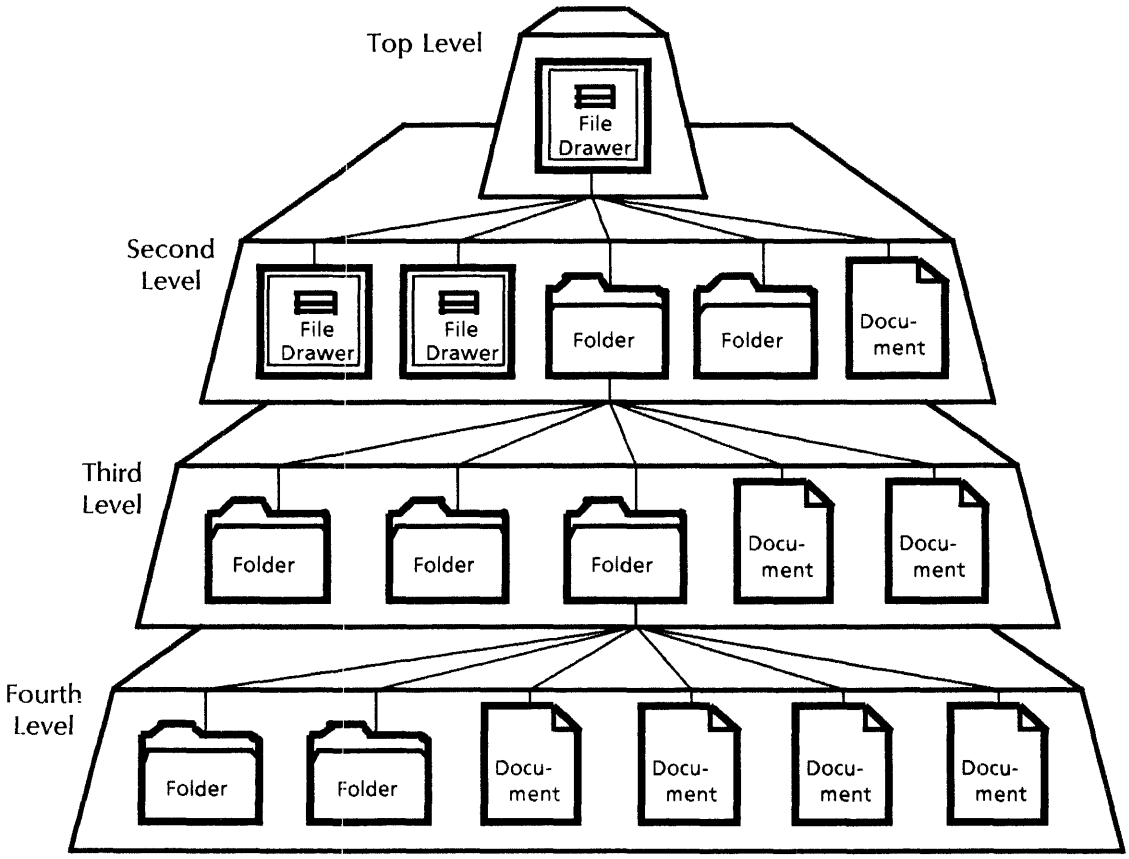
For example, you might create a folder at your 6085 or 8010 workstation and name the folder "Reports." This folder might contain other folders (subdirectories) named for each month of the year. These folders might in turn contain folders (sub-subdirectories) named "Progress Reports" or "New Hire Adjustments," within which you can store any number of related documents. By enclosing folders within folders, you can group related files. There is no limit on the number of directory levels. However, there is a limit on the drawer size and the amount of storage space available on the server running the File Service.

The File Service automatically sorts the contents of file drawers and folders according to the attributes set for each. Files in a folder may be sorted to appear in ascending or descending alphabetical order by name, or by creation date. Files may also appear in the order sorted by the user.

The File Service uses only the first 34 characters (fewer for foreign language characters) of the file name to sort files within a directory or file drawer. Thus, file names longer than 34 characters may appear to be out of order.

The hierarchy develops as users access the file drawer and add folders and documents. Figure 7-2 shows an example of a hierarchy with four levels. Note that the File Service has a filing system feature that lets users store and retrieve complete hierarchies of directories and documents in one operation.

Figure 7-2. **Hierarchy example**



Creating file drawers

You can create private file drawers for individual users and public file drawers for groups of users to share. Users can store files in a file drawer and retrieve them from the drawer through their workstations. The available volume space limits the number of file drawers residing on a volume.

If you have more than one File Service volume available, divide the private file drawers among the volumes to allow room on each volume for future expansion.

Consider creating a file drawer for System Administration use. An appropriate name for the drawer might be "Administration Statistics." Set up folders inside the drawer, naming them for each server, and store in them Server Monitor Service logs, scavenger logs, backstop logs, configuration dialogues, and the server profile. Your Systems Analyst will find this data useful when reviewing the server's performance.

You assign file drawer attributes when you create file drawers. Attributes include the file drawer name, file drawer owner, page limit, and access list. The access list contains the name and access rights for each user.

If your server is also running PC File Service, consider the needs of its users as well. Since the PC File Service does not set page limits on the file drawers it creates, you must set the page limit for each PC File Service drawer at the File Service.

File drawer name

The file drawer name you assign must be unique on the volume, and must be no longer than 100 characters. You cannot use the wildcard symbols (* or #) when you name a file drawer.

Related Procedures: Creating private file drawers for users, Creating public file drawers for users

Filling out the worksheet:

① Record the name of the file drawer you will create on the File Drawer Worksheet. Also, record the name, domain, and description of the File Service on which you will create the file drawer. Use a separate worksheet for each file drawer.

File drawer owner

Each file drawer is associated with an internetwork user, known as the owner of the file drawer. Users and group members who have file drawer ownership or access must be registered in the Clearinghouse.

Related Procedures: Creating private file drawers for users, Creating public file drawers for users

Filling out the worksheet:

① Record on the File Drawer Worksheet the name of the owner of the file drawer you will create.

Page limit

You assign a page limit to each file drawer so you can control its size. The file drawer and all the files it contains cannot exceed the page limit.

You can set the page limit at any number between 0 and 2,147,483,647 disk pages. When you set the page limit at 0, a file drawer can consume unlimited disk pages. Setting the page limit at a very large number is the same as specifying 0; the capacity of the volume becomes the limiting factor, not the page limit.

Because all file drawers are not always filled to capacity, you can set page limits that are cumulatively greater than the volume capacity. Thus, a volume may fill even though no file drawer has exceeded its limit. The maximum volume capacity for a 300 Mb File Service is about 430,000 disk pages.

For a primary volume on a multiple-drive server, consider also the space requirements of other services as you determine the number of file drawers to create and their page allocations.

Limit file drawer size based on how the drawer will be used. To determine the appropriate size, create the file drawer with a

page limit of 0. Then monitor the file drawer use over time and change the page limit, if necessary. For example, you might limit file drawers for individual users to fewer than 1,000 pages, if they store most of their work in public file drawers.

Table 7-1 shows the approximate number of disk pages consumed by standard 8.5" x 11" documents.

Table 7-1. **Document pages and disk pages**

Standard Document Pages	Description	Number of Disk Pages
1	Simple text	10
10	Simple text	100
1	Complex graphics	15 to 20
10	Complex graphics	150 to 200

Related Procedures: Creating private file drawers for users, Creating public file drawers for users

Filling out the worksheet:

① Record on the File Drawer Worksheet the page limit for each file drawer you will create.

Access list

The access list restricts user access to a file drawer, ensuring privacy and security of the data. An access list contains the names of individuals and groups who have access to a file drawer, along with the type of access rights they have.

When you add a file drawer, the name of the owner automatically appears on the access list with full access. (Full access means that all five access rights are granted.) A System Administrator, owner, or user with "change" access rights to a file drawer can make changes to the access list.

For example, suppose the owner of a file drawer is a publications manager with full access to the drawer. You may want to give employees reporting to this manager limited access to copy documents and folders to and from the file drawer.

To simplify the access list, you can create a user group in the Clearinghouse Service that includes all members of the publications group. You can assign access to the file drawer by specifying the user group name you registered in the Clearinghouse Service.

You can use name patterns containing the wildcard symbol (*) to specify access list entries. A pattern is a string of characters including an asterisk. The asterisk is treated like a wildcard and matches any character or group of characters. Any individual whose user name matches the given pattern has the specified access to the file drawer.

Only those patterns in which asterisks replace the local name, domain, or organization are allowed in access list entries. If you

use an asterisk for the domain name, you must also use an asterisk for the local name. If you use an asterisk for the organization name, you must also use asterisks for the local and domain names. Table 7-2 shows examples of valid and invalid patterns.

Table 7-2. **Examples of patterns**

Valid patterns	Invalid patterns
*:Chicago:Acme[1]	*Smith:Chicago:Acme
::Acme[2]	Smith:*:Acme
::*[3]	*:Chicago:*

[1]Specifies all users within the Chicago domain of the Acme organization
[2]Specifies all users and domains of the Acme organization
[3]Specifies all users, domains, and organizations within the internetwork

You can shorten the time required to validate access list entries and help control the workload of the Clearinghouse Service by organizing entries in this order:

1. Name patterns using wildcard symbols (*) - These entries are evaluated first; they are the most efficient because the File Service evaluates them without using the Clearinghouse Service.
2. Individual names - These entries are the second most efficient. Order the most frequently used names first.
3. Group names - These entries are the least efficient. Order the most frequently used names first. To improve the efficiency of these entries:
   - Replace a group entry with a name pattern using wildcard symbols (*), whenever possible.
   - Place a group in the same Clearinghouse domain as the individuals and groups it contains, so access is required only at one Clearinghouse Service.

If your server is also running PC File Service, a File Service user cannot access PC File Service file drawers unless you assign access rights at the File Service using the **Change File Drawer** command. File Service access rights do not affect users of the PC File Service.

Related Procedures: Creating private file drawers for users, Creating public file drawers for users

Filling out the worksheet:

② Record on the File Drawer Worksheet the fully qualified names of users or groups who will access each file drawer.

Access rights

You can grant a user any combination of the five access rights:

- Read - Lets the user list and copy objects from a file drawer.

- Write - Lets the user change the attributes and the content of objects in the file drawer. The user also needs read access to be able to list the file drawer contents before changing their attributes.
- Add - Lets the user place new files in a file drawer or folder.
- Remove - Lets the user remove a file from the file drawer or folder. Users must have write access to the file drawer; 6085 or 8010 ViewPoint users must also have read access to list the files.
- Change access list - Lets the user add and remove entries from the access list for the file drawer.

Table 7-3 shows the minimum access required for specific operations.

Table 7-3. **Minimum access rights**

Operation	Minimum required access				
	Read	Write	Add	Remove	Change
Open Drawer/Copy out	X				
Change Properties	X	X			
Copy/Move in			X		
Move out/Delete[1]		X		X	
Change Access List					X

[1]6085 or 8010 ViewPoint users must also have read access to list the files.

Related Procedure: Creating public file drawers for users

Filling out the worksheet:

② Check off on the File Drawer Worksheet the access rights for each user or group who will access the file drawer.

Planning for maintenance

After you install and set up the File Service, you are responsible for maintaining it. See the File Service chapter in the *Services Maintenance Guide* for complete maintenance procedures.

Your most important scheduled maintenance activities are maintaining file drawers and monitoring File Service disk space.

Scheduled maintenance also includes backing up the File Service to protect data from loss. See the File Service chapter in the *Backup and Restore Guide* for more information.

Maintaining file drawers

File drawer maintenance includes adding private and public file drawers for users, deleting file drawers, changing file drawer attributes, and assigning access rights. You perform these activities as needed.

Normally, you create a file drawer when a new employee is hired. You delete a file drawer when an employee leaves.

You can change the attributes of a file drawer at any time. You may change the page limit to control the amount of disk space the drawer consumes. If you change the file drawer owner, you must also add the new owner to the access list so that access is granted. You can change the access list by specifying new access rights for an existing entry. To delete an entry, grant no access rights.

For more information on file drawer attributes and access rights, see "Creating File drawers" under "Planning for setup" earlier in this chapter.

Related Procedures: Changing file drawer information, Creating private file drawers for users, Creating public file drawers for users, Deleting file drawers

Wildcard symbols

You can use the wildcard symbol (*) to list or delete file drawers or files. Use the (*) alone to select all entries on the volume. Specify a pattern to select only those file drawers or files matching the pattern. You can use these patterns:

*name	Specifies all files with the suffix *name*
name *	Specifies all files with the prefix *name*
na*me	Specifies all files with the prefix *na* and the suffix *me*

You can also use the wildcard symbol (#) to list or delete file drawers or files. The symbol (#) matches any one single character. For example, if you want to select file drawers named Reports A, Reports B, and Reports C, you can specify Reports #.

Related Procedures: Creating public file drawers for users, Deleting file drawers, Listing file drawers, Monitoring file drawer disk usage, Recovering file drawer space by deleting old file versions, Recovering File Service disk space by deleting obsolete

desktops, Recovering File Service disk space by moving file drawers

Monitoring File Service disk space

You must regularly monitor the number of available pages on the File Service volume. If your server is also running PC File Service, be sure to consider the needs of PC File Service users when you monitor disk space. If you have more than one server, check each one. If a File Service volume regularly becomes more than 90 percent full, consider expansion to an additional or larger capacity server. A File Service that is too full cannot hold additional file drawers or perform necessary backup operations.

CAUTION: A volume should NEVER be more than 98 percent full. Otherwise, File Service performance becomes impaired and may fail.

You monitor a volume's disk space by displaying this information:

- The volume name
- The amount of used and available disk space
- The percentage of disk space used
- The status of the volume
- The drive number

Multiple-drive servers show this information for each volume that the File Service manages.

Related Procedure: Monitoring your services volume. See the Services System Software chapter of the *Services Maintenance Guide* for this procedure.

Disk usage report

The disk usage report lets you monitor file drawers with many files, many versions of files, and files that are seldom or never used. Consider archiving or deleting any files that have not recently been used.

You can create a disk usage report for specified file drawers on a particular volume. The report includes:

- The file drawer name
- The total number of files and pages consumed
- The number of files and pages used for old versions of files
- The number of pages referenced in the last 30, 60, 90, and 180 days
- The number of pages never referenced

To create a disk usage report, you must specify where you want to store it. Be sure you have access to the file drawer you specify. To specify a remote location for the report, use the form:

(Volume:Domain:Organization)DiskUsage/Reports

To specify a local location for the report, you may also use one of the following forms:

()DiskUsage/Reports

(Volume:)DiskUsage/Reports

In the first form, the volume name, domain, and organization default to those specified in the command that creates the report. In the second form, only the domain and organization default to those specified in the command that creates the report.

After the file is created, you can retrieve it at your workstation, convert it to the proper format, display it, and print a copy for your files. See the "Monitoring file drawer disk usage" procedure in the File Service chapter of the *Services Maintenance Guide* for a sample disk usage report.

Related Procedure: Monitoring file drawer disk usage

Recovering disk space

As System Administrator, you can perform several activities to increase the disk space on the server volume. These activities include:

- Deleting obsolete desktops
- Deleting unused file drawers
- Deleting old versions of files
- Moving file drawers to a different volume with more available disk space

Regularly monitor the desktops stored on the File Service. Desktops consume a large amount of disk space.

Before you delete any desktops, file drawers, or files, be sure to inform the owners to ensure that they are not needed. You may want to notify the owners so they can delete their own obsolete files, then follow up later to ensure that the files were deleted.

If your server is also running PC File Service, before you delete or move file drawers that are shared by PC File Service users, you must first perform the "Removing network resources and deleting directories" procedure at the PC File Service. Also, after you move a file drawer, you must perform the "Creating directories and adding network resources" procedure. These procedures are in the PC File Service chapter of the *Services Maintenance Guide*. Also, see "Planning for maintenance" in the PC File Service chapter later in this book for more information.

Related Procedures: Deleting file drawers, Recovering file drawer space by deleting old file versions, Recovering File Service disk space by deleting obsolete desktops, Recovering File Service disk space by moving file drawers

Monitoring File Service activity

Monitor File Service activity and statistics regularly. The File Service requires more time to respond to users' requests when activity increases.

You display File Service activity to check the current remote connections to the File Service. For each connection, the listing includes:

- The user who initiated the connection
- The volume with which the connection is established
- The time the connection was initiated
- The time of the last activity

You display File Service statistics to check current and cumulative activity. Statistics include:

- The total number of connections to the File Service
- The maximum, minimum, and average length of connections
- The number of list operations
- The number of file accesses (open operations)
- The number of files deleted
- The number of files stored
- The number of files retrieved

The File Service compiles statistics since the last reset or the last server reboot. The statistics are cumulative for all the volumes that the File Service manages. Statistics are not available for individual volumes.

Reset the counters that track statistics regularly. Resetting the counters to 0 lets you compare File Service activity from day to day or from week to week.

Related Procedure: Monitoring File Service activity

Validating desktops

The File Service has an optional desktop validation feature that is enabled by default. This feature maintains each desktop stored in the Desktops directory and automatically deletes non-desktop objects.

The desktop validation feature informs you of possible damage to a desktop so you can restore it from the most recent backup data. You cannot restore a desktop that was never backed up. See the "Restoring a container" procedure in the File Service chapter of the *Backup and Restore Guide* for information on restoring damaged desktops.

Related Procedure: Validating desktops

8. PC File Service

This chapter helps you prepare for installation, setup, and maintenance of the PC File Service (PCFS). The information supports the procedures you perform from an 8000 or 8090 server.

Service description

The PC File Service expands the capabilities of a server by providing shared filing service to personal computers (PCs) running XC20 version 1.2 software, and workstations using standard XNS protocols. The "personal computer" can be any of the following:

- Xerox 6060 series workstation
- IBM Personal Computer
- IBM PC-compatible personal computer

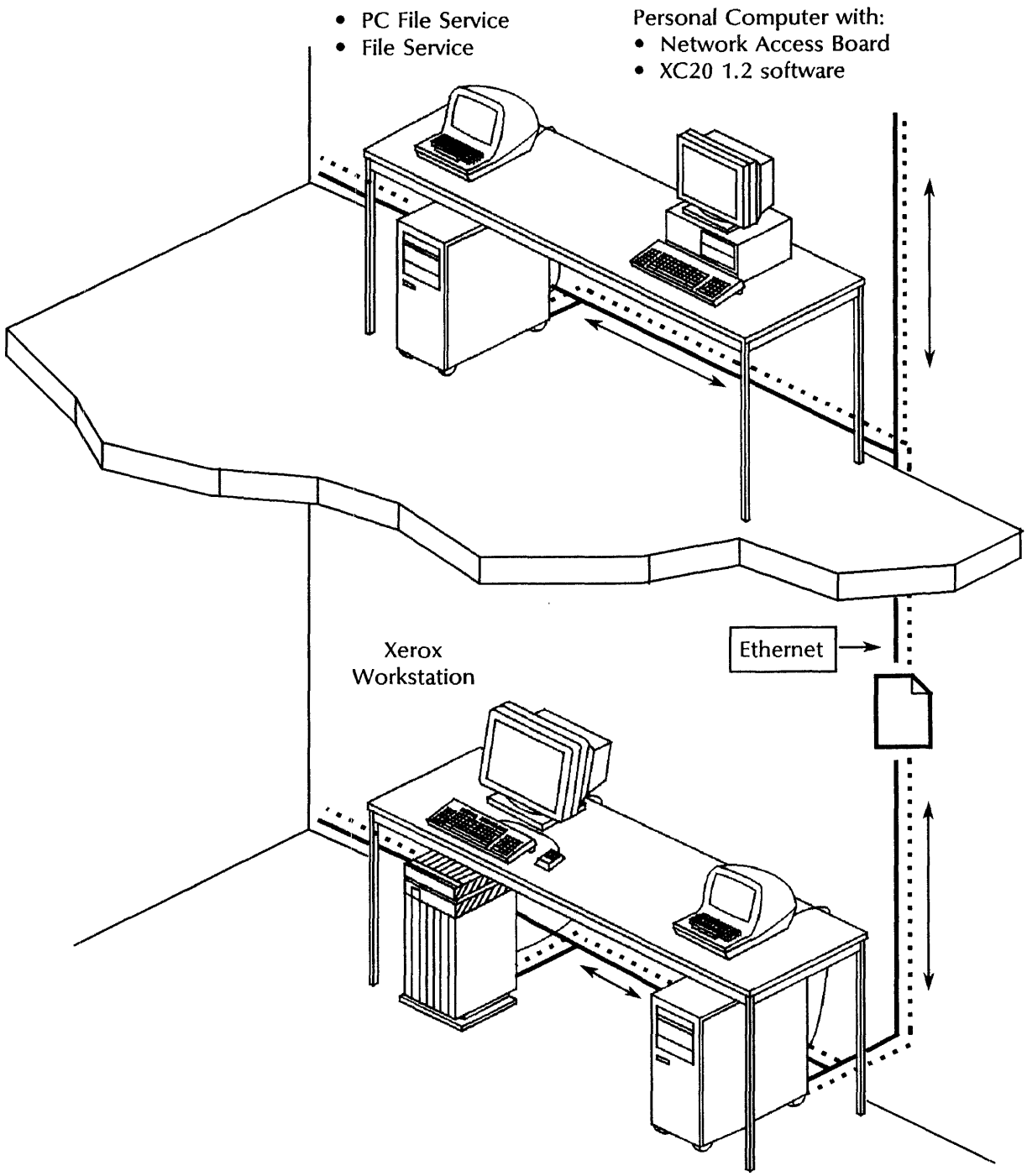
The PC File Service acts as a translator between PC clients (networked PC users) and the server. The PC File Service enables PC clients to access the server to store and retrieve files, and to share files with other network users. When you install the PC File Service on the same server as the File Service, a networked Xerox client may also access the same files that PC clients use.

Before a PC client can access files on the network, the System Administrator must previously offer the files as a resource to networked PC clients. See "Planning for setup" later in this chapter.

The PC File Service provides backup and restore capabilities to preserve PC client data from loss. These backup and restore procedures are the same procedures used to back up and restore the File Service. See the File Service chapter in the *Backup and Restore Guide* for more information.

Figure 8-1 shows the file-sharing capability between networked PC and Xerox clients.

Figure 8-1. **Networked PC and Xerox clients exchanging documents.**



How the software works

When the PC File Service is running on the same server as the File Service, Xerox and PC clients may share files. Files in the PC File Service are arranged hierarchically by directory, subdirectory, and files.

The term directory is used throughout this chapter to represent file drawers or folders.

PC clients can access only the contents of directories and subdirectories that have been made available as a resource to the network. A unique network name assigned to the resource can be either a pathname (directory name, subdirectory name and filename) or short name for the pathname. PC clients access files by specifying the network name to a file.

PC clients connect to the PC File Service and access files the same way they normally connect to and access files on a PC running XC20 software configured as a server. The PC File Service interacts with XC20 clients as if it is an XC20 server. It stores, lists and retrieves files as well as PC File Service commands. See the XNS/PC documentation for more information.

Filename translation

Xerox clients can create filenames containing up to 100 characters, as well as multiple versions of files containing the same name. PC clients are limited to creating filenames with up to eight characters (plus an optional three-character extension), and cannot have different versions of the same file.

The PC File Service performs filename translation only to convert Xerox filenames to MS-DOS syntax. This conversion enables PC clients to list and access files that have valid Xerox names. The name of the Xerox file is not changed, but if the file is copied, then its copy receives the translated version of the Xerox filename.

Filename translation occurs when:

- The filename is longer than eight valid ASCIIZ characters (ASCIIZ characters are a subset of the ASCII character set)
- The filename contains non-ASCIIZ characters
- The directory supports different versions of the same file (filenames are not unique)

When a PC client specifies an existing filename, the PC File Service looks for the filename. If it does not find the filename, the PC File Service translates all the filenames in the specified directory and selects the first file that matches the translated name.

The first eight valid ASCIIZ characters of the Xerox filename are converted into PC (MS-DOS) filename syntax. Valid ASCIIZ characters are:

- A-Z 0-9 !@#$%^&()_-{}~``'

Non-valid ASCIIZ characters include spaces and control characters, as well as"*+,./:;<=>?[\]|

If fewer than eight valid ASCIIZ characters are in a Xerox filename, then the PC File Service uses all the characters, capitalizing all lowercase letters. If a filename has no valid ASCIIZ characters, the filename will not be translated and cannot be accessed by the PC client.

If more than eight valid ASCIIZ characters are in a Xerox filename, the PC File Service adds together the ASCII numerical values of any remaining valid ASCIIZ characters and divides by the total number of valid ASCIIZ characters (52). The remainder is used to determine the first character of the three-character extension. The last two characters of the extension are the last two digits of the file version number (01-99).

For example, the filename Gem;SystemCo in Xerox syntax translates into GEMSYSTE.601 in PC filename syntax, where 01 is the version number.

The PC File Service applies filename translation to the names of directories as well as names of files. For pathnames, filename translation might occur on each directory name in the pathname and also on the name of the actual file, but the entire pathname is not translated into an eleven character MS-DOS name. The PC File Service locates a file when given a pathname where one or more of the directory names has been translated. If volumes on the PC File Service have names that contain non-ASCIIZ characters, then the volume appears to have no name when the PC client lists files on that volume.

Many Xerox multinational characters are not valid ASCIIZ characters and are ignored in the filename translation. If a filename does not contain any ASCIIZ characters, the filname will not be translated. In this case, PC clients cannot list or access the file. Therefore, Xerox clients should use only valid ASCIIZ characters in filenames.

Security

The PC File Service provides access controls you can place on its directories to protect information. For example, you may permit a client to copy files and to read their contents, but not to add or delete files.

Xerox clients are subject to File Service access control. PC clients are subject to the password and access control you specify when you offer the directory as a resource available to PC clients. PC File Service access controls are valid only for PC clients, and File Service access controls are valid only for Xerox clients.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the PC File Service Worksheet located at the end of this chapter.
- Installing the PC File Service software as described in the Server Software Installation chapter of the *Services Installation and Setup Guide*.
- Setting up directories for use by PC clients as described in the PC File Service chapter of the *Services Installation and Setup Guide*.
  - Informing PC clients of the service name and network name for available network resources.
- Maintaining your PC File Service as described in the PC File Service chapter of the *Services Maintenance Guide*. Perform maintenance procedures as needed to keep your PC File Service operating at an optimum level.
  - Monitoring network sessions and available volume space.
- Performing backup procedures regularly, and setting incremental backup parameters as described in the File Service chapter of the *Backup and Restore Guide*.
- Upgrading hardware and software as required.
- Notifying users of any change or disruption in the service.
- Troubleshooting the service as described in *Basic Network Troubleshooting*.

You can perform most PC File Service procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter in the *Services Installation and Setup Guide* contains the procedures for installing your PC File Service software. This section explains the hardware, software, and other requirements to help you prepare for installation.

Hardware requirements

The PC File Service operates on an 8090 server with a single 20, 40, or 80 Mb internal hard disk, or with up to seven 310 Mb external disk drives.

The PC File Service operates on an 8000 server with a single 10, 29, or 42 Mb hard disk, or with any combination of up to four 80 or 300 Mb removable disk drives, or 300 Mb fixed disk drives.

Software requirements

The PC File Service requires Services System Software and these PC File Service program files:

- PCFileSDF.bcd
- PCFileOpsConfig.bcd
- PCFileService.messages
- PCFileServiceConfig.bcd
- PCProtocolConfig.bcd
- FSCommonConfig.bcd
- FSCommon.messages

If you are using an 8090 or 8000 server, use services version 10.4.

The PC File Service software uses approximately 365 pages of the system file area on the PC File Service volume.

PC requirements

Personal computers must have installed XC20 version 1.2 network software and a Network Access Board connected to an Ethernet cable. The PC File Service is compatible with XC24, which is the same as XC20 on Ethernet. Additionally, the XC20 network of personal computers and the PC File Service must both be connected to the same local area network (LAN). See the XNS/PC documentation for more information.

Dependencies and limitations

The PC File Service depends on the Clearinghouse Service to verify the user name and access rights of the System Administrator.

When the PC File Service and the File Service are running on the same server, Xerox and PC clients can share files and directories.

It is recommended that the File Service be installed first, if the PC File Service and File Service are being installed on the same server. See the File Service chapter in this book.

If the PC File Service is backed up to a remote File Service, then the File Service must be installed on the remote server. Backup operations to a local backup volume do not require the File Service to be coresident with the PC File Service.

In addition, a remote session limit of 15 is recommended for the File Service and the PC File Service, if both are installed on the same server.

PC File Service Worksheet

Use the PC File Service Worksheet to record server-related and service-related information that helps you perform setup procedures. For your convenience, the PC File Service Worksheet is at the end of this chapter.

Make a copy of the PC File Service Worksheet and fill it out as directed. Record the original worksheet for future copying, store the completed worksheet in your *Activities Guide*.

Using the worksheet

Before you install software on a server and set up you PC File Service, complete the PC File Service Worksheet. It is important that you fill out the worksheet accurately and update it whenever changes occur. The completed worksheet saves you time as you perform your procedural duties. It also serves as an information source for new System Administrators unfamiliar with your network configuration.

Filling out the worksheet

As you read the rest of this chapter, you are directed to make entries on the PC File Service worksheet. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and services installed on the server. Copy this information from the Services Installation Worksheet. If you need more information, see the Services System Software chapter in this book. Use sections ② and ③ to record the directory structure and network resources.

Planning for setup

After you install the PC File Service, you initialize the primary volume and any secondary volumes that have not already been initialized.

You then create a simple directory structure for the PC File Service volume. You add the names of these directories to the list of resources available to PC clients, specifying passwords and access rights for each directory.

See the PC File Service chapter in the *Services Installation and Setup Guide* for complete setup procedures.

Initialize volumes

The collection of files contained on a fixed disk drive or removable disk drive is known as a volume. Because a removable disk can be used on different servers, the location of a directory is tied to a volume and not to a server. You initialize each volume to make it available for use by the PC File Service, beginning with the primary volume.

A single-drive server has only a primary volume. A multiple-drive server has a drive for the primary volume, as well as secondary drives that contain secondary volumes.

Primary volume

During initialization of the primary volume, you determine a service name for the PC File Service. In addition, the name of the primary volume defaults to a pre-determined name. If the PC File Service is installed on a server without a coresident File Service, the PC File Service primary volume name defaults to the name PRIMARY.

If the PC File Service and File Service are coresident on the server, the name for the PC File Service primary volume defaults to the File Service primary volume name. You can change volume names; see the Services System Software chapter in the *Services Maintenance Guide*.

After you initialize the PC File Service primary volume, you then inform PC clients of the service name of the PC File Service.

Related procedure: Initializing the primary volume

Secondary volumes

Initializing secondary volumes for the PC File Service depends on whether the PC File Service is coresident with a File Service, and if secondary volumes have already been initialized:

- If the PC File Service is installed on a server without a coresident File Service, initialize the secondary volumes by naming each volume dedicated to PC File Service use.
- If the PC File Service and File Service are coresident on the same server and secondary volumes have not been initialized

through the File Service, initialize the secondary volumes by naming each volume dedicated to PC File Service use.

- If the PC File Service and File Service are coresident on the same server and secondary volumes have been initialized through the File Service, do not initialize the secondary volumes a second time. The initialization process deletes all data on the volume.

You determine a local name for each secondary volume that must be initialized. The domain and organization names default to that of the server.

Related procedure: Initializing secondary volumes

Filling out the worksheet

Make a copy of the worksheet for the primary volume and each secondary volume you have to initialize.

① Record the name of your server, its processor number, network number, and serial number (see the Services System Software chapter in this book).

Record the domain and organization of the server, its physical location, and its hardware (including the type of server and any peripherals attached to it).

Record the service name for the PC File Service. You can use up to 15 valid ASCIIZ characters (A-Z 0-9 !@#$%^&()__-{}~`') for the PC File Service name. Do not use commas, parentheses, asterisks, or pound signs in a service name.

Note whether coresident services are activated, the number of disk pages they require, and the names and descriptions.

② Record the primary volume name (if you want to change it from the default), or the secondary volume name. You can use up to 40 characters. Do not use commas, parentheses, asterisks, or pound signs in a volume name.

Determining directory structure

Files in the PC File Service are organized hierarchically. A root directory (volume) at the top can contain major directories (file drawers) and several subdirectories (folders), each of which can contain additional levels of subdirectories, as well as record files, spreadsheets, and so on. PC clients access a file by specifying the network name (pathname or short name) for the directory when establishing the remote connection, and then specifying the file name as they would for local PC files.

You can assign a short name you want PC clients to use to access the directory, instead of the complete pathname for the directory. A short name can be from 1 to 8 characters in length.

You have as many levels of subdirectories, and as many subdirectories at each level, as you want. However, the file drawer size and the File Service storage capacity is limited; see the File Service chapter in this book for more information.

You need to plan the directory structure of each volume (root directory) you designate for use by the PC File Service. Determine how many directories and files will be stored on the

volume, who needs access to the files, and the frequency of that access.

If the PC File Service uses only one volume, you can add directories as needed. If the PC File Service uses more than one volume, plan the directory structure based on the number of directories and the frequency of use for each directory.

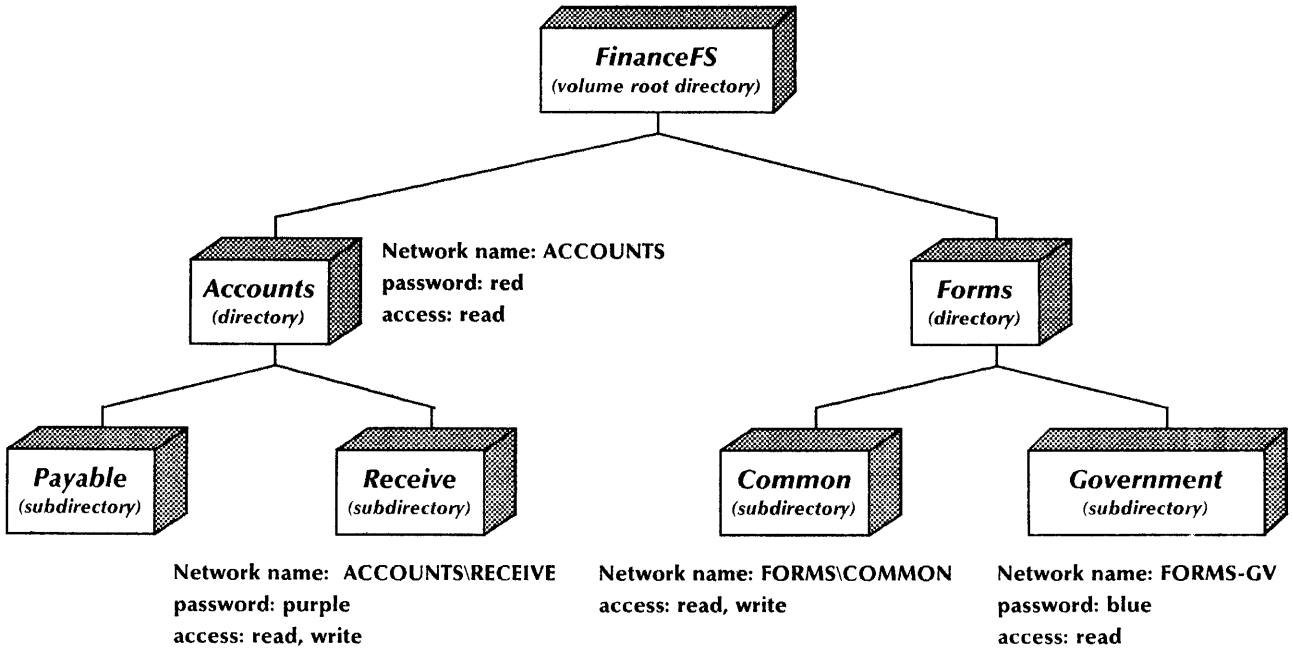
For example, you can group directories used more frequently on one volume and those used less frequently on another volume. In this way, you can configure different backup requirements for each volume. If you prefer a similar number of sessions for each volume, you can choose to include both frequently used and less frequently used directories on a volume.

To create a directory, you specify the volume and then the name for the new directory. You repeat this procedure for each directory you want to create. You use the same procedure to structure subdirectories within the directories as free disk space permits.

Once you decide on the basic directory structure, the rest of the directory structure (including other subdirectories as well as files) can be created by PC clients.

Figure 8–2 shows an example of the hierarchical directory structure for the PC File Service. (You enter the network name and password, as well as the required access rights, when you make the directory available to the network.)

Figure 8-2. **Sample hierarchical directory structure**



The *Accounts, Receive, Common,* and *Government* directories are resources that have been offered to the network. The *Receive* subdirectory was offered separately to allow greater access than connecting to the *Accounts* directory. The *Payable* subdirectory is connected to the *Accounts* directory and has the same password and access rights as the *Accounts* directory.

The *Forms* directory cannot be accessed; only the *Common* and *Government* directories within the *Forms* directory can be accessed. Note that the *Government* subdirectory is assigned a short name as the network name because the name is longer than eight characters.

Related procedure: Creating directories for PC clients

Filling out the worksheet

Section ② of the worksheet is helpful only when setting up the directory structure for the first time. Once the basic directory structure is in place, PC clients can create subdirectories and files as needed.

The worksheet accommodates a simple structure with two directories and four subdirectories. If your directory structure is more complex, use the worksheet as a model to create your own structure.

② Record the local name of the PC File Service volume. The domain and organization default to that of the server. If the File Service runs on the same server as the PC File Service, the domain name for the PC File Service must exist, and the local name must be unique within the domain.

Record the name of the directory(s) and subdirectories. It is recommended that you use no more than eight ASCIIZ characters (A-Z 0-9 !@#$%^&()_-{}~`') for the name, and an optional three-character extension.

Making resources available to networked clients

PC clients can access only those resources (directories, subdirectories, and files) you make available. You determine access rights and an optional password for a resource to maintain security, as well as a network name. Passwords can be from 1 to 8 characters in length.

NOTE

If you enter a password for a resource, there is no way to determine the password if it is forgotten. You must then enter a new password for that resource.

The subdirectories and files created under a directory have the same access rights and optional password as the directory, unless you specify different access rights and/or password for the subdirectories.

If you determine that a subdirectory has the same access rights and password as the directory, only the directory from which the subdirectory and files descend needs to be offered as a resource to the network. If you determine different access rights and/or password for the subdirectory, you must offer the subdirectory as a resource to the network.

In addition to access rights and passwords, you also determine network names for resources. The network name is either a pathname or a short name, and is used by PC clients to access a resource.

NOTE

To permit a resource to be accessed by either its pathname or its short name, you must add the resource to the network twice; once by the short name, and once by the pathname.

If you make a Xerox directory available to PC clients, and at least one of the directories in its pathname must be translated to enable a PC client to specify it, then you must assign a short name to offer the resource to the network. In addition, you can optionally assign a short name even if none of the directories in the pathname require name translation. In both instances, PC clients enter only the short name to access the directory.

See Figure 8-2 for examples of passwords, short names, and access rights.

After you make the directories available to the network, inform PC clients of the new resources, including the network name, access rights, and password.

Related procedure: Adding network resources

Filling out the worksheet

The worksheet accommodates up to 12 resources that you want to make available to the network. Make additional copies of the worksheet to accomodate more than 12 resources.

③ Record the name of the volume on which the resources are located. This name should be the same volume name entered in section ② of the worksheet.

Record the pathname for each directory/subdirectory being offered as a resource. It is recommended that you use up to eight valid ASCIIZ characters (A-Z 0-9 !@#$%^&()_-{}~`') in the directory/subdirectory name. Include a backslash between directory levels, as in Accounts\Receive.

Record the network name, which can be the pathname (if none of the directory/subdirectory names in the pathname is longer than eight characters), or an optional short name for each directory/subdirectory being offered as a resource. (A short name can be from 1 to 8 characters in length.) If the pathname is not usable as a network name, you must create a short name for the network name.

Record the number identifying the access rights for each directory/subdirectory being offered as a reaource.

1 Read - Allows the remote client to read the contents of any file in the network resource.

2 Write - Allows the remote client to change the contents of any file in the network resource.

3 Read, Write - Allows the remote client to read and change the contents of any file in the network resource.

4 Write, Create - Allows the remote client to change, create, delete, and rename files in the network resource.

5 Read, Write, Create - Allows the remote client to read, change, create, delete, and rename files in the network resource.

Planning for maintenance

After you install and set up the PC File Service, you are responsible for maintaining it. You perform maintenance as needed; there are no scheduled duties.

Use the information in "Planning for setup" in conjunction with the information here to further your understanding of PC File Service maintenance. See the PC File Service chapter in the *Services Maintenance Guide* for complete maintenance procedures.

Updating the worksheet

Whenever you make a change in the availability of network resources, update the PC File Service Worksheet. In this way, you always have a record of the resources available, including the network name and access rights, for each resource.

Maintaining the directory structure

You may need to create new directories or delete existing directories used by PC clients. You create new directories using the commands to add and delete existing directories (and associated files).

Check with PC clients to make sure files are not being used before you delete a directory. In addition, before you delete a directory, remove it from the list of available resources (if it was offered as a network resource); see "Maintaining the list of network resources," next.

If you do not remove a deleted directory from the list of available resources, an error occurs each time a PC client tries to access the directory or any files within it.

Related procedure: Creating directories and adding network resources, Listing directories and network resources

Maintain the list of network resources

When you decide to allow PC clients access to a directory and all it contains, you must add the directory to the list of network resources. See "Planning for setup" in this chapter for information on directory structures.

You use the command to add a net share to make a resource immediately available and to record its name on the appropriate volume. You then must inform PC clients of the availability of the new resource, and update the worksheet.

You can remove a network resource from the list of available resources. You must then notify all PC clients of the change, and update the worksheet.

Any user can display the list of available network resources. For each resource, the list shows volume and pathname, network name, access rights, and current users.

CAUTION: It is important to update the PC File Service worksheet when there is a change to the list of resources offered on the network. In some instances, it is not possible to acquire a complete list of available network resources, except as documented on the worksheet.

Related procedures: Creating directories and adding network resources, Listing directories and network resources, Removing network resources and deleting directories

Changing resource passwords and access rights

To enhance security, you should regularly change the password associated with network resources. You can also change the access rights allowed for a network resource. You use the command to change network resources to change passwords or access rights.

Changes to passwords or access rights do not affect clients currently connected to the resource. If you want the changes to take effect immediately, remove the resource and then add it to the network with the new password and access rights.

Related procedure: Changing network resources

Monitor activities and network sessions

Routinely monitor the PC File Service using the command to show activity. When the number of simultaneous sessions increases, the performance for each network client begins to degrade. You can improve performance for network clients by:

- Reducing the number of sessions allowed by the PC File Service
- Moving active directories to another PC File Service volume on another server (see "Monitoring available volume space," next).

You can display and change the current remote session limit using the Services System Software **Show Profile** and **Change Profile** commands. After you change the remote session limit, you stop and start the PC File Service so the new limit can take effect.

The maximum limit is 20 simultaneous remote sessions. It is recommended that you maintain a limit of less than 15 if the PC File Service and File Service are coresident on the server.

You can list the statistics compiled since the last reset or the last reboot of the server, whichever is later, as well as reset the counters that keep track of statistics. Reset the counters weekly so you can compare activity from week to week. You can use the Remote System Administration Make Document or Make Screen option to copy the displayed statistics for your records.

Related procedure: Showing activity and statistics

Monitor available volume space

Regularly check the number of available pages on each volume for the PC File Service. Use the Services System Software **List Volumes** command to display the number of pages used, the

number of available pages, and the percentage of pages used. The file drawer size and the File Service storage capacity is limited; see the File Service chapter in this book for more information.

If the PC File Service regularly becomes more than 90 percent full on any of its volumes, consider expansion to an additional or larger capacity server. A PC File Service that is too full cannot hold additional directories or perform necessary backup operations.

CAUTION: A volume should NEVER exceed 98 percent full. The PC File Service performance degrades and may become inoperative.

When a volume becomes full, you can make space available by moving directories to another volume. You use the **Copy Container** command to copy the directory (and associated files) from the volume to a cartridge tape or floppy disk, and the **Restore Container** command to restore the directory from the tape or floppy disk to the new volume. (See the *Backup and Restore Guide* for more information.)

To move directories from one volume to another, first remove the directory from the list of available network resources, then move the directory to the new volume. Next, add the directory to the new volume and inform PC clients of the change you made.

When moving entire volumes by removable disk packs, no change to the list of available network resouces is necessary. If the disk pack is moved to a different PC File Service, inform PC clients of the new service name.

Related procedure: Moving directories to another volume

Monitoring open files

You can view the files currently accessed by PC clients using the command to list open files. This command ignores files that are open and available only to Xerox clients.

A file left open but not in use cannot be accessed. The command to close the file applies only to files available to PC clients. Check with PC clients to make sure the file is not being used before using the command to close the file. If the file is closed while a PC user is copying a file, only a portion of the file is copied.

Related procedure: Listing and closing open files

Displaying a translated filename

A PC client may want to determine the translated name of a file or directory. Any logged-on user can display the translated name of a file or directory.

Related procedure: Showing name translation

Opening and closing volumes

Opening and closing volumes, which are Services System Software operations, also affect the PC File Service.

If the PC File Service and File Service are coresident, then the volumes must be open (and network resources made available) for PC File Service volumes to be accessible to remote clients. For File Service volumes to be accessible to remote clients, the volumes must be online.

The term online refers to a File Service state which is possible to activate only if the volumes are open.

When you want to open a volume containing resources that the PC File Service offers to the network, first stop the service then open the volume and restart the PC File Service. In this way, the PC File Service can make available network resources on the volume.

When you want to close a volume to move a removable disk pack on an 8000 server or use the **Copy Volume** command, first stop the PC File Service. Stopping the PC File Service makes all network resources unavailable to the network so secondary volumes can be closed. Then close the volume, and restart the service. When you restart the PC File Service, all network resources on open volumes become available.

The PC File Service name is not displayed after rebooting or opening a volume. Use the **List Services** or **Show Profile** commands to display the service name after the service is running.

Epunging the PC File Service

You expunge the PC File Service from the server following the directions to expunge a service in the Services System Software chapter in the *Services Maintenance Guide*. Before expunging the service, make sure you delete the directories using the PC File Service procedure, "Removing network resources and deleting directories" in the *Services Maintenance Guide*.

9. Librarian Service

This chapter helps you prepare for installation, setup, and maintenance of the Librarian Service (LS). The information supports the procedures you perform from an 8000 or an 8090 server.

Service description

The Librarian Service manages various types of information for applications such as the ViewPoint Shared Books feature. Shared Books uses both the Librarian Service and the File Service to provide multi-part documents that can be shared by many users:

- The File Service stores the documents of a shared book in a file drawer and controls user access to the drawer.
- Shared Books uses the Librarian Service to help provide an additional level of access to shared book contents. It allows only one user at a time to access and change a document.

How the software works

The Librarian Service manages and holds information for features such as Shared Books. The libject (or library object) is the basic unit of information. Applications like Shared Books manipulate libjects and store information within them.

For example, libjects are used as flags or markers for each shared book and shared book entry. When users lock or unlock shared book entries, the Shared Books application is actually locking or unlocking the libject flags.

The workstation user fills out the Shared Book property sheet to create a shared book. The user designates the name of the shared book, the fully qualified name of a Librarian Service database that will be used to monitor access to the book, and the fully qualified name of the File Service file drawer and folders that will store the shared book.

The File Service provides a file drawer to store the shared book and a file drawer to store the backup copy of the Librarian Service database.

Shared Books uses the Librarian Service to monitor its shared data: the shared book entries and the additional information Shared Books maintains about them.

The database files

A Librarian Service database contains three files:

- The Records file, which contains the libjects
- The HashTable file, which contains an index of the records file
- The Log file, which records the transactions made since the last database backup took place

A Librarian Service can maintain more than one database. Each database has its own read and write access lists.

The database parameters

The database parameters include the authentication level required to open a session, the lists of readers and writers, and the pathname to the remote backup location.

The libjects

Librarian Service applications may query, store information in, check out (lock), or check in (unlock) a libject. However, the libject is always in the database once it has been created, unless you explicitly delete it. If a shared book entry is currently checked out by another user, and you attempt to access the entry, the message "Entry locked" appears. The current user must unlock the shared book entry libject to make it available to other users. Unlocking the entry allows Shared Books to check in that entry's libject.

Workstation users use the Shared Books property sheet to initially specify a Librarian Service database for Shared Books to use in all operations. See the VP Series Reference and Procedures Library for more information about shared books.

If the user is unable to return the libject, the System Administrator can use the **Checkin Libject** command to return it to the database. Users should not attempt to access the database at this time. This is the only command available to you that lets you directly affect a libject.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the Librarian Service Worksheet located at the end of this chapter.
- Installing the LS software as described in the Services System Software chapter of the *Services Installation and Setup Guide*.
- Setting up the LS as described in the Librarian Service chapter of the *Services Installation and Setup Guide*.
- Maintaining the LS as described in the Librarian Service chapter of the *Services Maintenance Guide*.
  - Upgrading hardware and software as required
  - Notifying users of any change or disruption in the service
- Backing up the LS as described in the Librarian Service chapter of the *Backup and Restore Guide*.
- Troubleshooting the service as described in *Basic Network Troubleshooting*.

You can perform most Librarian Service procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter of the *Services Installation and Setup Guide* contains the procedures for installing your LS software. This section explains the hardware, software, and other requirements of the Librarian Service to help you prepare for installation.

Hardware requirements

The Librarian Service can run on an 8000 or an 8090 server.

Software requirements

The LS requires Services System Software and these Librarian Service program files:

- LibrarianSDF.bcd
- LibrarianService.bcd
- LibrarianService.messages

Allow 120 disk pages for the Librarian Service. In addition, you should initially allow 92 pages for each new database. If you expect the database to grow beyond 20 libjects, add least one page for each additional libject.

Dependencies and limitations

The Librarian Service has these dependencies and limitations:

- The Librarian Service needs access to these services to perform its tasks:
  - The File Service, which contains the file drawer used to store the backup copy of the database files
  - The Clearinghouse Service, which verifies access control (for individuals or groups)
- Do not install the Librarian Service on the same server as the File Service that is storing the backup copy of the LS database files.
- The Librarian Service places a moderately heavy load on the server when communicating with network clients. For optimum results, do not install the LS on the same server with active services such as the Clearinghouse Service, Mail Service, or Print Service.

Librarian Service Worksheet

Use the Librarian Service Worksheet to record server-related and service-related information. The worksheet is at the end of this chapter.

Fill out a separate copy of the worksheet for each Librarian Service for which you have System Administrator responsibility. Retain the original for future use, and store the completed worksheet in your *Activities Guide*.

Using the worksheet

Before you install the software and set up your Librarian Service, complete the worksheet. It is important that you fill out the worksheet accurately, and update it whenever changes occur.

The completed worksheet saves you time as you perform the setup and maintenance procedures. It also serves as an information source for new System Administrators unfamiliar with your configuration.

Filling out the worksheet

As you read the rest of this chapter, you are directed to make entries on the Librarian Service Worksheet. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and the services installed on that server. Copy this information from the Services Installation Worksheet you filled out while reading the Services System Software chapter of this book.

Use section ② to describe the Librarian Service databases.

Database information

When you create an LS database, you name it and describe its parameters.

Related procedures: Creating the Librarian Service database, Setting the database parameters

Filling out the worksheet

② **Name** - Record the name of the database.

Authentication level - Circle simple or strong to identify the authentication level required to open a session. Strong is the default authentication level. It's best to use strong as it does not allow passwords to appear on the screen.

Readers - Record the name of the individual or group you want to have read access; use the default wildcard symbol (*) to give access to all users.

Writers - Record the name of the individual or group you want to have write access; use the default wildcard symbol (*) to give access to all users.

Backup path - Record the pathname for the remote backup location. If you leave this parameter empty, the database will not be backed up.

Number of backup versions - Record the number of backup copies you want to store (1 to 100).

See the Librarian Service chapter of the *Backup and Restore Guide* for more information on backup.

Planning for maintenance

After you install and set up the Librarian Service, you are responsible for maintaining it. You perform maintenance as needed; there are no scheduled duties.

This section provides guidelines for deleting or moving a database and changing database parameters.

See the Librarian Service chapter of the *Services Maintenance Guide* for the complete maintenance procedures.

Deleting or moving a database

Deleting or moving a database requires stopping the service. Make sure you notify all users that the LS will be temporarily interrupted, and verify that all users are not accessing the database. If you stop or back up the Librarian Service database while users are using Shared Books, the shared book may be damaged.

To delete a database, you need to:

- Delete the database from the Librarian Service
- Remove the database name registration from the Clearinghouse
- Delete any backup versions of the database

To move a database, you back up the Librarian Service databases to create current copies at the remote location. You then destroy and unregister the database you want to move. Recover the database at the new server location by specifying the original pathname.

Related procedures: Deleting a database, Setting the database parameters, Moving a database

Changing database parameters

You cannot change the name of a database after you create it. You can change the authentication level, the read and write access lists, the database backup path, and the number of remote backup versions to be kept.

10. External Communication Service

This chapter helps you prepare for installation, setup, and maintenance of the External Communication Service (ECS). This information supports the procedures you perform from an 8000 or 8090 server.

Service description

The External Communication Service supports information exchange between Xerox Network System devices and non-Xerox devices. Its main role is to initiate and maintain emulation sessions between workstations and remote host computers, employing these terminal emulation options:

- Asynchronous terminal emulation and dial-in
  - Interaction with the Interactive Terminal Service
  - Use of a remote server
- IBM 3270 BSC (Binary Synchronous Communication) terminal emulation
- IBM 3270 SNA (System Network Architecture) terminal emulation

The ECS also manages Communication Interface Unit ports for the Internetwork Routing Service, which interconnects all services and workstations on the internetwork and provides access to all hosts by eligible workstations. See the Internetwork Routing Service chapter in this book for details about its communication options.

With emulation software, Xerox Network System workstations can emulate these terminals: the IBM 3278-2, -3, -4, and -5 model terminals, the DEC VT100, and the standard TTY terminal.

The External Communication Service also manages RS232C ports, the Multiport Option Kit, and the 873 Communication Interface Unit.

How the software works

To communicate with remote host computers, the External Communication Service:

- Communicates with the host in the host's native protocol
- Communicates with the networked workstation in XNS protocols
- Provides the shared physical communication resources to connect the host to all networked workstations

When a workstation user requests an emulation session with a host computer, the workstation uses information from the Clearinghouse to locate an External Communication Service that

supports connections with that particular host. A cluster controller enables multiple workstations to share a single phone line. A workstation can use either the local External Communication Service or any External Communication Service on the internetwork. The workstation then initiates a connection with the External Communication Service.

The External Communication Service initiates a session with the remote host and performs protocol conversions between the Xerox Network System and the remote host. The workstation presents a user interface similar or identical to that of the emulated terminal. Emulation sessions are available as long as an External Communication Service supporting the host exists somewhere on the internetwork.

Terminal emulation gives a more flexible access to remote computers than terminals directly connected to hosts or cluster controllers. As with directly connected terminals, the total number of terminal emulation sessions is limited to eight per emulated cluster controller, or the number of TTY or VT100 ports available on a remote host. However, the number of sessions per user is limited only by the number of windows allowed by the workstation software.

Multi-function workstations can handle multiple concurrent emulation sessions. They can receive information from several hosts, place it in a document, format, mail and file it. Users of TTY terminals or personal computers can access the Mail Service and File Service on the network through the External Communication Service Greeter and the Interactive Terminal Service.

The External Communication Service also supports dial-in users. A user on a non-networked personal computer, DEC VT100, or TTY-compatible terminal can access the network by a dial-up connection to the External Communication Service. This connection is provided by the Interactive Terminal Service.

Asynchronous communication protocol

Many time-sharing hosts and public data networks support some type of asynchronous communication protocol, including the TTY and VT100 protocols. The asynchronous communication protocol supports terminal and emulation sessions between workstations and non-networked hosts. It also supports access to the File Service, Print Service, and Mail Service from TTY-compatible terminals and personal computers.

The interaction between the External Communication Service and the host is governed by the asynchronous ASCII conventions.

How it works

Asynchronous terminal emulation uses two separate features: the Asynchronous Communication Protocol option, and emulation software.

Protocol The Asynchronous Communication Protocol Option enables the External Communication Service to connect the workstation and the host. The Ethernet connects the workstation to an External Communication Service, and then an auto-dialed telephone line provides the connection to the host. The External Communication Service provides communication compatibility

through bidirectional protocol translation between the host and workstation.

Software

The emulation software found on the workstation creates a user interface similar to that on an actual DEC VT100 or TTY-compatible terminal. Incoming information is displayed in ASCII format.

When you configure a port for asynchronous communication, you assign to it the Asynchronous Communication Protocol Option, the modem, and phone line connections to hosts, making them available to any requesting workstation. A small number of modems and phone lines can serve multiple workstations.

The Greeter

When you enable the Asynchronous Communication Protocol Option and designate a port for dial-in access, the External Communication Service provides a Greeter function. Users of dumb terminals and PCs with dumb terminal emulation software need only a modem and phone line to connect to the ECS.

When the user dials in, the Greeter displays for the user a menu of types of remote hosts for dial-in device connection, including:

- One or more Interactive Terminal Services, for mailing, printing and filing
- One or more servers for remote System Administration

The user need not remember the name of an Interactive Terminal Service or server; the Greeter lists the possible candidates within a Clearinghouse domain. After the user designates a service or server, the Greeter establishes the virtual terminal circuit and becomes invisible until the end of the session.

You can configure the Greeter so that it is invisible to the user, and automatically connects each user to an Interactive Terminal Service that you specify. See "Planning for setup" later in this chapter for more information.

3270 BSC and SDLC/SNA communication protocols

The 3270 bisynchronous communication protocols enable users of workstations configured with IBM 3270 emulation software to initiate IBM 3270 BSC or SDLC/SNA emulation sessions. The 3270 communication protocols enable you to use the application, development, and database tools supported by IBM host computers.

The External Communication Service emulates a 3276-2 cluster controller when using BSC protocols, or a 3276-12 cluster controller for SDLC/SNA protocols. The External Communication Service translates the IBM communication protocols into the Xerox Network System protocols, and vice versa. In BSC communications, the physical link to the host is a dedicated leased line. In SDLC/SNA communications, a dedicated or switched (manual or auto-dial) line provides the physical link.

The External Communication Service supports up to eight concurrent interactive terminal sessions with an IBM host, just like an IBM cluster controller. These eight terminals do not have to

be hard-wired and physically close to the cluster controller to communicate with the IBM host. Any authorized workstation user with access rights anywhere on the internetwork can connect to an IBM host. Because multiple workstations can use the ports, one External Communication Service can support many emulation sessions.

How the protocol works

Two separate features emulate the IBM terminal and cluster controller system: the 3270 SDLC/SNA Communication Protocol option, and the 3278 Terminal Emulation software.

Protocol The 3270 SDLC/SNA Communication Protocol option resides on the server, and enables the External Communication Service to emulate either the IBM 3276-2 or 3276-12 cluster controller. The External Communication Service maintains bidirectional communication with the IBM host, using the IBM protocol that the actual IBM cluster controller uses. By temporarily binding the terminal to the host at the time of actual use, a single network server running the External Communication Service with 3270 Communication Protocol can support the communication requirements of multiple users on the internetwork.

Software The 3278 Terminal Emulation software on the workstation enables the workstation to emulate an IBM 3278-2, -3, -4, and -5 display terminal. The workstation receives information from the IBM host through the External Communication Service and displays it exactly as on an IBM 3278 display terminal. The workstation software also sends the user information to the External Communication Service, where it is converted into IBM BSC or SNA protocols.

After information from a host is brought to a workstation, it can be merged with other information, enhanced, distributed, filed, or printed.

Relationship with other services

The Clearinghouse Service maintains the user group lists that the External Communication Service checks for access rights for dial-in users.

The Interactive Terminal Service relies on the ECS for RS232C port management. The ECS enables you to designate a port for asynchronous dial-in.

The Interactive Terminal Service relies on the ECS when the Internetwork Routing Service uses a Communication Interface Unit port. The Internetwork Routing Service cannot access a Communication Interface Unit port until you have used the ECS to create an entry in the Clearinghouse for the Communication Interface Unit. The ECS with the Communication Interface Unit must be started before the Internetwork Routing Service on the same server can use the Communication Interface Unit.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the External Communication worksheets located at the end of this chapter.
- Installing the External Communication Service software as described in the Server Software Installation chapter of the *Services Installation and Setup Guide*.
- Setting up the External Communication Service communication options as described in the External Communication Service chapter of the *Services Installation and Setup Guide*.
- Maintaining the External Communication Service as described in the External Communication Service chapter of the *Services Maintenance Guide*.
  - Monitoring External Communication Service port activity.
  - Expanding lines and ports as communication needs increase.
- Notifying users of any change or disruption in the service.
- Upgrading hardware and software as required.
- Troubleshooting the service as described in *Basic Network Troubleshooting*.

You can perform most ECS procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter in the *Services Installation and Setup Guide* contains the procedures for installing your External Communication Service software. This section explains the hardware, software, and other requirements for installation.

Communication components include an 8000 or 8090 server , one or more RS232C ports (hardware), and local and remote modem hardware if needed, communication software on the server, and communication software on the workstation.

Hardware requirements

The External Communication Service operates on an 8000 or 8090 server. The ECS requires a minimum of 512 Kb RAM (Random Access Memory). A memory of 768 Kb is recommended for memory-intensive uses such as 3270 emulation. The 3280 BSC and SNA terminal emulations require synchronous modems.

You can configure an RS232C communication port, a Multiport Option Kit, or an 873 Communication Interface Unit (CIU) as a port option for your server.

Consult your systems analyst for the configuration selected for your External Communication Service; see your *Network Planning Guide* for more details.

Table 10-1 shows the hardware options you can use with each communication option. The hardware options are described below.

Table 10-1. **Available port options**

Communication option	RS232C port	Multiport Option Kit	873 CIU
Asynchronous Communication Protocol	x	x	x
IBM 3270 BSC terminal emulation	x		
IBM 3270 SNA terminal emulation	x	x	x

RS232C communication port

The RS232C communication port provides a single port on an 8000 or 8090 server. It requires a board and an RS232C connector. The RS232C port supports the Asynchronous Communication Protocol option, 3270 BSC terminal emulation, and 3270 SNA terminal emulation.

The IBM 3270 BSC terminal emulation can use only the server RS232C communication port.

Multiport Option Kit

The Multiport Option Kit provides four RS232C ports on an 8000 or 8090 server, and one RS366 autodialer port. It requires a board, RS232C connectors, and software. The Multiport Option Kit supports the Asynchronous Communication Protocol and 3270 SNA terminal emulation.

873 Communication Interface Unit

The 873 Communication Interface Unit provides four or eight RS232C ports in a one-board or two-board configuration. It consists of a box separate from the server that has its own Ethernet transceivers and drop cables. The 873 Communication Interface Unit supports the Asynchronous Communication Protocol, 3270 SNA terminal emulation, and Internetwork Routing Service circuits.

The Communication Interface Unit is managed by the server running the External Communication Service. You can either use the External Communication Service commands to configure its ports or allocate it for Internetwork Routing Service use.

Data rates

The maximum data rates in kilobytes per second for the External Communication Service port options are shown in Table 10-2. Actual rates will vary with port use. When the line usage is low to moderate, the actual rates approach the raw speed. When the line usage is high, actual rates drop. Under these types of circumstance, you can increase your actual data rates at lower line speeds.

Table 10-2. **Data rate for ECS options (Kb/s)**

	Asynchronous Communication	BSC	SNA
RS232C	9.6 (with flow control)	9.6	9.6
Multiport	19.2 (with flow control) distributed over 4 ports at 1.2, 2.4, 4.8, 7.2, 9.6, 19.2	n.a.	9.6
CIU	19.2 (per board or 9.6 full duplex single port)	n.a.	9.6

Autodialer

The autodialing protocols supported by the ECS are shown in Table 10-3.

Table 10-3. **Autodial support for ECS options**

	Asynchronous	BSC	3270 SNA
RS232C	Racal-Vadic, Ven-Tel, V.25bis, Hayes Smartmodem 2400 Command Language dialing protocols	n.a.	RS366 port
Multiport Option Kit	RS366 port (port 0 only) Racal-Vadic, Ven-Tel, V.25bis, Hayes Smartmodem 2400 Command Language dialing protocols	n.a.	RS366 port (port 0 only)
CIU	Racal-Vadic and Ven-Tel protocols	n.a.	n.a.

Software requirements

The software for the External Communication Service and communication protocols is included with the Standard Services Software floppy disk for 8000 servers, and loaded automatically from the cartridge tape for 8090 servers.

To run the External Communication Service communication options, you need to set software options. Set the correct software option for the type of communication you will be configuring:

- Asynchronous Communication Protocol
- 3270 BSC Communication Protocol
- 3270 SDLC/SNA Communication Protocol

You must load these required External Communication Service software files when you install the system software. Allow about 700 disk pages for these files:

- ExternalCommunicationSDF.bcd
- ECServiceConfig.bcd
- GreeterConfig.bcd
- CommSvcComSoft.bcd
- CommunicationServicesArea.messages
- RS232CCommon.bcd
- ExternalCommunicationService.messages
- TTYGreeter.messages

You load these Multiport Option Kit software files from a separate floppy disk for 8000 servers. Allow about 4disk pages for these files:

- MultiportOptionSDF.bcd
- MultiportOption.messages

Dependencies and limitations

These dependencies and limitations exist for the External Communication Service.

- The External Communication Service consumes a large amount of server resources. The ECS performs best when the Server Monitor Service and the Communications Monitoring Service are the only other services on the same server with it. Do not install a File Service on the same server. See the exceptions for the ports below.

Modems

For asynchronous communication, the modem you attach to the 8000 or 8090 server port or the Communication Interface Unit must be compatible with the modem attached to the host.

Autodialing

If you use the autodialing feature and are running the External Communication Service software version 10.3, do not run version 10.0 of these services on the same server:

- Communications Monitoring Service
- 850/860 Gateway Service
- Internetwork Routing Service
- Mail Service with the External Mail Gateway option
- Remote Batch Service

RS232C communication port

- Do not install any of these services or options that use the same RS232C port on the server running the External Communication Service with the RS232C port configured: 850/860 Gateway Service, the IBM 3270 BSC Communication Protocol, the Facsimile Print Service, the External Mail Gateway option, and the Remote Batch Service. The ECS can share the RS232C port serially, but not concurrently.
- If the ECS is to support 3270 BSC emulation, do not run other services on the same server. If you must assign additional services or additional ECS functions to the same server (for example, the control of a Communication Interface Unit), the services should be low-demand in nature, such as a lightly used File Service.

Multiport Option Kit

- No restrictions exist on the combinations of line speeds for the Multiport Option Kit, as long as the sum of the line speeds of all four ports does not exceed 56 Kb/sec. For example, an ECS running without coresident services on a Multiport Option Kit server can support four asynchronous connections at 9.6 Kb/sec.; or three connections at 9.6 Kb/sec. and one connection at 19.2 Kb/sec.; or two connections at 19.2 Kb/sec. and one connection at 9.6 Kb/sec.
- If one or more Multiport Option Kits are used for 3270 emulation, the Internetwork Routing Service can be the only coresident service.

Communication Interface Unit

- Limitations exist for the simultaneous connections supported by the CIU. The maximum throughput for one CIU board is 9600 baud. Mixed baud rates on a single-board CIU must conform to one of these ranges:

  1st range - 300, 600, and 1200
  2nd range - 600, 1200, and 4800
  3rd range - 1200, 2400, and 4800
  4th range - 2400, 4800, and 9600

- If you are mixing asynchronous and bisynchronous communication on the same board, you must assign the asynchronous communication to the lowest-numbered ports.
- If an RS232C port is configured for the Interactive Terminal Service and is on a Communication Interface Unit with no autodialer attached, you cannot reconfigure that port for TTY emulation.
- A break (pressing the BREAK key) cannot be received through RS232C ports on a Communication Interface Unit.
- When an RS232C port on a Communication Interface Unit is assigned to TTY emulation or the Interactive Terminal Service (asynchronous communication), the Communication Interface Unit discards any character received with baud parity. The workstation or the Interactive Terminal Service gives no explicit indication of this event, and the user will only notice a missing character.
- The Communication Interface Unit can co-exist with the local server port or the Multiport Option Kit. You can configure one server to support one Multiport Option Kit and one one-board or two-board CIU.
- The External Communication Service and the Internetwork Routing Service must co-exist on the same server when the Internetwork Routing Service is to use CIU ports for any of its circuits.

Asynchronous Communication Protocol

- Never configure an asynchronous port connected to a dedicated line for both dial-in and terminal emulation.

- A single port configured for asynchronous use cannot have a line speed greater than 19.2 Kb.

IBM 3270 BSC

- The 3270 BSC Communication Protocol must use the local port on the server running the External Communication Service.
- Any service that utilizes the server port cannot be active if 3270 emulation is using that port.
- Each External Communication Service with 3270 communication protocol can support up to eight concurrent emulation sessions with workstations--a maximum of eight per port and twelve per server.
- A single port configured for IBM 3270 BSC use cannot have a line speed greater than 56 Kb.

IBM 3270 SNA

- The 3270 SNA Communication Protocol can use the server port, a port on the Multiport Option Kit, or a Communication Interface Unit. If you use a Communication Interface Unit, use a full-duplex leased line.
- Over 3270 SNA connections, the data moves in increments called Response Units (RUs). The emulated cluster controller of the ECS cannot handle an RU greater than 4096 bytes. Check with the host site to make sure that the hosts you access do not use RUs greater than this limit.
- Up to eight simultaneous sessions can take place with one host connection. Up to twelve simultaneous sessions can take place with two 3270 SNA connections to the same host or different hosts, and up to eight simultaneous sessions with three connections to the same host or different hosts. No more than three ports can be used for 3270 SNA communication at one time.
- The sum of the number of IBM 3270 host ports on the controller for each active IBM 3270 SNA connection cannot exceed 12, if two ports are configured for use. This number should not exceed eight if three ports are configured for use. This sum should be less in all cases if other services, excluding the Communications Monitoring Service, are coresident.
- If you use the ViewPoint 1.0 version of 3270 terminal emulation software to connect to an IBM host, the host's SSCP must send messages that can be displayed in 23 lines or less. If the host sends a 24-line message, it leaves no place for the user to type.
- A single port configured for IBM 3270 SNA use cannot have a line speed greater than 56 Kb.
- The 3270 SNA communication option uses server resources quite heavily. When many simultaneous emulation sessions are active, the External Communication Service can take over this limited resource and crash the server. Server overload may also cause 3270 emulation clients to lose their connection with the server housing the External Communication Service.

These server resources are allocated, freed, and reallocated constantly, depending on the services that are running. It is impossible for you to be aware of exceeded limits, and to take corrective action.

Ensure that you configure the server so that the services on it are unlikely to over-extend its resources. Do not place a heavily used 3270 SNA emulation on a server with a Print Service, Interactive Terminal Service, Mail Service, Clearinghouse Service, or File Service. If you experience server overload, add memory to the servers supporting a heavy use of 3270 emulation.

Relationship with other services

The Remote System Administration capability and the Interactive Terminal Service depend on the External Communication Service. To support these dial-up activities, the External Communication Service answers calls that come in to one or more of its ports.

External Communication Service worksheets

Use the External Communication Service worksheets to record server-related and service-related information, as well as port configuration and host configurations and assignments. The worksheets are at the end of this chapter.

Fill out a separate copy of the worksheet for each External Communication Service for which you have System Administrator responsibility. Retain the original worksheets for future use, and store the completed worksheets in your *Activities Guide*.

Using the worksheets

Before you install the software on a server and set up your External Communication Service, complete the External Communication Service worksheets. It is important that you fill out the worksheets accurately and update them whenever changes occur.

The completed worksheets save you time as you perform the setup and maintenance procedures. They also serve as an information source for new System Administrators unfamiliar with your network configuration.

Filling out the worksheets

As you read the rest of this chapter, you are directed to make entries on the External Communication worksheets. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and the services installed on the server. Copy this information from the Services Installation Worksheet you filled out while reading the Services System Software chapter of this book.

Use section ② of the first worksheet for information about the Communication Interface Unit. Use sections ③ and ④ for information about the asynchronous port configurations. Use

sections ⑤ and ⑥ for information about IBM 3270 BSC server port and host configuration.

On the second worksheet, use sections ⑦ through ⑨ for information about IBM 3270 SNA port and host configurations.

Planning for setup

After you install the External Communication Service, initialize it and register each port you will be using. See the External Communication Service chapter in the *Services Installation and Setup Guide* for complete setup procedures.

The following information will help you perform those procedures. Refer to the section for the communication option you are setting up.

External Communication Service names and descriptions

When you name the External Communication Service, use a name different from all other names in the domain. The fully qualified name of the External Communication Service has the format:

External Communication Service name:Domain:Organization

The domain and organization must be the same as the domain and organization of the server. For example, if the server name is Wombat:Abilene:Acme, then the External Communication Service name might be Echo:Abilene:Acme. This naming convention gives the System Administrator enabled for the server domain access to all External Communication Service commands.

To avoid possible errors, enter only the local name when you name the External Communication Service. This approach lets the domain and organization default to those of the server.

A description for the External Communication Service is optional. The description can help you identify the location or the function of the External Communication Service. For example, if an External Communication Service is used for IBM emulation only, include that information in the description.

Related procedure: Initializing the External Communication Service

Filling out the worksheet

① Record the name and description of the External Communication Service.

Communication Interface Unit information

Use a unique name for a Communication Interface Unit. The description for the Communication Interface Unit is optional; however, it does help identify the function of the CIU. For example, if you are using the Communication Interface Unit for IBM 3270 SNA terminal emulation, supply this information for the description.

A Communication Interface Unit may be a one-board or two-board unit. Each board provides four ports to be configured for communication.

Each Communication Interface Unit has an identification number, which begins with 949.

Related procedure: Adding a Communication Interface Unit

Filling out the worksheet

② Record the Communication Interface Unit name, description, board type (one-board or two-board), and processor number for the server you are setting up.

Asynchronous communication

Asynchronous communication includes TTY and VT100 terminal emulation and asynchronous dial-in. Configure for asynchronous dial-in when users need to access the Interactive Terminal Service or use Remote System Administration. Configure for both asynchronous terminal emulation and dial-in when a port should be used for either. You can configure asynchronous terminal emulation and/or asynchronous dial-in on a server port, multiport, or CIU.

The information you need for configuring your asynchronous port depends on how you are setting up your asynchronous communication.

Related procedures: Configuring the server port or a Multiport for asynchronous terminal emulation and/or dial-in, Configuring a CIU port for asynchronous terminal emulation and dial-in

Filling out the worksheet

③ and ④ **Port name and description** - Record the unique name of the RS232C server port or multiport.

③ **Port number** - If you installed a CIU, record the port number. A one-board CIU has four ports that you can configure for asynchronous communication. A two-board CIU has four additional ports. Configure the port for a set port number only if you are connecting to a CIU.

④ If you installed the Multiport Option Kit, you need to know the local port number, a value from 0 to 3.

③ and ④ **Port use** - Record the type of asynchronous communication for which you will be using this port. Port use depends on the communication protocol you are using, and the communication software options you enabled when you installed the software. For example, if you are using the port for asynchronous terminal emulation, you must enable the Asynchronous Communication Protocol option and specify asynchronous terminal emulation for port use.

③ and ④ **Interactive Terminal Service (ITS) connection** - Specify whether the port will be used for an Interactive Terminal Service connection. When you configure an asynchronous port, you can set it up so that dial-in users are restricted to use only the Interactive Terminal Service residing on the same server as the External Communication Service. The user must press RETURN

within 30 seconds after dialing or autodialing the local Interactive Terminal Service, or the connection is dropped.

You can give the dial-in user the option of either using the Interactive Terminal Service or enabling Remote System Administration functions from the remote terminal. The user must press RETURN within five seconds after dialing or autodialing the local Interactive Terminal Service, even if the Greeter's sign-on message does not appear.

③ **Port behavior** - Specify whether the port is to behave as a modem or terminal. If you are using a CIU, configure an asynchronous port to behave as a modem or a terminal. (A local server port set up for asynchronous communication always behaves as a terminal, so you do not need to configure it.)

If a modem is connected to the port, configure the port to behave as a terminal (DTE for Data Terminal Equipment). If a terminal is connected to the port, then configure the port to behave as a modem (DCE for Data Communications Equipment). If you are connecting a dumb terminal to a CIU port for Interactive Terminal Service connection or Remote System Administration, set the port behavior to DCE.

③ and ④ **Data bits (per character)** - Record the number of data bits per character for this port. You must determine whether your equipment supports XOn/XOff flow control. If it does, you must configure the port for 7 data bits per character. If you will be storing or retrieving files using XModem, configure the port for 8 data bits per character.

If you are using a parity of "None" as determined by the setting on the device with which you wish to communicate, configure the port for eight data bits as well.

③ and ④ **Stop bits (per character)** - Record the number of stop bits per character for this port. Check the baud rate of your equipment. If it is below 300 bits per second (bps), configure your port for 2 stop bits. Otherwise, configure the port for 1 stop bit.

③ and ④ **Parity** - Record the parity setting for this port. Check the setting on the device with which you will be communicating. Usually, even parity is used. If you are planning to use the port for Interactive Terminal Service XModem file transfers, configure the port for even parity.

③ and ④ **Autodialer type** - The autodialing protocols supported by the Multiport Option Kit include the Hayes Smartmodem 2400 Command Language, Racal-Vadic, Ven-Tel, RS366, and V25bis dialing protocols.

Select the Hayes pulse-dialed option when the modem is connected to a pulse-dialed line. Select the touch-tone option when the modem is connected to a touch-tone dialed line. Services 10.0 users must enter a T (touch tone) or a P (pulse dial) before the phone number to tell the modem which dialing method to use.

You must specify the autodialer type, regardless of port use. Use only Hayes modems if you use the Hayes dialing protocol.

If you are using another type of autodialer, you must dial from the TTY emulation window instead of the TTY option sheet when you are using the port.

NOTE

You cannot have a Racal-Vadic modem on one port and a Ven-Tel modem on another port that uses the same Communication Interface Unit.

Keep in mind that only RS366 dialers are approved for use on port 0.

③ and ④ **XOn/XOff flow control** - Set the flow control for data rates of 19.2 Kb/sec per line for the Multiport Option Kit, 9.6 Kb/sec per line for server ports. If your equipment supports XOn/XOff flow control, you must determine the OCTAL values of the XOn and XOff characters. The OCTAL values can range from 0 to 77.

Check with your remote host representative to verify correct OCTAL values for your communication configuration. DC1 is the normal XOn character, with an OCTAL value of 21. DC3 is the normal XOff character, with an octal value of 23.

If you are using the XModem protocol, including STerm with PC on the network, ITS File transfer, and TTY emulation on a 6085/8010 workstation, do not turn on the flow control. If flow control is on, data blocks are transmitted incorrectly.

④ **Duplexity** - Record the duplexity of your equipment. Duplexity (full duplex or half duplex) is determined by the modem you have connected.

③ and ④ **Line speed** - Record the line speed of your equipment. Line speed is determined by the modem or the type of communication line attached to the server. When you set up a CIU, the asynchronous line speeds must be within the same range on the same board. The External Communication Service will not configure the CIU if you violate this range of line speeds:

1st range - 110 bps
2nd range - 75, 150, and 300 bps
3rd range - 150, 300, and 600 bps
4th range - 300, 600, and 1200 bps
5th range - 600, 1200, and 2400 bps
6th range - 1200, 2400, and 4800 bps
7th range - 9600 bps

Line speeds for the Multiport Option Kit are assigned to ports in this order: 1 (highest), 0, 3, and 2.

③ and ④ **Access group** - Record the group name for each port to which you are controlling access. You can maintain access control for an asynchronous terminal emulation port or for an asynchronous terminal emulation and dial-in port.

Access control enables you to ensure that only a select group of users access asynchronous terminal emulation, providing a greater control on security. If you do not limit access control to a specific group, anyone on the internetwork can access asynchronous terminal emulation.

Make sure the group name you use is valid. The External Communication Service does not validate group names with the Clearinghouse Service.

IBM 3270 BSC terminal emulation

You can configure IBM 3270 BSC terminal emulation only on the server port. The information you need for configuring your IBM 3270 port depends on how you are setting up your port.

Related procedure: Configuring the server port for IBM 3270 BSC terminal emulation

Filling out the worksheet

⑥ **Port name and description** - Record the name of the port. The name of the RS232C server port must be unique. The description is optional, but can help identify the port configuration.

Port use - Record the port use. Port use depends on the communication protocol you are using, and the communication software options you enabled when you installed the software. For example, if you are using the port for IBM 3270 BSC terminal emulation, you must enable the 3270 BSC Communication Protocol option and specify 3270 BSC terminal emulation for port use.

Duplexity - Record the equipment duplexity as determined by the modem you have connected. If the modem has a multidrop line, then define the port as half duplex, even if the modem and communication line attached to the port are full duplex. Multidrop lines can be used only on the server port.

Line speed - Record the line speed as determined by the dialing hardware or the dedicated line attached to the server.

IBM 3270 SNA terminal emulation using a CIU port

You can configure IBM 3270 SNA terminal emulation on a CIU. The information you need to configure your IBM 3270 port depends on how you are setting up your port.

Related procedure: Configuring a CIU port for IBM 3270 SNA terminal emulation

Filling out the worksheet

⑦ **Port name and description** - The name of the RS232C server port must be unique. The description is optional, but can help identify the port configuration.

CIU - Record the name of the CIU you will be using as a connection.

Port number and use - Record the port number for this type of communication. A one-board CIU has four ports that you can configure for communication. A two-board CIU has four additional ports. Configure the port for a set port number only if you are connecting to a CIU.

Line speed - Record the line speed as determined by the dialing hardware or the dedicated line attached to the server.

The CIU port connections are full duplex for a switched 3270 SNA line.

Assign a line speed for SNA ports in this order: 1 (highest), 4, 3, and 2.

IBM 3270 SNA terminal emulation using a server port or Multiport Option Kit

You can configure IBM 3270 SNA terminal emulation on a server port or the Multiport Option Kit. The information you need for configuring your IBM 3270 port depends on how you are setting up your port.

Related procedure: Configuring the server port or a Multiport for IBM 3270 SNA terminal emulation

Filling out the worksheet

⑧ **Port name and description** - The name of the RS232C server port or Multiport Option Kit must be unique. The description is optional, but can help identify the port configuration.

Port number - If you installed the Multiport Option Kit, record the local port number, a value from 0 to 63.

Port use - Port use depends on the communication protocol you are using. In this case, record the port use as IBM 3270 terminal emulation for a server port or the Multiport Option Kit.

Autodialer type - The supported autodialing protocols include Hayes, RS366, and V25bis.

Data encoding - The Multiport Option Kit offers the standard bitsynchronous data-encoding scheme (NRZI) used by IBM communication devices. If you are using a server port, specify NRZ for the link to the 3270 controller.

Duplexity - Record the equipment duplexity as determined by the modem you have connected. If the modem is a multidrop, then define the port as half duplex, even if the modem and communication line attached to the port are full duplex. Multidrop lines can be used only on the server port and cannot be used for SNA emulation.

Line speed - Line speed is determined by the dialing hardware or the dedicated line attached to the server. If you have the Multiport Option Kit installed, your line speed potential increases to 56000 bps.

Information for the host site

When you configure IBM 3270 BSC or SNA terminal emulation, you must also give the host site the details of your configuration to aid host site personnel with their configuration.

Related procedure: Configuring the server port for IBM 3270 BSC terminal emulation, Configuring the server port or a Multiport for IBM 3270 SNA terminal emulation, Configuring a CIU port for IBM 3270 SNA terminal emulation

Filling out the worksheet

⑩ Record the cluster controller model you are emulating:

- 3276-12 (SNA) or 3276-2 (BSC): The ECS has a switched line connection to the host, or is supporting terminal emulation for a ViewPoint version prior to 1.1.
- 3274: Dedicated line to host, supporting 3270 emulation and ViewPoint version 1.1, with no more than eight terminal connections.

Record the terminal model being emulated:

- 3278-5: The ECS is supporting 3270 emulation for a ViewPoint version prior to 1.1.
  - 3278-2: The ECS is supporting 3270 emulation for a ViewPoint version prior to 1.1.
- The number of ports per cluster controller, a limit of eight.
- The line duplexity setting.
- The data encoding (for SNA only) - NRZI for the Multiport Option Kit.
- The language used.

Controller address information

Before you can add an IBM 3270 host to the External Communication Service, you must determine the controller address for BSC or SNA communication.

IBM 3270 BSC controller address

Your IBM host site tells you the controller address, which is a number between 0 and 31. If your host site provides you with an address in another format, use Table 10-4 to determine the corresponding number in the correct format.

Related procedure: Adding and assigning an IBM 3270 BSC host

Table 10-4. **Character to controller address mapping**

EBCDIC Hex	Character	Controller Address	EBCDIC Hex	Character	Controller Address
40	SPACE	0	50	&	16
C1	A	1	D1	J	17
C2	B	2	D2	K	18
C3	C	3	D3	L	19
C4	D	4	D4	M	20
C5	E	5	D5	N	21
C6	F	6	D6	O	22
C7	G	7	D7	P	23
C8	H	8	D8	Q	24
C9	I	9	D9	R	25
4A	¢	10	5A	!	26
4B	.	11	5B	$	27
4C	<	12	5C	*	28
4D	(	13	5D	)	29
4E	+	14	5E	;	30
4F	▮ or !	15	5F	¬ or ?	31

Source: Figure 6-1, page 6-11, *IBM 3270 Information Display System Component Description,* Document GA27-2749-9, 10th edition, August 1979.

Filling out the worksheet:

⑥ **Controller address** - Record the IBM 3270 BSC controller address.

IBM 3270 SNA controller address

Your computer site tells you the controller address, which is a decimal number between 1 and 255. This address is sometimes called the "SDLC station address."

If your host site tells you the address is "10," be sure you know if this address is 10 decimal or 10 hexadecimal (which is 16 decimal). If the host site provides you with a hexadecimal address (a number between 1 and FE), you must convert it to decimal.

Use Table 10-5 to convert one-digit hexadecimal numbers to decimal.

Table 10-5. **Hexadecimal/decimal chart**

Hexadecimal	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
Decimal	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

Use Table 10-5 and the formula below to convert a two-digit hexadecimal number to a decimal number. The formula for converting two-digit hexadecimal to decimal is:

16(H1) + (H2) = the decimal equivalent

where:

H1 = decimal equivalent of the first hexadecimal digit

H2 = decimal equivalent of the second hexadecimal digit

For example, to convert the hexadecimal number AF, multiply the value of the first hexadecimal digit (H1) by 16, then add the value of the second digit.

AF = hexadecimal digit

H1 = A(hexadecimal) = 10 (decimal)

H2 = F(hexadecimal) = 15 (decimal)

AF = 16(H1) + (H2) = the decimal equivalent

AF = 16(10) + (15)

AF = 160 + (15) = 175 = decimal equivalent of AF

Related procedure: Adding and assigning an IBM 3270 SNA host

Filling out the worksheet:

⑨ **Controller address** - Record the IBM 3270 SNA controller address.

IBM 3270 BSC host

You must register IBM 3270 BSC hosts with the External Communication Service.

Related procedure: Adding and assigning an IBM 3270 BSC host

Filling out the worksheet

⑥ **Name and description** - Record the name and description for the IBM 3270 BSC host. An IBM 3270 BSC host must have a unique name. The description is optional, but may be useful if you include information such as the IBM host location or status.

Port name - Record the name of the RS232C port through which the host is accessed. Make sure that you have configured the port for host terminal emulation. The IBM 3270 BSC host is on a non-switched, dedicated line to the port. With a non-switched, dedicated line, you can define only a single IBM 3270 BSC host for each RS232C port.

Buffer size - Record the buffer size that the IBM 3270 host expects the ECS emulated cluster controller to maintain during communication. This size is typically 265, but must be between 60 and 512 (PU macro MAXDATA parameter). Obtain this information from the host site.

Number of ports - Record the number of ports on the emulated 3276 controller (from 1 to 8). Obtain this number from the host site.

Access control - You can maintain access control for IBM 3270 BSC hosts. Access control enables you to ensure that only a select group of users can access IBM 3270 terminal emulation, providing a greater control on security. If you do not limit access control to a specific group, anyone on the internetwork can access the terminal emulation.

You can specify a different group for access to each of the eight ports, or you can allow the same group access to all eight ports. Groups can be in the same or different domains.

Make sure the group name you use is valid. The External Communication Service does not validate group names with the Clearinghouse Service.

Language - The emulated 3276 controller supports 26 languages. The language supported by the controller refers to a variant of the EBCDIC code. Make sure the language matches an equivalent setting in the 3270 host. For the host, assign US English, unless told otherwise by your host site.

IBM 3270 SNA hosts

You must register IBM 3270 SNA hosts with the External Communication Service.

Related procedure: Adding and assigning an IBM 3270 SNA host

Filling out the worksheet

⑨ **Name and description** - Record the name and description of the host. An IBM 3270 SNA host must have a unique name. The description is optional, but may be useful if you include information such as the IBM host location or status.

Port name - Record the name of the RS232C port through which the host is accessed. Make sure that you have configured the port for host terminal emulation.

Phone number - Record the phone number for the line to the IBM 3270 host. Your line to the IBM 3270 SNA host is a dial-up line if it is either a manually dialed or an autodialed (switched) line. For switched lines, a phone number is necessary for connection to the host. When configuring dial-up lines, know which dialing method is used on the associated phone line.

Because the IBM 3270 SNA communication protocol supports switched connections, you can use a single RS232C port to communicate with several different hosts.

Valid phone number characters are 0 through 9, *, #, = (EON or end of number), < (SEP, wait for dial tone), and > (six-second pause). You can enter up to 31 characters. Do not use hyphens or spaces. When entering phone numbers for an SNA

synchronous port, enter a T or P before the number; T is for touch-tone dialing, P is for pulse dialing.

The RS366 dialing protocol is allowed only with port 0.

Controller XID - Record the emulated 3276 controller XID (switched line to SNA host). This number is used in addition to the controller address to further identify a device on a switched line. The five hexadecimal characters are the XID (PU macro IDNUM parameter). Obtain this number from the host site.

Buffer size - Record the buffer size that the IBM 3270 host expects the ECS emulated cluster controller to maintain during communication. This size is typically 265, but must be between 60 and 512 (PU macro MAXDATA parameter). Obtain this information from the host site.

Number of ports - Record the number of ports on the emulated 3276 controller (from 1 to 8). Obtain this number from the host site.

Access control - You can maintain access control for IBM 3270 SNA hosts. Access control enables you to ensure that only a select group of users can access IBM 3270 terminal emulation, providing a greater control on security. If you do not limit access control to a specific group, anyone on the internetwork can access the terminal emulation.

You can specify a different group for access to each of the eight ports, or you can allow the same group access to all eight ports. Groups can be in the same or different domains.

Make sure the group name you use is valid. The External Communication Service does not validate group names with the Clearinghouse Service.

Language - The emulated 3276 controller supports 26 languages. The language supported by the controller refers to a variant of the EBCDIC code. Make sure the language matches an equivalent setting in the 3270 host. For the host, assign US English, unless told otherwise by your computer host.

Planning for maintenance

After you install and set up the External Communication Service, you are responsible for maintaining it. This section provides guidelines for changing your communication configurations.

See the External Communication Service chapter in the *Services Maintenance Guide* for complete maintenance procedures.

Verifying port and host entries with the Clearinghouse Service

When you create or modify port and IBM host entries, some of the configuration information is stored in the Clearinghouse database. The External Communication Service can usually register the port or host successfully.

However, if an External Communication Service error message reports that the ECS cannot register information with the Clearinghouse Service, or if you cannot copy a 3270 emulation icon onto your workstation, re-register information manually by verifying the Clearinghouse entries.

You can check all External Communication Service entries for consistency, or check only the inconsistent entries--those entries where the External Communication Service was unable to register a port or host with the Clearinghouse Service.

Note that asynchronous dial-in ports are not verifiable with the Clearinghouse. Dial-in users are never known to the Clearinghouse Service.

Related procedure: Verifying Clearinghouse entries

Changing the port or host configuration

You may need to change information in a port or host configuration or assignment. The information you need to obtain for such a procedure is the same information you needed when you set up the port or host. See "Planning for setup" earlier in this chapter for details.

Before changing a port name, number, location, or use, or before deleting a port, list the IBM 3270 hosts to see if any hosts require the port you are changing. Also display information about the port to see which host is assigned to the port as the default host. If you change a port name, you must also make the change in every host entry that specifies that port. If you change the port use or delete the port entry, you must first change the host entry to specify a different port.

After any port entry change, reassign the default host for a new host port assignment. You do not need to reassign the host if there is only one host defined for a port.

To change the host name, you must first delete the old host, then add the new host with a different name.

Be sure you update the appropriate sections of the worksheet when you make any changes to a port or host configuration.

Related procedures: Changing an asynchronous CIU port configuration, Changing an IBM 3270 SNA CIU port

configuration, Changing an asynchronous server port or Multiport configuration, Changing an IBM 3270 BSC server port configuration, Changing an IBM 3270 SNA server port or Multiport configuration, Changing an IBM 3270 BSC host configuration, Changing an IBM 3270 host configuration

Monitoring External Communication Service activity

Monitor External Communication Service activity and statistics on a regular basis. For example, if you want to know which users are using particular ports, you can show port statistics and display the performance, loading, and error information for that port. You can also display information about each port, and list configured ports and assigned hosts.

Related procedure: Showing RS232C port statistics

Asynchronous port activity

This information is displayed for an asynchronous communication port:

Name - The name of the port.

Current state - The state of the port:

- Idle - Means that the port is not being used by any user and is not monitoring the phone line for incoming calls. "Idle" is the normal available state. Ports shared between emulation and dial-in users may also be in the "idle" state for short periods (less than 10 minutes). If they stay in the idle state longer, check for possible hardware or software problems.
- Listening - Means that the port is idle, but is monitoring the phone line for incoming calls. "Listening" is the available state for ports shared between asynchronous terminal emulation and dial-in users, and for ports that support only dial-in users.
- In use - Means that the port is being used for either asynchronous terminal emulation or dial-in access.

User - The current user of the port. If the user is unknown to the External Communication Service, the user field is empty. This parameter is shown only if the port is in use. (Dial-in users are never known to the External Communication Service and are never shown.)

Session length - The number of minutes since the current session started. This parameter is displayed only if the port is in use.

Speed - The current line speed for the port. This parameter is displayed only if the port is in use.

Character format - The current settings of the RS232C parameters that affect the asynchronous character format. The format includes:

- The number of bits per character
- The number of stop bits
- Any parity sent or checked

These parameters are displayed only if the port is in use.

Total characters sent - The number of characters sent from the RS232C port in the current user session. This parameter is displayed only if the port is in use.

Total characters received - The number of characters received on the RS232C port in the current user session. This parameter is displayed only if the port is in use.

Parity errors - The number and percentage of characters received with parity errors on the RS232C port in the current user session. This parameter is displayed only if the port is in use.

Since boot - Introduces statistics that refer to cumulative totals since the server was last booted:

- **Total time** - The number of minutes since you last booted the External Communication Service.
- **Number of connections** - The number of user sessions since you last booted the External Communication Service.
- **Percent utilized** - The percentage of time that the port was in use since you last booted the External Communication Service.
- **Connect time** - The time the port was in use:
  - **Total** - The total time in minutes that the port was in use since you last booted the External Communication Service.
  - **Minimum** - The time in minutes for the shortest user session since you last booted the External Communication Service.
  - **Maximum** - The time in minutes for the longest user session since you last booted the External Communication Service.
  - **Total characters received** - The number of characters received on the RS232C port since you last booted the External Communication Service.
  - **Parity errors** - The number and percentage of characters received with parity errors on the RS232C port since you last booted the External Communication Service.

IBM 3270 BSC or SNA port activity

This information is displayed for an IBM 3270 BSC or SNA terminal emulation port:

Name - The name of the port.

Controller - The total elapsed time since you enabled the 3270 controller emulation, and the utilization averaged over all eight terminal emulations.

Current number of users - The number of people (from 0 to 8) using this 3270 emulation facility.

Errors - The number and percentage of transmission errors. These error statistics can help identify problems with the communication medium.

Device <number> - The device type (such as a display or printer), total session time, and percent of utilization. For each terminal emulation, this statistic gives the total time the device was in use and the number of busy rejects. If the device is currently in use, a second line identifies, if possible, the user of the terminal emulation. If the emulation session was established

from an older version of 8010 or 860 software, "no user" is displayed. Entries for a particular device are displayed only after a user has accessed that device.

11. SNA Mail Relay

This chapter helps you prepare for installation, setup, and maintenance of the SNA Mail Relay (SMR) and the Foreign Gateway Assistant (FGA). The information supports the procedures you perform from an 8000 server.

Service description

The SNA Mail Relay is part of a group of software products that together provide electronic mail exchange between Xerox Network System (XNS) users and IBM SNA Distribution Services (SNADS) users running DISOSS (Distributed Office Support System). These products include:

- SNA Mail Relay
- SNA Access
- Foreign Gateway Assistant
- Mail Service with External Mail Gateway option enabled

The SNA Mail Relay, Foreign Gateway Assistant, and Mail Service are installed separately. SNA Access is installed automatically with the SNA Mail Relay.

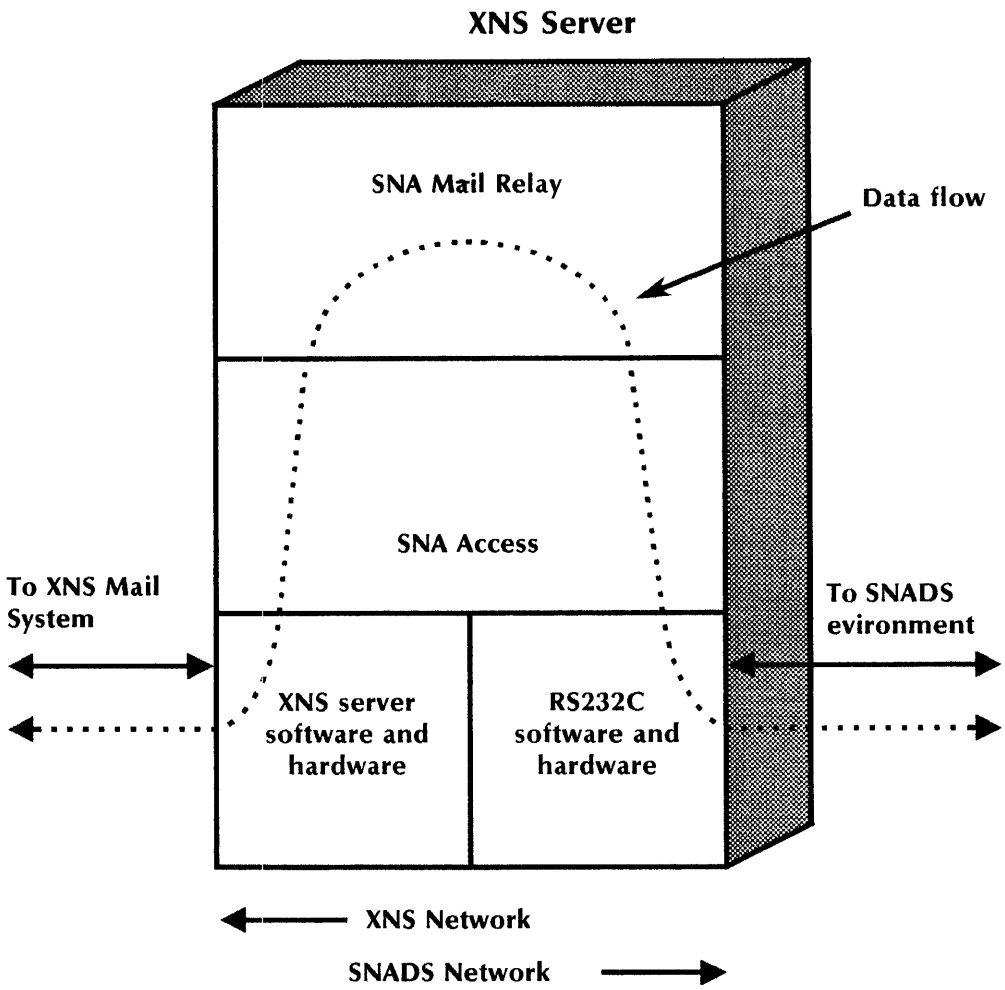
The SNA Mail Relay supports XNS users of 6085 Professional Computer Systems, 860 Information Processing Systems, or PCs connected to an XNS network. These users must have access to Mail Service applications such as ViewPoint or Star Mail, 860 Mail, PC-on-the-net XMail, or ITS Mail.

The SNA Mail Relay also supports SNADS users of IBM (or compatible) computers connected to an SNA network, provided they have access to DISOSS. The computers require software that implement SNADS, Document Interchange Architecture (DIA), and Document Content Architecture (DCA).

SNADS and DIA define the way documents are packaged, sent, received, and protected in an SNA network. DCA defines a document's format.

Figure 11-1 shows how SNA Mail Relay provides mail exchange between XNS and SNADS users.

Figure 11-1. **SNA Mail Relay components on an XNS server**



SNA Mail Relay

The SNA Mail Relay moves mail from an XNS network to a SNADS network, and moves mail from a SNADS network to XNS.

XNS to SNADS - The SNA Mail Relay retrieves mail from its mailbox, converts the recipient names as required, and passes it to SNA Access for forwarding to the SNADS network. SNA Mail Relay converts only XNS mail notes to DCA documents. The attachments can be converted through ViewPoint workstation software (VP File Conversion of IBM DCA documents).

SNADS to XNS - The SNA Mail Relay receives mail from SNA Access, converts the SNADS names to XNS recipient names, and posts the mail to any XNS Mail Service able to accept postings. If a document has a memo attached, the SNA Mail Relay converts it to a mailnote. The SNA Mail Relay converts only mailnotes. When the SNA Mail Relay receives SNADS mail that contains a request for Confirmation of Delivery (COD), it confirms delivery after it has posted the mail with the XNS system. It does not confirm that the message has reached the user's mailbox.

Foreign Gateway Assistant

The Foreign Gateway Assistant provides a bridge between the XNS Mail System and the SNA Mail Relay. It moves mail from the Mail Service gateway queue to the SNA Mail Relay mailbox.

The FGA extends the function of the Mail Service External Mail Gateway option. You install the FGA on the same server as a Mail Service with the External Mail Gateway option enabled. See the Mail Service chapter in this book for information on the External Mail Gateway.

SNA Access and DISOSS

SNA Access provides communications support so that applications, such as the SNA Mail Relay, can communicate with a SNADS network. SNA Access implements the SNA protocol to enable communication with SNA hosts and processors. SNA Access also implements SNA Distribution Services (SNADS), which is the application level protocol for the packaging and delivery of mail in an SNA network.

SNA Access connects to the IBM Distributed Office Support System (DISOSS). DISOSS is a package of office automation applications that run on IBM System/370 mainframes. DISOSS also implements SNA and SNADS protocols to route and deliver mail.

Comparison of SNADS and XNS features

The following Table shows the feature comparison of SNADS and XNS networks.

Table 11-1. **SNADS and XNS feature comparison**

Feature	XNS Mail System	SNADS
Specifying recipients	Fully qualified three-part user name.	Distribution User Name (DUN) which is made up of an 8-character Distributuion Group Name (DGN) and an 8-character Distribution Element Name (DEN)
Recipient validation	Yes	No
Confirmation of delivery (COD)	No	Yes
Expand distribution list	Yes	Only if implemented on local machine.
Document size	Unlimited	Limited to 25% of the database size
Error reporting	Message timed out, no such user, or not a serialized file	Unknown recipient or other
Mail returned if undeliverable	Yes, if error is reported within 48 hours of posting	No
Password protection for individual files	No	Yes
Message size	8000 charaters (bytes)	256 characters (bytes)
Mail prioritization	No	Yes, 15 levels plus FAST and Status.

The terms used to describe features within the XNS and SNADS environment are different. The following Table lists the SNADS equivalent of XNS terms.

Table 11-2. **SNADS and XNS terms**

XNS term	SNADS equivalent
alias	nickname
attachment	document of distribution object
distribution list	shared distribution list
domain:organization	Distribution Group Name (DGN) or user set
file attribute	document profile
file type	document type
fully qualified name	Distribution User Name (DUN)
inbasket (ViewPoint)	mail log (PS products)
mail note or cover sheet	memo
message	Distribution Interchange Unit (DIU)
user name	Distribution Element Name (DEN) or user ID

How the software works

This section describes how mail moves between the XNS Mail System and SNADS environment. In this example, the XNS mail correspondent is using ViewPoint; the SNADS correspondent is using PS/36.

XNS to SNADS

1. The XNS workstation user writes a mail note to a SNADS mail recipient and selects "Send."
2. The workstation application software posts the mail to an XNS Mail Service.
3. The Mail Service forwards the mail to a Mail Service with an External Mail Gateway option. This Mail Service has a foreign gateway that receives SNADS-bound mail.
4. The Mail Service places the mail in its gateway queue, ready for delivery.

At this point, the mail begins its route into the SNADS environment.

5. The Foreign Gateway Assistant moves the mail from the gateway queue to the SNA Mail Relay mailbox.

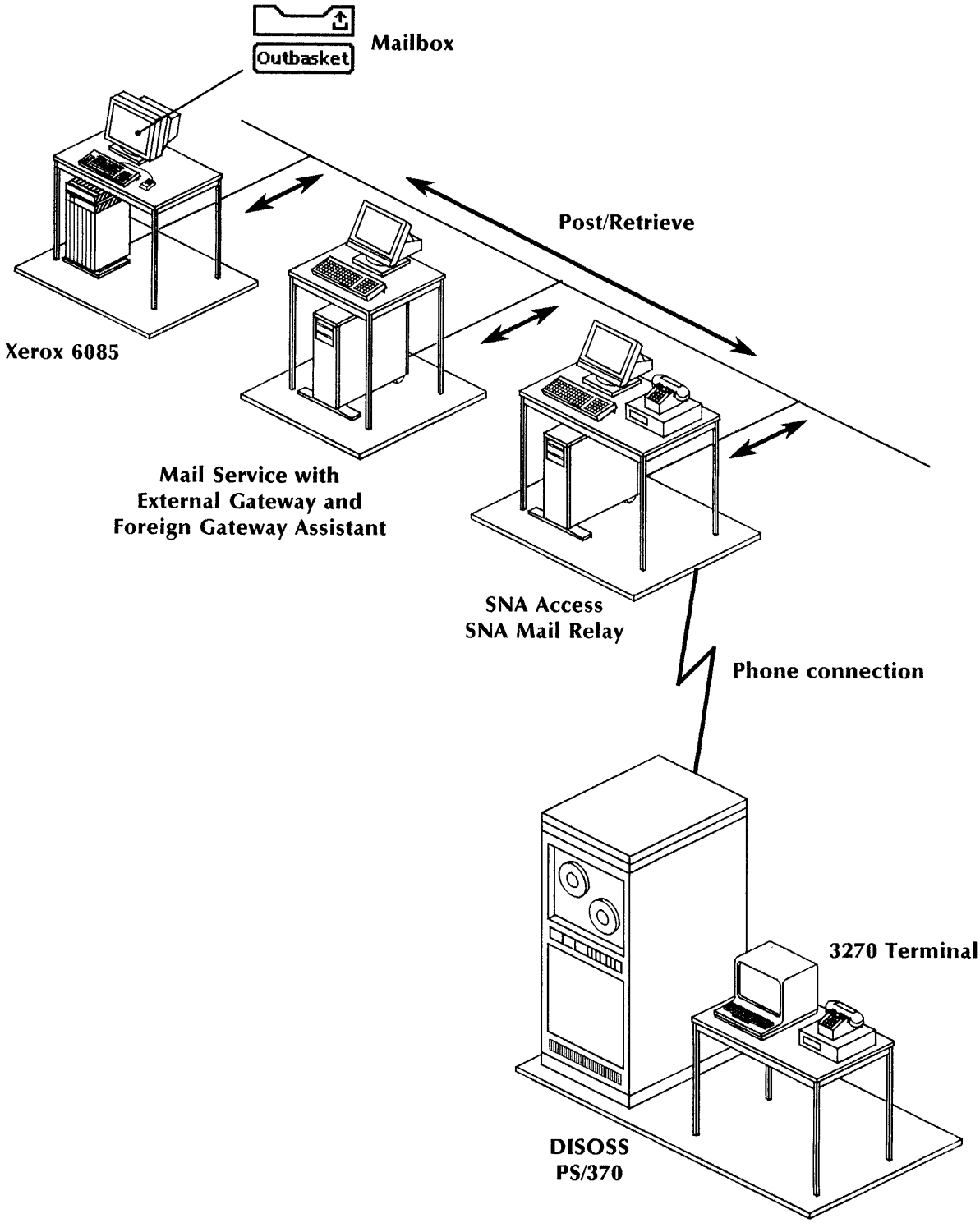
6. The SNA Mail Relay retrieves the mail from its mailbox, converts the recipient name from XNS to SNADS form and the mail note to DCA format, and passes the mail to SNA Access.
7. The SNA Access prepares the mail for delivery, and then sends it to SNADS.
8. SNADS receives the mail and directs it to the mail recipient.

SNADS to XNS

1. The SNADS user prepares a reply and enters the key sequence to deliver the mail note.
2. The DISOSS mail application software places the mail in a forwarding queue for delivery.
3. DISOSS checks the recipient name and forwards it over a phone line to SNA Access, which is actually another node in the SNADS network, even though it is running on a Xerox server.
4. SNA Access receives the mail, removes it from the SNADS package, and makes it available to the SNA Mail Relay.
5. SNA Mail Relay converts mail from DCA format to an XNS mail note and then posts the mail to the Mail Service.
6. The Mail Service forwards the mail to the Mail Service containing the recipient's mailbox.

Figure 11-2 shows the mail route from an XNS environment to an IBM environment.

Figure 11-2. **Mail route from an XNS to SNADS environment**

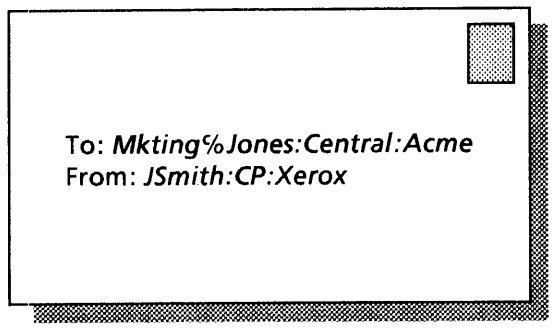


ViewPoint user interface

XNS ViewPoint users should be aware of a few differences between sending mail to an XNS or to a SNADS recipient. Some of the apparent differences include:

- Filling in the "To:" and "Copies:" fields for a SNADS recipient is the same as for an XNS recipient except you must include a percent sign (%) in the first part of the fully qualified name.

Figure 11-3. **Example of addressing mail to a SNADS user**



  - The first part of the XNS fully qualified name maps directly to a SNADS Distribution User Name (DUN).
  - Any characters preceding the percent sign become the SNADS Distribution Group Name (DGN).
  - The characters following the percent sign is the user ID or SNADS Distribution Element Name (DEN).
  - To conform to SNADS requirements, no more than eight characters can precede or follow the percent sign in the first part of the fully qualified name.

- The SNADS network does not have an equivalent to the Clearinghouse Service so SNADS recipient validation is not possible.
- Before a SNADS recipient can read or edit a document created in ViewPoint, the XNS user must first convert it to a DCA document using DCA/VP convertion software.
- XNS users can create groups within the Clearinghouse Service whose members are SNADS recipients or a combination of SNADS and XNS recipients.
- If an error is detected after the mail is forwarded to the SNADS network, an error message is posted to the sender, but the SNA Mail Relay does not return attachments.
- SNADS users cannot use reference icons.

XNS users receiving mail from SNADS users will also notice some differences.

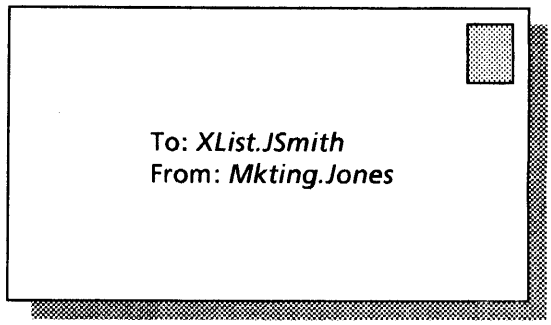
- Mail from SNADS user contains a header delimited by rows of asterisks. This header contains information the SMR uses to return an error message to the sender if the message cannot be delivered.
- When a SNADS user sends a memo without a document, the SNA Mail Relay inserts the first 40 characters of the memo in the mail note's subject field.

SNADS user interface

SNADS users have few limitations and added improvement in service when exchanging mail with XNS users.

- The DUN for an XNS user has the same form as a SNADs user DUN.

Figure 11-4. **Example of addressing mail to an XNS user**



- A SNADS user can ask for Confirmation of Delivery (COD). The SNA Mail Relay confirms only if the message was successfully delivered. If it was not, the SNA Mail Relay sends a status distribution to the SNADS user, indicating the reason for non-delivery.
- The SNA Mail Relay converts XNS mail notes and cover sheets to DCA documents. Attachments are not converted. The SNADS user receives a DCA document containing the complete contents of the cover sheet and a second document containing the attachment. The DCA coversheet document indicates its relationship to the attachment document in its "Subject field."
- SNADS users are not able to password-protect documents.
- SNADS users can send DCA documents without converting them.

ViewPoint file conversion of IBM DCA documents

VP File Conversion of IBM DCA Documents software runs on the 6085 Professional Computer System and the 8010 Information System. It lets the workstation user exchange information with IBM and other systems supporting the IBM DCA file format.

Conversion takes place when the user copies the document to the converter icon on the 6085 or 8010 ViewPoint desktop. There are three types of conversion:

- From RFT/DCA (revisable form text) to ViewPoint format
- From FFT/DCA (final form text) to ViewPoint format
- From ViewPoint to RFT/DCA

ViewPoint/DCA conversion software cannot convert final form text (FFT/DCA). The conversion capability between data icons adheres to the text standards defined in IBM's Document Content Architecture (DCA), and cannot translate incompatible or unrecognizable features.

During conversion, similar characteristics (main body text, headers and footers, tabs, etc.) convert. Dissimilar characteristics (DCA columns, VP tables, DCA footnotes, etc.) convert as best as possible. Non-common characteristics (special symbols, frames, frame captions, etc.) are flagged or ignored. Refer to the VP File Conversion on DCA documents in the VP Reference Library.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Exchanging configuration information with the SNADS Administrator.
- Completing and maintaining the SNA Mail Relay Worksheet located at the end of this chapter.
- Installing the SNA Mail Relay and Foreign Gateway Assistant software as described in the Server Software Installation chapter of the *Services Installation and Setup Guide*.
- Installing the Mail Service and enabling the External Mail Gateway option as described in the Server Software Installation chapter of the *Services Installation and Setup Guide*.
- Setting up the SNA Mail Relay and Foreign Gateway Assistant as described in the SNA Mail Relay chapter of the *Services Installation and Setup Guide*.
- Creating and updating a mailing list of XNS user names, and giving this list to the SNADS Administrator.
- Maintaining your SNA Mail Relay and Foreign Gateway Assistant as described in the SNA Mail Relay chapter of the *Services Maintenance Guide*.
- Troubleshooting the SNA Mail Relay and Foreign Gateway Assistant as described in *Basic Network Troubleshooting*.
- Upgrading hardware and software as necessary.

You can perform most SNA Mail Relay and Foreign Gateway Assistant procedures from a workstation using Remote System Administration (RSA).

Planning for installation

This section explains the hardware, software, and other requirements to prepare for installation. The Server Software Installation chapter in the *Services Installation and Setup Guide* contains the procedures for installing your SNA Mail Relay and Foreign Gateway Assistant software.

Hardware requirements

The SNA Mail Relay requires two XNS servers - one supporting SNA Mail Relay and one supporting the Mail Service and Foreign Gateway Assistant.

The SNA Mail Relay runs on an 8000 server with the following requirements:

- Minimum 768K RAM
- Minimum 42 Mb hard disk
- RS232C Communication Kit or Multiport Option Kit (873 Communications Interface Unit is not supported) installed on the server supporting SNA Mail Relay
- Synchronous modem

The Foreign Gateway Assistant runs on an 8000 or 8090 server and has no unique hardware requirements.

Software requirements

The SNA Mail Relay has these software requirements:

- On the server supporting the SNA Mail Relay:
  - SNA Access, which is automatically installed when the SNA Mail Relay is installed
  - Services System Software must be the same as the version of the SNA Mail Relay
- On the server supporting the Mail Service:
  - Foreign Gateway Assistant (version 10.2 or later)
  - Mail Service (version 10.2 or 10.3) with the External Mail Gateway option enabled

Dependencies and limitations

The SNA Mail Relay has these dependencies and limitations:

- You must install the Foreign Gateway Assistant and the Mail Service (with the External Mail Gateway enabled) on the same server. The Foreign Gateway Assistant cannot be coresident with the Communications Monitoring Service.
- You must install the SNA Mail Relay on a different server.
- The server with the SNA Mail Relay should be on the same network as the servers with the Clearinghouse Service and the Mail Service.

NOTE

It is recommended that the Communications Monitoring Service be the only service coresident with the SNA Mail Relay.

The Foreign Gateway Assistant requires the dedicated operation of the External Mail Gateway option and, in this case, the EMG cannot dial out to Xerox internetworks. A single foreign gateway can support more than one SNA Mail Relay.

SNA Mail Relay Worksheet

Use the SNA Mail Relay Worksheet (pages 1 through 3) to record server-related and service-related information to help you perform setup procedures. The worksheet is at the end of this chapter.

Make a copy of the worksheet for each SNA Mail Relay for which you have System Administration responsibilities. Retain the original worksheet for future use, and the completed worksheets in your *Activities Guide*.

Using the worksheet

Before you install the software on a server and set up the SNA Mail Relay Service, complete the SNA Mail Relay Worksheet. It is important that you fill out the worksheet accurately and update it whenever changes occur.

The completed worksheet saves you time as you perform the setup and maintenance procedures. It also serves as an information source for new System Administrators unfamiliar with your network configuration.

Filling out the worksheet

As you read this chapter, you are directed to make entries on the SNA Mail Relay Worksheet. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and the services installed on the server. If you need more information, see the Services Installation Worksheet in the Services System Software chapter in the *Guide to System Administration Activities*.

Use section ② for information about the RS232C port. Use section ③ for information about the controller. Use section ④ to enter SNADS network information. Use section ⑤ for entering mail link information.

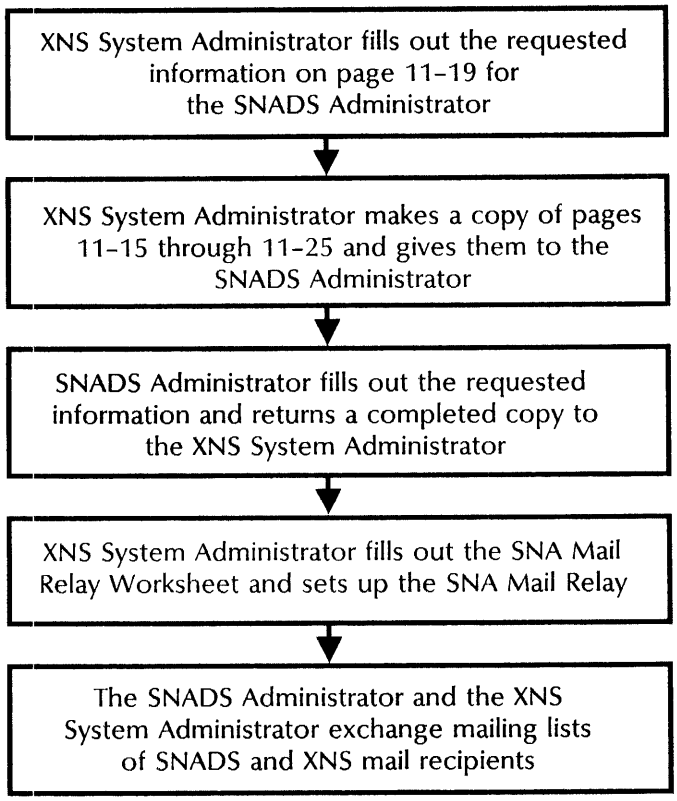
Use section ⑥ on page 2 of the worksheet for XNS domain-to-DGN mappings. Use section ⑦ to record foreign gateway, foreign domain, and foreign gateway mailbox information.

Use section ⑧ on page 3 of the worksheet to record the size of the SNA Mail Relay database. Use sections ⑨ and ⑩ to record mailing list and backup file location.

Planning for setup

Before you can set up the SNA Mail Relay, you need to exchange configuration information with the SNADS Administrator.

The following flowchart describes the interaction between the XNS System Administrator and the SNADS Administrator in setting up the SNA Mail Relay.



Information for the XNS System Administrator

This section contains two questionnaires. You fill out the first questionnaire to define your modem and phone line. The SNADS Administrator fills out the second questionnaire to define the SYSGEN parameters you need to complete the SNA Mail Relay Worksheets.

- Fill out the questionnaire on page 11-19 that describes your modem and phone line.
- List the XNS domains and organizations that will be using the SNA Mail Relay on page 11-19.
- Make a copy of pages 11-15 through 11-25 and give it to the SNADS Administrator.

After you receive the filled-in questionnaire from the SNADS Administrator, proceed to the "Setting up the SNA Mail Relay" section on page 11-26.

Information for the SNADS Administrator

This section, pages 11- 15 through 11-25, is intended for the SNADS Administrator.

This document allows you to exchange information with the XNS System Administrator. Fill out the questionnaire on page 11-18 and return a copy to the XNS System Administrator. The information is used by the XNS System Administrator to complete the setup of the SNA Mail Relay.

The XNS System Administrator is installing a SNADS mail gateway on a Xerox server to communicate with DISOSS. The Xerox server uses a phone line and synchronous data link control (SDLC) protocol and these two XNS products: the SNA Mail Relay to convert mail, and the SNA Access to provide a SNADS transaction program and LU 6.2 and SDLC support.

It is recommended that the SNA Access be viewed as a System/36 with two logical units (LUs), one for sending and one for receiving. For your information:

- SNA Access is a Type 2.0 node
- SNA Access has single-session LUs of Type 6.2 (base subset only)
- SNA Access LUs cannot accept unsolicited BINDS
- SNA Access is a Distribution Service Unit without intermediate routing capabilities
- SNA Access SNADS transaction program is compatible with CICS version 1.6 or 1.7, and DISOSS version 3.1, 3.2 or 3.3.

You need to perform these tasks so the XNS System Administrator can set up the SNA Mail Relay Service:

- Update your tables and files as required.
- Fill out the questionnaire (page 11-18) that defines your SNADS configuration.

- List the DGNs that will map to the XNS domains (page 11-19).
- List the addresses for the SNADS users (page 11-20).
- Return a copy of the completed questionnarie, the list of DGNs, and addresses of SNADS users to the XNS System Adminitrator.

Updating tables and files

The following information should assist you in making updates to these tables and files:

- CICS/VS Terminal Control Table (TCT)
  - Set the TRMTYPE field to LUTYPE62
  - Make sure the SYSIDNT field matches the QUEUE field of the DISOSS Routing Table
- ACF/NCP line definitions
- ACF/VTAM PU and LU definitions
- DISOSS Host User Profile (HUP)
  - Set the DGN field to the DGN that the XNS System Administrator defined for the SNA Mail Relay Service
  - Set the SA field to *
  - Set the USERTYPE field to remote
- DISOSS SNADS Routing Table
  - Set the SSL to *
  - Set TRANSID to DSVE
  - Set the QUEUE field to match the SYSIDNT field of the CICS TCT entry whose NETNAME field specifies the local receiving LU
  - Do not put the QUEUE entry for the local sending LU in the DISOSS Routing Table

Filling out the questionnaire

Figure 11-5 assists you in matching the parameters the XNS System Administrator needs with the corresponding SYSGEN parameters. There is an example of SYSGEN parameters on pages 11-21 through 11-25.

The answers you provide on the following questionnaire is used by the XNS System Administrator to complete the set up of the SNA Mail Relay.

Figure 11-5. **SBS-SYSGEN Parameters**

SNA Access Parameters	Corresponding SYSGEN Parameters
Data encoding type	NZRI parameter in NCP LINE macro
SDLC station or link address	ADDR parameter in VTAM PU macro
XID number	Concatenation of IDBLK and IDNUM parameters in VTAM PU macro
MAXDATA PIU size	MAXDATA parameter in VTAM PU macro
LU name (controller)	VTAM LU macro label and NETNAME parameter in CICS TCT macro
LU address (controller)	LOCADDR parameter in VTAM LU macro
RGN for Xerox server	RGN in DISOSS Routing Table and DISOSS HUP
REN for Xerox server	REN in DISOSS Routing Table and DISOSS HUP
Names of local (XNS) sending and receiving LUs	VTAM LU macro label and NETNAME parameter in CICS TCT macro
Names of remote (host) sending and receiving LUs	APPLID in CICS TCT
Mode names for sending and receiving	LOGMODE entry in VTAM Mode Entry (MODEENT) Tables

Questionnaire to be filled out by the SNADS Administrator

Information you give to the XNS System Administrator:

Data encoding type (NRZ or NRZI) _____

Phone number to host _____

XID number (for switched lines only) _____

SDLC station or link address _____

MAXDATA (PIU size) _____

Local LU name (sending) _____

Local LU address (sending) _____

Local LU name (receiving) _____

Local LU address (receiving) _____

RGN for host _____

REN for host _____

RGN for Xerox server _____

REN for Xerox server _____

LOGMODE entry in the VTAM MODEENT Table for sending a pacing value from 1 to 8)

_____

LOGMODE entry in the VTAM MODEENT Table for receiving a pacing value from 1 to 8)

_____

LU name for sending to an XNS network (corresponds to the DISOSS APPLID entry in the CICS TCT)

_____

LU name for receiving from an XNS network (corresponds to the DISOSS APPLID entry in the CICS TCT)

_____

Number of nodes in network _____

DIA document types _____

_____

_____

The SNA Mail Relay automatically maps between file types and document types for RFT and FFT DCA documents. In order for a document to pass through the IBM environment without being converted to DCA, fill in the hexadecimal number fo the various XNS file and document types. The XNS System Administrator enters the hexadecimal numbers at the time of SNA Mail Relay installation.

For IBM (DIA) document types other than DCA documents, see *Document Interchange Architecture Technical Reference PGM # 5743-DIA*, order number SC23-0781-0.

Questionnaire to be filled out by the XNS System Administrator

Synchronous modem manufacturer name and model _____

Data rate in bits per second (max. of 9.6) _____

Half or full duplex mode _____

Switched or dedicated phone line _____

Continuous or non-continuous connection _____

Establish connection between the hours of _____ and _____

Creating DGNS for the XNS System Administrator

You need to give the XNS System Administrator a list of DGNs that map to Xerox domains. The XNS System Administrator will then supply you with a mailing list of aliases for each XNS user.

Fill out the DGN information for each XNS domain, and return a completed copy to the XNS System Administrator. A DGN can be mapped to only one XNS domain. The XNS domain information is supplied by the XNS System Administrator.

Figure 11-6. **DGN-to-XNS domain mappings**

DGNs	XNS domains

Creating a mailing list for the XNS System Administrator

Prepare a mailing list of SNADS user names with whom XNS users can exchange mail. List each SNADS user name for each DGN in the form provided below.

To create an address for a SNADS user: Record the DGN that maps to a foreign domain, insert a percent sign %,, and add the DEN (user ID). For example, assume the DGN "Sales" maps to the foreign domain "Phone Sales:San Diego." The complete address for the SNADS user might look like:

Sales%Smith:Phone Sales:San Diego

The foreign domain name is provided by the XNS System Administrator.

Figure 11-7. **Mailing list for XNS System Administrator**

DGN%[DEN]:[foreign domain]

Make a copy of this completed form and give it to the XNS System Adminitrator. At the same time, the XNS System Adminitrator should provide you with a list of XNS user names to whom SNADS users can send mail.

Sample SYSGEN parameters

The following pages contain excerpts from a SYSGEN that was used by a DISOSS host to communicate with the SNA Mail Relay. The parameters displayed here are intended as examples only. Specific parameters will vary among different installations.

The Table below lists the host data sets and tables that must be modified to allow communication with the SNA Mail Relay.

Table 11-3. **Host tables and data sets**

Host program	Data set or table
DISOSS	Routing table, HUP
CICS	PCT, TCT
ACF/VTAM	APPLID, LOGMODE table, PU and LU macros
ACF/NCP	Line definitions

The parameters for the SNA Mail Relay are the same as the parameters for a System/36, with the exception that there are two, single-session LUs, one for sending, one for receiving.

```
*************************************************************************
*  NCP LINE DEFINITION (SWITCHED LINE CONNECTED TO MPOK PORT THAT USES
*  NRZI DATA ENCODING)
*************************************************************************
L22SO3E     LINE   ADDRESS=(03E), 408/555-1212
                NRZI=YES,                NRZI MODE
                ISTATUS=ACTIVE           INITIAL STATUS OF LINE

*************************************************************************
*  VTAM PU and LU MACROS
*  SWITCHED NETWORK DEFINITION - REMOTE SYSTEM 36 CONNECTION
*************************************************************************
DIALS36  VBUILD TYPE=SWNET
*
DSXR36PU    PU     ADDR=C1,
                   IDBLK=03E,
                   IDNUM=00103,
                   MAXDATA=265,
                   MAXOUT=7,
                   PACING=7,
                   PASSLIM=7,
                   PUTYPE=2,
                   DISCNT=NO,
                   IRETRY=YES,
                   ISTATUS=ACTIVE,
                   MODETAB=DSVMODE, DLOGMODE=S36CONFIG
                   SSCPFM=USSSCS
                   BATCH=NO
                   VPACING=7
*
DSX36LU1    LU     LOCADDR=1,
                   ISTATUS=ACTIVE,

*
DSX36LU2    LU     LOCADDR=2,
                   ISTATUS=ACTIVE,
```

```
*************************************************************************
*  VTAM APPLICATION IDENTIFICATION
*
*************************************************************************
DISOSAPL VBUILD TYPE=APPL
DISOSS72 APPL ACBNAME=DISOSS72,       MUST MATCH HOSTID PARM IN HOSTDEF *
               AUTH=(ACQ,VPACE),      AND TCT ENTRY IN THE REMOTE HOST  *
               EAS=64,                                                  *
               MODETAB=DSVMODE,                                         *
               VPACING=3,                                               *
               PARSESS=YES,                                             *
               SONSCIP=YES


*************************************************************************
*  VTAM LOGMODE TABLE ENTRY - BIND FOR SYSTEM 36 LU'S
*
*************************************************************************
S36MODE    MODEENT  LOGMODE=S36CONFIG  MUST MATCH NCP LU DLOGMOD OPERAND
           MODENED
           END

*************************************************************************
*  CICS PCT
*
*************************************************************************
       DFHPCT  TYPE=PROFILE,
                  PROFILE=S36PROF1,
                  JFILEID=SYSTEM,
                  MODENAM=S36CONFIG,
                  MSGJRNL=(INPUT,OUTPUT)
       DFHPCT  TYPE=FINAL
       END
```

```
*************************************************************************
*  CICS TCT
*
*************************************************************************
    DSX36LU1    DFHTCT TYPE=SYSTEM,
                   SYSIDNT=S36XRX1,
                   NETNAME=DSX36LU1,
                   TRMTYPE=LUTYPE62,
                   FEATURE=SINGLE,
                   MODENAM=S36CONFIG
                   RELREQ=(YES,YES),
                   ACCMETH=VTAM,
                   BUFFER=256,
                   RUSIZE=256,
                   TRMSTAT=TRANSCEIVE
    *
    DSX36LU2    DFHTCT TYPE=SYSTEM,
                   SYSIDNT=S36XRX2,
                   NETNAME=DSX36LU2,
                   TRMTYPE=LUTYPE62,
                   FEATURE=SINGLE,
                   MODENAM=S36CONFIG
                   RELREQ=(YES,YES),
                   ACCMETH=VTAM,
                   BUFFER=256,
                   RUSIZE=256,
                   TRMSTAT=TRANSCEIVE
```

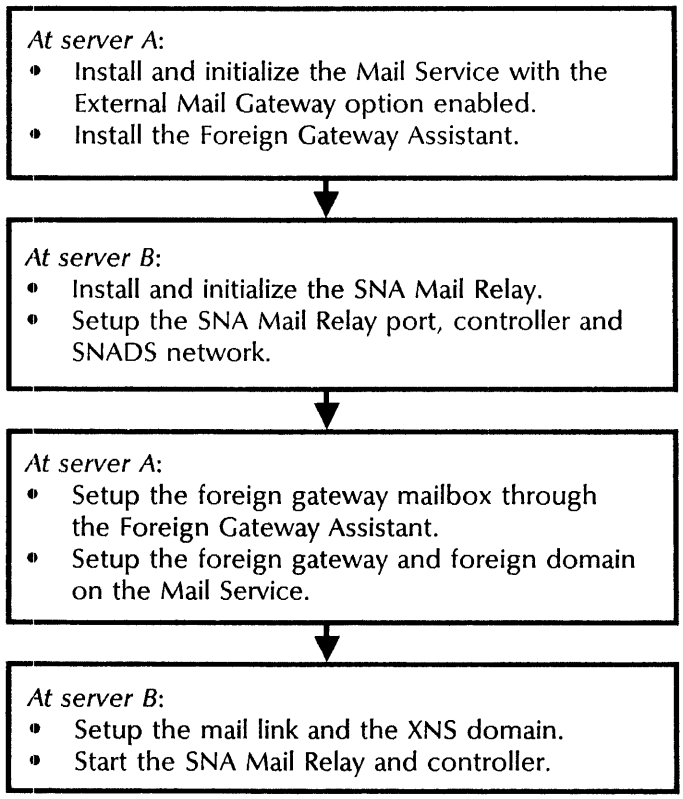
```
*****************************************************************************
*  DISOSS HUP FOR S36 USER "DSXR36PU"
*
*****************************************************************************
   ADD USERTYPE=REMOTE,
       RGN=DISHOSTA,
       SA=*,
       DDN=XRXGROUP,
       REN=SYS36XRX
 *     ACCESS=1048,
 *     REQPWD=3333333
 *

-----------------------------------------------------------------------------
QUALIFIED NAME  PASSWORD                    USER DATA
-----------------------------------------------------------------------------

XRXGROUP.*     XRXS36  RGN=DISHOSTA  REN=SYS36XRX            OBTAINID=
                                     SIDC=  OPNO=  REQNAME=      REQID=  LOCATION=
                                     ACCOUNT=                     TRANID=     USERTYPE=REMOTE
                                     NCIPDT= TEXTPDT=    NCINAME=    GROUP=  DEFNAME=YES
                                     NODISTR=NO EXTERN=NO   EXTERNAL=
                                     ACCESS=  100TO 199

*****************************************************************************
*  DISOSS ROUTING TABLE
*
*****************************************************************************
    RGN            REN            SSL            TRANSID            QUEUE
    ===            ===            ===            =======            =====

    DISHOSTA       SYS36XRX        *             DSVE               S36XRX1
```

Setting up the SNA Mail Relay

Make sure you have the completed questionnaire from the SNADS Administrator before continuing.

You perform the procedures for installing and setting up the SNA Mail Relay and the Foreign Gateway Assistant on two servers: one server supports the SNA Mail Relay, and one server supports the Foreign Gateway Assistant and the Mail Service with the External Mail Gateway enabled.

The flowchart shows the sequence of the steps required to complete installation and setup. The process involves going from one server to the other:



For the complete installation procedures see the Services Software Installation chapter of the *Services Installation and Setup Guide*.

See the SNA Mail Relay chapter and the Mail Service chapter of the *Services Installation and Setup Guide* for the complete setup procedures.

Naming the SNA Mail Relay

During initialization you enter the service name and description of the SNA Mail Relay.

Related procedure: Initializing the SNA Mail Relay

Filling out the worksheet

Use page one of the SNA Mail Relay worksheet to fill in the following information:

① Record the name for the SNA Mail Relay. You can use up to 40 characters. It is recommended that you include the server's name in the service name.

The domain and organization default to that of the server, unless you specify a different domain and organization name. Include the domain and organization names in the space provided.

Do not use commas, parentheses, asterisks, or pound signs in a service name.

Optionally, record the SNA Mail Relay description. You can use up to 100 characters for the SNA Mail Relay description.

Setting up the SNA Mail Relay

This includes information regarding the RS232C port, controller, SNADS network, mail link and XNS domains. Some of this information is supplied by the SNADS Administrator. Make sure you have the completed copy of the questionnaire from the SNADS Administrator before continuing.

RS232C port

The SNA Mail Relay supports the RS232C standard for serial communication through either the RS232C Communication Kit (port 0 only), or the Multiport Option Kit, which provides four ports.

Both communications options support manually dialed or autodialed capability. Manual dialing is supported on a single port, and through any of the four ports available on a Multiport Option Kit. Autodialing is supported on a single port, and only thorugh port 0 on the multiport option.

Related procedure: Adding the port, controller, and SNADS network

Filling out the worksheet: Use page one of the SNA Mail Relay Worksheet to record the following information:

② **Port number** - Record the number of the port the SNA Mail Relay is using. If your server is equipped with the RS232C Communications Kit, only port 0 is available. If you intend to use autodialing, you must select port 0.

Port name - Record the name of the port. You can use up to 40 characters. It is helpful to include the port number in the name, if you have more than one port.

Port description - Record a comment that describes the purpose of the port. You can use up to 100 characters. This field is optional.

Access - Circle either dedicated or switched to identify the type of phone access. Select switched only if you are using either autodialed or manually dialed lines.

Autodialer hardware - Record whether the modem has autodialer hardware. The SNA Mail Relay supports only RS366 autodialing. Check your modem for autodialing specifications.

NRZ or NRZI - Record the encoding protocol (either NRZ or NRZI). Xerox servers equipped with the Multiport Option Kit can accept either type of data encoding. Servers equipped with the RS232C Communication Kit can accept only NRZ encoding. The encoding protocol information is supplied by the SNADS Administrator.

Half or full duplex - Record whether the modem is full or half duplex. Full duplex indicates the modem can transmit data in both directions at the same time. Half duplex indicates the modem can transmit data in both directions, but not at the same time. The port must be configured for half duplex if a multi-drop line is being used. Check your modem specifications.

Controller

Most of the controller information needed for setting up the SNA Mail Relay is supplied by the SNADS Administrator.

Related procedure: Adding the port, controller, and SNADS network

Filling out the worksheet: Use page one of the SNA Mail Relay Worksheet to record the following information:

③ **Name** - Record the controller name. You can use up to 40 characters. Create a name that identifies the host and refers to the SNA Access server name.

Description - Record the controller description. You can use up to 100 characters. This field is optional; you can use it to describe the applications using the controller.

Port name - Record the name of the RS232C port in use. The name should match the RS232C port name you entered in section ② of the worksheet.

Autostarted - Record whether the controller should be started when the server is rebooted. You should autostart the controller if you have a dedicated or autodialed line. In the event of a communication break, the controller restarts and returns to the state prior to the break. You cannot autostart a manually dialed line.

Host phone number - Record the telephone number for the host. This number is supplied by the SNADS Administrator and is required only if you have a switched line. Indicate the area code if different than yours, and whether 9 (or other digits) must be dialed to obtain an outside line.

If you are using an autodialed line, the SNA Access uses this number to dial the host. If you are using a manually dialed line, the SNA Access displays this number for you to dial.

XID number - Record the eight-digit hexadecimal number for the XID (Exchange ID). The XID allows the host to identify the SNA Access over the phone line. This number is required only if you have switched lines. This information is supplied by the SNADS Administrator.

The XID number has two parts: the block number (the first three digits) and the station identifier (the last five digits). The block number identifies the controller device to the host. For example, 018 identifies the controller as a 3276 cluster controller and 03E identifies the controller as a System/36. The station number assignment uniquely identifies controllers of the same type.

SDLC number - Record the two-digit hexadecimal number for the SDLC. This is a station or link address for the controller that identifies the number of frames exchanged between the controller and the host. This information is supplied by the SNADS Administrator.

MAXDATA number - Record the decimal number for MAXDATA. Refers to the maximum size for a data block; 265 is recommended. This information is supplied by the SNADS Administrator.

The MAXDATA size for all additional controllers should be the same as the first controller, and must NOT be greater than that given for the first controller.

LU name - There are two types of local logical unit (LU) names and addresses you specify: one for sending and one for receiving. Record the name (up to eight characters) of the local LU used for sending. This information is supplied by the SNADS Administrator.

LU address - Record the two-digit hexadecimal number for the address of the local sending logical unit. This number lets the host identify a logical unit within a controller and is supplied by the SNADS Administrator.

Local LU name - Record the name (up to eight characters) of the local LU used for receiving. This information is supplied by the SNADS Administrator.

Local LU address - Record the two-digit hexadecimal number for the address of the local receiving logical unit. This number lets the host identify a logical unit within a controller and is supplied by the SNADS Administrator.

SNADS network

Most of the SNADS network information you need to set up the SNA Mail Relay is supplied by the SNADS Administrator. This includes information about communication between the SNA Access and the host.

Related procedure: Adding the port, controller, and SNADS network

Filling out the worksheet: Use page one of the SNA Mail Relay Worksheet to record the following information:

④ **Name** - Record name of the SNADS network. You can use up to 40 characters. Create a name that refers to the host or SNADS network with which you are exchanging mail. The SNA Mail Relay associates this name with the name of the Xerox foreign domain.

RGN of host - Record the Routing Group Name of the host. This name can be up to eight characters in length.

REN of host - Record the Routing Element Name of the host. This name can be up to eight characters in length.

The host RGN and REN together form the address of a computer in a SNADS network. The computer is called a Distribution Service Unit (DSU). The address is referred to as a DSUN. The RGN and REN are supplied by the SNADS Administrator.

RGN of XNS server - Record the RGN of the server supporting SNA Mail Relay. This name can be up to eight characters in length.

REN of XNS server - Record the REN of the server supporting SNA Mail Relay. This name can be up to eight characters in length.

The Xerox RGN and REN identify the SNA Access server as a DSU in a SNADS network. When one SNA Access server has connections to two SNADS networks, you can use the same RGN and REN as long as they are unique entries within each network.

Controller name - Record the name of the controller for sending and receiving. This is the same controller name you entered in section ③ of the worksheet.

Local sending LU name - Record the logical unit (LU) name for sending to a SNADS network. This is the sending logical unit name you entered in section ③ of the worksheet.

LOGMODE for sending - Record the LOGMODE for sending to a SNADS network. This name can be up to eight characters in length and is optional.

Local receiving LU name - Record the logical unit name for receiving from a SNADS network. This is the receiving logical unit name you entered in section ③ of the worksheet. An SNA Access LU must be dedicated to either sending or receiving.

LOGMODE for receiving - Record the LOGMODE for receiving from a SNADS network. This name can be up to eight characters in length and is optional.

Remote sending LU name - Record the remote logical unit name for sending to a SNADS network. This name can be up to eight characters in length. The host may use a single LU for both sending and receiving.

Remote receiving LU name - Record the remote logical unit name for receiving from a SNADS network. This name can be up to eight characters in length. The host may use a single LU for both sending and receiving.

Number of hops - Record the maximum hops for delivery. Multiply by two the number of nodes in the SNADS network obtained from the SNADS Administrator to calculate the total.

24-hour connection - Record whether you want a continuous 24-hour connection to the host. If you want to establish a number of connection intervals within a 24-hour period, indicate "N." You can specify up to 30 intervals.

Start time - Record the start time of the connection interval only if you are not establishing a continuous 24-hour connection to the host. Enter the number in the HH:MM format.

Length - Record the length of the connection interval. Enter the number in the HH:MM format.

Mail link

Most of the mail link information you need to set up the SNA Mail Relay is supplied by the SNADS Administrator. This information includes the SNADS network name, XNS domains and DIA document types.

You need to specify document types only if you want ViewPoint documents and folders, and 860 documents to retain their Xerox characteristics when going from the XNS to SNA and back to the XNS environment; and if SNADS users need to make a distinction between different types of XNS documents.

It is not always necessary to establish mappings for file and document types. If no mappings are specified, a document might return with a different file type than when it started.

If you choose to establish mappings between XNS file and SNA document types:

- Enter the hexadecimal number for the document type as given to you by the SNADS Administrator.
- Communicate with other XNS System Administrators connected to the SNADS network to ensure the file type/document type mappings are uniform across connected networks.
- Establish these mappings for each SNADS network with which an XNS network exchanges mail. If the SNA Mail Relay is linking an XNS network to two SNADS networks, you use the same mappings for both SNADS networks.

Related procedure: Adding the mail link and XNS domain-to-DGN mappings

Filling out the worksheet: Use page one of the SNA Mail Relay Worksheet to record the following information:

⑤ **SNADS network name** - Record the SNADS network name you entered in section ④ of the worksheet.

Foreign domain name - The XNS foreign domain name is the same name you use when setting up the foreign domain. You will be asked to record this name later.

DIA for VP documents - Depending on mail recipient requirements, you accept the default for this entry at the time of setup, or enter the information given to you by the SNADS Administrator.

DIA for VP folders - Depending on mail recipient requirements, you accept the default for this entry at the time of setup, or enter the information given to you by the SNADS Administrator.

DIA for 860 documents - Depending on mail recipient requirements, you accept the default for this entry at the time of setup, or enter the information given to you by the SNADS Administrator.

DIA for XNS documents - Record 0 to specify the default document type.

Other XNS file types - Record additional DIA document types for other XNS file types. These file types are common to the ViewPoint environment:

0	Unspecified
1	Folder
2	tText
3	Serialized
4	Mail note
4098	File drawer
4101	Binary file
4226	BravoText
4230	XDE bcd file
4290	Print Service fonts
4352	Desktop
4353	Star Document
4355	Inbasket
4360	Outbasket
4361	Interpress master
4365	Record file
4379	Reference icon
5120	860 document

DIA for other file types - Record any other document types supplied by the SNADS Administrator.

XNS domain-to-DGN mappings

The XNS domain and Distribution Group Name (DGN) information is gathered from both the XNS System Administrator and the SNADS Administrator. Make sure you have the completed form, Figure 11-6 from the SNADS Administrator.

To allow mail exchange between XNS and SNADS users, you provide mappings between XNS domains and SNADS networks. The mappings are different in each direction.

For mail exchange in the SNADS-to-XNS direction, you provide mappings between DGNs and XNS domains. You have one DGN for every XNS domain receiving mail from SNADS users, and one XNS domain for every DGN.

There are some instances where you may have more than one XNS domain mapped to a DGN. See the "Mapping additional XNS domains to an existing SNADS network" section in the "Planning for maintenance" area later in this chapter.

In the XNS-to-SNADS direction, you provide one foreign domain-to-SNADS mapping for each SNADS network with which you are communicating.

You can have up to 63 XNS domains mapped to DGNs for each server supporting the SNA Mail Relay Service.

Related procedure: Adding the mail link and XNS domain-to-DGN mappings

Filling out the worksheet: Use page two of the SNA Mail Relay Worksheet to record the following information:

⑥ **DGNs** - Record the DGN for the XNS domain. The DGN is supplied by the SNADS Administrator.

XNS domains - Record the XNS domain name of users who are exchanging mail with SNADS users. Include the domain and organization name.

Setting up foreign gateway and foreign domains

You provide the information regarding foreign gateways and foreign domains at the server supporting the Mail Service with the External Mail Gateway enabled. See the Mail Service chapter in this book for more information.

Even though phone number and calling interval are entered as part of setup, the system does not use this information. In addition, the fictitious calling interval must be deleted when you change the foreign gateway.

Related procedure: Adding the foreign gateway, mailbox, and foreign domain

Filling out the worksheet

Use page two of the SNA Mail Relay Worksheet to record the following information:

⑦ **Phone number** - Record a fictitious phone number for the foreign gateway. The phone number is entered as part of setting up the foreign gateway, but is not used.

Start time and length - Record the start and length of the calling interval as 00:00. The calling intervals are entered as part of setting up the foreign gateway, but are not used.

Name - Record the domain and organization name for the foreign domain. You can use up to 20 characters for the domain name and for the organization name. Choose a name that relates to the SNADS network to which the SNA Mail Relay directs mail. Also, record this information in the "Foreign domain name" field in section ⑤.

Phone number - Record the fictitious phone number for the foreign gateway that you entered above.

Setting up the foreign gateway mailbox

You provide the information regarding the foreign gateway mailbox at the server supporting the Mail Service.

Related procedure: Adding the foreign gateway, mailbox, and foreign domain

Filling out the worksheet

Use page three of the SNA Mail Relay Worksheet to record the following information:

⑦ Record the fully qualified name of the mailbox. This is the fully qualified name for the SNA Mail Relay. See section ① of the SNA Mail Relay Worksheet.

Setting the database size

SNADS-to-XNS mail is stored in the SNA Mail Relay database as long as it takes to convert the mail and post it to an XNS Mail Service. However, all XNS-to-SNADS mail is stored for 48 hours from the time it is forwarded.

You need to specify a database size to limit the amount of hard disk space the SNA Mail Relay can use. Services that are coresident with the SNA Mail Relay are not restricted by the size of the SNA Mail Relay database in the amount of disk space they use.

It is recommended that you enter the maximum number of disk pages available on the services volume.

Related procedure: Adding the mail link and XNS domain-to-DGN mappings

Filling out the worksheet

Use page three of the SNA Mail Relay Worksheet to record the following information:

⑧ **Number of disk pages** - Record the number of disk pages you want to allow for the database. The maximum space available in the services volume depends on the size of the hard disk. The following is a list of the approximate disk pages available for the size of a hard disk, if no other services are installed:

Hard disk size	*Disk pages*
42	52,000
80	106,000
300	433,000

Creating a mailing list for the SNADS Administrator

After installing and setting up the SNA Mail Relay, prepare a list of XNS user names to whom SNADS users can send mail. Upon completion, make a copy of the list and give it to the SNADS Administrator. At the same time, the SNADS Administrator should provide you with a list of SNADS user names to whom XNS users can send mail.

Filling out the worksheet

Use page three of the SNA Mail Relay Worksheet to record the following information:

⑨ **Mailing list** - Record the address for each XNS user in each XNS domain mapped to a Distribution Group Name (DGN). Make sure the alias or user name is eight characters or less in length.

To do this, take the DGN that maps to a Xerox domain, insert a period, and add the user name or alias. For example, assume the DGN "Sales" maps to the XNS domain "Phone Sales:San Diego." The address of an XNS user in the Phone Sales:San Diego domain might look like:

Sales.Perkins

Planning for maintenance

After you install and set up the SNA Mail Relay and Foreign Gateway Assistant, you are responsible for maintaining them. You perform maintenance as needed; there are no scheduled duties.

This section enhances your understanding of SNA Mail Relay and Foreign Gateway Assistant maintenance. See the SNA Mail Relay chapter in the *Services Maintenance Guide* for complete maintenance procedures.

The maintenance information and procedures for the Mail Service are described in the Mail Service chapter of this book and the *Services Maintenance Guide*.

Changing the database size

You can make the database smaller or larger, although you must attribute a minimum of 2,000 disk pages.

It is recommended that you enter the maximum number of disk pages available on the services volume.

Adding a new SNADS network

On a server equipped with a Multiport Option Kit (four RS232C ports), the SNA Mail Relay can support connections to two SNADS networks. Adding a new SNADS network connection involves many of the steps taken to install the SNA Mail Relay the first time.

Before you add a new SNADS network, do the following:

- Make a copy of the SNA Mail Relay Worksheet to assist you in acquiring the information you need, and refer to the "Planning for setup" section in this chapter.
- Obtain the DGN from the SNADS Administrator for every new XNS domain.
- Use the Mail Service command to list foreign domains to view the phone number for the foreign gateway. This is the phone number you use to add the new foreign domain(s) mapped to the new SNADS network.
- Establish XNS file type to DIA document type mappings, if required.

After adding the new SNADS network, wait 24 hours for the new foreign domain name to propagate to other Clearinghouse Services on the network before notifying users of the availability of the new SNADS network. In addition, exchange mailing list information with the SNADS Administrator regarding SNADS and XNS recipient names.

Related procedure: Moving the SNA Mail Relay

Mapping an additional XNS domain to an existing SNADS network

You can map an additional XNS domain to an existing SNADS network by adding the new domains to the XNS domain-to-DGN mapping table, and having the SNADS Administrator modify the host user profile (HUP).

You add the new XNS domain to the mapping table using the SNA Mail Relay **Add XNS Domains** command at the server where the SNA Mail Relay is installed. The new XNS domain is mapped to the new DGN. The SNADS Administrator then adds the new DGN to the existing HUP.

This example illustrates a sample HUP before the new DGN is added by the SNADS Administrator. By specifying DEN = * and UserType = Remote, a set of users is defined with the same DGN.

Table 11-4. **Existing HUP**

DGN	DEN	RGN	REN	Usertype
Mkting1	*	Acme	SEA1	Remote

This example illustrates the HUP after the new DGN is added.

Table 11-5. **Edited HUP**

DGN	DEN	RGN	REN	Usertype
Mkting1	*	Acme	SEA1	Remote
Mkting2	*	Acme	SEA1	Remote

Mail addressed to 'Mkting2.user' is routed through the existing RGN/REN, and then forwarded to the SNA Mail Relay where the Mkting2 DGN is converted to its corresponding XNS domain.

Related procedure: *Services Installation and Setup Guide:* Adding the mail link and XNS domain-to-DGN mappings

Removing an existing SNADS network

You can terminate the SNA Mail Relay connection to a specific SNADS network. It does not affect a connection to another SNADS network supported by the SNA Mail Relay.

Before you delete an existing SNADS network, do the following:

- Make a copy of the SNA Mail Relay Worksheet to assist you in acquiring the information you need, and refer to the "Planning for setup" section in this chapter.
- Let XNS users know that the foreign domain mapped to the SNADS network is no longer accessible.
- Have the SNADS Administrator inform SNADS users in DGNs served by the foreign domain that the foreign domain is no longer accessible.

- Wait 12 hours to allow any mail in transit to be delivered before deleting the SNADS network.
- Delete any XNS domains that do not need to exchange mail with the SNADS network.

If the SNA Mail Relay supports more than one SNADS network, delete the XNS domains that are mapped only to the SNADS network you intend to delete.

- Delete associated controller information.

Then make necessary changes to domain-to-DGN mappings. In addition, exchange mailing list information with the SNADS Administrator regarding SNADS and XNS recipient names.

Related procedures: Displaying mail links, XNS domains, and SNADS networks, Deleting XNS domain-to-DGN mappings, Deleting the controller and RS232C port

Modifying domain-to-DGN mappings

You can change domain-to-DGN mappings. These mappings usually change only when a connection to a SNADS network is added or deleted.

Before you add or delete existing domain-to-DGN mappings, do the following:

- Make a copy of the SNA Mail Relay Worksheet to assist you in acquiring the information you need, and refer to the "Planning for setup" section in this chapter.
- Let XNS users know that the domain mapped to the DGN is no longer accessible.
- Have the SNADS Administrator inform SNADS users that the DGN mapped to the XNS domain is no longer accessible.
- Wait 12 hours to allow any mail in transit to be delivered before changing the domain-to-DGN mapping.

Then exchange mailing list information with the SNADS Administrator regarding SNADS and XNS recipient names.

Related procedures: Displaying mail links, XNS domains, and SNADS networks, Changing XNS domain-to-DGN mappings

Modifying XNS file type-to-DIA document types

You can add or delete new XNS file type-to-DIA document types when you add or change a mail link. Mappings are required if XNS documents must maintain the same file type after going to the SNADS network and back, or if SNADS users need to distinguish among different types of XNS documents. If no mappings are specified, a document could return with a different file type than the one with which it originated.

Make a copy of the SNA Mail Relay Worksheet to assist you in acquiring the information you need, and refer to the "Planning for setup" section in this chapter.

Related procedure: Changing XNS file-to-IBM document mappings

Relocating the SNA Mail Relay

Moving the SNA Mail Relay from one server to another involves backing up the server profile information, expunging the SNA Mail Relay from one server, installing the SNA Mail Relay on another server, and restoring the server profile information. This process lets you retain the SNA Mail Relay name, server name, configuration information, and database size.

NOTE

Do not wait longer than two hours between expunging and reinstalling the SNA Mail Relay. Within 24 hours of the removal of the SNA Mail Relay, the Mail Service automatically deletes the expunged SNA Mail Relay mailbox. If this occurs, use the command to add the foreign gateway mailbox to create a new mailbox.

Before you move the SNA Mail Relay, make a copy of the SNA Mail Relay Worksheet (page 1 through 3) to assist you in acquiring the information you need, and refer to the "Planning for setup" section in this chapter.

Related procedure: Moving the SNA Mail Relay

Backing up/restoring server profile

The commands to backup and restore the SNA Mail Relay server profile are used when moving the SNA Mail Relay to another server.

Before you move the SNA Mail Relay, add a file drawer on a remote File Service to store the backup copy of the SNA Mail Relay server profile. See the procedure "Creating private file drawers for use" in the File Service chapter of the *Services Installation and Setup Guide*.

- Use a name such as "SNAbackup" to identify its purpose.
- Enter your name as the owner of the drawer; this gives you full access rights.
- Specify a page limit greater than the size of the SNA Mail Relay database (see the SNA Mail Relay Worksheet).
- Give the administrative user group (if you have one on your network) full access to the drawer.

Related procedure: Moving the SNA Mail Relay

Filling out the worksheet: Make a copy of the SNA Mail Relay Worksheet and use section ⑩ to record backup information:

⑩ Record the fully qualified name of the backup location. This is the fully qualified name of the File Service where the SNA Mail Relay server profile will be backed up.

Record the name of the file drawer that was added to the remote File Service.

Removing the SNA Mail Relay from the server

When you expunge an SNA Mail Relay Service, XNS and SNADS users cannot exchange mail. The SNA Mail Relay mailbox is automatically deleted by the Mail Service within 24 hours of the removal of the SNA Mail Relay. Before you expunge the service:

- Notify network users of the time when the SNADS network will no longer be available.
- Wait two or three hours after this time to allow any mail already posted to reach the SNA Mail Relay mailbox.
- Perform a shutdown to make sure there is no mail in the queue and then expunge the SNA Mail Relay.

After you expunge the SNA Mail Relay, you then expunge the Foreign Gateway Service from the server supporting the Mail Service with the External Mail Gateway enabled.

Related procedure: Expunging the SNA Mail Relay, Moving the SNA Mail Relay

Relocating the Foreign Gateway Assistant

You can move the Foreign Gateway Assistant from one server location to another. The Foreign Gateway Assistant requires that a Mail Service (with the External Mail Gateway option enabled) be coresident on the same server. The External Mail Gateway option must be dedicated to the Foreign Gateway Assistant.

Before you move the Foreign Gateway Assistant, do the following:

- Make a copy of the Mail Service Worksheet to assist you in acquiring the information you need, and refer to the "Planning for setup" section in this chapter.
- Use the **List Maps** command to display the foreign domain(s) associated with the Foreign Gateway Assistant.
- Make sure a Mail Service with the External Mail Gateway enabled is installed on the new server location.
- Notify network users that the foreign domain associated with the SNADS network is not available for the next 24 hours.
- Wait two or three hours after notifying users that the foreign domain is not available, to allow any mail already posted to reach the SNA Mail Relay mailbox, before beginning the procedure to move the Foreign Gateway Assistant.

Upon completion, notify users of the availability of the foreign domain.

Related procedures: Moving the Foreign Gateway Assistant, Expunging the Foreign Gateway Assistant

Removing the Foreign Gateway Assistant from the server

You remove the Foreign Gateway Assistant from the server with the coresident Mail Service.

Before you expunge the Foreign Gateway Assistant:

- Notify network users of the time when the foreign domain associated with the SNADS network will not be available.
- Wait two or three hours after this time, to allow any mail already posted to reach the SNA Mail Relay mailbox.

Related procedures: Expunging the Foreign Gateway Assistant, Moving the Foreign Gateway Assistant

Looking at SNA Mail Relay activity

There are several ways to monitor SNA Mail Relay activity. Routinely monitor activity to establish a baseline to analyze the performance of the SNA Mail Relay and Foreign Gateway Assistant.

You can use the **Show Status** command in the Mail Service context to:

- List the database size of the Mail Service.
- List the number of messages on the gateway queue and pending queue.

You can use the **List Mailboxes** command in the Mail Service context to show:

- Number of messages in the SNA Mail Relay mailbox.

You can use the **List Maps**, **List Problems**, and **Show Status** command in the Foreign Gateway Assistant context to display:

- The number and types of FGA problems.
- Mappings of foreign domain to mailboxes

You can use the **Show Status**, **Show History**, and **Show Mail Link Parameters** commands in the SNA Mail Relay context to identify:

- Any SNA Mail Relay problem with other services.
- The number of mail messages sent and received by the SNA Mail Relay.
- Messages queued to and from the SNA Mail Relay Service.
- The maximum database size.
- The size and usage of the database.
- The number of mail messages that were not forwarded.

You can use the **Show Status** and **Show History** in the SNA Access context to identify:

- Any communication breakdown.
- Configuration problems.

Related procedures: Monitoring SNA Mail Relay activity, Monitoring SNA Mail Relay events

12. Internetwork Routing Service

This chapter helps you prepare for installation, setup, and maintenance of the Internetwork Routing Service (IRS). This information supports the procedures you perform from an 8000 or 8090 server.

Service description

The Internetwork Routing Service links local area networks (LANs) into a single internetwork. It allows sharing of information and computing resources beyond the geographical boundaries of a single LAN.

A local device sending information to another network first sends the information to an IRS, which forwards it to its destination. For example, the IRS lets users send a document to a file drawer located on a File Service in another city or to a printer in another building.

The IRS provides:

- Access to all network services for internetwork users.
- Routing of information over Ethernet networks, X.25 networks, or telephone lines.
- Optional X.25 Communications Protocol software and Clusternet Communications software.
- Optional 873 Communication Interface Unit and Multiport Option Kit.

How the software works

The IRS transfers information between networks over telephone lines or X.25 circuits. Communication between networks can take place as long as each network has an operating IRS. Information can be routed through as many as 15 IRSs to reach its destination.

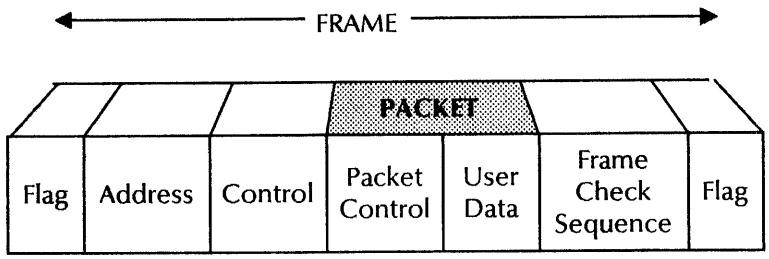
Routing tables

The IRS uses routing tables to select the most efficient route to a destination. A routing table lists all the networks comprising the internetwork and provides a step count between them. The step count indicates the number of internetworks between the originating network and the destination. The table also shows the circuits along the route.

Information transmission

Information is transmitted over the network in packets. A packet is a block of data accompanied by control characters. The complete unit is called a frame. Flags mark each end of the frame. Figure 12-1 shows the structure of a typical packet.

Figure 12-1. **Packet structure**



The control characters perform certain functions during transmission. The functions include addressing, synchronization of transmission, and error checking.

To forward a packet to a remote network, the IRS wraps it in an electronic envelope. This envelope prepares the packet for transmission either over phone lines or through a public data network using X.25 protocol.

Using a modem, the IRS sends the envelope from the server to the next step, an adjacent IRS, on the way to the final destination. When the envelope arrives at the next step, the receiving modem converts the information for the server containing the IRS. The IRS refers to the routing table and prepares for the next step. The preparation may involve rewrapping the information in:

- An Ethernet network envelope to send to a recipient on the local network or to another IRS on the local network
- A circuit envelope (phone line or data network) to send to another network
- A circuit envelope to send to a remote workstation using Clusternet Communications

Routing updates

IRS configuration changes are automatically broadcast throughout the internetwork. Each IRS updates its routing table and exchanges the information it contains with adjacent IRSs every 30 seconds.

Connections

Multiple connections (links) provide alternate routes between networks and increase the reliability of an internetwork. A network can be structured so that it has several links to other networks, which in turn can have links to other networks. This interconnected network structure has no size limit.

IRS connections are made using one or a combination of these circuit types:

- X.25 switched virtual circuit (SVC)
- Auto-dialed
- Manually dialed
- Dedicated

Auto-dialed, dedicated, and manually dialed circuits can use full or half duplex modems. Full duplex modems, which allow communication in both directions at the same time, are recommended. Half duplex modems allow communication in both directions, but not at the same time. CIU circuits and X.25 SVCs require full duplex modems.

X.25 SVCs connect Ethernets through a public data network, allowing up to eight active IRSs at a time. X.25 SVCs must be installed at both sending and receiving ends. The IRS retries calls until a connection is made.

Auto-dialed circuits require an autodialer at the port of the IRS initiating the call. The destination IRS must have a started, manually dialed circuit to receive the call. The IRS automatically retries calls once.

Manually dialed circuits require dialing to make a connection. They are often used to answer calls.

Dedicated circuits must be started at both sending and receiving ends to establish a connection.

Software options

The IRS offers two software options: X.25 Communications Protocol and Clusternet Communications.

X.25 Communications Protocol

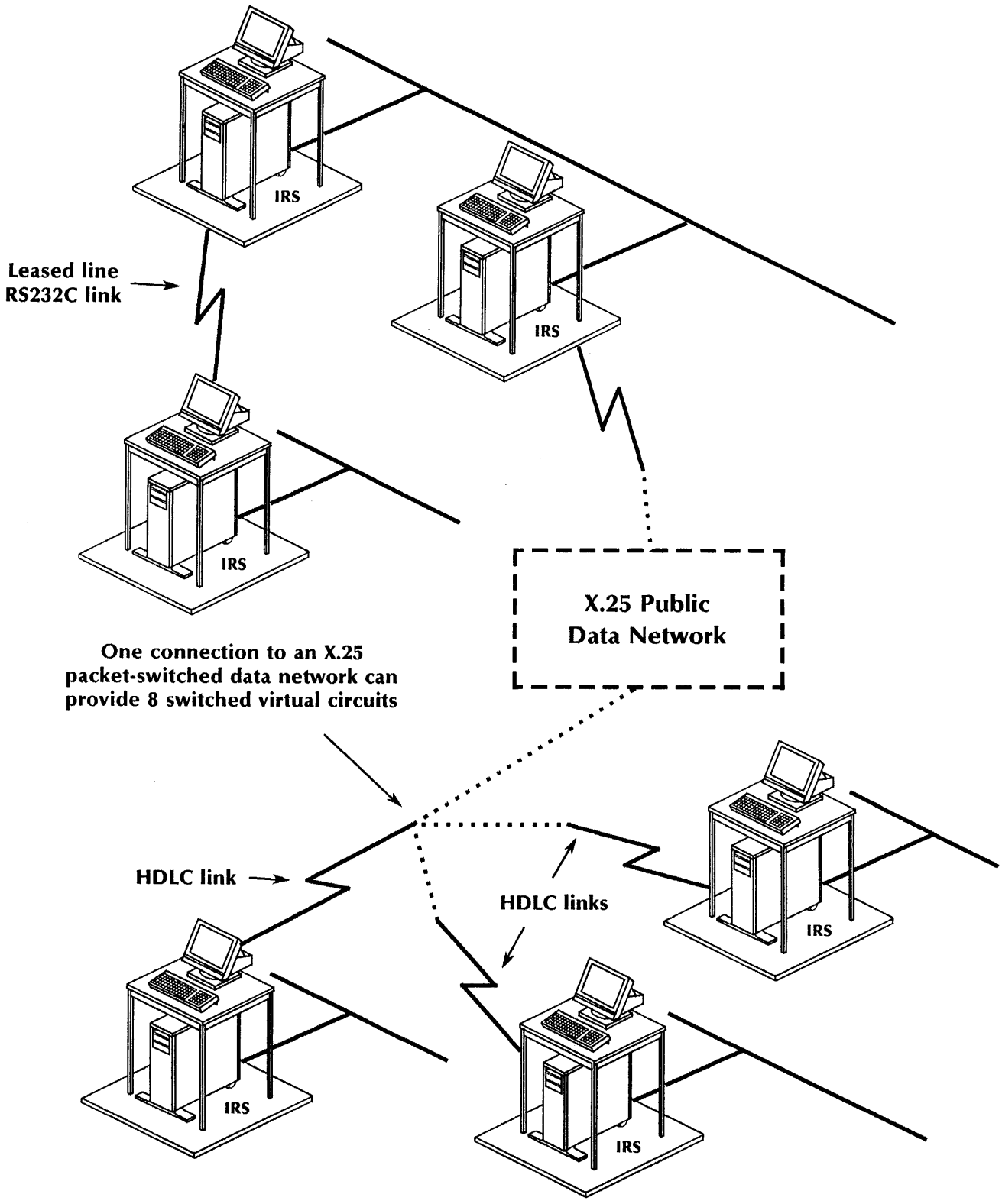
The X.25 Communications Protocol option interconnects Ethernets over leased line links through a public data network. The X.25 Communications Protocol is based on the high-level data link control (HDLC) procedures specified by the International Standards Organization (ISO).

The X.25 network directs the flow of information. When information is transmitted, the IRS electronically wraps the data and sends it to the local X.25 network. The network refers to its routing table to identify the route to the destination IRS. The receiving IRS unwraps the data and routes it to its final destination.

An IRS can support only one X.25 physical link, but each X.25 connection can support up to eight active IRSs at a time.

Figure 12-2 shows how the IRS can utilize the X.25 public data network to make several connections as compared to a simplified leased line link.

Figure 12-2. **IRS with X.25 network and RS232C links**



Clusternet Communications

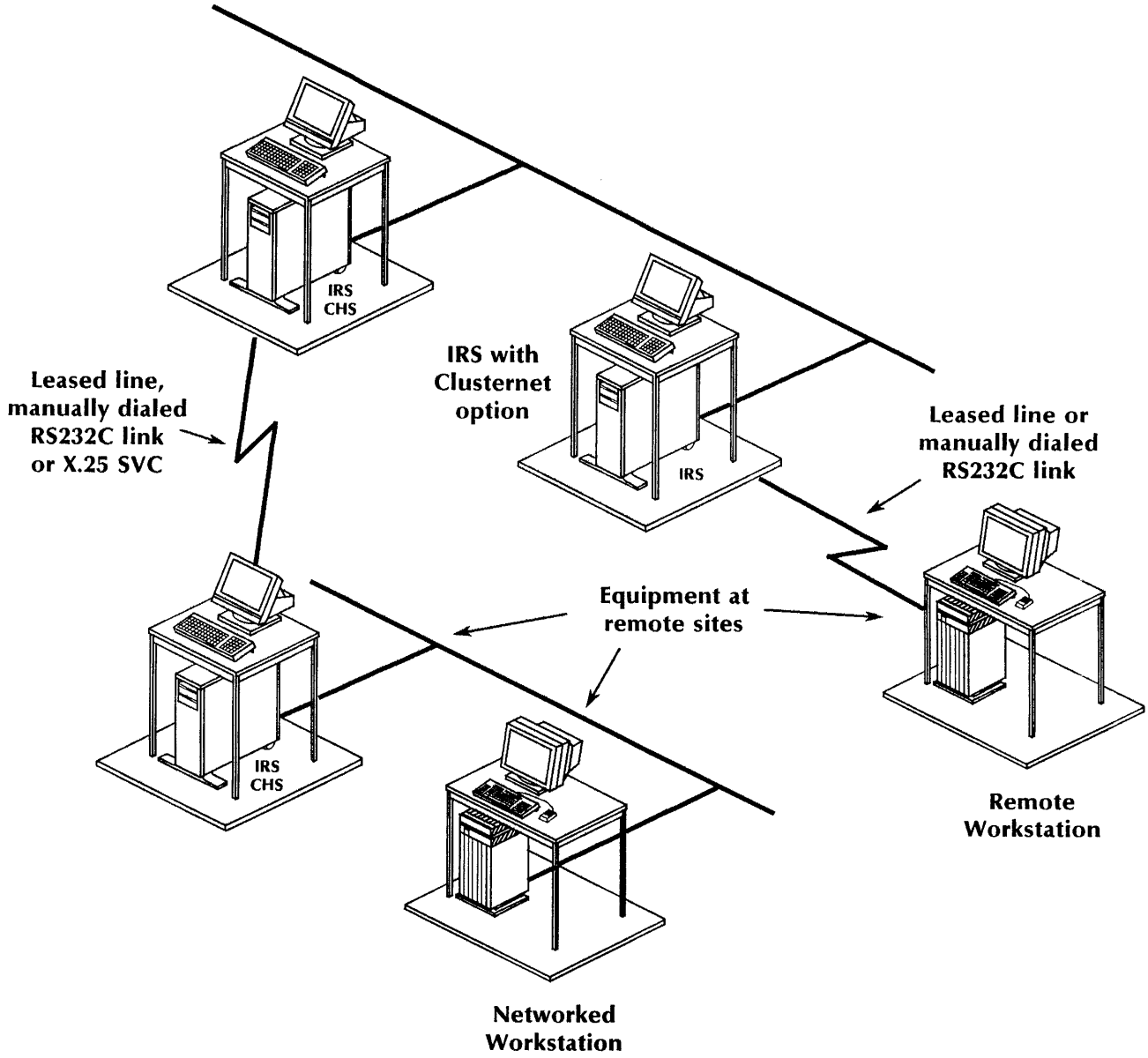
Clusternet Communications option lets remote workstation users access network services through a dial-up session. The remote workstation is networked when the user dials an IRS clusternetwork port.

The Clusternet Communications option considers one or more RS232C ports to be a clusternetwork. You can assign a network number to a clusternetwork, enabling communication with other networks.

The IRS includes a clusternetwork router that provides routing information to the clusternetwork. The router uses the clusternetwork number and the host numbers of the remote workstation to route information to and from the clusternetwork ports.

Figure 12-3 shows two approaches to enable remote workstations to access network services.

Figure 12-3. **IRS with RS232C link or Clusternet**



System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the Internetwork Routing Service Worksheet, located at the end of this chapter.
- Installing the IRS software as described in the Server Software Installation chapter of the *Services Installation and Setup Guide.*
- Setting up the IRS as described in the Internetwork Routing Service chapter of the *Services Installation and Setup Guide.*
- Maintaining the IRS as described in the Internetwork Routing Service chapter of the *Services Maintenance Guide.*
  - Analyzing IRS phone line statistics.
  - Monitoring service performance using the Communications Monitoring Service (see the Communications Monitoring Service chapter in this book).
  - Upgrading hardware and software as required.
  - Notifying users of any change or disruption in the service.
- Troubleshooting the service as described in *Basic Network Troubleshooting.*

You can perform most IRS procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter in the *Services Installation and Setup Guide* contains the procedures for installing your IRS software. This section explains the hardware, software, and other requirements of the Internetwork Routing Service to help you prepare for installation.

Hardware requirements

The Internetwork Routing Service operates on an 8000 or an 8090 server. To connect communicating servers, each server must have an RS232C Port Communication Kit, an 873 Communication Interface Unit, or the Multiport Option Kit. The servers must also have a modem, modem cable, and connectors for each port that the IRS supports. Workstations can make a direct connection to the internetwork using a Shared Interface Unit.

RS232C Port Communication Kit

The RS232C Port Communication Kit adds one external RS232C communication port to the processor. Installed on a server, the kit can support a communication application. Installed on an 8010 workstation, the kit enables the workstation to communicate with the network.

The RS232C Port Communication Kit supports the IRS, Clusternet Communications, and X.25 Communications Protocol.

The modem specifications depend on the type of circuit you are using:

- X.25 switched virtual circuit -- use synchronous, full duplex modem with a line speed up to 9,600 bps
- Auto-dialed or manually dialed circuits -- use synchronous, full duplex modem with a line speed up to 9,600 bps; if using Clusternet Communications, speed can be up to 19,200 bps
- Dedicated circuits -- use synchronous, full duplex modem with a line speed up to 56 Kbps

873 Communication Interface Unit

The 873 Communication Interface Unit (CIU) increases the number of RS232C ports on a network without requiring the addition of a server. The 873 CIU adds four external ports; the 873 CIU Extension Kit adds four more.

The 873 CIU supports the IRS and Clusternet Communications.

The 873 CIU uses a synchronous, full duplex modem with a line speed up to 9,600 bps.

Multiport Option Kit

The Multiport Option Kit adds four external RS232C ports to the processor. Servers with an installed 873 CIU Extension Kit can use the Multiport Option Kit to increase the number of ports to 12.

The Multiport Option Kit supports the IRS, Clusternet Communications, and X.25 Communications Protocol.

The Multiport Option Kit with auto-dialed (port 0), manually dialed, or dedicated circuits can use modems providing:

- synchronous, full duplex transmission from 1,200 bps to 56Kbps
- synchronous, half duplex transmission from 1,200 bps to 9,600 bps
- asynchronous, full duplex transmission up to 9,600 bps

Shared Interface Unit

The Shared Interface Unit (SIU) provides two RS232C ports that one or two workstations can use to connect to the internetwork. Workstations can connect directly to the ports or use dial-up or leased line modems to make the connection.

The Shared Interface Unit with a manually dialed or dedicated circuit uses a synchronous, full duplex modem with a line speed from 1,200 to 19,200 bps (2,400 bps is a recommended minimum speed).

Software requirements

The Internetwork Routing Services requires these program files:

- InternetworkRoutingSDF.bcd
- IRS.bcd
- RS232CCommon.bcd
- X25Config.bcd
- CommSvcComSoft.bcd
- ESRConfig.bcd
- SMStub.bcd
- CommunicationServicesArea.messages
- InternetworkRoutingMessages

Allow 625 disk pages for these program files.

In addition to the Internetwork Routing Service software, your configuration may require these software programs:

- To use an X.25 network, the X.25 Communications Protocol software
- To create a clusternetwork, Clusternet Communications software
- To use CIU ports, the External Communication Service software

Allow another 250 disk pages for the Internetwork Routing Service using either the X.25 Communications Protocol option or the Clusternet Communications option.

Dependencies and limitations

Depending on your configuration, the Internetwork Routing Service has certain dependencies and limitations.

Internetwork Routing Service

The Internetwork Routing Service has these dependencies and limitations:

- The IRS depends on the Services System Software utilities to communicate with users. It stores circuit and X.25 network information in the server profile.
- An IRS must be installed on each network that is communicating with another network.
- The IRS can use an RS232C port, the 873 Communication Interface Unit, or the Multiport Option Kit. When an IRS uses an RS232C port, the RS232C Communication Kit or the Multiport Option Kit is required.
- If you are using an RS232C port on the 873 CIU, the External Communication Service (ECS) must be on the same server as the IRS. The ECS keeps track of the name, processor number, state, and ownership of the CIU ports.
- If the circuits use CIU ports, ensure that the External Communication Service is installed so you can add the CIU. The ECS must be restarted for these circuits to start.
- If the sending server's Multiport Option Kit is configured for 56,000 bits per second, the receiving server must be configured the same way.
- Use the X.25 Communications Protocol if you require circuit switching.
- To communicate with each other, two devices must be within 15 IRS links of each other. The IRS always chooses the shortest route, if more than one route to a destination is available.

X.25 Communications Protocol option

The X.25 Communications Protocol has these dependencies and limitations:

- The X.25 Communications Protocol can use these public data networks:
  - Tymnet, Uninet
  - Telenet
  - DDX
  - International DDX
  - DDX 80
  - Passive DTE
- An IRS can support one X.25 link to the public packet switching data network (PSDN). This link, in turn, can support up to eight virtual connections to other IRS destinations.
- The X.25 Communications Protocol requires the dedicated use of the server's RS232C port or one of the four RS232C ports offered by the Multiport Option Kit.
- The X.25 network uses only switched virtual circuits. Switched virtual circuit describes the public data network method to connect devices. The public data network uses one of its available circuits to establish the connection as requested by each user.
- To communicate over the X.25 network, X.25 switched virtual circuits must be installed at the sending IRS and the receiving IRS. Each SVC must use the local X.25 address of the other IRS as its remote address.

Clusternet Communications option

The Clusternet Communications option has these dependencies and limitations:

- The Clusternet Communications option considers one or more RS232C ports to be a clusternetwork.
- You can designate RS232C ports on a server, a CIU, or the Multiport Option Kit as clusternet ports.
- If Clusternet Communications is configured for the port, no other application can use the port.
- Shared Interface Unit (SIU) ports cannot be configured for Clusternet Communication.

Multiport Option Kit

The Multiport Option Kit has these dependencies and limitations:

- The Multiport Option Kit supports only one autodialer. The autodialer controls port 0 only.
- The Multiport Option Kit can be used on 10 Mb or 42 Mb server processors. It cannot used on 29 Mb, 80 MB, or 300 Mb processors.
- The Multiport Option Kit cannot be installed on a server running the Print Service.
- The Multiport Option Kit can have a maximum throughput of 112,000 bits per second (bps) for synchronous communications or 76,800 bps for asynchronous communications. Either type of communication configuration can be distributed over its four ports in any combination of these line speeds: 300 bps, 1200 bps, 2400 bps, 4800 bps, 9600 bits, and 19200 bps.

  Throughput relates to the speed of transmission. Asynchronous refers to communication in which timing (synchronization) is determined by the transmitted data rather than from the transmitting device (modem). Synchronous communication derives its timing from the device.
- The Multiport Option Kit can support these synchronous IRS combinations:
  - Two IRS lines at 56 Kbps
  - One IRS line at 56 Kbps and up to three IRS or Clusternet lines at 19.2 Kbps
  - Four IRS or Clusternet lines at 19.2 Kbps
  - Three IRS lines at 19.2 Kbps and one X.25 line at 9.6 Kbps
- The Multiport Option Kit can support these synchronous and asynchronous IRS combinations:
  - Two IRS lines at 56Kbps and two asynchronous lines up to 1200 bps
  - One IRS line at 56 Kbps and three synchronous lines up to 19.2 Kbps
  - One IRS line at 19.2 Kbps or one Clusternet line at 19.2 Kbps and three asynchronous lines up to 19.2 Kbps.
- To use a line speed of 56,000 bps, both sending and receiving servers must have a Multiport Option Kit and must have matching line speeds.
- Only full duplex is supported for asynchronous communication.
- Assign line speeds to the Multiport Option Kit ports in this order:
  - Port 1 - highest line speed
  - Port 0 - second highest line speed
  - Port 3 - third highest line speed
  - Port 2 - lowest line speed

Internetwork Routing Service Worksheet

Use the Internetwork Routing Service Worksheet to record server-related and service-related information. The worksheet is at the end of this chapter.

Fill out a separate copy of the worksheet for each IRS for which you have System Administrator responsibility. Make several copies if you are adding multiple circuits. Retain the original for future use, and store the completed worksheet in your *Activities Guide*.

Using the worksheet

Before you install the software and set up your Internetwork Routing Service, complete the IRS worksheet. It is important that you fill out the worksheet accurately, and update it whenever changes occur.

The completed worksheet saves you time as you perform the setup and maintenance procedures. It also serves as an information source for new System Administrators unfamiliar with your configuration.

Filling out the worksheet

As you read the rest of this chapter, you are directed to make entries on the Internetwork Routing Service Worksheet. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and the services installed on that server. Copy this information from the Services Installation Worksheet you filled out while reading the Services System Software chapter of this book.

Use section ② to check off the hardware and software options of your IRS. Use section ③ to note the information you need to define a new circuit or change an existing one.

Planning for setup

After you install the Internetwork Routing Service, you initialize it, add the X.25 network (if necessary), and add circuits.

After you complete the Internetwork Routing Service Worksheet, see the Internetwork Routing Service chapter in the *Services Installation and Setup Guide* for complete setup procedures.

IRS name and description

You name and describe the Internetwork Routing Service during initialization. The name and description become part of the system-wide directory function that the Clearinghouse maintains.

When you name the Internetwork Routing Service, use a name different from all other names in the domain. The fully qualified Internetwork Routing Service name takes the form:

Internetwork Routing Service name:Domain:Organization

The domain and organization MUST be the same as the domain and organization of the server. For example, if the server name is Dallas:Home Office:ABC Company, then the Internetwork Routing Service name might be Sales:Home Office:ABC Company. It is recommended that you enter the local name only when you name the Internetwork Routing Service. This avoids possible errors and lets the domain and organization default to that of the server.

This naming convention gives the System Administrator for the server domain access to System Administrator commands for the Internetwork Routing Service. These commands are available only when you are enabled.

The service description may be the location, a department name, the name of the assigned System Administrator, or any other descriptive information. You may want identify the type of communication option in the service description.

Related procedure: Initializing the Internetwork Routing Service

Filling out the worksheet

① Record the name and description of the Internetwork Routing Service.

② Check off the type of communications options installed on the IRS.

The X.25 network and switched virtual circuits

The X.25 SVC column of section ③ provides fields that describe the high-level data link control (HDLC) parameters of the X.25 network and the X.25 switched virtual circuits. You define the X.25 network before you add an X.25 SVC. You add an X.25 SVC for each remote IRS with which you want to establish a connection.

Related procedures: Adding an X.25 network, Adding an X.25 switched virtual circuit

Filling out the worksheet

③ **Line speed** - Record the line speed in bits per second. Valid speeds are 1200, 2400, 3600, 4800, 7200, and 9600 bps.

Local address - Record the local address supplied by the X.25 vendor.

Port number - If you have installed a Multiport Option Kit, identify the port number.

Retransmission timeout - Record the number of seconds (from 3 through 20) you want the X.25 SVC to wait for a response before it tries to resend a packet. Ask the X.25 vendor for this information.

Number of retransmissions - Record the number of times (from 1 through 100) you want the circuit to try to send the packet. The recommended entry is 30.

Number of outstanding frames - Record the number (from 1 through 7) of outstanding frames you want to allow. (A frame is a preset number of bits transmitted as a unit.) The recommended entry is 7.

Network type - Record the name of the packet switched data network (PSDN) you are using for X.25 communications. Valid types are Tymnet, Uninet, Telenet, DDX, International DDX, DDX 80, and Passive DTE.

Protocol ID - Record the eight hexadecimal digits of the protocol identification. The IRS sends this information in the call request packet to identify to the next recipient of the packet the protocol in use. The default value is FFFFFFFF.

SVC start/stop channel - Enter the range of channels (from 1 through 4095) the SVCs may take, as supplied by the X.25 vendor. The numbers define a range from the start number to the number before the stop number. A range of 1000/2000 includes the channels from 1000 to 1999.

Network description - Record a comment that describes the X.25 network.

Address of remote host - Record the local address of the destination IRS.

Autostart - Indicate whether or not the X.25 SVC is to be autostarted. (If you do not autostart a circuit, it must be manually started.) When you set up the X.25 network, you can select the autostart option for the network. Then as you add each X.25 SVC, you can individually choose to autostart each one.

Circuit description - Record a comment that describes the purpose and location of the network and its SVCs.

Auto-dialed circuits

The Auto-dialed column of section ③ provides fields that describe an auto-dialed circuit.

Related procedures: Adding an auto-dialed circuit

Filling out the worksheet

③ **Line speed** - Record the line speed in bits per second. Valid speeds are 1200, 2400, 3600, 4800, 7200, 9600, 19200, 28800, 38400, 48000, and 56000 bps.

Circuit description - Record a comment that describes the purpose and location of the circuit.

Duplexity - Indicate whether the modem is full duplex or half duplex. Only the local RS232C port can use either full or half duplex; full duplex is recommended.

Phone number - Record the phone number for this circuit.

Phone description - Record a comment that describes the purpose and location of the phone line.

Manually dialed circuits

The Manually dialed column of section ③ provides fields that describe a manually dialed circuit.

Related procedures: Adding a manually dialed or dedicated circuit

Filling out the worksheet

③ **Line speed** - Record the line speed in bits per second. Valid speeds for the local port and clusternetwork ports are 1200, 2400, 3600, 4800, 7200, 9600 19200, 28800, 38400, 48000, and 56000 bps. A CIU can use line speeds up to 9600 bps.

Autostart - Indicate whether or not the circuit is to be autostarted. If you indicate yes, the circuit starts when you start the IRS.

Circuit description - Record a comment that describes the purpose and location of the circuit.

Duplexity - Indicate whether the modem is full duplex or half duplex. CIUs cannot use a half duplex line.

873 port - If you are using an 873 Communication Interface Unit, record the description of the CIU.

8000 server local port - If the IRS is using the local port, check this box.

Clusternet number - If you are using Clusternet Communications, record the clusternet number. This number follows the same format as a network number; it cannot duplicate an existing network number. After you assign a clusternetwork number, all additional circuits automatically have the same number.

Port number - If you are using the CIU or Multiport option, identify the port number for this circuit.

Use CIU for autoboot - If you are not using the IRS to autostart this circuit, indicate whether or not you want to use the CIU to start it.

Dedicated circuits

The Dedicated column of section ③ provides fields that describe a dedicated circuit.

Related procedures: Adding a manually dialed or dedicated circuit

Filling out the worksheet

③ **Line speed** - Record the line speed in bits per second. Valid speeds are 1200, 2400, 3600, 4800, 7200, and 9600 bps.

Autostart - Indicate whether or not the circuit is to be autostarted. If you indicate yes, the circuit will start when you start the IRS.

Circuit description - Record a comment that describes the purpose and location of the circuit.

Duplexity - Indicate whether the modem is full duplex or half duplex. CIUs cannot use a half duplex line.

873 CIU - If the IRS is using an 873 Communication Interface Unit, check this box.

8000 server local port - If the IRS is using the local port check this box.

Clusternet number - If you are using Clusternet Communications, record the clusternet number. This number follows the same format as a network number; it cannot duplicate an existing network number. After you assign a clusternetwork number, all additional circuits automatically have the same number.

Port number - If you are using the CIU or Multiport option, identify the port number for this circuit.

Planning for maintenance

After you install and set up the Internetwork Routing Service, you are responsible for maintaining it properly. You perform maintenance as needed; there are no scheduled duties.

This section provides guidelines for monitoring the service performance, analyzing circuit statistics, checking current circuit status, displaying routing information, and making configuration changes.

See the Internetwork Routing Service chapter in the *Services Maintenance Guide* for complete maintenance procedures.

Monitoring phone lines

The Server Monitor Service (SMS) can monitor phone lines for auto-dialed, or manually dialed, dedicated circuits. When the activity at a phone line changes, the IRS notifies the SMS, which then sends mail messages to specified users. This early notification shortens response time to problems. See the Server Monitor Service chapter in this book for more information.

Related procedure: Configuring the Server Monitor Service database

Monitoring the X.25 network

The Communications Monitoring Service (CMS) can monitor the performance of the X.25 network. This valuable tool lets you analyze the transmission through the communication links. See the Communications Monitoring Service chapter in this book for more information.

Related procedure: Monitoring X.25 communications

Analyzing circuit statistics

Set a schedule for regularly monitoring the IRS circuit statistics to determine how efficiently the service is operating. To provide the most accurate analysis, always create the statistical record in the same way.

First, display all statistics since the server was last started. Next, reset the statistics counter, allowing 15 minutes for the reset process. Then use the incremental statistics option to reduce the reporting period. This shorter period helps you analyze current performance.

Analyzing the statistics can help you:

- Identify phone line problems, which usually relate to the number of packets successfully sent or received.
- Prevent overloading of the IRS.

Related procedures: Showing the Internetwork Routing Service statistics

The following sections describe the statistics. See *Basic Network Troubleshooting* for more information.

Load statistics

These statistics help you maintain the proper load on the IRS:

<number> packets forwarded/sent/received - The number of packets forwarded, actually sent, and then received. Compare the numbers to analyze performance.

<number> bytes forwarded/sent/received - The number of bytes forwarded, actually sent, and then received. The number of bytes received indicates the utilized throughput in the receiving direction. Compare the numbers to analyze performance.

Throughput relates to the speed of transmission. Maximum throughput is a number less than 25 percent of the line speed for half duplex circuits, and less than 50 percent of the line speed for full duplex circuits. Increase the line speed if the number of bytes received is greater than the maximum throughput for longer than 10 minutes.

<number> congestion count - The number of packets discarded to prevent congestion. (The IRS uses a sending queue for each phone line. If a new packet would be delayed too long in the queue, the IRS discards the packet.) If the number is greater than 10 percent of the line speed, consider increasing the line speed. If you cannot increase the line speed, reduce remote network activity or relocate remote services.

<number> bps sent - The utilized throughput in the sending direction. Increase the line speed if the number is greater than the maximum throughput for longer than 10 minutes.

<number> bps throughput - The sum of the bits per second sent and received. Increase the line speed if the number is greater than the maximum throughput for longer than 10 minutes.

Phone line problem indicators

These statistics indicate potential problems with the communication kit, modems, cables, and phone lines. In many cases, you can reduce the line speed as a temporary solution.

<number> send error, bad status - The number of packets not sent because of hardware errors. If the number is greater than 1 percent of the packets sent, you may have a problem with your communication kit.

<number> packets rejected - The number of packets not received or partially received. If the number is greater than 5 percent of the packets received, you may have a problem with your communication kit.

<number> receive error - The number of packets not received because of hardware errors. If the number is greater than 5 percent of the packets received, you may have a problem with your communication kit.

<number> CRC errors - The number produced by a cyclic redundancy check (CRC) method of error detection; the number of packets not received because of errors in sending or transmission. If the number is greater than 5 percent of the packets received, you may have a problem with your communication kit.

<number> too long since last receive - The number of times no packets were received from the remote station for longer than 80 seconds (normally an IRS sends a packet every 30 seconds). The remote station may be sending, but the local station is not receiving. Check the lines for bad cables or modems. Check also, whether the remote station is inoperable or the remote IRS stopped.

Phone line activity statistics

These statistics are explanatory rather than problem indicators:

<number> times dsr dropped - The number of times the modem was not ready because of a lowered Data Set Ready (DSR) value. A problem may exist with the modem, cable, or Communication Interface Unit.

<number> connection established count - The number of successful connections since the IRS was started.

<number> no response count - The number of unsuccessful responses to a connection attempt.

Checking circuits

You can list the name, description, type, duplexity, line speed, and current status of circuits to verify port information. If a connection is established to a remote host, the list identifies the name and address of the host and the destination networks each circuit can reach.

Related procedure: Listing circuits, X.25 networks, and routes

Listing circuit status can help you isolate problems. See *Basic Network Troubleshooting* for more information.

The circuit status messages include:

stopped - The circuit is defined but not started.

port has been acquired - The port has been manually started, but the connection to the remote IRS is not yet established.

awaiting physical medium - The modem is not ready. If this message persists, check the modem and cable.

connection being retried - The local IRS is trying to establish communication with the remote IRS. If this message persists, check the status of the circuit on the receiving end.

connection is being established to remote host - The IRS has received at least one phone line packet from the remote IRS; the connection is being established.

connection established to remote host - The two IRSs should be able to communicate. If they cannot communicate, use the **Show Statistics** command to analyze the situation.

connection being terminated - The connection is ending, but the circuits are not yet stopped.

Checking routes

You can verify routing table information by listing all network routes that can be reached from the router's Ethernet and RS232C port connections. The list describes the transmission medium used to reach the next IRS. The medium may be the same Ethernet or a circuit.

If the remote network you want to reach is listed, you can determine the path by checking the step count and the medium used. If the remote network is not listed, the two networks cannot communicate.

Listing routes can help you identify inefficient paths that result in slow communication, or determine that a path does not exist or is inoperable. See *Basic Network Troubleshooting* for more information.

Related procedure: Listing circuits, X.25 networks, and routes

Making configuration changes

You may need to change circuit types, or change the parameters of the X.25 network and its switched virtual circuits.

Make another copy of the Internetwork Routing Service Worksheet, and see "Planning for setup" earlier in this chapter to define the new parameters.

Related procedure: Changing circuit parameters, Changing the X.25 network location, Changing the X.25 network parameters

13. Interactive Terminal Service

This chapter helps you prepare for installation, setup, and maintenance of the Interactive Terminal Service (ITS). This information supports the procedures you perform from an 8000 or an 8090 server.

Service description

The Interactive Terminal Service acts as a gateway, providing access to and from the Xerox Network System (XNS). The Interactive Terminal Service lets users of teletype (TTY) terminals and personal computers exchange information over telephone lines and take advantage of network resources. The remote users can also access the Mail Service, File Service, and Print Service.

How the software works

The Interactive Terminal Service communicates with TTY-type terminals and non-networked personal computers using telephone lines and modems. The remote user must initiate communication with the Interactive Terminal Service. A "Greeter" answers the call and provides the option to make the Interactive Terminal Service connection. After logon, users can send, answer and forward mail; store, retrieve, move, delete, and copy files; and print documents.

A personal computer or standard ASCII terminal uses asynchronous ASCII protocols to initiate a dial-up communication session. Access is through the server's local RS232C port or a Communication Interface Unit (CIU). The connection is made through the External Communication Service (ECS), unless you configure the port to automatically connect with the Interactive Terminal Service. See the External Communication Service chapter in this book for more information about configuring the ECS port to receive incoming asynchronous calls.

After the connection is made, the remote terminal and the Interactive Terminal Service communicate using standard teletype protocols.

Refer to the *Interactive Terminal Service User Guide* for complete step-by-step instructions on interacting with the Interactive Terminal Service to file, mail, and print documents.

Document format

The Interactive Terminal Service supports two document formats for mailing and filing: 860 and plain text. To send a document to a workstation on the internetwork, the user can instruct the Interactive Terminal Service to convert the document to 860 format. If the document is sent to a 6085/8010 workstation, the recipient converts it to 6085/8010 format to retrieve it. A document intended for another remote teletype device can use the plain text format.

Interactive Terminal Service supports these document formats for printing: Interpress, Memorywriter, ASCII text, and 860 files. A document in Interpress format is sent directly to the Print Service. A document in another format is converted to Interpress before being sent to the Print Service.

Mailing

Interactive Terminal Service users can access the Mail Service to list and display messages as well as create, edit, and send messages.

Users may send documents sent with their messages. After conversion at a 6085/8010 workstation, these documents can be handled like any internetwork document. Remote users can read mail notes created at 6085/8010 workstations and mail forms created 860 workstations without converting them.

Filing

The File Service can function as a central storage facility or as a vehicle for transmitting large documents. TTY-type terminals can access the File Service to move, copy, or delete objects.

Personal computers must have XModem protocol to exchange documents between the PC and the File Service. Remote personal computer users can create files using any word processing or spreadsheet software and then transmit them to the Interactive Terminal Service for storage on a File Service. The files are available to users of remote personal computers or networked workstations.

Remote users can display or edit files stored as 860 documents, then store them on the File Service in 860 or plain text format. Remote users cannot display or create 6085/8010 files using the Interactive Terminal Service, but can manipulate such files at the File Service. A 6085/8010 document must be converted to 860 format before users can can work with it through the Interactive Terminal Service.

Printing

Interactive Terminal Service users can print Interpress, Memorywriter, ASCII or 860 documents on any Print Service on the network. These documents can be located on a File Service or on a remote computer.

Remote users can set the printing options, such as paper size, number of copies, and pages to be printed. The Interactive Terminal Service converts the document to Interpress format, if necessary, before sending the document to the Print Service.

User profiles

When a remote user logs off, the Interactive Terminal Service stores a profile for the user in a file drawer on the user's home File Service. The profile contains information such as the directory path, terminal options, and Print Service data in effect at logoff. The user need not enter new information to start a session, unless some of the information needs to change.

Multinational considerations

The Interactive Terminal Service has multinational language capabilities to let users compose messages in any language supported by the 6085/8010 workstation. The Interactive Terminal Service also supports alternate character codes sometimes found on terminals outside the United States.

Relationship with other services

The Interactive Terminal Service works with these other network services:

- The Clearinghouse Service maintains a directory of registration information which the Interactive Terminal Service uses to verify users and check access controls.
- The Mail Service contains mailboxes which hold messages until they are requested by the user.
- The File Service contains individual and group file drawers, as well as the file drawer for the Interactive Terminal Service user profile.
- The Print Service prints Interpress, Xerox Memorywriter, or ASCII plain text documents.
- The External Communication Service is configured to receive the incoming asynchronous calls.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the Interactive Terminal Service Worksheet located at the end of this chapter.
- Installing the Interactive Terminal Service software as described in the Interactive Terminal Service chapter of the *Services Installation and Setup Guide*.
- Setting up the Interactive Terminal Service as described in the Interactive Terminal Service chapter of the *Services Installation and Setup Guide*.
- Maintaining the Interactive Terminal Service as described in the Interactive Terminal Service chapter of the *Services Maintenance Guide*.
  - Monitoring Interactive Terminal Service activity and user sessions
  - Notifying users of any change or disruption in the service
  - Upgrading hardware and software as required
- Troubleshooting the service as described in *Basic Network Troubleshooting*.

You can perform most Interactive Terminal Service procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter of the *Services Installation and Setup Guide* contains the procedures to install your software. This section explains software, hardware and disk space requirements to help you prepare for installation.

Hardware requirements

The Interactive Terminal Service runs on an 8000 or an 8090 server.

To allow dial-up access, the ECS port configuration requires an asynchronous, full duplex modem, which can operate at line speeds up to 9,600 bps.

Software requirements

The Interactive Terminal Service requires these program files:

- InteractiveTerminalSDF.bcd
- MailStubConfig.bcd
- ITServiceConfig.bcd
- NSPrintClientConfig.bcd
- InterpressClientImpl.bcd
- InteractiveTerminalService.messages

Allow approximately 552 disk pages for the above files and about 740 free disk pages as working space for a maximum of eight users. If the Clearinghouse Service, Mail Service, and/or Remote Batch Service is coresident with the Interactive Terminal Service, allow another 34 free disk pages on the server.

Dependencies and limitations

The Interactive Terminal Service has these dependencies and limitations:

- The External Communication Service receives incoming asynchronous calls from remote users. The ECS must be running the Asynchronous Communication Protocol option configured for asynchronous terminal emulation and dial-in. You may also need to add a Communication Interface Unit (CIU). See the External Communication Service chapter in this book and in the *Services Installation and Setup Guide* for more information.

If your port uses XModem protocol, specify eight data bits, no parity, and one stop bit. Also, disable XOn/XOff flow control.

- The Interactive Terminal Service can share a port with the Asynchronous Communication Protocol option of the External Communication Service. It cannot share a port configured for asynchronous communication with a TTY emulation session.

- The Interactive Terminal Service can support a maximum of eight users at the same time. If the service must consistently support this number of users, install only the Interactive Terminal Service on the server.

  The Interactive Terminal Service can support only six users at the same time if it is used heavily for high-speed transmissions, long messages, or large distribution lists. To improve server performance, install only the Interactive Terminal Service on the server or add more memory to the server.

- The Interactive Terminal Service accesses any Mail or File Service on the same or different network on behalf of its dial-up user. Either or both of these services must be accessible to the Interactive Terminal Service.

- The File Service lets users perform all network filing activities and store their log-off values in the Interactive Terminal Service User Profiles drawer.

- The Mail Service lets users perform all network mailing activities.

- The Print Service lets users access all network printers.

- For optimum results, do not install the Interactive Terminal Service on the same server with the Print Service. The Print Service requires much of the server's processing resources, restricting the resources available to sustain a communication session.

Interactive Terminal Service Worksheet

Use the Interactive Terminal Service Worksheet to record server-related and service-related information. The worksheet is at the end of this chapter.

Fill out a separate copy of the worksheet for each Interactive Terminal Service for which you have System Administrator responsibility. Retain the original for future use, and store the completed worksheet in your *Activities Guide*.

Using the worksheet

Before you install the software and set up your Interactive Terminal Service, complete the Interactive Terminal Service Worksheet. It is important that you fill out the worksheet accurately and update it whenever changes occur.

The completed worksheet saves you time as you perform the setup and maintenance procedures. It also serves as an information source for new System Administrators unfamiliar with your configuration.

Filling out the worksheet

As you read the rest of this chapter, you are directed to make entries on the Interactive Terminal Service Worksheet, The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and the services installed on the server. Copy this information from the Services Installation Worksheet you filled out while reading the Services System Software chapter of this book.

Use section ② to identify the number of remote users and the number of file pages to allow each user.

Use section ③ for information specific to configuring the ITS User Profiles drawer.

Planning for setup

After you install the Interactive Terminal Service, you initialize it and create an Interactive Terminal Service User Profiles drawer.

See the Interactive Terminal Service chapter in the *Services Installation and Setup Guide* for complete procedures.

Interactive Terminal Service name and description

You name and describe the Interactive Terminal Service Service during initialization. The name and description become part of the system-wide directory function that the Clearinghouse maintains.

When you name the Interactive Terminal Service, use a name different from all other names in the domain. The fully qualified Interactive Terminal Service name takes the form:

Interactive Terminal Service name:Domain:Organization

The domain and organization MUST be the same as the domain and organization of the server. For example, if the server name is Dallas:Home Office:ABC Company, then the Interactive Terminal Service name might be Sales:Home Office:ABC Company. It is recommended that you enter the local name only when you name the Interactive Terminal Service. This avoids possible errors and lets the domain and organization default to that of the server.

This naming convention gives the System Administrator for the server domain access to System Administrator commands for the Interactive Terminal Service. These commands are available only when you are enabled.

The service description may be the location, a department name, the name of the assigned System Administrator, or any other descriptive information.

Related procedure: Initializing the Interactive Terminal Service

Filling out the worksheet

① **Name** - Record the name of the Interactive Terminal Service.

Description - Record the description of the Interactive Terminal Service.

Interactive Terminal Service parameters

During initialization, you identify the maximum number of remote users (up to eight) the Interactive Terminal Service will support at one time. You also identify the number of disk pages the Interactive Terminal Service may use during a user's mailing and filing operations.

The Interactive Terminal Service needs this space on the user volume for temporary file storage. The Interactive Terminal Service acquires space as necessary to fill user requests, then releases it. If space is not available for any reason, users may be unable to access the Interactive Terminal Service.

To estimate the number of file pages, determine the space available on the server. Then reduce this space by the disk pages required by the Interactive Terminal Service and the other services on the server. Finally, divide the number of free pages available to the Interactive Terminal Service by the total number of remote users.

Related procedure: Initializing the Interactive Terminal Service

Filling out the worksheet

② **Number of simultaneous users** - Record the number of users who can access the Interactive Terminal Service at the same time.

File pages per user - Record the number of file pages per user. If you enter 0, the amount of space for each user is limited only by the number of free pages available (up to 10,000 pages).

ITS User Profiles drawer

The Interactive Terminal Service stores values users set when they log off. These values include the user's current directory path, terminal options, and Print Service information. The Interactive Terminal Service User Profiles drawer makes this information available when the user logs on again.

You need to create a special file drawer on each File Service an Interactive Terminal Service user can access. So that the Interactive Terminal Service can recognize the drawer, name it "ITS User Profiles." Name the System Administrator as the owner of the drawer.

Assign a page limit for the drawer equal to two pages per Interactive Terminal Service user. For example, if you have 100 Interactive Terminal Service users, enter 200 for the page limit.

After you add the ITS User Profiles drawer, change the access list. Specify the name of the user, alias, or group that you want to allow access to the file drawer. Then identify the type of access you want to provide.

Provide read, write, and add access for all Interactive Terminal Service users. Reserve the other access rights for the System Administrator.

Related procedure: Creating the ITS User Profiles drawer

Filling out the worksheet

③ **File Service Volume** - Record the File Service volume containing the ITS User Profiles drawer, if applicable. The worksheet already lists the name of the drawer.

Owner's name - Record the name of the owner of the drawer. The owner is automatically given full access rights.

Page limit - Record the page limit for the file drawer.

User / alias / group name - Record the name of the user, alias, or group that will have access to the drawer. The access rights are noted on the worksheet.

Planning for maintenance

After you install and set up the Interactive Terminal Service, you are responsible for maintaining it. You perform maintenance as needed; there are no scheduled duties.

See the *Services Maintenance Guide* for complete maintenance procedures.

Making configuration changes

You can modify the parameters of the Interactive Terminal Service User Profiles drawer. The parameters include the owner's name, the access privileges, and the page limit for a specific user, alias, or group.

You can change the number of users who can access the Interactive Terminal Service at the same time and the number of file pages per user.

You can also change the name and description of an existing Interactive Terminal Service.

Related procedures: Changing the ITS User Profiles drawer, Reconfiguring Interactive Terminal Service resources, Renaming the Interactive Terminal Service

Monitoring service activity

Your most important maintenance task is monitoring Interactive Terminal Service activity and user sessions.

You can list the remote users currently logged on to the Interactive Terminal Service. You can also continuously monitor Interactive Terminal Service activity.

You may want to monitor the Interactive Terminal Service to determine the load on the service or whether it is logging off users in error. The system displays the start and stop time of each user's session.

Related procedures: Listing user activity, Monitoring Interactive Terminal Service sessions

14. Remote Batch Service

This chapter helps you prepare for installation, setup, and maintenance of the Remote Batch Service (RBS). This information supports the procedures you perform from an 8000 or an 8090 server.

Service description

The Remote Batch Service lets users exchange files with many devices that implement binary synchronous communications (BSC) data transmission protocol. BSC is a character-oriented protocol that IBM developed. The IBM 2770, IBM 2780, and IBM 3780 Remote Batch Terminals use BSC. Other data processors and word processors emulate it. Both networked workstations and Interactive Terminal Service (ITS) users can use the Remote Batch Service.

The Remote Batch Service:

- Emulates BSC data transmission protocol.
- Transfers data to and from standard file drawers.
- Transfers data in three modes:
  - Document interchange mode, in which the Remote Batch Service converts the document to ensure compatibility between the communicating devices.
  - Document transfer mode, in which the Remote Batch Service acts only as a transfer agent, sending and receiving documents in formats it does not understand.
  - Document archiving mode, in which the Remote Batch Service stores and retrieves documents without altering them.

How the software works

The workstation, the File Service, and the communicating device join the Remote Batch Service in document exchange.

The Remote Batch Service communicates with devices called partners to fulfill requests from workstation users. Partners can be data processing (DP) systems and word processing (WP) devices. WP devices include word processors, personal computers, and other intelligent communicating workstations.

Users can send information created on a mainframe computer or a word processor to network devices, such as the 6085/8010 workstation. Network users can then process the information further or integrate it into other documents.

Network users can also send information created on a Xerox device to a mainframe for processing or archiving. For example, users can store monthly reports on the mainframe, retrieve them to create the year-end report, and then archive that report on the mainframe.

The Remote Batch Service communicates with partners over telephone lines, making it and its partners available to all workstations on the internetwork. The Remote Batch Service and the workstations can be on different networks, as long as the networks share the same internetwork. One Remote Batch Service can support multiple remote partners, but it can communicate with only one partner at a time.

Task management

Each request to the Remote Batch Service is called a task or a job. A task consists of a folder (in 6085/8010 format) containing an instructions document (in 860 format) and the actual data, which may be documents, files, and folders. Tasks sent to a mainframe require an additional document (in 860 format) that specifies the Job Control Language (JCL) for executing the task. Tasks sent to a DP partner also require job control documents.

Users prepare task folders at a workstation. They submit tasks by placing the folder in an input file drawer.

The name of the instructions document must begin with the word "Instructions." The instructions document specifies the order of transmission for each object in the task folder and whether the object needs format conversion. If the instructions document is not sent in the task folder, the job remains in the input file drawer and the Remote Batch Service cannot process it.

The instructions document contains a statement for each object within the task folder. The format for a statement is:

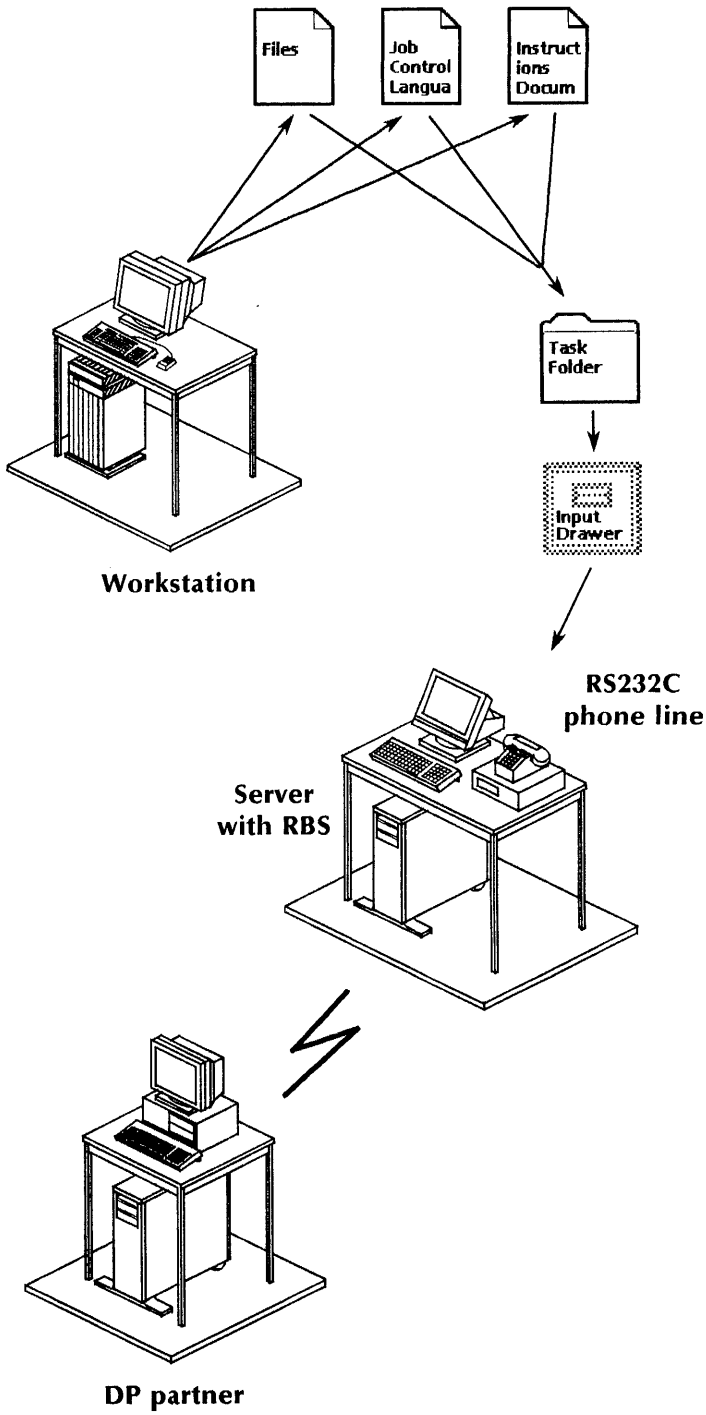
<transmission type>:<document name/folder name>

Transmission types are:

- DP, which refers to the IBM extended binary coded decimal interchange code (EBCDIC) DP code set
- WP, which refers to the IBM EBCDIC WP code set
- Foreign, which refers to an uninterpreted file transfer
- XNS, which refers to archive format

Users submit jobs by placing the task folders in an input file drawer on the File Service. Each partner has its own file drawer, which the Remote Batch Service periodically checks for tasks. The task remains in the file drawer until the Remote Batch Service copies it, interprets the instructions, converts the format if necessary, and transmits the data to the partner. Figure 14-1 shows the process for transmitting data to a DP partner

Figure 14-1. **Transmitting data to a data processing partner**



If an error occurs during job submission, the Remote Batch Service copies the task folder to an error folder in the input file drawer and, if the Mail Service is available, sends an error summary note to the submitter. The Remote Batch Service deletes from the input file drawer tasks that are successfully submitted.

If the partner is a mainframe, task completion may create output that is sent back to the Remote Batch Service. The Remote Batch Service converts the format if necessary, and places the data in an output file drawer on the File Service, where users can retrieve it.

The types of tasks available correspond to the three Remote Batch Service data transfer modes: document interchange, document transfer, and document archiving.

Document interchange

Document interchange provides document format and structure compatibility between the network and the partner. The Remote Batch Service converts a document from 860 format to the appropriate format for the DP or WP device, and then sends the data to the partner.

If the partner has data for the Remote Batch Service, the Remote Batch Service converts it into 860 format. An 820-II Personal Computer, 860 Information Processing System, 8010 Information Processing System, 6085 Professional Computer System, or an IBM Personal Computer can then retrieve it.

The Remote Batch Service supports:

- The 860 document format
- The IBM 2770/3780 EBCDIC WP code set
- The IBM 2770/3780 EBCDIC DP code set
- The IBM 2780 code set

Document transfer

You can use the Remote Batch Service to transfer documents without format conversion. This mode lets you transfer documents whose format and structure are unknown.

Document archiving

When the user submits a document archiving task, the Remote Batch Service sends files or folders to a mainframe for storage and archiving without altering them in any way. The data and its structure (such as fonts, tabs, or margins) as well as the attributes of the file or folder (such as its name, type, or size) remain intact.

The task folder

Users can create Remote Batch Service tasks on any workstation that can access the File Service. These workstations include the 820-II Personal Computer, 860 Information Processing System, 8010 Information Processing System, 6085 Professional Computer System, and IBM Personal Computer.

6085/8010 workstations

At a 6085/8010 workstation, the user creates the instructions document and, if necessary, the JCL document, placing them in a task folder with the data. The user then places the folder in the input file drawer assigned to the partner.

If the partner returns data, the Remote Batch places the data in the output file drawer assigned to that partner. The user retrieves the output from the file drawer and uses the converter icon to convert the document to 6085/8010 format. The user can then view and edit the document on the 6085/8010 workstation.

Other workstations

Workstations without the folder facility require a slightly different procedure. The user creates the instructions, JCL, and data documents at the workstation. However, the user creates and assembles the task folder in the input file drawer at the File Service.

The user retrieves output from the output file drawer to any workstation. The user can then convert and enhance the output with graphics and formatting, or mail, print, or integrate the output into other documents.

Filenames

The Remote Batch automatically identifies each file by the time it was received, its file type, and the name of the communication partner. The format for the default filename is:

<time of day>(file type)<partner name>

Users can specify their own filenames within the first 100 lines of each file or as a comment line in the JCL document.

The format for a name entered in a file is:

RBSRECEIVEDFILENAME:(number of bytes)<name>

The format for a name entered as a comment in a JCL document is:

//*RBSRECEIVEDFILENAME:(number of bytes)<name>

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the Remote Batch Service Worksheet located at the end of this chapter.
- Installing the Remote Batch Service software as described in the Remote Batch Service chapter of the *Services Installation and Setup Guide.*
- Setting up the Remote Batch Service as described in the Remote Batch Service chapter of the *Services Installation and Setup Guide.*
- Maintaining the Remote Batch Service as described in the Remote Batch Service chapter of the *Services Maintenance Guide.*
  - Analyzing the Remote Batch Service statistics to determine whether the service is efficiently handling user requests.
  - Upgrading hardware and software as required.
  - Notifying users of any change or disruption in the service.
- Troubleshooting the service as described in *Basic Network Troubleshooting.*

You can perform most Remote Batch Service procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter of the *Services Installation and Setup Guide* contains the procedures for installing your Remote Batch Service software. This section explains the hardware, software, and other requirements of the Remote Batch Service to help you prepare for installation.

Hardware requirements

The Remote Batch Service can run on an 8000 or an 8090 server. The Remote Batch Service requires the RS232C Communication Kit to provide dedicated use of the server's local port. The Remote Batch Service cannot use the 873 Communication Interface Unit or the Multiport Option Kit.

The Remote Batch Service uses a synchronous modem operating at either full or half duplex. Line speeds range up to 9600 bits per second. Autodialing requires the installation of automatic dialing hardware at the RS366 port which interfaces with the modem.

Software requirements

The Remote Batch Service requires these program files:

- RemoteBatchSDF.bcd
- RBServiceConfig.bcd
- RS232CCommon.bcd
- CommSvcComSoft.bcd
- MailStubConfig.bcd
- RemoteBatchService.messages
- CommunicationServicesArea.messages

Allow 741 disk pages for the program files. Allow 500 disk more pages for the work space the Remote Batch Service needs.

The Remote Batch Service also requires access to the File Service, Clearinghouse Service, and Internetwork Routing Service.

Workstations accessing the Remote Batch Service require the installation of additional software.

6085 and 8010 workstations

Each 6085/8010 workstation must have VP NetCom or VP RemoteCom software installed. The VP NetCom software provides access to the File Service, Print Service, and Mail Service as well as to local resources. The VP RemoteCom software enables a remote workstation to access a wide range of network functions over a telephone line. Alternatively, an 8010 workstation can use the Standard 8010 Software for networked or remote operation.

860 workstations

The 860 workstation must have the 860 Ethernet Information Processing System (IPS) Services Software option installed. This option enables users to access the File Service and Print Service on the network.

Non-Xerox systems

Non-Xerox systems require asynchronous communication software with XModem protocol to provide access to network resources.

Dependencies and limitations

The Remote Batch Service has these dependencies and limitations:

- Access to the File Service, which contains the input and output file drawers for each partner.
- Access to the Clearinghouse Service, which locates the File Service, verifies user access to the Remote Batch Service file drawers, and assists the Mail Service in distributing error messages.
- Access to the Internetwork Routing Service, which provides access to services on other networks.
- Optionally, access to the Mail Service, which distributes error messages for incorrectly specified tasks.
- For optimum results, do not install the Remote Batch Service on the same server with highly interactive services such as the Clearinghouse Service, Mail Service, or Print Service.
- Do not install the Remote Batch Service on the same server with other services requiring the dedicated use of the local port. The other services include the External Communication Service IBM 3270 BSC emulation, the Internetwork Routing Service X.25 Communication Protocol, and the 850/860 Gateway Service.

Remote Batch Service Worksheet

Use the Remote Batch Service Worksheet to record server-related and service-related information. The worksheet is at the end of this chapter.

Fill out a separate copy of the worksheet for each Remote Batch Service for which you have System Administrator responsibility. Retain the original for future use, and store the completed worksheet in your *Activities Guide*.

Using the worksheet

Before you install the software and set up your Remote Batch Service, complete the worksheet. It is important that you fill out the worksheet accurately, and update it whenever changes occur.

The completed worksheet saves you time as you perform the setup and maintenance procedures. It also serves as an information source for new System Administrators unfamiliar with your network configuration.

Filling out the worksheet

As you read the rest of this chapter, you are directed to make entries on the Remote Batch Service Worksheet. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and the services installed on that server. Copy this information from the Services Installation Worksheet you filled out while reading the Services System Software chapter in this book. Also use section ① to record the name of the Clearinghouse group to which Remote Batch Service will become a member.

Use section ② to describe the RS232C port. Use section ③ to define a communication partner.

Planning for setup

After you install the Remote Batch Service, you must initialize it, add the port, and add a communication partner. You must also add the Remote Batch Service as a member of a Clearinghouse group and create two file drawers for each communication partner.

See the Remote Batch Service chapter in the *Services Installation and Setup Guide* for complete setup procedures.

Remote Batch Service name and description

You name and describe the Remote Batch Service during initialization. The name and description become part of the system-wide directory function that the Clearinghouse maintains.

When you name the Remote Batch Service, use a name different from all other names in the domain. The fully qualified Remote Batch Service name takes the form:

Remote Batch Service name:Domain:Organization

The domain and organization MUST be the same as the domain and organization of the server. For example, if the server name is Dallas:Home Office:ABC Company, then the Remote Batch Service name might be Sales:Home Office:ABC Company. It is recommended that you enter the local name only when you name the Remote Batch Service. This avoids possible errors and lets the domain and organization default to that of the server.

This naming convention gives the System Administrator for the server domain access to administrative commands for the Remote Batch Service. These commands are available only when you are enabled.

The service description may be the location, a department name, the name of the assigned System Administrator, or any other descriptive information.

You also perform a procedure to add the Remote Batch Service as a member of a group in the Clearinghouse Service. The Clearinghouse Service locates the File Service and verifies user access to the Remote Batch Service file drawers.

Related procedures: Initializing the Remote Batch Service, Creating a group for t;he Remote Batch Service

Filling out the worksheet

① **Name** - Record the name of the Remote Batch Service.

Description - Record the description of the Remote Batch Service.

Clearinghouse group name - Record the name of the Clearinghouse group to which you will add the Remote Batch Service.

Remote Batch Service port information

You configure the local port for the Remote Batch Service.

Related procedures: Adding the port for the Remote Batch Service

Filling out the worksheet

② **Name** - Record the name of the port the Remote Batch Service is using.

Description - Record a comment describing the purpose and location of the port.

Duplexity - Record whether the modem is full duplex or half duplex. Full duplex means the modem can transmit data in both directions at the same time. Half duplex means the modem can transmit data in both directions, but not at the same time. This setting must match at both the server and the partner.

Autodialer - Circle Y or N to indicate whether automatic dialing hardware is installed.

Line speed - Record the modem's line speed in bits per second. Valid speeds are 1200, 2400, 3600, 4800, 7200, and 9600 bps. This setting must match at both the server and the partner.

Autostarted - Circle Y or N to indicate whether this line is started when you start the Remote Batch Service.

Communication partner information

When you add a communication partner for the Remote Batch Service, you describe the partner for the software and create the file drawers the partner uses for job submission and retrieval. You can define more than one partner, but the Remote Batch Service can communicate with only one partner at a time.

Related procedures: Adding a communication partner, Creating file drawers for the communication partner

Filling out the worksheet

The Remote Batch Service has space for information about one communication partner. Use additional copies of the worksheet to record information about more partners.

③ **Name** - Record the name of the communication partner.

Description - Record a comment that describes the purpose and location of the partner.

File Service - Record the fully qualified name of the File Service supporting the Remote Batch Service.

Job submission file drawer - Record the name of the file drawer that holds Remote Batch Service jobs for transmission to the partner. Use a name that describes the function of the file drawer, such as Input Bin.

Check time - Record how often (number of minutes, 1 through 59) you want the Remote Batch Service to check the job submission file drawer for jobs.

Page limit - Record the number of disk pages you want to assign to the job submission file drawer.

Output retrieval file drawer - Record the name of the file drawer that holds the output from the partner. Use a name that describes the function of the file drawer, such as Output Bin.

Page limit - Record the number of disk pages you want to assign to the output retrieval file drawer.

Access rights - Assign read, write, add, and remove access rights to both file drawers.

Line usage - Record the type of line the Remote Batch Service is using: dedicated, automatic dialing, manual dialing, or answer only. Autodialing requires the installation of automatic dialing hardware at the RS366 port, which interfaces with the modem.

Restricted hours - Circle Y or N to indicate whether you want to restrict the hours during which Remote Batch Service operates. If you circle Y, you can automatically establish and terminate the connection with the partner. Record the start and stop times for this connection in 24-hour format.

Re-create connection - Record the number of jobs (1 through 32767) in the submission file drawer and the number of minutes to pass before the connection is re-established.

Terminate inactive connection - Circle Y to end the connection if the line is inactive for a specific number of seconds. Record the number of seconds (15 through 32767). Circle N to maintain the connection indefinitely.

Phone number - Record the number the Remote Batch Service dials to make the connection to the communication partner.

Terminal ID - Record the terminal identification. The host site supplies this information, which identifies the Remote Batch Service as a valid user to the host. The Terminal ID may be up to 15 characters long.

User security ID - Record the user password. The host site supplies this information, which validates the Remote Batch Service user to the host. The user security ID may be up to 15 characters long.

Station operation - Record whether this station is primary or secondary. The primary station has priority when two stations try to send at the same time.

Emulation device - Record the type of device protocol being emulated.

Communication device - Indicate whether the partner is a mainframe, a word processor, or an IBM 5520 Processor. If the partner is a mainframe or an IBM 5520 Processor, record the appropriate information:

- **Spooling program** - Circle the spooling program the partner uses to hold output awaiting transmission:

  JES (MVS) refers to the Job Entry Subsystem, which runs under the Multiple Virtual Storage operating system.

  POWER (DOS/VSE) refers to the POWER spooling program, which runs under the virtual storage version of the Disk Operating System (DOS).

  RSCS (VM/370) refers to the Remote Spooling Communications Subsystem file transfer system used by the 370 mainframe. This spooling system runs under the virtual memory version of DOS.

- **SIGNON** - Record the code that signals the beginning of a session; may be required by the partner.
- **SIGNOFF** - Record the code that signals the end of a session; may be required by the partner.

Record the codes exactly as required by the mainframe including capitalization or special spacing. Any errors could prevent communication.

- **Initial bid response** - Record whether the partner will use WACK/ACK (wait acknowledge/acknowledge) or NAK/ACK (negative acknowledge/acknowledge) to signal unsuccessful or successful transmission.

Block size - For 2770 devices, circle the maximum block size that can be sent to and received from the device. Valid sizes are 128, 256, and 512 bytes. A size of 400 bytes is preset for 2780 devices; a size of 512 bytes is preset for 3780 devices.

Default data interpretation - Circle the type of received data.

- DP refers to the IBM EBCDIC DP code set. This set retains line-ending codes. The received document looks like the original document.
- WP refers to the IBM EBCDIC WP code set. This set does not retain line-ending codes. The document is ready for editing.
- XNS refers to archive format. No changes are made to the document or its format.
- Uninterpreted means the data has an unknown format.

File type - If you circled Uninterpreted, now circle the type of file received:

- Text identifies the file as a typical ViewPoint document and is the same as user-defined file type 2. Text is the default option.
- Unspecified indicates the file is a text document and is the same as user-defined file type 0.
- User defined (numeric value) refers to application-oriented file types. Record the number that identifies the type of file. These file types are common in the ViewPoint environment:

0	Unspecified
1	File folder
2	Text
3	Serialized
4	Mail note
4098	File drawer
4101	Binary file
4226	BravoText
4230	XDE bcd file
4290	Print Service fonts
4352	Desktop
4353	Star Document
4355	Inbasket
4360	Outbasket
4361	Interpress master
4365	Record file
4379	Reference icon
5120	860 document

Print data interpretation - Record the text type of print data received:

- DP refers to the IBM EBCDIC DP code set. This set retains line-ending codes. The received document looks like the original document.
- WP refers to the IBM EBCDIC WP code set. This set does not retain line-ending codes. The document is ready for editing.
- XNS refers to archive format. No changes are made to the document or its format.
- Uninterpreted means the data has an unknown format.

Punch data interpretation - Record the text type of punch data received:

- DP refers to the IBM EBCDIC DP code set. This set retains line-ending codes. The received document looks like the original document.
- WP refers to the IBM EBCDIC WP code set. This set does not retain line-ending codes. The document is ready for editing.
- XNS refers to archive format. No changes are made to the document or its format.
- Uninterpreted means the data has an unknown format.

ETX - Circle Y or N to indicate whether you want the ETX (end of text) separator to appear between files in a task folder. This separator makes it easy to identify the end of each file.

Default partner option - Circle Y or N to start this partner when you start the Remote Batch Service.

Planning for maintenance

After you install and set up the Remote Batch Service, you are responsible for maintaining it. You perform maintenance as needed; there are no scheduled duties.

See the Remote Batch Service chapter of the *Services Maintenance Guide* for the complete maintenance procedures.

Making configuration changes

You make Remote Batch Service configuration changes by modifying port information, or by adding a communication partner or changing an existing one. You can also change the name of the service. See "Planning for setup" for explanations of port and partner information.

Notifying users

Reconfiguring the Remote Batch Service requires stopping the service. Make sure you notify all users that the Remote Batch Service will be temporarily interrupted.

Related procedures: Changing communication partner information, Changing RS232C port information, Deleting a communication partner, Deleting an RS232C port, Displaying a communication partner definition, Displaying RS232C port information, Renaming the Remote Batch Service

Changing the data interpretation

You can change a partner's data interpretation parameters without completely re-configuring the communication partner. These changes remain in effect until you restart the Remote Batch Service.

Related procedures: Setting and displaying data interpretation

Analyzing service statistics

The Remote Batch Service keeps a running log of all service statistics. Check this information to analyze service performance.

Most of the statistics simply provide information. However, certain communications statistics may indicate a problem. See *Basic Network Troubleshooting* for more information.

Related procedures: Showing Remote Batch Service statistics

Remote Batch Service statistics

This section of the statistics report shows when the Remote Batch Service was started and how long it has been running. The

section also indicates when data collection started and ended for this report.

Job processing statistics

This section of the statistics report details the number of jobs sent, received, and aborted.

Communications statistics

This section of the statistics report shows how the Remote Batch Service and the partner are handling communication. Check the following statistics carefully for possible problems.

<number> total send blocks NAK'd by remote - The total number of blocks not received (negatively acknowledged) by the partner. A large number may indicate a problem with the modem or communication link.

<number> TTDs sent - The number of temporary text delays sent by the binary synchronous communications (BSC) driver.

<number> ENQs sent - The number of times the Remote Batch Service asked the communication partner to resend the block.

<number> WAKs sent - The number of times the partner sent wait acknowledgments to the Remote Batch Service causing transmission delays.

<number> received checksum errors - The number of data blocks received containing errors. A large number may indicate a problem with the modem or communication link.

<number> garbled errors - The number of incomplete blocks received. If this number is larger than the number of sessions, you may have a problem with the modem or communication link.

Remote filing and code conversion statistics

This section of the statistics report provides information regarding the number of bytes converted and filed on the remote File Service, and the number of errors that occurred during this process.

Resource usage statistics

This section of the statistics report shows how the input bin is utilized, the total wait time, and how the scratch file space met the needs of the Remote Batch Service.

Service profile statistics

This section shows of the statistics report how much time the Remote Batch Service spent performing tasks.

Character codes

Tables 14-1 and 14-2 show how the Remote Batch Service translates 860 character codes to these IBM character codes:

- 2770/3780 EBCDIC WP
- 2770/3780 EBCDIC DP
- 2780 EBCDIC DP/WP

Table 14-1 lists the 860 characters and their corresponding EBCDIC characters. Several entries appear in square brackets:

- [Discard] indicates a reasonable equivalent does not exist; the Remote Batch Service discards the character or code.
- [unknown] indicates a reasonable equivalent does not exist; the Remote Batch Service inserts a question mark in the text.
- Any other entry within square brackets identifies a software procedure that is performed when the code is encountered.

Table 14-2 lists the software procedures, which are named after the 860 characters they convert.

Table 14-1. **860 to EBCDIC character code conversion**

	860		2770/3780 EBCDIC WP		2770/3780 EBCDIC DP		2780 EBCDIC DP/WP	
Sym	**Name**	**Hex**	**Name**	**Hex**	**Name**	**Hex**	**Name**	**Hex**
	EOS	00	[Discard]		[Discard]		[Discard]	
	NUL	01						
	space	20	space	40	space	40	space	40
!	exclamation	21	. (period)	4B	!	5A	!	5A
"	quotes	22	"	7F	"	7F	"	7F
#	pound	23	#	7B	#	7B	#	7B
$	dollar	24	$	5B	$	5B	$	5B
%	percent	25	%	6C	%	6C	%	6C
&	ampersand	26	&	50	&	50	&	50
'	apostrophe	27	'	7D	'	7D	'	7D
(	left paren	28	(	4D	(	4D	(	4D
)	right paren	29	)	5D	)	5D	)	5D
*	asterisk	2A	*	5C	*	5C	*	5C
+	plus	2B	+	4E	+	4E	+	4E
,	comma	2C	,	6B	,	6B	,	6B
-	hyphen	2D	- (req. hyphen)	60	- (req. hyphen)	60	- (req. hyphen)	60
.	period	2E	.	4B	.	4B	.	4B
/	slash	2F	/	61	/	61	/	61
0	zero (digit)	30	0	F0	0	F0	0	F0
1	one (digit)	31	d1	F1	d1	F1	d1	F1
2	two (digit)	32	d2	F2	d2	F2	d2	F2
3	three (digit)	33	d3	F3	d3	F3	d3	F3
4	four (digit)	34	d4	F4	d4	F4	d4	F4
5	five (digit)	35	d5	F5	d5	F5	d5	F5
6	six (digit)	36	d6	F6	d6	F6	d6	F6
7	seven (digit)	37	d7	F7	d7	F7	d7	F7
8	eight (digit)	38	d8	F8	d8	F8	d8	F8
9	nine (digit)	39	d9	F9	d9	F9	d9	F9
:	colon	3A	:	7A	:	7A	:	7A
;	semicolon	3B	;	5E	;	5E	;	5E
<	less than	3C	((leftParen)	4D	<	4C	<	4C
=	equals	3D	=	7E	=	7E	=	7E
>	greaterThan	3E	) (rightParen)	5D	>	6E	>	6E
?	question mark	3F	?	6F	?	6F	?	6F
@	at	40	@	7C	@	7C	@	7C
A	(upper-case)	41	A	C1	A	C1	A	C1
B	(upper-case)	42	B	C2	B	C2	B	C2
C	(upper-case)	43	C	C3	C	C3	C	C3
D	(upper-case)	44	D	C4	D	C4	D	C4
E	(upper-case)	45	E	C5	E	C5	E	C5
F	(upper-case)	46	F	C6	F	C6	F	C6
G	(upper-case)	47	G	C7	G	C7	G	C7

Sym	860 Name	Hex	2770/3780 EBCDIC WP Name	Hex	2770/3780 EBCDIC DP Name	Hex	2780 EBCDIC DP/WP Name	Hex
H	(upper-case)	48	H	C8	H	C8	H	C8
I	(upper-case)	49	I	C9	I	C9	I	C9
J	(upper-case)	4A	J	D1	J	D1	J	D1
K	(upper-case)	4B	K	D2	K	D2	K	D2
L	(upper-case)	4C	L	D3	L	D3	L	D3
M	(upper-case)	4D	M	D4	M	D4	M	D4
N	(upper-case)	4E	N	D5	N	D5	N	D5
O	(upper-case)	4F	O	D6	O	D6	O	D6
P	(upper-case)	50	P	D7	P	D7	P	D7
Q	(upper-case)	51	Q	D8	Q	D8	Q	D8
R	(upper-case)	52	R	D9	R	D9	R	D9
S	(upper-case)	53	S	E2	S	E2	S	E2
T	(upper-case)	54	T	E3	T	E3	T	E3
U	(upper-case)	55	U	E4	U	E4	U	E4
V	(upper-case)	56	V	E5	V	E5	V	E5
W	(upper-case)	57	W	E6	W	E6	W	E6
X	(upper-case)	58	X	E7	X	E7	X	E7
Y	(upper-case)	59	Y	E8	Y	E8	Y	E8
Z	(upper-case)	5A	Z	E9	Z	E9	Z	E9
[	left bracket	5B	[	4A	{ (left brace)	C0	((left paren)	4D
\	backslash	5C	/ (slash)	61	\	E0	/ (slash)	61
]	right bracket	5D	[	5A	} (rightBrace)	D0	) (right paren)	5D
↑	up arrow	5E	| (vertical bar)	4F	| (vertical bar)	4F	| (vertical bar)	4F
_	underscore	5F	_	6D	_	6D	_	6D
¢	cent	60	¢	5F	¢	4A	¢	4A
a	(lower-case)	61	a	81	a	81	a	81
b	(lower-case)	62	b	82	b	82	b	82
c	(lower-case)	63	c	83	c	83	c	83
d	(lower-case)	64	d	84	d	84	d	84
e	(lower-case)	65	e	85	e	85	e	85
f	(lower-case)	66	f	86	f	86	f	86
g	(lower-case)	67	g	87	g	87	g	87
h	(lower-case)	68	h	88	h	88	h	88
i	(lower-case)	69	i	89	i	89	i	89
j	(lower-case)	6A	j	91	j	91	j	91
k	(lower-case)	6B	k	92	k	92	k	92
l	(lower-case)	6C	l	93	l	93	l	93
m	(lower-case)	6D	m	94	m	94	m	94
n	(lower-case)	6E	n	95	n	95	n	95
o	(lower-case)	6F	o	96	o	96	o	96
p	(lower-case)	70	p	97	p	97	p	97
q	(lower-case)	71	q	98	q	98	q	98
r	(lower-case)	72	r	99	r	99	r	99
s	(lower-case)	73	s	A2	s	A2	s	A2
t	(lower-case)	74	t	A3	t	A3	t	A3
u	(lower-case)	75	u	A4	u	A4	u	A4
v	(lower-case)	76	v	A5	v	A5	v	A5
w	(lower-case)	77	w	A6	w	A6	w	A6

Sym	860 Name	860 Hex	2770/3780 EBCDIC WP Name	2770/3780 EBCDIC WP Hex	2770/3780 EBCDIC DP Name	2770/3780 EBCDIC DP Hex	2780 EBCDIC DP/WP Name	2780 EBCDIC DP/WP Hex
x	(lower-case)	78	x	A7	x	A7	x	A7
y	(lower-case)	79	y	A8	y	A8	y	A8
z	(lower-case)	7A	z	A9	z	A9	z	A9
{	left brace	7B	[(left bracket)	4A	{	C0	((left paren)	4D
|	vertical bar	7C	|	4F	|	4F	|	4F
}	right brace	7D	] (right bracket)	5A	}	D0	) (right paren)	5D
~	tilde	7E	- (req. hyphen)	60	~	A1	- (req. hyphen)	60
	DEL	7F	DEL	07	DEL	07	[Discard]	
	BSO	80	[Discard]		[Discard]		[Discard]	
	ESO	81	[Discard]		[Discard]		[Discard]	
	BBD	82	[Discard]		[Discard]		[Discard]	
	EBD	83	[Discard]		[Discard]		[Discard]	
	BUS	84	[Discard]		[Discard]		[Discard]	
	EUS	85	[Discard]		[Discard]		[Discard]	
	PGNO	88	# (pound)	7B	# (pound)	7B	# (pound)	7B
	CDU	89	[Discard]		[Discard]		[Discard]	
	RVN	8A	[Discard]		[Discard]		[Discard]	
	HLT	8B	BEL	2F	[Discard]		[Discard]	
	ESI	8D	[ESIxwp]		[ESIxdp]		[ESIx80]	
	AREF	8E	[AREFxwp]		[AREFxdp]		[AREFx80]	
	REF	8F	[REFxwp]		[REFxdp]		[REFx80]	
	FMT	90	[FMTxwp]		[FMTxdp]		[FMTx80]	
	CMD	91	[CMDxwp]		[CMDxdp]		[CMDx80]	
	NCOL	92	[Discard]		[Discard]		[Discard]	
	RNCOL	93	[Discard]		[Discard]		[Discard]	
	PGE	94	FF	0C	FF	0C	FF	0C
	RPGE	95	EOP	3A	FF	0C	FF	0C
	CRN	96	[CRNxwp]		IRS	1E	[CRNx80]	
	PCR	97	[PCRxwp]		IRS	1E	[PCRx80]	
	RET	98	IRS	1E	IRS	1E	[CRNx80]	
	TAB	99	IT	39	HT	05	[TABx80]	
	PTB	9A	HT	5	HT	05	[PTBx80]	
	LFEED	9B	LF	25	LF	25	LF	25
	INX	9C	[INXxwp]		[INXxdp]		[INXx80]	
	RIX	9D	[RIXxwp]		[Discard]		[Discard]	
	UBS	9E	UBS	1A	[Discard]		[Discard]	
	PBS	9F	NBS	36	BS	16	BS	16
	PSP	A0	RSP	41	RSP	41	SP	40
	THYP	A1	[THYPxwp]		[THYPxdp]		[THYPx80]	
2	(superscript)	A2	2	C0	2 (digit)	F2	2 (digit)	F2
3	(superscript)	A3	3	D0	3 (digit)	F3	3 (digit)	F3
°	degree	A4	°	A1	* (asterisk)	5C	* (asterisk)	5C
µ	micro	A5	u (lower-case)	A4	u (lower-case)	A4	u (lower-case)	A4
¶	paragraph	A6	¶	6E	P (upper-case)	D7	P (upper-case)	D7
§	section	A7	§	4C	S (upper-case)	E2	S (upper-case)	E2

Sym	860 Name	860 Hex	2770/3780 EBCDIC WP Name	2770/3780 EBCDIC WP Hex	2770/3780 EBCDIC DP Name	2770/3780 EBCDIC DP Hex	2780 EBCDIC DP/WP Name	2780 EBCDIC DP/WP Hex
(	(expanded)	A8	((left paren)	4D	((left paren)	4D	((left paren)	4D
)	(expanded)	A9	) (right paren)	5D	) (right paren)	5D	) (right paren)	5D
	ESPA	AA	NSP	E1	(space)	40	(space)	40
±	plus or minus	AB	±	79	+ (plus)	4E	+ (plus)	4E
,	(expanded)	AC	, (comma)	6B	, (comma)	6B	, (comma)	6B
-	(expanded)	AD	- (RHY)	60	- (RHY)	60	- (RHY)	60
.	(expanded)	AE	. (period)	4B	. (period)	4B	. (period)	4B
.	abbreviation	AF	. (period)	4B	. (period)	4B	. (period)	4B
÷	divide	B0	/ (slash)	61	/ (slash)	61	/ (slash)	61
®	registered	B1	r (lower-case)	99	r (lower-case)	99	r (lower-case)	99
•	dot	B2	. (period)	4B	. (period)	4B	. (period)	4B
™	trademark	B3	T (upper-case)	E3	T (upper-case)	E3	T (upper-case)	E3
©	copyright	B4	c (lower-case)	83	c (lower-case)	83	c (lower-case)	83
↓	down arrow	B5	v (lower-case)	A5	v (lower-case)	A5	v (lower-case)	A5
≠	not equal	B6	# (pound)	7B	# (pound)	7B	# (pound)	7B
∇	diamond	B7	° (degree)	A1	? [unknown]	6F	* (asterisk)	5C
▶	DELL	B8	? [unknown]	6F	? [unknown]	6F	? [unknown]	6F
	grave accent	B9	' (apostrophe)	7D	' (apostrophe)	7D	' (apostrophe)	7D
	circumflex	BA	? [unknown]	6F	? [unknown]	6F	? [unknown]	6F
¼	quarter	BB	¼	E0	[QUARxdp]		[QUARx80]	
⅓	third	BC	[THRDxwp]		[THRDxdp]		[THRDx80]	
½	half	BD	½	6A	[HALFxdp]		[HALFx80]	
⅔	two-third	BE	[THRDxwp]		[THRDxdp]		[THRDx80]	
¾	three-quarter	BF	[THREEQUARxwp]		[THREEQUARxdp]		[THREEQUARx80]	
+	graphic intersect	C0	+ (plus)	4E	+ (plus)	4E	+ (plus)	4E
-	graphic horiz line	C1	notInXtoWPTable		notInXtoDPTable		notInXtoE80Table	
|	graphic vert line	C2	- (RHY)	60	- (RHY)	60	- (RHY)	60
+	bold graphic	C3	+ (plus)	4E	+ (plus)	4E	+ (plus)	4E
-	bold graphic	C4	- (RHY)	60	- (RHY)	60	- (RHY)	60
|	bold graphic	C5	| (vertical bar)	4F	| (vertical bar)	4F	| (vertical bar)	4F
	shade	C6	? [unknown]	6F	? [unknown]	6F	? [unknown]	6F
Æ	(upper-case)	D0	A (upper-case)	C1	A (upper-case)	C1	A (upper-case)	C1
æ	(lower-case)	D1	a (lower-case)	81	a (lower-case)	81	a (lower-case)	81
Ø	slashed O (u-case)	D2	O (upper-case)	D6	O (upper-case)	D6	O (upper-case)	D6
ø	slashed o (l-case)	D3	o (lower-case)	96	o (lower-case)	96	o (lower-case)	96
ł	lind	D4	? [unknown]	6F	? [unknown]	6F	? [unknown]	6F
œ	Œ	D5	o (lower-case)	96	o (lower-case)	96	o (lower-case)	96
ij	IJ	D6	i (lower-case)	89	i (lower-case)	89	i (lower-case)	89
'n	apostrophe-n	D7	n (lower-case)	95	n (lower-case)	95	n (lower-case)	95
₡	cruz (money)	D8	C (upper-case)	C3	C (upper-case)	C3	C (upper-case)	C3
Pts	pesetas (money)	D9	P (upper-case)	D7	P (upper-case)	D7	P (upper-case)	D7
ƒ	florin (money)	DA	f (lower-case)	86	f (lower-case)	86	f (lower-case)	86
£	pounds (money)	DB	L (upper-case)	D3	L (upper-case)	D3	L (upper-case)	D3
¥	yen (money)	DC	Y (upper-case)	E8	Y (upper-case)	E8	Y (upper-case)	E8
$		DD	? [unknown]	6F	? [unknown]	6F	? [unknown]	6F
¡	inverted excl	DE	i (lower-case)	89	i (lower-case)	89	i (lower-case)	89
¿	inverted question	DF	? (question)	6F	? (question)	6F	? (question)	6F

Sym	860 Name	860 Hex	2770/3780 EBCDIC WP Name	2770/3780 EBCDIC WP Hex	2770/3780 EBCDIC DP Name	2770/3780 EBCDIC DP Hex	2780 EBCDIC DP/WP Name	2780 EBCDIC DP/WP Hex
ß	German ss	E0	B (upper-case)	C2	B (upper-case)	C2	B (upper-case)	C2
ℓ	litre	E1	l (lower-case)	93	l (lower-case)	93	l (lower-case)	93
o̲	underlined o	E2	o (lower-case)	96	o (lower-case)	96	o (lower-case)	96
a̲	underlined a	E3	a (lower-case)	81	a (lower-case)	81	a (lower-case)	81
Å	A with circle	E4	A (upper-case)	C1	A (upper-case)	C1	A (upper-case)	C1
å	a with circle	E5	a (lower-case)	81	a (lower-case)	81	a (lower-case)	81
`	u-case grave	E7	' (apostrophe)	7D	`(grave)	79	' (apostrophe)	7D
^	u-case circumflex	E8	? [unknown]	6F	? [unknown]	6F		
¨	umlaut	E9	[Discard]		NUL	00	[Discard]	
~	tilda	EA	[Discard]		NUL	00	[Discard]	
'	accent	EB	' (apostrophe)	7D	' (apostrophe)	7D	' (apostrophe)	7D
`	l-case grave	EC	apostrophe	7D	grave	79	apostrophe	7D
^	l-case circumflex	ED	[Discard]		NUL	00	[Discard]	
	CDL	EE	[Discard]		NUL	00	[Discard]	
	ULN	EF	[Discard]		NUL	00	[Discard]	
	USEP	FB	? [unknown]	6F	? [unknown]	6F	? [unknown]	6F
	GSEP	FC	? [unknown]	6F	? [unknown]	6F	? [unknown]	6F
	FSEP	FD	? [unknown]	6F	? [unknown]	6F	? [unknown]	6F
	RSEP	FE	? [unknown]	6F	? [unknown]	6F	? [unknown]	6F
	SOS	FF	[Discard]		[Discard]		[Discard]	

Notes

1. FMT is the 860 format group character. FMT is followed by a set of parameters that define such properties as margins, tabs, line spacing, and justification. Values for these properties remain in effect until another FMT is encountered. FMT parameters are arranged in fields, separated by FSEP characters. Only one field, format type, is required; there are six remaining optional fields.

   The FMT conversion procedures translate FMT parameters to their nearest equivalents among EBCDIC page formatting codes. See the "860 Document File Format," Version 1.4, for a description of FMT parameters.

2. CMD is the 860 command group character. A leading CMD is followed by one of six command classifiers that dictates the action to be performed on text that lies between CMDs. Actions include recording a null, centering within columns or margins, and making text flush right.

   The CMD conversion procedures look for a command specifier immediately following the CMD. If a command classifier is present it looks for an optional argument to that classifier and translates the command to its nearest EBCDIC equivalent. See the "860 Document File Format," Version 1.4, for a description of CMD command classifiers and arguments.

Table 14-2. **Conversion procedures**

Procedure Name	860 Character Description	Function
AREFxwp, AREFxdp, AREFx80	Alternate reference group	Discard AREF and all characters up to and including next AREF.
CMDxwp, CMDxdp, CMDx80	Command group	See note 2.
CRNxwp, CRNx80	Carriage return	If CRN, PCR, or PTB is encountered, output an RCR (06h, an EBCDIC WP carriage return), then an IRS (1Eh).
ESIxwp, ESIxdp, ESIx80	Used in conversions. 860 ignores intervening characters.	Once ESI is encountered, discard all characters until HLT is encountered.
FMTxwp, FMTxdp, FMTx80	Format group	See note 1.
HALFxdp, HALFx80	$\frac{1}{2}$	Output a one, a slash, and a two.
INXxwp	Index. Move vertical position down 1/24 inch.	Outputs SBS (38h).
INXxdp, INXx80	Index. Move vertical position down 1/24 inch.	Discard INX character.
PCRxwp, PCRx80	Precedented (required) carriage return.	Same as procedures for CRN.
QUARxdp, QUARx80	$\frac{1}{4}$	Output a one, a slash, and a four.
REFxwp, REFxdp, REFx80	Reference group.	Same as procedures for AREF.
RIXxwp	Reverse Index. Move vertical position up 1/24 inch.	Output SPS (9h).
THRDxwp, THRDxdp, THRDx80 (in response to $\frac{1}{3}$)	$\frac{1}{3}$	Output a one, a slash, and a three.
THRDxwp, THRDxdp, THRDx80 (in response to $\frac{2}{3}$)	$\frac{2}{3}$	Output a two, a slash, and a three.
THREEQUARxwp, THREEQUARxdp, THREEQUARx80	$\frac{3}{4}$	Output a three, a slash, and a four.
THYPxwp	Temporary hyphen	Look for a following CRN or PCR character. If a CRN is found, procedures output SHY (CAh), then IRS (1Eh). If a PCR is found, procedures output SHY, then RCR (06h). If neither a CRN or PCR is present, the THYP is discarded.
THYPxdp, THYPx80	Temporary hyphen	Look for a following CRN or PCR character. If a CRN is found, procedures output RHY (60h), then IRS (1Eh). If a PCR is found, procedures output SHY, then RCR. If neither a CRN or PCR is present, the THYP is discarded.

Notes

The following EBCDIC 2770 WP characters have no mapping from Xerox 860 characters (all numerical equivalents are in hexadecimal):

NUL	00	BS	16	CU2	2B
RCR	06	IGS	1D	IRT	33
SPS	09	WUS	23	SBS	38
RPT	0A	ESC	27	SHY	CA
NL	15	SW	2A		

The following EBCDIC 2770 DP characters have no mapping from Xerox 860 characters (all numerical equivalents are in hexadecimal):

RCR	06	ESC	27	IT	39
SPS	09	SW	2A	EOP	
RPT	0A	CU2	2B	negation	5F
NL	15	BEL	2F	or	6A
UBS	1A	IRT	33	SHY	CA
IGS	1D	NBS	36	NSP	E1
WUS	23	SBS	38		

The following EBCDIC 2780 DP/WP characters have no mapping from Xerox 860 characters (all numerical equivalents are in hexadecimal):

HT	05	ESC	27
EM	19	BEL	2F
IUS	1F		

15. 850/860 Gateway Service

This chapter helps you prepare for installation, setup, and maintenance of the 850/860 Gateway Service (GWS). This information supports the procedures you perform from an 8000 or 8090 server.

Service description

The 850/860 Gateway Service acts as a gateway to and from the Xerox Network System (XNS) internetwork. Users can move information originating outside the internetwork to workstations on the internet and vice versa.

Users of non-networked, communicating 850 and 860 workstations can exchange information over telephone lines with users on the internetwork. The 850/860 Gateway Service also functions as an access agent for computers or terminals that are not compatible with XNS protocols.

The 850/860 Gateway Service:

- Lets users of 850 and 860 workstations access the Mail Service
- Transfers documents through the mail to 6085 or 8010 workstations

The 850/860 Gateway Service expands the computing resources of workstations. For example, a user can create a document using an 850 or 860 workstation located outside the internetwork and send the document to a 6085 user by dialing the 850/860 Gateway Service. The 6085 user can change the document, print it, and store it on a File Service that other individuals can access.

How the software works

The 850/860 Gateway Service communicates in 850 and 860 protocols as well as XNS protocols. A networked 860 workstation can connect directly to an Ethernet cable and function as an XNS workstation. A non-networked user can dial the 850/860 Gateway Service and exchange documents with workstation users on the internet or with other remote workstations.

Because the XNS can handle information in the 860 format, the 850/860 Gateway Service acts as a transfer agent between the 860 and the internetwork. It moves documents back and forth without altering the original document.

The 850/860 Gateway Service converts documents from 850 to 860 format before transferring them to the internetwork. The 850/860 Gateway Service does not alter the document during the format conversion.

How the 850/860 Gateway Service works with 850/860 workstations

An 850/860 workstation uses a modem to communicate over telephone lines to the 850/860 Gateway Service. The 850/860 user begins communication with the internetwork by dialing the 850/860 Gateway Service. The 850/860 Gateway Service communicates with one stand-alone workstation at a time. If the 850/860 Gateway Service is already in use, the user receives a busy signal.

When the connection is made, the user instructs the 850/860 to transmit one or more documents to the 850/860 Gateway Service. At this point, the procedure is the same as sending documents to other communicating 850 or 860 workstations.

The 850/860 Gateway Service communicates with a remote workstation in 850/860 protocol. It converts documents from 850 to 860 format incorporating messages or files from the remote user into mail messages. The 850/860 Gateway Service then directs the mail messages to the Mail Service using the XNS protocol.

Users can send 860 documents to any network member. Users can read a document at an 850 or an 860 workstation and can convert a document to ViewPoint format at a 6085 workstation.

Mail delivery

The 850/860 communication protocols do not support delivery to individual recipients. You assign a user as a mail clerk. The 850/860 Gateway Service sends all documents to the mail clerk's mailbox. The mail clerk regularly checks the mailbox, determines the intended recipients, and uses the Mail Service to forward the documents.

Communicating 850/860 users can transmit the contents of their mailboxes. When the 850/860 Gateway Service receives a request, it transmits the documents in the mailbox over the telephone line to the user's workstation. If the receiving workstation is an 850, the 850/860 Gateway Service converts documents from 860 to 850 format.

Since mail is sent to individual users rather than specific workstations, users can retrieve their mail at any workstation as long as they can access the Mail Service containing their mailbox.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the 850/860 Gateway Service Worksheet, located at the end of this chapter.
- Installing the 850/860 Gateway Service software as described in the Server Software Installation chapter of the *Services Installation and Setup Guide*.
- Setting up the 850/860 Gateway Service as described in the 850/860 Gateway Service chapter of the *Services Installation and Setup Guide*.
- Maintaining the 850/860 Gateway Service as described in the 850/860 Gateway Service chapter of the *Services Maintenance Guide*.
  - Analyzing the statistics gathered by the 850/860 Gateway Service to determine how it is handling user requests.
  - Upgrading hardware and software as required.
  - Notifying users of any change or disruption in the service.
- Troubleshooting the service as described in *Basic Network Troubleshooting*.

You can perform most 850/860 Gateway Service procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter in the *Services Installation and Setup Guide* contains the procedures for installing the 850/860 Gateway Service software. This section explains hardware, software, and other requirements to prepare you for installation.

Hardware requirements

The 850/860 Gateway Service operates on an 8000 or an 8090 server.

The 850/860 Gateway Service requires an RS232C Communication Kit to provide dedicated use of the server's local port. The 850/860 Gateway Service cannot use the 873 Communication Interface Unit or the Multiport Option Kit.

The 850/860 Gateway Service uses a synchronous modem operating at full or half duplex. The server modem must be set for auto-answer. The connection is manually dialed by the remote 850 or 860 user.

If an 860 user wants to use the same type of modem for both 850/860 Gateway Service communication (synchronous) and 860 point-to-point communication (asynchronous or synchronous), the modem must have a switch setting to alternate between the two types.

Software requirements

The 850/860 Gateway Service requires these program files:

- GatewaySDF.bcd
- GWServiceConfig.bcd
- RS232CCommon.bcd
- CommSvcComSoft.bcd
- MailStubConfig.bcd
- GatewayService.messages
- CommunicationServicesArea.messages

Allow 462 disk pages for these program files.

In addition, the 850/860 Gateway Service requires access to the Mail Service and the Clearinghouse Service.

Workstation requirements

The workstations accessing the 850/860 Gateway Service require the installation of additional software.

850 workstation

This workstation requires the installation of the Xerox 850 Communication Kit and Communication Mode 1 Software. These options let stand-alone 850s communicate with other Xerox devices in point-to-point mode and communicate with the network's Mail Service to access the 850/860 Gateway Service.

860 workstation

This workstation requires the installation of the 860 Communications Accessory, which is a hardware option consisting of a circuit board, cables and internal RS232C connectors. The workstation also requires point-to-point communication software (2770/2780/PTP Communication Software or TTY/PTP Communication Software). The hardware and software combination lets 860s access the Mail Service by communicating in point-to-point mode.

Dependencies and limitations

- You cannot install the 850/860 Gateway Service on the same server with other services requiring the dedicated use of the server's local port. These services include the Remote Batch Service, Internetwork Routing Service X.25 option, and IBM 3270 BSC.
- The 850/860 Gateway Service needs access to these services to perform its tasks:
  - The Mail Service, which contains the mailboxes for each individual
  - The Clearinghouse Service, which provides address information for mail delivery

850/860 Gateway Service Worksheet

Use the 850/860 Gateway Service Worksheet to record server-related and service-related information. The worksheet is at the end of this chapter.

Fill out a separate copy of the worksheet for each 850/860 Gateway Service for which you have System Administrator responsibility. Retain the original for future use, and store the completed worksheet in your *Activities Guide*.

Using the worksheet

Before you install the software and set up your 850/860 Gateway Service, complete the 850/860 Gateway Service worksheet. It is important that you fill out the worksheet accurately, and update it whenever changes occur. The completed worksheet saves you time as you perform the setup and maintenance procedures. It also serves as an information source for new System Administrators unfamiliar with your configuration.

Filling out the worksheet

As you read the rest of this chapter, you are directed to make entries on the 850/860 Gateway Service Worksheet. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and the services installed on that server. Copy this information from the Services Installation Worksheet you filled out while reading the Services System Software chapter of this book.

Use section ② to describe the mail clerk you want to distribute mail. Use section ③ to define the server's modem.

Planning for setup

After you install the 850/860 Gateway Service, you must initialize it, add a mail clerk, assign the clerk a mailbox, and define the local port. See the 850/860 Gateway Service chapter in the *Services Installation and Setup Guide* for complete setup procedures.

850/860 Gateway Service name and description

You name and describe the 850/860 Gateway Service during initialization. The name and description become part of the system-wide directory function that the Clearinghouse maintains.

When you name the 850/860 Gateway Service, use a name different from all other names in the domain. The fully qualified 850/860 Gateway Service name takes the form:

850/860 Gateway Service name:Domain:Organization

The domain and organization must be the same as the domain and organization of the server. For example, if the server name is Dallas:Home Office:ABC Company, then the 850/860 Gateway Service name might be Sales:Home Office:ABC Company. To avoid possible errors, enter only the local name when you name the 850/860 Gateway Service. This approach lets the domain and organization default to those of the server.

This naming convention gives the System Administrator for the server domain access to System Administrator commands for the 850/860 Gateway Service. These commands are available only when you are enabled.

The service description may be the location, a department name, the name of the assigned System Administrator, or any other descriptive information.

Carefully choose the service name. You can only change the Gateway Service name by expunging and reinstalling the service.

Related procedure: Initializing the 850/860 Gateway Service

Filling out the worksheet

① Record the name and description of the 850/860 Gateway Service.

850/860 Gateway Service mail clerk

After you initialize the 850/860 Gateway Service, you must specify the name of the mail clerk and create a mailbox for the mail clerk. When you specify the mail clerk's name, use the local name only so the domain and organization can default to those of the 850/860 Gateway Service. If the mail clerk's domain and organization are not the same as those of the 850/860 Gateway Service, the 850 or 860 cannot retrieve mail from the 850/860 Gateway Service.

Related procedures: Adding a mail clerk, Giving your clerk a mailbox

Filling out the worksheet

② **Fully qualified name** - Record the fully qualified name of the mail clerk.

Password - Record the password for the mail clerk.

Aliases - Record any aliases the mail clerk use.

Description - Record a comment that describes the purpose or function of the mail clerk.

Home File Service - Record the name of the File Service supporting the mail clerk.

850/860 Gateway Service port information

You must configure the local port for the 850/860 Gateway Service. When you specify the mail clerk's domain and organization, they must be the same as those of the 850/860 Gateway Service. Otherwise, the 850 or 860 cannot retrieve mail from the 850/860 Gateway Service.

Related procedures: Configuring a local port

Filling out the worksheet

③ **Line speed** - Record the modem's line speed in bits per second. Valid speeds are 300, 1200, and 2400 bps. This setting must match at both the sending and receiving ends.

Duplexity - Record whether the modem is full duplex or half duplex. Full duplex means the modem can transmit data in both directions at the same time. Half duplex means the modem can transmit data in both directions, but not at the same time. This setting must match at both the sending and receiving ends.

Planning for maintenance

After you install and set up the 850/860 Gateway Service, you are responsible for maintaining it properly. You perform maintenance as needed; there are no scheduled duties.

This section provides guidelines for making configuration changes and analyzing service statistics.

See the 850/860 Gateway Service chapter in the *Services Maintenance Guide* for the complete maintenance procedures.

Making configuration changes

You make 850/860 Gateway Service configuration changes by adding a different mail clerk or changing the port information. When you make configuration changes, you need to stop and restart the service. Be sure to notify all users that the 850/860 Gateway Service will be temporarily interrupted.

See "Planning for setup" for explanations of the mail clerk and port information.

Related procedure: Changing the 850/860 Gateway Service information

Forwarding mail to 850/860 network users

As System Administrator, you have already assigned a network user to be the mail clerk. Now you must ensure that the mail clerk has the required information to perform the job. The mail clerk's major duties are checking daily for incoming mail and forwarding it to the appropriate receiver.

The mail clerk receives mail from remote 850 or 860 workstation users through the 850/860 Gateway Service. Incoming mail is stored in the mail clerk's In-Box. Document titles display with a prefix of X860 (for example, X86047689).

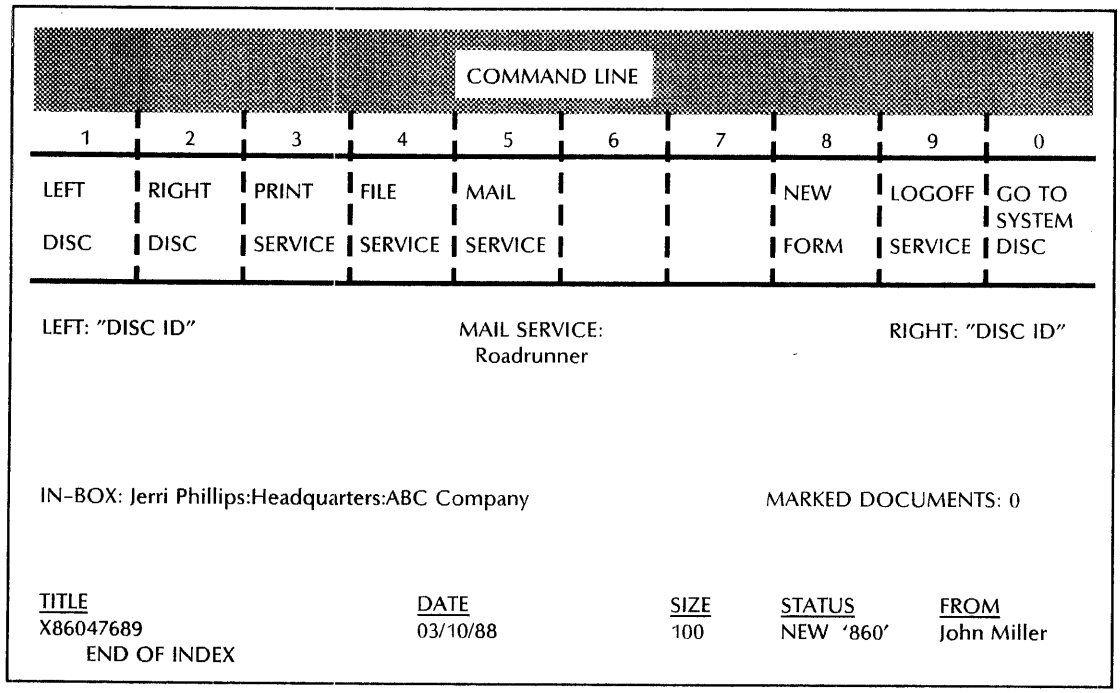
The mail clerk must view each incoming document to find out the intended receiver before forwarding it. Since the documents are in 860 format, the mail clerk can view a document from an 860 workstation without converting it. If the mail clerk is using an 850 workstation, the Gateway Service automatically converts the document from 860 to 850 format. If the mail clerk is using a 6085 or 8010 workstation, he or she must convert the document before forwarding it.

Once the mail clerk has forwarded a document, the receiver can log on to the Mail Service and retrieve it from his or her In-Box.

ViewPoint documents are converted into 860 format when sent through the 850/860 Gateway Service. If the receiver intends to return this document through the 850/860 Gateway Service, he or she first must use the 860 editor to properly format the document.

Figure 15-1 shows an 850/860 workstation display of the Mail Service Activity Page. Note that the mail clerk's In-Box contains incoming mail.

Figure 15-1. **Mail Service Activity Page showing incoming mail**



See the 850/860 Gateway Service chapter of the *Services Maintenance Guide* and the documentation accompanying your 850/860 workstation for more information.

Related procedure: Checking for mail

Analyzing service statistics

The 850/860 Gateway Service keeps a running log of all service statistics. Periodically check this information to analyze the performance of the 850/860 Gateway Service.

You can display configuration information, list statistics, and determine the state of the RS232C line. The display includes the current configuration data including the local port line number, the line speed, and the fully qualified name of the mail clerk. The display also shows the state of the RS232C line:

- Awaiting incoming calls - indicates there is no active user of the 850/860 Gateway Service at this time, the 850/860 Gateway Service is initialized, and is awaiting the next dial-in user.
- Active - indicates someone is using the 850/860 Gateway Service.
- Idle - indicates the line is not in use and is not awaiting the next dial-in user. If this condition persists, reactivate the line by restarting the 850/860 Gateway Service.

Statistics are reset when you boot the server or restart the 850/860 Gateway Service. Unless otherwise noted, a statistic does not display unless its value is greater than zero.

Statistics and their meanings are:

Communication session statistics

 # total sessions - the number of dial-in sessions since the last boot or restart; the list always contains this statistic.

 # total blocks sent - the number of data blocks sent by the 850/960 Gateway Service; sent data is data retrieved by an 860; the list always contains this statistic.

 # total send blocks NAK'd by remote - the total number of data blocks not received (negatively acknowledged) by the 860; a large number may indicate a problem with the modem or communication link.

 # good data blocks received - the number of good data blocks received by the 850/860 Gateway Service from an 860; the list always contains this statistic.

 # WAKs sent - the number of wait acknowledges (WAKs) sent; the 850/860 Gateway Service sends WAKs when it has received data from the 860, but is waiting for a response from the Mail Service before it transfers the data; under normal circumstances, this number will be fairly large.

 # ENQs sent - the number of enquiries (ENQs) the 850/860 Gateway Service sent to the 860 or 850 requesting that the previous block be resent; a large number may indicate a problem with the modem or communication link.

 # received checksum errors - the number of data blocks received by the 850/860 Gateway Service containing errors; a large number may indicate a problem with the modem or communication link.

 # garbled data errors - the number of incomplete blocks received. When the modem disconnects, one or more incomplete blocks are generally received. This statistic is not an indication of a problem unless the number is much larger than the number of sessions. A large number may indicate a problem with the modem or communication link.

 # audible signals received - the number of audible signals (BELs) received by the 850/860 Gateway Service. Normally, the Xerox 860 does not send BELs to the 850/860 Gateway Service because there is no operator present there.

 # invalid terminal IDs received - the number of times a session ended before the dial-in terminal was able to identify itself as an 860 or 850. This may occur when terminals try to connect to the 850/860 Gateway Service at the same time, or if there are other failures at either the terminal or the 850/860 Gateway Service.

Mail Service or related failures

 # open mail folder failures - the number of times the user's mail folder could not be opened due to a Mail Service failure; this may also occur because an invalid user name/password was used.

 # delete mail failures - the number of times the delete operation failed. After the 850/860 Gateway Service transfers mail to the 860, it deletes the message from the user's mailbox. A

large number of failures could indicate a problem with the Mail Service or an access control problem.

 # deliver mail failures - the number of times the 850/860 Gateway Service could not deliver a piece of received mail. A large number of failures could indicate a problem with the Mail Service or an access control problem.

 # security IDs received - the number of security identifications received; the 860s and 850s do not send security identifications.

 # invalid file polls received - the number of times the 850/860 Gateway Service received an invalid name or password.

 # mail folder search failures - the number of times the 850/860 Gateway Service could not locate the user's mailbox; this occurs when an invalid name/password was used or the user did not have a mailbox.

Translation/format errors

 # 850 to 860 translation logic failures - the number of translation failures; to communicate with an 850, the 850/860 Gateway Service must translate mail between 850 and 860 format.

 # 850 format errors - the number of translation failures caused by Xerox 850 documents. To communicate with an 850, the 850/860 Gateway Service must translate the mail received from 850 to 860 format.

 # 860 format errors - the number of translation failures caused by Xerox 860 documents; to communicate with an 850, the 850/860 Gateway Service must translate the mail sent from 860 to 850 format; documents containing invalid formats create these failures.

Session termination statistics

 # gets aborted - the number of times a transfer from the 860 to the 850/860 Gateway Service was aborted before completion.

 # get timeouts - the number of times a session terminated after a period of inactivity; if the 850/860 Gateway Service does not receive any data or poll requests from the 860 within two minutes, the 850/860 Gateway Service terminates the session.

 # puts aborted - the number of times a data transfer to the 860 was aborted before completion.

 # put timeouts - the number of times a session was terminated after a period of inactivity; if the 850/860 Gateway Service is sending data and the 860 does not accept that data within two minutes, the 850/860 Gateway Service terminates the session.

 # remote disconnects - the number of disconnect requests received; the 860 may request that the 850/860 Gateway Service disconnect.

 # control send timeouts - the number of times a session was terminated due to inactivity; if the 850/860 Gateway Service is sending control information and the 860 does not accept it within two minutes, the 850/860 Gateway Service terminates the connection.

Server-related or service-related statistics

 # clearinghouse down - the number of times an operation failed because the Clearinghouse Service was not available.

 # create failures - the number of times the 850/860 Gateway Service was unable to access the RS232C line. A large number of create failures may indicate a problem with the server configuration.

 # create timeouts - If this statistic is not zero, there is a problem with the configuration of the server. Delete the 850/860 Gateway Service configuration and add it again.

 # unexpected controls received - the number of times the 850/860 Gateway Service received an unexpected control from the binary synchronous communications (BSC) driver; a large number may indicate a problem with the BSC driver.

 # unexpected remote behavior - the number of times that the BSC driver reported that the 860 was acting in an unexpected manner; a large number may indicate a problem with the 860 or a problem with the BSC driver.

Related procedure: Listing the 850/860 850/860 Gateway Service configuration

16. Server Monitor Service

This chapter helps you prepare for the installation, setup, and maintenance of the Server Monitor Service (SMS). This information supports the procedures you perform from an 8000 or 8090 server.

Service description

The Server Monitor Service is a network management tool that lets the System Administrator monitor from one server the availability and performance of a group of servers.

The Server Monitor Service:

- Regularly checks a specified set of servers to determine their availability.
- Reports changes in a server's availability to the System Administrator and other specified users through mail messages.
- Maintains a database of server availability and other statistics.
- Provides an Event Site Reporting (ESR) option to allow event reporting from remote sites to the monitoring server.

How the software works

The Server Monitor Service is a monitoring program that runs on a server and periodically interacts with a specified set of servers to detect their availability. A change in a server's availability is called an event.

If the monitored server is available, the Server Monitor Service records the information and the total number of hours the server has been running. If the availability changes for any reason, the Server Monitor Service sends mail messages to notify specified users of this event.

The monitored servers also report any event as it occurs by sending a message to the monitoring server. The message identifies the event, the local time at the monitored server, and any information related to the event. Such messages enable you to give timely attention to critical events and to evaluate server performance quickly.

Event site reporting

The Event Site Reporting (ESR) option enables the Server Monitor Service to monitor leased or dial-up telephone circuits controlled by the Internetwork Routing Service (IRS). When IRS phone lines on a monitored server become available or go out of service, the Event Site Reporting option notifies the Server Monitor Service so it can notify specified users.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the Server Monitor Worksheet located at the end of this chapter.

The Server Monitor Service is not registered with the Clearinghouse, so it is your responsibility to keep accurate records.

- Installing the Server Monitor Service software as described in the Server Software Installation chapter of the *Services Installation and Setup Guide*.
- Setting up the SMS as described in the Server Monitor Service chapter of the *Services Installation and Setup Guide*.
- Maintaining the SMS as described in the Server Monitor Service chapter of the *Services Maintenance Guide*.
  - Analyzing the performance of monitored servers.
- Backing up the SMS database as described in the Server Monitor Service chapter of the *Backup and Restore Guide*.
- Notifying users of any change or disruption in the service.
- Troubleshooting the service as described in *Basic Network Troubleshooting*.

You can perform most Server Monitor Service procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter of the *Services Installation and Setup Guide* contains the procedures for installing your Server Monitor Service software. This section explains the hardware, software, and other requirements of the Server Monitor Service to help you prepare for installation.

Hardware requirements

The Server Monitor Service can run on an 8000 or an 8090 server and needs no unique hardware.

Software requirements

The Server Monitor Service requires these program files:

- ServerMonitorSDF.bcd
- DistSVCConfig.bcd
- SMServiceConfig.bcd
- ESRConfig.bcd
- CommSvcComSoft.bcd
- MailStubConfig.bcd
- CommunicationServicesArea.messages
- SMS.messages

Allow 907 disk pages for these program files.

The Server Monitor Service must have access to a Mail Service and a remote File Service.

Dependencies and limitations

The Server Monitor Service has these dependencies and limitations:

- The Server Monitor Service uses the Mail Service to send messages to specified users.
- The Server Monitor Service uses a File Service to back up its database. It's best to use a remote File Service for backup.
- The Server Monitor Service and the Event Site Reporting option must be installed at the remote servers to allow monitoring of Internetwork Routing Service phone lines.
- One server should not be monitored by more than three Server Monitor Services.

Server Monitor Service Worksheet

Use the Server Monitor Service Worksheet to record server-related and service-related information. The worksheet is at the end of this chapter.

Fill out a separate copy of the worksheet for each Server Monitor Service for which you have System Administrator responsibility. Retain the original for future use, and store the completed worksheet in your *Activities Guide*.

Using the worksheet

Before you install the software and set up your Server Monitor Service, complete the Server Monitor Service Worksheet. It is important that you fill out the worksheet accurately, and update it whenever changes occur.

The completed worksheet saves you time as you perform the setup and maintenance procedures. It also serves as an information source for new System Administrators unfamiliar with your configuration.

Filling out the worksheet

As you read the rest of this chapter, you are directed to make entries on the Server Monitor Service Worksheet. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and the services installed on that server. Copy this information from the Services Installation Worksheet you filled out while reading the Services System Software chapter of this book.

Use section ② to identify two monitored servers, how often they will be polled, and who will be notified if there is any change in their availability. Use additional copies of the worksheet to identify additional monitored servers.

Use section ③ to note the names of the servers that will receive event site reporting.

Use section ④ to record statistics about the monitored servers.

Planning for setup

After you install the Server Monitor Service, you initialize it and configure its database.

You fill out the Server Monitor Service Worksheet as you read this section. Then see the Server Monitor Service chapter in the *Services Installation and Setup Guide* for the complete procedures.

Initialization

Immediately after installation, you need to initialize the Server Monitor Service. The Server Monitor Service is not registered with the Clearinghouse.

The Server Monitor Service keeps a local copy of its database configuration. You can keep a copy of this database in a remote backup location.

See the Server Monitor Service chapter in the *Backup and Restore Guide* for more information on backup.

Related procedure: Initializing the Server Monitor Service

Monitored servers

When you configure the Server Monitor Service database, you identify the servers to monitor, specify how often you want to poll each one, and name the users who are to receive a message when an event occurs at the monitored server. Monitoring occurs even if no users are notified of events.

To determine the sampling rate, consider the load that the server handles and whether any other servers are monitoring it. You may want to poll the server less frequently if it is handling a heavy load or if other servers are monitoring it. Always restrict the number of monitoring servers to three or less. In this way, you ensure that the monitored server spends more time performing services than answering queries from monitoring servers.

Related procedure: Configuring the Server Monitor Service database

Filling out the worksheet

Section ② of the worksheet has space for information about two monitored servers. Use additional copies of the worksheet to record information about more servers.

② **Server name** - Record the name of the server you want to monitor. If you are monitoring a server in a different domain, use its fully qualified name.

Sampling rate - Record the number that represents in minutes how often the Server Monitor Service polls this server. If you enter 15, the monitoring server checks the monitored server every 15 minutes. The sampling rate cannot be less than 15 minutes.

Users to notify - Record the names of the users you want to receive a mail message when the server's availability changes.

Event recipients

When you add a monitored server to the database, the Server Monitor Service registers the monitoring server as the event recipient of the monitored server.

Related procedure: Configuring the Server Monitor Service database

Filling out the worksheet

③ Record the names of the monitoring servers to be registered as event recipients of each monitored server.

Planning for maintenance

After you install and set up the Server Monitor Service, you are responsible for maintaining it. You perform maintenance as needed; there are no scheduled duties.

This section provides guidelines for monitoring server performance and making configuration changes.

See the Server Monitor Service chapter of the *Services Maintenance Guide* for complete maintenance procedures.

Reviewing server performance

The Server Monitor Service collects information about all servers it monitors. To analyze how monitored servers are performing, routinely review the statistics for all monitored servers or for each individual server. The categories of information to review include:

Monitoring session start time - The time when the monitoring server started to monitor the specified server.

Sampling rate - The frequency at which the monitoring server tried to poll the specified server.

Server state - The condition of the server:

unknown	The Server Monitor Service has not yet polled the server.
responding	The server is available.
not sure yet	The server did not respond; the Server Monitor Service will retry.
not responding	The server is not available to network users.

Up time - The length of time the server has been available.

Down time - The length of time the server has been unavailable.

Up-down count - The number of times the server switched from being available to being unavailable, and back again.

Total up time - The total length of time the server has been available since the start of the monitoring session.

Total down time - The total length of time the server has been unavailable since the start of the monitoring session.

Last response - The time the monitoring server was last able to communicate with the monitored server while the monitored server was available.

Last checked - The time the monitoring server last tried to communicate with the monitored server.

Last restart - The time the monitored server was last rebooted.

After you review these statistics, you may decide to change the sampling rate. You may want to check the server less frequently if it is performing efficiently, or check it more often if you need to analyze a problem.

Related procedure: Showing server statistics

Keep a running log of the availability of the monitored servers. If you are using Remote System Administration (RSA), keep a record of these statistics by using the Make Document or Make Screen option. If you are not using RSA, fill out section ④ of the worksheet with some key statistics.

Filling out the worksheet

④ **Date** - Record the date you displayed the statistics.

Up time - Record the length of time the monitored server has been available.

Down time - Record the length of time the monitored server has been unavailable.

Up-down count - Record the number of times the monitored server became available after becoming unavailable.

Making configuration changes

You can add monitored servers or users to the Server Monitor Service database, or delete them from the database. Whenever you make any changes to the database, update your records.

Changing the monitored servers

As you add each server to the database, identify how often you want the Server Monitor Service to poll it and specify the users you want to receive a mail message when an event occurs.

You can delete a monitored server from the database by specifying its name. This deletion also instructs the Server Monitor Service to cancel its registration as an event recipient of the monitored server.

If you first delete the server from the Clearinghouse Service, you must specify the server's address instead of its name when you remove the server from the Server Monitor Service database. The Clearinghouse no longer recognizes the name.

Related procedures: Adding, listing, and verifying monitored servers; Removing monitored servers

Changing the user list

You can add user names to or delete them from the notification list. Monitoring occurs even if no names appear on the list.

You can display the notification list to confirm that a name was added or deleted.

Related procedure: Adding users for notification, and listing user notifications

Changing the sampling rate

You can enter a new value to control how often the monitoring server checks on the monitored server. The sampling rate cannot be less than 15 minutes.

Related procedure: Changing sampling rates

17. Boot Service

This chapter helps you prepare for installation, setup, and maintenance of the Boot Service (BS). This information supports the procedures you perform from an 8000 or an 8090 server.

Service description

Users can start up ("boot") their workstations from floppy disk, rigid disk, cartridge tape, or over the network. The Boot Service enables workstations and other servers to boot diagnostic and installation utility files over the Ethernet.

How the software works

The Boot Service functions as a remote server constantly monitoring the Ethernet for boot file requests. It responds to these requests by locating the required boot files and sending them to the requesting device.

Etherboot files

The Boot Service maintains a database of boot files, called Etherboot files, that you anticipate users may need. Upon request, the Boot Service sends out files so that users can run either the diagnostic utility or the installation utility to boot a workstation over the network. This process is called etherbooting.

The Boot Service database is stored on the server's working directory. Only the System Administrator in the domain of the server has access to the database files. The name and number of each database file are registered in the server profile. A boot request contains a boot file number so the Boot Service can quickly locate the file.

The database contains microcode files, germ files, and boot files for various workstation hardware configurations. Microcode files provide basic instructions to the hardware. Germ files load a boot file into memory and start its execution. Boot files provide the bootable system with either the diagnostic or the installation utility.

Diagnostic and installation utilities

The diagnostic utility lets users perform diagnostic procedures for workstation and server rigid disks, as well as for server large-capacity secondary rigid disks. By etherbooting remote diagnostics, a user can troubleshoot a workstation that cannot boot from its own drive.

The installation utility lets workstation users load application software, such as the ViewPoint operating system and VP Series applications, over the network. The utility provides a menu of installation options so users can select application software from a file drawer. The installation utility shortens the time required to upgrade network workstations when new software becomes available.

File drawers for the installation utility

To support the installation utility, the File Service you use must have the alias Installation Server. It must also contain the file drawers named Installation Drawer and VP Applications.

The file drawers need not reside on the same file server, and need not be on the same network as the workstations accessing them. However, for optimum Boot Service response, create the file drawers on the same network.

Boot switches for requesting utilities

The following boot switches select the Boot Service as the source for booting:

- 0003 -- Installer, Help, and offline diagnostics
- 0004 -- Ethernet diagnostic boot of utility
- 0006 -- Ethernet boot of offline diagnostics

Each of these boot switches sends out the a request for a specific utility boot file. After receiving a request, the Boot Service retrieves the specified utility from its local database and sends the to the requesting device.

The Boot Service responds to one request at a time, placing additional requests in a holding queue. A numeric code (such as 0149, 0199, or 0928) appears on the maintenance panel of the requesting processor as it waits for a response from the Boot Service.

If the Boot Service does not respond within a short time, the requesting processor displays the code 0151 or 0201.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the Boot Service Worksheet located at the end of this chapter.
- Installing the Boot Service software as described in the Server Software Installation chapter of the *Services Installation and Setup Guide.*
- Setting up the Boot Service as described in the Boot Service chapter of the *Services Installation and Setup Guide.*
- Maintaining the Boot Service as described in the Boot Service chapter of the *Services Maintenance Guide.*
- Monitoring the of Boot Service to analyze whether it is efficiently fulfilling user booting requests.
- Upgrading hardware and software as required.
- Notifying users of any change or disruption in the service.
- Troubleshooting the service as described in *Basic Network Troubleshooting.*

You can perform most Boot Service procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter in the *Services Installation and Setup Guide* contains the procedures for installing your Boot Service software. This section explains hardware, software, and other requirements of the Boot Service to prepare you for installation.

Hardware requirements

The Boot Service can run on an 8000 or an 8090 server and needs no unique hardware.

Software requirements

The Boot Service requires these program files:

- BootServiceMessages.messages
- BootServiceSDF.bcd
- BootServiceConfig.bcd

Allow approximately 50 disk pages for the Boot Service program files.

Etherboot file requirements

The Boot Service package includes a database called Standard Etherboot Files, which contains the network diagnostics and installation utilities.

- For an 8000 server, the package includes a set of floppy disks labeled Standard Etherboot Files.
- For an 8090 server, the package includes a cartridge tape containing the Standard Etherboot Files.

One of the files in the installed database is BootService.profile. This file contains server profile information, such as filenames and numbers, for all other files in the database.

Disk page requirements

Use the information in this section to estimate the disk page requirements for the Etherboot files and the page limits for the installation utility file drawers. These disk page requirements are general guidelines.

Etherboot files

You may not need to install all Etherboot files. The files needed depend on the server you are using and on the types of workstations that will boot over the network.

Table 17-1 lists the filenames and disk page requirements for the Etherboot database files needed by the devices your network supports.

Table 17-1. **Etherboot database disk page requirements**

	Boot Functions and Diagnostics	Installation Utility	Disk Diagnostics
8000 or **8010** Total 2518	BootService.profile DLion.germ EtherInitial.db Mesa.db MoonBoot.db SimpleNetExecDLion.boot NetExecAnnouncerDLion. boot (subtotal = 1091)	InstallerNSDLion.boot (subtotal = 804)	EtherInitialAlt.db MesaAlt.db DLionAlt.germ ElDiskDLion.boot (subtotal = 623)
6085 Total 3243/ 3044	SimpleNetExecDove.boot BootService.profile Dove.germ MesaDove.db MoonRise.db NetExecAnnouncerDove. boot (subtotal = 997)	InstallerNSDove.boot (subtotal = 818)	EtherInitialDove.db Moonrise12.5.db MesaDaybreak.db Dove12.5.germ OfflineDiagnosticsDove. boot OR OfflineScnrDiagDove.boot (subtotal = 1428/1229)
8090 Total 4451	BootService.profile DLight.germ EtherInitialDLight.db RavenMesaDLight.db MoonDLight.db SimpleNetExecDLight.boot (subtotal = 986)	InstallerTapeDLight.boot (subtotal = 1165)	ElDiskDLight.boot DiagOfflineHiCapDLight. boot DiagOfflineFlTapeDLight. boot (subtotal = 2300)
8000 LCD Total 2481	BootService.profile TriDLion.germ EtherInitial.db TridentRavenMesa.db MoonBoot.db SimpleNetExecTriDLion.boot NetExecAnnouncerDlion. boot (subtotal = 1091)	InstallerNSTriDLion.boot (subtotal = 804)	ElLCDDiagDLion.boot (subtotal = 586)

File drawer page limits

You also need to estimate the page limit for each file drawer based on the disk page requirements of the ViewPoint software.

See your ViewPoint documentation to determine disk page requirements for the application software and for instruction on placing a copy of the ViewPoint software in the correct file drawer. The exact number of disk pages, depends on the type of workstations accessing the drawers, the software version you are using, and the features you want to make available over the network.

Dependencies and limitations

The Boot Service has these dependencies and limitations:

- For optimum performance and response to Etherboot requests, do not install the Boot Service on a server that is running another highly interactive service, such as the Print Service, Mail Service, or Clearinghouse Service.
- Do not install the Boot Service on the same server with a Print Service whose Image Gap Printing feature is enabled.
- The Boot Service only supports processors on a single network. You must install a Boot Service on each network with workstations that will etherboot. You can install any number of Boot Services on a single network.
- The File Service containing the Installation Drawer and the VP Applications drawer must be on the same network as the Boot Service.
- Workstations may etherboot through a repeater. Workstations cannot etherboot through an Internetwork Routing Service (IRS), or through that service's Clusternet Communications or the X.25 Communications Protocol options.
- Remote workstations, which are networked through the Internetwork Routing Service, cannot use the Boot Service.

Boot Service Worksheet

Use the Boot Service Worksheet to record server-related and service-related information. The worksheet is at the end of this chapter.

Fill out a separate copy of the worksheet for each Boot Service for which you have System Administrator responsibility. Retain the original for future use, and store the completed worksheet in your *Activities Guide*.

Using the worksheet

Before you install the software and set up your Boot Service, complete the Boot Service Worksheet. It is important that you fill out the worksheet accurately and update it whenever changes occur. The completed worksheet saves you time as you perform the setup and maintenance procedures. It also serves as an information source for new System Administrators unfamiliar with your configuration.

Filling out the worksheet

As you read the rest of this chapter, you are directed to make entries on the Boot Service Worksheet. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and the services installed on that server. Copy this information from the Services Installation Worksheet you filled out while reading the Services System Software chapter of this book.

Use section ② for recording the disk page requirements for the Etherboot database files. Use sections ③ and ④ for the page limits for the Installation Drawer and the VP Applications drawer.

Use section ⑤ to total all disk page requirements.

Planning for setup

After you install the Boot Service, you must initialize it and install the Boot Service database. Then you can prepare for network installation of workstation software.

See the Boot Service chapter in the *Services Installation and Setup Guide* for complete setup procedures.

Service name and description

You name and describe the Boot Service Service during initialization. The name and description become part of the system-wide directory function that the Clearinghouse maintains.

When you name the Boot Service, use a name different from all other names in the domain. The fully qualified Boot Service name takes the form:

Boot Service name:Domain:Organization

The domain and organization MUST be the same as the domain and organization of the server. For example, if the server name is Dallas:Home Office:ABC Company, then the Boot Service name might be Sales:Home Office:ABC Company. It is recommended that you enter the local name only when you name the Boot Service. This avoids possible errors and lets the domain and organization default to that of the server.

This naming convention gives the System Administrator for the server domain access to System Administrator commands for the Boot Service. These commands are available only when you are enabled.

The service description may be the location, a department name, the name of the assigned System Administrator, or any other descriptive information.

Related procedure: Initializing the Boot Service

Filling out the worksheet

① **Service name** - Record the name of the Boot Service.

Description - Record the description of the Boot Service.

Etherboot files

During the Boot Service database installation, you store the Etherboot files on the server's working directory. These files support the etherbooting function for the types of servers and workstations on your network.

Related procedure: Installing the Boot Service database

Filling out the worksheet

② **Etherboot files** - Record the number of disk pages required for each type of device your network supports. Total the number of disk pages required. For example, if both 8010 workstations and 8000 large-capacity disk servers will boot over your network, your disk page total will be 4,110.

Installation Drawer and VP Applications

To prepare for network installation of workstation software, you need to create two file drawers and assign a page limit for each drawer. Create these file drawers on a File Service that uses the alias Installation Server. Name the file drawers Installation Drawer and VP Applications.

Related procedure: Preparing for network installation of workstation software

Filling out the worksheet

① **File Service** - Record the name of the File Service you are using for the Installation Drawer and VP Applications drawer.

Owner - Record the name of the owner of the file drawers. The owner has full access rights to the drawer. You can use the name of any person who has access to the drawer, but using your name is best.

User, group, alias - Record the user name, alias, or group name that identifies the users you want to have access to the file drawers.

Access rights - Record the access rights you want to assign to the users who have access to the file drawers. Typically, you want to provide read access only. Read access lets each user list, read, and copy the files in the drawer, but does not let the user alter the files. Reserve the write, add, remove, and change access for the System Administrator.

③ **Installation Drawer files** - Record the number of disk pages for the Installation Drawer, based on the types of workstations your network supports. The worksheet already notes the disk pages required for common software. Total the number of disk pages required.

④ **VP Applications drawer files** - Record the number of disk pages for the VP Applications drawer, based on the applications your workstation users will require. The worksheet already notes the disk pages required for common software. Total the number of disk pages required.

Total disk page requirements

To be aware of the load the server will handle, total the disk pages required by the Boot Service and other installed services.

Related procedures: Installing the Boot Service database, Preparing for network installation of workstation software

Filling out the worksheet

⑤ **Total disk page requirements** - Record the total number of disk pages required by all services installed on the server (see section ①).

Record the total number of disk pages required for the Etherboot files (see section ②).

If the File Service is installed on the same server as the Boot Service, record the total number of disk pages for the Installation Drawer and the VP Applications drawer (see sections ③ and ④).

Calculate the total disk page requirements.

Planning for maintenance

After you install and set up the Boot Service, you are responsible for maintaining it properly. You perform maintenance as needed; there are no scheduled duties.

This section provides guidelines for monitoring service performance and making configuration changes. See the Boot Service chapter in the *Services Maintenance Guide* for complete maintenance procedures.

Monitoring service performance

The Boot Service keeps track of the number of files it sends over the network. You may want to monitor the Boot Service weekly to ensure that it is receiving and fulfilling all boot requests.

You can display Boot Service statistics, including the number of boot and microcode boot files requested and the number actually sent. Typically, each boot file request is preceded by three requests for microcode boot files.

Keep a log of the statistics. The statistics counter returns to zero only when you reboot the server running the Boot Service, so you must manually separate the weekly statistics. By comparing information from week to week, you can determine the load on the service.

If users complain about longer booting times but you do not see an increase in booting requests, check for additional server load caused by other services or by network communications interruptions. You may decide you need to install the Boot Service on a second server on the local network.

Related procedure: Listing boot statistics

Making configuration changes

The Boot Service will not use a damaged file. You may receive messages indicating that specific Etherboot files are damaged or cannot be located. Note the filenames in the messages so you can delete the damaged files and install them again from the installation media.

Each file in the Boot Service database has a set of associated parameters registered in the server profile. A full entry contains these parameters:

TypeOfHardware TypeOfFile FileNumber BootFilename

The parameters are:

- Type of hardware - The class of processors this file serves.
- Type of file - The type of boot file (microcode, germ, or boot).
- Boot file number - A number that Xerox assigns.
- Boot filename - A name that Xerox assigns.

For example, the entry for a germ file might look like:

DLion Germ 25200000030 DLion.germ

If you need to reconfigure the Boot Service database, obtain the floppy disks or the cartridge tape containing the Standard Etherboot Files. List the files on the floppy disks or cartridge tape to display all parameters for each file.

When you install a replacement file, enter the complete filename entry.

Notifying users

Reconfiguring the database requires that you stop the Boot Service. Notify all users that the service will be temporarily interrupted.

Verifying the database

After you install the replacement files, list all files in the Boot Service database to confirm that the files you added are included.

Related procedures: Listing boot files in the Boot Service database, Listing files on the installation media, Reconfiguring the Boot Service database

18. Communications Monitoring Service

This chapter helps you prepare for installation, setup, and maintenance of the Communications Monitoring Service (CMS). This information supports the procedures you perform from an 8000 or 8090 server.

Service description

To support popular computing systems, some of which are incompatible with the Xerox Network System communication protocol, Xerox provides a family of communication services. These services act as gateways that let remote users access various other network services.

You configure these gateways by setting a number of parameters to begin communication. Communication problems can occur when gateway configurations are incompatible with the remote terminal or host.

The Communications Monitoring Service provides protocol monitoring for the communication services to aid in diagnosing communication problems. The CMS lets you create monitoring profiles to meet your needs and maintains a log which you can use to analyze the performance of the communication services.

The Communications Monitoring Service collects communication data passing through a gateway to help diagnose communication problems. Without this data, you would need time-consuming trial-and-error testing and even the assistance of Xerox personnel, to isolate and interpret problems.

How the software works

The Communications Monitoring Service provides three types of monitoring:

- SNA monitoring for the External Communication Service IBM 3270 SNA emulation. This type of monitoring interprets the collected data at the synchronous data link control (SDLC) and Path Control protocol levels.
- X.25 monitoring for the Internetwork Routing Service X.25 Communication Protocol option. This type of monitoring interprets the collected data at the high-level data link control (HDLC) protocol level.
- RS232C monitoring for the External Communication Service asynchronous communication protocol and IBM 3270 binary synchronous communication (BSC) emulation, the Interactive Terminal Service, the Remote Batch Service, and the 850/860 Gateway Service. This type of monitoring does not interpret the collected data to a higher-level protocol. However, you

can display the data in different numeric formats: hexadecimal, octal, ASCII and EBCDIC.

The Communications Monitoring Service captures data passing through an RS232C port. The RS232C port may be the local server port or a port on a Multiport Option Kit or Communication Interface Unit.

You can initiate monitoring activities from any networked or remote workstation using Remote System Administration.

Log file contents

The Communications Monitoring Service generates a log file of captured data for the monitored service. Each log file begins with a banner that identifies the parameters of the monitoring activity.

After the banner, each log file contains:

- Services software version number
- Name of the Communications Monitoring Service
- Type of monitoring
- Server name, network number, and processor number
- Type of hardware and memory size
- Name of the System Administrator who started the service
- The log file storage location
- Name and type of RS232C port from which the data was collected
- Collected data

The log file is a plain text document that both Xerox and non-Xerox products can interpret. Refer to *Basic Network Troubleshooting* for an explanation of log file interpretation.

Working and stored log files

The Communications Monitoring Service records captured data as log entries in a working log file kept at the sever running the Communications Monitoring Service. A working log file is temporary; if the server crashes or is re-booted, the data is lost.

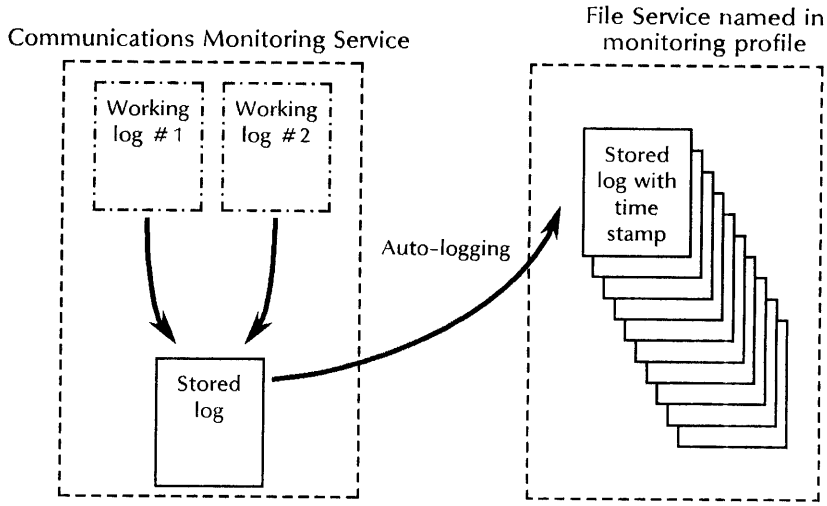
The Communications Monitoring Service creates as permanent log file to retain the data in the server's working directory every time a working file log fills up.

When the working log file becomes full, a second working log file continues to capture data. The new working log file writes over the old file of the same name. You can keep a working log file without overwriting it by renaming each file as it is stored.

Figure 18-1 shows the process for storing the working log file. Although there are two working log files, only one is active at a time. As the active working log file reaches its limit, the Communications Monitoring Service closes, copies and stores it. The Communications Monitoring Service then activates the second working log file.

The Communications Monitoring Service automatically stores the log file on a File Service if you enabled auto-logging.

Figure 18-1. **Storing log files**



Auto-logging

The auto-logging feature of the Communications Monitoring Service lets you automatically store log files on a File Service. The Communications Monitoring Service makes a copy of the working log file, adds a time stamp to the name to create a unique filename, and then stores the copy in a file drawer. The file drawer can reside on the same server as the Communications Monitoring Service, or on any server on the internetwork. You can set the frequency for storing log files and the maximum number of log files that can be stored.

Manually storing a log file to a remote location

You can manually save a working file to a File Service you specify and include a comment in the file. This may help serve as a memory jogger when you inspect the log file later.

Viewing a log file

You can view any of the working log files. RS232C level monitoring lets you select a display format for the working log file. You can also save log files with different display formats by changing the display format in the Monitoring Profile.

Relationship with other services

The Communications Monitoring Service monitors communication services which use RS232C ports, the local port on an 8000 server, a Communication Interface Unit port, or one of the ports on a Multiport Option Kit.

The services include the External Communication Service, the 850/860 Gateway Service, the Internetwork Routing Service, the

Interactive Terminal Service, the Remote Batch Service, and the SNA Mail Relay Service.

The Communications Monitoring Service uses the File Service to store the log files.

System Administrator duties

As System Administrator, your major duties and responsibilities include:

- Completing and maintaining the Communications Monitoring Service Worksheet located at the end of this chapter.
- Installing the Communications Monitoring Service software as described in the Server Software Installation chapter of the *Services Installation and Setup Guide*.
- Setting up the Communications Monitoring Service as described in the Communications Monitoring Service chapter of the *Services Installation and Setup Guide*.
- Maintaining the Communications Monitoring Service as described in the Communications Monitoring Service chapter of the *Services Maintenance Guide*.
- Regularly reviewing the performance of the monitored communication devices.
- Upgrading hardware and software as required.
- Troubleshooting the service as described in *Basic Network Troubleshooting*.

You can perform most Communications Monitoring Service procedures from a workstation using Remote System Administration (RSA).

Planning for installation

The Server Software Installation chapter of the *Services Installation and Setup Guide* contains the procedures for installing your Communications Monitoring Service software. This section explains hardware, software, and other requirements of the CMS to help you prepare for installation.

Hardware requirements

The CMS can run on an 8000 or 8090 server and needs no unique hardware.

Software requirements

The Communications Monitoring Service requires these program files:

- CommunicationsMonitoringServiceSDF.bcd
- CommunicationsMonitoringService.bcd
- CommunicationsMonitoringService.messages
- CommunicationsServicesArea.messages
- RS232CCommon.bcd

Allow approximately 500 disk pages for these files.

Disk space required for log storage

The CMS requires disk space for storing working log files and stored log files. When you set up the monitoring profile, you specify the number of data bytes per log entry and the number of log entries per log file. These parameters affect the space consumed by both the working and the stored log files.

The size of each log file is approximately equal to the number of bytes per entry times the number of entries. The actual size is slightly bigger, because the log file also contains banner information.

The Communications Monitoring Service does not need additional disk space for the most recent working file, as long as you use the same file storage name. If you change the file storage name, then the disk space must increase to store the new file.

Dependencies and limitations

The Communications Monitoring Service has these dependencies and limitations:

- Install the Communications Monitoring Service on the same server as the monitored communication service.
- Do not install the File Service on the same server as the CMS. In this way, you have access to stored log files even when a

communications problem disables communication to the monitored server.

- The Communications Monitoring Service can monitor only one RS232C port and one protocol at a time.
- Do not install the Foreign Gateway Assistant on the same server as the Communications Monitoring Service. If both are installed on the same server, they cannot be expunged, and the server must then be repartitioned.

Communications Monitoring Service Worksheet

Use the Communications Monitoring Service Worksheet to record server-related and service-related information. The worksheet is located at the end of this chapter.

Fill out a separate copy of the worksheet for each Communication Monitoring Service for which you have System Administrator responsibility. Retain the original for future use and store the completed worksheet in your *Activities Guide*.

Using the worksheet

Before you install the software on a server and set up a Communications Monitoring Service, complete the Communications Monitoring Service Worksheet. It is important that you fill out the worksheet accurately and update it whenever changes occur.

The completed worksheet saves you time as you perform the setup and maintenance procedures. It also serves as an information source for new System Administrators unfamiliar with your configuration.

Filling out the worksheet

As you read the rest of this chapter, you are directed to make entries on the Communications Monitoring Service Worksheet. The worksheet section number appears with these directions, so you know where to make each entry.

Use section ① for information about the server and the services installed on the server. Copy this information from the Services Installation Worksheet you filled out while reading the Services System Software chapter in this book.

Use section ② to define the protocol for the monitored communication services.

Use section ③ to indicate where you want to store the log files.

Planning for setup

After you install the Communications Monitoring Service, initialize it and configure the monitoring profile. See the Communications Monitoring Service chapter of the *Services Installation and Setup Guide* for complete setup procedures.

Communications Monitoring Service name and description

When you name the Communications Monitoring Service, use a name different from all other names in the domain. The fully qualified name of the Communications Monitoring Service has the format:

> Communications Monitoring Service name :Domain: Organization

The domain and organization must be the same as the domain and organization of the server. For example, if the server name is Wombat:Abilene:Acme, then the Communications Monitoring Service name might be Spy:Abilene:Acme. This naming convention gives the System Administrator enabled for the server domain access to all Communications Monitoring Service commands.

To avoid possible errors, enter only the local name when you name the Communications Monitoring Service. This approach lets the domain and organization default to those of the server.

A description for the Communications Monitoring Service is optional. The description can help you identify the location or the function of the Communications Monitoring Service. For example, if the CMS is monitoring only the 850/860 Gateway Service, include that information in the description.

Related procedure: Initializing the Communications Monitoring Service

Filling out the worksheet

① Record the name and description of the Communications Monitoring Service.

The monitoring profile

The monitoring profile contains parameters that define the type of protocol and the port to be monitored, as well as the log file contents and name. The parameters you need for setting up the monitoring profile depend on the type of protocol.

② **Protocol** - Record the type of protocol to be monitored:

- SNA, to monitor External Communication Service 3270SNA emulation (this is the default setting)
- X.25, to monitor Internetwork Routing Service X.25 Communication Protocol option.
- RS232C, to monitor External Communication Service asynchronous communication protocol and IBM 3270 BSC

emulations, the Interactive Terminal Service, the Remote Batch Service, and the 850/860 Gateway Service.

③ **Product option** - For the SNA protocol, record the product option (3270 only)

Protocol level - For the SNA protocol, record the protocol level:

- SDLC
- Path Ctrl (LU & PU)
- Path Ctrl (PU only)
- All

Data bytes per entry - Record the maximum number of data bytes for each communication, whether transmitted or receiving. The range is 40 to 600 bytes. Each communication mode change resets the byte counter.

Number of log file entries - Record the maximum number of entries in the working log file before the Communications Monitoring Service can save it. The range is 100 to 200.

Comment - Record a description of the log file purpose. The comment can contain up to 100 characters.

③ **Statistics?** - For the SNA protocol, circle whether or not the log file will contain additional information.

④ **Display format** - Record the format for recording data bytes in the log file:

- Hex (SNA and X.25 protocols), data bytes recorded are shown in $base_{16}$ (numbers from 0 to F)
- Octal (RS232C protocol only), data bytes recorded are shown in $base_8$ (numbers from 0 to 7)
- ASCII (RS232C protocol only), data bytes recorded are shown translated following the ASCII standard.
- EBCDIC (RS232C protocol only), data bytes recorded are shown translated following the EBCDIC standard.

RS232C port - Record the name of the RS232C port to be monitored.

Log name - Record the name for the stored file.

Auto-logging? - Circle whether or not you want to automatically store log files to a remote location.

Related procedures: Monitoring SNA communications, Monitoring X.25 communications, Monitoring RS232C communications, Setting up auto-logging

Auto-logging

If you use auto-logging, you must specify for log storage a file drawer on a remote File Service on the internetwork. After you initialize the Communications Monitoring Service, add the file drawer to the File Service and give the Communications Monitoring Service access to the file drawer. Then set up the monitoring profile for auto-logging.

Auto-logging also requires that you specify the maximum number of log files to be stores and the frequency for storing the working log file. You must archive and/or delete log files from the file

drawer to ensure the number of stored log files never exceeds the limit. Otherwise, you will have to reset that limit to resume auto-logging.

Filling out the worksheet

⑤ **Remote directory** - Record the complete pathname to the file drawer that will store the log files.

Maximum number of logs stored - Record the maximum number of log files to be stored in the file drawer. The range is 1 to 100. The stored log files use the log name specified in the monitoring profile; a timestamp individualizes each file.

Frequency of log storage (store every Nth log) - Record the frequency for storing the working log. The range is 1 to 10. For example, if you specify 4, the first fifth, and ninth log files are stored, and so on.

Planning for maintenance

After you install and set up the Communications Monitoring Service, you are responsible for maintaining it properly. You perform maintenance as needed; there are no scheduled duties. This section provides guidelines for managing your file resources.

See the Communications Monitoring Service chapter in the *Services Maintenance Guide* for complete maintenance procedures.

Managing auto-logging

The rate of accumulating log files varies with the communications service being monitored, the type of activity being monitored, and the level of monitoring selected. File space can be a scarce resource in a network community and you should monitor its consumption closely.

If you are using auto-logging, regularly archive log files, particularly those files containing information related to a problem. Ensure that the file drawer storing log files does not become full, thus halting further filing.

Be sure to establish guidelines about when and how often to change the log file name, delete older log files on the server, and to modify the type of monitoring selected.

Related procedure: Saving a log

Index

A

B

C

D

E

F

I

J

M

N

Q

R

S

T

U

V

W

X