WANG

Networking

WSN VS Network Control and Monitoring Guide

Networking
WSN VS Network Control and Monitoring Guide

1st Edition — March 1985

715-0164

WANG

WANG LABORATORIES, INC., ONE INDUSTRIAL AVENUE, LOWELL, MA 01851 • TEL (617) 459-5000, TWX 710-343-6769, Telex 94-7421

DISCLAIMER OF WARRANTIES AND LIMITATION OF LIABILITIES

The staff of Wang Laboratories, Inc., has taken due care in preparing this manual. However, nothing contained herein modifies or alters in any way the standard terms and conditions of the Wang purchase, lease, or license agreement by which the product was acquired, nor increases in any way Wang's liability to the customer. In no event shall Wang or its subsidiaries be liable for incidental or consequential damages in connection with or arising from the use of the product, the accompanying manual, or any related materials.

SOFTWARE NOTICE

All Wang Program Products (software) are licensed to customers in accordance with the terms and conditions of the Wang Standard Software License. No title or ownership of Wang software is transferred, and any use of the software beyond the terms of the aforesaid license, without the written authorization of Wang, is prohibited.

WARNING

This 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. 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.

PREFACE

This manual describes the programs and operations involved in controlling and monitoring a network that uses Wang Systems Networking (WSN) communications products. It is written for VS system administrators who are responsible for the operation of their systems within the context of a network, and for individuals involved in network-wide monitoring and maintenance.

Chapter 1 introduces communications control and monitoring on a VS system. The chapter introduces the Communication Network Services (CNS) control and monitoring utility WSNMON, the standard VS operational control facility, and the Wang Band monitor, which monitors the activity on each CIU on the Wang Band of WangNet.

Chapter 2 describes how to use WSNMON to control and monitor WSN transports. Chapter 3 describes how to use WSNMON to monitor sessions. Chapter 4 describes how to use WSNMON to monitor applications attached to the network. Chapter 5 describes how to use WSNMON to monitor routes over which data is transmitted between systems. Chapter 6 describes how to use WSNMON to control and monitor general network activity. Chapter 7 describes how to run various network diagnostic programs from WSNMON. Chapter 8 introduces the WSNMON trace point table.

Chapter 9 describes the operational features of the network that are available at the VS Operator's Console.

Chapter 10 describes the Wang Band monitor.

Appendix A lists and defines those File Transfer and VS Terminal Emulation utilities error messages that require System Administrator actions. Appendix B covers error messages associated with Communication Network Services (CNS). Appendix C lists and defines the Operator's Console error messages associated with Wang network services. Appendix D describes the problems you may encounter with your system's network communications, and possible responses to those problems. Appendix E contains a list of the Transfer Log return codes and their meanings.

Those who use this manual should have access to the following Wang publications.

- WSN VS Network Configuration Guide (715-0165)
- Network User Guide to VS Systems (800-1316-D)
- VS System Operation Guide (800-1102SO-07)

CONTENTS

CONTENTS (continued)

CONTENTS (continued)

FIGURES

TABLES

CHAPTER 1
INTRODUCTION TO VS COMMUNICATIONS CONTROL AND MONITORING

1.1 OVERVIEW

When a VS system is equipped with the appropriate components, it can control a set of hardware and software elements that allow it to communicate with other systems in the network. The Wang Systems Networking control and monitoring facility WSNMON provides users with information concerning Communications Network Services (CNS) activity on the local system.

WSNMON also allows users to perform the following operations:

- Enable and disable transports. Transports are said to be enabled when they can perform the functions required to initialize themselves (e.g., establishing transport connections).
- Control CNS. WSNMON allows users to start and stop the CNS task.
- Alter a transport's base cost to manage transport congestion. Refer to Chapter 1 of the WSN VS Network Configuration Guide for an explanation of base cost.

NOTE

The term "local system" refers to the system to which you are logged on. The system could be the system to which your workstation is physically attached, or a remote system to which you are logged on using the WSN VS Terminal Emulation service (i.e., remote logon).

The standard VS operational control facility also allows VS Operators to perform various network control and monitoring functions. These functions are

- Control and monitor sessions between applications on the local system and applications on other systems
- Control and monitor communications across a specific transport

- Control and monitor WSN service activity between the local system and a specific remote system

- Display the status of individual DLPs

- Report on network events

VS systems that use the WSN Wang Band transport to communicate over the Wang Band of local-area WangNet are also equipped with the Wang Band Monitor. This monitor polls the Cable Interface Unit (CIU) on each system that shares the Wang Band to determine the number of virtual circuits each CIU is currently supporting.

1.2 WSNMON

WSNMON uses inter-task messages to communicate with the CNS task on a VS system. CNS is a layered software architecture that provides applications with a method of network access. CNS control software queries each layer for information on that particular layer's activity. WSNMON provides an interface to the CNS control software, allowing users to monitor this information.

CNS architecture is summarized in Chapter 1 of the WSN VS Network Configuration Guide.

Accessing WSNMON

To access WSNMON, press PF1 from the Command Processor screen. Type WSNMON in the PROGRAM field on the screen that appears. Then you need only press ENTER, if WSNMON resides in the system library on the system volume. If WSNMON does not reside in the system library on the system volume, enter the names of the appropriate library and volume in the LIBRARY and VOLUME fields. The WSNMON Main menu appears, as shown in Figure 1-1.

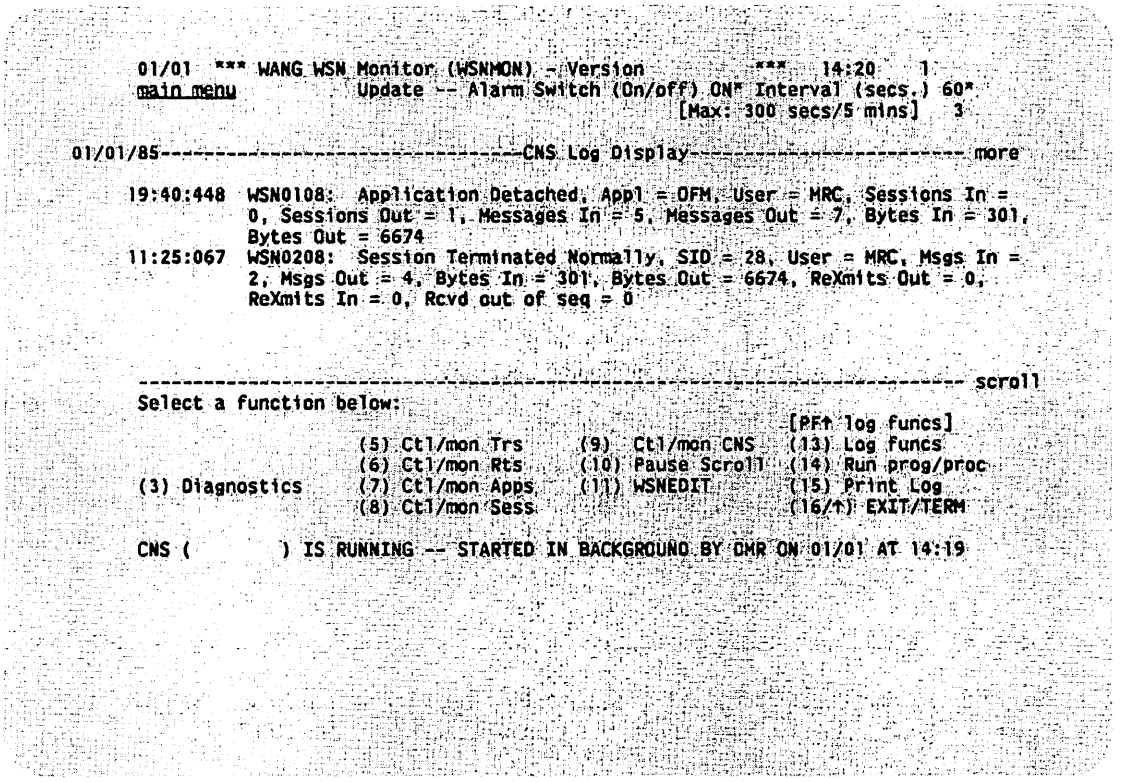

Figure 1-1. WSNMON Main Menu

Several fields appear at the top of the WSNMON Main menu. These fields are described as follows.

ALARM SWITCH - Allows you to specify whether or not your workstation will make a beeping sound when the WSNMON Main menu is refreshed (i.e., the log file is read). Type ON (to activate the alarm switch) or OFF (to render the alarm swith inactive) in this field.

INTERVAL - Allows you to specify the amount of time (in seconds) between the attempts WSNMON makes to read the CNS log file and to verify that the CNS task is running. The information from the log file appears on the Main menu in the form of messages that scroll automatically when the WSNMON Main menu is in scroll mode. The WSNMON Main menu is in scroll mode when the word "Scroll" appears at the bottom right-hand part of the log display section of the screen.

The WSNMON Main menu displays messages that give real-time information on network activity (e.g., reasons for failed attempts to communicate). After leaving the screen, the messages are stored in chronological order in a log file. WSNMON allows you to scroll through this log of messages.

The following PF keys appear on the WSNMON Main menu as it first appears when you run WSNMON.

PF3 - Enables you to access the Diagnostics function.

PF5 - Enables you to access the Control/Monitor Transports function.

PF6 - Enables you to access the Monitor Routes function.

PF7 - Enables you to access the Monitor Applications function.

PF8 - Enables you to access the Monitor Sessions function.

PF9 - Enables you to access the Control/Monitor CNS function.

PF10 - Enables you to stop the messages on the log display section of the screen from scrolling automatically. Press PF10 to "freeze" the messages on the screen; press PF10 again to restore automatic scrolling.

PF11 - Enables you to run WSNEDIT. Running WSNEDIT allows you to view network directory and local-view configuration file information.

NOTE:

The VS system administrator should assign a 1024K segment two size to all users who wish to run WSNEDIT from WSNMON.

PF↑ - When you access WSNMON log functions, several new PF keys appear. Each PF key invokes a specific log function. When the WSNMON Main menu is not in log function mode, you can press SHIFT, then the appropriate PF key to call a specific log function. For example, pressing PF18 (SHIFT PF2) displays the first screen of log messages in the log file on the log display section of the WSNMON Main menu.

PF13 - Enables you to access WSNMON log functions. These functions allow you to scroll through the CNS log messages stored in the log file. Refer to the section on WSNMON log functions that appears later in this chapter.

PF14 - Enables you to run programs or procedures. Pressing this PF key results in the appearance of three fields through which a user can enter the name of the program and the library and volume in which it resides. Pressing ENTER then runs the program.

PF15 - Enables you to print the log messages stored in the CNS log file. When you press PF15, the fields that appear at the bottom of the screen allow you to enter the range (between specific dates and times) of log messages you wish to print. For example, you can print all the messages that were displayed from 3 PM on 01/28/85 to 10 AM on 01/30/85. The fields that appear when PF15 is pressed are

From date/time - Log messages are stored in the log file according to the date and time they were displayed on the WSNMON Main menu. The "From" date/time fields allow you to specify the date and time of the message you want to print first. The date field defaults to today's date; the time field defaults to 0 (the beginning of the day). To change the date default setting, enter the new date in YYMMDD format; to change the time default setting, enter the new time in HHMMSS format.

To date/time - The "To" date and time fields allow you to specify the date and time of the message you want to print last. The date field defaults to today's date; the time field defaults to the current time. Change the default settings for the "To" fields as you would change those of the "From" fields.

NOTE

If the date and time you specify in the "From" fields is earlier than the date and time you specify in the "To" fields, the messages print out in chronological order. If the date and time in the "To" fields is earlier than the date and time in the "From" fields, the messages print out in reverse chronological order.

Press ENTER when you have specified the range of specific dates and times. WSNMON will display a message that tells you the print is in progress. When the messages are through printing, WSNMON will display a message that tells you the print is completed.

PF16 - Enables you to exit from WSNMON.

PF32 - Enables you to exit from WSNMON.

The functions that can be accessed through WSNMON are

- Control/Monitor Transports - This function displays the current status of all transports that have been defined through WSNEDIT, as well as the number of bytes and messages sent and received, the number of incoming messages rejected, the base and total costs for the transport, and the reactivation timer. This function also allows users to enable or disable transports and to modify base cost and reactivation timer values.

- Monitor Applications - This function displays the status of all applications currently attached to CNS, as well as the ID of the application's user and the number of messages and bytes that the application has sent or received. This function also displays the current number of sessions the application has initiated, the current number of sessions that applications on remote systems have initiated with the application, and the maximum number of sessions the application can support.

- Monitor Sessions - This function displays the status of all sessions that are currently active. It displays the session ID, whether the session was initiated by the local system or a remote system, the name and local application session ID of the application that is the local session partner, and the number of data messages, bytes, acknowledgements, and credits sent and received during the session.

- Monitor Routes - This function displays the status of the routes that were defined through WSNEDIT. It displays whether or not destination systems have been initialized, the path cost of each route, and the status of transports that connect the local system and adjacent systems. It is recommended that you read the CNS Routing Overview in Chapter 1 of the WSN VS Network Configuration Guide before you access the Monitor Routes function for the first time.

- Control/Monitor CNS - This function displays the general status of CNS. The general status includes information on the number of transports the version of CNS that is running can support, the number of applications attached to CNS, and the number of sessions currently established. There is also information on CNS buffers, the number of areas, and the number of systems in the network. This function also allows you to start and terminate CNS.

- Diagnostics - WSNMON provides a set of diagnostic test tools. These tools allow the user to assess the rate of data transfer across a line, the amount of time between the sending and receiving of a message, the accuracy of data transfer, and the number of systems the local system can contact in the network. WSNMON also provides a trace table function.

WSNMON Log Functions

When you access WSNMON log functions, several new PF keys appear at the bottom of the WSNMON Main menu. These keys and the specific functions they allow you to access are listed and described as follows:

PF2 (First) - Displays the first screen of log messages in the log display section of the WSNMON Main menu. These messages are the first messages listed in the first log file in library @LOG@. A new log file is created for each day. Messages in the log file are listed in chronological order, according to the time at which the events they record occurred.

PF3 (Last) - Displays the latest log messages stored in the log file in the log display section of the WSNMON Main menu. If you press PF3, the PF10 key appears, allowing you to inhibit automatic scrolling. Press PF10 to inhibit automatic scrolling; press PF10 again to restore automatic scrolling.

PF4 (Previous) - Displays the previous screen of log messages on the log display section of the WSNMON Main menu. This screen consists of messages in the log file just prior to the messages you were viewing before you pressed PF4. PF4 also allows you to scroll back to earlier messages in the log file. To scroll back, keep pressing PF4.

PF5 (Next) - Displays the next screen of log messages on the log display section of the WSNMON Main menu. This screen consists of messages in the log file that follow in chronological order the messages you were viewing before you pressed PF5. You can scroll to the end of the file by continuing to press PF5.

PF6 (Down 1 Msg) - Allows you to display the message that immediately precedes, in chonological order, the message that appears at the top of the log display portion of the WSNMON Main menu. The message at the bottom of the log display portion scrolls off the screen, creating room for the message to scroll on to the screen from the top. You may have to press PF6 more than once to display the entire message.

PF7 (Up 1 Msg) - Allows you to display the message that immediately follows, in chonological order, the message that appears at the bottom of the log display portion of the WSNMON Main menu. The message at the top of the log display portion scrolls off the screen, creating room for the message to scroll on to the screen from the bottom. You may have to press PF7 more than once to display the entire message.

PF8 (Find Msg/Text) - Pressing this PF key displays three new fields on the WSNMON Main menu. These fields allow you to search for specific log messages in the log file. These fields are

YYMMDD - This field allows you to enter a specific day in YYMMDD format. If you enter information in this field without entering information in the other fields, the first messages that appeared on that day will appear on the WSNMON Main menu. You can then scroll through the rest of the messages for that day.

HHMMSS - This field allows you to enter a specific time during the day you specified in the YYMMDD field. Enter time in HHMMSS format. You should fill the entire field. If you enter a time in this field, the first message that appeared at that time (or after) will be displayed at the top of the WSNMON Main menu. Messages that follow the first message in chonological order are displayed beneath the first message.

Text - This field allows you to search for occurences of a text string. If you enter text in this field and specify a day and time in the other fields, the YYMMDD and HHMMSS fields are overridden. It does not matter whether you enter text in upper or lower case. However, if the text for which you are searching contains quotation marks, you must enter the quotation marks.

This field allows you to search for just those messages with occurences of the text you specified in the Text field. For example, you might want to enter "Session". Many log messages contain this specific word, indicating whether or not sessions have been terminated normally. The log display portion of the WSNMON Main menu then displays the most recent occurence of a message with the word "Session." You can press ENTER to scroll back through the log file to earlier messages with the occurence of the word "Session." You can press PF8 to scroll forward through the log file to find other messages with the word "Session."

Press ENTER after you have typed in the appropriate information in the YYMMDD, HHMMSS or Text fields. This action initiates the search operation.

PF13 (Main funcs) - Enables you to exit from log function mode and access the other WSNMON functions.

Starting the Log Task and CNS

After your VS has been configured for network communications (refer to the WSN VS Network Configuration Guide) and IPLed, you are ready to start the log task and the CNS task. You must start the CNS task before your VS can utilize CNS capabilities to communicate with other systems. Your VS can communicate with other systems even if the log task is not running; however, no record of CNS and Wang Office (Store-and-Forward) activity will be kept.

The log task program LOGTSK is a background task that creates and maintains the log files. You defined the volume on which these files reside when you ran LOGCNTRL (refer to the WSN VS Network Configuration Guide, Chapter 1). These files keep a record of CNS and Wang Office (Store and Forward) activity.

There are several ways to start the log task and the CNS task. The best method is as follows:

- Press PF14 (Run Prog/Proc) from WSNMON or access the Run Program or Procedure function through the Command Processor. If you press PF14 from WSNMON, proceed by typing "WSNSTART" in the PROGRAM field and pressing ENTER. This action brings up the CNS task and the log task. When you return to the WSNMON Main menu, the menu may indicate that the CNS task is not running, even though the CNS task is up. Several seconds may elapse before the WSNMON Main menu indicates that the CNS task is running.

You can also start the CNS task and the log task separately. To start the log task, submit the procedure $LOGTSK$. This procedure starts the program LOGTSK. You submit this procedure through the RUN PROGRAM OR PROCEDURE facility that you invoke from the Command Processor. Then run WSNMON after the submit procedure has been completed. Use the Command Processor facility to run WSNMON also.

To start the CNS task, press PF9 (Ctl/Mon CNS) from the WSNMON Main menu. When the next screen appears, press PF11 (Start CNS). When you return to the WSNMON Main menu, the menu may indicate that the CNS task is not running, even though the CNS task is up. Several seconds may elapse before the WSNMON Main menu indicates that the CNS task is running.

Common PF Keys

Certain PF keys are common to most of the WSNMON screens. These keys and their functions are

PF1 (RETURN) - From most screens, PF1 allows you to return to the previous screen.

PF1 (CANCEL FIND, RUN, MODIFY, PRINT) - If you initiate a "Find", "Run Program or Procedure", "Modify" or "Print" operation, you can press PF1 to cancel the operation.

PF8 (FIND) - Allows you to search for information on a specific application, transport, session, or destination system. When this PF key is pressed, a field appears in which you type the name of the application, transport, session, or destination system you wish to find. You then press ENTER.

PF10 (CHANGE PAGE OR GO TO PAGE) - Not all information about application, transport and session activity can be displayed on one screen. Within the Control/Monitor Transports, Monitor Applications, and Monitor Sessions functions, you can press PF10 to display information fields that cannot fit on the first screen. The field next to PF10 tells you which page you can go to by pressing PF10.

PF13 (OTHER FUNCTIONS) - When you have accessed one function from the WSNMON Main menu, you can press PF13 to display the PF keys that allow you to access other WSNMON functions without returning to the WSNMON Main menu. These PF keys are the same ones that appear on the WSNMON Main menu.

PF14 (RUN PROG/PROC) - Press this PF key to run programs or procedures. Pressing this PF key displays three fields on the screen; these fields allow you to enter the name of the program and the library and volume in which it resides. You can then press ENTER to run the program.

PF16/↑ (EXIT/TERM) - You can press PF 16 to return to the WSNMON Main menu. You can press PF32 (shift PF16) to terminate WSNMON.

PF↑ (OTHER FUNCTIONS) - From any WSNMON screen other than the WSNMON Main menu, you can press SHIFT, then the PF key that allows you to access a particular WSNMON function. The keys that allow you to access particular functions are displayed at the bottom of the WSNMON Main menu. For example, if you were viewing a screen within the Control/Monitor Transports function, you could press PF23 (i.e., SHIFT PF7) to access the Monitor Applications function.

1.3 VS OPERATIONAL CONTROL

Whereas WSNMON currently controls only transports and CNS, the VS operational control facility can control sessions, WSN services, and remote access to the local system. Like WSNMON, the VS Operational Control facility can enable and disable transports (i.e., links).

VS Operational Control and WSNMON differ in their control functions. WSNMON can enable or disable a transport. When a transport is enabled, it can support communications between systems; when disabled, it cannot. When WSNMON disables a transport, it terminates all sessions (with the exception of remote logon sessions) currently supported by that transport.

VS Operational Control can only inhibit File Transfer and VS Terminal Emulation (i.e., remote logon) sessions that originate from either the local VS or a remote system across a particular transport. When VS Operational Control disables a transport, it terminates all sessions currently supported by that transport.

1.4 WANG BAND MONITOR

The Wang Band Monitor sequentially polls the Cable Interface Units (CIUs) attached to each system in a network connected by Wang Band. When you run the Wang Band Monitor, the CIUs that are polled send formatted status information back to the screen. If a CIU does not respond to a poll, the poller waits 3 seconds before declaring the CIU off-line. Then it starts polling the next system.

Three categories of status information can be accessed using the Wang Band Monitor. They are

- Listing of all systems on the Wang Band
- Circuit integrity (active/inactive) on each CIU
- Single system display that interprets all the status information

For more information on how to access the Wang Band Monitor and its status messages, refer to Chapter 10. The meanings of the status messages are also included.

CHAPTER 2
CONTROL/MONITOR TRANSPORTS

2.1 INTRODUCTION

The WSNMON Control/Monitor transports function allows you to control and monitor all the transports defined for the local VS. These transports were defined in the local-view configuration file when WSNEDIT was run to create the local-view configuration (refer to the WSN VS Network Configuration Guide, Chapter 4).

When an application on the local system attempts to establish a session with an application on a remote system, a transport on the local system establishes a transport connection with the same transport on an adjacent system. The transport connection uses physical media and remains established until all sessions supported by the transport are terminated.

Adjacent systems are directly connected; that is, there are no intermediate systems between them. An application on the local system can establish a session with applications on both adjacent and non-adjacent systems. If the remote system is non-adjacent, then the appropriate transports connecting intermediate systems must establish transport connections. Refer to the WSN VS Network Configuration Guide, Chapter 1, for a more detailed explanation of the term "adjacent."

The WSNMON Control/Monitor Transports function displays three pages of information about each transport defined for the local system. This information includes

- The current status (enabled or disabled) of all transports that have been defined through WSNEDIT.
- The number of bytes and messages sent and received since the transport was enabled.
- The number of out-going messages rejected.
- The base and total costs for the transport.
- The reactivation timer value for the transport.

The Control/Monitor transports function also allows you to enable and disable transports and to modify base cost and reactivation timer values.

2.2 USING THE CONTROL/MONITOR TRANSPORTS FUNCTION

To access the Control/Monitor Transports function, press PF5 from the WSNMON Main menu. The First Control/Monitor Transports Page screen appears, as shown in Figure 2-1.

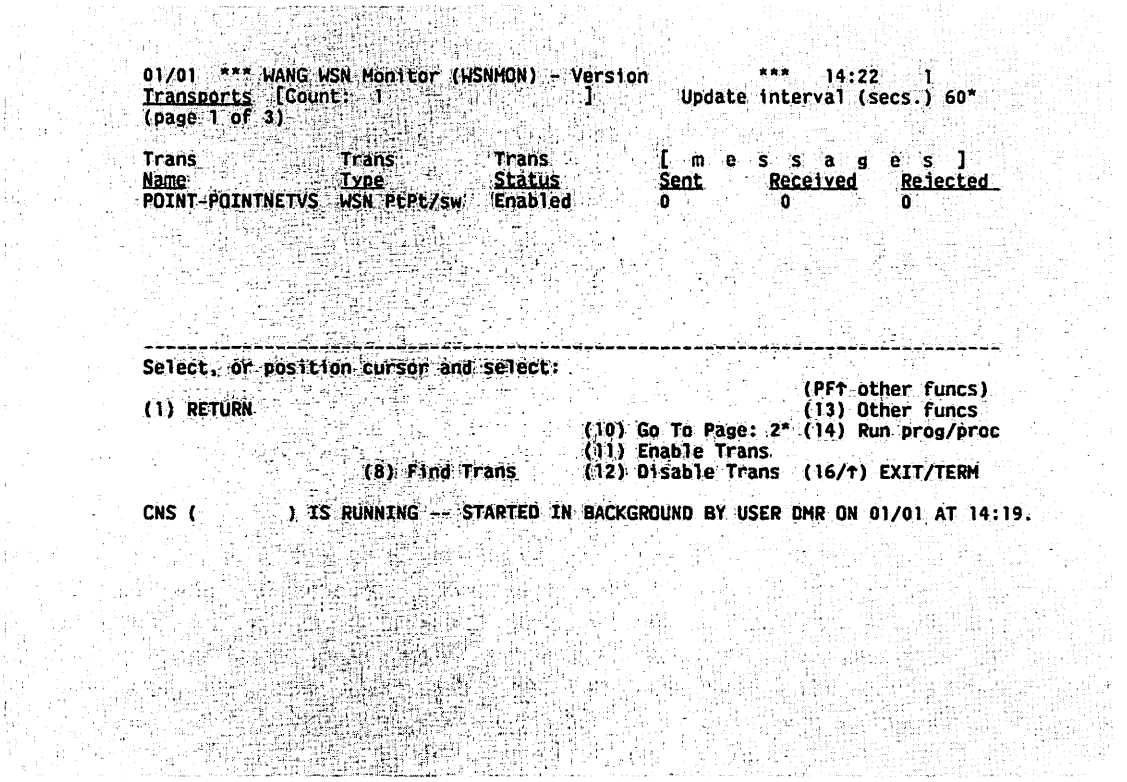

Figure 2-1. First Control/Monitor Transports Page Screen

The First Control/Monitor Transports Page screen displays the first of three pages of transport activity information. The screen lists the names of transports defined for the VS system when WSNEDIT was run to create the local-view configuration. For each transport, the screen lists the transport type, transport status, the number of messages and bytes received, and the number of messages rejected.

The following fields appear on the First Control/Monitor Transports Page screen:

UPDATE INTERVAL (SECS.) - Displays the update interval value (refer to Chapter 1 for an explanation of this field). You can enter a new value or keep the existing one.

COUNT - Displays the current number of transports defined for the local system.

NAME - Displays the name of the transport that was entered when WSNEDIT was run to create or modify the local-view configuration file for the system.

TRANS TYPE - Displays the transport type for a defined transport (e.g., WSN Pt-Pt, IDS etc.).

TRANS STATUS - Displays the status of the transport. The following listing describes the Status messages:

ENABLED - A transport is said to be enabled when it has successfully performed the functions required to initialize itself. These functions include establishing transport connections.

DISABLED - A transport is said to be disabled when it is not enabled, either because it was never enabled or because an operator has removed its enabled status.

PEND ENBL (PENDING ENABLE) - Appears when a transport is in the process of being enabled.

PEND DSBL (PENDING DISABLE) - Appears when a transport is in the process of being disabled.

ENBL FAIL (ENABLE FAIL) - Appears when an attempt to enable a transport fails or an enabled transport loses its enabled status without operator intervention.

DSBL FAIL (DISABLE FAIL) - Appears when an attempt to disable a transport fails.

MSGS SENT - Displays the number of messages the system has sent via the transport since the transport was enabled.

A message is the unit of information transfer. Each message consists of a certain amount of control information (e.g., headers) and, in most cases, user data. However, messages may also consist of just control information (e.g., restart commands).

MSGS RCVD - Displays the number of messages that the system has received via the transport since the transport was enabled.

MSGS REJ - Displays the number of out-going messages that the transport could not deliver since the transport was enabled.

The following PF keys are named at the bottom of the First Control/Monitor Transport Page screen (PF2 through PF7 are named if more than 7 transports are defined):

PF1, 2, 3, 4, 5, 6, 7, 8, 10, ↑, 13, 14, 16 - Refer to Chapter 1 for an explanation of these PF keys.

PF11 - Press this PF key to enable a selected disabled transport. The user selects a transport by positioning the cursor next to it.

PF12 - Press this PF key to disable a selected enabled transport. The user selects a transport by positioning the cursor next to it.

NOTE:

If you press PF12 to disable a transport, all sessions that the transport is supporting at the time are terminated.

If you press PF10 while viewing the First Control/Monitor Transport Page screen, the second page of fields for the Control/Monitor function appears. There are few differences between the first page of fields (i.e., the First Control/Monitor Transport Page screen), and the second page of fields. The PF keys that are named on the two screens are the same.

The fields that are specific to the second page of fields display the number of bytes that the system has sent and received. The following listing describes these fields:

BYTES SENT - Displays the number of bytes that the system has sent via the transport since the transport was enabled.

BYTES RCVD - Displays the number of bytes that the system has received via the transport since the transport was enabled.

If you press PF10 while viewing the second page of fields, the third page of fields for the Control/Monitor function appear. There are few differences between the first page of fields (i.e., the First Control/Monitor Transport Page screen), and the third page of fields.

The fields that are specific to the third page of fields display the base cost of the transport, the total cost of the transport, and the reactivation timer value (in seconds) of the transport. The following listing describes these fields:

BASE COST - Displays the base cost of the transport that was specified when WSNEDIT was run. (The base cost is the initial cost of communicating via a transport. The base cost is not a value that represents the amount of congestion a transport detects. The base cost simply establishes an initial value used to determine the total congestion cost of communicating by means of a transport; see TOTAL COST).

Base cost is explained in detail in Chapters 1 and 4 of the WSN VS Network Configuration Guide.

TOTAL COST - Displays the total cost of the transport. (The total cost is equal to the sum of the base cost and a congestion factor. The congestion factor is a value that a transport sends to CNS whenever CNS loads data to the transport faster than it can be transmitted. CNS then adds this value to the base cost to determine the total cost. If other transports are available to send data, CNS will use the total cost to select the transport with the least congestion.)

Total cost is explained in detail in Chapters 1 and 4 of the WSN VS Network Configuration Guide.

A transport is not heavily loaded if its base cost is equal to its total cost. For example, a transport whose base and total costs are both equal to 6 is not carrying much traffic. On the other hand, a transport whose base cost is 6 and whose total cost is 9 is subject to a good deal of congestion. The congestion factor would be equal to 3.

REACTIVATION TIMER - The reactivation timer displays the amount of time (in seconds) that CNS will wait after detecting that a transport cannot deliver data before making another attempt to send that data via that transport. The reactivation timer is set during WSNEDIT. Refer to Chapter 4 of the WSN VS Network Configuration Guide.

The PF keys named on the third page of fields are almost the same as those that appear on the first and second pages. The sole exception is as follows:

PF9 (MODIFY) - Enables you to modify the BASE COST and REACTIVATION TIMER fields. These fields appear in modify (high-lighted) mode when this PF key is pressed. You can then enter new base cost and reactivation timer values in these fields. A new base cost value does not modify the base cost value entered in the local-view configuration file through WSNEDIT.

Displaying the Summary Screen for a Transport

To display all three pages of fields for a particular transport on one screen, position the cursor next to the transport you wish to review and press ENTER. The summary screen for that transport appears. A sample summary screen is shown in Figure 2-2.

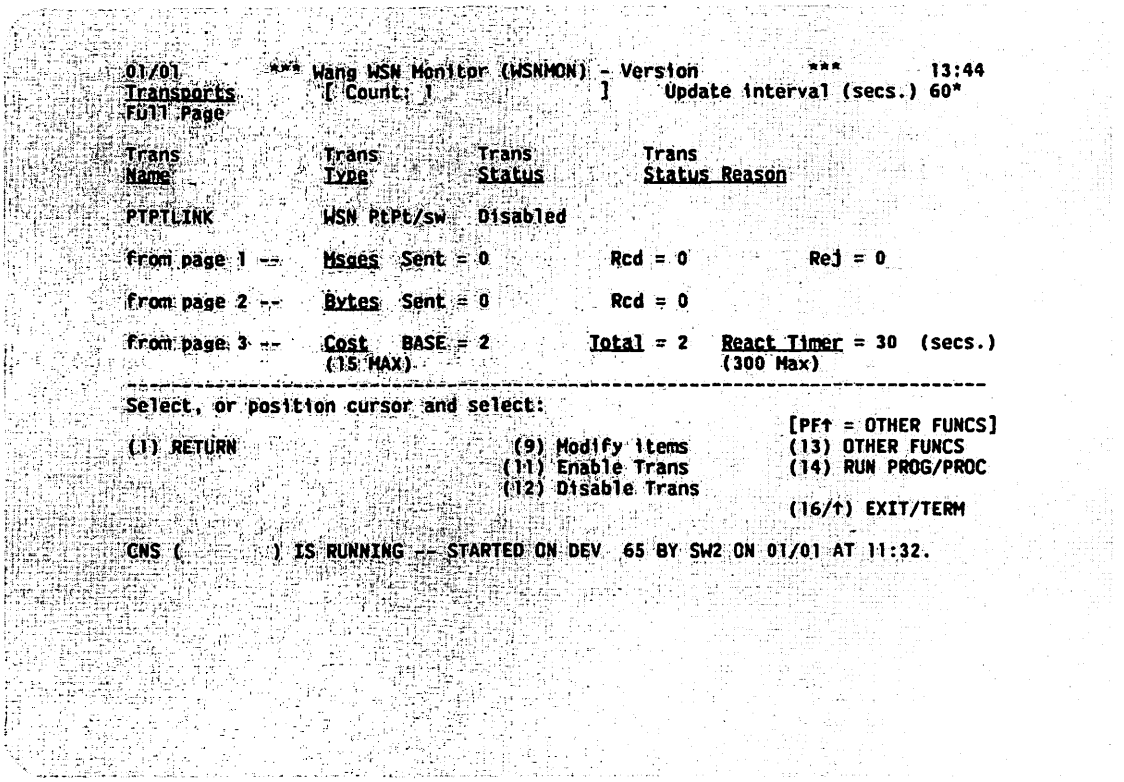

Figure 2-2. Sample Transport Summary Screen

Most of the fields and PF keys on this screen were described earlier when the individual pages were discussed. The following PF key is additional:

Trans Status Reason - This field displays a message that explains the reason for a transport failure. The possible messages are described in Appendix B.

CHAPTER 3
MONITORING SESSIONS

3.1 INTRODUCTION

The WSNMON Monitor Sessions function allows you to monitor all the sessions in which applications on the local VS are involved. CNS assigns a unique ID to each session. You can determine the amount of session activity involving applications on the local VS and take measures to reduce this activity if you consider it excessive. Chapter 9 describes how to control session activity.

A session is a sequenced stream of data between two applications. The application at the local system is called the local session partner. The application at the remote system is called the remote session partner. Each session partner must attach to CNS through an ATTACH subroutine at its respective system before a session can be established.

When the local session partner attempts to establish a session with a remote session partner, the End-To-End layer at which the local session partner resides sends a connect request to the remote system. A connect request is a header attached to an OPEN command message that is sent when the application attempts to initiate a session through an OPEN subroutine. The End-To-End layer attaches this header to the message. If the connect request is accepted at the remote system, the End-To-End layer at the remote system returns a connect accept header to the originating system. The session cannot be established until the connect accept header is returned.

If the remote system rejects the connect request, the End-To-End layer of the remote system returns a connect reject header.

During a session, the CNS End-To-End layers on the systems at which the respective session partners reside exchange units of network control information called credit messages. For every credit message one End-To-End layer sends, the session partner on the receiving end can send one message. A message is a unit of data transfer that consists of control information (e.g., headers) and, in most cases, user data.

When an application attaches to CNS, CNS allocates an initial number of credits to the application. The number of credits an application receives from a remote system is added to this initial value.

Suppose that application A and application B are session partners. The End-To-End layer on the system at which application A resides sends three credit messages to the End-To-End layer on the system at which application B resides. This means that application B can send up to three messages to application A before application B must wait to send another message. If application A can receive more messages, the CNS End-To-End layer on the system at which application A resides sends more credit messages. Both End-To-End layers can send as many credits messages as they can receive messages, up to a certain limit.

A session partner can only receive so many messages (due to memory restriction) before it must acknowledge that they have been received. The receiving application acknowledges by sending a unit of network control information called an acknowledgement to the session partner that sent the data.

Figure 3-1 illustrates how systems exchange credit messages, messages with user data, and acknowledgement messages during a session.

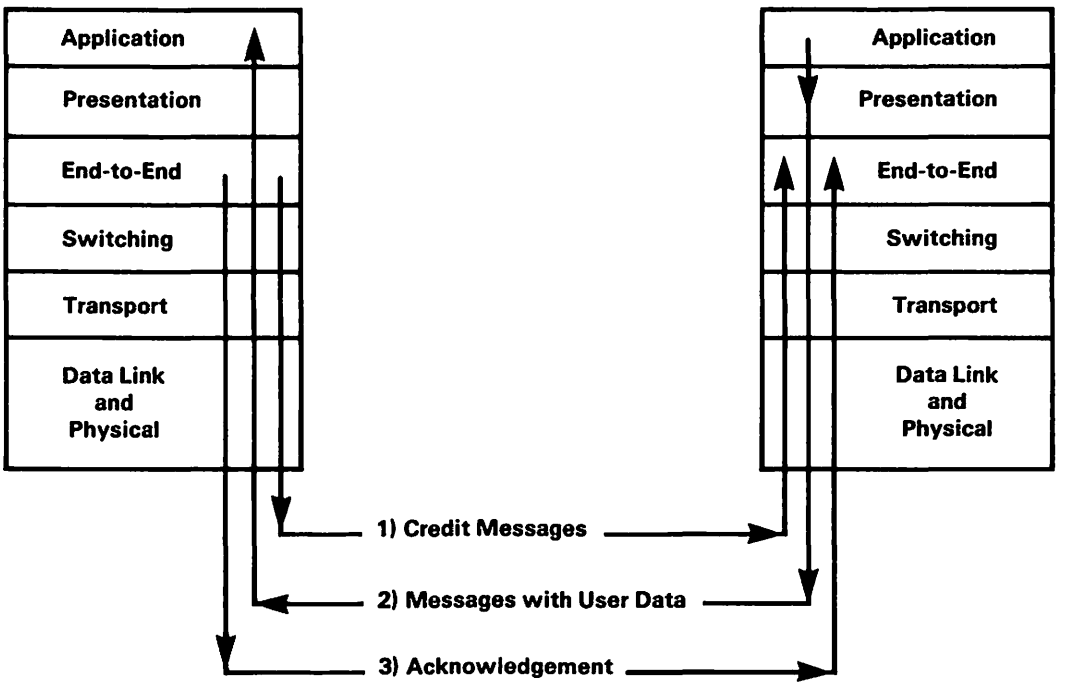

Figure 3-1. Credit, User Messages and Acknowledgement Exchange

Whenever the End-To-End layer sends data to a remote system, the End-To-End layer starts a "wait-for-acknowledgement" timer. Expiration of the timer before receipt of an acknowledgement causes CNS to attempt to retransmit the messages. The number of retransmission attempts CNS makes corresponds to a reactivation timer value entered through WSNEDIT when the transport was configured (refer to Chapter 4 of the WSN VS Network Configuration Guide). If the number of retransmission attempts exceeds the retry count, CNS declares an error condition. Receipt of an acknowledgement prior to timer expiration indicates successful reception of all messages sent up to that point.

CNS allocates a retransmit buffer for messages that may have to be retransmitted. CNS releases this buffer space when an acknowledgement is received.

Each message of transmitted data is assigned a sequence number in the order that it is sent. CNS uses the sequence number to insure that received data is reconstructed in proper order. Suppose that messages labeled 1, 2, 3, and 4 have been sent. If 4 were to arrive at the destination session partner before 3, the CNS End-to-End layer would resequence the data and deliver it to the application in the correct order.

CNS sets a maximum sequence number. Once the maximum sequence number is reached, the next sequence number CNS assigns to a data message is 0. Suppose that the maximum sequence number is 5. CNS would assign the numbers 0 through 5 to the first five messages of data sent. The sixth message of data would be assigned 0, and the sequence would begin again.

To terminate a session, an application sends a close request (a unit of network control data) to its session partner. The session does not terminate, however, until the End-To-End layer on the system at which the session partner resides acknowledges the close request.

The WSNMON Control/Monitor Sessions function displays five pages of fields of information about each session that is currently active. This information includes

- The status of all sessions that are currently active.
- The application name of the local session partner.
- The application name of the remote session partner.
- The name of the system at which the remote session partner resides.
- The session ID of the session.

- Whether or not the local session partner initiated the session (outbound session).
- Whether or not the remote session partner initiated the session (inbound session).
- The number of messages, bytes, acknowledgements, and credits the local session partner has sent and received during the session.
- The number of messages that have been received out of sequence during the session.

3.2 USING THE MONITOR SESSIONS FUNCTION

To access the Monitor Sessions function, press PF8 from the WSNMON Main menu. The First Monitor Sessions Page screen appears, as shown in Figure 3-2.

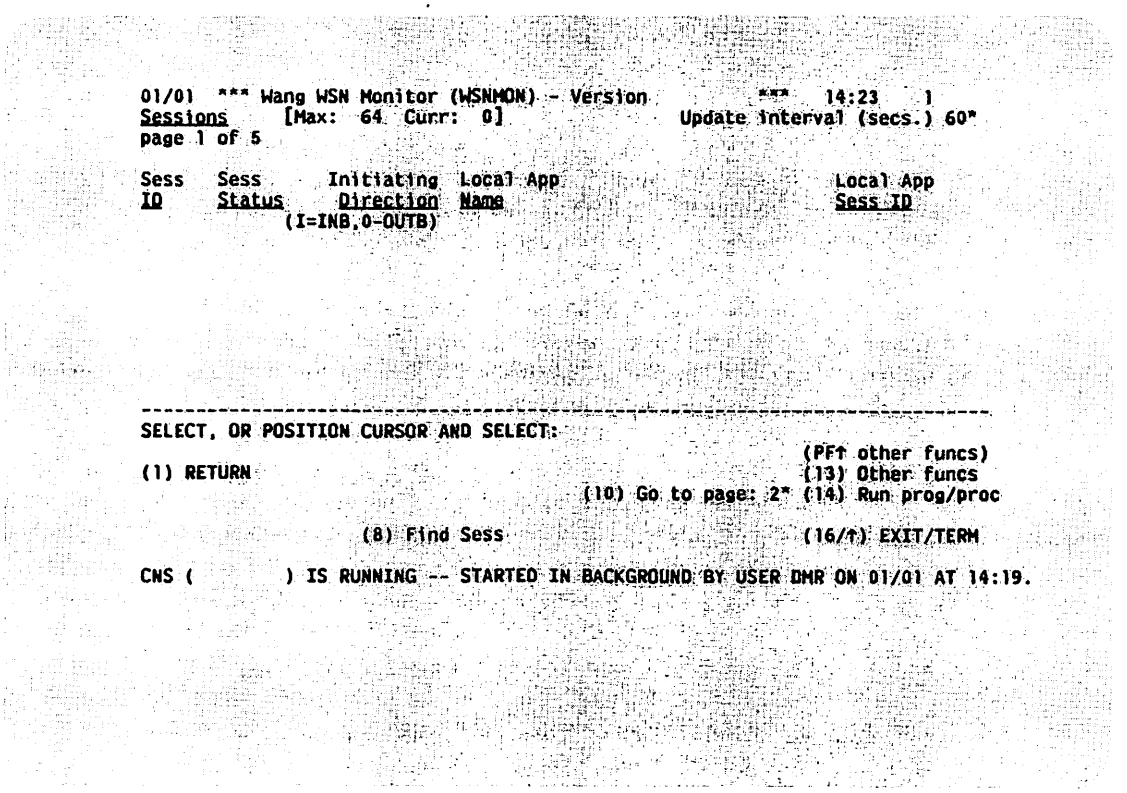

Figure 3-2. First Monitor Sessions Page Screen

The First Monitor Sessions Page screen displays the first of five pages of session activity information. The following fields appear on the First Monitor Sessions Page screen:

SESS ID - Displays the session ID that CNS assigns to each session. The session ID uniquely identifies the session to CNS.

SESS STATUS - Displays the status for each session. There are several status types. These status types are as follows:

INACTIVE - An application on the local system is attempting to establish a session with an application on a remote system. However, restarts have not been exchanged between the two systems. The session is on hold pending the exchange of restarts.

OPEN PENDING RCV CA (Open Pending Receive Connection Accept) - A local application is attempting to establish a session with a remote application, but the session will not be completely established until the remote application has sent a connection-accept response to the connect request.

OPEN PENDING SND CA (Open Pending Send Connection Accept) - An application at a remote system is attempting to establish a session with a local application, but the session will not be completely established until the local application sends an acknowledgement that it has accepted the connection-accept request.

OPEN - The session is completely established; data transfer can take place in either direction.

INACT PND RCV CLS (Inactive Pending Receive Close) - A local application is attempting to terminate a session. This attempt is made when the local application sends a close request to its session partner at the remote system. However, the session cannot become inactive until CNS receives an acknowledgement of the close request from the remote system.

INACT PND SND CLS (Inactive Pending Send Close) - A remote application is terminating a session. This attempt is made when the CNS End-to-End layer at the remote system sends a close request to the CNS End-to-End layer at the local system. However, the session cannot become inactive until the remote End-to-End layer receives an acknowledgement of the close request from the End-to-End layer at the local system.

INACT PND RCV CA (Inactive Pending Receive Connection Accept) - The local application has sent a connection request to a remote application. However, before the remote application acknowledged that it had received the connection request, the local application attempted to terminate the session. The session will terminate as soon as the local application receives the connection-accept request.

INITIATING DIRECTION - This field tells you whether a remote or a local application initiated session establishment. The field displays I (inbound) if a remote application initiated session establishment or O (outbound) if a local application initiated session establishment.

LOCAL APP NAME (Local Application Name) - Displays the name of the application that is the local session partner.

LOCAL APP SESS ID (Local Application Session ID) - An application can be a partner in more than one session. The local application session ID is the ID that a local application uses for a particular session. This ID allows CNS and the application to distinguish one session from another.

The following PF keys are named at the bottom of the First Monitor Sessions Page screen (PF2 through PF7 appear if more than seven sessions are being monitored):

PF1, 2, 3, 4, 5, 6, 7, 8, 10, ↑, 13, 14, 16 - Refer to Chapter 1 for an explanation of these PF keys.

If you press PF10 while viewing the First Monitor Sessions Page screen, the second page of fields for the Monitor Sessions function appears. There are few differences between the first page of fields (i.e., the First Monitor Sessions Page screen), and the second page of fields. The PF keys mentioned on the two pages are the same. The fields that are specific to the second page are described in the following listing:

REMOTE APP NAME (Remote Application Name) - Displays the name of the remote application involved in the session.

REMOTE APP SYS NAME (Remote Application System Name) - Displays the name of the system on which the remote session partner resides.

If you press PF10 while viewing the second page of fields, the third page of fields for the Monitor Sessions function appears. There are few differences between the first page of fields (i.e., the First Monitor Sessions Page screen), and the third page of fields. The PF keys mentioned on the two pages are the same. The fields that are specific to the third page are described in the following listing:

DATA MESSAGES SENT - Displays the number of data messages sent since the session was established.

DATA MESSAGES RECEIVED - Displays the number of data messages received since the session was established.

NOTE

A message is a unit of data transfer that includes data and control information (e.g., headers).

TOTAL BYTES SENT - Displays the total number of bytes sent since the session was established.

TOTAL BYTES RCVD - Displays the total number of bytes received since the session was established.

If you press PF10 while viewing the third page of fields, the fourth page of fields for the Monitor Sessions function appears. There are few differences between the first page of fields (i.e., the First Monitor Sessions Page screen), and the fourth page of fields. The PF keys mentioned on the two pages are the same. The terms "acknowledgement" and "credit" are explained at the beginning of this chapter. The fields that are specific to the fourth page are described in the following listing:

ACKS SENT (Acknowledgements Sent) - Displays the number of acknowledgements that have been sent since the session was established.

ACKS RCVD (Acknowledgements Received) - Displays the number of acknowledgements that have been received since the session was established.

CREDITS SENT - Displays the number of credit messages that have been made available to the application at the remote system since the session was established.

CREDITS RECEIVED - Displays the number of credit messages that the remote system has made available to the local application since the session was established.

If you press PF10 while viewing the fourth page of fields, the fifth page of fields for the Monitor Sessions function appears. There are few differences between the first page of fields (i.e., the First Monitor Sessions Page screen), and the fifth page of fields. The PF keys mentioned on the two pages are the same. The fields that are specific to the fifth page are described in the following listing:

CURRENT SEQ # SENT (Current Sequence Number Sent) - Displays the sequence number of the last message sent. The concept of sequence numbers is explained at the beginning of this chapter.

CURRENT SEQ # RECEIVED (Current Sequence Number Received) - Displays the sequence number of the last message received.

OUT-OF-SEQ COUNT (Out-Of-Sequence Count) - Displays the number of messages that have been received out-of-sequence since the session was established.

Displaying the Summary Screen for a Session

To display all five pages of fields for a particular session on one screen, position the cursor next to the ID of the session you wish to review and press ENTER. The summary screen for that session appears, displaying all five pages of fields for that particular session. A sample summary screen is shown in Figure 3-3.

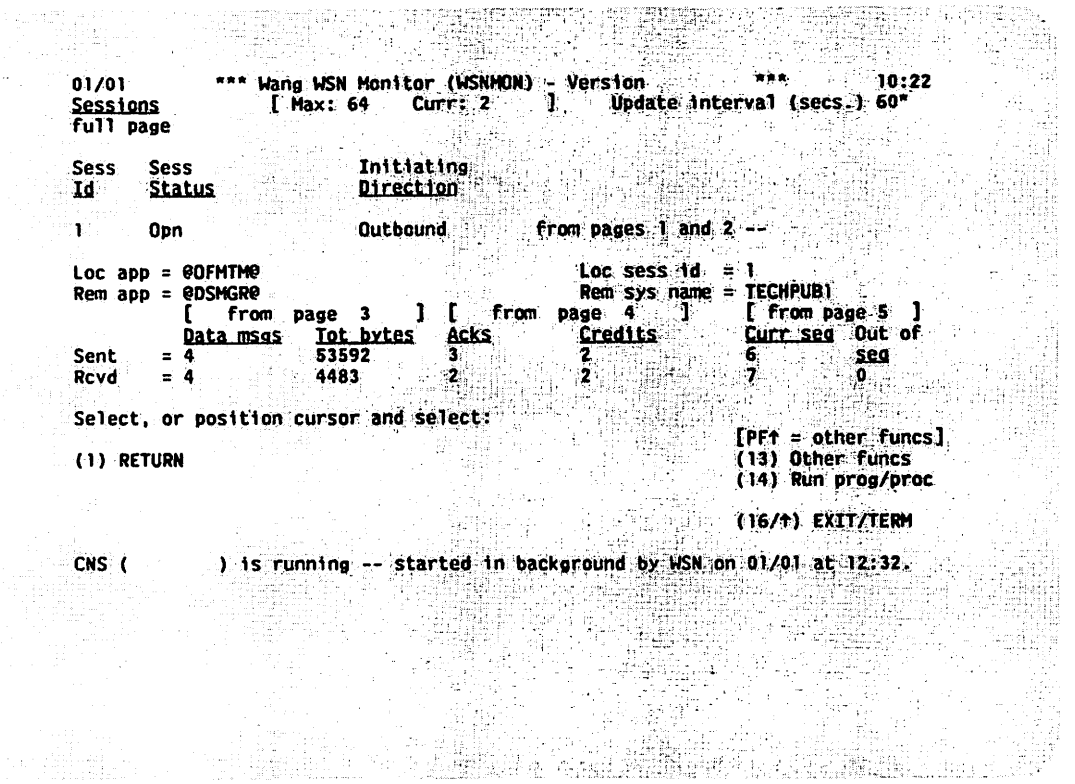

Figure 3-3. Sample Session Summary Screen

The fields and PF keys on this screen were previously described in this chapter.

CHAPTER 4
MONITORING APPLICATIONS

4.1 INTRODUCTION

The WSNMON Monitor Applications function allows you to monitor all the applications currently attached to CNS. An application is said to be attached when CNS provides the application with full access to the network. An application can be the WSN File Transfer Service (identified as FTM to CNS), Wang Office Store-and-Forward (S&F), Wang Office Office File Manager (OFM), Directory Services Manager (@DSMGR@), Directory Synchronization, or others as they are made available. The Monitor Applications function enables you to determine the amount of network activity in which these applications are involved.

An application attaches to CNS by means of a program subroutine called ATTACH that interfaces with the CNS presentation layer. Once the application is attached to CNS, the CNS presentation layer can map data from the application into the network during a session. The presentation layer then insures delivery of the data to the session partner (i.e., the peer application at the remote system) in the same format in which it was sent.

The WSNMON Monitor Applications function displays three pages of fields of information about each application that is attached to CNS. This information includes

- The status of all applications that are currently attached to CNS.
- The number of messages that the application has sent and received since it attached to CNS.
- The number of bytes the application has sent and received since it attached to CNS.

4.2 USING THE MONITOR APPLICATIONS FUNCTION

To access the Monitor Applications function, press PF7 from the WSNMON Main menu. The First Monitor Applications Page screen appears, as shown in Figure 4-1.

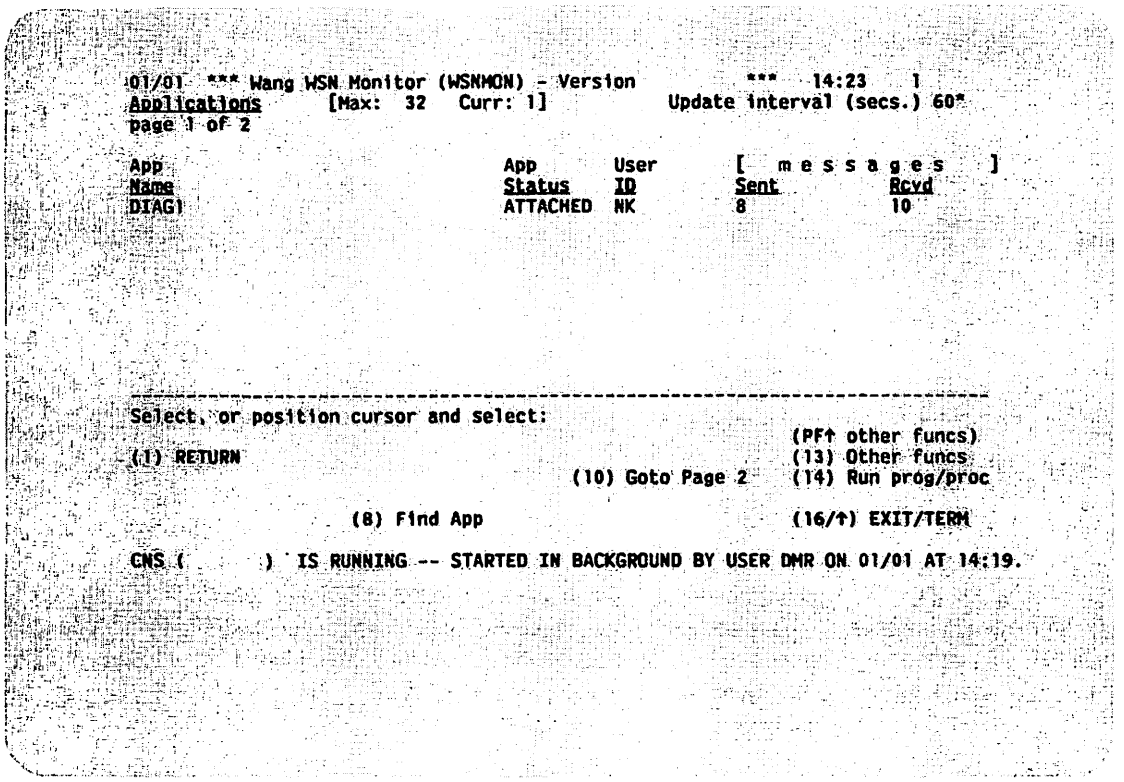

Figure 4-1. First Monitor Applications Page Screen

The First Monitor Applications Page screen displays the first of three pages of application activity information. The screen lists the name, status, user ID and number of messages sent and received for each local application attached to CNS.

The following fields appear on the First Monitor Applications Page screen:

INTERVAL - Refer to Chapter 1 for an explanation of this field.

MAXIMUM - Displays the maximum number of applications on a system that can attach to CNS at one time.

CURRENT - Displays the current number of applications attached to CNS.

APP NAME (Application Name) - Displays the name of the application (e.g., file transfer) attached to CNS.

APP STATUS (Application Status) - Displays ATTACHED for all applications attached to CNS.

USER ID - Displays the user ID (i.e., the logon ID of the user running the application) of each application attached to CNS. Applications that attach to CNS are considered network users.

MESSAGES SENT - Displays the number of messages that the application has sent since attaching to CNS.

MESSAGES RCVD (Messages Received) - Displays the number of messages that the application has received since attaching to CNS.

The following PF keys are named at the bottom of the First Monitor Applications Page screen (PF2 through PF7 appear if more than seven applications are being monitored).

PF1, 2, 3, 4, 5, 6, 7, 8, 10, ↑, 13, 14, 16 - Refer to Chapter 1 for an explanation of these PF keys.

If you press PF10 while viewing the First Monitor Applications Page screen, the second page of fields for the Monitor Applications function appears. There are few differences between the first page of fields (i.e., the First Monitor Applications Page screen), and the second page of fields. The PF keys mentioned on the two pages are the same. The fields that are specific to the second page of fields are described in the following listing:

BYTES SENT - Displays the number of bytes the application has sent since attaching to CNS.

BYTES RCVD (BYTES RECEIVED) - Displays the number of bytes the application has received since attaching to CNS.

If you press PF10 while viewing the second page of fields, the third page of fields for the Monitor Applications function appears. There are few differences between the first page of fields (i.e., the First Monitor Applications Page screen), and the third page of fields. The PF keys mentioned on the two pages are the same. The fields that are specific to the third page of fields are described in the following listing:

SESSIONS IN - Displays the number of inbound sessions in which the local application is currently involved. Inbound sessions are initiated by remote applications.

SESSIONS OUT - Displays the number of outbound sessions in which the local application is currently involved. Outbound sessions are initiated by the local application.

SESSIONS LIMIT - Displays the maximum number of inbound and outbound sessions in which the application can be involved. The value in the SESSIONS IN field plus the value in the SESSIONS OUT field cannot exceed the value in the SESSIONS LIMIT field.

Displaying the Summary Screen for an Application

To access all three pages of fields for a particular application on one screen, position the cursor next to the ID of the application you wish to review and press ENTER. The summary screen for that application appears, displaying the three pages. A sample summary screen is shown in Figure 4-2.

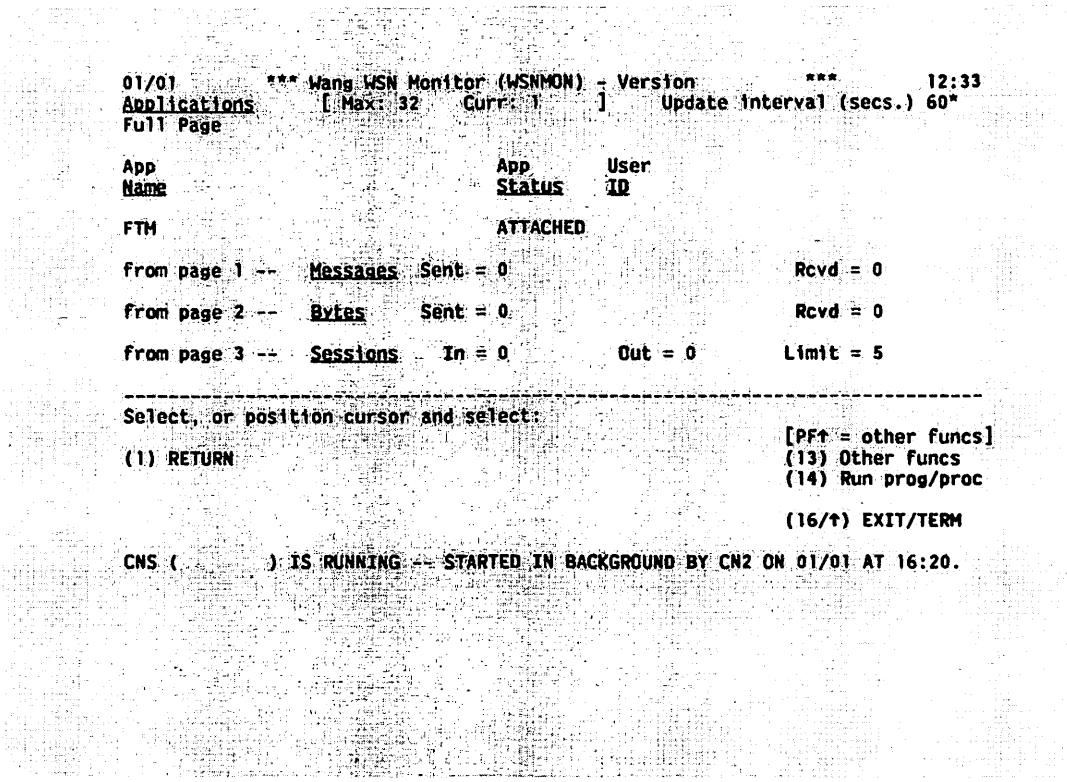

Figure 4-2. Sample Application Summary Screen

The fields and PF keys on this screen were previously described in this chapter.

CHAPTER 5
MONITORING ROUTES

5.1 INTRODUCTION

WSNMON allows you to monitor network activity on paths to destination systems. The course over which a message travels between two systems in a network is called a path. A path between two systems can consist of a single transport, or it can consist of multiple transports and intermediate systems. Two systems that are directly connected are called adjacent systems. (The term "adjacent" is explained in the WSN VS Network Configuration Guide, Chapter 1.) Paths are defined when WSNEDIT runs to create the local-view configuration (refer to Chapter 5 of the WSN VS Network Configuration Guide).

A series of protocol level exchanges must take place before two systems can communicate across a given path. The types of protocol level exchanges are as follows:

- Restart Exchange - For applications on two systems to communicate across a given path, their respective CNS End-To-End layers must exchange restart commands. A restart command is a unit of network control information that two systems exchange to negotiate the CNS revision level at which they can communicate.

  Restart commands are exchanged first as restart headers that identify the specific system and its CNS revision level. Systems then exchange units of network control information called restart acknowledgement headers; these headers notify systems involved in restart exchanges that restart commands were received.

  Two systems running CNS can communicate with each other if they have the same CNS revision levels. They can also communicate if one has the CNS revision level that is an immediate successor of the revision level used by the other. The higher CNS revision level makes the final determination as to whether or not communications can take place. Communications cannot take place under any other conditions.

If a system determines that it cannot communicate with another system, it sends a restart reject header to that system. The restart reject header is a unit of network control information that one system running CNS sends to another when it determines that communication between the two is impossible because CNS revision levels are incompatible.

- XID Exchange - Two adjacent systems exchange XID commands in addition to restart commands. Whereas restart commands determine whether or not two systems (adjacent or non-adjacent) have compatible CNS revision levels, XID commands determine whether or not messages received from an adjacent system's switching layer are accepted (i.e., can pass through or be received by) the receiving system's switching layer. XID commands also determine whether or not a system can send messages to the switching layer of an adjacent system. If an XID command is rejected, communications cannot take place between the adjacent systems.

Figure 5-1 illustrates protocol revision level exchanges.

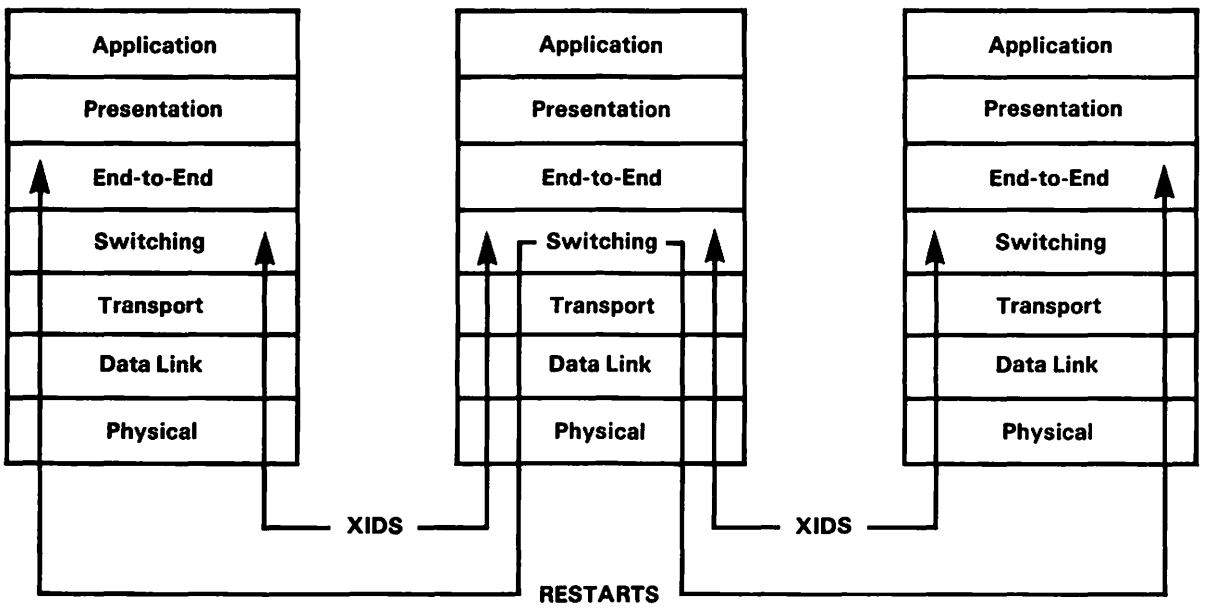

Figure 5-1. Sample Protocol Revision Level Exchanges

In the illustration above, the first system is equipped with CNS revision level N. The first system can successfully exchange restarts with the second system, which is also equipped with CNS revision level N. The first system can successfully exchange restarts with the third system, which is equipped with CNS revision level N-1. The adjacent systems in the illustration can successfully exchange XIDs.

A situation may occur in which an intermeditate system on a path between two end point systems is equipped with a CNS revision level that is two steps lower than the revision level installed on one of the end points. Messages can still pass through this intermediate system; however, the intermediate system cannot be a destination for messages originating from the end point with the higher CNS revision level. Figure 5-2 illustrates this situation.

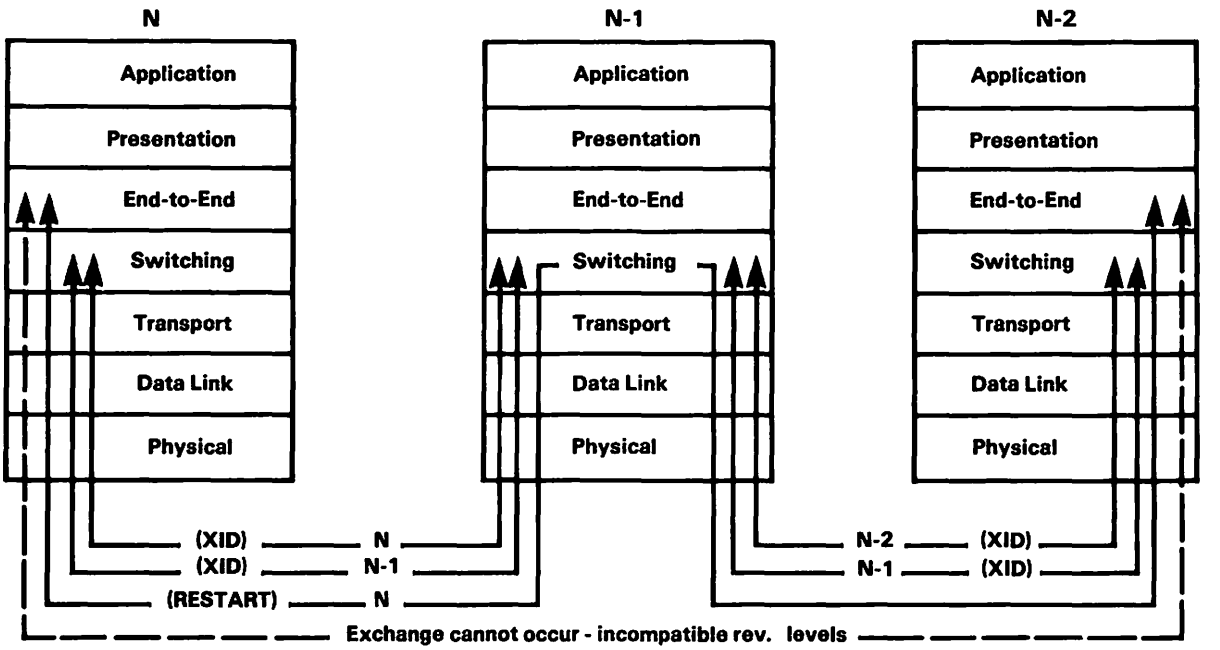

Figure 5-2. Path through a System with Incompatible CNS Revision

In Figure 5-2, XIDs are successfully exchanged between all the adjacent systems along the path. Due to incompatibility, CNS revision N and CNS revision N-2 cannot exchange restarts. However, messages originating from N that are transmitted to another system can pass through N-2. This pass-through can occur because N-1 has successfully exchanged XIDs with its adjacent systems.

During a session, applications on two adjacent systems use the transport that was prioritized through WSNEDIT to send messages to each other. If the prioritized transport fails, a backup transport can be used if the adjacent systems are properly configured. If applications on two non-adjacent systems establish a session, multiple transport types can be used to send and receive messages, depending on the local-view configurations of the end-point and intermediate systems involved and/or network congestion.

Suppose that an application on N in Figure 5-2 attempts to establish a session with an application on another system by way of N-1. Messages can travel from N to N-1 over one transport type (e.g. Wang Band). At N-1, the CNS switching layer can route the message over another transport type (e.g., X.25).

Refer to Chapter 3 for more information on sessions.

5.2 USING THE CONTROL/MONITOR ROUTES FUNCTION

Press PF6 from the WSNMON Main menu to access the Control/Monitor routes function. The Control/Monitor Routes Page screen appears, as shown in Figure 5-3.

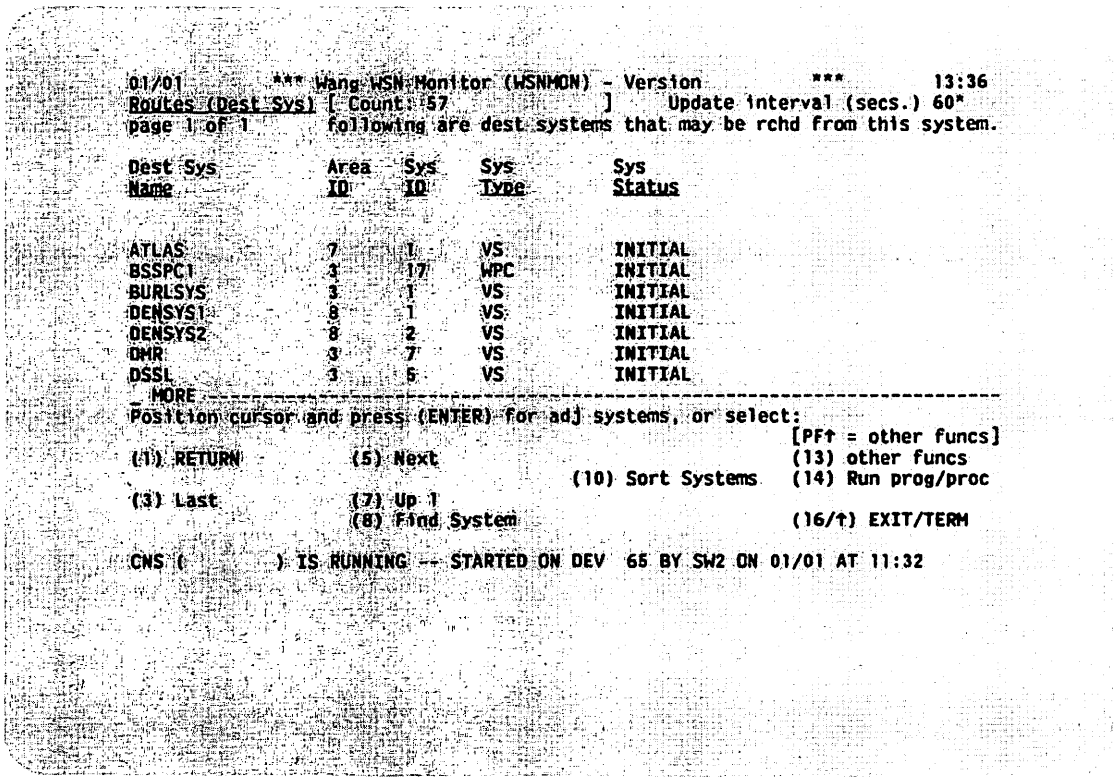

Figure 5-3. Control/Monitor Routes Page Screen

The Control/Monitor Routes Page screen displays the first page of routing activity information. The menu shows the number of destination systems in the Count field. Like other WSNMON screens, you can modify the Update Interval.

The screen lists all the destinations for messages originating from the local VS defined in the directory file. These fields are as follows:

AREA ID - Displays the system's area ID that is entered in the network directory. This ID was defined when WSNEDIT was run to define areas and systems in the network (refer to Chapter 3 of the WSN VS Network Configuration Guide).

SYS ID - Displays the system ID that is entered in the network directory. This ID was defined when WSNEDIT was run to define areas and systems in the network (refer to Chapter 3 of the WSN VS Network Configuration Guide).

SYS TYPE - Displays the system type. System types include IBM (for IBM or plug-compatible mainframes running IDS), OIS (for Office Information Systems), ALLIANCE (for Alliance systems), WPC (for Wang PCs), 2200 (for 2200 systems), and VS (for VS systems).

SYS STATUS - Displays the system status. The four status types are as follows:

CONTACTED - The CNS End-to-End layer on the local VS has successfully exchanged restart commands with the CNS End-to-End layer on the destination system during the first attempt an application on one of the systems makes to establish a session with an application on the other system.

INITIAL - No attempt has yet been made to contact the system. INITIAL indicates that no restart exchanges have taken place with CNS on the destination system since CNS was brought up.

LOST - An attempt to establish communications with this system has failed.

PENDING - An attempt is being made to establish communications with the system.

Several PF keys appear at the bottom of the menu. All but one of these keys appear throughout WSNMON and are described in Chapter 1. The key that is specific to the Control/Monitor Routes function is

- PF10 (SORT SYSTEMS) - The Control/Monitor Routes function initially lists systems according to system name in alphabetical order. Press PF10 if you want systems to be listed according to area/system ID or system type. Several new fields appear at the bottom of the Control/Monitor Routes Page screen, including Sys name, Area/System ID, and Sys type. If you want systems to be listed according to area/system ID, position the cursor under the selection block next to Area/System ID and press ENTER. The systems are then listed in numerical order according to area/system ID. If you want systems to be listed according to system type, position the cursor under the selection block next to Sys type and press ENTER. The systems are then listed according to system type.

You can position the cursor next to a destination system and press ENTER to display the list of adjacent systems by way of which messages can be routed to that destination. If the local system and adjacent systems are properly configured, you can use the VS Terminal Emulation Service to logon to an adjacent VS from which you can run WSNMON and examine the local-view routing configuration for that system.

To run the VS Terminal Emulation Service, press PF14 from WSNMON. Then type @ATTACH@ in the Program field. Press ENTER. From there, follow the instructions in the WSN VS Network User Guide for operations that can be performed during remote logon sessions.

NOTE

It is recommended that users who run @ATTACH@ from WSNMON be assigned a 1024K segment two address space.

The screen in Figure 5-4 appears when you display adjacent systems.

```
01/01        *** Wang WSN Monitor (WSNMON) - Version          ***        13:39
Routes (Adj Sys)  [ Max: 3     Curr: 3     ]    Update interval (secs.) 60*
page 1 of 1       following are adj systems to rch dest sys:              DSSR

Adj Sys          Area  Sys   Sye          Path          Path Path
Name             ID    ID    Type         Status        Cost Rejects
                                                       (1-99)

VS1              3     1     VS           INACTIVE      1    0
VS2              3     9     VS           ACTIVE        1    0
VS856027         2     9     VS           INACTIVE      1    0


--------------------------------------------------------------------------------
Position cursor and press (ENTER) for alt routes, or select:
                                                       [PF↑ = other funcs]
(1) RETURN                                             (13) Other funcs
                                                       (14) Run prog/proc

                                                       (16/↑) EXIT/TERM

CNS (        ) IS RUNNING -- STARTED ON DEV  65 BY SW2 ON 01/01 AT 11:32.
```

Figure 5-4. Adjacent System List Menu

The Adjacent System List menu displays the adjacent CNS systems that lead to the destination. Like most other WSNMON screens, the Adjacent System List menu allows you to modify the update interval.

The Adjacent System List menu displays several fields of information for each adjacent system. These fields are as follows:

AREA ID - Refer to the description of area ID for the First Control/Monitor Routes Page screen.

SYSTEM ID - Refer to the description of system ID for the First Control/Monitor Routes Page screen.

SYS TYPE - Refer to the description of system type for the First Control/Monitor Routes Page screen.

PATH STATUS - Displays the status of the communications path between the local VS and the adjacent system. The three status types that can appear in this field are as follows:

ACTIVE - Indicates that the CNS switching layer on the local VS has successfully exchanged XID commands with the CNS switching layer on the adjacent system.

INACTIVE - Indicates that the CNS switching layer on the local VS and the switching layer on the adjacent system have not exchanged XID commands. Communications cannot take place across the path until XID commands are successfully exchanged.

PENDING - Indicates that the CNS switching layer on the local VS has sent an XID command to the switching layer on the adjacent system. The switching layer on the local VS is waiting to receive an XID acknowledgment from the adjacent system.

PATH COST - Displays the path cost of the route between the local VS and the destination system by way of the adjacent system. The path cost was entered when WSNEDIT was run to configure routes (refer to Chapter 5 of the WSN VS Network Configuration Guide). Path cost is dynamically updated as network congestion and connectivity change.

PATH REJECTS - Displays the number of messages that could not be delivered to the destination system by way of the adjacent system. Whenever a path reject occurs during a session, the session is automatically terminated.

Several PF keys appear by name at the bottom of the screen. These keys appear throughout WSNMON and are described in Chapter 1.

You can position the cursor next to the ID of an adjacent system and press ENTER to display a list of transports that lead to the adjacent system. The local VS uses these transports to communicate with a destination system by way of an adjacent system. The transports were defined when WSNEDIT was run to create the communications configuration for the local VS (refer to Chapter 4 of the WSN VS Network Configuration Guide). The screen in Figure 5-5 appears when you display transports.

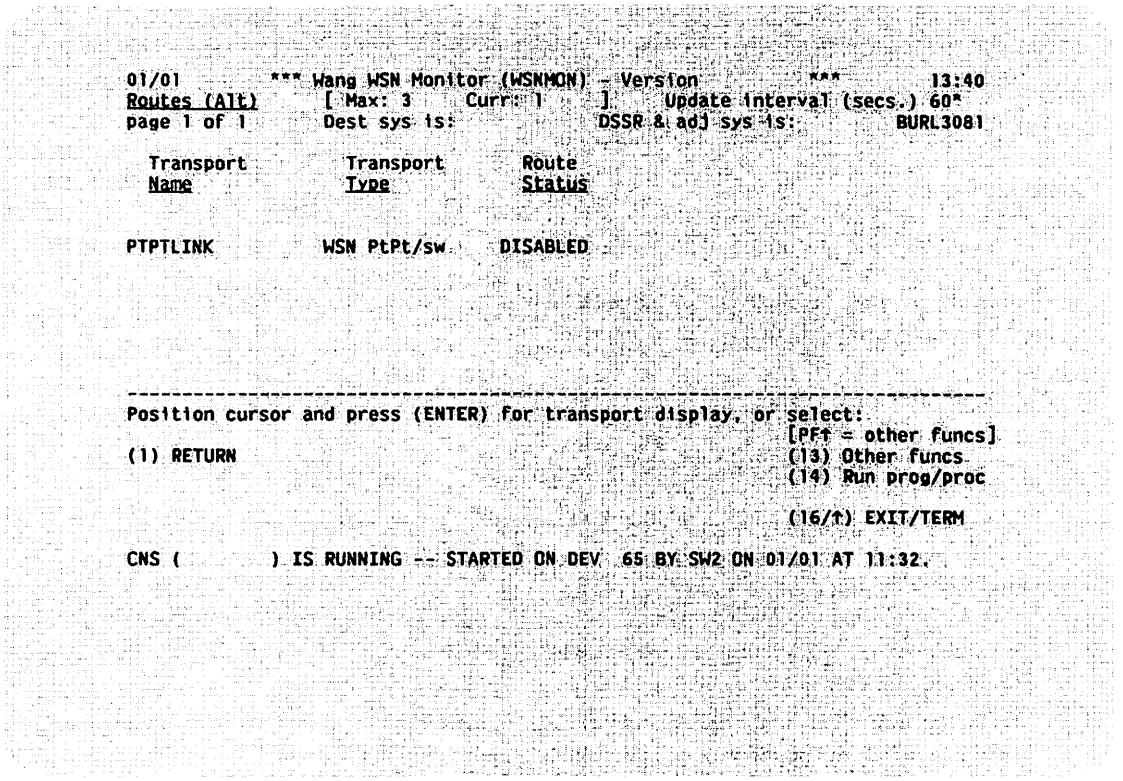

Figure 5-5. Transports to Adjacent Systems Menu

The local VS uses the transports listed on the Transports to Adjacent Systems Menu to send messages to and receive messages from the adjacent system. The top of the menu displays the maximum and current number of transports that can connect the local VS and the adjacent system. The top of the menu also displays the name of the destination system to which messages will be routed by way of the adjacent system. Like other WSNMON screens, the menu allows you to modify the update interval.

The fields that display transport information are as follows:

TRANSPORT NAME - Displays the name of the transport as defined in the local-view configuration file when WSNEDIT was run (refer to Chapter 4 of the WSN VS Network Configuration Guide).

TRANSPORT TYPE - Displays the type of transport.

ROUTE STATUS - Displays the status of the route. The three status types are as follows:

Active - A transport connection is currently established to the adjacent system across the transport.

Inactive - The transport is enabled (i.e., capable of establishing a transport connection) but is not currently supporting a transport connection to the adjacent system.

Disabled - The transport is not capable of supporting a transport connection. To enable the transport, you must access the Control/Monitor Transports function. Refer to Chapter 2 for more information on this function.

Several PF keys are named at the bottom of the menu. These keys appear throughout WSNMON and are described in Chapter 1.

You can position the cursor next to the transport ID and press ENTER to display the Transport Summary screen (Figure 2-2) for that transport. Chapter 2 describes transport specific information that can be viewed using WSNMON.

CHAPTER 6
CONTROL/MONITOR CNS

6.1 INTRODUCTION

The Control/Monitor CNS function displays the general status of CNS. The general status includes information on the number of transports defined, the number of applications attached to CNS, and the number of sessions currently established as well as the number of messages sent, received and that have passed through the local system. There is also information on CNS buffers, the number of areas, and the number of systems in the network.

You can also start CNS and terminate CNS through the Control/Monitor CNS function.

6.2 USING THE MONITOR CNS FUNCTION

To access the Monitor CNS function, press PF9 from the WSNMON Main menu. The Monitor CNS screen appears, as shown in Figure 6-1.

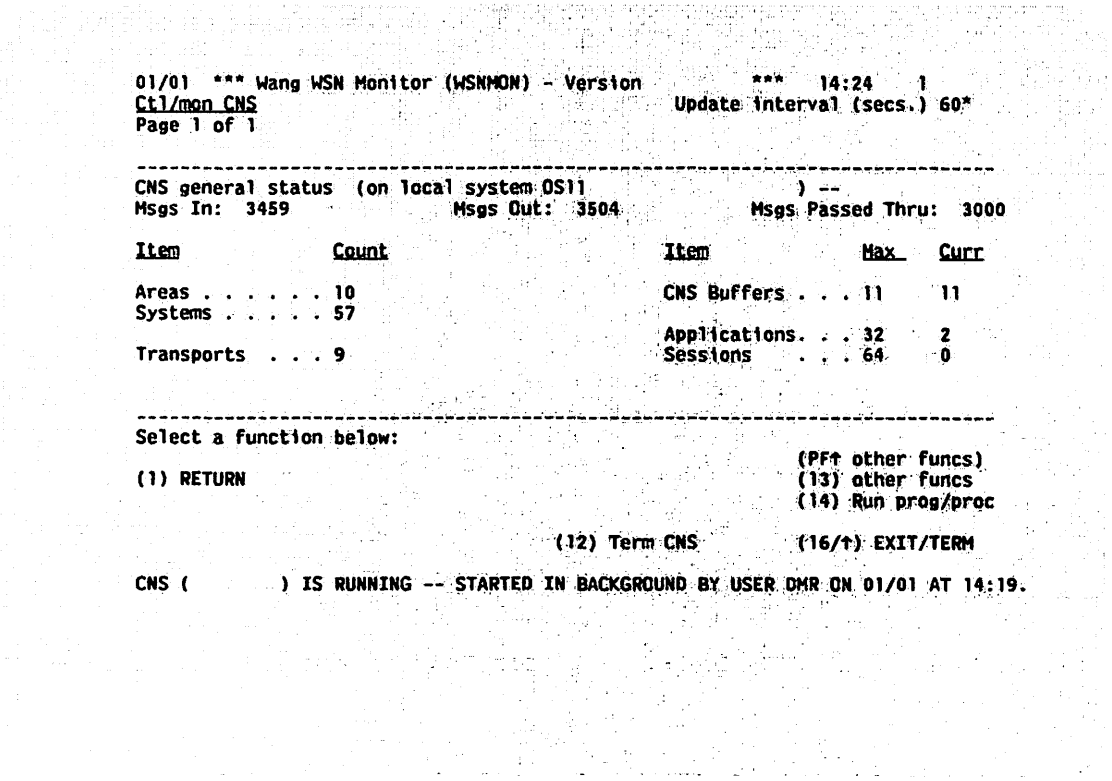

Figure 6-1. Monitor CNS Screen

The Monitor CNS screen displays the only page of CNS activity information. The fields that appear on the screen are described in the following listing:

INTERVAL - Refer to Chapter 1 for information on this field.

TRANSPORTS (COUNT) - Displays the maximum number of transports that the version of CNS running can support.

APPLICATIONS (MAX) - Displays the maximum number of applications that can attach to CNS.

APPLICATIONS (CURR) - Displays the current number of applications attached to CNS.

SESSIONS (MAX) - Displays the maximum number of sessions that CNS can support.

SESSIONS (CURR) - Displays the number of sessions currently established.

CNS BUFFERS (MAX)- Whenever a module within CNS attempts to send a message to another module, the sending module must submit a request to CNS to allocate buffer or memory space to format the message. When the message is received, the receiving module can retain that buffer space to send a reply or release the buffer space back to CNS. If a module attempts to send a message and no buffer space is available, the module must wait until space is available. This field displays the maximum number of buffers that have been concurrently allocated (one buffer represents the amount of memory needed to format a message).

CNS BUFFERS (CURR) - Displays the number of buffers that are currently available.

AREAS (COUNT) - Displays the number of areas defined in the network directory. These areas are defined through WSNEDIT.

SYSTEMS (COUNT) - Displays the number of systems defined in the network directory. These systems were defined through WSNEDIT.

MSGS IN - Displays the number of messages the system has received since CNS was last initialized.

MSGS OUT - Displays the number of messages the system has sent since CNS was last initialized.

MSGS PASSED THROUGH - Displays the number of messages that have passed through the system since CNS was last initialized. These messages were routed on behalf of other systems.

The following PF keys are named at the bottom of the Monitor CNS screen.

PF11 (START CNS) - If the CNS task is not running, you can press PF11 to start the CNS task.

PF12 (TERM CNS) - If the CNS task is running, you can press PF12 to terminate CNS.

PF1, ↑, 13, 14, 16 - Refer to Chapter 1 for an explanation of these PF keys.

CHAPTER 7
DIAGNOSTICS

7.1 INTRODUCTION

WSNMON allows you to run several diagnostic programs. Once you have specified the appropriate parameters, these programs attach to CNS and initiate sessions with a peer application known as PASSTEST at a user-specified remote system. PASSTEST is identified as DIAG1 when you view it attached to CNS through the Monitor Applications function. The remote system starts PASSTEST automatically when contacted by one of the diagnostic programs. These programs then perform their respective diagnostic functions. The diagnostic programs are summarized in the following list:

THRUTEST - Measures the data transfer rate in bits/second between two systems.

PROPTEST - Measures the propagation delay for data transfer between systems. The propagation delay is the amount of time it takes to transmit a message to a remote system and back to the originating system. When this program is run, the local system sends one message to a remote system where the message passes through CNS to PASSTEST, then back through CNS to the originating system.

SYNCTEST - Measures the accuracy of data transferred between two systems. When SYNCTEST is run, messages are sent to PASSTEST at the remote system, which returns each message it receives to the orginating system. A comparison is then made at the originating system between the messages originally sent and the messages returned. The originating system can then detect inconsistencies between the two sets of messages, thereby determining message integrity.

CONECTST - Determines the remote systems running CNS in the network and attempts to connect to PASSTEST on each.

7.2 USING THE DIAGNOSTICS FUNCTION

To access the Diagnostics function, press PF3 while viewing the WSNMON Main menu. The Diagnostics screen appears, as illustrated in Figure 7-1.

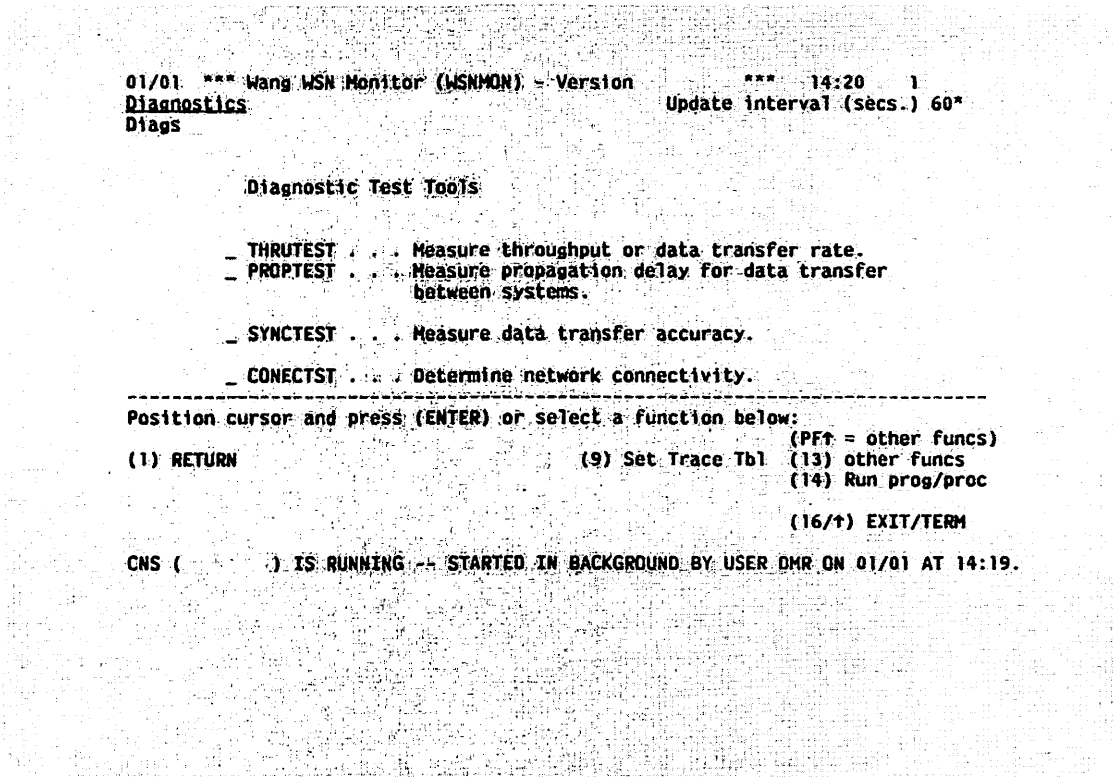

Figure 7-1. The Diagnostics Screen

The Diagnostics screen lists several diagnostic programs. Each diagnostic program can be accessed through the Diagnostics screen, but is independent of WSNMON. To run a diagnostic program, position the cursor next to the name of the appropriate program. Press ENTER (or PF14), type in the program name and the library and volume on which it resides, and press ENTER. You then must enter certain parameters that the program requires. In the sections that follow, these parameters are described for each program.

The following PF keys are mentioned at the bottom of the Diagnostics screen.

PF1, ↑, 13, 14, 16 - Refer to Chapter 9 for an explanation of these PF keys.

PF9 - Allows you to access the WSNMON Trace Table function. Refer to Chapter 16 for a description of this function.

Using THRUTEST

The first screen that appears when you run THRUTEST is shown in Figure 7-2.

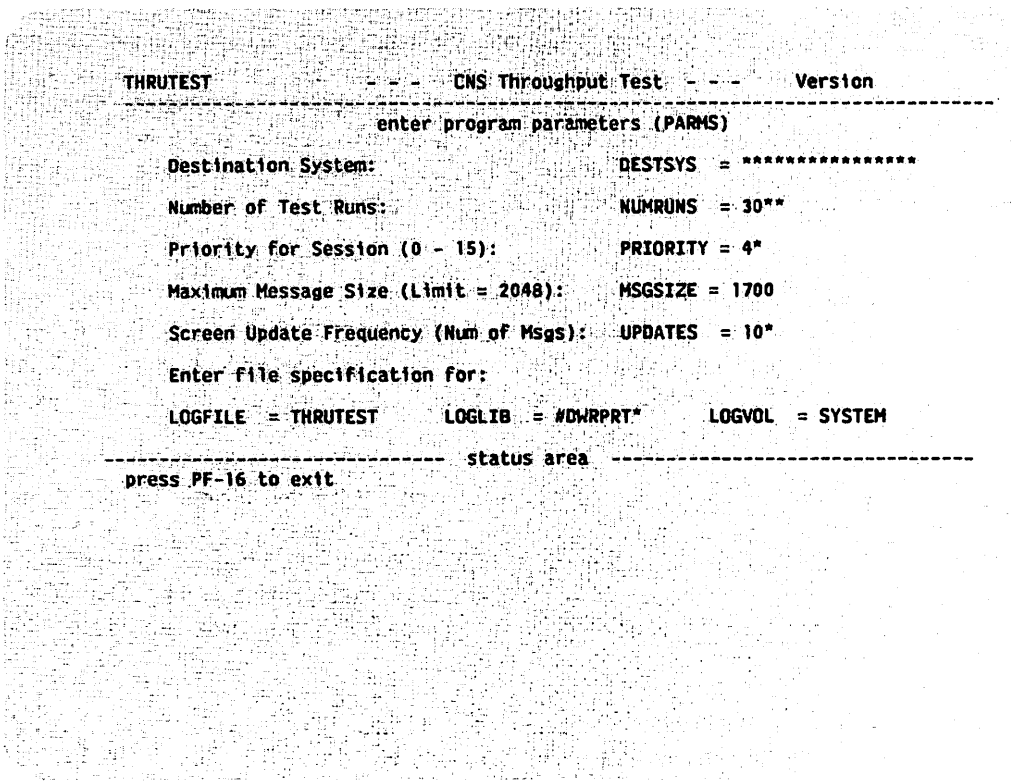

Figure 7-2. THRUTEST Parameters Screen

The THRUTEST Parameters screen allows you to enter the parameters the program requires to measure the data transfer rate between the local system and a remote system. You must enter these parameters before THRUTEST can make test runs. To delete characters from these fields, position the cursor under the character you wish to delete and press the DELETE key.

DESTSYS - Enter the name of the remote system. The name must be one that was defined in the network directory when WSNEDIT was run to define areas and systems in the network (refer to WSN VS Network Configuration Guide, Chapter 3).

NUMRUNS - Enter the number of test runs you want THRUTEST to make. In effect, this number will be the number of times THRUTEST will measure the rate of data transfer between two systems. The accuracy of the test results tend to increase as the number of test runs increase. To obtain meaningful results, you should specify at least 30 runs. (Do not specify 0 runs.)

PRIORITY - ENTER the priority window value to be assigned to the THRUTEST session. CNS uses priority windows to manage sessions. Sessions with lower priority window values are given greater access to the network than sessions with higher priority window values. The THRUTEST test runs tend to be faster if they are assigned lower priority window values. The lowest valid priority window value that can be assigned is 0; the highest is 15. Enter the default value 4 or specify another valid priority window value.

MSGSIZE - Enter the message size (in bytes) to be allocated to the THRUTEST session. The message size is the maximum amount of memory CNS will use to format a message that THRUTEST will transmit to the remote system. The message size can be no larger than 2048 bytes (2K). The MSGSIZE field determines the size of the message transmitted to the remote system.

UPDATES - THRUTEST displays the number of the message being sent at intervals you specify in this field. For example, if you enter 1 in this field, THRUTEST will display the number of every message as it is sent (1, 2, 3 etc.). If you enter the default value 10, THRUTEST will only display the number of every tenth message as it is sent (10, 20, 30 etc.).

LOGFILE - Enter the name of the VS print file in which THRUTEST results will be stored. You can use the default name THRUTEST or specify another file.

LOGLIB - Enter the name of the library in which you want the log file to reside. You can use the default library (your VS print file library) or specify another valid library.

LOGVOL - Enter the name of the volume on which your log library resides. The default volume is the system volume.

Press ENTER when you have specified the parameters required to run THRUTEST. A series of messages appear on the screen after you press ENTER. These messages give you the following information:

- THRUTEST is attaching to the network (i.e., CNS).
- An attempt is being made to open a session with the PASSTEST program at the remote system.
- The open attempt has succeeded or failed. If the open attempt does not succeed, an error message is displayed that tells you the reason for the open attempt failure. You then must press ENTER to continue. The THRUTEST Statistics screen appears, allowing you to exit from THRUTEST or run the program again.
- Test runs are in progress.

- Test runs have been completed and an attempt is being made to close the session with the THRUTEST program at the remote system. An attempt is also being made to detach from the network (i.e., CNS).

Once the test runs have been completed, a screen appears displaying the statistics gathered during testing. The same screen also appears if the THRUTEST program at the remote system could not be contacted and ENTER is pressed to continue. This screen is shown in Figure 7-3.

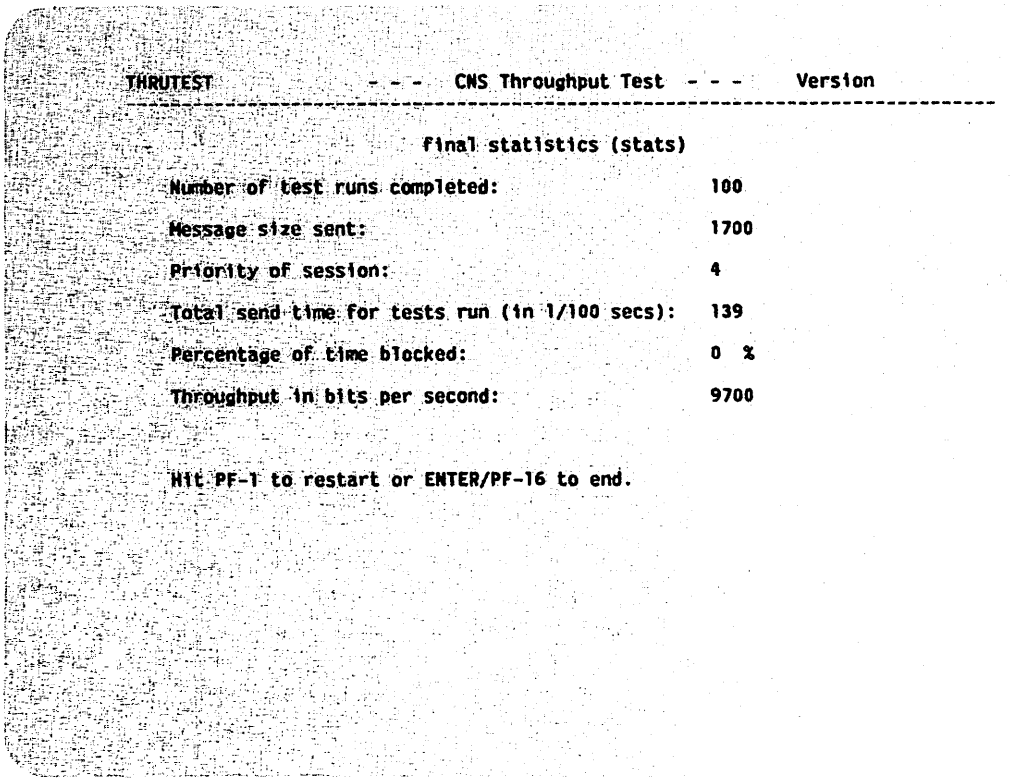

Figure 7-3. THRUTEST Statistics Screen

The statistics THRUTEST gathers during testing are as follows:

Number of test runs - Displays the number of test runs made during testing. If this number does not match the number of runs you entered on the THRUTEST Parameters screen, an error has occured during testing.

Message size sent - This field should display the value that you entered in the MSGSIZE field on the THRUTEST Parameters screen. If it does not, an error has occurred.

Priority of session - This field should display the priority window value you assigned on the THRUTEST Parameters screen. If it does not, an error has occurred.

Total send time for tests run (in 1/100 secs) - Displays the time it took to send the messages during the test runs.

Percentage of time blocked - This figure represents the percentage of send time in which messages could not be sent due to network congestion.

Throughput in Bits Per Second - Displays the effective data transfer rate between the THRUTEST on the local system and PASSTEST on the remote system. The effective data transfer rate will in most cases be less than the maximum line speed supported. The maximum line speed supported reflects the modem-to-modem data transfer rate. The value that appears in this field is the application-to-application data transfer rate.

When you have finished viewing the information on the THRUTEST Statistics screen, you can press PF1 to run THRUTEST again or PF16 to return to the Diagnostics screen.

Using PROPTEST

The first screen that appears when you run PROPTEST is almost identical to the THRUTEST Parameters screen. This screen is called the PROPTEST Parameters screen. The PROPTEST Parameters screen allows you to enter the parameters the program requires to measure the propagation delay between the local system and a remote system (refer to the introductory section for an explanation of propagation delay).

You must enter these parameters in the fields on the PROPTEST Parameters screen before PROPTEST can make test runs. The fields on this screen are the same as the fields on the THRUTEST Parameters screen. To delete characters from these fields, position the cursor under the character you wish to delete and press the DELETE key. Refer to the Using THRUTEST section for more information on these fields.

Press ENTER when you have specified the parameters required to run PROPTEST. A series of messages appear on the screen after you press ENTER. These messages give you the following information:

- PROPTEST is attaching to the network (i.e., CNS).
- An attempt is being made to open a session with the PASSTEST program at the remote system.
- The open attempt has succeeded or failed. If the open attempt does not succeed, an error message is displayed that tells you the reason for the open attempt failure. You then must press ENTER to continue. The PROPTEST Statistics screen appears, allowing you to press PF16 to exit from PROPTEST or press PF1 to run the program again.
- Data is being sent to the remote system.

- Test runs have been completed and an attempt is being made to close the session with the PROPTEST program at the remote system. An attempt is also being made to detach from the network (i.e., CNS).

Once the test runs have been completed, a screen appears displaying the statistics gathered during testing. The same screen also appears if the PROPTEST program at the remote system could not be contacted and ENTER is pressed to continue. This screen is shown in Figure 7-4.

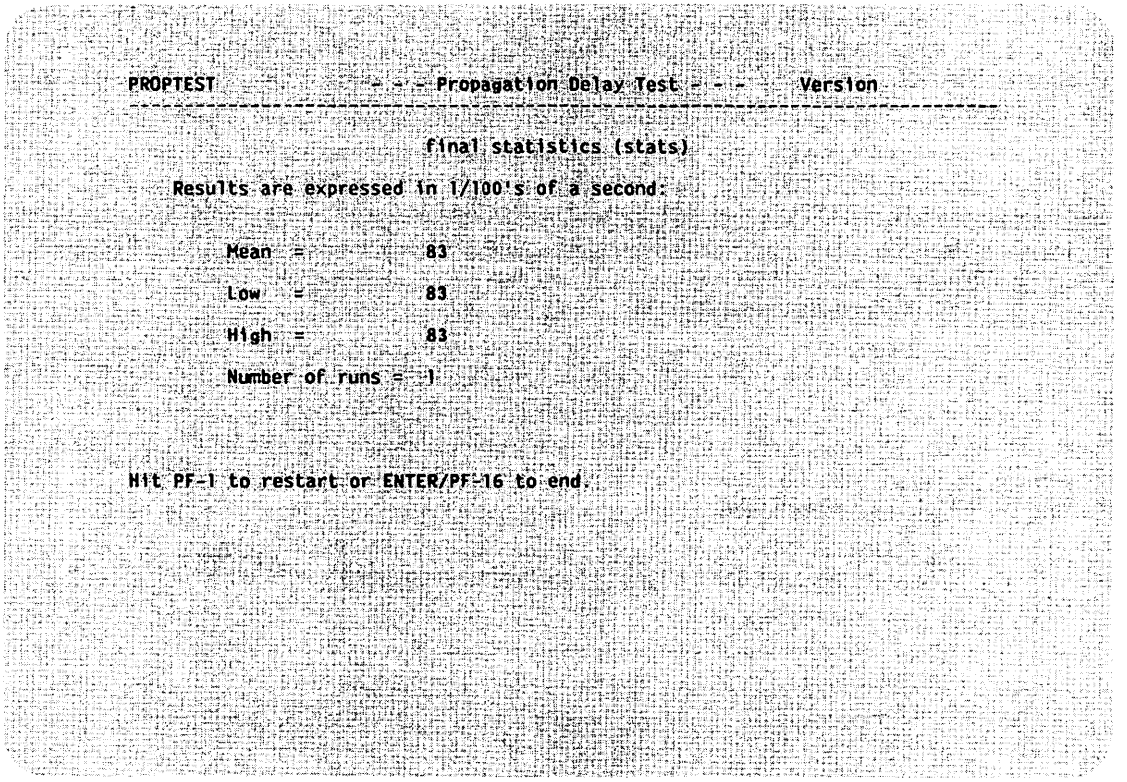

Figure 7-4. PROPTEST Statistics Screen

The statistics PROPTEST gathers during testing are described in the following listing:

Mean - Displays the average period (in 1/100s of a second) of time it took for a message to travel to the remote system and back.

Low - Displays the shortest period of time (in 1/100s of a second) it took for a message to travel to the remote system and back.

High - Displays the longest period of time (in 1/100s of a second) it took for a message to travel to the remote system and back.

Number of runs - This field should display the same number of runs you specified on the PROPTEST Parameters screen. If these two numbers do not match, there has been an error in testing.

When you have finished viewing the information on the PROPTEST Statistics screen, press PF1 to run PROPTEST again or PF16 to return to the Diagnostics screen.

Using SYNCTEST

SYNCTEST performs a series of comparisons to determine whether or not messages are formatted correctly and are received in the proper sequence. When a SYNCTEST message is formatted prior to being sent, each byte in the message is numbered. When PASSTEST returns the message to the local system, the bytes must be received in order as originally numbered. For example, bytes labelled 1, 2, and 3 respectively should be received in numerical order. If the bytes are not received in the right order or one or more of them is missing, SYNCTEST records the error as a "miscompare".

The messages themselves must also be received in the proper sequence. Each message is uniquely identified by the number of bytes it contains and is sent to PASSTEST at the remote system in sequence with other messages according to that number. These messages must then be returned in the proper sequence.

The first message SYNCTEST sends contains one byte; the next message contains two bytes; the third message contains three bytes; and so on until the buffer size is reached. If the messages are not received in the right sequence or one or more of them is missing, SYNCTEST records the error as a miscompare.

The first screen that appears when you run SYNCTEST is shown in Figure 7-5.

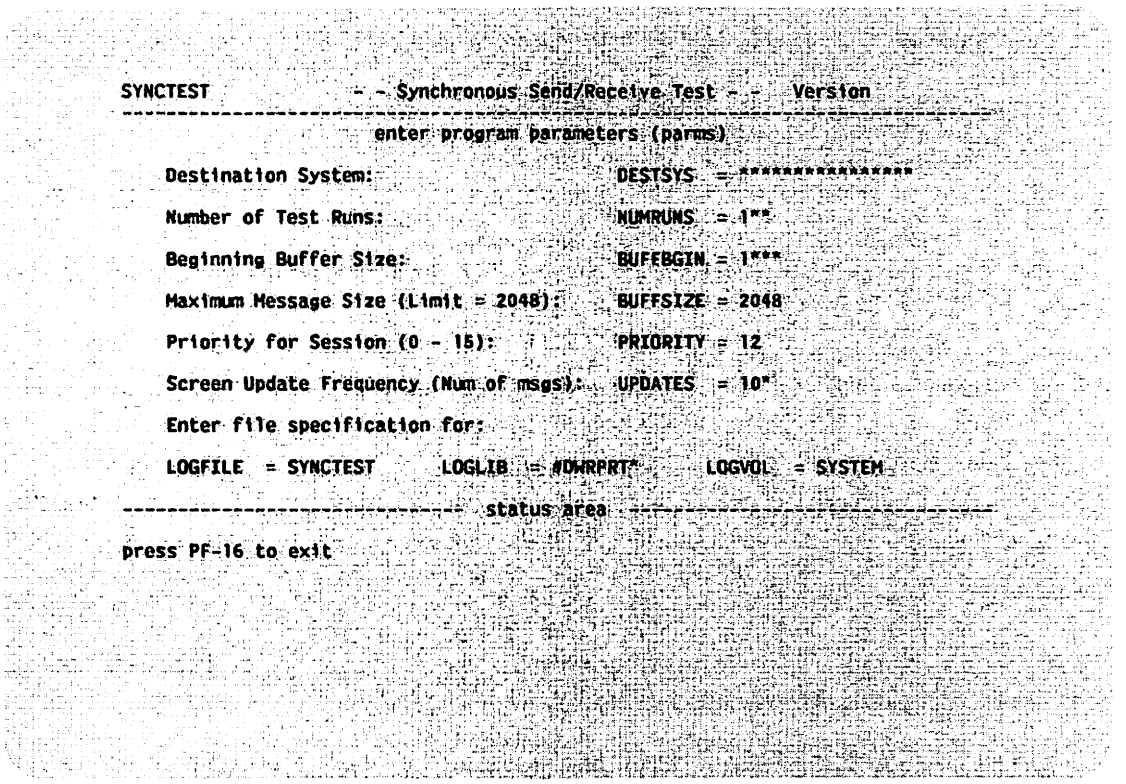

Figure 7-5. SYNCTEST Parameters Screen

The SYNCTEST Parameters screen allows you to enter the parameters the program requires to determine the integrity of data transferred between two systems. You must enter these parameters in the fields on the SYNCTEST Parameters screen before SYNCTEST can make test runs. To delete characters from these fields, position the cursor under the character you wish to delete and press the DELETE key.

The fields on the SYNCTEST Parameters screen are described in the following listing:

DESTSYS - Enter the name of the remote system. The name must be the one that was defined in the network directory when WSNEDIT was run to define areas and systems in the network (refer to Chapter 3).

NUMRUNS - Enter the number of test runs you want SYNCTEST to make. In effect, this number will be the number of times SYNCTEST will measure the integrity of data transferred between two systems. Do not specify 0 runs.

NOTE

The number of times that SYNCTEST measures data integrity is caluculated using the following formula: (BUFFSIZE Value - BUFFBGIN Value) x NUMRUNS Value = Number of times data integrity is measured.

BUFFBGIN - This field allows you to set the minimum size buffer to be sent.

BUFFSIZE - This field allows you to set the maximum size buffer to be sent.

PRIORITY - ENTER the priority window value to be assigned to the SYNCTEST session. CNS uses priority windows to manage sessions. Sessions with lower priority window values are given greater access to the network than sessions with higher priority window values. The SYNCTEST test runs tend to be faster if they are assigned lower priority window values. The lowest valid priority window value that can be assigned is 0; the highest is 15. Enter the default value 12 or specify another valid priority window value.

UPDATES - SYNCTEST displays the number of the message being sent at intervals you specify in this field. For example, if you enter 1 in this field, SYNCTEST will display the number of every message as it is sent (1, 2, 3 etc.). If you enter the default value 10, SYNCTEST will display the number of every tenth message as it is sent (10, 20, 30 etc.).

LOGFILE - Enter the name of the VS print file in which SYNCTEST results will be stored. You can use the default name SYNCTEST or specify another file.

LOGLIB - Enter the name of the library in which you want the log file to reside. You can use the default library (your VS print file library) or specify another valid library.

LOGVOL - Enter the name of the volume on which your log library resides. The default volume is the system volume.

Press ENTER when you have specified the parameters required to run SYNCTEST. A series of messages appear on the screen after you press ENTER. These messages give you the following information:

- SYNCTEST is attaching to the network (i.e., CNS).
- An attempt is being made to open a session with the SYNCTEST program at the remote system.

- The open attempt has succeeded or failed. If the open attempt does not succeed, an error message is displayed that tells you the reason for the open attempt failure. You then must press ENTER to continue. The SYNCTEST Statistics screen appears, allowing you to press PF16 to exit from SYNCTEST or press PF1 to run the program again.

- Test runs are in progress.

- Test runs have been completed and an attempt is being made to close the session with the SYNCTEST program at the remote system. An attempt is also being made to detach from the network (i.e., CNS).

Once the test runs have been completed, a screen appears displaying the statistics gathered during testing. The same screen also appears if the SYNCTEST program at the remote system could not be contacted and ENTER is pressed to continue. This screen is shown in Figure 7-6.

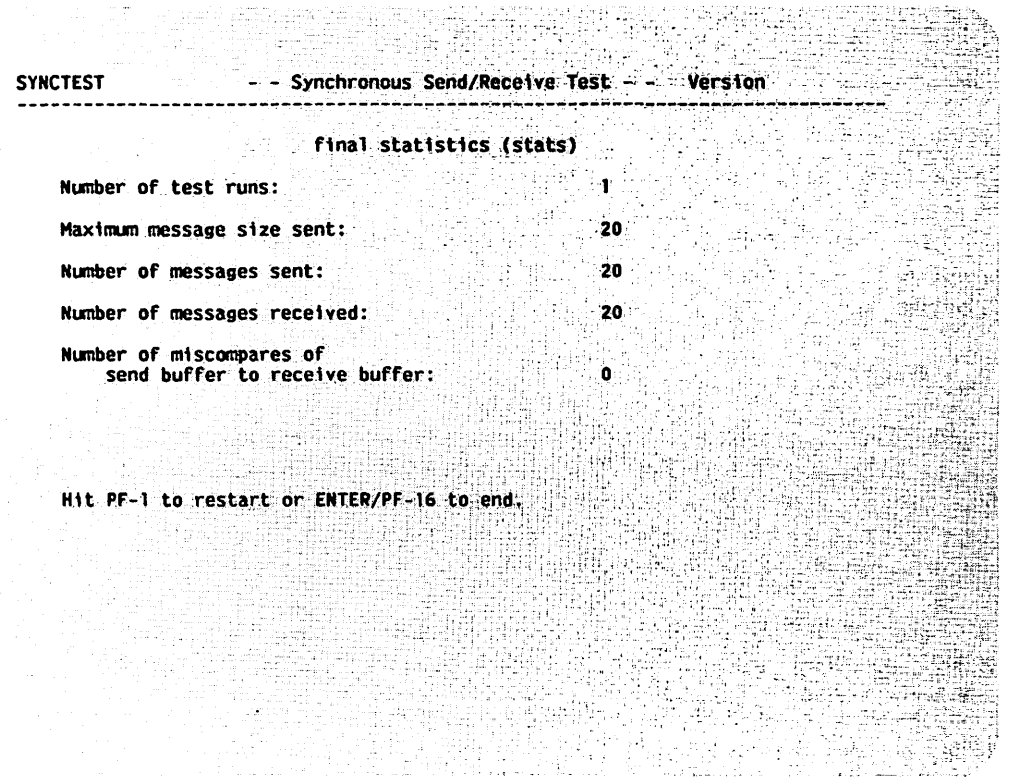

Figure 7-6. SYNCTEST Statistics Screen

The statistics SYNCTEST gathers during testing are described in the following listing:

Number of test runs - This field should display the number of test runs you specified in the NUMRUNS field on the SYNCTEST Parameters screen. An error in testing has occurred if the number of test runs does not match the value entered in the NUMRUNS field.

Maximum message size sent - This field should display the value you entered in the BUFFSIZE field on the SYNCTEST Parameters screen. An error in testing has occurred if the value in this field does not match the value entered in the BUFFSIZE field.

Number of messages sent - This field should display the number of messages (i.e., buffers) sent to the remote system. An error has occurred if the value in this field is not as given by the following formula:

(BUFFSIZE Value - BUFFBGIN Value) x NUMRUN Value

Number of messages received - This field should display the same value that is displayed in the Number of messages sent field. If it does not, an error has occurred.

Number of miscompares of message sent to message received - Displays the number messages that were received incorrectly.

When have finished viewing the information on the SYNCTEST Statistics screen, you can press PF1 to run SYNCTEST again or PF16 to return to the Diagnostics screen.

Using CONECTST

CONECTST determines the systems in the network the local system can contact. You can run CONECTST to attempt to contact any of the systems in the network or in a specific area, or to attempt to contact any of the systems from a list of systems you create in a VS source file. CONECTST allows you to create this file.

To run CONECTST, position the cursor under the selection block next to CONECTST and press ENTER. The First CONECTST screen appears, as illustrated in Figure 7-7.

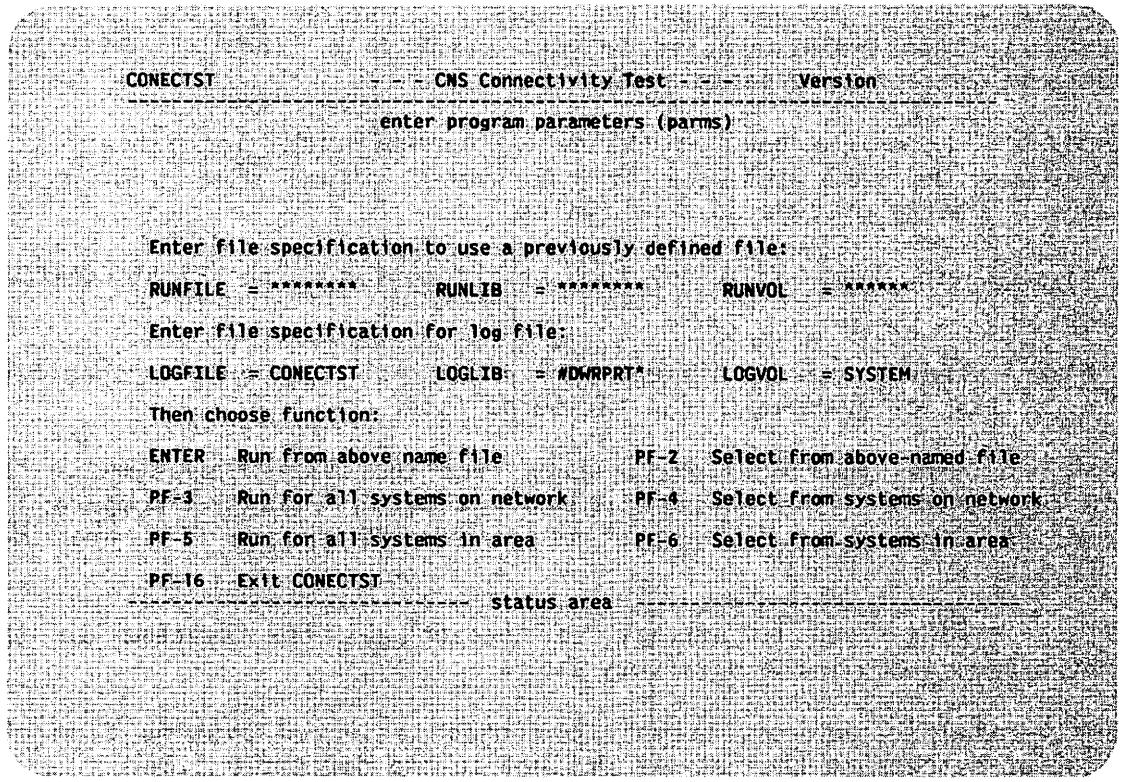

Figure 7-7. First CONECTST Screen

The First CONECTST screen allows you to specify whether or not the list of systems the local system will attempt to contact is stored in a VS source file or the directory file. If the list of systems is stored in a VS source file, specify the appropriate information in the following fields:

RUNFILE - Enter the name of the VS source file in which the list is stored.

RUNLIB - Enter the name of the library in which the VS source file resides.

RUNVOL - Enter the name of the volume on which the library specified in the RUNLIB field resides.

You specify information in the following fields regardless of your choice of files (VS source or directory):

LOGFILE - Enter the name of the file in which CONECTST statistics are to be stored. The name defaults to CONECTST. Enter the default setting or type in a new file name.

LOGLIB - Enter the name of the library in which the log file will reside. This field defaults to your print file library. Enter the default setting or type in a new value.

LOGLIB - Enter the name of the library in which the log file will reside. This field defaults to your print file library. Enter the default setting or type in a new value.

LOGVOL - Enter the name of the volume on which the log library will reside. The name defaults to the system volume name. Enter the default settng or type in a new value.

The following keys appear by name at the bottom of the First CONECTST screen.

ENTER - Enables you to attempt to contact all the systems specified in the list of systems in the VS source file.

PF2 - Enables you to select systems from the list of systems in the VS source file. The entire directory file is read and compared to the VS source file. The systems in the VS source file are then preselected.

PF3 - Enables you to attempt to contact all the systems in the network defined in the directory file.

PF4 - Enables you to attempt to contact selected systems from the list of systems in the network defined in the directory file.

PF5 - Enables you to attempt to contact all the systems in your area defined in the directory file.

PF6 - Enables you to attempt to contact selected systems in your area defined in the directory file.

PF16 - Returns you to the Diagnostics screen.

If you press ENTER, PF3, or PF5, the CONECTST Status screen appears (refer to Figure 7-9). If you press PF keys 2, 4, or 6, the following screen appears.

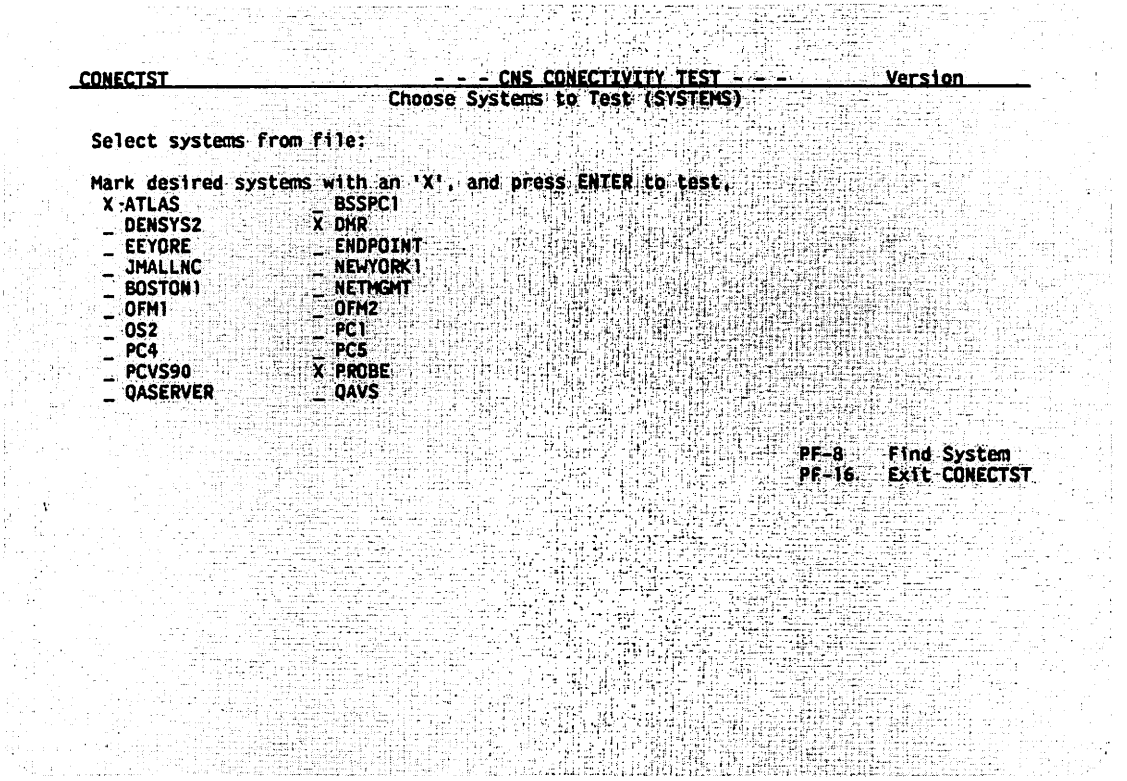

Figure 7-8. Select Systems Screen

The Select Systems screen allows you to select individual systems from a list of systems. If you pressed PF2 from the First CONECTST screen, the systems in the VS source file that correspond to systems in the directory file are marked with an 'X'. If you pressed PF4 from the First CONECTST screen, the list is read from the directory file and is comprised of all the systems in the network. If you pressed PF6 from the First CONECTST screen, the list is read from the directory file and is comprised of all the systems in the local system's area.

Type X next to each system running CNS you wish to attempt to contact. If an X already exists next to a system you do not wish to contact, position the cursor under that X and use the space bar or the DELETE key to remove it.

The following PF keys appear by name at the bottom of the Select Systems screen.

PF2 (First), PF3 (Last), PF4 (Prev), PF5 (Next) - Enable you to scroll through the list of systems when the list consists of more than one screen.

PF8 - Refer to the Common PF keys section in Chapter 9 for an explanation of this key.

PF16 - Enables you to terminate CONECTST.

Press ENTER when you have finished selecting and/or deleting systems from the list. The CONECTST Results screen appears, as illustrated in Figure 7-9.

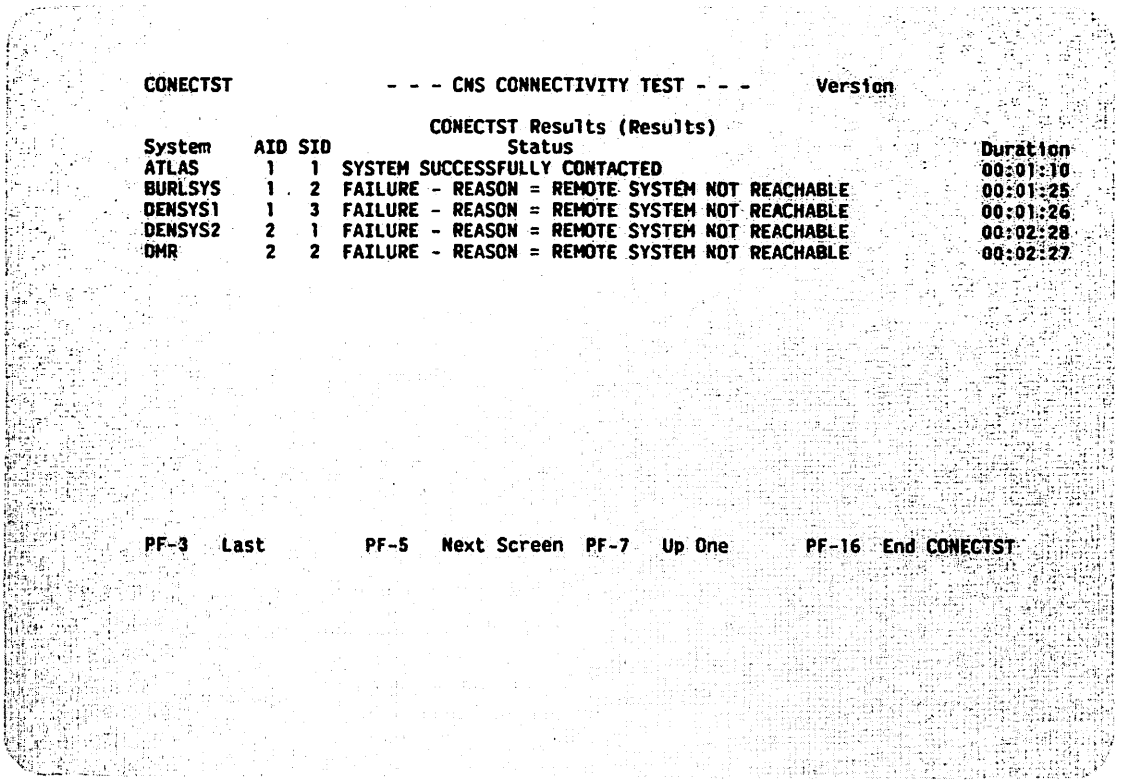

Figure 7-9. CONECTST Results Screen

The CONECTST Results screen lists the names, area IDs, and system IDs of all the systems the local system is attempting to contact. The screen also lists the status of CONECTST's attempt to contact each system. When CONECTST initially attempts to contact remote systems, the message "Initial - Connection attempt beginning" appears in the Status column for each system. This message is eventually replaced by "Open Sent - Waiting for response".

For remote systems that cannot be contacted, a message appears in the Status column for each system explaining why contact is not possible. Refer to the appendix on CNS Log Messages and Reason Codes for an explanation of these messages. For remote systems that can be contacted, a message appears indicating that the system has been successfully contacted.

When a message indicating whether or not a system can be contacted appears, the amount of time it took to attempt to contact that system appears in the Duration field.

When CONECTST has concluded testing, several PF keys appear by name at the bottom of the CONECTST Status screen. These keys are described in the listing that follows:

PF2 (First), PF3 (Last), PF4 (Prev), PF5 (Next) - Enable you to scroll through the list of systems when the list consists of more than one screen.

PF7 (UP ONE) - Allows you to scroll through the list of systems.

PF16 (END CONECTST) - Displays the CONECTST Statistics screen. The CONECTST Statistics screen is shown in Figure 7-10.

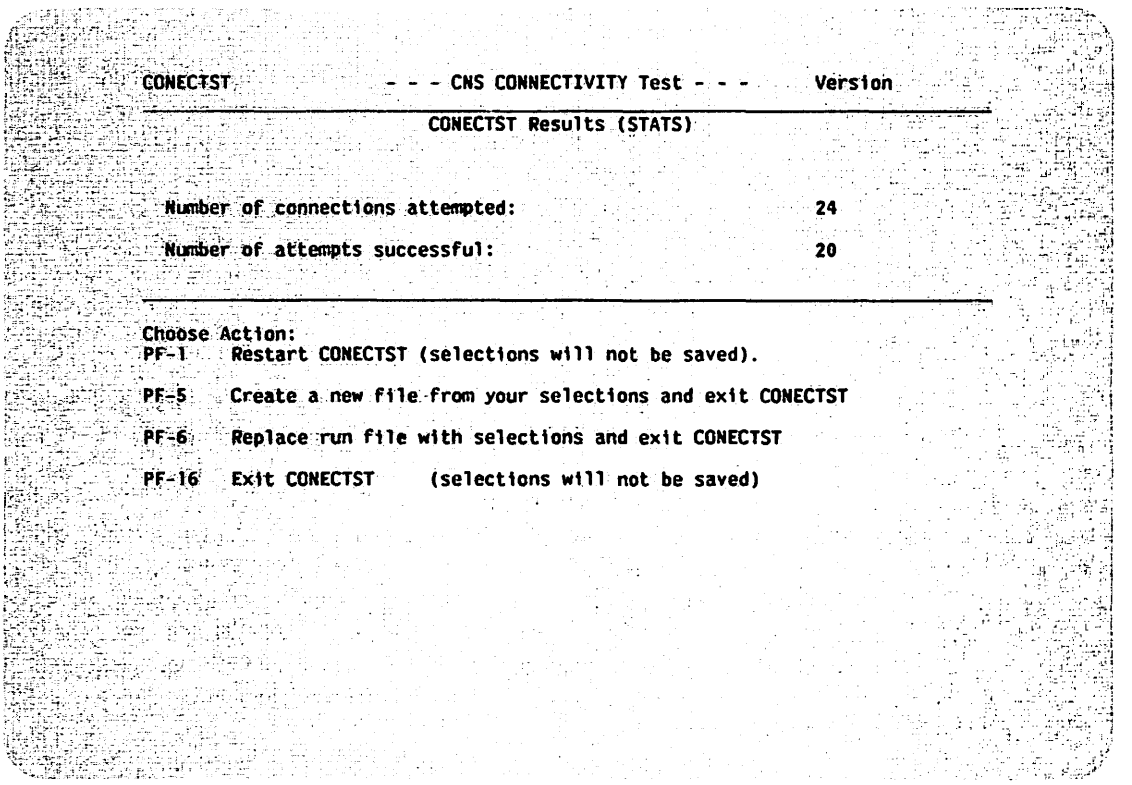

Figure 7-10. CONECTST Statistics and Options Screen

The CONECTST Statistics screen displays the statistics gathered during testing. If systems were read from a VS source file during CONECTST and a system that did not correspond to a system in the directory file was discovered, a message appears on the CONECTST Statistics and Options screen indicating that the source file should be replaced.

The statistics gathered during CONECTST testing are described in the following listing:

Number of Connections Attempted - Displays the number of remote systems CONECTST attempted to contact. CONECTST made one connection attempt to contact each system.

Number of Attempts Successful - Displays the number of systems that could be contacted.

The following keys appear by name at the bottom of the CONECTST Statistics and Options screen.

PF1 - Enables you to run CONECTST again. The First CONECTST screen appears when this PF key is pressed.

PF5 - Enables you to create a new file to store the list of systems you attempted to contact. If you press PF5, a screen appears that asks you to specify the file in which the list of systems is to be saved. CONECTST will automatically create the file once it is specified. You also must specify an existing library and volume in which the file will reside. Press ENTER once you have specified the file, library and volume or press PF1 to cancel the save operation. Pressing ENTER or PF1 returns you to the CONECTST Statistics and Options screen.

PF6 - This PF key appears only if CONECTST attempted to contact systems listed in a VS source file. PF6 enables you to replace the source file with a new file consisting of a list of systems you selected on the Select Systems screen. If PF6 is pressed, a screen appears that asks you to specify the file in which the list of systems is to be saved. CONECTST will automatically create the file once it is specified. You must also specify an existing library and volume in which the file will reside. Press ENTER once you have specified the file, library and volume or press PF1 to cancel the save operation. Pressing ENTER or PF1 returns you to the CONECTST Statistics and Options screen.

PF16 - Enables you to exit from CONECTST without saving the list of systems CONECTST attempted to contact. A screen will appear warning you that the list will not be saved. If you wish to save the list, you can press PF1 to return to the CONECTST Status and Options screen. You can then press the appropriate PF key to save the list. If you do not wish to save the list, you can press PF16 to terminate CONECTST. The Diagnostics screen will appear if PF16 is pressed.

CHAPTER 8
WSNMON TRACE TABLE

8.1 INTRODUCTION

The WSNMON Trace Table function displays the current status of the trace point table. The trace point table is a debugging tool that identifies CNS program modules that exchange internal messages using specific protocols. These messages travel between the various layers of CNS. If the tracing facility is activated, the first 56 bytes of each message that a CNS module sends or receives are stored at a memory address.

The Trace Table function also allows the user to log internal CNS messages into a log file. When one module sends a message to another, the entire message is stored in this log file.

NOTE

The WSNMON Trace Table function is useful only to qualified WANG personnel with a knowledge of CNS internals.

8.2 USING THE TRACE TABLE FUNCTION

To access the Trace Table function, press PF9 from the Diagnostics Screen. The Trace Table screen appears, as shown in Figure 8-1.

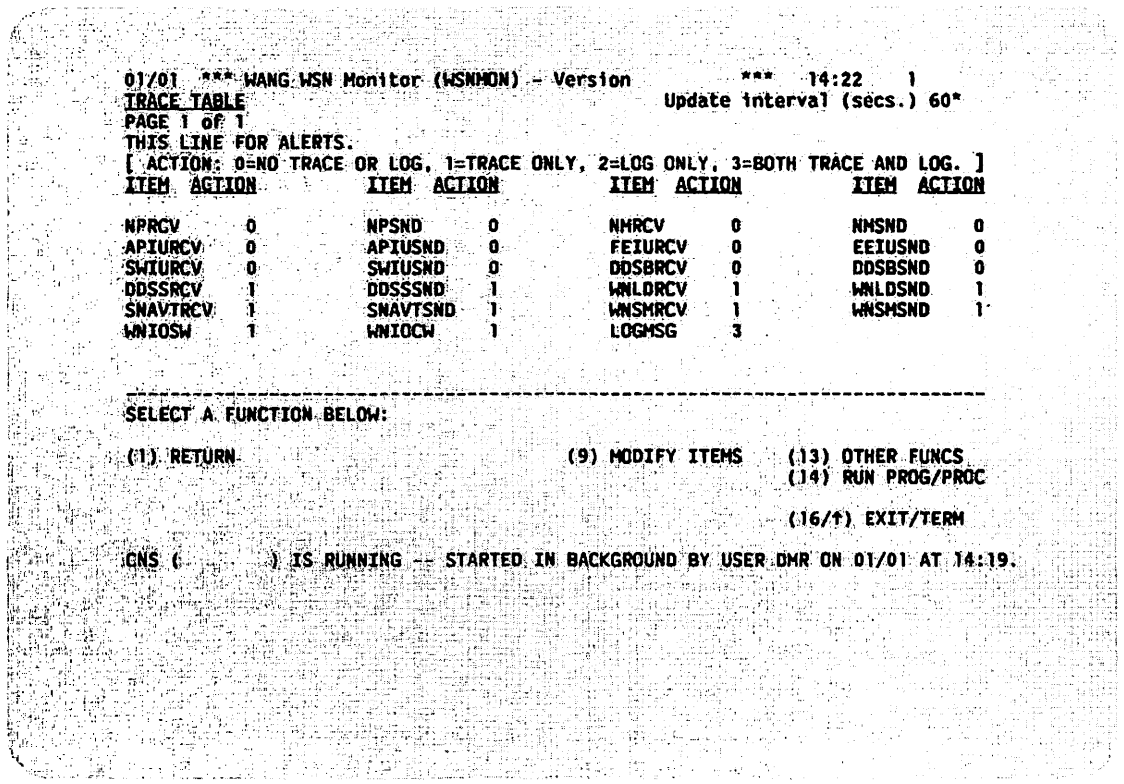

Figure 8-1. Trace Table Screen

The Trace Table screen lists all the CNS modules in the ITEM columns. The ACTION columns list fields that allow the user to specify the action to be taken to monitor a module. To specify an action to be taken on a module, press PF9. All the action fields appear in modify (highlighted) mode. You then enter the appropriate action codes next to the module or modules you wish to monitor and press ENTER. The following listing describes the action codes:

0 (NO TRACE OR LOG) - An action code of 0 means that no action will be taken to monitor the module.

1 (TRACE ONLY) - An action code of 1 means that only a trace will be performed to monitor messages sent from or received by a module. When a trace is performed, you can view the address in memory where the first 56 bytes of a message sent from or received by a module is stored.

2 (LOG ONLY) - An action code of 2 means that messages only get logged (no trace) to a log file (@CNSLOG@).

3 (BOTH TRACE AND LOG) - An action code of 3 means that messages will be both traced and logged.

CAUTION

Entering an action code of 3 (i.e., enabling trace and log) may adversely affect CNS performance.

The listing that follows describes the PF keys mentioned on the Trace Table screen:

PF9 (MODIFY) - Displays the ACTION fields in modify (highlighted) mode. The user can then enter action codes in these fields.

PF1, ↑, 13, 14, 16 - Refer to Chapter 1 for an explanation of these PF keys.

CHAPTER 9
VS OPERATIONAL CONTROL

9.1 INTRODUCTION

This chapter describes the network features listed on the VS Operator's Console menu. These features enable you to control your system links, the Logon and File Transfer service sessions, and your system's transfer queue. For more information on how to use the VS network services, refer to the Network User Guide to VS Systems.

The control functions described in this chapter are listed on the Control Communications screen (see Figure 9-1). To access this screen, press PF12 (Telecommunications) from the VS Operator's Console menu. Network users can access this information through PF8, Manage Communications, but they have no control options.

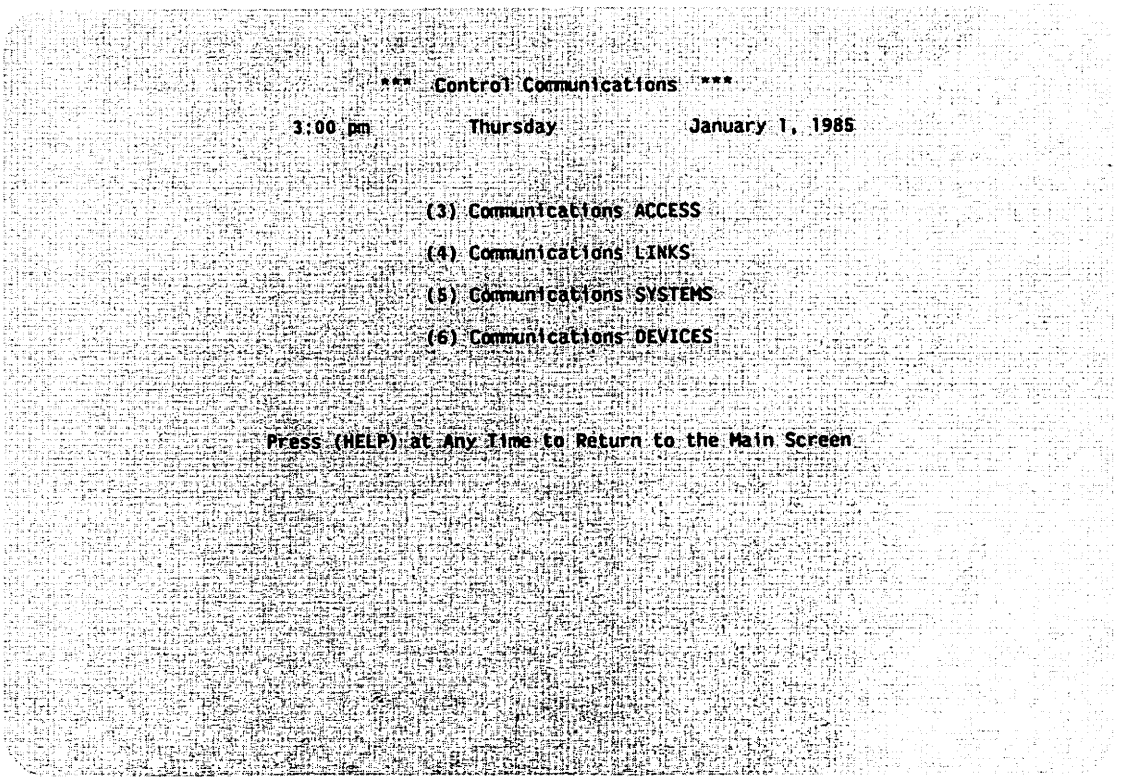

Figure 9-1. Control Communications Screen

Communications Access

To control communications between your system and all other systems, select the Control Communications screen, then press PF3 (Communications Access). You are presented with the following options:

PF2 (Allow Communications) -- Allows all properly configured remote systems access to your VS through either the VS Terminal Emulation Virtual Terminal Interface or the File Transfer service.

PF3 (Inhibit Communications) -- Inhibits any new sessions with your VS. Pressing this key does not affect current users (users who have established active sessions with your system); they can complete their sessions.

PF4 (Inhibit Communications Immediately) -- Causes your system to inhibit any new sessions and stop all current sessions. Sessions that your system interrupts return to their original status. For example, pressing PF4 during a File Transfer session returns the document or file being transferred to the transfer queue of the sending system; it will be transferred the next time a session is established.

After you press the appropriate PF key, the system prompts you to confirm your selection. Press ENTER to confirm your choice.

Communications Links

To control communications with all systems on a specific link or DLP, display the Control Communications screen and press PF4 (Communications Links). The screen displays a list of links on your system, the names of the systems on each link, and the services that each link supports. Press TAB to position the cursor next to the name of the link you want to control and press PF6 (Control Link).

After you press PF6, the screen displays the same options as those described in the previous section, accessed by the same PF keys. However, pressing any of the PF keys affects communications only on the link you selected.

Communications Systems

To access Communications Systems, press PF17. This option lets you monitor and control communications services between your VS and a specific remote system. Section 9.3 describes this option.

Communications Devices

To display the status of a specific Data Link Processor (DLP), press PF6 (Communications Devices). If the DLP is not running, either a blank space occupies the Status field or the DLP type is displayed (TCB1 or CIU). If the DLP is active, its status appears as "Reserved and in use". The control path for each DLP uses the lowest device number. Your VS should label it "Reserved".

Move the cursor to the device number of the DLP you want to control and press the appropriate PF key. The PFkeys (6 through 10, and 13) do not apply to DLPs. The following PF keys and their assignments apply to this screen.

PF2 (FIRST) -- Displays the first screen of your system's DLP list.

PF3 (LAST) -- Displays the last screen of your system's DLP list.

PF4 (PREV) -- Displays the previous screen of your system's DLP list.

PF5 (NEXT) -- Displays the next screen of your system's DLP list.

9.2 CONTROLLING SELECTED COMMUNICATIONS SERVICES

The communications services that your VS supports include document and File Transfers and inbound Logons (logons to your VS). When connected to another VS, your system also supports outbound Logon service. When you display the Control Communications screen and press PF5 (Communications Systems), the system displays the Control Communications Systems screen, as shown in Figure 9-2.

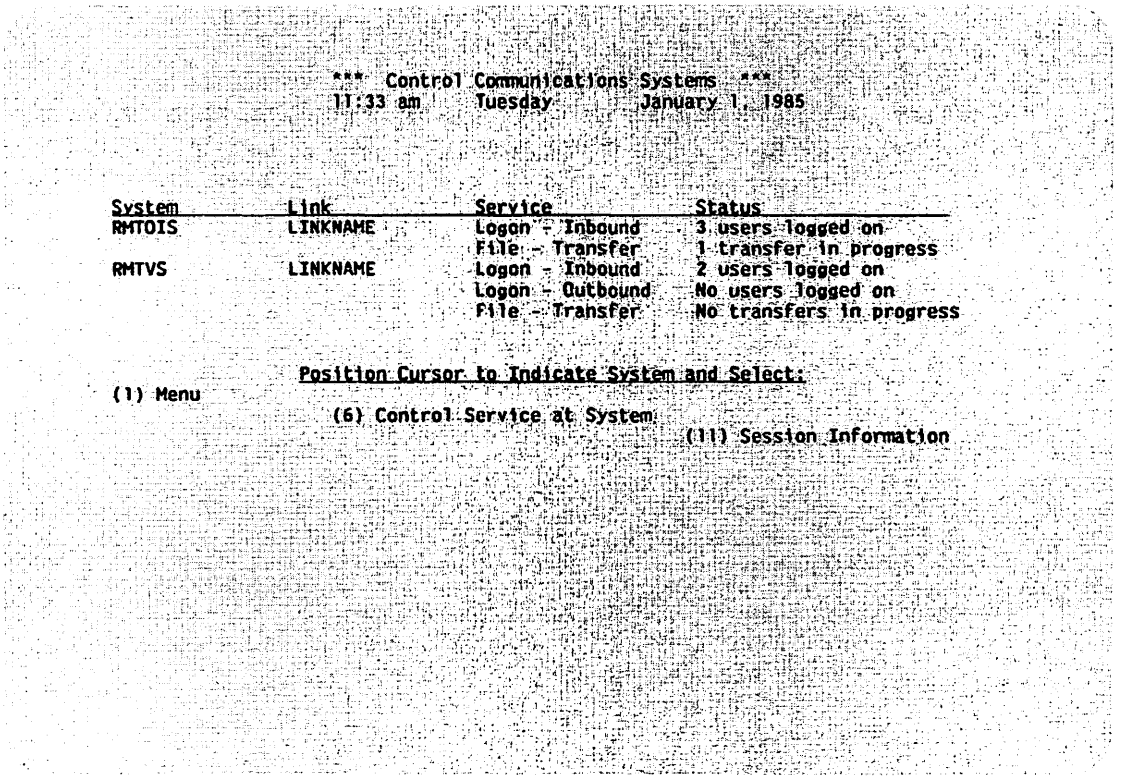

Figure 9-2. Control Communications Systems Screen

Under the first column heading, System, this screen lists the name of each system. The second column, labeled Link, lists the name of the link through which you can access the particular system. The third column, Service, lists the service associated with each system. The last column indicates the status of each system's services. For an inhibited service, the word inhibited appears; otherwise, the screen shows the number of logons (inbound or outbound) and the number of transfers in progress.

From the Control Communications Systems screen, you can control all sessions that are using a specific service available to the system that you choose. You make your choice by pressing PF6 (Control Service at System). You can also select the remote system and choose to control its individual sessions (that is, specific transfers and logons) by pressing PF11 (Session Information).

PF6 (Control Service at System) lets you inhibit or enable a specific service for the system you select. This key can call up three different screens, one for each type of service. The position of the cursor at the time this key is pressed determines the choice of screen. For example, to inhibit all File Transfer sessions from a remote system, move the cursor to the File Transfer selection for that system and press PF6. The system displays the Control File Transfer screen, lists the name of the remote system, and offers two options: PF3 (Inhibit Transfers Without Affecting Active Transfers), and PF6 (Inhibit Transfers, Cancel Active Transfers and Hold Entries).

PF11 (Session Information) lists all active sessions that involve the remote system you select with the cursor. For example, Figure 9-3 illustrates the Control Sessions screen for a remote system named RMTOIS.

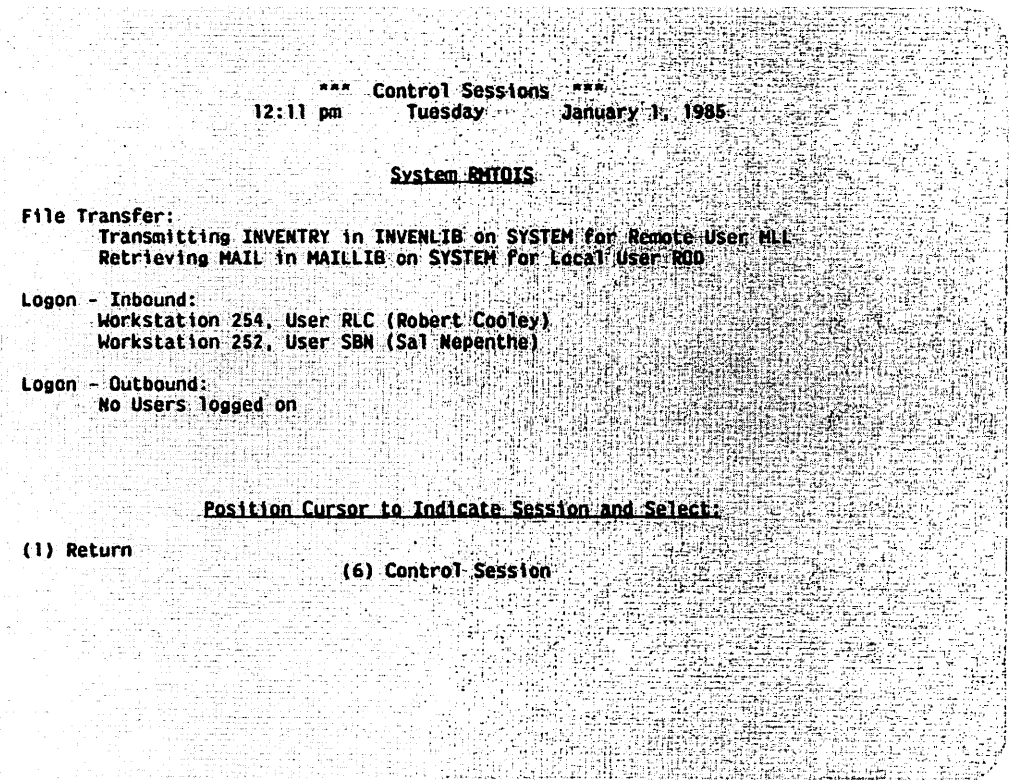

Figure 9-3. Control Sessions Screen

To control an inbound Logon session, position the cursor next to the name of that session and press PF6 (Control Session). You can then disconnect the remote workstation (PF4) and: log off the remote user immediately (PF6), or log off the remote user at program completion (PF5).

To control an outbound Logon session, place the cursor next to the name of that session and press PF6 (Control Session). You can then terminate (PF4) or suspend (PF3) the workstation's access to the remote VS to which it is logged on.

When the cursor is next to a File Transfer session and you press PF6 (Control Session), you can cancel the current transfer and requeue it with a status of "hold" by pressing PF6 again.

9.3 CONTROLLING WORKSTATION AND INTERACTIVE TASKS

Two selections on the VS Operator's Console menu, PF6 (Interactive Tasks) and PF13 (Workstations), enable you to control workstation and interactive tasks for remote systems just as you would for local users.

Figure 9-4 shows a sample Control Workstations screen that displays information for workstations logged on from remote systems. For complete information about the Control Workstations screen, refer to the VS System Operation Guide.

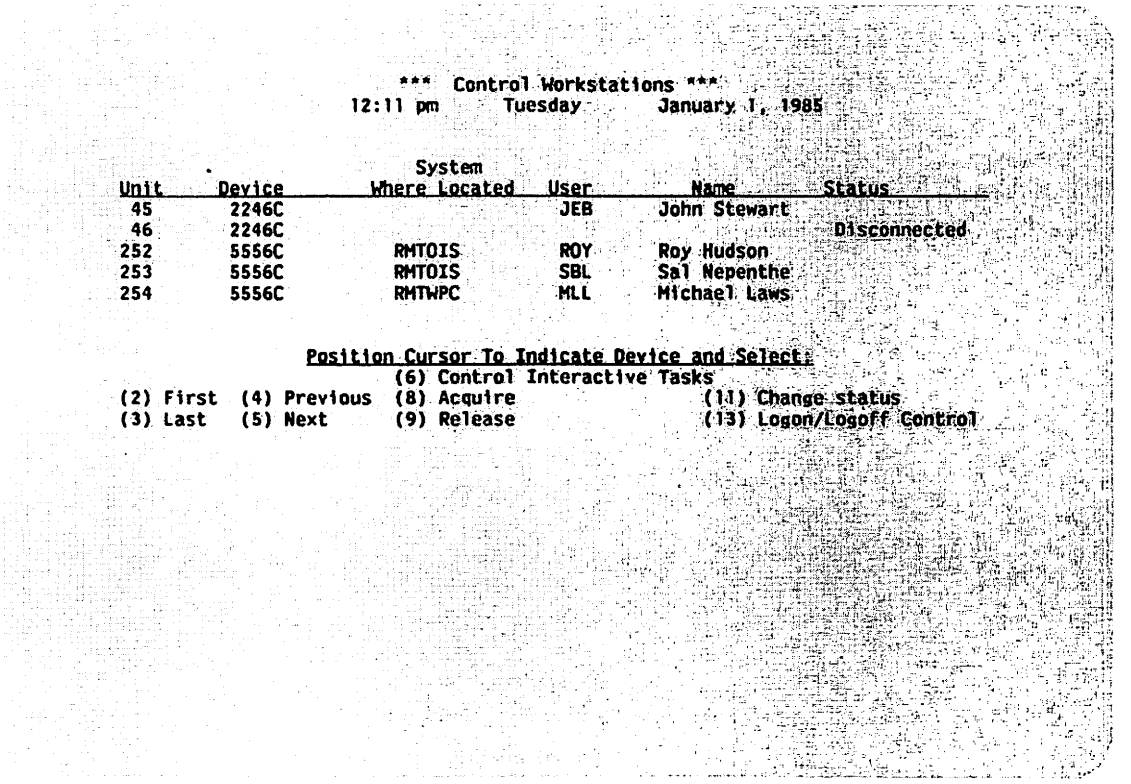

Figure 9-4. Control Workstations Screen

Unit numbers (i.e., workstation device numbers) for inbound logons (logons to your system) are dynamically assigned numbers in descending order from 254.

The System column specifies the name of the remote system whose user is logged on (inbound) to your VS or the remote VS to which a local user is logged on (outbound).

A status of disconnected indicates that a local workstation is physically disconnected from the network or powered off.

PF6 (Control Interactive Tasks) displays the same screen as PF6 (Interactive Tasks) on the VS Operator's Console menu. This screen is illustrated in Figure 9-5.

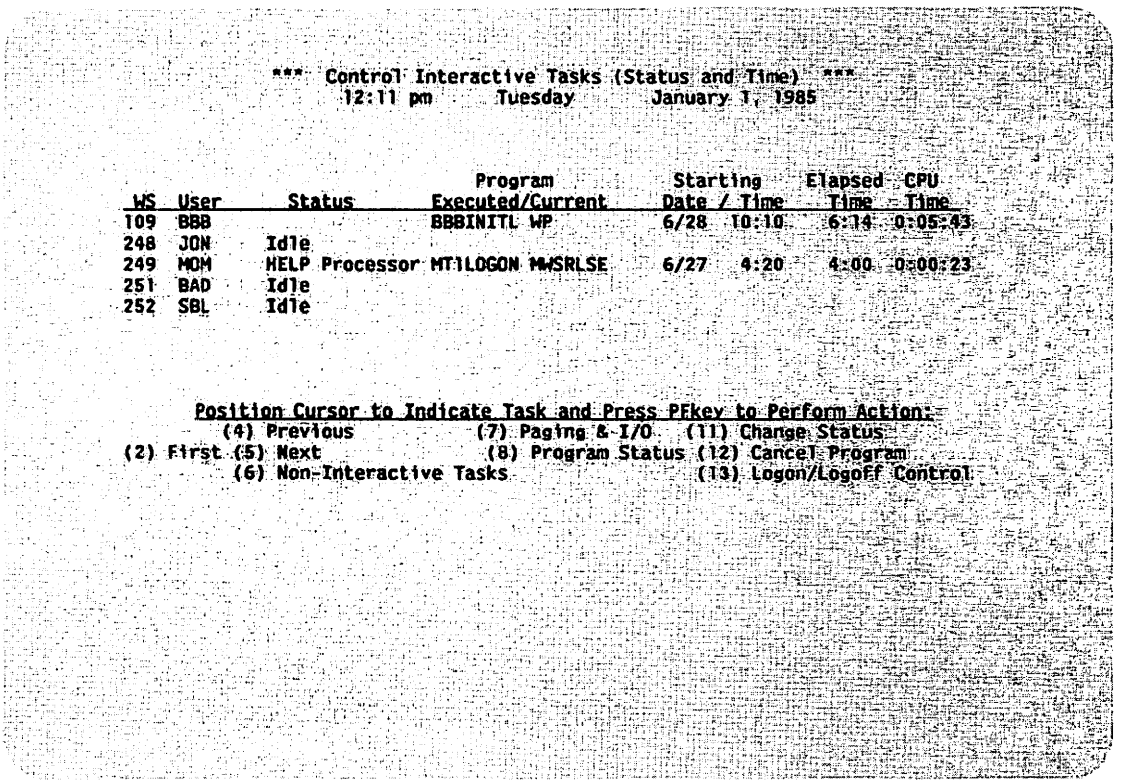

Figure 9-5. Control Interactive Tasks Screen

PF13 (Logon/Logoff Control) is available from either the Control Workstation screen or the Control Interactive Tasks screen; it gives direct control of the workstation whose name is at the current cursor position. PF13 followed by PF10 (Control Logon Service) on the subsequent screen enables you to control all workstations logged on to your VS.

You can allow (PF2) or inhibit (PF3) logons from a local workstation. You can disconnect the workstation of an inbound remote logon by using PF4 (DISCONNECT Workstation). Disconnecting the workstation suspends the task currently under way until the user logs on again.

9.4 CONTROLLING TRANSFER QUEUES

The VS Transfer Manager software maintains two transfer queues that you can access from the VS Operator's Console menu. Press PF4 (Transmit Queue) or PF5 (Retrieve Queue).

The VS transmit queue lists all files awaiting transmission from your (local) system to the remote system specified in the File Destination column. The VS retrieve queue lists all files awaiting retrieval from the remote system specified in the File Origin column.

Your local users are the initiators of all requests on these queues. For each request on either queue, the Status column indicates: "Xfering" if the transfer is in progress, "Hold" if the request is suspended, or a blank status for a request actively awaiting transfer (refer to Figure 9-6).

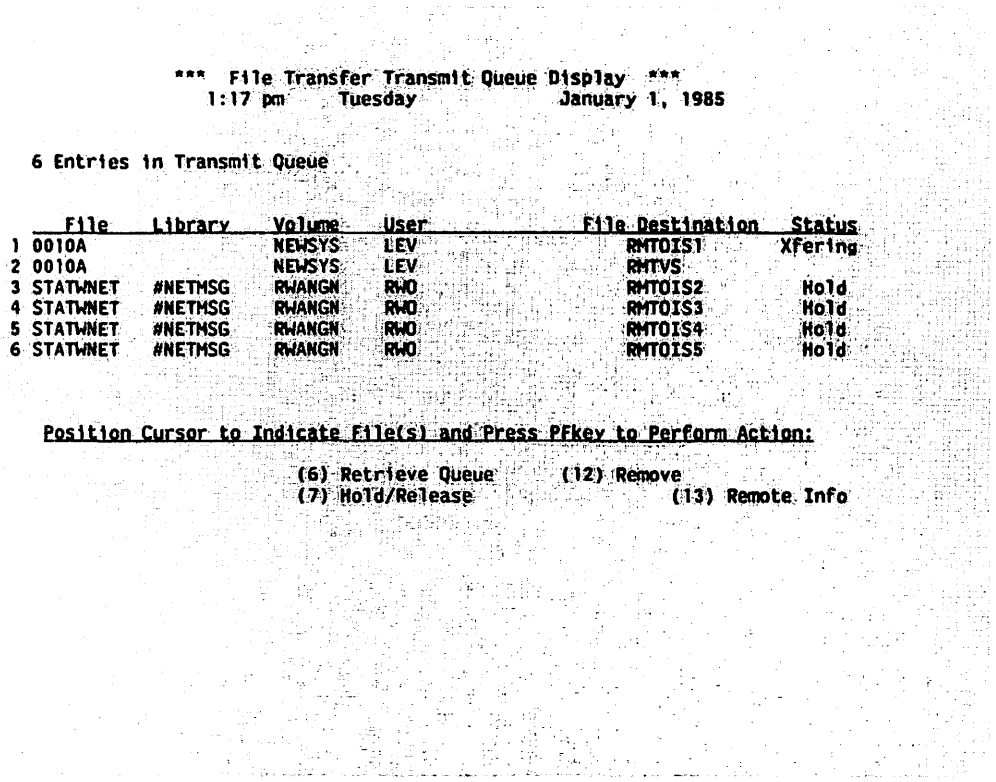

Figure 9-6. Transmit Queue -- Local Information

To change the status of a request, position the cursor at the line on which the name of the request is listed and press one of the following PF keys:

PF7 (Hold/Release) -- Places an active request on hold (the status changes from blank to Hold) or places a held request on the active waiting list (the status changes from Hold to blank).

PF12 (Remove) -- Removes the selected request from the queue. (This action does not delete the file.) A system administrator can remove a request, if the queue is accessed through PF11, Telecommunications, on the Operator's Console screen. If the queue is accessed through the command console, PF8, the file owner is the only person who can remove the request.

PF6 (Retrieve Queue) -- Displays information concerning the file on your local system. The Local Information includes the file, library and volume name, where appropriate. From the Local Information screen, press PF6 again to display the Remote Information screen. Remote information includes the file, library, and volume name, where appropriate, assigned to the file at the remote system.

PF13 (Remote/Local Information) -- Displays the remote or local form of the queue. The remote form of the transmit queue and the local form of the retrieve queue contain a column labeled Transfer Group. Your VS user assigns the transfer group to the request. The group must be defined on the destination system (your system for retrieving a file, or the remote system for sending a file). The groups named on the transmit queue must be defined on the destination system.

9.5 VS FILE TRANSFER LOG

The VS records all transfer requests in a log file. To print this file, run the TRANSFER utility. Press PF5 (Auxiliary Functions), then PF3 (Print Transfer Log) to produce the screen options illustrated in Figure 9-7.

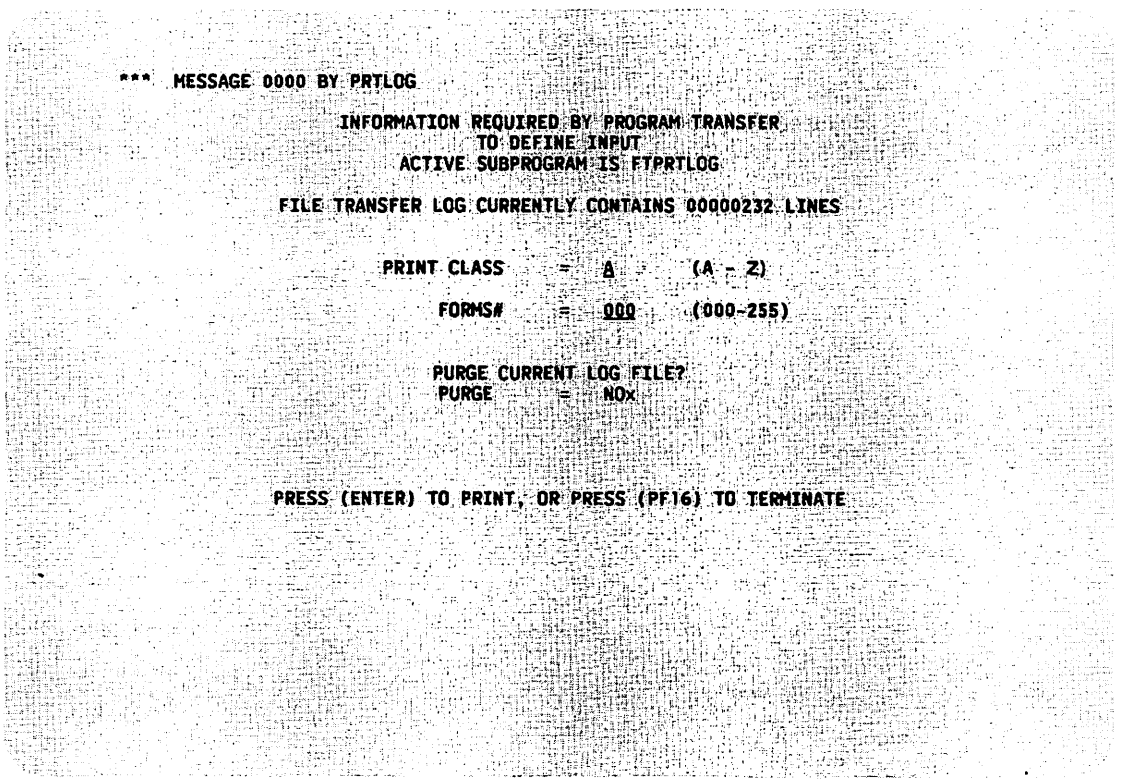

Figure 9-7. VS Log Utility Screen

Do not change the purge default setting (NO) on the VS Log Utility screen unless you are in charge of maintaining the log file. If you do change it, the log is initialized after it is printed, and the printed copy is the only record of the log file.

The VS File Transfer log records the date, time, local file name, remote file name, user, remote site, transfer group, transfer type, and return code (RC) for all file transfer requests that have entered the transmit or retrieve queues. (RC equals zero on a successful transfer.) A complete list of the file transfer log return codes and their meanings is given in Appendix H.

The (S) and (U) next to the transfer type stand for solicited and unsolicited. Solicited means the transfer request was initiated by a local user; unsolicited means the request was initiated by a remote user. Figure 9-8 illustrates a sample VS File Transfer log.

```
                                WANG FILE TRANSFER FACILITY LOG FILE

                          SYSTEM RCF#2                                                    PAGE 01

DATE      TIME      LOCAL FILE NAME REMOTE FILE NAME          USER REMOTE SITE TRANSFER GROUP TRANSFER TYPE RC

10/16/83 08:51:36  ELOG0003 #PRT   SYSTEM T:JBHPRINT.JPRT0063  ART  CLUSTR11 TRANSMIT (S)                 000
*** TRANSFER COMPLETED SUCCESSFULLY ***                            ** REQUEST REMOVED FROM QUEUE **

10/16/83 12:25:01  2010J           SYSTEM 0010J                    CLUSTR11      GROUP01 RECEIVE (U)     000
*** TRANSFER COMPLETED SUCCESSFULLY ***                            ** INITIATED BY REMOTE USER **

10/16/83 12:25:16 ELOG0003 #PRT    SYSTEM T:JBHPRINT.JPRT0064  DM   CLUSTR11      TRANSMIT (S)            000
*** TRANSFER COMPLETED SUCCESSFULLY ***                            ** REQUEST REMOVED FROM QUEUE **

10/19/83 13:54:52 COPY0007 #APBPRT SYSTEM                      APB  CLUSTR11      TRANSMIT (S)            028
*** TRANSFER OPERATION ABORTED BY A LOCAL OPERATOR ***             ** REQUEST HELD ON QUEUE **

10/19/83 16:10:19 0002S            SYSTEM 0002S       FLOPPY   APB  CLUSTR11      RETRIEVE (S)            028
*** TRANSFER OPERATION ABORTED BY A LOCAL OPERATOR ***             ** REQUEST HELD ON QUEUE **

10/21/83 14:45:51 2001R            SYSTEM 1001R                 ART  CLUSTR11      TRANSMIT (S)            076
*** I/O ERROR OCCURRED WHILE ACCESSING DOCUMENT FILE FOR PASSWORD VERIFICATION **REQUEST REMOVED FROM QUEUE**

10/30/83 14:51:00 0001B            SYSTEM 2001B                 FTS  CLUSTR12      TRANSMIT (S)            172
*** DOCUMENT PASSWORD IS NOT CORRECT - DOCUMENT TRANSFER OPERATION REJECTED *** ** REQUEST REMOVED FROM QUEUE

10/30/83 15:51:44 0001B            SYSTEM 2001B                 FTS  CLUSTR12      TRANSMIT (S)            004
*** INPUT VOLUME NOT MOUNTED - TRANSFER REQUEST NOT PROCESSED ***       ** REQUEST HELD ON QUEUE **

10/30/83  16:01:19  0001B          SYSTEM 2001B                 FTS  CLUSTR12      TRANSMIT (S)            020
*** INPUT FILE POSSESSION CONFLICT - TRANSFER REQUEST NOT PROCESSED *** ** REQUEST HELD ON QUEUE **

10/30/83 16:26:25   0001B          SYSTEM 2001B                 FTS  CLUSTR12      TRANSMIT (S)            004
*** INPUT VOLUME NOT MOUNTED - TRANSFER REQUEST NOT PROCESSED ***       ** REQUEST HELD ON QUEUE **
```

Figure 9-8. Sample VS File Transfer Log

The File Transfer log shows the status and final disposition of each request queued. The following kinds of status appear:

- Transfer completed successfully
- Transfer operation aborted by a local operator
- Transfer operation aborted by a remote operator
- I/O error occurred while accessing document file for password verification
- Document password is not correct -- document transfer operation rejected
- Input volume not mounted -- transfer request not processed
- Input file possession conflict -- transfer request not processed
- User has insufficient access rights -- the VS does not have access rights through inter-system security to the remote system

The following kinds of final disposition appear:

- Request removed from queue
- Request held on queue
- Initiated by remote user

The queue records transfer events from the point of view of the local VS. There are three types of transfers:

- TRANSMIT -- a send request by a local user
- RETRIEVE -- a retrieve request by a local user
- RECEIVE -- a file/document transfer initiated by a remote user

CHAPTER 10
WANG BAND MONITOR

10.1 USING THE WANG BAND MONITOR

The Wang Band Monitor capabilities are contained in the program LWNMON, which can be accessed through the Run Program or Procedure function via the VS Command Processor.

The first screen of the program lists all the systems on the network that are connected by Wang Band (see Figure 10-1).

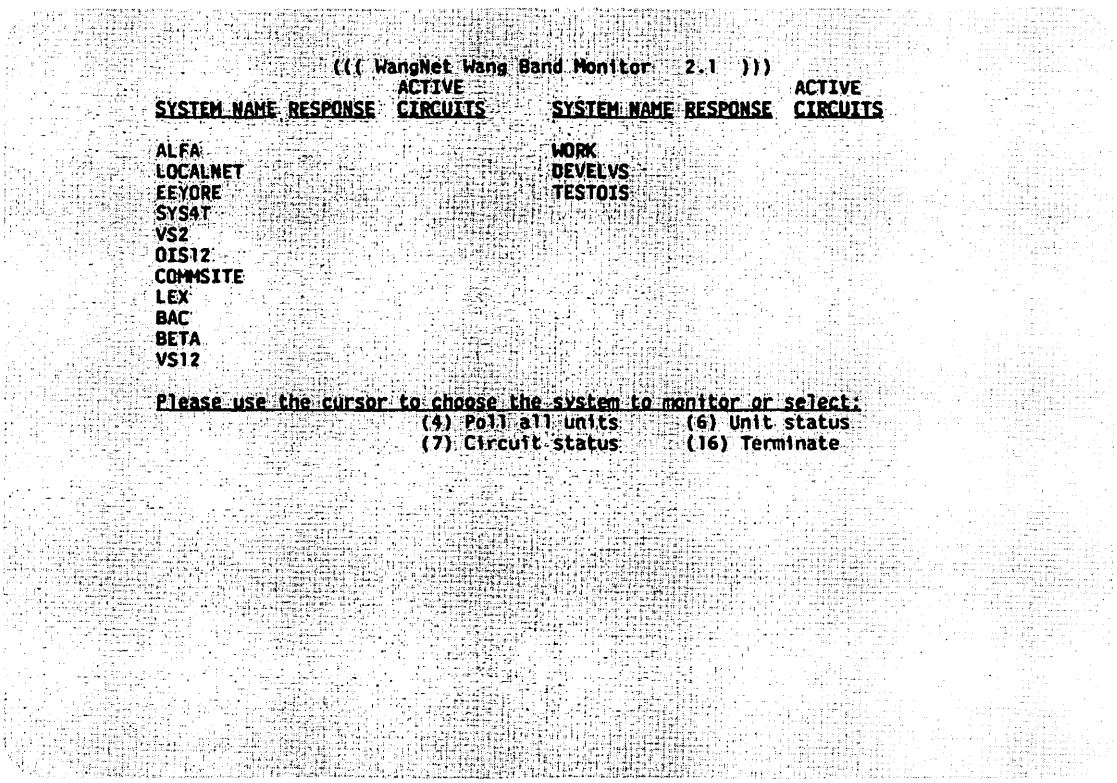

Figure 10-1. Wang Band Monitor System Screen

When you press PF4, Poll all units, the Wang Band Monitor begins to poll all the Cable Interface Units (CIUs) in sequence and displays the results of those polling attempts on the screen (see Figure 10-2). The arrow points to the system currently being polled.

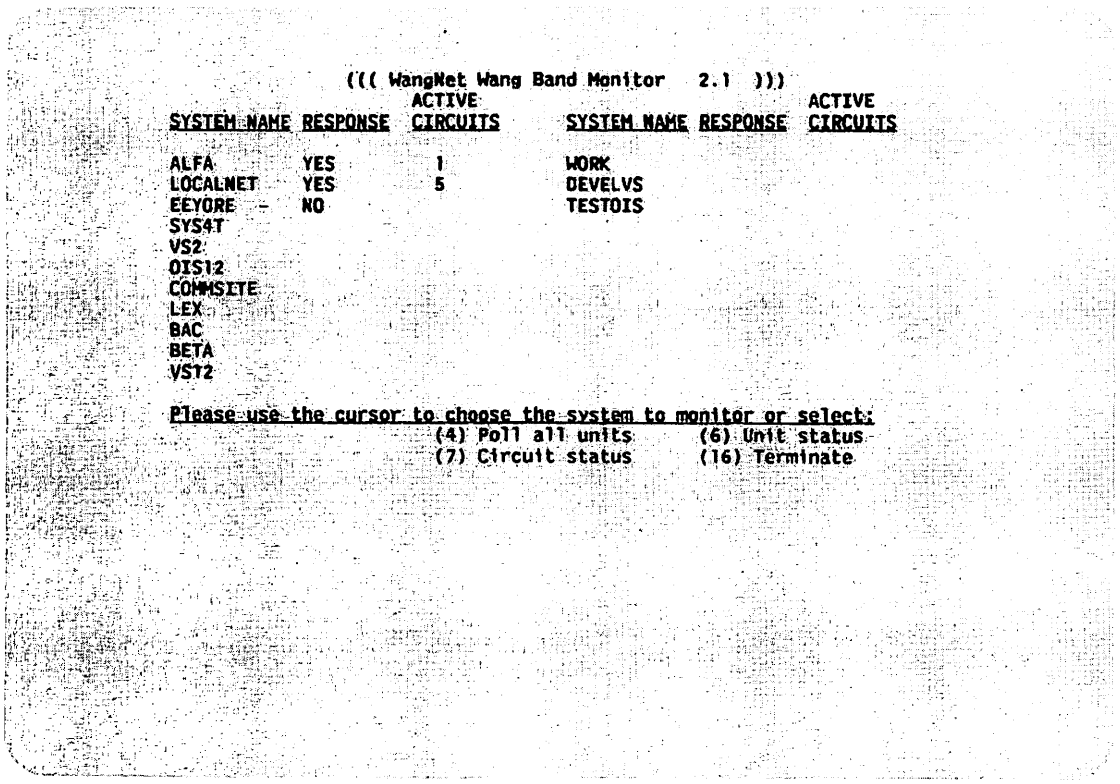

Figure 10-2. Wang Band Monitor Polling All Units Screen

When you select a system and press PF7 (Circuit status), the screen displays the status of the CIU's 24 virtual circuits (VC) as either active or inactive. If the circuit is active, the system using that circuit is listed beside the status under the remote system heading (see Figure 10-3).

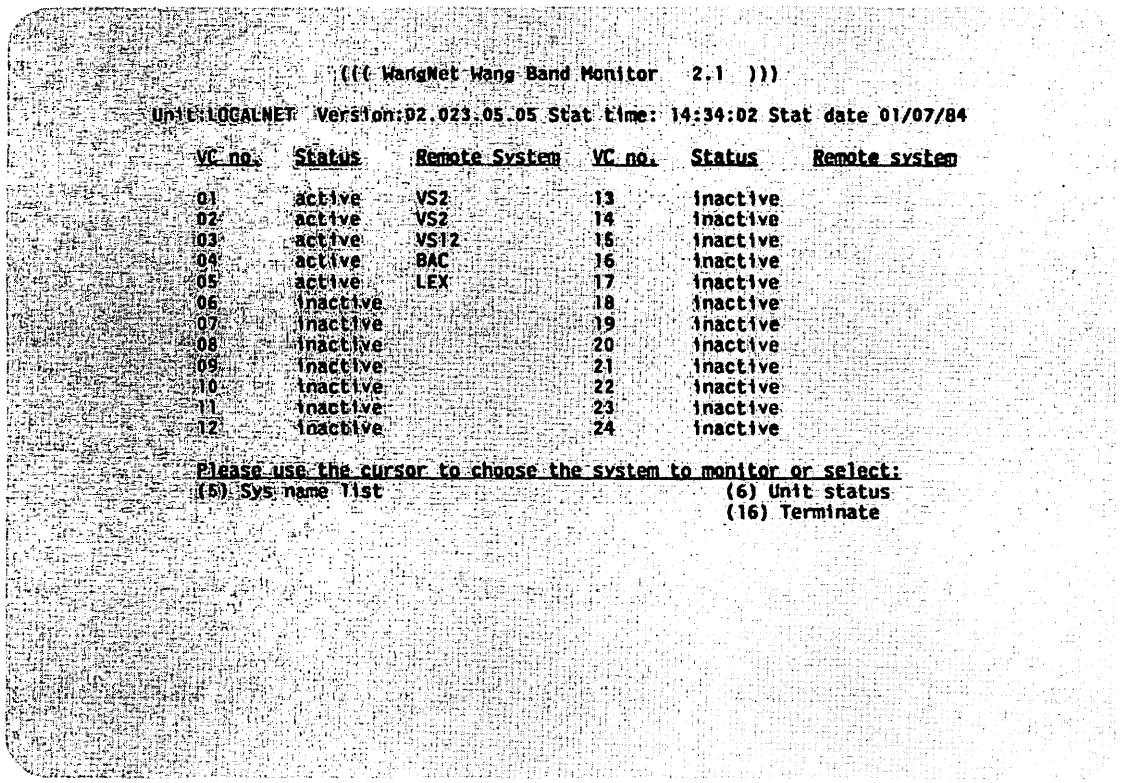

Figure 10-3. Wang Band Monitor Circuit Status Screen

When you press PF6, Unit status, the screen displays the status block contents for the CIU on the system that you selected (see Figure 10-4). The display includes totals in decimal and hexadecimal of general traffic statistics and error counts.

NOTE

The Wang Band Monitor Circuit Status screen always shows 24 virtual circuit numbers, regardless of the maximum number of virtual circuits the named system can actually support.

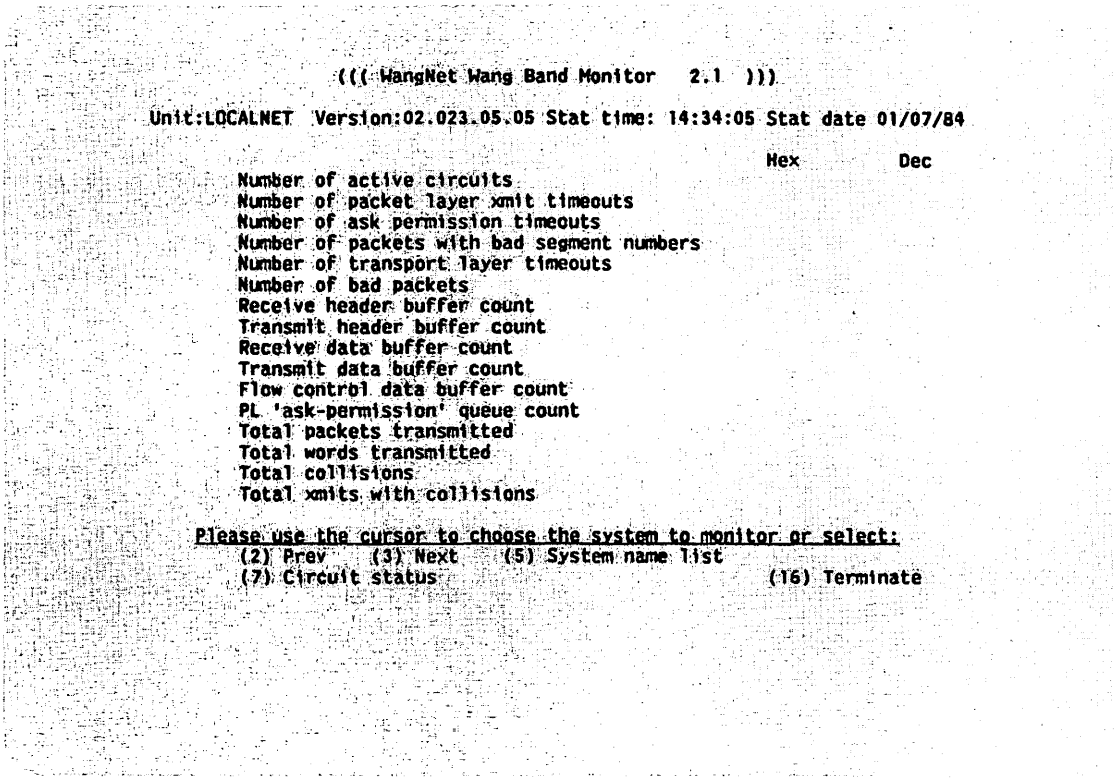

Figure 10-4. Wang Band Monitor Unit Status Screen

Table 10-1 contains a complete listing of the unit status messages and their meanings.

Table 10-1. Wang Band Monitor Unit Status Messages and Their Meanings

Message	Meaning
Number of active circuits	Total number of inbound and outbound sessions currently active.
Number of packet layer xmit timeouts	Number of times a packet had to be retransmitted because no ack signal was received within the timeout period.
Number of ask permission timeouts	Number of times a flow control packet had to be retransmitted because no response was received within the timeout period.

(continued)

Table 10-1. Wang Band Monitor Unit Status Messages and Their Meanings (continued)

Message	Meaning
Number of packets with bad segment numbers	Number of times a packet was discarded because of an invalid control field.
Number of transport layer timeouts	Number of times a circuit was cleared because the higher layer (VS or OIS host application) did not read a pending message before the end of the timeout period.
Number of bad packets	Number of times a packet was discarded because it was received garbled.
Receive header buffer count	Number of buffers available to receive control packets. A lower number indicates a high amount of traffic or delay in this unit.
Transmit header buffer count	Number of buffers available to transmit control packets.
Receive data buffer count	Number of buffers available to receive control packets.
Transmit data buffer count	Number of buffers available to transmit user data packets.
Flow control data buffer count	Maximum allowable number of buffers to be allocated to messages in flight. This value is the upper limit on the 'ask permission queue count'.
PL 'ask-permission' queue count	Outstanding number of requests to transmit long user data packets.
Total packets transmitted	Number of control and user data packets transmitted.
Total words transmitted	Number of 16-bit words in all packets transmitted.

(continued)

Table 10-1. Wang Band Monitor Unit Status Messages and Their Meanings (continued)

Message	Meaning
Total collisions	Number of times a packet had to be retransmitted because of collision.
Total xmits with collisions	The number of packets that were involved in at least one collision.
Total words received	Number of 16-bit words in all packets.
Error record high and low bits	OR'ed error status bits for all receptions and transmissions. A bit set indicates that the corresponding error occurred at least once. Bit values are:
8000 Reserved. 4000 A packet was received that was larger than the agreed upon maximum packet size. 2000 Reserved. 1000 Memory did not respond fast enough during a reception. 0800 The packet received did not have a closing flag or was not a multiple of 16 bits. 0400 Receive memory address overflowed X'FFFF'. 0200 CRC error detected. 0100 Abort character received. 0080 Data Set Ready signal went off. 0040 Data Terminal Ready signal went off. 0020 Reserved. 0010 Maximum number of collision retries was exceeded on xmit. 0008 Reserved. 0004 Reserved. 0002 A transmit was aborted, either because of slow memory or parity error. 0001 Reserved.	
Receive abort count	An abort character detected in an incoming packet.
CRC error count	CRC error detected on received packet.

(continued)

Table 10-1. Wang Band Monitor Unit Status Messages and Their Meanings (continued)

Message	Meaning
Address overrun count	Attempt to store an incoming packet past memory address X'FFFF'.
Framing error count	A packet was received that did not have a closing flag or did not contain a multiple of 16 bits.
Memory overrun count	Memory did not respond fast enough during a receive operation.

APPENDIX A
VS USER ERROR MESSAGES

This appendix contains VS File Transfer error messages that direct the user to contact the VS system administrator. The messages are presented as they appear on the screen but in alphabetical order. Table A-1 lists each message, the reason for each message, and the appropriate response.

Table A-1. VS User Error Messages

Message	Reason/Response
Hardware error encountered during device initialization	This message appears when you attempt to initialize an unmounted volume. Mount the correct volume.
The remote system cannot support word processing	This message appears on the Send a Document Options and Retrieve a Document Options screens. Cancel the request. WSNEDIT controls this feature.
The specified location has not been defined	This message appears on the following screens: Send a File Options, Send a Document Options, Retrieve a File Options, and Retrieve a Document Options. The system name contained in the Location field cannot be located in the network directory file. Move the cursor to the Location field and enter another location name.
The specified volume is mounted for exclusive use	This message appears on the following screens: Send a File Input, Send a Document Input, and Retrieve a Document Output. The files and documents on the specified volume cannot be accessed at this time. Dismount and remount the volume with shared privileges if possible.

(continued)

Table A-1. VS User Error Messages (continued)

Message	Reason/Response
User has insufficient access rights	This message appears on the Send a File Input and Send a Document Input screens. The transfer request cannot be processed because the requestor is not authorized to access the requested file or document. VS Security controls file access rights. This message also appears on the Transfer Group Selection screen. Only users with security access rights and the owner of a transfer group can access a transfer group.

APPENDIX B
CNS REASON MESSAGES

B.1 INTRODUCTION

WSNMON displays various reason messages which, in most cases, give information on problems that have occured within CNS. These messages are stored in a log file. These messages appear on the WSNMON Main menu. Most of these messages are explained in the following sections.

B.2 ERROR MESSAGES

WSNMON can display the following error messages:

Application Abnormally Terminated, Appl = %01, User = %02, Sessions In = %03, Sessions Out = %04, Messages In = %05, Messages Out = %06, Bytes In = %07, Bytes Out = %08, Reason = %09&03 - This message means that an application at the local system was terminated due to insufficient resources at a remote system. The application at the local system had established a session with an applicaion at the remote system.

GETHEAP error, buffers may have been discarded - Not enough buffers could be allocated to an application. The buffers may have been lost. Increase the Segment 2 size for CNS.

Application %01 not submitted, Reason = Directory lookup failure - An application could not be found in the directory that identifies applications to CNS.

Inbound Session Rejected, SID = %01, LocAppl = %02, RemAppl = %03, RemSys ID = %04, RemArea ID = %05, Reason = %06&03 - An application at a remote system attempted to establish a session with an application on the local system and the attempt was rejected. The session may have been rejected due to a failure to find one of the applications in the application directory.

Outbound Session Rejected, SID = %01, LocAppl = %02, RemAppl = %03, RemSys ID = %04, RemArea ID = %05, Reason = %06&03 - An application on the local system could not establish a session with an application at a remote system due to a directory look-up failure (the local application could not be found in the directory).

Session Terminated Abnormally, SID = %01, User = %02, Messages In = %03, Messages Out = %04, Bytes In = %05, Bytes Out = %06, ReXmits Out = %07, ReXmits In = %08, Rcvd out of seq = %09, Reason = %10&03 - A session has been terminated abnormally (before a close request has been sent and acknowledged). Possible reasons include a line failure, insufficient resources at a system, a system failure, etc.

End to End Restart Failure with System %01 in Area %02, Local Rev = %03, RemRev = %04, Reason = %05&03 - The local system could not exchange restarts with a remote system. (A session cannot be established with a remote system until the CNS End to End layer at the local system successfully exchanges a restart with the CNS End to End layer on a remote system.)

Contact has been lost with System %01 in Area %02, Reason = %03&03 - Contact can be lost with a remote system for various reasons, including a system failure, line failure, transport failure or problems within CNS.

The following error messages reflect information gathered from the CNS switching layer.

Route Disabled to System %01, Area %02 using transport %03, Reason = %04&05 - A path to a remote system cannot support communications. The message identifies the remote system, its area, and the transport the local system uses to route messages to an adjacent system from which the message is eventually routed to the destination. The message appears for a number of reasons, including a transport failure, a line failure, or problems at intermediate systems along the path.

CNS revision level has been unsuccessfully exchanged with System %01, Area %02, Local Rev = %03, RemoteRev = %04, Reason = %05&05 - The local system's attempt to exchange XID commands with an adjacent system has been unsuccessful. Adjacent systems cannot communicate, nor can one send data through another to a destination, until they exchange XID commands. These commands identify the CNS revision level that is installed on the respective systems. Systems with the same revision level can communicate. Systems with different revision levels can communicate if one revision level is the immediate successor of the other.

Path has been disabled to System %01, Area %02, via adjacent System %03, Area %04, Reason %05&05 - A path has been disabled to a destination in a particular area by way of an adjacent system. The path definition may have been deleted from the local-view configuration file (refer to the WSN VS Network Configuration Guide, Chapter 5) of the local system or intermediate systems along the path. Or there may have been a line, transport or system failure along the path.

No Path Found to System %01, Area %02, Reason %03&05 - A path to a particular destination system could not be found. That system may lack a route definition. Run WSNEDIT to verify that a path to that system was defined.

Protocol Violation Inbound, Command = %01, Reason = %02 - A received message was not formatted properly (e.g., missing header).

Protocol Violation Outbound - A sent message was not formatted properly.

No path available to System %01, Area %02, Reason %03&05 - No communications path to a system is available. The reason may be network congestion, a line failure, a transport failure, or a failure at an intermediate system.

The following error messages are related to problems with a configuration file.

Config open error by 55 - There is an error in opening a configuration file.

Config Close error by 56 - There is an error in closing a configuration file.

Config Record not found by 57 - A record has not been found in a configuration file.

Config not alt by 58 - The configuration file does not have an alternate index structure needed to support the function required of it.

Config read err by 59 - There has been an error in reading the configuration file.

The following are WSN transport driver error messages.

Unable to Read Configuration on Link %01, Reason = %02 - The local-view configuration file cannot be read. The file may be missing, or it may not be on the IPL (system) volume.

Unable to Connect to Session Manager on Link %01, Reason = %02 - The transport cannot connect to the session manager. Transports must be able to connect to the session manager before they can support sessions. There may be a transport software or session-manager software problem.

Unable to Establish Transport Connection to System %01 on Link %02, Reason %03&04 - A transport connection (i.e., virtual circuit) cannot be established with an adjacent system. The DLP at the adjacent system may not be running, or there may be problems with the transport software.

Transport Connection Abnormally Terminated with System %01 on Link %02, Reason = %03 - The transport connection was terminated abnormally, possibly because of a DLP crash on either the local or an adjacent system, a transport software crash, a line failure, or a system failure.

APPENDIX C
OPERATOR'S CONSOLE NETWORK ERROR MESSAGES

C.1 INTRODUCTION

This appendix contains a list of error messages that are sent to the Operator's Console of a VS system by either the File Transfer Manager (FTM) or the Session Manager. These error messages indicate that the FTM (of the local system) was unable to establish a File Transfer session with a remote FTM or that a session was established but could not be completed.

Some of these messages contain the name of the remote system. as part of the message. In this appendix, "SYSNAME" indicates where the name of a remote system appears. Similarly, each message displays the time (indicated in the samples as "TIME") at which the system detected the error.

Each message in this appendix is followed by an explanation of its cause and a brief description of what you can do to correct the problem. Some of the messages have return codes that refer to more specific reasons for the transfer problem.

C.2 SERVICE CONNECTION ERRORS

One of the following messages may appear if your VS cannot activate the File Transfer service for a remote system:

DLP for SYSNAME is currently in use for other purposes ....TIME
Allow File Transfer service to SYSNAME has failed .....TIME

All the available sessions to the remote system are active. Try to establish a session later.

File Transfer configuration error for system SYSNAME .....TIME
Allow File Transfer service to SYSNAME has failed .....TIME

The remote system may not be defined properly in your network directory file or local-view configuration, or the File Transfer service was not declared for that system. Check your network directory file and your local-view configuration file.

System SYSNAME is not available at this time .....TIME
File Transfer session establishment has failed .....TIME

All available virtual circuits to the remote system are in use. Try to establish a session later.

Network Server directory file error, Data not found .....TIME
Allow File Transfer Service to SYSNAME has failed .....TIME

System record cannot be found. Run WSNEDIT to check the directory for the name of the system in question. If the name is not in the directory, use WSNEDIT to enter the system name. (Return Code = 01.)

Remote FTM at SYSNAME not attached to network server .....TIME
File Transfer session establishment has failed .....TIME

File Transfer service at the remote system is either completely inhibited or not currently attached to the network. (Reason Code = 02.)

Network Server directory file error, File access error ...TIME
Allow File Transfer Service to SYSNAME has failed .....TIME

An error occured while the directory file was being read. Check the directory file to determine whether or not it requires reorganization. (Return Code = 03.)

Network application limit exceeded .....TIME
Allow File Transfer Service to SYSNAME has failed .....TIME

File Transfer Service cannot attach to CNS because maximum number of applications that can attach to CNS has been exceeded. (Return Code = 03.)

Configuration Error, Data truncated due to lack of space .TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

This is a software error. Call your Wang customer engineer. (Return Code = 4.)

FTM communication with Network Server failed .....TIME
Will try to re-attach to Network Server when its running.TIME

This message appears under two conditions. The first condition occurs when CNS is not running. If CNS is not running, it must be started before FTM can use it. The second condition occurs when communication with CNS fails during the processing of transfer requests. In either case, transfer requests should be released after CNS is re-activated. FTM will then attempt to re-attach to CNS and process the next release entries on the queue. (Return Code = 07.)

Configuration Error, Connection not possible.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

This is a general message indicating that an error may exist either in your network configuration file defined through WSNEDIT or in the configuration file of the remote system. If your VS is a secondary system on a Multipoint transport, the connection request may have been for another secondary system. Since secondary systems cannot communicate directly, a connection is not possible. (Return Code = 8.)

Configuration Error, Invalid service or service ID.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

File Transfer was not declared as a service for the remote system. Check your WSNEDIT local-view configuration file to see if the File Transfer service is declared for the remote system. (Return Code = 12.)

Configuration Error, Invalid system or system ID.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Check your WSNEDIT local-view configuration file and the network directory file to see if the remote system is defined properly and to see if its network name (as defined in its configuration file) matches the name assigned to it in your configuration file and the network directory file. (Return Code = 16.)

Local system is not configured .....TIME
Allow File Transfer service to SYSNAME has failed .....TIME

Run WSNEDIT (Manage Services) to check the local-view configuration file. The local system must be defined for the File Transfer service. (Return Code = 20.)

Configuration Error, Invalid link or link definition.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Invalid transport or transport definition. Check the definition of the transport that you attempted to use. Check to see if the remote system is defined for that transport. (Return Code = 20.)

Cannot access directory access file .....TIME
Allow File Transfer service to SYSNAME has failed .....TIME

Check validity of network directory file. The directory file must correspond to the directory file specified through WSNDIRM. (Return Code = 21.)

Not enough memory to create an inter-task message port ..TIME
Allow File Transfer service to SYSNAME has failed .....TIME

Check your system's memory usage. (Return Code = 22.)

Configuration Error, System not configured for service....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

The File Transfer service was not specified as a service for the remote system. Check with the system administrator of the remote system. (Return Code = 24.)

Configuration Error, Invalid function in parameter list...TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

This is a software error. Call your Wang customer engineer. (Return Code = 28.)

Configuration Error, Invalid operand.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

This is a software error. Call your Wang customer engineer. (Return Code = 32.)

Configuration Error, No configuration file available.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Perform IPL on your system with a valid WSNEDIT configuration file. (Return Code = 36.)

Configuration Error, Link initialization not possible.....TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Transport initialization not possible. Check your system configuration file to see if the DLP for that transport is configured properly. Or use WSNMON to see if the transport is disabled. (Return Code = 40.)

Configuration Error, Unknown network config file problem..TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

Unknown problem with network configuration file. Save the file for your Wang customer engineer and try to re-create the transport and system definition. (Return Code = 44.)

Configuration Error, DLP not found in system config file..TIME
Allow File Transfer Service to SYSNAME has failed.....TIME

There is no DLP serving the WangBand transport. Compare the DLP device name you entered through WSNEDIT in your local-view configuration file to your device configuration in the system configuration (i.e., GENEDIT) file. Determine whether or not the device name in the WSNEDIT local-view file properly reflects the port to which the DLP is connected. (Return Code = 48.)

C.3 SESSION ESTABLISHMENT ERRORS

One of the following messages may appear if your VS can establish a connection with a remote system but cannot establish a File Transfer session. The VS File Transfer Manager will try to establish a session every few seconds up to a specified number of times. When the File Transfer Manager has tried for the last time, the message

Maximum session retries with SYSNAME reached ...TIME

will be displayed in conjunction with any of the following messages:

Unable to open a TC path for system SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

A problem may exist with the configuration of the DLP or with the communications line. Check your DLP, its configuration, and its status lights.

System SYSNAME is unable to establish File Transfer .....TIME
File Transfer session establishment has failed .....TIME

A problem exists at the remote system. Contact the remote system administrator.

File Transfer service inhibited by system SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

The remote system administrator has inhibited communications. Try to establish a session later.

All available circuits are busy for system SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

There are no available logical circuits to the remote system. Try to establish a session later.

System name received from SYSNAME is not as configured .....TIME
File Transfer session establishment has failed .....TIME

The name the remote system uses to identify itself on the network is not the name your system expected to receive. Check your configuration file to see if the name you entered for that system is correct.

Maximum number of File Transfer sessions for SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

All sessions to the remote system are in use. Try to establish a session later.

Password received by SYSNAME is not as configured .....TIME
File Transfer session establishment rejected by SYSNAME .....TIME

The password that your VS sent to the remote system does not match the password that it expected to receive. Check with the remote system administrator to see if your system's password (as listed in WSNEDIT) matches the Receive password listed in the remote system's network configuration file.

FTM not active at SYSNAME or passwords do not agree .....TIME
File Transfer session establishment has failed .....TIME

Check to determine whether or not transfers are allowed to the remote system named. Use WSNEDIT (Manage Services function) to verify that the expected password at the remote system is the one contained in the local system's local-view configuration file. (Reason Code = 00.)

System SYSNAME unable to establish File Transfer Session .....TIME
Cannot open a telecommunications path .....TIME

A problem may exist with your DLP or with the DLP of the remote system. Check the system configuration files of both systems to verify the configuration of the DLPs. Check the status LEDs of the DLPs. (Return Code = 01.)

File Transfer mailbox ID not attached to network server .....TIME
File Transfer session establishment has failed .....TIME

File Transfer has a mailbox ID that allows CNS to deliver messages to it. This ID must be attached to CNS in order for file transfers to take place. If the above message appears, inhibit File Transfer and re-allow it for all systems. (Return Code = 01.)

Invalid system, system record not found on directory .....TIME
File Transfer session establishment has failed .....TIME

System record for a system was not found in the directory. Use WSNEDIT to check the directory file for the name of the system. (Return Code = 02.)

Remote FTM at SYSNAME not attached to Network Server .....TIME
File Transfer session establishment has failed .....TIME

Remote File Transfer service is either completely inhibited or not currently attached to CNS. (Return Code = 02.)

File Transfer session limit exceeded .....TIME
File Transfer session establishment has failed .....TIME

The maximum number of concurrent incoming "open session" requests sent by CNS has been reached. The maximum number of concurrent sessions allowed is 32. Check the number of active sessions. Try to establish a session later. (Return Code = 04.)

Session is not active .....TIME
File Transfer session establishment has failed .....TIME

A session that was active is no longer active. All active transfers will be placed on hold. Check transfer and retrieve queues as well as and release items to re-initiate transfers. (Return Code = 05.)

Remote session limit at SYSNAME exceeded .....TIME
File Transfer session establishment has failed .....TIME

The maximum number of concurrent sessions at the remote system has been exceeded. Check the number of active sessions using CNS at the remote system. (Reason Code = 06.)

System SYSNAME is unable to establish File Transfer .....TIME
System is not active .....TIME

Either the local VS is not listed in the configuration file of the remote VS, or the File Transfer service has not been activated for the local VS by the remote VS system administrator. Call the system administrator of the remote VS. (Return Code = 11.)

System SYSNAME is unable to establish File Transfer .....TIME
DLP has the maximum number of active sessions .....TIME

Either the local or remote DLP is conducting the maximum number of sessions. Try to establish a session later. (Return Code = 12.)

System SYSNAME is unable to establish File Transfer .....TIME
Session will shut down other system's guaranteed session .....TIME

The session you have tried to establish has a higher priority than a current session. The other session will be canceled if you continue. (Return Code = 13.)

System SYSNAME is unable to establish File Transfer .....TIME
Unable to access user list. .....TIME

A specific User ID or password cannot be validated. You must run the SECURITY utility on the remote VS and correct the user ID error condition. (Return Code = 19.)

System SYSNAME is unable to establish File Transfer .....TIME
Maximum number of sessions per system has been reached .....TIME

All guaranteed file transfer sessions to a remote system are in use. Try to establish a session later. (Return Code = 49.)

System SYSNAME is unable to establish File Transfer .....TIME
Invalid VS device number .....TIME

A system cannot access a VS device (in this case a DLP). Check the network configuration file to see if the DLP is identified properly. (Return Code = 241.)

System SYSNAME is unable to establish File Transfer .....TIME
DLP not running (outbound) .....TIME

Either the remote or local DLP is not operating. Activate the DLP. (Return Code = 242.)

System SYSNAME is unable to establish File Transfer .....TIME
All virtual circuits are busy .....TIME

The remote system is currently engaged in its maximum number of communications sessions. Try to establish a session later. (Return Code = 243.)

System SYSNAME is unable to establish File Transfer .....TIME
Local DLP timeout .....TIME

The local DLP did not receive a response from the remote DLP in the allotted period of time. (Return Code = 244.)

System SYSNAME is unable to establish File Transfer .....TIME
Transportation error .....TIME

Possible reasons for the appearance of this message are

Called VS has all circuits in use
Communications are lost
Switched line establishment has failed
Leased line is not up yet
System name is not in destination table
Line is in the process of closing
Switched line is not up. It is configured for incoming calls only
Close requested (manual dial timer has expired)

(Return Code = 245 for the message above.)

Insufficient resources at remote system SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

The remote system lacks the resources required to handle a session. Check with the system administrator at the remote system about the amount of activity there. (Reason Code = 09.)

Remote FTM at SYSNAME could not be found .....TIME
File Transfer session establishment has failed .....TIME

Check the status of File Transfer at the remote system. (Reason Code = 10.)

Remote system SYSNAME is not reachable .....TIME
File Transfer session establishment has failed .....TIME

Check all physical connections and system along the routes between the originating system and the destination system. (Reason Code = 17.)

Communication timeout while trying to reach SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

Timer expired while waiting for a response from the remote system. Check routes, traffic volume, and other network factors to determine the cause of the delaying response. (Reason Code = 18.)

Local FTM session limit at SYSNAME exceeded .....TIME
File Transfer session establishment has failed .....TIME

The maximum number of concurrent File Transfer sessions at the local system has been exceeded. Check the number of active sessions at the local system. (Reason Code = 22.)

Insufficient resources at local system SYSNAME .....TIME
File Transfer session establishment has failed .....TIME

Check the volume of activity at the local system. (Reason Code = 25.)

C.4 VS TERMINAL EMULATION ERRORS

Invalid User ID or password.

A local user has attempted to log on to a remote system with an invalid User ID or password.

A local user has attempted to log on to a remote system, but another user has already logged on with the same ID and password.

APPENDIX D
PROBLEM SOLVING

D.1 INTRODUCTION

This appendix explains the light emitting diode (LED) status lights for CIUs and VS-TCs. LEDs indicate the operational status of their devices; you can use them to determine if there are problems with either the devices or the data link.

This appendix also covers some of the steps you might take when trying to discover the cause of a communications failure. Some of the hardware descriptions in this appendix are for your information only. Only a qualified Wang customer engineer should perform certain adjustments to hardware devices.

D.2 TCB1 LEDS

Figure D-1 illustrates the VS-TC LEDs as they appear on the front panel of a VS TCP. Reading from left to right, they are numbered 1 through 8. Table D-1 lists and explains the meaning of each VS-TC LED.

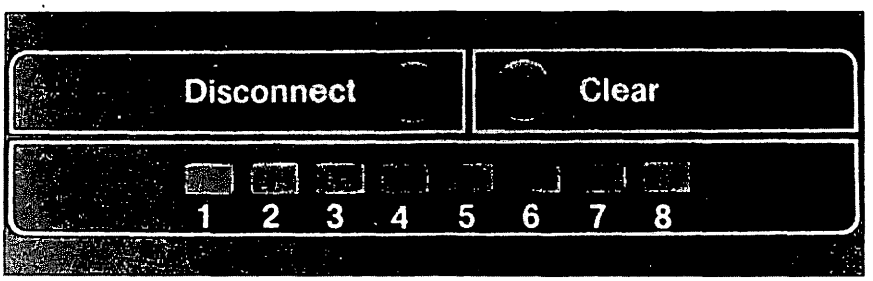

Figure D-1. VS-TC LEDs

Table D-1. VS-TC Status

LED	Indicates	Description
1	System activity	When the VS-TC is operating normally, this LED blinks several times per second to indicate that the VS-TC has been loaded successfully. If no other LEDs are lit (LED number 8 should be ON), it is waiting for a line to come up. If the LED is blinking slowly, large amounts of message traffic requiring compression are being processed.
2	Receive data	This LED indicates that the VS-TC received data without transmission errors. The LED changes each time the VS-TC receives a message (it should always be blinking if operations are either polling on Multipoint or continuity checking for Point-to-Point).
3	Transmit data	When this LED is on, the VS-TC is transmitting data on the line (data, polls, continuity checking). Unlike LED 2, this LED is on only when the VS-TC is actively transmitting.
4	Data carrier detect	This LED means that both your system's and the remote system's modems are operating. It may stay on or blink in normal operation, depending on the mode (half duplex or full duplex).
5	Session active	If this LED is lit, at least one communications session has been established. This LED can mean, for example, that a user has logged on to a remote VS or that the File Transfer Manager is active.
6	System traffic active	When this LED is on, the VS-TC is exchanging information with your system. LEDs 2 and 3 indicate that the VS-TC is exchanging data over the link. This LED indicates that the VS-TC is exchanging data with your system.
7	Refusing new traffic	When this LED is lit, the VS-TC has more traffic than it can handle and is temporarily refusing additional user messages. This is not a fatal condition, since the software has extensive logic to prevent traffic from increasing to a fatal level. If this LED is on frequently, however, performance is suffering, and you should consider more communications hardware or operating at a faster line speed.

(continued)

Table D-1. VS-TC Status (continued)

LED	Indicates	Description
8	Diagnostic mode	This LED should be on and not blinking during an operation. It indicates that the VS-TC is in normal operation.
	Idle mode	LEDs flashing in sequence from left to right indicate that the VS-TC is in an idle state.

D.3 CIU LEDs

The front panel of a CIU has three LEDs and a recessed reset button as shown in Figure D-2.

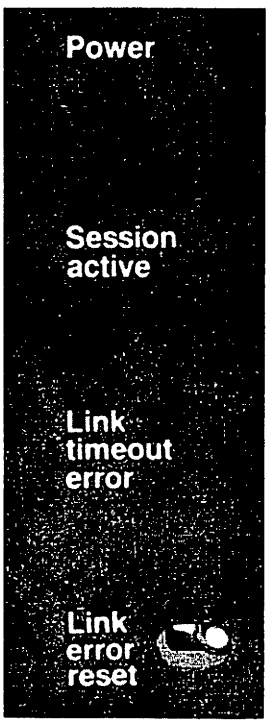

Figure D-2. CIU Front Panel LEDs

Table D-2 lists and explains each CIU LED.

Table D-2. CIU Status

LED	Description
Power	Flashes for 30 seconds while internal CIU diagnostics are being performed, and stays on while the CIU is operational. It continues flashing if power-on diagnostics detect a malfunction. Internal diagnostics should be completed in less than 90 seconds. If the Power LED keeps flashing after 90 seconds, call your Wang customer engineer.
Session Active	On when the CIU has one or more active sessions.
Link Timeout Error	On if the CIU transmitter is active longer than the maximum specified transmit time (3 milliseconds). A transmitter that is on longer automatically shuts off. To restart the transmitter, press and release the Link Error Reset button on the front panel. Once restarted the transmitter tries to access Wang Band to allow normal communications to be reestablished without reinitializing the CIU. If the Link Timeout Error LED stays on after several tries, call your Wang customer engineer.

In addition to the front panel LEDs, a CIU has eight internal LEDs that are used by Wang customer engineers. These LEDs are visible through the vent in the side panel of the CIU. They provide both diagnostic and normal activity information. Table D-3 explains the meaning of each LED.

Table D-3. CIU Diagnostic LEDs

LED	Description
1	This LED is off if the CIU is in the idle state. If it appears to be on almost constantly, the CIU is heavily loaded.
2	The status of this LED changes each time a message is transmitted to the network.
3	The status of this LED changes each time a message is received from the network.
4	When this LED is on, the CIU is available to transmit or receive over the network (CIU ready: DTR).
5	When this LED is on, the CIU is available to exchange data with the system that it serves (initialization complete).
6	The status of this LED changes each time the CIU receives a message from its system.
7	The status of this LED changes each time the CIU sends a message to its system.
8	If this LED is on, it indicates a CIU error, due either to a software or a hardware problem. In this case, the meaning of the other seven LEDs change in relation to the problem.

The meaning of each LED that is listed in Table D-3 changes if LED 8 is illuminated along with it. Those changes are listed in Table D-4.

Table D-4. Changes to CIU Diagnostic LEDs

LED	Description
1	Indicates a network transmit status error. Such an error may be due to a missing or broken drop cable or a failure in the main WangNet cable. Call your Wang customer engineer.
2	Indicates a hardware problem. Call your Wang customer engineer.
1 & 2	Indicates a hardware problem. Call your Wang customer engineer.
3	Indicates a possible hardware problem. If LEDs 8 and 3 are on, the Link Timeout LED on the front panel may also be on.
1 & 3	Indicates a duplicate cable address. Another CIU on the network with the same address is active at the time your CIU is initialized. Check your configuration file to see if there is a remote system network address that is the same as your system's network address. If there is no duplication, an active system exists on the network that is not defined in your configuration file.

If one of the errors in Table D-4 occurs, the VS Operator's Console displays the message "Assistance required on device ##," and your system shuts down communications with the CIU.

D.4 COMMUNICATIONS SUSPENSION AND RESUMPTION

Network communications can be suspended for a number of reasons, such as transmission line or hardware failures. However, problems with the network should not affect the local operation of your system. If communications to or from your system are suspended, or you cannot resume communications, check the Operator's Console for operator notification messages (refer to Appendix C), or try to work through the suggestions listed in Table D-5.

Table D-5. Communications Problems and Responses

Problem	Response
System can't load microcode to DLP	1. Check the GENEDIT file to see how many device numbers are allocated to the DLP on the IOP. Check the active WSNEDIT file to ensure that the DLP name is correct and that the protocol for the link has been specified accurately. 2. Check the cable connectors between the DLP and the VS. Try another cable. Make sure that the system name you entered through the Manage Areas function of WSNEDIT matches the System WangNet ID defined during GENEDIT. 3. Check to see if the DLP power cord is plugged in and the unit is turned on. 4. Try another port on the IOP. If possible, try one that you know is working. This may necessitate a different WSNEDIT file to get the DLP name to match the port number. This action is a last resort, as it is necessary to reIPL the VS.
Assistance required by device ####.	1. If the device number indicated in the error message matches the lowest device number assigned to the CIU, there may be a duplicate address problem (check for lights on the side: 8, 1, and 3). Check with the Network Administrator for a system with the same address as the one you tried to use for your system. 2. If the DLP is a CIU, check the side LEDs and refer to Section D.4. 3. This message may also mean that the DLP name in WSNEDIT is wrong. If it identifies the wrong IOP port, the microcode may have been loaded into the wrong device.

(continued)

Table D-5. Communications Problems and Responses (continued)

Problem	Response
VS and DLP IPL, but there is no communication.	1. Press PF12 (Telecommunications), then PF6 (Communications Devices) to see that the lowest device number assigned to the DLP is labeled "Reserved and in use". If not, a configuration error probably exists. Verify that the WangNet ID assigned in the GENEDIT file is defined in the directory file. 2. Press PF12 (Telecommunications), then PF3 (Communications Access) to see if communications are inhibited. 3. Press PF12 (Telecommunications), then PF4 (Communications Links) to see if communications are inhibited for the link.
The VS cannot communicate with a specific system but can communicate with other systems.	1. Call the remote system administrator to see if that system is running. Ask if your WangNet ID (as defined in GENEDIT) is the same as the name assigned to your system in the remote system's configuration file. 2. Check the active WSNEDIT file and the directory file. Is the remote system defined, and are its network name and address correct? 3. Check to see if the remote system can be reached in some other way. For example, if you cannot log on to the remote system, can you transfer files to that system? If so, check to see if either service is inhibited for each system. 4. Have the configuration files of either system been changed? Has either system been upgraded to a new software release?
Can't attach to another VS.	1. Check to see if there is any communication to the remote VS. Is the File Transfer service running between the two systems? If there is no communication at all, check the configuration files of both systems to see if the necessary addresses and IDs are correct.

(continued)

Table D-5. Communications Problems and Responses (continued)

Problem	Response
	2. See if any local user can attach to the remote VS. If so, either the ID and password are invalid, or no more virtual circuits to the remote VS are available. 3. Press PF12 (Telecommunications), then PF5 (Communications Systems) to see if the service has been inhibited to the remote VS.
The File Transfer Manager cannot connect with a remote system.	1. If the remote system is a VS, is the File Transfer service inhibited to your system? 2. Are passwords specified at either system? If so, does the Send password of the remote system match the Receive password listed in your WSNEDIT file? Does the Receive password of the remote system match the Send password listed for your system in your WSNEDIT file? 3. Is the File Transfer Manager able to connect with any remote system? Are there circuits available?
Cannot find file or document sent to the local VS.	1. If the request was a retrieve request, check the retrieve queue for its status. 2. Print or display the File Transfer Log to see if the transfer took place. 3. Find out if a transfer group was used. If so, check its default WP library (for documents), or default file, volume, and library names (for files). Check to see if a remote system group is associated with the remote system, and check its defaults. See if user override is allowed in the transfer group definition. If so, check with the sender to see what document ID or file, library, and volume were entered when the request was made.

D.5 PERIPHERALS BAND TROUBLESHOOTING

Table D-6 lists several possible Peripherals Band problems and possible responses to those problems.

Table D-6. Peripherals Band Problems and Responses

Problem	Response
Nothing works on a given channel.	1. Check to see if other channels are working. If none are working, the backbone signal levels probably need checking. Call your Wang customer engineer. 2. If the other channels are working, check the local ports and the channel setting on the CPU. If two CPUs are on the same channel, or if two WangNet IOPs in the same system are on the same channel, neither will function properly. Turn off one CPU and see if the other one functions properly. 3. Make sure that the numbered setting on the NETMUX or Ergo workstations correspond to the channel number listed in the GENEDIT file.
An Ergo workstation gets no response from its CPU.	1. Check to see if any other devices can communicate with the same CPU through the Peripherals Band. 2. Check the manufacturing ID and make sure the same ID is listed in the configuration. 3. Check that the channel number on the Ergo workstation matches the channel number on the CPU. 4. Try a user outlet that you know is working, or try another cable between the Ergo workstation and the user outlet.
A device connected to a local port does not work.	1. Check the configuration file to see if the port is included. If so, check to see if the devices connected to the other ports are working. 2. If possible, try to connect the device to a local port that you know is working.

(continued)

Table D-6. Peripherals Band Problems and Responses (continued)

Problem	Response
A device connected to a local port does not work (continued).	3. Try another cable between the device and the IOP. 4. Check the configuration file to ensure that the correct type of device is configured.
NETMUX does not work.	1. Check the channel thumbwheel setting. If it matches the setting in GENEDIT, check to see if other NETMUXES or Ergo workstations on the channel are working. Make sure the CPU is functioning normally. 2. Check the manufacturing ID of the NETMUX. See if the ID matches the one listed in the configuration file. 3. Try a different user outlet (one that you know is working). Try a different cable between the Netmux and the user outlet.
A NETMUX port does not work	1. Check the configuration file to see if the port is configured. Check to see if the device type listed in the Description field is the correct type for the device connected to the NETMUX port. 2. If the port is configured properly, try a working device of the same type on the port. 3. Try the device on a port that is working. (Be sure that the Description field for that port is configured for the type of device that you are checking.)

APPENDIX E
TRANSFER LOG FILE RETURN CODES

The File Transfer Log includes a three-digit return code under the column heading, RC. Each return code refers to a specific member of a set of messages that inform you of the outcome of the File Transfer attempt. Any return code other than a 000 indicates that the transfer was unsuccessful. Table E-1 gives a complete list of the return codes and their meanings.

Table E-1. File Transfer Return Codes and Their Meanings

Return Code	Meaning
000	Transfer completed successfully.
004	Input volume not mounted. The volume containing the file or document to be transferred was not mounted.
008	Output volume not mounted. The volume on which the user requested to have the transferred file placed was not mounted.
012	Input volume exclusive. Input volume mounted for exclusive use.
016	Output volume exclusive. Output volume mounted for exclusive use.
020	Input file conflict (possession conflict).
024	Output file conflict.
028	Transfer aborted by local operator.
032	Transfer aborted by remote operator.
036	Insufficient memory to process transfer.
040	File Transfer software error. Program logic error within File Transfer Manager code.

(continued)

Table E-1. File Transfer Return Codes and Their Meanings (continued)

Return Code	Meaning
044	File Transfer Manager is busy. It cannot accept a transfer request at this time.
048	The disk is full. The transfer request cannot be processed at this time.
064	Warning -- conditional completion: input file could not be scratched as requested.
068	Input/Output (I/O) error on input file.
072	I/O error on output file.
076	I/O error on WP document (during password verification.
080	I/O error on WSDATA. Word Processing (WP) was not installed properly on the VS system.
084	I/O error on Inter-System Security List file.
088	I/O error on File Transfer Group List file.
092	I/O error on system Userlist file.
096	Disk I/O error on Volume Table of Contents (VTOC).
100	VTOC unreliable.
104	Input file not found.
108	WPSDATA file not found. Word Processing (WP) was not installed properly on the VS system.
112	Inter-System Security List file not found.
116	File Transfer Group List file not found.
120	System Userlist File not found.
124	REPLACE option was specified as "NO" and duplicate output file exists.
128	REPLACE = YES but violation.
132	SCRATCH = YES but violation.
136	Insufficient access to send file.

(continued)

Table E-1. File Transfer Return Codes and Their Meanings (continued)

Return Code	Meaning
140	Insufficient access to request file.
144	User does not exist (not found in system Userlist).
148	Remote site's access rights are undefined.
152	Remote site not configured.
156	File Transfer Service not supported for remote site.
160	No default Transfer Group record defined.
168	Invalid parameter specified.
172	Incorrect document password specified.
176	Warning -- file was created, but submit was unsuccessful.
180	Transfer failed because of communication error.
184	File type not supported at remote node.
188	Transfer operation not supported by remote site.
255	Undefined error occurred.

WANG

Customer Comment Form

Publication Number 715-0165

Title NETWORKING WSN VS NETWORK CONTROL AND MONITORING GUIDE

Help Us Help You . . .

We've worked hard to make this document useful, readable, and technically accurate. Did we succeed? Only you can tell us! Your comments and suggestions will help us improve our technical communications. Please take a few minutes to let us know how you feel.

How did you receive this publication?

- ☐ Support or Sales Rep
- ☐ Wang Supplies Division
- ☐ From another user
- ☐ Enclosed with equipment
- ☐ Don't know
- ☐ Other _____

How did you use this Publication?

- ☐ Introduction to the subject
- ☐ Classroom text (student)
- ☐ Classroom text (teacher)
- ☐ Self-study text
- ☐ Aid to advanced knowledge
- ☐ Guide to operating instructions
- ☐ As a reference manual
- ☐ Other _____

Please rate the quality of this publication in each of the following areas.

	EXCELLENT	GOOD	FAIR	POOR	VERY POOR
Technical Accuracy — Does the system work the way the manual says it does?	☐	☐	☐	☐	☐
Readability — Is the manual easy to read and understand?	☐	☐	☐	☐	☐
Clarity — Are the instructions easy to follow?	☐	☐	☐	☐	☐
Examples — Were they helpful, realistic? Were there enough of them?	☐	☐	☐	☐	☐
Organization — Was it logical? Was it easy to find what you needed to know?	☐	☐	☐	☐	☐
Illustrations — Were they clear and useful?	☐	☐	☐	☐	☐
Physical Attractiveness — What did you think of the printing, binding, etc?	☐	☐	☐	☐	☐

Were there any terms or concepts that were not defined properly? ☐ Y ☐ N If so, what were they? _____

After reading this document do you feel that you will be able to operate the equipment/software? ☐ Yes ☐ No ☐ Yes, with practice

What errors or faults did you find in the manual? (Please include page numbers) _____

Do you have any other comments or suggestions? _____

Name _____ **Street** _____

Title _____ **City** _____

Dept/Mail Stop _____ **State/Country** _____

Company _____ **Zip Code** _____ **Telephone** _____

Thank you for your help.

Printed in U.S.A. 14-3140 7-83-5C

WANG

Fold

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY CARD

FIRST CLASS PERMIT NO. 16 LOWELL, MA

POSTAGE WILL BE PAID BY ADDRESSEE

WANG LABORATORIES, INC.
PUBLICATIONS DEVELOPMENT
ONE INDUSTRIAL AVENUE
LOWELL, MASSACHUSETTS 01851

Fold

Cut along dotted line.

WANG

To Order by Phone, Call:
(800)225-0234

Order Form for Wang Manuals and Documentation

① Customer Number (If Known)

② Bill To: Ship To:

③ Customer Contact: ( ) ( ) Phone Name

④ Date Purchase Order Number

⑤ Taxable Yes ☐ No ☐ ⑥ Tax Exempt Number ⑦ Credit This Order to A Wang Salesperson Please Complete Salesperson's Name Employee No. RDB No.

⑧ Document Number	Description	Quantity	⑨ Unit Price	Total Price

⑩ Authorized Signature Date

☐ Check this box if you would like a free copy of **The Literature Catalog** (700-7647)

Sub Total	
Less Any Applicable Discount	
Sub Total	
LocalStateTax	
Total Amount	

Ordering Instructions

1. If you have purchased supplies from Wang before, and know your Customer Number, please write it here.
2. Provide appropriate Billing Address and Shipping Address.
3. Please provide a phone number and name, should it be necessary for WANG to contact you about your order.
4. Your purchase order number and date.
5. Show whether order is taxable or not.
6. If tax exempt, please provide your exemption number.
7. If you wish credit for this order to be given to a WANG salesperson, please complete.
8. Show part numbers, description and quantity for each product ordered.
9. *Pricing extensions and totaling can be completed at your option; Wang will refigure these prices and add freight on your invoice.*
10. Signature of authorized buyer and date.

Wang Supplies Division Terms and Conditions

1. **TAXES** — Prices are exclusive of all sales, use, and like taxes.
2. **DELIVERY** — Delivery will be F.O.B. Wang's plant. Customer will be billed for freight charges; and unless customer specifies otherwise, all shipments will go best way surface as determined by Wang. Wang shall not assume any liability in connection with the shipment nor shall the carrier be construed to be an agent of Wang. If the customer requests that Wang arrange for insurance the customer will be billed for the insurance charges.
3. **PAYMENT** — Terms are net 30 days from date of invoice. Unless otherwise stated by customer, partial shipments will generate partial invoices.
4. **PRICES** — The prices shown are subject to change without notice. Individual document prices may be found in the Corporate Publications Literature Catalog (700-5294)
5. **LIMITATION OF LIABILITY** — In no event shall Wang be liable for loss of data or for special, incidental or consequential damages in connection with or arising out of the use of or information contained in any manuals or documentation furnished hereunder.

Printed in U.S.A. 14-3141 7-83

WANG

Fold

NO POSTAGE
NECESSARY
IF MAILED
IN THE
UNITED STATES

BUSINESS REPLY CARD

FIRST CLASS PERMIT NO. 16 LOWELL, MA

POSTAGE WILL BE PAID BY ADDRESSEE

WangDirect
Attention: Order Entry
800 Chelmsford Street
Lowell, MA 01851

Fold

WANG

ONE INDUSTRIAL AVENUE
LOWELL, MASSACHUSETTS 01851
TEL. (617) 459-5000
TWX 710-343-6769, TELEX 94-7421

Printed in U.S.A.
715-0164
3-85