COMMUNICATIONS MONITORING SERVICE

XEROX

Network Administration Library

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

The content of this booklet is based on the Services 10.0 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.

Printed in the United States of America. Publication number: 610E02870

Preface

Purpose

The Communications Monitoring Service booklet describes all that you need to know to set up and maintain your Communications Monitoring Service (CMS). This booklet explains all the service commands and shows how these commands are used to perform service-related tasks. In addition, this booklet lists all the messages that can be generated while running this service and tells you what to do when a message is displayed.

Intended audience

This publication is intended for System Administrators who are responsible for starting up and keeping the Communications Monitoring Service running efficiently.

Before you read this booklet

There is some general information about services that you will need to be familiar with before you can understand this booklet. Read the "Services Executive" section in the *Server Operation and Maintenance* booklet, and the *Introduction to Network Administration* booklet. All of these publications can be found in the *Network Basic Services* volume.

Before you can use this service

As part of the preparation for setting up the Communications Monitoring Service, you need to perform the procedures described in the *Server Software Installation* booklet. This booklet is also part of the *Network Basic Services* volume.

(This page intentionally blank)

Table of contents

(This page intentionally blank)

1. Introduction

The Communications Monitoring Service (CMS) monitors the communications supported by the Xerox Communication Services. It saves a log of the communication being monitored, providing a permanent record of the communication. You can use the resulting logs to analyze communication problems and to document the behavior of communication programs. Communications supported by the following Xerox Communications Services can be monitored with the Communications Monitoring Service:

- External Communication Service (3270 BSC, 3270 SNA, and Asynchronous)
- Interactive Terminal Service
- Remote Batch Service
- Gateway Service
- External Mail Gateway Service
- Internetwork Routing Service (X.25 only)

Note: CMS will not work with the Mail Gateway Service or Internal Routing Service without the X.25 option (i.e., regular Internal Routing Service and Clusternet, for example, cannot be monitored by CMS).

The CMS monitors communications using one of three monitoring options: SNA, X.25, and RS-232C. When monitoring with the SNA or X.25 option, the CMS captures the data being communicated and interprets it according to the SNA or X.25 protocol. When monitoring with the RS-232C option, the Communications Monitoring Service captures the data being communicated but does not interpret it according to any protocol. You can use the RS-232C option to monitor any communication through an RS-232C port, such as 3270 BSC or TTY asynchronous, except for Internetwork Routing Service communications.

You set up and control monitoring by using Communications Monitoring Service commands. The Communications Monitoring Service commands can be entered at the server's local terminal. The commands can also be entered at any workstation, remote or on the network, that supports remote network administration. All CMS commands must be entered by an enabled System Administrator, except for the **Help** command which is available to all users.

The Communication Service being monitored must reside on the same server as the CMS. The CMS can monitor only a single protocol and RS-232C port at a time. The RS-232C port must reside on the server's local port, on a local multiport option card, or on a CIU that is managed by the local ECS.

2. Commands

This chapter lists all the Communications Monitoring Service commands. The commands below are listed in alphabetical order, followed by a brief explanation. All Communications Monitoring Service commands (except the **Help** command) require that you have System Administrator privileges, and that you are logged on and have typed the **Enable** command. The **Help** command can be used by any user.

To address the Communications Monitoring Service, you must be in the Communications Monitoring Service context (CMS!). You only need to type the number of characters that uniquely identifies the commmand you want to use.

If a command parameter has a default, it is displayed on the prompt line where you type an answer. To keep a default or current value, press <RETURN>. To change the default or current value, type the new value and press <RETURN>.

All logging commands except **Show Active Log** stop logging, and you must explicitly start logging when you want to resume logging. The monitoring profile can be set with the **Set Monitoring Profile** command, or portions of the monitoring profile can be set with the other **Set** commands.

Help Provides a brief explanation about how to use the Communications Monitoring Service.

Register Communications Monitoring Service Registers the Communications Monitoring Service with the Clearinghouse. Use this command if the service self-registration fails.

Rename Communications Monitoring Service Renames the Communications Monitoring Service.

Save Log Saves a working log file to a remote directory. Any outstanding filing operations are completed before this command is executed. You can save logs with different display formats by changing the display format of the monitoring profile before using the **Save Log** command. Saving a log file to a remote directory does not change any values you have set in the monitoring profile.

Set Log Attributes Sets the logging portion of the monitoring profile by specifying the display format and the port you want to monitor.

Set Log Name Names the local log file. If you do not name the local log file, the Communications Monitoring Service provides a default name based on the protocol you choose (SNA, X.25, or RS-232C) and the RS-232C port you select for monitoring.

Set Monitoring Profile

Sets all the parameters of the monitoring profile. The parameters you can set are the protocol, the protocol level, the number of data bytes per log entry, maximum log entries per log file, a comment, whether or not to include statistics, the display format, the port you want to monitor, the log name, whether or not you want automatic log backup, the name of the remote directory to which you are backing up the log, and the maximum number of logs stored remotely. Some of these parameters can be set individually with other **Set** commands.

Set Protocol

Specifies the protocol you want to monitor. You can choose SNA, X.25, or RS-232C. The Communications Monitoring Service is initially set to monitor RS-232C. The protocol you choose is used until you change it.

Set Remote Log Handling

Enables auto-logging. You are prompted for the name of the remote directory where the log files will be stored, the maximum number of log files you want to store, and the frequency with which you want to store them. Auto-logging copies the local log file to a remote log file in the remote directory you name. To disable auto-logging, you must use the **Set Monitoring Profile** command, and respond **N** to the "Backup Log Automatically" prompt.

Show Active Log

Displays the working log file (Log #1 or Log #2) in which the captured data is currently stored (the current log file). While logging is active, the current log file is displayed with a message indicating that it is active. When logging is stopped, the log file last used is displayed with a message indicating that it is not active. When logging is resumed, the other log file becomes the current log file.

Show Log

Causes logging to stop and displays the working log file you specify (Log #1 or Log #2). To resume logging, you must use the **Start Logging** command.

Show Monitoring Profile

Displays the current values for the monitoring profile.

Show Statistics

Displays statistics for the service you are monitoring. Statistics can only be displayed when you are monitoring SNA protocol. This command is not available if you specify a protocol other than SNA in the monitoring profile.

Start Communications Monitoring Service

Restarts the Communications Monitoring Service if you have stopped it with the **Stop Communications Monitoring Service** command.

Start Logging

Starts the logging process. The captured data is written to the current log file (Log #1 or Log #2). The current log file is the working log file that was not last used. For example, if Log #1 was the last current log file, the current log file when logging is restarted is Log #2. Use the **Show Active Log** command to see which working log file is current.

Stop Communications Monitoring Service

Stops the Communications Monitoring Service. All outstanding file operations are completed before the service is stopped.

Stop Logging

Stops the logging process. To save the data in the current log file, you must use the **Save Log** command.

3. Setting up your Communications Monitoring Service

The Xerox Communication Service that you want to monitor must reside on the same server as the CMS. The Communication Service must be installed and running before its communications can be monitored by the CMS. The CMS must also be enabled, installed, and registered in the Clearinghouse before you begin monitoring.

Use these procedures to initialize and register the CMS:

- Initializing the Communications Monitoring Service - names the CMS and automatically registers it in the Clearinghouse Service if possible. Registration will fail if the Clearinghouse is unavailable.

- Manual registration - required only if the CMS was unable to register itself during the first procedure.

Use the following information and procedures to set up to monitor communications and logging:

- Communications Monitoring overview - describes the types of monitoring and logging that the Communications Monitoring Service can perform.

- Setting up to monitor SNA communications - gives step-by-step instructions to set up the monitoring profile for monitoring SNA communications.

- Setting up to monitor X.25 communications - gives step-by-step instructions to set up the monitoring profile for monitoring X.25 communications.

- Setting up to monitor RS-232C communications - gives step-by-step instructions to set up the monitoring profile for monitoring RS-232C communications.

- Setting up auto-logging - gives step-by-step instructions to set up the monitoring profile for auto-logging.

Initializing the Communications Monitoring Service

When the Communications Monitoring Service is started for the first time, you must supply a name and description for the service. Given a name and description, the Communications Monitoring Service then attempts to register itself in the appropriate Clearinghouse domain. A message is displayed to indicate whether the registration was successful or not.

Before you can perform the following procedure, you must first install the Communications Monitoring Service software on the server. This procedure is based on the assumption that you have followed Steps 1-12 in the *Server Software Installation* booklet. The Clearinghouse Service should be running, and you should have already proceeded your server.

Procedure

1. Type **Y** in response to the "CMS: Normal Startup?" prompt and press <RETURN>.

2. Type the name for this Communications Monitoring Service in response to the "Enter service name:" prompt and press <RETURN>. If the Clearinghouse Service is not available for any reason, you must enter the fully-qualified name of the Communications Monitoring Service.

3. Type a description for the Communications Monitoring Service in response to the "Enter service description:" prompt and press <RETURN>.

4. Type **Y** and press <RETURN> in response to the "Confirm (Y/N)?" prompt if you want to continue with registration.

   Type **N** and press <RETURN> if you want to stop without attempting registration. You would want to do this if, for example, you made a mistake when typing the service's name or description. If you type **N**, you must restart the server and repeat this procedure to register the service.

5. If you typed **Y** in response to the "Confirm" prompt, the Communications Monitoring Service attempts to register itself in the appropriate Clearinghouse domain.

   If the registration is successful, a message is displayed indicating that a new Clearinghouse entry was created. Continue with the next section "Communications Monitoring overview."

   If the registration was not successful, a message is displayed indicating that a new Clearinghouse entry was not created. You must manually register the Communications Monitoring Service when the Clearinghouse is available. Continue with the next procedure, "Manual registration," after the Clearinghouse is available.

This is an example of the prompts and responses for this procedure.

```
CMS:Normal Startup (Y/N): YRETURN
Attempting to determine the name of this Communications Monitoring Service.
Service name and description unknown.
    Enter service name: OurCMSRETURN
    Enter service description: Com monitor for OurServerRETURN
    Confirm? (Y/N): YRETURN
CMS: Validating Clearinghouse entry for OurCMS:OurDomain:OurOrg
CMS: A new Clearinghouse entry was created.
CMS: Done
CMS: Communications Monitoring Service is running.
CMS: Communications Monitoring Service is started.
Communications Monitoring Service run.
```

Manual registration

If the Communications Monitoring Service was unable to register itself when started for the first time, the Clearinghouse was unavailable. Usually this is due to the Clearinghouse not being operational at the time. It could also mean there is a problem in the network cabling or hardware. You must correct the problem and then use the **Register Communications Monitoring Service** command to register the service manually when the Clearinghouse is available.

Note: You must perform the "Initializing the Communications Monitoring Service" procedure before you can manually register the CMS.

Procedure

1. Type **Stop Service** and press <RETURN>.

2. Enter the number corresponding to Communications Monitoring Service and press <RETURN>. Type **Y** to the Stop Immediately? prompt.

3. Log on and enable in the Communications Monitoring Service context.

```
Logon:RETURN
    User's Name: MWBRETURN
    Password: ****RETURN
>EnableRETURN
Add Another User? (Y/N):  NRETURN
!Communications Monitoring ServiceRETURN
CMS!
```

4. Type **Register Communications Monitoring Service** and press <RETURN>.

```
CMS!Register Communications Monitoring ServiceRETURN
CMS: Validating Clearinghouse entry for OurCMS:OurDomain:OurOrg
CMS: A new Clearinghouse entry was created.
CMS: Done
```

5. Continue with the next section, "Communications Monitoring overview."

Communications Monitoring overview

Before you can use the Communications Monitoring Service, you must specify the type of monitoring and logging to be performed. The information that specifies the monitoring and logging is called the monitoring profile and is stored in the Communications Monitoring Service section of the server's profile.

Once specified, the monitoring profile values remain set until explicitly changed with one of the Communications Monitoring Service **Set** commands. Restarting the server does not alter the monitoring profile.

Monitoring

The Communications Monitoring Service can perform three types of monitoring: SNA, X.25, and RS-232C. All three types of monitoring capture data from an RS-232C port, either a port local to the server, or a CIU port managed by an External Communication Service on the same server as the Communications Monitoring Service. The difference between the three types of monitoring is in how the data is interpreted. The communication service being monitored must be co-resident with the CMS.

The type of monitoring you specify in the monitoring profile must agree with the configuration of the RS-232C port being monitored. You cannot, for example, use X.25 monitoring to monitor SNA communications.

SNA monitoring

For SNA monitoring, the data is interpreted according to SNA protocol. SNA communications can be monitored at several levels: SDLC, Path Control (LU & PU), Path Control (PU Only), or all three levels at once. The data is always stored and displayed in hexadecimal. SNA monitoring also accumulates a number of statistics regarding the communication, including the BIND parameters for LU sessions. Only one SNA link can be monitored at a time.

X.25 monitoring

For X.25 monitoring, the data is interpreted according to X.25 protocol. X.25 communications are always monitored at the HDLC level. The data is always stored and displayed in hexadecimal. Only one IRS/X.25 circuit can be monitored at a time.

RS-232C monitoring

For RS-232C monitoring, the data is not interpreted according to any protocol. Therefore, you can use RS-232C monitoring to monitor any protocol, such as 3270 BSC or asynchronous TTY. The data can be stored and displayed in four different formats: hexadecimal, octal, ASCII, or EBCDIC. If multiple instances of the ECS 3270/SNA controller software are running on a single server, only RS-232C level monitoring may be performed. RS-232C monitoring is not available for the Internetwork Routing Service. The CMS does not monitor more than one RS-232C port simultaneously.

Logging

During monitoring, data is captured from the RS-232C port being monitored. The captured data is written to a temporary file, called a working log file, in fixed length records called log entries. You specify the size (in bytes) of each log entry, and the capacity (in log entries) of a working log file.

Working log files

There are two working log files. The captured data is written to one of the working log files, called the current log file. When the current log file becomes full, it is written to a local log file in the server's working directory. The other working log file is made by the current log file, and the captured data is written to it. One working log file is always being filled with captured data while the other is being copied to the local log file in the server's working directory.

The two working log files are stored in virtual memory and are lost whenever the server is started or restarted. The local log file is permanent, but it is overwritten each time the active log file fills to capacity. If you want to save the local log file once, you can rename it to prevent it from being overwritten. If you want to save the local log file a number of times in succession, you can use auto-logging.

Auto-logging

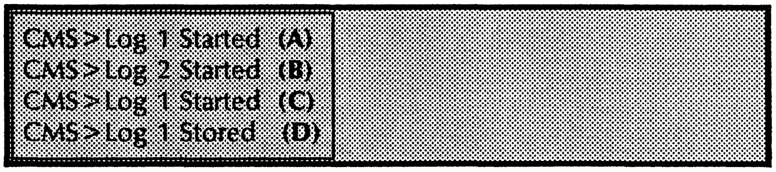
Auto-logging automatically copies the local log file to a remote log file on a File Server. You specify the number of times (store frequency) a working log file is written to the local log file before the local log file is copied to a remote log file. A frequency of one causes the local log file to be copied every time a working log file is written to it. A frequency of three causes the local log file to be copied every third time a working log file is written to it.

The local log file is copied to a remote log file. The remote log file has the same name as the local log file plus an appended time stamp. The time stamp makes the remote log file's name unique and prevents the last remote log file from being written over.

You specify the File Server and directory in which the remote log files are stored. You must also add the name of the Communications Monitoring Service to an access list (with write access) for the remote directory before the service can store files to the remote directory.

Because a new remote log file is created each time the local log file is copied, auto-logging can use large amounts of storage space. To limit the amount of space that can be used, a filing threshold is specified. Once the number of remote log files reaches the threshold, auto-logging is stopped until it is explicitly started again (and the threshold raised or old remote log files deleted). You can also limit the amount of space used by auto-logging by putting a size limit on the file drawer in which the remote log files are stored. Auto-logging will stop when the file drawer becomes full.

Under rare circumstances, the Communications Monitoring Service can display a series of messages like the following if auto-logging is in effect (bold letters are not part of messages):



```
CMS>Log 1 Started (A)
CMS>Log 2 Started (B)
CMS>Log 1 Started (C)
CMS>Log 1 Stored  (D)
```

You might interpret these messages to mean that the log file (Log 1) referenced in line A is being overwritten by the operation in line C. It is not. The actual sequence of events is:

(A) CMS starts writing to log 1.
(B) Log 1 fills and is stored locally. CMS begins writing to log 2 and begins writing log 1 to a remote disk.
(C) Log 2 fills and is stored locally after log 1 has been written to a remote disk. CMS begins writing to a second log 1.
(D) CMS displays the message that log 1 has been written to a remote disk.

Potential confusion arises from line C being displayed before line D. In fact, writing to the second log 1 cannot begin until the first log 1 has been successfully stored on a remote disk.

The log file banner

Both local log files and remote log files contain a log banner at the beginning of the file. The log banner identifies the server, the Communications Monitoring Service, and the Monitoring Profile entries that produced the log file. See Appendix C, Sample log file for example log files and a complete description of the log banner.

Stopping and starting logging

All monitoring and logging must be explicitly started and stopped, except that auto-logging will stop automatically as noted above. To start and stop monitoring and logging, use the **Start Logging** and **Stop Logging** commands. These two commands control both monitoring and logging. You cannot monitor a communication without logging it.

Setting up to monitor SNA communications

Use SNA monitoring to monitor the communication between an External Communication Service providing IBM 3270 SNA emulation and the IBM host. When an External Communication Service is set to provide IBM 3270 SNA emulation, the External Communication Service allows workstations with the appropriate terminal emulation software to communicate with an IBM host through an RS-232C port. The External Communication Service provides protocol conversion between SNA and Xerox Network System protocols.

Complete CMS Form 1, SNA Monitoring, in Appendix A.

The SNA protocol can be monitored at several levels: SDLC, Path Control (LU & PU), Path Control (PU Only), or all three at once. Additionally, SNA monitoring keeps a number of statistics regarding the communication, including the BIND parameters for LU sessions. These statistics can be included in the log file. Data from SNA monitoring is always displayed in hexadecimal.

Procedure

1. Log on and enable in the Communications Monitoring Service context.

```
>LogonRETURN
   User's Name: MWBRETURN
   Password: ****RETURN
>EnableRETURN
!Communications Monitoring ServiceRETURN
CMS!
```

2. Type **Set Monitoring Profile** and press <RETURN>.

   The service prompts for the information required for the monitoring profile. Answer each prompt and press <RETURN>. The answer to each prompt is discussed in the following steps.

3. Type **1**, for SNA protocol monitoring, in response to the "Select protocol" prompt and press <RETURN>.

4. Type **1**, for 3270, in response to the "product option" prompt and press <RETURN>. SNA protocol monitoring currently supports 3270 emulation only.

5. Type the number that corresponds to the level at which you want to monitor the SNA protocol in response to the "protocol level" prompt and press <RETURN>. Option 2, Path Control (LU & PU), is the most common choice.

6. Type the size, in bytes, of each log file entry in response to the "bytes to record per log entry" prompt and press <RETURN>. This is the number of bytes that must be captured from the port being monitored before an entry

is written to the current log file. The allowed range is 40 through 600.

7. Type the size, in log entries, of a log file in response to the "Maximum number of entries" prompt and press <RETURN>. The allowed range is 100 through 200. The number of log entries times the number of bytes in a log entry is the approximate size of a working log file.

8. Type a comment or description (up to a maximum of 100 characters) in response to the "Log file comment" prompt and press <RETURN>. The comment you type will be included in the log banner of each log file made with this monitoring profile.

9. Type **Y** and press <RETURN> in response to the "Include Statistics" prompt if you want to include SNA monitoring statistics in the log files. Otherwise, type **N**. If you type **N**, the statistics can still be displayed with the **Show Statistics** command.

10. Type **1**, for "HEX," and press <RETURN> in response to the "display format" prompt. With SNA monitoring, data can be displayed only in hexadecimal.

11. Type the number that corresponds to the port you want to monitor and press <RETURN> in response to the "Choose RS232-C port to monitor" prompt. The protocol used on the port you select must agree with the type of monitoring you have selected.

12. Type a name for the local log file and press <RETURN> in response to the "Log name" prompt.

13. Type **N** and press <RETURN> in response to the "Backup log automatically" prompt if you do not want to use auto-logging. Type **Y** and press <RETURN> if you want to enable auto-logging.

    If you typed **N**, you can enable auto-logging later without changing the rest of the monitoring profile by using the **Set Remote Log Handling** command. However, once auto-logging has been enabled, you must use the **Set Monitoring Profile** command to stop it.

    If you typed **Y** to enable auto-logging now, skip to the "Setting up auto-logging" section later in this chapter.

14. Type **Y** and press <RETURN> in response to the "Confirm this monitoring profile" prompt if all the answers to the earlier prompts are correct. If you type **N**, the command is canceled and the monitoring profile is not changed. To correct errors, type **N** and repeat the **Set Monitoring Profile** command.

Here is an example of the complete sequence.

```
CMS!Set Monitoring ProfileRETURN
   Select protocol to be monitored
   1  SNA
   2  X.25
   3  RS232C
   Enter choice number: 1RETURN
   Possible product option(s)
   1 3270
   Enter choice number: 1RETURN
   Select protocol level
   1  SDLC
   2  Path Control (LU & PU)
   3  Path Control (PU ONLY)
   4  All
   Enter choice number: 2RETURN
   Amount of data bytes to record per log entry (40..600): 300RETURN
   Maximum number of entries in log file (100..200): 200RETURN
   Log file comment: Sample log file, SNA monitoringRETURN
   Include Statistics in log? (Y/N): NRETURN
   Specify display format
   1  HEX
   Enter choice number: 1RETURN
   Choose RS232C port to monitor
   1  SNAport1
   Enter choice number: 1RETURN
   Log name: SNAlogRETURN
   Backup log automatically? (Y/N): NRETURN
   Confirm this monitoring profile (Y/N): YRETURN
Monitoring profile set.
```

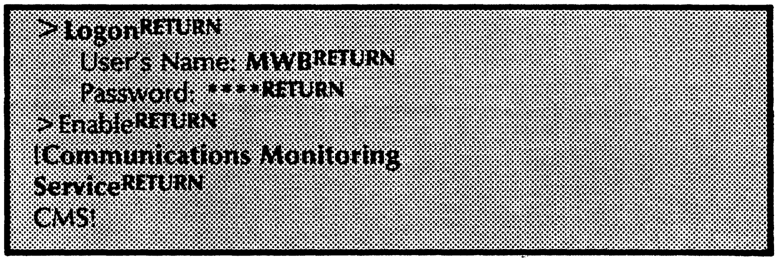
Setting up to monitor X.25 communications

Use X.25 monitoring to monitor communications between an Internetwork Routing Service and an X.25 public data network. An X.25 public data network, such as Tymnet or Telenet, allows an Internetwork Routing Service to establish connections (virtual circuits) to multiple Internetwork Routing Services on other networks through a single RS-232C port. Before you start, complete CMS Form 2, X.25 Monitoring, in Appendix A.

The X.25 protocol is always monitored at the HDLC level. The data is displayed in hexadecimal.

Procedure

1. Log on and enable in the Communications Monitoring Service context.



```
>LogonRETURN
  User's Name: MWBRETURN
  Password: ****RETURN
>EnableRETURN
!Communications Monitoring
ServiceRETURN
CMS!
```

2. Type **Set Monitoring Profile** and press <RETURN>.

   The service then prompts for the information required for the monitoring profile. Answer each prompt and press <RETURN>. The answer to each prompt is discussed in the following steps. An example is provided at the end.

3. Type **2**, for X.25 protocol monitoring, in response to the "Select protocol" prompt and press <RETURN>.

4. Type the size, in bytes, of each log file entry in response to the "bytes to record per log entry" prompt and press <RETURN>. This is the number of bytes that must be captured from the port being monitored before an entry is written to the active log file. The allowed range is 40 through 600.

5. Type the size, in log entries, of a log file in response to the "Maximum number of entries" prompt and press <RETURN>. The allowed range is 100 through 200. The number of log entries times the number of bytes in a log entry is the approximate size of a working log file.

6. Type a comment or description (up to a maximum of 100 characters) in response to the "Log file comment" prompt and press <RETURN>. The comment you type will be included in the log banner of each log file made with this Monitoring Profile.

7. Type **1**, for "HEX," and press <RETURN> in response to the "display format" prompt. Data can be displayed only in hexadecimal with X.25 monitoring.

8. Type the number that corresponds to the port you want to monitor and press <RETURN> in response to the "Choose RS232C port to monitor" prompt. The protocol used on the port you select must agree with the type of monitoring you have selected.

9. Type a name for the local log file and press <RETURN> in response to the "Log name" prompt.

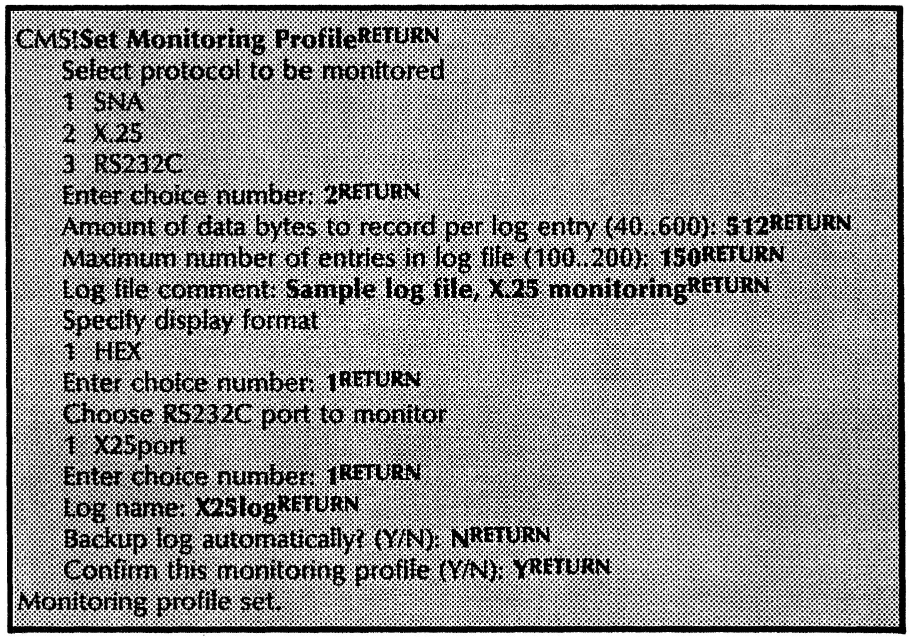
10. Type **N** and press <RETURN> in response to the "Backup log automatically" prompt if you do not want to use auto-logging. Type **Y** and press <RETURN> if you want to enable auto-logging.

    If you typed **N**, you can enable auto-logging later without changing the rest of the monitoring profile by using the **Set Remote Log Handling** command. However, once auto-logging has been enabled, you must use the **Set Monitoring Profile** command to stop it.

    If you typed **Y** to enable auto-logging now, skip to the "Setting up auto-logging" section later in this chapter.

11. Type **Y** and press <RETURN> in response to the "Confirm this monitoring profile" prompt if all the answers to the earlier prompts are correct. If you type **N**, the command is canceled and the monitoring profile is not changed. To correct errors, type **N** and repeat the **Set Monitoring Profile** command.

    Here is an example of the complete sequence.



```
CMS!Set Monitoring ProfileRETURN
    Select protocol to be monitored
    1  SNA
    2  X.25
    3  RS232C
    Enter choice number: 2RETURN
    Amount of data bytes to record per log entry (40..600): 512RETURN
    Maximum number of entries in log file (100..200): 150RETURN
    Log file comment: Sample log file, X.25 monitoringRETURN
    Specify display format
    1  HEX
    Enter choice number: 1RETURN
    Choose RS232C port to monitor
    1  X25port
    Enter choice number: 1RETURN
    Log name: X25logRETURN
    Backup log automatically? (Y/N): NRETURN
    Confirm this monitoring profile (Y/N): YRETURN
Monitoring profile set.
```

Setting up to monitor RS-232C communications

Use RS-232C monitoring to monitor any Xerox Communication Service that communicates through an RS-232C port, except the Internetwork Routing Service. This type of monitoring captures the data and does not interpret it. Because the data is not interpreted according to a particular protocol, RS-232C monitoring can be used to monitor communications using any protocol, such as BSC or asynchronous TTY. Before you start, complete CMS Form 3, RS-232C Monitoring, in Appendix A.

When monitoring a communication with RS-232C monitoring, you or an analyst must interpret the captured data according to the protocol being used. You can select the format in which the captured data is displayed: hexadecimal, octal, ASCII, or EBCDIC. The last three formats are only available for monitoring at the RS-232C level.

Procedure

1. Log on and enable in the Communications Monitoring Service context.

```
>LogonRETURN
   User's Name: MWBRETURN
   Password: ****RETURN
>EnableRETURN
!Communications Monitoring ServiceRETURN
CMS!
```

2. Type **Set Monitoring Profile** and press <RETURN>.

   The service then prompts for the information required for the monitoring profile. Answer each prompt and press <RETURN>. The answer to each prompt is discussed in the following steps.

3. Type **3**, for RS-232C protocol monitoring, in response to the "Select protocol" prompt and press <RETURN>.

4. Type the size, in bytes, of each log file entry in response to the "bytes to record per log entry" prompt and press <RETURN>. This is the number of bytes that must be captured from the port being monitored before an entry is written to the active log file. The allowed range is 40 through 600.

5. Type the size, in log entries, of a log file in response to the "Maximum number of entries" prompt and press <RETURN>. The allowed range is 100 through 200. The number of log entries times the number of bytes in a log entry is the approximate size of a working log file.

6. Type a comment or description (up to a maximum of 100 characters) in response to the "Log file comment" prompt and press <RETURN>. The comment you type will be

included in the log banner of each log file made with this monitoring profile.

7. Type the number corresponding to the format in which you want the data to be stored and displayed in response to the "display format" prompt and press <RETURN>.

8. Type the number that corresponds to the port you want to monitor and press <RETURN> in response to the "Choose RS232-C port to monitor" prompt. The protocol used on the port you select must agree with the type of monitoring you have selected.

9. Type a name for the local log file and press <RETURN> in response to the "Log name" prompt.

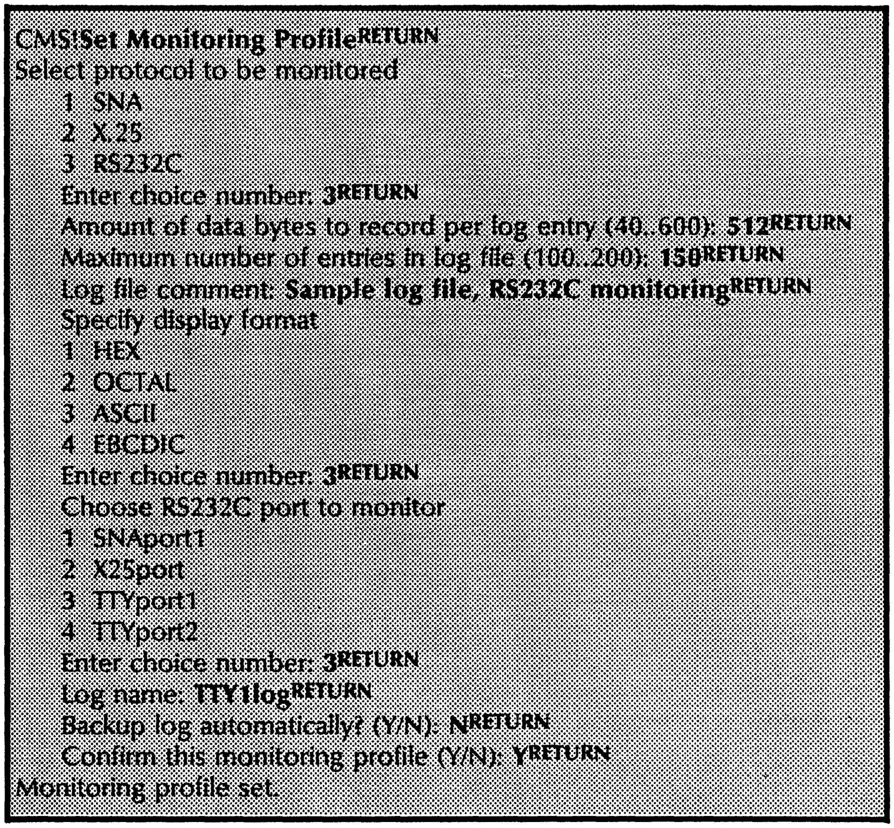
10. Type **N** and press <RETURN> in response to the "Backup log automatically" prompt if you do not want to use auto-logging. Type **Y** and press <RETURN> if you want to enable auto-logging.

    If you typed **N**, you can enable auto-logging later without changing the rest of the monitoring profile by using the **Set Remote Log Handling** command. However, once auto-logging has been enabled, you must use the **Set Monitoring Profile** command to stop it.

    If you typed **Y** to enable auto-logging now, skip to the "Setting up auto-logging" section later in this chapter.

11. Type **Y** and press <RETURN> in response to the "Confirm this monitoring profile" prompt if all the answers to the earlier prompts are correct. If you type **N**, the command is canceled and the monitoring profile is not changed. To correct errors, type **N** and repeat the **Set Monitoring Profile** command.

    See the next page for an example of the complete sequence.



```
CMS!Set Monitoring ProfileRETURN
Select protocol to be monitored
    1 SNA
    2 X.25
    3 RS232C
    Enter choice number: 3RETURN
    Amount of data bytes to record per log entry (40..600): 512RETURN
    Maximum number of entries in log file (100..200): 150RETURN
    Log file comment: Sample log file, RS232C monitoringRETURN
    Specify display format
    1 HEX
    2 OCTAL
    3 ASCII
    4 EBCDIC
    Enter choice number: 3RETURN
    Choose RS232C port to monitor
    1 SNAport1
    2 X25port
    3 TTYport1
    4 TTYport2
    Enter choice number: 3RETURN
    Log name: TTY1logRETURN
    Backup log automatically? (Y/N): NRETURN
    Confirm this monitoring profile (Y/N): YRETURN
Monitoring profile set.
```

Setting up auto-logging

Auto-logging provides automatic storing of log files to a specified File Service. Use auto-logging with any type of monitoring. You must create or assign a file drawer to store the logs before doing this procedure. Refer to the "Creating file drawers for users" section in the *File Service* booklet for details on creating a new file drawer.

To enable auto-logging, first follow the "Setting up to monitor SNA communications," "Setting up to monitor X.25 communications," or "Setting up to monitor RS-232C communications" procedures to set up the type of monitoring you want to perform. When the service prompts "Backup log automatically?" answer **Y** and continue with the procedure given below.

Filing threshold

When the filing threshold is met during auto-logging, the System Administrator must explicitly change the remote log handling parameters in the monitoring profile **(Set Remote Log Handling** or **Set Monitoring Profile)** if they want to have auto-logging restarted. The filing threshold may be met for the following reasons.

1. The File Service which contains the remote log storage file drawer is full.

2. The remote log storage file drawer is full.

3. The maximum number of files that can be stored to a remote directory (which is specified in the monitoring profile) has been reached.

The reason for the threshold being met must be changed as well. Otherwise, the same condition will cause the filing threshold to be met immediately again.

Procedure

1. Perform the steps under "Setting up to monitor SNA communications," "Setting up to monitor X.25 communications," or "Setting up to monitor RS-232C communications" procedures, depending on the type of monitoring to be performed.

2. Type **Y** in response to the "Backup log automatically?" prompt and press <RETURN>.

3. Type the path name of the File Service and directory where the remote log files are to be stored in response to the "Remote Directory" prompt and press <RETURN>.

   The File Service name must be enclosed within parentheses. If the File Service is in the same domain and organization as the Communications Monitoring Service, you can omit the domain and organization from the File

Service name. If you omit the domain and organization, the File Service name must be followed by a colon (:).

The Communications Monitoring Service must be a member of a group with write access to the specified remote directory.

4. Type the maximum number of remote log files to allow in the remote directory in response to the "Maximum number of logs" prompt and press <RETURN>. Once this number is reached, auto-logging will stop.

5. Type the frequency for storing the local log file remotely in response to the "Store every Nth log" prompt and press <RETURN>. If you type **1**, the local log file is stored remotely each time it is updated from a working log file. If you type **5**, the local log file is stored remotely every fifth time it is updated from a working log file.

6. Type **Y** and press <RETURN> in response to the "Confirm this monitoring profile" prompt if all the answers to the earlier prompts are correct. If you type **N**, the command is canceled and the monitoring profile is not changed. To correct errors, type **N** and repeat the **Set Monitoring Profile** command.

   Here is an example of the complete sequence.

```
Backup log automatically? (Y/N):  YRETURN
Remote Directory: (FileService1:)ComLogs/SNAlogsRETURN
Maximum number of logs stored remotely (1..100): 60RETURN
Store every Nth log (1..10): 1RETURN
Confirm this monitoring profile (Y/N): YRETURN
```

(This page intentionally blank)

3. Maintaining your Communications Monitoring Service

Use the procedures in this chapter to monitor communications, display and store log files, and maintain the Communications Monitoring Service.

This information is contained in this chapter:

- Getting on-line help
- Starting the logging process
- Showing an active log
- Stopping the logging process
- Saving a log
- Displaying a log
- Displaying statistics
- Displaying monitoring parameters
- Changing monitoring parameters
- Renaming the Communications Monitoring Service
- Removing the Communications Monitoring Service from a server

Getting on-line help

The Communications Monitoring Service has an on-line help facility that displays a brief explanation of the service. Use this help facility when the Communications Monitoring Service booklet is not available.

Procedure

1. Log on in the Communciations Monitoring Service context.

2. Type **Help** and press <RETURN>.

```
CMS!HelpRETURN
The Communications Monitoring Service provides protocol monitoring for Xerox
Communications Services. It creates a monitoring profile for customizing monitoring. The
monitoring parameters are recorded in the Communications Monitoring Service section of
the server profile.

Monitoring is provided at various levels of SNA, X.25, and RS232C. Two working log files
capture information from the communication line. When a working log file is full, a local NS
file is created in the working directory of the server. The Network Administrator may
choose to have a remote NS file created automatically on a File Service at this time as well.
Parameters for monitoring are set by using either Set Monitoring Profile (for all parameters),
or Set Protocol, Set Log Attributes, Set Log Name, Set Remote Log Handling for setting
portions of the profile parameters. Initial values of the profile default to monitor RS232C.
The protocol may be changed with Set Protocol. A default log name for the NS file will be
created based on the type of monitoring selected. The Network Administrator may change
this to a name of their choice with the Set Log Name command.

The amount of data bytes collected during monitoring, the number of entries in a working
log file, whether an optional comment or statistics (SNA only) should be inserted into the
log file, the type of display format for the data, and the RS232C port to monitor may be
specified with the Set Log Attributes command. Statistics are also available with the Show
Statistics command.

Auto-logging of NS files is initiated with the Set Remote Log Handling command.
Parameters include the File Service path name, the maximum number of logs to store, and
the store frequency to remotely store every Nth local NS file created. All profile values may
be set with Set Monitoring Profile and shown with Show Monitoring Profile.

Logging may be started and stopped with the Start Logging and Stop Logging commands.
Working log files may be displayed with Show Log. A working log file may be stored to a
File Service with Save Log.

Starting and stopping the service is accomplished with the Start Communications Monitoring
Service and Stop Communiations Monitoring Service commands. If service self-registration
fails, Register Communications Monitoring Service is available. To rename the service, use
the Rename Communications Monitoring Service command.
```

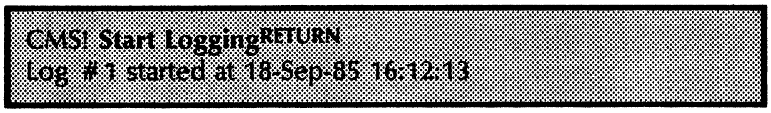
Starting the logging process

Once the Communications Monitoring Service is running, you must explicitly start logging. Logging is never started automatically even if the server running the CMS crashes or is rebooted.

Procedure

1. Log on and enable in the Communications Monitoring Service context.

2. Type **Start Logging** and press <RETURN>.



```
CMS! Start LoggingRETURN
Log #1 started at 18-Sep-85 16:12:13
```

Showing an active log

The **Show Active Log** command is used to see which log file is current and whether or not it is active. If the current log file is not active, the other log file becomes the current log file when logging is started.

Procedure

1. Log on and enable in the Communications Monitoring Service context.

2. Type **Show Active Log** and press <RETURN>.

```
CMS! Show Active LogRETURN
Log #1 is the current log.  It is active.
```

The message displayed after you type the command indicates whether or not the current log file is active.

Stopping the logging process

You can stop logging at any time by using the **Stop Logging** command. If the current log file is only partially full when you stop logging, and you want to save the data, you must use the **Save Log** command.

Procedure

1. Log on and enable in the Communications Monitoring Service context.

2. Type **Stop Logging** and press <RETURN>.

```
CMS! Stop Logging RETURN
CMS: Logging Stopped.
```

Saving a log

You can save the data that is in a working log file using the **Save Log** command. When you type this command, any outstanding filing operations are completed before the save takes place, and logging stops.

You supply a remote directory name and can insert a comment in the log file with this command. If you do not fully qualify the File Service name with its domain and organization, you must use a terminating colon after the File Service name and before the closed parenthesis. The directory name and comment you supply do not replace those you have supplied in the monitoring profile.

You can save logs in different formats by changing the display format portion of the monitoring profile before typing the **Save Log** command.

Procedure

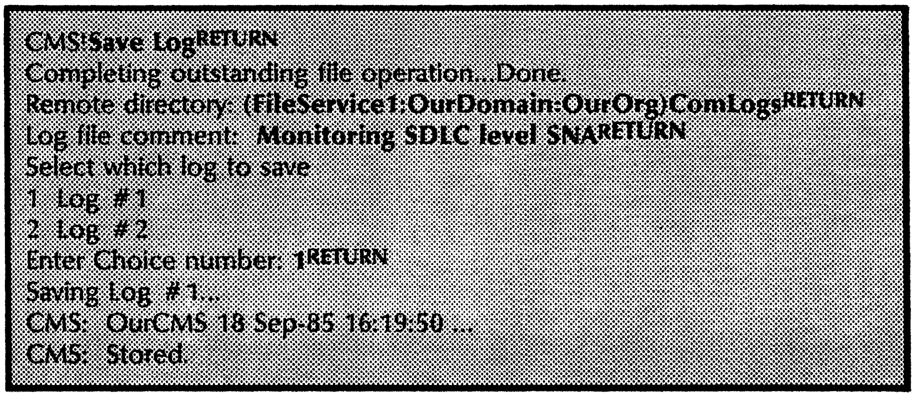
1. Log on and enable in the Communications Monitoring Service context.

2. Type **Save Log** and press <RETURN>.

3. Type the name of the remote directory to which you want to save the working log file in response to the "Remote Directory:" prompt and press <RETURN>.

4. Type a comment in response to the "Log file comment:" prompt and press <RETURN>.

5. Type **1** for Log #1, or **2** for Log #2 in response to the "Enter choice number:" prompt and press <RETURN>.



```
CMS!Save LogRETURN
Completing outstanding file operation...Done.
Remote directory: (FileService1:OurDomain:OurOrg)ComLogsRETURN
Log file comment:  Monitoring SDLC level SNARETURN
Select which log to save
1  Log #1
2  Log #2
Enter Choice number: 1RETURN
Saving Log #1...
CMS:  OurCMS 18 Sep-85 16:19:50 ...
CMS:  Stored.
```

Displaying a log

You can see a display of the contents of a working log file by using the **Show Log** command. Logging stops before the log file is displayed. This command is useful to determine whether or not you want to save a particular log file. If you are monitoring with the RS-232C option, this command lets you specify the display format in which you want the data displayed.

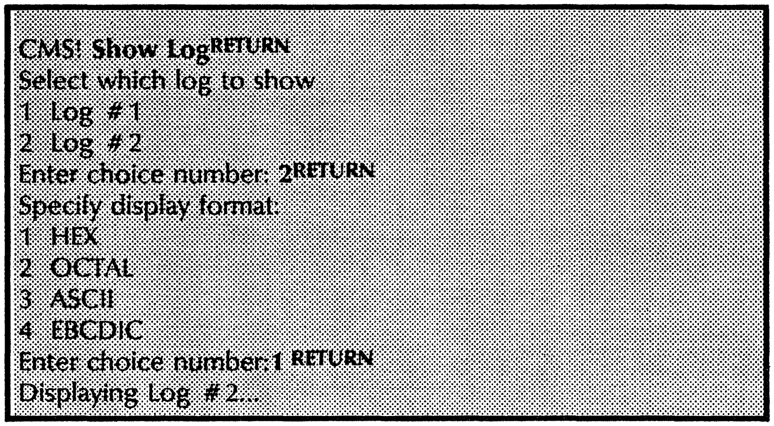
Procedure

1. Log on and enable in the Communications Monitoring Service context.

2. Type **Show Log** and press <RETURN>.

3. Type **1** for Log #1 or **2** for Log #2 in response to the "Enter Choice Number" prompt and press <RETURN>.

4. If you are monitoring RS-2232C protocol, type the number of the display format in which you want the log file displayed in response to the "Specify display format:" prompt, and press <RETURN>.



```
CMS! Show LogRETURN
Select which log to show
1 Log #1
2 Log #2
Enter choice number: 2RETURN
Specify display format:
1 HEX
2 OCTAL
3 ASCII
4 EBCDIC
Enter choice number:1 RETURN
Displaying Log #2...
```

Displaying statistics

To display the statistics collected for SNA, use the **Show Statistics** command. Statistics are only collected when you are monitoring SNA protocol. You need to have knowledge of the SNA protocol for these statistics to be meaningful.

These are the statistics that are displayed:

- SNA Buffer Stats - Displays statistics for SNA buffers and how the buffers have been used.

- SNA Dispatcher Stats - Displays statistics for the SNA dispatcher.

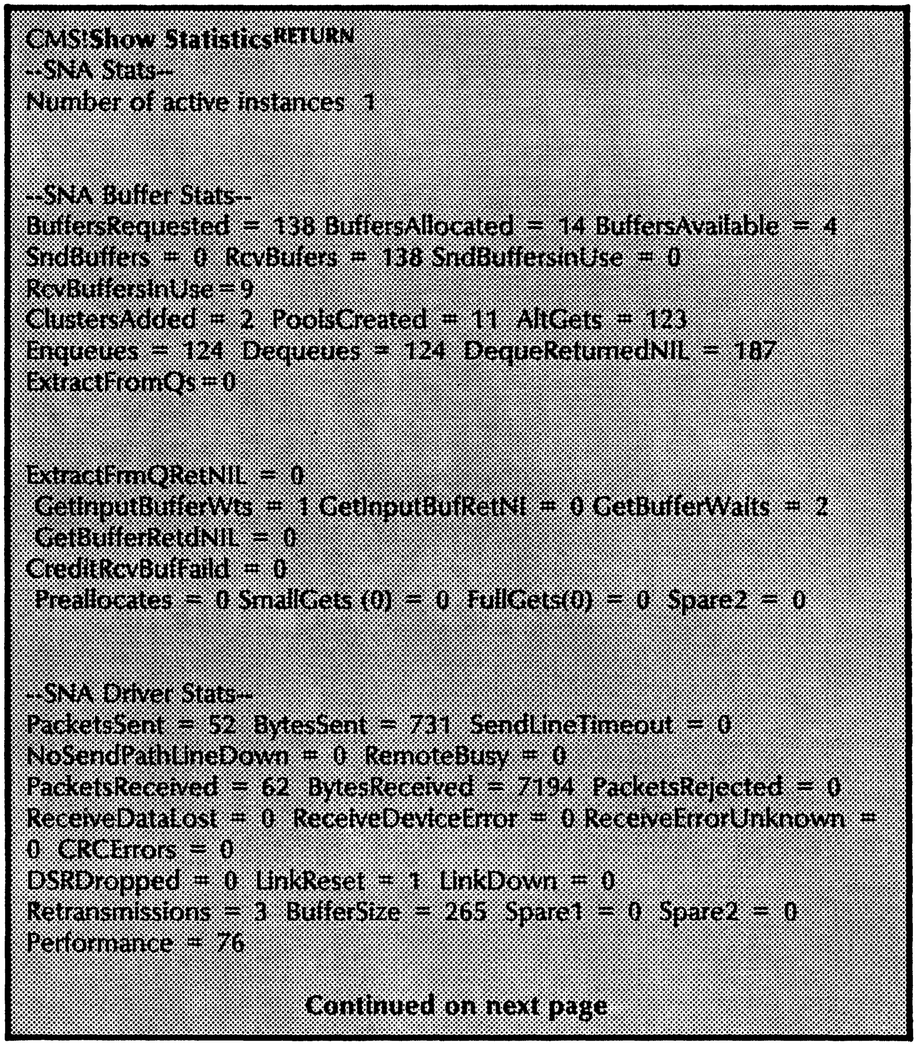
- SNA PU Stats - Displays statistics for a physical unit.

- SNA LU Stats - Displays statistics for logical units, including information about user sessions and BIND parameters. These statistics can be helpful in diagnosing problems with users sessions.

Procedure

1. Log on and enable in the Communications Monitoring Service context.

2. Type **Show Statistics** and press <RETURN>.



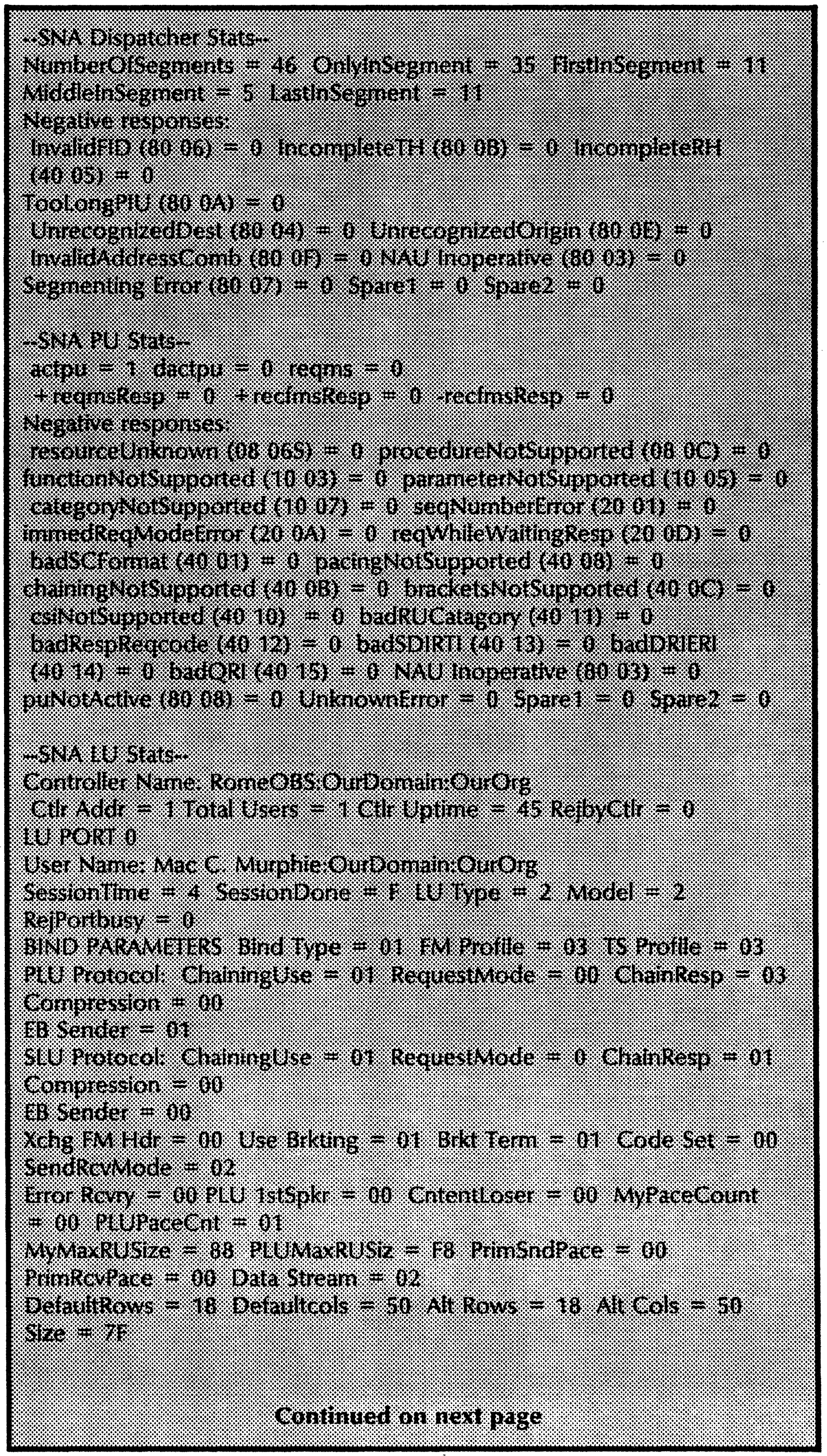
```
CMS!Show StatisticsRETURN
--SNA Stats--
Number of active instances  1


--SNA Buffer Stats--
BuffersRequested = 138 BuffersAllocated = 14 BuffersAvailable = 4
SndBuffers = 0  RcvBufers = 138 SndBuffersinUse = 0
RcvBuffersInUse=9
ClustersAdded = 2  PoolsCreated = 11  AltGets = 123
Enqueues = 124  Dequeues = 124  DequeReturnedNIL = 187
ExtractFromQs=0


ExtractFrmQRetNIL = 0
 GetInputBufferWts = 1 GetInputBufRetNI = 0 GetBufferWaits = 2
 GetBufferRetdNIL = 0
CreditRcvBufFaild = 0
 Preallocates = 0 SmallGets (0) = 0  FullGets(0) = 0  Spare2 = 0


--SNA Driver Stats--
PacketsSent = 52  BytesSent = 731  SendLineTimeout = 0
NoSendPathLineDown = 0  RemoteBusy = 0
PacketsReceived = 62  BytesReceived = 7194  PacketsRejected = 0
ReceiveDataLost = 0  ReceiveDeviceError = 0 ReceiveErrorUnknown =
0  CRCErrors = 0
DSRDropped = 0  LinkReset = 1  LinkDown = 0
Retransmissions = 3  BufferSize = 265  Spare1 = 0  Spare2 = 0
Performance = 76
```

Continued on next page

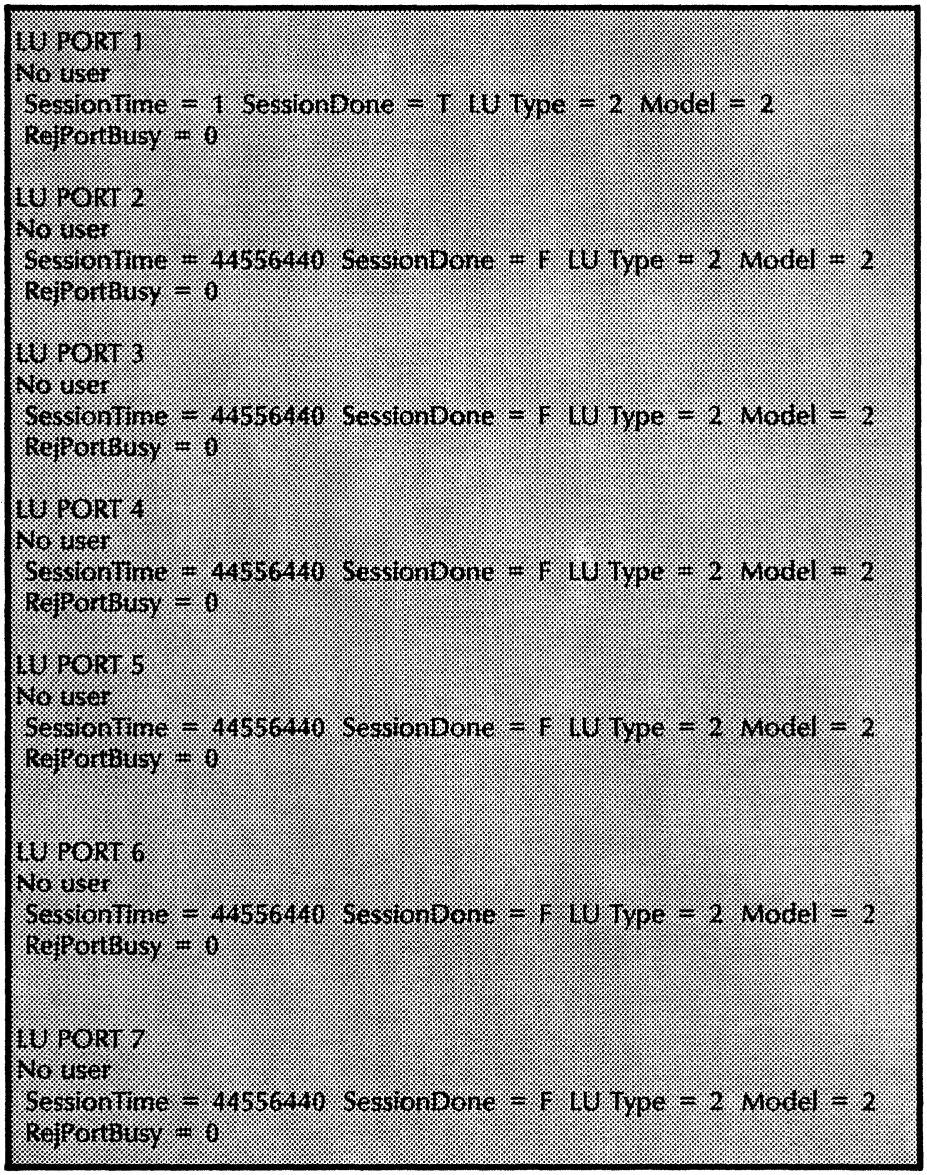


```
--SNA Dispatcher Stats--
NumberOfSegments = 46  OnlyInSegment = 35  FirstInSegment = 11
MiddleInSegment = 5  LastInSegment = 11
Negative responses:
 InvalidFID (80 06) = 0  IncompleteTH (80 0B) = 0  IncompleteRH
 (40 05) = 0
TooLongPIU (80 0A) = 0
 UnrecognizedDest (80 04) = 0  UnrecognizedOrigin (80 0E) = 0
 InvalidAddressComb (80 0F) = 0 NAU Inoperative (80 03) = 0
Segmenting Error (80 07) = 0  Spare1 = 0  Spare2 = 0

--SNA PU Stats--
 actpu = 1  dactpu = 0  reqms = 0
 +reqmsResp = 0  +recfmsResp = 0  -recfmsResp = 0
Negative responses:
 resourceUnknown (08 06S) = 0  procedureNotSupported (08 0C) = 0
functionNotSupported (10 03) = 0  parameterNotSupported (10 05) = 0
 categoryNotSupported (10 07) = 0  seqNumberError (20 01) = 0
immedReqModeError (20 0A) = 0  reqWhileWaitingResp (20 0D) = 0
 badSCFormat (40 01) = 0  pacingNotSupported (40 08) = 0
chainingNotSupported (40 0B) = 0  bracketsNotSupported (40 0C) = 0
 csiNotSupported (40 10)  = 0  badRUCatagory (40 11) = 0
 badRespReqcode (40 12) = 0  badSDIRTI (40 13) = 0  badDRIERI
 (40 14) = 0  badQRI (40 15) = 0  NAU Inoperative (80 03) = 0
puNotActive (80 08) = 0  UnknownError = 0  Spare1 = 0  Spare2 = 0

--SNA LU Stats--
Controller Name: RomeOBS:OurDomain:OurOrg
 Ctlr Addr = 1 Total Users = 1 Ctlr Uptime = 45 RejbyCtlr = 0
LU PORT 0
User Name: Mac C. Murphie:OurDomain:OurOrg
SessionTime = 4  SessionDone = F  LU Type = 2  Model = 2
RejPortbusy = 0
BIND PARAMETERS  Bind Type = 01  FM Profile = 03  TS Profile = 03
PLU Protocol:  ChainingUse = 01  RequestMode = 00  ChainResp = 03
Compression = 00
EB Sender = 01
SLU Protocol:  ChainingUse = 01  RequestMode = 0  ChainResp = 01
Compression = 00
EB Sender = 00
Xchg FM Hdr = 00  Use Brkting = 01  Brkt Term = 01  Code Set = 00
SendRcvMode = 02
Error Rcvry = 00 PLU 1stSpkr = 00  CntentLoser = 00  MyPaceCount
 = 00  PLUPaceCnt = 01
MyMaxRUSize = 88  PLUMaxRUSiz = F8  PrimSndPace = 00
PrimRcvPace = 00  Data Stream = 02
DefaultRows = 18  Defaultcols = 50  Alt Rows = 18  Alt Cols = 50
Size = 7F
```

Continued on next page



```
LU PORT 1
No user
 SessionTime = 1  SessionDone = T  LU Type = 2  Model = 2
 RejPortBusy = 0

LU PORT 2
No user
 SessionTime = 44556440  SessionDone = F  LU Type = 2  Model = 2
 RejPortBusy = 0

LU PORT 3
No user
 SessionTime = 44556440  SessionDone = F  LU Type = 2  Model = 2
 RejPortBusy = 0

LU PORT 4
No user
 SessionTime = 44556440  SessionDone = F  LU Type = 2  Model = 2
 RejPortBusy = 0

LU PORT 5
No user
 SessionTime = 44556440  SessionDone = F  LU Type = 2  Model = 2
 RejPortBusy = 0


LU PORT 6
No user
 SessionTime = 44556440  SessionDone = F  LU Type = 2  Model = 2
 RejPortBusy = 0


LU PORT 7
No user
 SessionTime = 44556440  SessionDone = F  LU Type = 2  Model = 2
 RejPortBusy = 0
```

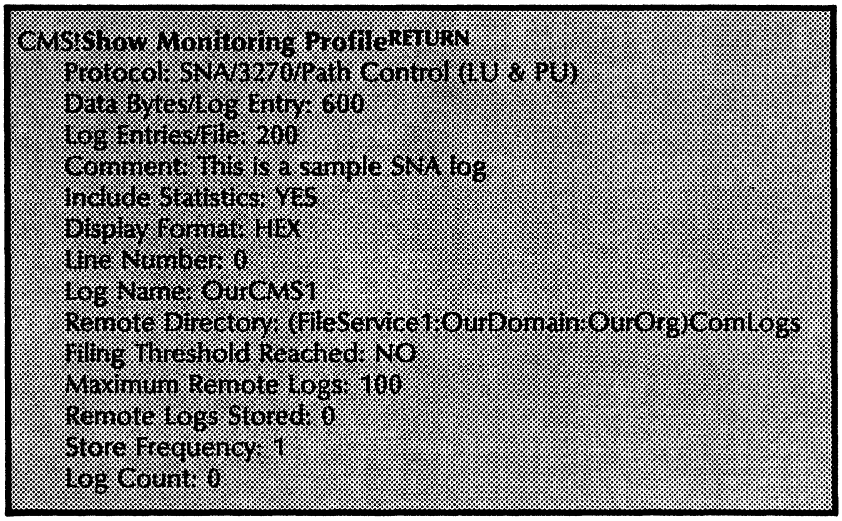
Displaying monitoring parameters

You can display a list of the values currently set in the monitoring profile using the **Show Monitoring Profile** command. If auto-logging is enabled, remote logging parameters are listed. The Communications Monitoring Service determines the line number parameter from the RS-232C port name you supplied in the **Set Monitoring Profile** command.

Procedure

1. Log on and enable in the Communications Monitoring Service context.

2. Type **Show Monitoring Profile** and press <RETURN>.



```
CMS!Show Monitoring ProfileRETURN
    Protocol: SNA/3270/Path Control (LU & PU)
    Data Bytes/Log Entry: 600
    Log Entries/File: 200
    Comment: This is a sample SNA log
    Include Statistics: YES
    Display Format: HEX
    Line Number: 0
    Log Name: OurCMS1
    Remote Directory: (FileService1:OurDomain:OurOrg)ComLogs
    Filing Threshold Reached: NO
    Maximum Remote Logs: 100
    Remote Logs Stored: 0
    Store Frequency: 1
    Log Count: 0
```

Changing monitoring parameters

You can set or change all monitoring profile parameters by using the **Set Monitoring Profile** command. Monitoring parameters are saved in the Communications Monitoring Service section of the server profile, and the values you set are retained until you explicitly change them.

The Communications Monitoring Service initially sets the profile to monitor RS-232C protocol with auto-logging disabled, and creates a default file based on the type of monitoring and the RS-232C port selected. If you do not specify an RS-232C port, the local port is used. If you select the SNA or X.25 protocol, the only display format you can choose is HEX.

If you are monitoring with SNA protocol, you are prompted to select a product option. Currently, 3270 is the only product option supported, and will be the only option displayed from which to choose.

Several parameters can be changed individually with a specific command. Use Procedure A to change all monitoring parameters. Use Procedure B to change the protocol. Use Procedure C to change log attributes. Use Procedure D to change the log name. Use Procedure E to change remote log handling.

Procedure A: Changing all monitoring parameters

1. Log on and enable in the Communications Monitoring Service context.

2. Type **Set Monitoring Profile** and press <RETURN>.

3. Type **1**, **2**, or **3** to select the protocol in response to the "Select protocol to be monitored" prompt and press <RETURN>.

4. If you selected SNA protocol, select the product option (3270) by typing **1** in response to the "possible product option(s)" prompt and press <RETURN>.

5. If you selected SNA, type the corresponding number of the protocol level in response to the "Select protocol level" prompt and press <RETURN>.

6. Type the number of data bytes per log entry (40 to 600) in response to the "Amount of data bytes to record" prompt and press <RETURN>.

7. Type the maximum number of entries to be included in each log file (100 - 200) in response to the "Maximum number of entries" prompt and press <RETURN>.

8. Type a comment about the log file in response to the "Log file comment prompt" and press <RETURN>.

9. If you selected SNA, type **Y** or **N** in response to the "Include Statistics in log?" prompt and press <RETURN>.

10. Type the number of the display format for the log file in response to the "Specify display format" prompt and press <RETURN>.

11. Type the corresponding number of the port you want to select in response to the "Choose RS232C port to monitor" prompt and press <RETURN>.

12. Type the name of the log file in response to the "Log name:" prompt and press <RETURN>.

13. Type **Y** and press <RETURN> in response to the "Backup log automatically?" prompt if you want to enable auto-logging. Type **N** and press <RETURN> if you do not want to enable auto-logging.

    If you typed **N**, you can enable auto-logging later without changing the other monitoring profile parameters. However, to stop auto-logging once it is enabled, you must use the **Set Monitoring Profile** command.

14. If you have enabled auto-logging in step 13, type the name of the remote directory in response to the "Remote Directory:" prompt and press <RETURN>.

15. If auto-logging is enabled, type the maximum number of logs to be stored in the remote directory in response to the "Maximum number of logs stored" prompt and press <RETURN>.

16. If auto-logging is enabled, type a number to represent the frequency of log storage in response to the "Store every Nth log" prompt and press <RETURN>.

17. Type **Y** and press <RETURN> in response to the "Confirm this monitoring profile" prompt if you want to keep the information you have entered. If you type **N**, the command is canceled and the monitoring profile is not changed. To correct errors, type **N** and repeat the **Set Monitoring Profile** command.

Note: Logging functions stop when the parameters are changed. Use the **Start Logging** command to start logging again.

```
CMS!Set Monitoring ProfileRETURN
    Select protocol to be monitored
    1  SNA
    2  X.25
    3  RS232C
    Enter choice number: 1RETURN
    Possible product option(s)
    1  3270
    Enter choice number: 1RETURN
    Select protocol level
    1  SDLC
    2  Path Control (LU & PU)
    3  Path Control (PU ONLY)
    4  ALL
    Enter choice number: 2RETURN
    Amount of data bytes to record per log entry (40..600): 600RETURN
    Maximum number of entries in log file (100..200): 200RETURN
    Log file comment  This is a sample log fileRETURN
    Include Statistics in log? (Y/N): YRETURN
    Specify display format
1  HEX
    Enter choice number: 1RETURN
    Choose RS232C port to monitor
    1  SNAPort1
    Enter choice number: 1RETURN
    Log name: OurCMS1RETURN
    Backup log automatically? (Y/N): YRETURN
    Remote Directory: (FileService1:OurDomain:OurOrg)/ComLogsRETURN
    Maximum number of logs stored remotely (1..100): 100RETURN
    Store every Nth log (1..10): 1RETURN
    Confirm this monitoring profile (Y/N): YRETURN
Monitoring profile set
```

Procedure B: Changing the protocol

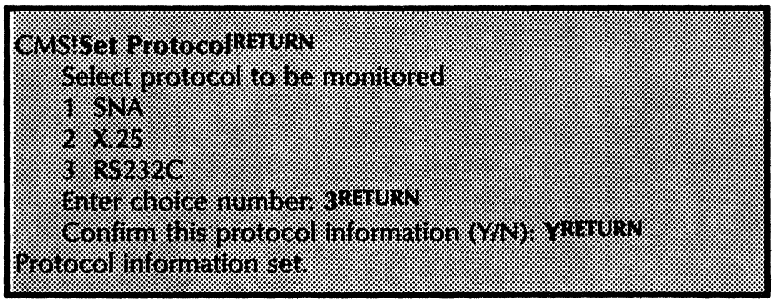
1. Log on and enable in the Communications Monitoring Service context.

2. Type **Set Protocol** and press <RETURN>.

3. Type **1**, **2**, or **3** in response to the "Select protocol to be monitored" prompt and press <RETURN>.

   When you change the protocol from RS-232C to either X.25 or SNA, the display format is automatically set to HEX.

4. Type **Y** and press <RETURN> in response to the "Confirm this protocol information" prompt to keep the information you entered. If you type **N**, the command is canceled and the protocol information in the monitoring profile is not changed. To correct errors, type **N** and repeat the **Set Protocol** command.



```
CMS!Set ProtocolRETURN
    Select protocol to be monitored
    1  SNA
    2  X.25
    3  RS232C
    Enter choice number: 3RETURN
    Confirm this protocol information (Y/N): YRETURN
Protocol information set.
```

Note: Logging functions stop when the protocols are changed. Use the **Start Logging** command to start logging again.

Procedure C: Changing log attributes

1. Log on and enable in the Communications Monitoring Service context.

2. Type **Set Log Attributes** and press <RETURN>.

3. Type the number of data bytes you want to record for each log entry in response to the "Amount of data bytes to record" prompt and press <RETURN>.

4. Type the maximum number of entries for each log file in response to the "Maximum number of entries" prompt and press <RETURN>.

5. Type a comment for the log file in response to the "Log file comment:" prompt and press <RETURN>.

6. Type the corresponding number of the display format in response to the "Specify display format" prompt and press <RETURN>.

7. Type the corresponding number of the port you want to monitor in response to the "Choose RS232C port to monitor" prompt and press <RETURN>.

8. Type **Y** and press <RETURN> in response to the "Confirm these log attributes" prompt to keep the information you just entered. If you type **N**, the command is canceled and the profile information in the monitoring profile is not changed. To correct errors, type **N** and repeat the **Set Profile** command.

Note: Logging functions stop when the log attributes are changed. Use the **Start Logging** command to start logging again.

```
CMS! Set Log AttributesRETURN
    Amount of data bytes to record per log entry (40..600):  600RETURN
    Maximum number of entries in log file (100..200):  200RETURN
    Log file comment: This is a sample RS232C logRETURN
    Specify display format
    1 HEX
    2 OCTAL
    3 ASCII
    4 EBCDIC
    Enter choice number: 4RETURN
    Choose RS232C port to monitor
    1 RS232CPort1
    2 RS232CPort2
    Enter choice number: 1RETURN
    Confirm these log attributes (Y/N): YRETURN
Log attributes set.
```

Procedure D: Changing the log name

1. Log on and enable in the Communications Monitoring Service context.

2. Type **Set Log Name** and press <RETURN>.

3. Type the the new log name in response to the "Log Name:" prompt and press <RETURN>.

```
CMS!Set Log NameRETURN
    Log name: OurCMS1RETURN
Log name set.
```

Note: Logging functions stop when the log name is changed. Use the **Start Logging** command to start logging again.

Procedure E: Changing remote log handling

1. Log on and enable in the Communications Monitoring Service context.

2. Type **Set Remote Log Handling** and press <RETURN>.

3. Type the name of the remote directory in response to the "Remote Directory:" prompt and press <RETURN>. (You must either fully qualify the File Service name or provide a terminating colon.)

4. Type the maximum number of logs you want to store in response to the "Maximum number of logs" prompt and press <RETURN>.

5. Type a number to represent how often a log will be stored in response to the "Store every Nth log" prompt and press <RETURN>.

6. Type **Y** and press <RETURN> in response to the "Confirm this log handling information" prompt to keep the information just entered. If you type **N**, the command is canceled and the log handling information in the monitoring profile is not changed. To correct errors, type **N** and repeat the **Set Remote Log Handling** command.

```
CMS!Set Remote Log HandlingRETURN
    Remote Directory: (FileService2:OurDomain:OurOrg)ComLogsRETURN
    Maximum number of logs stored remotely (1..100): 100RETURN
    Store every Nth log (1..10): 1RETURN
    Confirm this log handling information (Y/N): YRETURN
CMS: Remote Log Directory set to: (FileService2:OurDomain:OurOrg)ComLogs
at (18-Sep-85 17:08:04)
```

Note: Logging functions stop when remote log handling is changed. Use the **Start Logging** command to start logging again.

Renaming the Communications Monitoring Service

You can rename the Communications Monitoring Service using the **Rename Communications Monitoring Service** command.

Procedure

1. Log on and enable in the Communciations Monitoring Service context.

2. Type **Stop Communications Monitoring Service** and press <RETURN>.

3. Type **Rename Communications Monitoring Service** and press <RETURN>.

4. Type the new name in response to the "Enter service name:" prompt and press <RETURN>.

5. Type a description of the service in response to the "Enter service description:" prompt and press <RETURN>.

6. Type **Y** and press <RETURN> in response to the "Confirm" prompt to keep the name just entered. If you type **N**, the command is canceled, and the name is not changed. To correct errors, type **N** and repeat the **Rename Communications Monitoring Service** command.

7. Type **Start Communications Monitoring Service** and press <RETURN>.

```
CMS!Rename Communications Monitoring ServiceRETURN
 Deleting Clearinghouse entry for: OurCMS:OurDomain:OurOrg
 Done
 Service name and description unknown
  Enter service name: NewCMSRETURN
  Enter service description: Com monitor for OurServer RETURN
 Confirm (Y/N): YRETURN
 Validating Clearinghouse entry for: NewCMS:OurDomain:OurOrg
 A new Clearinghouse entry was created
 Done
CMS!Start Communications Monitoring ServiceRETURN
CMS: Communications Monitoring Services is running
CMS: Communications Monitoring Service is started
```

Removing the Communications Monitoring Service from a server

If you need to remove the Communications Monitoring Service permanently from a server, use the **Expunge Service** command. You will want to remove the service when you are moving it to a new server. When the service is removed, any server resources it has acquired (such as disk space) are returned to the server. The monitoring profile information that is stored in the server profile is not deleted.

Procedure

1. Stop all services currently running on the server.
2. Boot the server that currently supports the Communications Monitoring Service by pressing the B RESET button.
3. Type **N** in response to the "Normal Startup?" prompt and press <RETURN>.
4. Type the number that corresponds to the "Interrupt before running services" prompt and press <RETURN>.
5. Type **Expunge Service** and press <RETURN>.
6. Type the number that corresponds to the Communications Monitoring Service and press <RETURN>.
7. Boot the server again.
8. Type **Y** in response to the "Normal Startup?" prompt and press <RETURN>.

5. Messages

This chapter contains the error and informational messages that you might come across during the operations of the Communications Monitoring Service. They are listed in alphabetical order. If the probable cause is not obvious, it is given below the message next to the heading: *Probable cause.* If the message is such that action can be taken to resolve the situation, that action is listed next to the heading: *Action.*

If you encounter an error and need more information than is provided in the following list, contact the Network Support Center.

A directory is required for that operation.

Probable cause: A directory does not exist.

Action: Create a directory and try the operation again.

A file by that name already exists in the directory.

Probable cause: There are duplicate file names.

Action: Rename one of the files so that the files have unique names.

Access rights indeterminate.

Probable cause: The File Service is unable to determine the access rights.

Action: Add the Communications Monitoring Service to the access list with the appropriate access rights.

Access rights insufficient.

Probable cause: The operation you are performing requires more access rights.

Action: Add the Communications Monitoring Service to a group with the appropriate access rights to the file drawer in which your remote directory belongs.

Cannot operate on directories in which files are not ordered by name.

Probable cause: The operation you are performing cannot be done on the specified directory.

Action: Determine the cause of the error and correct it.

Cannot perform that operation on a directory.

Probable cause: The operation you are performing cannot be done on the specified directory.

Action: Determine the cause of the error and try again.

Cannot reach Authentication Service.

Probable cause: The Clearinghouse is unable to respond.

Action: Check to see that the Clearinghouse is operational and try again.

Clearinghouse busy.

Probable cause: The Clearinghouse is busy.

Action: Try again later.

Clearinghouse problem.

Probable cause: There is a problem with the Clearinghouse Service.

Action: Check to see that the Clearinghouse is operational. If not, start it and try again.

Clearinghouse unavailable.

Probable cause: The Clearinghouse cannot respond.

Action: Check to see that the Clearinghouse is operational and try again.

CMS: Communications Monitoring Service is running.
CMS: Communications Monitoring Service is started.
CMS: Communcations Monitoring Service run.

Informative messages. No action is required. These messages are displayed when the Communications Monitoring Service starts successfully.

Communications Monitoring Service is stopped.
Communications Monitoring Service is stoppping.

Informative messages. No action is required. These two messages are displayed when you enter the **Stop Communications Monitoring Service** command.

Completing outstanding file operation...Done.

Informative message indicating that a file operation that was in progress is completed before the requested operation is performed. No action is required.

Deleting name...Done.

Informative message confirms that the Communications Monitoring Service has been deleted with the **Expunge Service** command. No action is required.

File damaged.

Probable cause: The file you are accessing has been damaged.

Action: If the file has been backed up, restore that copy and try again.

File in use.

Probable cause: The file you are trying to access is currently in use.

Action: Try the operation again later.

<file name + time-stamp>... stored.

Informative message displayed when auto-logging stores the local log file to the Remote Directory. No action is required.

File not found.

Probable cause: The File System cannot find the file you are trying to access.

Action: Check to see that you have typed the correct name and try again.

Illegal domain name.

Probable cause: The domain you have specified in the three-part name is incorrect.

Action: Check to make sure you have spelled the name correctly and that it conforms to the rules for domain names; then try again.

Illegal file name specified.

Probable cause: The file name is syntactically incorrect.

Action: Specify the file name correctly.

Illegal local name.

Probable cause: The local name you have specified is incorrect.

Action: Check to see that you have typed the name correctly and that it conforms to the rules for local names; then try again.

Illegal organization name.

Probable cause: The organization you have specified in the three-part name is incorrect.

Action: Check to see that you have typed the name correctly and that it conforms to the rules for organization names; then try again.

Illegal pathname specified.

Probable cause: You have specified an incorrect path name.

Action: Specify the correct path name.

Illegal service name specified.

Probable cause: The service name you have typed is incorrect.

Action: Type the correct name of the service.

Illegal version number specified.

Probable cause: The version number specified is incorrect.

Action: Enter the correct version number.

Insufficient access for Clearinghouse operation.

Probable cause: The operation you are trying to perform requires System Administrator access.

Action: Have someone with the proper authority give you System Administrator access, or have someone with System Administrator access perform the operation.

Invalid name and password.

Probable cause: The name and password you entered are not known to the Clearinghouse.

Action: Check to see that you have typed the correct name and password, and try again.

Log # < > started at < >.

Informative message displayed when you start the logging process using the **Start logging** command. No action is required.

Log attributes set.

Informative message confirms that the values you have entered with the **Set Log Attributes** command have been accepted by the Communciations Monitoring Service. No action is required.

Log Name Set.

Informative message displayed when you use the **Set Log Name** command and confirms the new log name. No action is required.

Logging Stopped.

Informative message displayed when you use the **Stop Logging** command and confirms that the logging process has stopped. No action is required.

Monitoring profile information may not be changed at this time until outstanding file operation completes.

Informative message indicating that any file operations in progress are completed before modifying monitoring information when profile management commands are executed. No action is required.

Monitoring Profile Set.

Informative message displayed when you define the monitoring profile parameters using the **Set Monitoring Profile** command. The values you have defined are accepted by the service. No action is required.

Name not found in that domain.

Probable cause: The name you have typed is not in the domain you have specified.

Action: Check to see that you have entered the correct name and try again.

No attempt to perform remote filing operation.

Probable cause: A filing error occurred when the local log file was being created, so no attempt was made to copy the local log file to the remote directory.

Action: Determine the cause of the error that occurred with the local log file and correct it.

No clearinghouse available.

Probable cause: The Clearinghouse is not operational or does not yet exist.

Action: Make the Clearinghouse operational and try again.

No file was specified.

Probable cause: The operation you are trying requires a file name.

Action: Specify a file name.

No RS232C ports configured.
Logging NOT started.

Probable cause: No RS-232C ports were found.

Action: Check to see if the port has been deleted. The RS-232C port has been reset to the default (local port) in the monitoring profile.

No such domain.

Probable cause: The domain you have specified is not registered in the Clearinghouse.

Action: Try again and specify a registered domain.

No such organization.

Probable cause: The organization you have specified is not registered in the Clearinghouse.

Action: Try again and specify a registered organization.

Page allocation exceeded.
Volume full.

Probable cause: Inadequate space on the volume causes the Filing Threshold Reached parameter in the monitoring profile to be set.

Action: Delete files or use a remote directory on another volume. Remember to reset the filing threshold and the remote directory (if changed) using either the **Set Monitoring Profile** or **Set Remote Log Handling** command.

Problem with communication medium.

Probable cause: There is a cabling or hardware problem.

Action: Fix the hardware and try again.

Problems encountered with RS232C software, monitoring not started.

Probable cause: The RS-232C software is not loaded properly.

Action: Re-load the Communication Service software and try again.

Profile ERROR found in <Line Number> entry. No RS232C ports configured. Add RS232C port before starting logging.

Probable cause: A problem was encounterd with the line number entry in the monitoring profile, and no RS-232C ports were found.

Action: You must add an RS-232C port before you start logging operations, or the **Start Logging** command will also fail.

Profile ERROR found in <Line Number> entry. No RS232C ports configured. Illegal line number specified. Default line number being used.

Probable cause: The RS-232C port you specified in the monitoring profile does not exist. The Communications Monitoring Service will use the default RS-232C port (the server's local port).

Action: Use the **Set Monitoring Profile** or **Set Log Attributes** command, and specify an RS-232C port that does exist.

Profile ERROR found in Remote Directory...auto logging disabled.

Probable cause: A problem was encountered with the Remote Directory parameter when the File Service was accessed. The Communications Monitoring Service may not have the required access to the remote directory. All remote log handling values have been reset and auto-logging has been disabled.

Action: Add the Communications Monitoring Service to the remote file drawer's access list, then use the **Set Monitoring Profile** command to set the monitoring profile again. In addition, check to see that the File Service specified in the monitoring profile exists.

Protocol information set.

Informative message is displayed when you select a protocol using the **Set Protocol** command and confirms that the Communications Monitoring Service has accepted the protocol you selected. No action is required.

Remote directory not set.

Probable cause: Auto-logging is enabled, but no remote directory was specified.

Action: Disable auto-logging or specify a remote directory.

RS232C monitoring not available for this service.

Probable cause: The Internetwork Routing Service cannot be monitored at the RS-232C level.

Action: Monitor the Internetwork Routing Service using X.25 monitoring. You cannot monitor an Internetwork Routing Service that does use X.25.

RS232C monitoring stopped at <time stamp>.
RS232C monitoring restarted at <time stamp>.
RS232C monitoring restart failed at <time stamp>.

Probable cause: These messages appear when dial-up lines are disconnected.

Action: Re-establish the communication link. When the link is re-established, the service will make an attempt to restart monitoring.

RS232C software not loaded.

Probable cause: The software required to perform the particular type of monitoring was not loaded properly.

Action: Re-load the necessary software and try again.

Server being accessed not configured compatible software.

Probable cause: The server at which you are performing an operation does not have the necessary software configured, or has an incompatible version of the software.

Action: Add the software to the server (if it is not there), or update it to the current version before trying the operation again.

Server is busy.

Probable cause: The server is busy.

Action: Try the operation again.

Server not responding.

Probable cause: The server is not working.

Action: Check to see that the server is operational, and if so, try again.

SNA monitoring not available for this service.

Probable cause: The RS-232C port configuration does not correspond to the type of monitoring requested.

Action: Change the protocol selection to correspond to the configuration of the RS-232C port.

SNA software not loaded.

Probable cause: The software required to perform the particular type of monitoring was not loaded properly.

Action: Re-load the necessary software and try again.

Stronger credentials required.

Probable cause: The operation you are trying to perform requires System Administrator access.

Action: Have someone with the appropriate authority assign you System Administrator access.

That file may not be inserted into the specified directory.

Probable cause: The directory is full.

Action: Delete files from the directory that is full, or use another directory.

That operation is illegal for remote files.

Probable cause: The operation you are trying to perform is not allowed for remote files.

Action: Do not perform that operation on a remote file.

That service is not registered correctly.

Probable cause: The service you are trying to use has not been correctly registered in the Clearinghouse.

Action: See the documentation for that service and register the service with the Clearinghouse.

The Authentication Service is busy.

Probable cause: The authentication service cannot respond at this time.

Action: Try again later.

The clearinghouse became unavailable during the operation.

Probable cause: The Clearinghouse crashed.

Action: Fix the Clearinghouse Service and try the operation again.

Transfer aborted.

Probable cause: The entire file cannot be transferred to the File Service, possibly due to lack of space.

Action: If the problem is due to lack of space, create more space and try again.

Unexpected authentication problem.

Probable cause: The authentication service has encountered an unexpected problem.

Action: Try again later. If the problem persists see your Network System Analyst for help.

X25 monitoring not available for this service.

Probable cause: The RS-232C port configuration does not correspond to the type of monitoring requested.

Action: Change the protocol selection to correspond to the configuration of the RS-232C port.

X25 software not loaded.

Probable cause: The software required to perform the particular type of monitoring was not loaded properly.

Action: Re-load the necessary software and try again.

Glossary

American Standard Code for Information Interchange *(ASCII)* A digital code set which represents each character of the standard typewriter keyboard as a 7-bit digital code. It is used for information interchange among data processing systems, data communication systems, and associated equipment.

Auto-logging A process that automatically copies the local log file to a File Service. Auto-logging is enabled in the monitoring profile and started with the **Start Logging** command.

Current log file The working log file to which captured data is written during logging. If logging is stopped, the current log file is the working log file to which data was last written. When logging is started again, the other working log file will become the current log file. The current log file is said to be active during logging and not active if logging is stopped.

Extended Binary Coded Decimal Interchange Code *(EBCDIC)* An eight-bit code used for data communication.

High-Level Data Link Control *(HDLC)* The functional layer within the X.25 protocol that controls the flow of data on a communication line.

Local log file A copy of the last full working log file stored in the working directory of the server where the Communications Monitoring Service resides. The local log file is overwritten each time a working log file is copied to it.

Logical Unit *(LU)* A Network Addressable Unit within SNA through which an end-user process can access the network.

Monitoring profile The set of parameters that describes the monitoring and logging to be performed. The monitoring profile is stored in the Communications Monitoring Service section of the server's profile.

Path control The functional layer within SNA that controls the routing of messages.

Physical Unit *(PU)* A Network Addressable Unit within SNA that provides network administrative services for its node.

Remote log file A copy of the local log file stored in a File Service by auto-logging. A remote log file has the same name as the local log file plus an appended time stamp that ensures a unique name for each remote log file.

RS-232C port An EIA (Electronic Institute of America) specification of a standard electrical interface for the serial transmission of digital data. RS-232C ports are used by a Xerox 8000 Network to communicate with devices not on the network.

Synchronous Data Link Control (*SDLC*) An IBM communications line discipline or protocol associated with SNA.

System Network Architecture (*SNA*) The logical structure, formats, and protocols of operation sequences for transmitting information units through the communication system. Developed by IBM for distributed processing networks. Used by SDLC. As used in this booklet, SNA refers to the IBM specified protocols used in the different levels of communication in an SNA network.

Working directory The directory in the file system of the server where files can be stored for access by the Network Administrator.

Working log file An array of log entries in virtual memory which contains data captured from the communication line being monitored. There are two working log files.

X.25 circutis An international standard protocol that defines an interface between data terminal equipment and data circuit terminating equipment (DCE) for terminals operating in the packet mode on public data networks. The X.25 link between an Internetwork Routing Service and a public data network is an RS-232C leased line supplied by the network vendor. X.25 is structured to allow the multiplexing of many virtual circuits over a single physical link.

A. Forms

This section contains forms for setting up your Communications Monitoring Service. You may copy these forms and fill them out as required. It is important to update the forms with service and network configuration changes as they occur.

- CMS Form 1. SNA Monitoring
- CMS Form 2. X.25 Monitoring
- CMS Form 3. RS232C Monitoring

(This page intentionally blank)

B. Troubleshooting

This appendix provides the following procedures for using the Communications Monitoring Service to diagnose communications problems.

- General diagnostic procedures - provides an overview of using the Communications Monitoring Service in troubleshooting communication problems.

- SNA troubleshooting - provides specific information for troubleshooting SNA communications.

- Getting help from Xerox - provides information on what to do before requesting help from Xerox.

General diagnostic procedures

To diagnose problems in communicating with remote devices over RS-232C ports, use this procedure.

1. Check the hardware at each end for malfunctions.

2. Check that the communication parameters match at each end.

3. Check that application parameters match at each end.

Each step is discussed below.

Checking Hardware

First, check that the hardware involved in the communication is working correctly. This includes checking the processors, ports, and modems at each end of the communication. Also check that the communication line between the two ends is working.

If a hardware problem is discovered, correct the problem and try the communication again. If the communication still fails after the hardware has been checked and proven to work correctly, continue with the next step.

Checking communication parameters

In order for two devices to communicate using RS-232C ports, the parameters that control the transmission of data over the line must agree at each end. These parameters include the baud rate, parity, and other information. You can use the External Communication Service **Describe RS232C Port** command to see the values of these parameters for a port managed by an External Communication Service on your network. Consult the documentation supplied with the other device for instructions on checking the value of its parameters.

If the parameters at both ends do not agree, you must change the values at one end or both so that they do agree. After making any changes, try the communications again. If the parameters agree at both ends and the problem still occurs, continue with the next step.

Checking application parameters

In order for an application to work, the application software at each end must be compatible and its parameters must agree at each end.

Check that both ends are using compatible versions of the software. Consult the software documentation for information on compatibility.

Check that the application's parameters agree at each end. The actual parameters vary according to the communication protocol and the specific application. Consult the documentation supplied with the application for specific information. Information specific to SNA is supplied later in this appendix.

You can use the Communications Monitoring Service to log the communication and capture the data. With a knowledge of the appropriate protocol, you can interpret the data to determine the values of the parameters. In the case of SNA, the Communications Monitoring Service's statistics interpret the BIND application parameters for you and present the information in an easy to use format.

SNA troubleshooting

The following provides information specific to troubleshooting SNA communication problems. To use this information requires some knowledge of the IBM environment with which you want to communicate. If you do not have this knowledge, you will need the assistance of someone who does, typically a communications analyst at the IBM host operation.

IBM communication configuration

In an IBM mainframe environment, the communication and application (BIND) parameters are set in a front-end communication processor with the sys-gen (system generation) procedure. To compare parameters, you need a sys-gen listing. To change the parameters on the IBM side, you need to perform the sys-gen procedure again.

Communication parameters

There are two groups of communication parameters. On the IBM side, the groups are the VTAM Line Definition and the PU Definition. On the Xerox side, the groups are the RS-232C Port Entry, which corresponds to the VTAM Line Definition, and the IBM 3270 Host Entry, which corresponds to the PU definition.

To compare the parameters from each side, compare the VTAM Line and PU Definitions from the sys-gen with the output of the External Communication Service's **Describe RS232C Port** command. The parameters on each side must agree except as noted below.

On the IBM side, many numeric parameters are specified in hexadecimal, for example ADDR and IDNUM in the PU definition. On the Xerox side, all numeric parameters are specified in decimal. Problems will occur if the incorrect notation is used or the values are not correctly converted between the two number systems.

If the Xerox server is on a multi-drop line, the Duplexity parameter in the RS-232C Port Entry must be set to half regardless of the setting of the Duplex parameter in VTAM Line Definition. If the server is not on a multi-drop line, the values of the Duplexity/Duplex parameters must agree.

If the RS-232C port on the Xerox side is not on a multi-port option card, the RS-232C Port Entry Encoding parameter must be "nrz," and the corresponding VTAM Line Definition NRZI parameter must be "NO." Only ports on the multi-port option card can support Encoding set to "nrzi" and NRZI set to "YES."

BIND Parameters

The SNA BIND command contains 31 bytes of information that establish the parameters for the host application session. These parameters must be set correctly for Xerox software to communicate with the IBM host successfully.

The values of the BIND parameters required by Xerox software are listed below. The format of the parameters is the format of the SNA statistics collected by the Communications Monitoring Service. The required values are in bold. For MyMaxRUSize and PLUMaxRUSize, the values given are the maximum allowed; smaller values are acceptable. All numbers are in hexadecimal.

BIND PARAMETERS Bind Type = **01** FM Profile = **03** Ts Profile = **03**

PLU Protocol: ChainingUse = **01** RequestMode = **00** ChainResp = 03
Compression = **00** EB Sender = **01** SLU

Protocol: ChainingUse = **01** RequestMode = **00** ChainResp = 01
Compression = **00** EB Sender = **00**
Xchg FM Hdr = **00** Use Brkting = **01** Brkt Term = **01** Code Set = **00**
SendRcvMode = **02**
Error Rcvry = **00** PLU 1stSpkr = **00** CntentLoser = **00** MyPaceCount = 00 PLU PaceCnt = 01
MyMaxRUSize = **88** PLUMaxRUSize = **F8** PrimSndPace = 00 PrimRcvPace = 00 Data Stream = **02**
DefaultRows = **18** DefaultCols = **50** Alt Rows = **18** Alt Cols = **50** Size = 7F

You can examine the BIND parameters using the Communications Monitoring Service. The parameters can be seen with the **Show Statistics** command, or by including the statistics in the log files. If the BIND parameters are not those required by the Xerox software, the parameters must be changed at the front-end communication processor on the IBM host by performing another sys-gen.

Getting help from Xerox

If you require assistance from Xerox, you should do the following:

1. Document the problem as completely as possible. Note the software, including version numbers, and hardware involved in the problem. Also note the values of the communication parameters at each end of the communication. Use a Xerox Problem Report form to record the information.

2. Try to duplicate the problem. It is very difficult to diagnose a problem without seeing it. Be certain that you can duplicate the problem on request. If you cannot duplicate the problem, attempt to determine under what conditions the problem does occur. For example, does the problem always occur at a particular time of day?

3. Using the Communications Monitoring Service, create log files of the problem communication. This requires that you duplicate the problem while the Communications Monitoring Service is monitoring the appropriate RS-232C port. Use auto-logging to save the log files of the problem communication.

4. Contact your Xerox System Analyst and request assistance. Be prepared to duplicate the problem and to supply log files of the problem in a machine-readable form. You can send the log files to Xerox electronically (by using the Remote Batch Service, for example) or on a floppy disk. A hard copy of the log files is of very limited use in duplicating the problem at Xerox and should be sent as a last resort only.

C. Sample log files

This appendix provides sample log files for SNA, X.25, and RS-232C monitoring. In addition, a sample log banner is provided with a brief explanation of each banner line.

All local and remote log files contain a banner at the beginning of the file that contains basic information about the log file to which it belongs. The following is a sample banner from a log file that monitored SNA at the Path Control level for LU and PU.

```
Series 8000 Network Services Executive.  Version 10.0e
Rome-CMS:AlphaService-PA:Xerox SNA/3270/Path Control (LU & PU) monitor log of:
    Server Name: Rome:AlphaServices-PA:Xerox
    Network:0-667,Processor: 2-852-131-949
    Hardware: 8000 Processor,Memory: 992 KBytes
    Network  Administrator: Michalene M. Casey:AlphaServices-PA:Xerox
Filed on: (London-FS:)Scratch/TheRightStuff18-Sep-85 16:19:50
A Fabulous Dispatcher level SNA log via CMS

Data Collected from RS232C LocalPort RomeLocalPort,Line  # 0
```

The above banner, as with all banners, provides the following information about its log file in the order given below.

- The version of the Network Services Executive running on the server
- The name of the Communications Monitoring Service and the type of monitoring performed. In the case of SNA monitoring, the product type and protocol level are also included
- The server name
- The network and processor numbers
- The hardware configuration of the server: processor type and amount of memory
- The name of the System Administrator who set the Monitoring Profile
- The name of the File Service, file drawer, and file
- The comment entered in the monitoring profile
- The RS-232C port that was monitored

The information that follows a banner is protocol-specific. Interpretation depends on the type of monitoring. A sample log file for each type of monitoring follows.

Sample Log #1 - SNA with Path Control LU and PU

This is an example log of SNA monitoring at the Path Control level for LU and PU. Statistics were included in the log, and the first user session has the BIND parameters recorded.

```
Series 8000 Network Services Executive. Version 10.0eRome-CMS:AlphaService-PA:Xerox
SNA/3270/Path Control (LU & PU) monitor log of:
    Server Name: Rome:AlphaServices-PA:Xerox
    Network:0-667,Processor: 2-852-131-949
    Hardware: 8000 Processor,Memory: 992 KBytes
    Network Administrator: Michalene M. Casey:AlphaServices- PA:Xerox
Filed on: (London-FS:)Scratch/TheRightStuff18-Sep-85 16:19:50
A Fabulous Dispatcher level SNA log via CMS

Data Collected from RS232C LocalPort RomeLocalPort,Line #0

[T + 2440334 mSec] Dispatcher Put[length = 15] fid2, Normal, Only,DAF = 0, OAF = 2,
SNF = 02 Request, FMData, NoFmH, NoSDI, BCI, ECI,DR1, NoDR2, NoERI, ByPass, NoPace,
NoBB, NoEB, NoCD, CS = 0, NoED,NoPad, THP:<2C0000020002>,
RHP:<038000A3A29683>

[T + 1354 mSec] Dispatcher Get[length = 11] fid2, Normal, Only,   DAF = 2, OAF = 0,
SNF = 02 Response, FMData, NoFmH, NoSDI, BCI,ECI, DR1, NoDR2, = RTI, ByPass,
NoPace, NoBB, NoEB, NoCD, CS = 0, NoED, NoPad, THG:<2C0002000002>,
RHG:<838000>

[T = 433 mSec] Dispatcher Get[length = 45] fid2, Expedited, Only,DAF = 2, OAF = 1, ID
= 1DCF REquest, SEssion, FmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, NoPace,
NoBB, NoEB, NoCD, CS = 0,NoEd, NoPad, <BIND>, THG:<2D0002011DCF>,
RHG:<6B800031010303B1903080000188F800002000000000185018507F000005E2C3E3E2
D600>

[T + 6 mSec] Dispatcher Put[length - 12] fid2, Expedited, Only, DAF = 1, OAF = 2, ID =
1DCF Response, Session, FmH, NoSDI, BCI,ECI, DR1, NoDR2, +RTI, ByPass, NoPace, NoBB,
NoEB, NoCD, CS = 0,NoEd, NoPad, <BIND>, THP:<2D0001021DCF>,
RHP:<EB800031>

[T = 837 mSec] Dispatcher Get[length = 12] fid2, Expedited, Only,DAF = 2, OAF =1, ID
= 1DD0 Request, Session, FmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, NoPace,
NoBB, NoEB, NoCD, CS = 0,NoEDS, NoPad, <SDT>, THG:<2D0002011DD0>,
RHG:<6B8000A0>

[T + 7 mSec] Dispatcher  Put[length = 12] fid2, Expedited, Only, DAF = 1, OAF = 2, OD
= 1DD0 Response, Session, FmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, NoPace,
NoBB, NoEB, NoCD, CS = 0,NoED, NoPad, <SDT>, THP:<2D0001021DD0>,
RHP:<EB8000A0>

[T + 2400 mSec] Dispatcher Get[length = 13] fid2, Expedited, Only, DAF = 2, OAF = 1,
ID = 1DD1 Request, Session, FmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, NoPace,
NoBB, NoEB, NoCD, CS = 0, NoED, NoPad, <UNBIND>, THG:<2D0002011DD1>,
RHG:<6B80003202>

[T + 5 mSec] Dispatcher Put[length = 12] fid2, Expedited, Only, DAF = 1, OAF = 2, ID =
1DD1 Response, Session, FmH, NoSDI, BCI, ECI, DR1, NoDR2,, +RTI, ByPass, NoPace,
NoBB, NoEB, NoCD, CS = 0, NoED, NoPad, <UNBIND>, THP:<2D0001021DD1>,
RHP:<EB800032>[T + 661 mSec] Dispatcher Get[length = 47] fid2, Expedited, Only, DAF
= 2, OAF = 1, ID = 1DD2 Request, Session FmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI,
```

ByPass, NoPace, NoBB, NoEB, NoCD, CS = 0, NoED, NoPad, <BIND>, THG:<2D0002011DD2>, RHG:<6B800031010303B190308000188F80000200000000000185018507F000007E2C3E3E2D6F0F200>

[T + 8 mSec] Dispatcher Put[length = 12] fid2, Expedited, Only, DAF = 1, OAF = 2, ID = 1DD2 Response, Session, FmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, NoPace, NoBB, NoEB, NoCD, CS = 0, noED, NoPad, <BIND>, THP:<2D0001021DD2>, RHP:<EB800031>

[T + 900 mSec] Dispatcher Get[length = 12] fid2, Expedited, Only,DAF = 2, OAF = 1, ID = 1DD3 Request, Session, FmH, NoSDI, BCI, ECI, DR1, NoDR@, NoERI, ByPass, NoPace, NoBB, NoEB, NoCD, CS = 0, NoED, NoPad, <SDT>, THG:<2D0002011DD3S>, RHG:<6B8000A0>

[T + 5 mSec] Dispatcher Put[length + 12] fid2, Expedited, Only, DAF = 1, OAF = 2, ID = 1DD3 Response, Session, FmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, NoPace, NoBB, NoEB, NoCD, CS = 0, NoED, NoPad, <SDT>, THP:<2D0001021DD3>, RHP:<EB8000A0>

[T + 2814 mSec] Dispatcher Get[length = 22] fid2, Normatl, Only, DAF = 2, OAF = 1, SNF = 01 Request, FMData, NoFmH, NoSDI< BCI, ECI, DR1, NoDR2, NoERI, ByPass, Pace, BB, NoEB, NoCD, CS = 0, NoED, NoPad, THG:<2C0002010001>, RHG:<038180F5C1115D7F1D4011404013>

[T + 22 mSec] Dispatcher Put[length + 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF = 01 Response, FMData, NoFmH, NoSSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, BB, NoEB, NoCD, CS = 0, NoED, NoPad, THP:<2C0001020001>, RHP:<838180>

[T + 1226 mSec] Dispatcher Get[length = 23] fid2, Normal, Only, DAF = 2, OAF = 1, SNF = 02 Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, Pace, NoBB, NoEB, NoCD, CS = 0, NoED, NoPad, THG:<2C0002010002>, RHG:<038100F1C11140403C4040001DC813>

[T + 15 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF= 1, OAF = 2, SNF = 02 Response, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB, NoEB, NoCD, CS = 0, NoED, NoPad, THP:<2C0001020002>, RHP:<838100>

[T + 1031 mSec] Dispatcher Get[length = 54] fid2, Normal, Only, DAF = 2, OAF = 1, SNF = 03 Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, Pace, NoBB, NoEB, NoCD, CS = 0,NoED, NoPad, THG:<2C0002010003>, RHG:<038100F1C31140401DE8C1C3C6F8F2F0F0F34040C1C3C6F26B40C5D5E3C5D940D3D6C7D6D540C9C44060401DC413>

[T + 10 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF = 03 Response, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB, NoEB, NoCD, CS = 0. NoED, NoPad, THP:<2C0001020003>, RHP:<838100>[T + 1458 mSec] Dispatcher Get[length = 13] fid2, Normal, Only, DAF = 2, OAF = 1, SNF = 04 Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, Pace, NoBB, NoEB, CD, CS = 0, NoED, NoPad, THG:<2C0002010004>, RHG:<038120F1C2>

[T + 15 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF = 04 Response, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB, NoEB, CD, CS = 0, NoED, NoPad, THP:<2C0001020004>, RHP:<838120>

[T + 4916 mSec] Dispatcher Put[length = 24] fid2, Normal, Only, DAF = 1, OAF = 2, SNF = 01 Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, ERI, ByPass, NoPace, NoBB, NoEB, CD, CS = 0, NoEDS, NoPad, THP:<2C0001020001>, RHP:<0390207D406A1140E383F3F4F8F29483>

[T + 929 mSec] Dispatcher Get[length = 54] fid2, Normal, Only, DAF = 2, OAF = 1, SNF= 05 Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, sNoDR2, NoERI, ByPass, Pace, NoBB, NoEB, NoCD, CS = 0, NoED, NoPad, THG:<2C0002010005>,

```
RHG:<038100F1C311C1501DE8C1C3C6F8F2F0F0F44040C1C3C6F26B40C5D5E3C5D940D7
C1E2E2E6D6D9C44060401DCC13>

[T + 16 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF =
05 Response, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB,
NoEB, NoCD, CS = 0, NoED, NoPad, THP:<2C0001020005>, RHP:<838100>

[T + 435 mSec] Dispatcher Get[length = 13] fid2, Normal, Only, DAF = 2, OAF = 1, SNF
= 06 Request, FMData, NoFmH, NoSSDI, BCI, ECI, DR1, NoDRe2, NoERI, ByPass, Pace,
NoBB, NoEB, CD, CS = 0, NoED, NoPad, THG:<2C0002010006>, RHG:<038120F1C2>

[T + 15 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF =
06 Response, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB,
NoEB, CD, CS = 0, NoED, sNoPad, THP:<2C0001020006>, RHP:<838120>

[T + 1287 mSec] Dispatcher Put[length = 20] fid2, Normal, Only, DAF = 1, OAF = 2, SNF
= 02 Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, ERI, ByPass, NoPace, NoBB,
NoEB, CD, CS = 0, NoED, NoPad, THP:<2C0001020002>,
RHP:<0390207DC1F611C1F3949483>

[T + 1479 mSec] Dispatcher Get[length = 55] fid2, Normal, Only, DAF = 2, OAF = 1, SNF
= 07 REquest, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, Pace, NoBB,
NoEB, NoCD, CS = 0, NoED, NoPad, THG:<2C0002010007>,
RHG:<038100F1C311C2601DE8C1C3C6F8F2F0F0F04040C1C3C6F26B40D3D6C7D6D540C9
D540D7D9D6C7D9C5E2E2401DC413>

[T + 15 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF =
07 Response, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, sPace, NoBB,
NoEB, NoCDS, CS = 0, NoED, NoPad, THP:<2C0001020007>, RHP <838100>[T + 1051
mSec] Dispatcher Get[length = 85] fid2, Normal, Only, DAF = 2, OAF = 1, SNF = 08
Request, FMData, NoFmH, NoSDI, BCI, ECI,DR1, NoDR2, NoERI, ByPass, Pace, NoBB, NoEB,
NoCD, CS = 0, NoED, NoPad, THG:<2C0002010008>,
RHG:<038100F1C3F01DE8C1C3C6F0F1F1F3F740C3F3F4F8F2D4C340D3C1E2E340E2E8E2E3
C5D440C1C3C3C5E2E20F0F94BF4F360F0F361F2F761F8F540C6D9D6D440E4F0F2D9E9F1F1F
01DC413>

[T + 23 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF =
08 Response, FMData, NoFmH, NoSSDI, BCSI, ECI, DR1, NoDR2, +RTI, ByPass, Pace,
NoBB, NoEB, NoCD, CS = 0, NoED, NoPad, THP:<2C0001020008>, RHP:<838100>

[T + 1520 mSec] Dispatcher Get[length = 22] fid2, Normal, Only, DAF = 2, OAF = 1, SNF
= 09 Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, Pace, NoBB,
NoEB, NoCD, CS = 0, NoED, NoPad, THG:<2C002010009>,
RHG:<038100F140115D7F1D4011C54013>

[T + 15 mSec] Dispatcher Put[lenght = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF =
09 Response, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB,
NoEB, NCD, CS = 0, NoED, NoPad, THP:<2C0001020009>, RHP:<838100>

[T + 654 mSec] Dispatcher Get[length = 83] fid2, Normal, Only, DAF = 2, OAF = 1, SNF
= 0A Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass Pace, NoBB,
NoEB, NoCD, CS = 0, NoEDS, NoPad, THG:<2C000201000A>,
RHG:<038100F14011C5401DC8C3F3F4F8F2D4C340D3D6C7D6D540C9D540D7D9D6C7D9
C5E2E240C1E340F1F67AF1F47AF3F540D6D540E2C5Di7E3C5D4C2C5D940F1F86B40F1F9F8F
51D4011C65013>

[T + 15 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF =
0A Response, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB,
NoEB, NoCD, CS = 0, NoED, NoPad, THP:<2C000102000A>, RHP:<838100>

[T + 1073 mSec] Dispatcher Get[length = 87] fid2, Normal, Only, DAF = 2, OAF = 1, SNF
= 0B Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, Pace,
NoBB, NoEB, NoCD, CS = 0, NoED, NoPad, THG:<2C00201000B>,
RHG:<038100F14011C6501DC840E685938396948540A39640D69560D389958540C2A4A289
9585A2A240E2A8A2A38594A2406040E3E2D6618540A49584859940D4E5E261E2D74BF14BF3
4BF41D4011C76013>

[T + 18 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF =
0B Response, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDr2, +RTI, ByPass, Pace, NoBB,
NoEB, NoCD, CS = 0, NoEDS, NoPad, THP:<2C000102000B>, RHP:<838100>

[T + 14805 mSec] Dispatcher Get[length = 33] fid2, Normal, Only, DAF = 2, OAF = 1,
SNF = 0C Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, SPace,
NoBB, NoEb, CD, CS = 0, NoED, NoPad, THG:<2C000201000C>,
RHG:<038120F1C211C7601DC811C761D9C5C1C4E8401D4011C8F013>

[T + 15 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF =
0C Response, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB,
NoEB, CD, CS = 0, NoED, NoPad, THP:<2C000102000C>, RHP:<838120>

[T + 11020 mSec] Dispatcher Put[length = 22] fid2, Normal, Only, DAF = 1, OAF = 2,
SNF = 03 Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, ERI, ByPass, NoPace,
NoBB, NoEB, CD, CS = 0, NoED, NoPad, THP:<2C0001020003>,
RHP:<0390207DC8F511C7E8A2978640F2>

[T + 5270 mSec] Dispatcher Get[length = 220] fid2, Normal, First, DAF = 2, OAF = 1, SNF
= 0D Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, Pace,
NoBB, NoEB, CD, CS = 0, NoED, NoPad, THG:<28000201000D>,
RHG:<038120F1C31140401DF83C405C604040C5C4C9E3406040C5D5E3D9E840D7C1D5C5
D340403CC150601DE8C3D6D4D4C1D5C4407E7E7E6E1DC83CC25F001D601DE83CC3F040
1D60C9E2D7C640D3C9C2D9LC1D9E87A3CC540401D60404040D7D9D6D1C5C3E31DE87E
7E7E6E1DC8C3F3F4F8F2D4C3001D603CC650401D604040D3C9C2D9C1D9E81DE87E7E7E6E
1DC8C6D9D6DrD9C2E2001DE8407E7E7E6E1DC83CC6F8001DE8407E7E7E6E1DC83CC7C70
01DE8407E7E7E6E1DC83CC7D6001D603CC760401D60404040E3E8D7C54040401DE87E7iE7
E6E>

[T + 222 mSec] Dispatcher Get[length = 264] fid2, Normal, Middle, DAF = 2, OAF = 1,
SNF = 0D, THG:<20000201000D>,
<1DC8C1D9C3C800000001D603CC8F0401D60404040D4C5D4C2C5D9401DE87E7Ei7E6E
1DC83CC9C9001D603CC9D1404DC2938195924086969940948594828599 40A285938583A3
899695409389A2A35D3C4A40401D603C4B50401D60D6E3C8C5D940D7C1D9E3C9E3C9D6
D5C5C440D6D940E2C5D8E4C5D5E3C9C1D340C4C1E3C140E2C5E37A3C4C60401D604040
40C4C1E3C140E2C5E340C5C1D4C5401DE87E7E7E6E1DC83C4DF0001D60404040E5D6D3E4
D4C540E2C5D9C9C1D3401DE87E7E7E6E1DC83C4E4E001D60404DC986409596A3408381A
38193968785845D3C4F40401D603C5050401D60C4C1E3C140E2C5E340D7C1E2E2E6D6D9C
41dE87E7E7E6E1D>

[T + 112 mSec] Dispatcher Get[length = 131] fid2, Normal, Last, DAF = 2, OAF = 1, SNF
= 0d, THG:<24000201000D>,
<4C3C50F0001D604DC986409781A2A2A6969984409799 96A38583A38583A385845D3CD16
0401D603CD2F0401D60D7D9D6C6C9D3C540D5C1D4C53CD3C2401DE87E7E7E6E1DC83C
D350001D604DC293819592408485868 1A493A3A240A396408481A38140A285A340A3A8978
55D3CD440401DE83C5B61003C40400011C9C113>

[T + 7 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1 OAF = 2, SNF =
0D Response FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB,
NoEB, CD, CS = 0, NoESD, NoPad, THP:<C000102000D>, RHP:<838120>

[T + 18590 mSec] Dispatcher Put[length = 32] fid2, Normal, Only, DAF = 1, OAF = 2,
SNF = 04 Request, FMData, NoFmH, NoSDI, BCI, ECsI, DR1, NoDR2, ERI, ByPass, NoPace,
NoBB, NoEB, CD, CS = 0, NoED, NoPad, THP:<2C0001020004>,
RHP:<0390207DC7F511C66182A48487838595A311C7F1A385A7A3>

[T + 6155 mSec] Dispatcher Get[length = 220] fid2, Normal, First, DAF = 2, OAF = 1, SNF
= 0E Request, FMData, No;FmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, Pace,
NoBB, NoEB, CD, CS = 0, NoED, NoPad, THG:<28000201000E>,
RHG:<038120F1C31140C1C5C4C9E34060606040C3F3F4F8F2D4C34BC2E4C4C7C3C5D5E3
4BE3C5E7E3403C40F26011407E40C3D6D3E4D4D5E240F0F0F140F0F7F2404011C15E4011C2
4E1DE8E2C3D9D6D3D3407E7E7iE6E1DC8D7C1C7C51D601DC83CC2E75C1D603CC3C55C
40E3D6D740D6C640C4C1E3C1403CC3F05C1D403CC3F6F0F11D403CC37E4011C450D4C1
C7D5C140C3D6D9D7D6D9C1E3C9D6D5403CC540001D403CC5C6F0F21D403CC55C40C2
E4C4C7C5E340C3C5D5E3C5D940D9C5D7D6D9E3404DF0F0F05D403CC650001D403CC6D
6F0F31D40>

[T + 224 mSec] Dispatcher Get[length = 264] fid2, Normal, Middle DAF = 2, OAF = 1,
SNF = 0E, THG:<20000201000E>,
<3CC7D74011C7601D403CC7E6F0F41D403CC77A4011C77FD4C1D5E4C6C1C3E3E4D9C9
D5C740E4D5C9E3403CC8F0001D403CC8F6F0F51D403CC94040F1F9F9F34060604040D1C1
D511C9D1C6C5C23CC9D940D4C1D93CC96140C1D7D93CC9E940D4C1E83CC9F140D1E4
D511C9F9D1E4D3400000001D403C4AC6F0F61D40114B501D403C4BD6F0F71D40D3C1C2D
6D93C4BE840F1F0F5F040404040F1F0F6F740404040F1F0F9F2114C40F1F1F1F8114CC8F1F1F3
F7114C50F1F1F8F2114CD8F1F1F8F2400000001D403C4CE6F0F81D40D7D9D6C6C9E340E2C
8C1D9C9D5C7404040F1F4F13C4DC140F1F4F43C4DC94F1F4F73C4DD140F1F5F13C4DD940
F1F5F33C4D>

[T + 229 mSec] Dispatcher Get[length = 264] fid2, Normal, Middle, DAF = 2, OAF = 1,
SNF = 0E, THG:<20000201000E>,
<6140F1F5F73C4DE940F1F5F7400000001D403C4DF6F0F91D40D7C1E8D9D6D3D340C2E4D
9C4C5D5404040F1F5F73C4ED140F1F6F03C4ED940F1F6F43C4E6140F1F6F8114EE9F1F7F0114
Ef1F1F7F4114EF9F1F7F4400000001D40F0F0F0F0F1F01D40D6E5C5D9C8C5C1C4114F5AF3F31
14FE2F3F3114F6AF3F3114FF2F3F3114F7AF3F31150C2F3F311504AF3F3400000001D40F0F0F0F
0F1F11D40E3D6E3C1D340C3D6D4D74B3C50E840F1F3F8F240404040F1F4F0F440404040F1F
4F3F740404040F1F4F7F040404040F1F4F9F411D150F1F5F4F811D1D8F1F5F4F8400000001D40
F0F0F0F0F1F21D40E4E2C54ED6C3C3E4D7C1D5C3E811D1F9F1F9F211D2C1>

[T + 224 mSec] Dispatcher Get[length = 264] fid2, Normal, Middle, DAF = 2, OAF =1,
SNF = 0E, THG:<20000201000E>,
<F1F9F211D2C9F1F9F211D2D1F2F2F011D2D9F2F1F411D261F2F1F411D2E9F2F1F440000000
1D40F0F0F0F0F1F31D40E3C5D3C5D7C8D6D5C53CD34A40F4F83CD3D240F4F93CD35A40F
4F93CD3E240F4F93CD36A40F5F03CD3F240F5F011D37AF5F0400000001D40F0F0F0F0F1F41D
40E3D9C1E5C5D33CD45A40F8F83CD4E240F9F33CD4E940F1F0F13CD4F140F1F0F23CD4F94
0F1F0F73CD5C140F1F0F73CD5C940F1F1F2400000001D40F0F0F0F0F1F51D40E2E4D7Di7D3
C9C5E23CD56840F53CD5F340F73CD57B40F73CD6C340F73CD64B40F73CD6D340F73CD65
B40F7400000001D40F0F0F0F0F1F61D40D7D9C9D5E361D9C5D7D9D63CD67A40F2F33CD7
C240>

[T + 228 mSec] Dispatcher Get[length = 264] fid2, Normal, Middle, DAF = 2, OAF = 1,
SNF = 0E, THG:<20000201000E>,
<F2F43CD74A40F2F53CD7D240F2F53CD75A40F2F73CD7E240F2F73CD76A40F2F74000000
001D40F0F0F0F0F1F71D40C3D6D5E2E4D3E3C9D5C73CD84A40F2F83CD8D240F3F53CD85
A40F4F43CD8E240F5F33CD86A40F5F33CD8F240F5F73CD87A40F5F8400000001D40F0F0F0F
0F1F81D40C4C5D7D9C5C3C9C1E3C9D6D53CD9D940F1F4F23CD96140F1F4F53CD9E940F1
F4F83CD9F140F1F5F13CD9F940F1F5F43C5AC140F1F5F73C5AC940F1F6F0400000001D40F0F
0F0F0F0F1F91D40C6D9C5C9C7C8E33C5A6B40F33C5AF340F33C5A7B40F33C5BC340F33C5
B4B40F33C5BD340F33C5B5B40F3400000001D4F0F0LF0F0F2F01D40D9C5C3D9E4C9E3C9D5
C73C5B7B>[T + 97 mSec] Dispatcher Get[length = 112] fid2, Normal, Last, DAF = 2, OAF
= 1, SNF = 0E, THG:<24000201000E>,
40F33C5CC340F33C5C4B40F33C5CD340F33C5B40F33C5CE340F33C5C6B40F3400000001D
40F0F0F0F0F2F11D40C4C1E3C140D7D9D6C3C5E2E2C9D5C740404040F33C5DD340F33C5
D5B40F33C5DE340F33C5D6B40F33C5DF340F33C5D7B40F34000000011C15E13>

[T + 7 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1, OAf = 2, SNF =
0E Response, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB,
NoEB, CD, CS = 0, NoED, NoPad, THP:<2C000102000E>, RHP:<838120>

[T + 7654 mSec] Dispatcher Put[length = 19] fid2, Normal, Only DAF = 1, OAF = 2, SNF
= 05 Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, ERI, ByPass, NSoPace,
NoBB, NoEB, CD, CS = 0, NoED, NoPad, THP:<2C0001020005>,
RHP:<03900207DC16011C15E7EA7>

[T + 5978 mSec] Dispatcher Get[length = 38] fid2, Normal, Only, DAF = 2, SOAF = 1,
SNF = 0F Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, Bypass, Pace,
NoBB, NoEB, CD, CS = 0, NoED, NoPad, THG:<2C000201000F>,
RHG:<038120F5C3115D7F1D401140401DC81140C1D9C5C1C4E8401D4011C15013>

[T + 18 mSec] Dispatcher Put[lenght = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF =
0F Response, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB,
NoeB, CD, CS = 0, NoED, NoPad, THP:<2C000102000F>, RHP:<838120>

[T + 3955 mSec] Dispatcher Put[length = 23] fid2, Normal, Only, DAF = 1, OAF = 2, SNF
= 06 Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, ERI, ByPass, NoPace, NoBB,
NoEB, CD, CS = 0, NoED, NoPad, THP:<2C0001020006>,
RHP:<0390207DC1D61140C8939687968686>

[T + 3317 mSec] Dispatchr Get[length = 80] fid2, Normal, Only, DAF = 2, OAF = 1, SNF
= 10 Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, Pace, NoBB,
NoEB, NoCD, CS = 0, NoED, NoPad, THG:<2C0002010010>,
RHG:<038100F1C111C2601DC8C3F3F4F8F2D4C34D3D6C7C7C5C440D6C6C640E3E2D640
C1E340F1F67AF2F57AF5F440D6D540E2C5D940F1F86B40F1F9F8F51D4011C3F013>

[T+ 18mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF =
10 Response, FMData, NoFmH, NoSDI, BCI,ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB,
NoEB, NoCD, CS = 0, NoED, NoPad, THP:<2C0001020010>, RHP:<838100>

[T+ 415 mSec] Dispatcher Get[length = 30] fid2, Normal, Only, DAF = 2, OAF = 1, SNF
= 11 Request, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, Pace, NoBB,
NoEB, NoCD, CS = 0, NoED, NoPad, THG:<2C0002010011>,
RHG:<038100F14011C3F01DC85C5C5C5C5C5C1D4011C54013>

[T + 15 mSec] Dispatcher Put[length = 11] fid2, Normal, Only, DAF = 1, OAF = 2, SNF =
11 REsponse, FMData, NoFmH, NoSDI, BCI, ECI, DR1, NoDR2, +RTI, ByPass, Pace, NoBB,
NoEB, NoCD, CS = 0, NoED, NoPad, THP:<2C0001020011>, RHP:<838100>

[T + 6899 mSEc] Dispatcher Get[length = 12] fid2, Expedited, Only, DAF = 2, OAF = 0,
Id = 1B9A Request, Session, FmH, NoSDI, BCI, ECI, DR1, NoDR2, NoERI, ByPass, NoPace,
NoBB, NoEB, NoCD, CS = 0, NoED, NoPad, <DACTLU>, THG:<2D0002001B9A>,
RHG:<6B80000E>

[T + 5 mSec] Dispatcher Put[length = 12] fid2, Expedited, Only, DAF = 0, OAF = 2, ID =
1B9A Response, SEssion FmH,NoSDI, BCI, ECI, DR1, NoDr2, +RTI, ByPass, NoPace, NoBB,
NoEB, NOCD, CS = 0, NoED, NoPad, <DACTLU>, THP:<2D0000021B9A>,
RHP:<EB80000E>

SNA Stats
Number of active instances: 1

SNA Buffer Stats
BuffersRequested = 138 BuffersAllocated = 14 BuffersAvailable = 4
SndBuffers = 0 RcvBuffers = 138 SndBuffersInUse = 0
RcvBuffersInUse = 9
ClustersAdded = 2 PoolsCreated = 11 AltGets = 123
Enqueues = 124 Dequeues = 124 DequeReturnedNIL = 187
ExtractFromQs = 0 ExtractFrmQRetNIL = 0
GetInputBufferWts = 1 GetInputBufRetNI = 0 GetBufferWaits = 2
GetBufferRetdNIL = 0 CreditRcvBufFaild = 0
Preallocates = 0 SmallGets(0) = 0 FullGets(0) = 0 Spare1 = 0
Spare2 = 0

SNA Driver Stats
PacketsSent = 52 BytesSent = 731 SendLineTimeout = 0
```

```
NoSendPathLineDown = 0 RemoteBusy = 0
PacketsReceived = 62 BytesReceived = 7194 PacketsRejected = 0
ReceiveDataLost = 0 ReceiveDeviceError = 0 ReceiveErrorUnknown = 0
CRCErrors =0
DSRDropped = 0 LinkReset = 1 LinkDown = 0
Retransmissions = 3 BufferSize = 265 Spare1 = 0 Spare2 = 0
Performance = 76

SNA Dispatcher Stats
NumberOfSegments = 46 OnlyInSegment = 35 FirstInSegment = 11
MiddleInSegment = 5 LastInSegment = 11
Negative responses:
InvalidFID (80 06) = 0 IncompleteTH (80 0B) = 0 IncompleteRH (40 05) = 0
TooLongPIU (80 0A) = 0
UnreconizedDest (80 04) = 0 UnrecognizedOrigin (80 0E) = 0
InvalidAdressComb (80 0F) = 0 NAU Inoperative (80 03) = 0
SegmentingError (80 07) = 0 Spare1 = 0 Spare2 = 0

SNA PU Stats
actpu = 1 dacctpu = 0 reqms = 0
+reqmsRes = 0 +recfmsResp = 0 -recfmsResp = 0
Negaive responses:
resoureUnknown (08 06) = 0 procedureNotSupported (08 0C) = 0
functionotSupported (10 03) = 0 parameterNotSupported (10 05) = 0
caegorNotSupported (10 07) = 0 seqNumberError (20 01) = 0
immedReqMdeError (20 0A) = 0 reqWhileWAitingResp (20 0D) = 0
badSCFormat (40 01) = 0 pacingNotSupported (40 08) = 0
chainingNtSupported (40 0B) = 0 bracketsNotSupported (40 0C) = 0
csiNotSupportd (40 10) = 0 badRUCategory (40 11) = 0
badRespReqode (40 12) = 0 badSDIRTI (40 13) = 0
badDRIERI(40 14) = 0 badQRI (40 15) = 0 NAU Inoperative (80 03) = 0
puNotACtie (80 08) = 0
unknownErrr = 0 Spare1 = 0 Spare2 = 0

SNA LU Stats
Controller Name: RomeOBS:AlphaServices-PA:Xerox
Ctlr Addr = 1 Ttal Users = 1 Ctlr Uptime = 45 RejByCtrlr = 0

LUPORT
User Name: ichalene M.sssssCasey:OSBU North:Xerox
SessionTime = 4 SessionDone = F LU Type = 2 Model = 2 RejPortBusy = 0
BIND PARAMETERS Bind Type = 01 FM Profile = 03 TS Profile = 03
PLU Protocol:ChainingUse = 01 RequestMode = 00 ChainResp = 03
Compressio = 00 EB Sender = 01
SLU Protcol: ChainingUse = 01 RequestsMode = 00 ChainResp = 01
Compression = 0 EB Sender = 00
Xchg FMHdr = 00 Use Brkting = 01 Brkt Term = 01 Code Set = 00
SendRcvMode =02
Error Rcvry = 00 PLU 1stSpker = 00 CntentLoser = 00 MyPaceCount = 00
PLUPaceCnt = 01
MyMaxRUSize = 88 PLUMaxRUSiz = F8 PrimSndPace = 00 PrimRcvPasce = 00
DataStream = 02
DefaultRows = 18 DefaultCols = 50 Alt Rows = 18 Alt Cols = 50
Size = 7F

LU PORT 1
No User
SessionTime =1 SessionDone = T LU Type = 2 Model = 2 RejPortBusy = 0

LU PORT 2
No User
SessionTime =44556440 SessionDone = F LU Type = 2 Model = 2 RejPortBusy = 0
```

```
LU PORT 3
No User
SesionTime = 44556440 SessionDone = F LU Type = 2 Model = 2 RejortBusy = 0

LU PORT 4
No user
SessionTime = 44556440 SessionDone = F LU Type = 2 Model = 2 RejPortBusy = 0

LU PORT 5
No user
SesionTime = 44556440 SessionDone = F LU Type = 2 Model = 2 RejortBusy = 0

LU PORT 6
No user
SesionTime = 44556440 SessionDone = F LU Type = 2 Model = 2 RejPortBusy = 0

LU PORT 7
No user
SessionTime = 44556440 SessionDone = F LU Type = 2 Model = 2 RejPortBusy = 0
```

Sample Log #2 - X.25

This is an example log of X.25 monitoring at the HDLC level.

```
Series 8000 Network Services Executive Version 10.0e
Bern-CMS:Alphaservices-pa:Xerox  X.25 monitor log of:
    Server Name: Bern:Alphaservices-pa:Xerox
    Network: 0-667, Processor: 2-852-142-636
    Hardware: 8000 Processor, Memory: 992 KBytes
    Network Administrator: Lawrence S. Kluger:OSBU North:Xerox

Filed on: (UCB:osbu north:)Kluger/CMSMonitoringLog16-Sep-85 19:35:04
The Second X25 log brought to you by the CMS (and Michalene)

Data Collected from RS232C LocalPort Bern-LocalPort, Line #0

[T + 2135084 mSec] HDLC Put[length = 29] <01><I>, N(R)0, N(S)1 -- Q=0 D=0
Channel = 000007
CALLREQ<CC311021300163311041500121060021050706 40FFFFFFFF>
[T + 121 mSec] HDLC Get[length = 2]<01><RR>,N(R)2
[T + 390 mSec] HDLC Get[length = 39]<03><I>, N(R)2, N(S)0 Q=0 D=0
Channel = 000007
CLRINDICATE<0900CC311021300163311041500121120000C10400000001C2080
000000100000002>
[T + 17 mSec] HDLC Put[length = 5] <01><I>, N(R)1, N(S)2 -- Q=0 D=0
Channel = 000007 CLRCFRM
[T + 602 mSec] HDLC Get[length = 2] <01><RR>, N(R)3
[T + 69901 mSec] HDLC Put[length = 29] <01><I>, N(R)1, N(S)3 -- Q=0 D=0
Channel = 000007
CALLREQ<CB440147111163110415000690060021050706 40FFFFFFFF>
[T + 132 mSec] HDLC Get[length = 2] <01><RR>, N(R)4
[T + 2479 mSec] HDLC Get[length = 39] <03><I>, N(R)4, N(S)1 -- Q=0 D=0
Channel = 000007
CLRINDICATE<11C6CB440147111163110415001210120000C10400000003C2080
000000100000002>
[T + 17 mSec] HDLC Put[length = 5] <01><I>, N(R)2, N(S)4 -- Q=0 D=0
Channel = 000007 CLRCFRM
[T + 524 mSec] HDLC Get[length = 2] <01><RR>, N(R)5
[T + 113539 mSec] HDLC Get[length = 31] <03><I>, N(R)5, N(S)2 -- Q=0 D=0
Channel = 000001
INCOMINGCALL<BC31104150006944014711116008010000210502060 8FFFFFFFF>
[T + 445 mSec] HDLC Put[length = 25] <01><I>, N(R)3, N(S)5 -- Q=0 D=0
Channel = 000001
CALLACCEPT<BC311041500121440147111160060021050706 40>
[T + 63 mSec] HDLC Get[length = 2] <01><RR>, N(R)6
[T + 370 mSec] HDLC Get[length = 39] <03><I>, N(R)6, N(S)3 -- Q=0 D=0
Channel = 000001
CLRINDICATE<11C6BC311041500069440147111160120000C10400000001C2080
000000200000002>
[T + 1 mSec] HDLC Put[length = 5] <01><I>, N(R)4, N(S)6 -- Q=0 D=0
Channel = 000001 CLRCFRM
[T + 507 mSec] HDLC Get[length = 2] <01><RR>, N(R)7
[T + 109265 mSec] HDLC Put[length = 29] <01><I>, N(R)4, N(S)7 -- Q=0 D=0
Channel = 000007
CALLREQ<CB440147111163110415001210060021050706 40FFFFFFFF>
[T + 66 mSec] HDLC Get[length = 2] <01><RR>, N(R)0
[T + 737 mSec] HDLC Get[length = 39] <03><I>, N(R)0, N(S)4 -- Q=0 D=0
Channel = 000007
CLRINDICATE<F542CB440147111163110415001210120000C1040000000C20800
00000100000002>
[T + 1 mSec] HDLC Put[length = 5] <01><I>, N(R)5, N(S)0 -- Q=0 D=0
Channel = 000007 CLRCFRM
[T + 605 mSec] HDLC Get[length = 2] <01><RR>, N(R)1
```

```
[T + 59 mSec] HDLC Put{length =29 <01><I>, N(R)5, N(S)1 -- Q=0 D=0
Channel = 000007
CALLREQ<CC3110213001633110415001210600210507064OFFFFFFFF>
[T + 68 mSec] HDLC Get[length = 2] <01><RR>, N(R)2
[T + 388 mSec] HDLC Get[length = 39] <03><I>, N(R)2, N(S)5 -- Q=0 D=0
Channel = 000007
CLRINDICATE<0900CC31102130016331104150012112000C10400000000C2080
000000100000002>
[T + 27 mSec] HDLC Put[length = 5] <01><I>, N(R)6, N(S)2 -- Q=0 D=0
Channel = 000007 CLRCFRM
[T + 608 mSec] HDLC Get[length = 2] <01><RR>, N(R)3
[T + 188465 mSec] HDLC Get[length = 31] <03><I>, N(R)3, N(S)6 -- Q=0 D=0
Channel = 000001
INCOMINGCALL<BC31104150012144014711116008010000210502060 8FFFFFFFF>
[T + 372 mSec] HDLC Put[length = 25] <01><I>, N(R)7, N(S)3 -- Q=0 D=0
Channel = 000001
CALLACCEPT<BC311041500121440147111160060021050706 40>
[T + 76 mSec] HDLC Get[length = 2] <01><RR>, N(R)4
[T + 151 mSec] HDLC Put[length = 44] <01><I>, N(R)7, N(S)4 -- Q=0 D=0
Channel = 000001 <I>, N(R)0,
N(S)0(M)<00A6480026000100000000FFFFFFFFFFFF0001000000000000AA003E
200010002000004BD000B>
[T + 92 mSec] HDLC Get[length = 2] <01><RR>, N(R)5
[T + 177 mSec] HDLC Get[length =39] <03><I>, N(R)5, N(S)7 -- Q=0 D=0
Channel = 000001
CLRINDICATE<11C6BC3110415001214401471111601200 00C10400000000C2080
000200000003>
[T + 1 mSec] HDLC Put[length = 5] <01><I>, N(R)0, N(S)5 -- Q=0 D=0
Channel = 000001 CLRCFRM
[T + 584 mSec] HDLC Get[length = 2] <01><RR>, N(R)6
[T + 107337 mSec] HDLC Put[length = 29] <01><I>, N(R)0, N(S)6 -- Q=0 D=0
Channel 000007
CALLREQ<CB4401471111631104150012100600210507064OFFFFFFFF>
[T + 66 mSec] HDLC Get[length = 2] <01><RR>, N(R)7
[T + 788 mSec] HDLC Get[lenth = 39] <03><I>, N(R)7, N(S)0 -- Q=0 D=0
Channel = 000007
CLRINDICATE<0342CB44014711116311041500121012000 0C10400000001C2080
000000100000002>
[T + 1 mSec] HDLC Put[length = 5] <01><I>, N(R)1, N(S)7 -- Q=0 D=0
Channel = 000007 CLRCFRM
[T + 593 mSec] HDLC Get[length = 2] <01><RR>, N(R)0
[T + 52 mSec] HDLC Put[length = 29] <01><I>, N(R)1, N(S)0 -- Q=0 D=0
Channel = 0000007
CALLREQ<CC3110213001633110415001210600210507064OFFFFFFFF>
[T + 93 mSec] HDLC Get[length = 2] <01><RR>, N(R)5
[T + 347 mSec] HDLC Get[length =39] <03><I>, N(R)R, N(S)1 -- Q=0 D=0
Channel = 000007
CLRINDICATE<0900CC31102130016331104150012112000C10400000000C2080
00000100000002>
[T + 12 mSec] HDLC Put[length = 5] <01><I>, N(R)2, N(S)5 -- Q=0 D=0
Channel = 000007 CLRCFRM
[T + 603 mSec] HDLC Get[length = 2] <01><RR>, N(R)6
[T + 9032 mSec] HDLC Put[length = 2] <01><DISC>
[T + 57 mSec] HDLC Get[length = 2] <01><UA>
[T + 43 mSec] HDLC Get[status = aborted][length = 0] ... end  reached before expected.
```

Sample Log #3 - RS-232C (ASCII) TTY/ITS monitoring

This is an example log of ITS/TTY monitoring at the RS-232C level with ASCII display format.

```
Series 8000 Network Services Executive Version 10.0d
Pesky-CMS:AlphaServices-pa:Xerox RS232C monitor log of:
    Server Name: Pesky-server:AlphaServices-pa:Xerox
    Network: 0-667, Processor: 2-852-127-429
    Hardware: 8000 Processor, Memory 480 KBytes
    Network Administrator: Michalene M. Casey:AlphaServices-pa:Xerox
Filed on: (Paris-FS:)Paris-SNAlog/TheGreatTTYLog16-Sep-85 18:17:55
Checking out TTY monitoring

Data Collect from RS232c CIUPort CIU659-A3, Line #66

[T + 406560 mSec] RS232C Transducer Put[status = success] [length = 2] <CRLF>

[T + 724 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached
before expected

[T + 69 mSec] RS232C Transducer Put[status = success] [length = 68] <Continued
inactivity will force disconnection in fifteen seconds. CRLF>

[T + 85 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before
expected

[T + 4377 mSec] RS232C Transducer Get[status = success] [length = 1] <CR>

[T + 212 mSec] RS232C Transducer Put[status = success [length = 2] <CRLF>

[T + 86 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before
expected

[T + 35 mSec] RS232C Transducer Put[status = success] [length = 2] <> >

[T + 62 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before
expected

[T + 1909 mSec] RS232C Transducer Get[status = success] [length = 1] <l>

[T + 69 mSec] RS232C Transducer Put[status = success] [length = 1] <l>

[T + 45 mSec] RS232C Transducer Put[status = success] [length = 0] ... end reached
before expected

[T + 195 mSec] RS232C Transducer Get[status = success] [length = 2] <og>

[T + 93 mSec] RS232C Transducer Put[status = success] [length = 1] <o>

[T + 86 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before
expected

[T + 244 mSec] RS232C Transducer Put[status = success] [length = 1 <g>

[T + 106 mSec] RS232C Transducer Get[status = success] [length = 1] <CR>

[T + 63 mSec] RS232C Transducer Put[status = success] [length = 1] <o>
[T + 42 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before expected

[T + 76 mSec] RS232C Transducer Put[status = success] [length = 1] <n>

[T + 52 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before expected

[T + 39 mSec] RS232C Transducer Put[status = success] [length = 2] <CRLF>

[T + 58 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before expected

[T + 284 mSec] RS232C Transducer Put[status = success] [length = 18] <Your name please: >

[T + 159 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before expected

[T + 1960 mSec] RS232C Transducer Get[status = success] [length = 1] <b>

[T + 40 mSec] RS232C Transducer Put[status = success] [length = 1] <b>

[T + 55 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before expected

[T + 110 mSec] RS232C Transducer Get[status = success] [length = 1] <o>

[T + 55 mSec] RS232C Transducer Put[status = success] [length = 1] <o>

[T + 102 mSec] RS232C Transducer Get[status = success] [length = 1] <z>

[T + 64 mSec] RS232C Transducer Put[status = success] [length = 1] <z>

[T + 89 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before expected

[T + 104 mSec] RS232C Transducer Get[status = success] [length = 1] <z>

[T + 89 mSec] RS232C Transducer Put[status = success] [length = 1] <z>

[T + 29 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before expected

[T + 56 mSec] RS232C Transducer Get[status = success] [length = 1] <o>

[T + 69 mSec] RS232C Transducer Put[status = success] [length = 1] <o>

[T + 29 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before expected

[T + 190 mSec] RS232C Transducer Get[status = success] length = 2] <er>

[T + 39 mSec] RS232C Transducer Put[status = success] [length = 1] <e>

[T + 59 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before expected

[T + 104 mSec] RS232C Transducer Put[status = success] [length = 1] <r>
```

```
[T + 32 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before
expected

[T + 2451 mSec] RS232C Transducer Get[status = success] length = 1] <CR>

[T + 40 mSec] RS232C Transducer Put[status = success] length = 2] <CRLF>

[T + 43 mSec] RS232C Transducer Put[status = success] [length = 0] ...end reached before
expected

[T + 69 mSec] RS232C Transducer Put[status = success] length = 15] <Your password: >
```

Index

(This page intentionally blank)