System Manual

P/N 067296-004

DCS 300

Intermec

A UNOVA Company

Intermec Technologies Corporation
6001 36th Avenue West
P.O. Box 4280
Everett, WA 98203-9280

U.S. service and technical support: 1-800-755-5505
U.S. media supplies ordering information: 1-800-227-9947

Canadian service and technical support: 1-800-688-7043
Canadian media supplies ordering information: 1-800-268-6936

Outside U.S. and Canada: Contact your local Intermec service supplier.

Manual Change Record

This page records changes that have been made to this manual. This manual was originally released at version 001.

Version	Date	Description
002	11/98	Added information on using WTP devices with the DCS 300. Removed information on the terminal template application in Chapter 11, “Using Screen Mapping.” Rearranged the chapters. Made other minor corrections throughout the entire manual.
003	3/99	Added addendum 069283-001 that documents the v1.2 software. Includes information on using WTP devices that communicate in Norand Native mode. Also documents using TN3270/TN5250 terminal sessions.
004	9/99	Modified addendum to document v1.3 software. Includes information on the Data Collection Browser (dcBrowser). Removed *Fast Setup Quick Reference Guide*.

Contents

5 Connecting to an SDLC Network

6 Connecting to the Intermec RF Network

11 Using Screen Mapping

A

Troubleshooting

B

Helpful Information

C

Using Remote Console

D

Upgrading the DCS 300 and Devices

I

Index

Before You Begin

This section introduces you to standard warranty provisions, safety precautions, warnings and cautions, document formatting conventions, and sources of additional product information.

Warranty Information

To receive a copy of the standard warranty provision for this product, contact your local Intermec sales organization. In the U.S. call (800) 755-5505, and in Canada call (800) 688-7043. Otherwise, refer to the Worldwide Sales & Service list that comes with this manual for the address and telephone number of your Intermec sales organization.

Safety Summary

Your safety is extremely important. Read and follow all warnings and cautions in this book before handling and operating Intermec equipment. You can be seriously injured, and equipment and data can be damaged if you do not follow the safety warnings and cautions.

Do not repair or adjust alone Do not repair or adjust energized equipment alone under any circumstances. Someone capable of providing first aid must always be present for your safety.

First aid Always obtain first aid or medical attention immediately after an injury. Never neglect an injury, no matter how slight it seems.

Resuscitation Begin resuscitation immediately if someone is injured and stops breathing. Any delay could result in death. To work on or near high voltage, you should be familiar with approved industrial first aid methods.

Energized equipment Never work on energized equipment unless authorized by a responsible authority. Energized electrical equipment is dangerous. Electrical shock from energized equipment can cause death. If you must perform authorized emergency work on energized equipment, be sure that you comply strictly with approved safety regulations.

Warnings and Cautions

The warnings and cautions in this manual use the following format.

Warning
A warning alerts you of an operating procedure, practice, condition, or statement that must be strictly observed to avoid death or serious injury to the persons working on the equipment.

Avertissement
Un avertissement vous alerte d'une procédure de fonctionnement, d'une méthode, d'un état ou d'un rapport qui doit être strictement respecté pour éviter l'occurrence de mort ou de blessures graves aux personnes manupulant l'équipement.

Caution
A caution alerts you to an operating procedure, practice, condition, or statement that must be strictly observed to prevent equipment damage or destruction, or corruption or loss of data.

Conseil
Une précaution vous avertit d'une procédure de fonctionnement, d'une méthode, d'un état ou d'un rapport qui doit être strictement respecté pour empêcher l'endommagement ou la destruction de l'équipement, ou l'altération ou la perte de données.

Notes: *Notes are statements that either provide extra information about a topic or contain special instructions for handling a particular condition or set of circumstances.*

About This Manual

All the information you need to install, configure, maintain, and troubleshoot the DCS 300 is in this manual. Information in this manual should be used by the person who will be installing and configuring the DCS 300. Many of the parameters, must be set by the network administrator. This manual assumes that you are familiar with your network and data communications.

Terms

- The DCS 300 is usually referred to as “the server.”
- “JANUS devices” refers to all the readers and vehicle-mount computers (VMC) in the JANUS® family of data collection computers.
- “TRAKKER Antares terminals” refer to the radio frequency and batch terminals in the TRAKKER® Antares™ terminal family.
- “TCP/IP terminals” refers to all the devices and terminals that communicate using TCP/IP, instead of UDP Plus.
- “UDP Plus terminals” refers to all the devices and terminals that communicate using UDP Plus, instead of TCP/IP.
- “WTP devices” refers to all the devices and terminals that communicate using WTP (wireless transport protocol).
- “Data collection devices” and “devices” refers to the JANUS devices, TRAKKER Antares terminals, WTP devices, and other devices that communicate through the DCS 300.

Conventions

This manual uses these conventions to explain how to use your mouse and to emphasize input from a PC keyboard, a device keypad, and a bar code. It also uses special conventions for commands.

Mouse Actions

All the procedures in this manual assume that you are using a mouse to navigate within menus and dialog boxes. The following commands describe specific mouse actions:

Select/Choose Move the mouse pointer to an item and press the left mouse button once. The item or command is highlighted. For example, when you select an object in a list box, it is highlighted.

Double-click Move your mouse pointer to the item and click the left mouse button twice quickly. In many dialog boxes, you can double-click on an item instead of selecting it and choosing a button.

Input From a Host or PC Keyboard

When you need to press keys on your host or PC, they are emphasized in **bold**. For example, "press **Enter**" means you press the key labeled "Enter" on the keyboard.

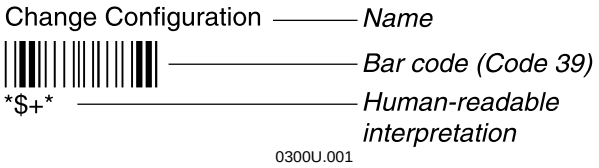
When you need to press and release a series of keys in order, the keys appear in order with no connectors. When you need to press more than one key at the same time, the keys are connected by a dash in the text. For example, press **Ctrl-Alt-Del** to perform a warm boot on a PC. When the keys are connected by a dash, you need to press and hold the keys in the order they appear in the text.

Input From a Device Keypad

When you need to press keys on the devices, they are illustrated with icons that resemble the keys. For example, "press enter" means you press the key labeled "Enter" on the device keypad.

Input From a Bar Code

You can use your devices to scan the bar codes that are provided in this manual to enter data or perform a command. The bar code labels in this manual are printed in the Code 39 symbology. Each bar code includes the name and human-readable interpretation.



The asterisks (*) at the beginning and end of the human-readable interpretation are the start and stop codes for a Code 39 bar code label. If you are creating bar code labels with a bar code utility, it may automatically supply the asterisks as the start and stop code, so that you only need to type the actual text of the command. You can also create and print configuration labels and reader command labels in Code 93, which has its own start and stop codes.

Commands

Command syntax is shown in the text as it should be entered. For example, to see a list of directories on the JANUS device, type this command:

```
dir
```

If a command line includes both required and optional parameters, optional parameters are enclosed in braces [ ].

Configuration commands use the convention *data* to indicate variables. Replace the term *data* with one of the options listed with the command syntax. For example, the configuration command for beep volume is BV*data* where *data* can be a number from 0 through 4.

Procedures

Throughout this manual you add, edit, and delete objects. For example, an object can be a host or a terminal session. Whenever you need to add objects, the procedure contains descriptions of all the fields, default values, and step-by-step instructions. Use these instructions for editing and deleting objects.

Editing an Object

1. In the dialog box, from the list box, select an object to edit.
2. Choose Edit. The next dialog box appears.
3. Edit the information in the fields.
4. Choose OK to save your changes and return to the first dialog box.

Deleting an Object

1. In the dialog box, from the list box, select an object to delete.
2. Choose Delete. A message box appears confirming that you want to delete the object.

   Note: *You may not be able to delete an object if it is linked to another object.*

3. Choose Delete. The object is removed from the list box.
4. Choose OK to save your changes and return to the main menu.

Other Intermec Manuals

You may need additional information when working with the DCS 300 in an Intermec data collection network. Please visit our web site at www.intermec.com to access many of our available manuals in PDF format. Your local Intermec representative or distributor can help you order printed versions of Intermec manuals.

Manual	Intermec Part No.
DCS 300 Technical Reference Manual	067717

1

Learning About the DCS 300

This chapter helps you learn about the features of the DCS 300 and how the server works with your LAN and Intermec's data collection network.

Chapter Checklist

Done?	Task	Page
❑	Understand the features of your DCS 300.	1-4
❑	Unpack the server.	1-6
❑	Identify the components on the front and rear panels.	1-7
❑	Understand the main menu, online help, how to navigate through dialog boxes, and the most common buttons in the graphical user interface (GUI).	1-9
❑	Understand how the server works and how transactions are routed in your data collection network.	1-12

If you already understand and have performed these tasks, proceed to Chapter 2, "Setting Up the DCS 300."

Features

The DCS 300 is a data collection server that connects Intermec's wired and wireless products either to your local area network or directly to a host. Your server has many important features that make it easy to integrate it into your data collection system. These features include:

- An easy-to-use Fast Setup program with a graphical user interface (GUI). Fast Setup uses default values to help you get the DCS 300 quickly connected to your network.
- An Advanced Setup program that uses a GUI to help you customize the DCS 300.
- Network adapter cards that support connections to hosts: Ethernet, token ring, twinaxial, coaxial, and SDLC networks.
- Dynamic Host Configuration Protocol (DHCP) client support for the DCS 300.
- Domain Naming Services (DNS) client support for the DCS 300.
- VT/ANSI terminal emulation for JANUS® devices and TRAKKER® Antares™ terminals to TCP/IP hosts.
- 5250/3270 terminal emulation for JANUS devices and TRAKKER Antares terminals to SNA hosts.
- TN5250/TN3270 for JANUS 2.4 GHz RF devices and TRAKKER Antares terminals to TCP/IP hosts that support Telnet.
- Peer-to-peer communications for TCP/IP and APPC.
- Direct TCP/IP socket interface between hosts and devices.
- Optional Script Builder Tool that lets you create custom screens and script files so that you can run VT, ANSI, 5250, or 3270 screen mapping.
- Optional RF cards (up to two) that support Intermec's 900 MHz RF network. Each card supports up to four 9181 Base Radio Units (BRUs).
- Migration to or support for Intermec's 9180 Network Controller.
- Support for Intermec's CrossBar network through existing CrossBar controllers.
- Ability to store and forward data from your devices to your hosts.
- Local management of external Intermec controllers and other devices.
- Routing of transactions to one or multiple hosts.
- Support for international text pass-through for peer-to-peer and direct TCP/IP applications.
- Localized language support for single-byte character sets (SBCS) in devices that are running terminal emulation.
- Support for double-byte character sets (DBCS) and data streams.

- Firmware Upgrade Utility that allows you to upgrade the firmware on your TRAKKER Antares terminals.
- Support for remote access to the DCS 300 using a third party remote console package.
- Ability to print to a printer attached to a terminal serial port that is within all VT/ANSI terminal emulation clients.

What's New in V1.1?

- VT/ANSI, 5250, and 3270 terminal emulation for WTP (wireless transport protocol) devices.
- TN5250 and TN3270 terminal emulation for WTP devices.
- Peer-to-peer communications for TCP/IP and APPC for the 6400.
- Optional VT/ANSI, 5250, and 3270 screen mapping for the 6400.
- Direct TCP/IP socket interface between hosts and the 6400.
- Support for up to 254 simultaneous connections.
- Support for multiple TE sessions running simultaneously on a WTP device.
- DCS 300 Upgrade Utility for upgrading the DCS 300 software.

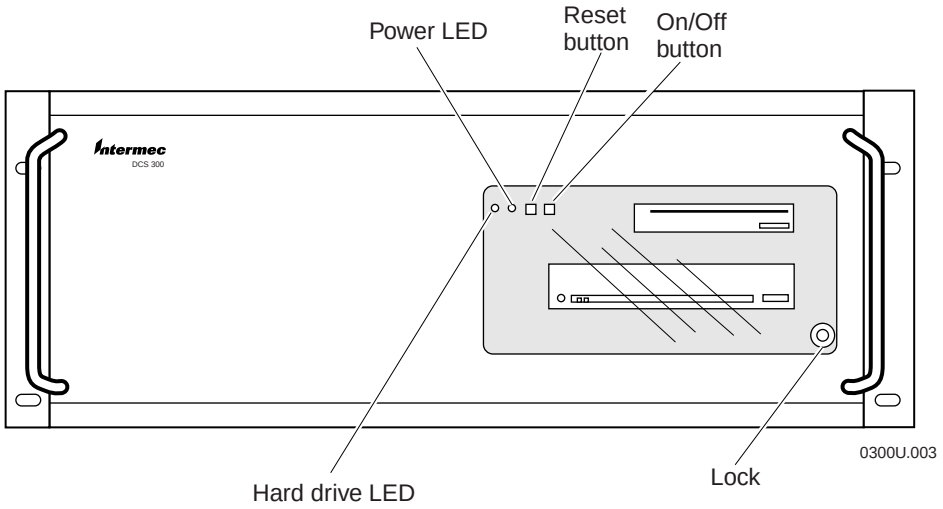
Unpacking the DCS 300

1. Set the DCS 300 box on a clean, stable, flat surface and remove the accessories, packing material, and the DCS 300 from the shipping container.
2. Save the shipping container and packing material in case you need to move or ship your server.
3. Verify the contents of the shipping container against the list below. If any parts are missing, contact your local Intermec representative.
   - DCS 300
   - AC power cord
   - Keyboard
   - Mouse
   - 3.5-inch disk to use for backing up your system files and run-time configuration
   - *DCS 300 Manual Supplement*
   - *DCS 300 System Manual*, which includes the *Fast Setup Quick Reference Guide* and the *DCS 300 User's Manual*
4. Report any damage or defects. Intermec thoroughly tested and inspected the server before it was shipped to you. If any items are damaged, please take the following steps to correct the problem.
   - Take photographs, if necessary.
   - Contact the transport carrier.
   - Return the DCS 300 package to Intermec.

Description

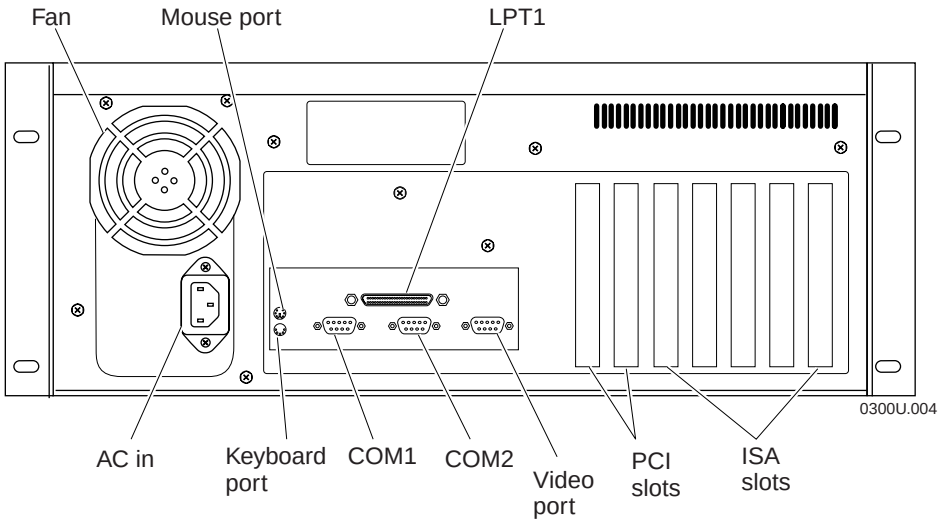
The DCS 300 contains several components on the front panel and on the rear panel that you should be able to identify.

Understanding the Front Panel



Component	Description
Hard drive LED	Lights when data is being read from or written to the hard disk.
Power LED	Lights when the server power is on.
Reset button	Performs a warm boot on the server. Same as pressing **Ctrl**-**Alt**-**Del** on the keyboard.
On/Off button	Turns the power to the server on and off.
Lock	Locks the front panel.

Understanding the Rear Panel



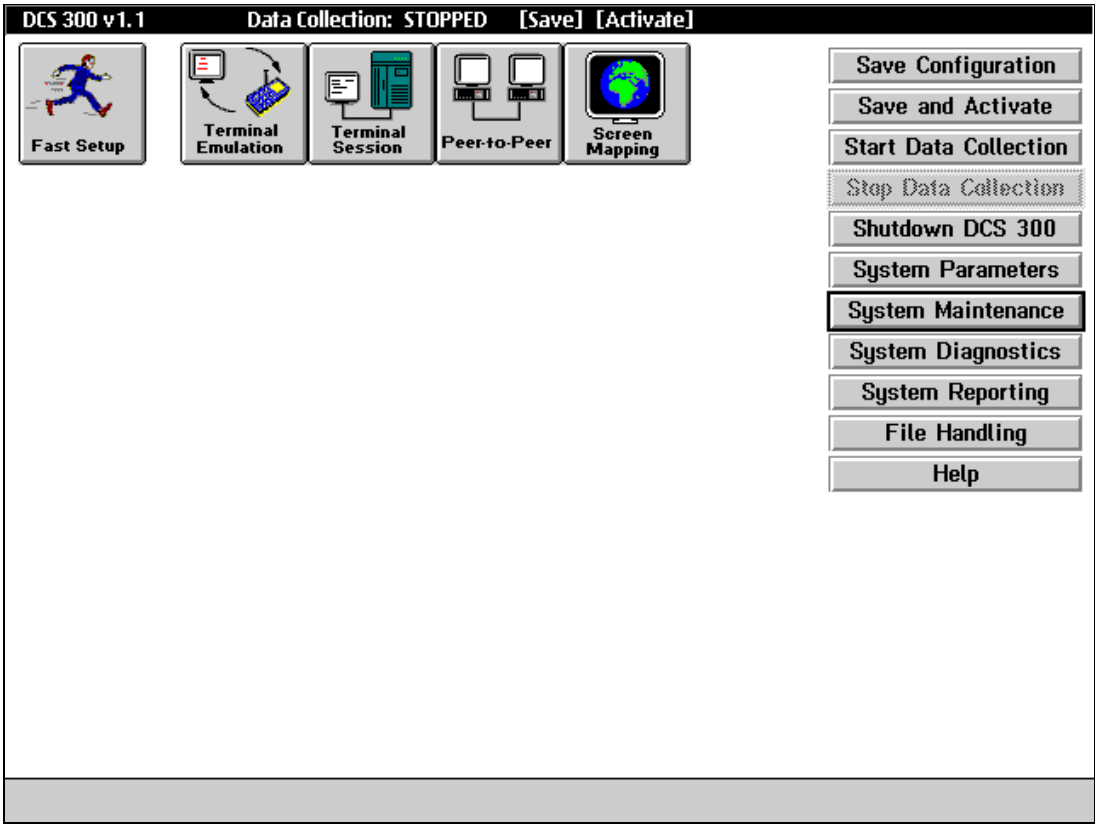
Component	Description
Fan	Prevents your server from overheating. When situating your server, do not place it where the fan is obstructed.
Mouse port	Connects the mouse to your server.
LPT1	Provides parallel port connection for accessories.
AC in	Connects to one end of the AC power cord that provides power to the server.
Keyboard port	Connects the keyboard to your server.
COM1, COM2	Provides serial port connections for external Intermec controllers, a modem, or other devices that require serial ports to connect to your server.
Video port	Connects the monitor to your server.
PCI slots	Contains your Ethernet cards.
ISA slots	Contains other network adapter cards.

About the Graphical User Interface

When you are ready to turn on the DCS 300, push the power button. When you power on the server for the first time, a dialog box appears that lists the network adapter cards in your server. Choose one of the following:

- If you want this dialog box to appear every time the server boots, choose Show at Boot Time. This dialog box may be helpful when troubleshooting the server.
- If you never want this dialog box to appear, choose Hide at Boot Time.

The main menu appears.



The main menu has three parts:

Title bar The bar at the top of the main menu contains the name and version. It also lets you know if data collection is started or stopped. If you are configuring the server, [Save] and [Activate] may appear in the title bar. These prompts remind you that you have made changes to the configuration that have not been saved or activated. When you choose Save Configuration or Save and Activate, these prompts disappear.

Toolbar buttons The buttons across the top of the main menu are grouped into two sections: Fast Setup and Advanced Setup. The *Fast Setup Quick Reference Guide* addresses how to use the first button, Fast Setup. This user's manual addresses how to use the next four buttons that comprise Advanced Setup.

Sidebar buttons The buttons on the right side of the main menu perform system functions on the server such as backing up the configuration files, viewing Hot Standby files, and defining system parameters.

Using Help

The DCS 300 includes online help that provides descriptions of the server toolbars, dialog boxes, and options. Help also provides procedural information and limited background information.

To get Help

- In any open dialog box, choose the Help button.

The Help window opens and displays the topic for the toolbar or dialog box you were using. If you requested help from the main menu, the Getting Started topic appears. You can resize and move your Help window to see more of a topic at one time or to see more of the configuration window.

Once the Help window appears, you operate the Help system by selecting topics, by choosing commands from the Help menus, or by choosing the Help control buttons at the bottom of the Help window. Topics that you can jump to are shown in colored or underlined text.

To jump to another Help topic

- Double-click the topic name. Or, press **Tab** until the topic is highlighted, and then press **Enter**.

To use the Help control buttons

- Choose Previous. Or, press **Esc**.
- Choose Search to search for help on a specific word or phrase.
- Choose Index to look up a topic in the index.
- Choose Contents to look up a topic in the contents.

To learn more about using Help

- From the sidebar buttons, choose Help.

Navigating Through Dialog Boxes

In the DCS 300, there are various ways that you can move through dialog boxes:

To Do This Action	Do This Action
Move between fields in a dialog box	Use the mouse to click a field and the cursor moves there. Use **Tab** to move the cursor from field to field. Press **Ctrl** or **Alt** and then the letter underlined in the field or button name.
Access the buttons in a dialog box	Use the mouse to click them. Press **Ctrl** or **Alt** and the letter underlined in the button name. If any button is highlighted, choose another button by pressing the letter underlined in the button name without pressing **Ctrl** or **Alt**.
Go to the end of a file	Press **Ctrl-End**.
Go to the top of a file.	Press **Ctrl-Home**.
Access a window that shows you which applications are running.	Press **Ctrl-Esc**.

Understanding the Dialog Box Buttons

These are the most common buttons that appear in the dialog boxes when you are configuring the DCS 300.

Button	Description
OK	Choose OK to save any changes you have made in the dialog box and exit from that dialog box. Your changes are saved in RAM. To save your changes to disk, from the main menu sidebar buttons choose Save Configuration.
Cancel	Choose Cancel to not save any changes you have made in the dialog box and exit from that dialog box.
Help	Choose Help in any dialog box to obtain help on the fields in that dialog box.
Close	Choose Close to exit a dialog box.
Add	Choose Add to add a new item such as a host. Choose OK to save this change. Choose Cancel to remove the item.
Edit	Select the item you want to change and choose Edit. Edit the information in the dialog box. Choose OK to save the change. Choose Cancel to restore the original values of the item.
Delete	Select the item you want to remove and choose Delete. A message box appears confirming that you want to delete the item. Choose Delete. ***Note:*** *You may not be able to delete an object if it is linked to another object.*

How the DCS 300 Works

The DCS 300 is composed of several software components working together to perform routing functions. For more information about these components, see your *DCS 300 Technical Reference Manual*.

Graphical user interface (GUI) The GUI is the software that runs on the server. You use it to set up your run-time configuration by defining the data collection equipment in the system, the names of the remote applications the server communicates with, and various transaction-related information. If you are using screen mapping, you can build script files that define how the server maps transaction fields to host screen fields. You can also define system parameters and monitor your data collection system.

Message handler The message handler performs transaction routing on transactions that are sent between devices, applications, and the server itself. The message handler routes transactions using two input Interprocess Communication (IPC) channels:

- Receive channel for data input
- ACK channel for transaction acknowledgment

When the message handler reads a transaction from the Receive channel, it examines the transaction header to determine which application(s) should receive it. The message handler then places the application name in the transaction header and writes the transaction into the input channel belonging to that application. Upon receiving the transaction, the application must write an ACK transaction into the ACK channel. Once the message handler receives the ACK transaction, it deletes its copy of the transaction.

Device communication processes (DevComms) DevComms are the interface between Intermec devices and the message handler. DevComms implement all protocols that are required to communicate with the devices. The server starts one DevComm for each communication channel that has been configured.

DevComms are designed to communicate with Intermec devices using the “out-of-box” or default protocol. You configure the DevComms when you configure the server and identify the devices.

Network communication processes (NetComms) NetComms are the communication links between remote applications and the server. TCP/IP NetComms use TCP sockets to send and receive data from the message handler. APPC NetComms use APPC sessions to send and receive data from the message handler.

NetComms provide network transparency. For example, the server writes a transaction into an input channel for an application. A local send NetComm reads the transaction from the input channel and sends it to a remote application. The remote application processes the transaction and acknowledges the receipt of the transaction from the local send NetComm. The local send NetComm then writes an ACK transaction to the ACK channel.

When a remote application sends a transaction to the server, the transaction is actually received by the receive NetComm and then forwarded to the input channel. When the server is started, it recognizes each remote application and then it creates the NetComms.

Emulator communications (EmComms) EmComms provide an interface between the server and applications running in a VT, ANSI, 5250, or 3270 terminal emulator. EmComms allow transaction data from a device to be mapped to host applications running in a terminal emulator.

Note: *The terminal sessions are established and run on the server, not on the devices.*

For example, a transaction is built by a JR2020 and then transmitted through the BRU to the server. The server DevComm routes the transaction to the Receive channel where the message handler receives it and passes the transaction along to the screen mapping application (EmComm) input channel. Then, the data in the transaction is routed to the screen mapping application that uses a script file to put the data into the 5250 emulator screens on the host. The screen mapping application then sends an ACK to the message handler indicating that it received the transaction data.

Terminal session manager (TSM) The server TSM establishes sessions and routes messages between a host application and the TE software running on the JANUS devices and TRAKKER Antares terminals. When the device requests a session to start, the terminal session manager verifies that sessions are available. If a session is available, the device is connected. If no session is available, the terminal session manager returns an error to the device.

About Transactions

Communications from an application through the DCS 300 to devices and other applications involve two types of transactions: data transactions and system transactions.

Data Transactions

The message handler uses the transaction ID to determine the destinations for a transaction; it is the primary routing mechanism used by the DCS 300. When a device transmits a data stream, the data stream contains the transaction ID. The DevComm locate the end of the transaction ID using the system delimiter. Then, the DevComm removes the transaction ID from the data stream, and places it in the header of the transaction. If a device cannot place a transaction ID in the data stream, you can configure one for it.

All transactions are date/time stamped in the transaction header. The server also maintains a unique message number counter for each application. All data transactions are sequential; therefore, an application can use its counter to check for transaction continuity. Each transaction has a well-defined structure consisting of a transaction header and a data field.

- The transaction header contains 96 bytes.
- The transaction data can consist of a maximum of 1024 bytes.

System Transactions

System transactions provide various system control and system operation functions. They consist of a single mnemonic string, such as Inter. To send a system transaction to the DCS 300, the application places the system transaction mnemonic into the destination field, DestApId, of the transaction header and sets the system transaction flag to S.

Applications must acknowledge all system transactions. For example, all applications must recognize the system transaction DcmSysHalt, which informs applications that the server has shut down.

For more information on system transactions, see the *DCS 300 Technical Reference Manual*.

How the DCS 300 Routes Transactions

Transactions have a well-defined structure consisting of a header and data. The header contains a transaction ID, which the DCS 300 uses to determine the destination for a transaction. The transaction ID is the primary routing mechanism used by the server.

When the server receives a transaction, it checks the system message flag. If the transaction is a system transaction, it is executed immediately. If the transaction is a data transaction, the server routes the transaction by examining the transaction header:

- If the destination field in the transaction header contains a name, the server treats the transaction as if it came from an application. It uses the destination name to forward the transaction to the correct application or device.
- If the destination field in the transaction header is blank, the server uses the transaction ID field of the header to determine where to send the transaction.

To ensure data integrity, a handshake is built into the routing system. When the server delivers a transaction to a destination, it retains a copy of the transaction until the application sends back an ACK transaction. This ACK transaction is received by the server ACK channel and it tells the server that the application has responsibility for the transaction. Only then does the server discard its copy and send another transaction to the application. Hot Standby logic controls how long the server waits for an ACK transaction and what it does with other transactions while waiting.

Routing Transactions From Applications

The DCS 300 can route transactions from applications to devices or to other applications. These transactions contain a logical name for the destination. The logical name is either the name of an application or the name given to a device. The server searches through internal tables that are created from the run-time configuration to find all the correct information about the destination.

If the destination is a device, the message handler determines the name of the DevComm that is servicing that device and forwards the transaction to it. The DevComm receives the transaction, translates the logical name into a physical device address, strips the header from the transaction, and transmits the data to the device.

If the destination is another application, the routing process is more direct: the message handler only needs to know if the receiving transaction is active or inactive.

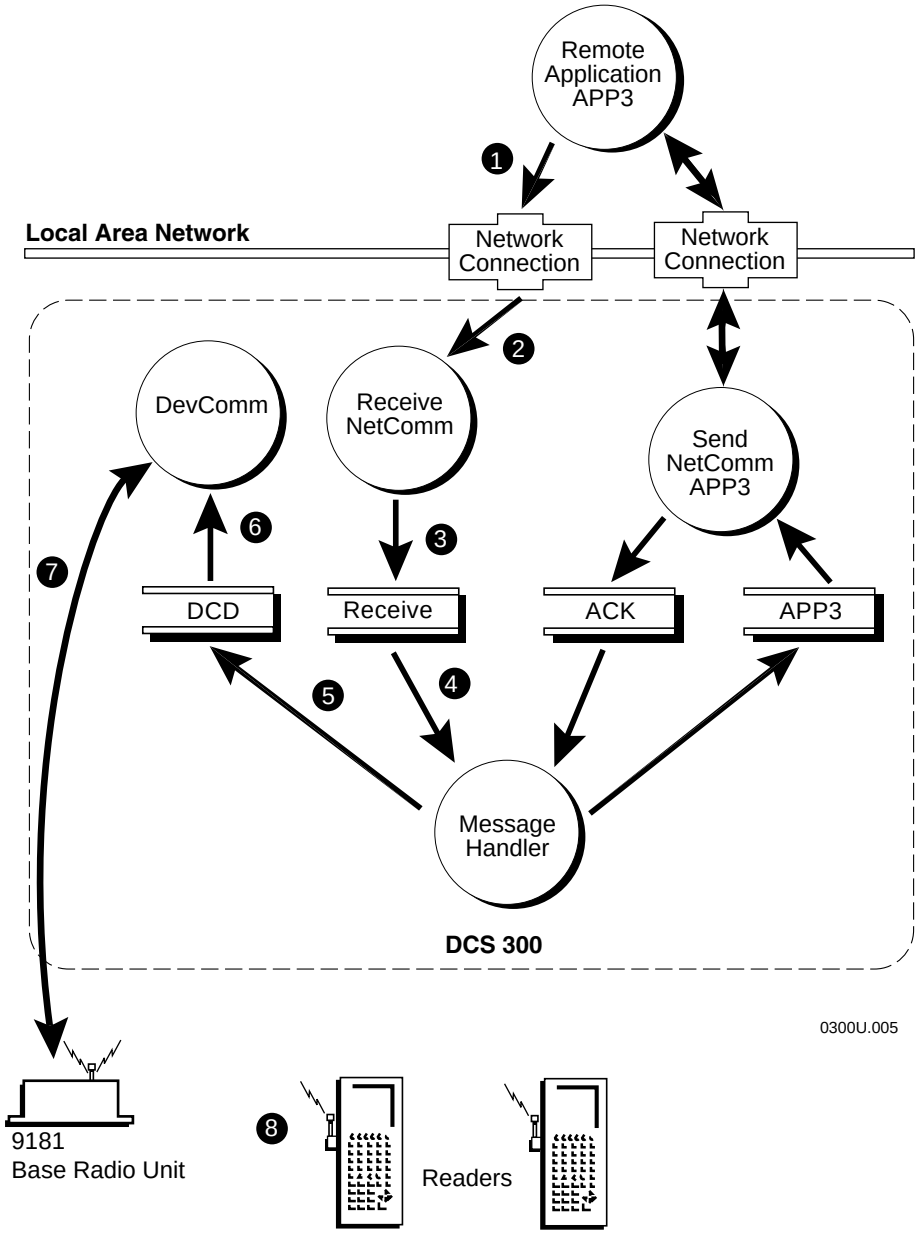
In this example, the application sends a transaction to a specific destination using the destination name in the transaction header. The numbers on the following paragraphs correspond to the numbers on the illustration on the next page.

1. The remote application (APP3) writes the transaction to the local receive NetComm through the network connection.
2. The receive NetComm reads the transaction from APP3 and processes it.
3. The receive NetComm writes the transaction to the Receive channel.
4. The message handler reads the transaction from the Receive channel.
5. The message handler determines the source of information and sends the transaction to the proper DevComm channel.
6. The DevComm reads the transaction from its DCD channel.
7. The DevComm translates the logical name into a physical address, strips the header information from the transaction packet, and delivers the data to the device.
8. The server delivers the transaction to the proper reader using the ID placed on the transaction by the DevComm.

Note: *A destination name is not a requirement. You can create an application that places a transaction ID in the transaction header instead of supplying a destination. This practice forces the message handler to route the transaction as if it came from a device.*

Note: *If a delivery response (success or failure) was configured in Advanced Setup, the DevComm delivers this response to the message handler. The response is then routed to APP3. DevComm responses only apply for interactive remote applications.*

Routing Transactions From Applications



Routing Transactions From Devices

This example discusses the steps to move data from the device to the application. The numbers on the following paragraphs correspond to the numbers on the illustration on the next page.

1. Data is entered at the bar code reader and transmitted through the BRU to the server.
2. A DevComm receives the transaction through its hardware link.
3. A header is attached to the transaction and the transaction is placed in the Receive channel.
4. The message handler retrieves the transaction from its Receive channel and completes the following sequence:

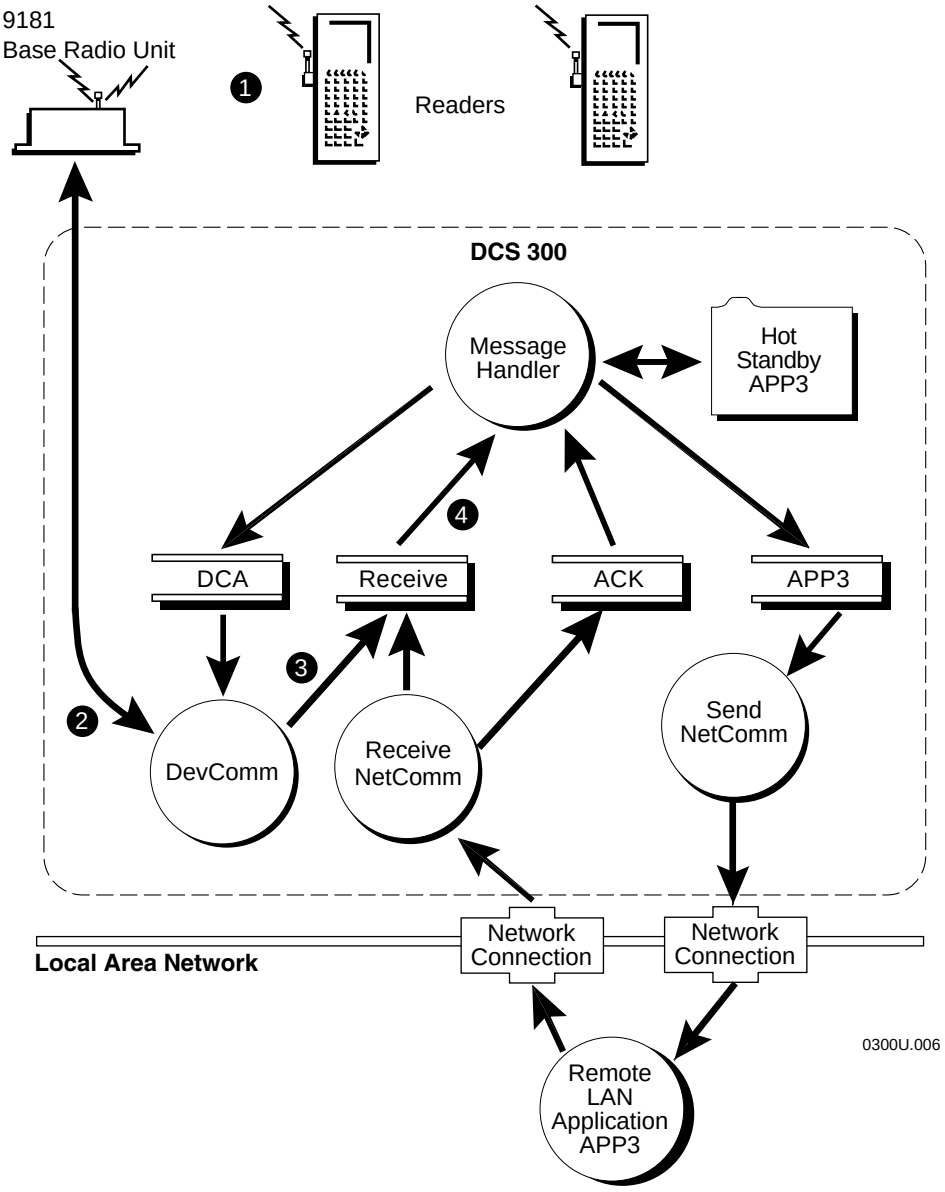
   Timestamp The message handler gets the current time from the system and places it in the transaction header.

   Determine source of transaction If the transaction has the system message flag set to D for data and the destination field is blank, the message handler assumes the transaction came from a device. If the destination field is not blank, the message handler assumes the transaction came from an application.

   Route transaction The message handler routes the transaction to the correct destination based on the transaction ID. Transactions from devices do not have a logical destination. The message handler searches its internal tables to find all the routes defined for the transaction ID. If the transaction ID is valid but has no routes defined for it, or if the transaction ID is invalid or unknown, it is treated as a failed transaction. If the routes are defined, the message handler proceeds to the next step.

   Assign message number The message handler assigns a message number and places it into the transaction header. The message handler maintains a separate counter for each application it knows about.

Routing Transactions From Devices



Note: *Steps 5 through 8 and 12 occur for each application that receives a transaction sent by the message handler. Steps 9, 10, and 11 are different for TCP/IP and APPC applications.*

5. The message handler determines the correct destination for the transaction. It then checks a flag for the destination to see if it is currently an active or an inactive application:
   - If the application is active, the message handler attempts to deliver the transaction to the application's channel.
   - If the application is inactive and the transaction cannot be delivered, the message handler stores the transaction in the application's Hot Standby file.
6. The send NetComm reads the transaction from the APP3 channel and processes the transaction.
7. The send NetComm routes the transaction to the remote application (APP3).
8. The remote application (APP3) reads the transaction sent from the send NetComm and processes it.

For TCP/IP Applications

T9. The remote application writes the network ACK transaction to the send NetComm.

T10. The remote application writes an ACK transaction to the receive NetComm. The receive NetComm reads the ACK transaction sent from the remote application.

T11. The receive NetComm writes the ACK transaction to the ACK channel and it writes a network ACK to the remote application.

The remote application reads the network ACK from the receive NetComm.

For APPC Applications

A9. The remote application sends the CONFIRMED verb to the send NetComm to acknowledge the transaction.

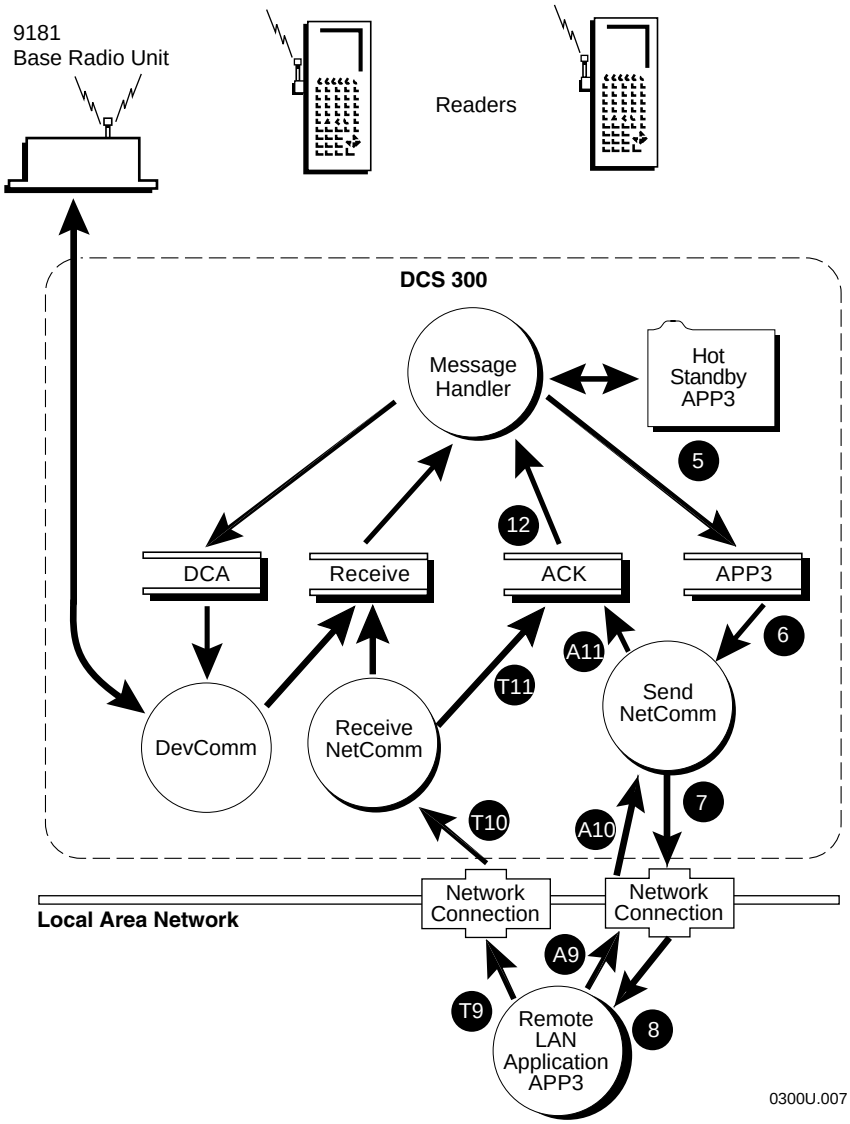
A10. The send NetComm receives the CONFIRMED verb.

A11. The send NetComm writes the ACK transaction to the message handler's ACK channel.

12. The message handler reads the ACK transaction from the ACK channel.

Note: *The APPC NetComms do not support the transmission of data in an ACK transaction. For the remote application to send acknowledgment data to a device, it must send an unsolicited transaction through the Receive channel.*

Routing Transactions From Devices (continued)



How the DCS 300 Acknowledges Transactions

After the DCS 300 attempts to deliver a transaction from an application to a data collection device, it can send a delivery response (success or failure) to the originating application. If you configure the server to send a delivery response, it returns a successful message indicating the transaction was accepted by the device or it returns a failure message if the transaction was not stored in the Hot Standby file.

A success delivery response for external controllers only indicates that the transaction was successfully transmitted to the device that is communicating directly with the server. For example, the response may only have reached the 9180 and not the JR2020. If the application needs confirmation from the device, the system must be configured so there is a complete application-to-device handshake.

If the server fails to deliver a transaction to a device, the transaction is not discarded. The server saves the transaction in the Hot Standby file and retransmits it when the device comes back online. You can use a failure delivery response to inform the application that the transaction was saved in the Hot Standby file.

How the DCS 300 Ensures Data Integrity

The DCS 300 ensures data integrity from data collection devices to applications through the protocol handshakes that exist between the various components of the system. The server guarantees data integrity for all three levels of interactivity (full, partial, and none) that exist in both data integrity modes (Faster and Safer).

Interactivity With Devices

Generally there is a tradeoff between response time and how interactive the device is with an application. It may not be practical to have a scanning device interact in real-time with an application at a remote location. Instead, the device can complete a handshake with the server, which then periodically uploads data to the application in a Batch mode.

There are three levels of interactivity which the server provides to an application when it is communicating with a device in a data collection network:

- Fully interactive
- Partially interactive
- Noninteractive

The levels of interactivity refer to an application's ability to complete a handshake with the device. This handshake consists of an agreed upon protocol for verifying the transfer of data between the application and the device. Typically, the protocol is implemented in both the application and the program that is running on the device (for example, a DOS executable or an IRL program). This protocol is independent of the data link protocol that the server implements while communicating with a device, such as a JR2020.

Fully Interactive System

A fully interactive system provides the safest way to move information from a device to an application because the application always sends an acknowledgment to the device. As long as the device can retransmit the transaction if communication fails, data is not lost.

If the application is too slow or does not respond, it cannot complete the required handshake with the device. In this case, the server can be configured to automatically assume responsibility for the application's transactions by becoming interactive with the device. When the server becomes interactive with the device, it invokes the Hot Standby feature. The server sends the device a response (called the Hot Standby message) that was configured with the GUI. While an application is in Hot Standby mode, the server saves the transactions bound for that application in a Hot Standby file. The server maintains a Hot Standby file for each application it knows about. When the server invokes Hot Standby mode for an application, the application is said to be partially interactive with respect to the device.

Partially Interactive System

In a partially interactive system, the device is interactive with the server instead of the application. To guarantee data integrity, the server sends its acknowledgment to the device only after it has written a transaction to the Hot Standby file. The data in the Hot Standby file is forwarded to the application when the application becomes active with the server.

When the application becomes active and is ready to accept more data from the server, the server checks the Hot Standby file and delivers transactions to the application in a first-in-first-out (FIFO) order. The server continues to accept new transactions from the device, appending them to the end of the Hot Standby file, while it is removing transactions from the beginning of the Hot Standby file. When the application has taken delivery of all transaction in the Hot Standby file, the server terminates the Hot Standby function and allows the device to once again become fully interactive with the application.

Noninteractive System

A noninteractive system offers the fastest method of operation. In this type of system, the device does not require any application response. The data link protocol is the only guarantee that there is data integrity between the device and the server. Once the server has received a transaction, features such as Hot Standby mode are still active to ensure data integrity.

To configure the server's Hot Standby feature for noninteractive systems, you set up the server so that it sends nothing to the device when Hot Standby mode is invoked. That is, you do not configure a Hot Standby message. As a result, the device is not informed that the application has gone away and that the server is accepting the data and storing it in the Hot Standby file.

Data Integrity Modes

The DCS 300 operates in one of two data integrity modes for external Intermec controllers: Faster and Safer. You define the data integrity mode for each external controller that the server uses to communicate with devices (such as terminals, readers, and printers). For more information, see the *DCS 300 Technical Reference Manual*.

Note: *These data integrity modes are provided in addition to the normal data integrity measures that are built into the server.*

Faster Mode

Faster mode is the default integrity mode. The advantage of Faster mode is speed: the external controller can forward data to the server faster than in Safer mode. The disadvantage is a small risk that transactions will be lost if the server loses power.

Safer Mode

Safer mode provides extra data integrity for both interactive and noninteractive devices. The advantage of Safer mode is extra security: the external controller retains its copy of the transaction until the transaction reaches either the application or the Hot Standby file. The disadvantage is that the external controller cannot forward another transaction from any device until the current transaction has been acknowledged.

Note: *The out-of-box protocol for the external Intermec controllers contains a 60-second transmission timeout. This means that when the controller delivers data to the DevComm, it waits 60 seconds for an acknowledgment. If the acknowledgment is not received within this time, the data is sent again to the DevComm, creating duplicate data. One solution to this is to set the controller timeout to zero, which disables the timeout.*

Retaining Transactions in Memory

AUX_Q is an auxiliary queue in volatile memory. By default, the DCS 300 uses this queue as a temporary holding place for transactions that are waiting to be sent to a destination while the server is waiting for an ACK from that destination.

AUX_Q is used only in this situation:

- The server sends a transaction to a destination, the Hot Standby timeout begins counting down, and the server waits for an ACK.
- While waiting, the server receives another transaction for the destination. The server cannot send the transaction until it receives an ACK for the last transaction, so the server writes both transactions to AUX_Q.
- All other transactions that subsequently arrive for the destination are written to AUX_Q.
- If the server receives the ACK before the Hot Standby timeout expires, the server sends the transactions in FIFO order from AUX_Q to the destination.
- If the server does not receive the ACK before the Hot Standby timeout expires, the server writes the contents of AUX_Q to the Hot Standby file.

You can specify the number of transactions the server can hold in AUX_Q for each application and DevComm before it writes the transactions to a Hot Standby file. To do this, use the GUI to set the Transactions held in volatile memory parameter on the Peer-to-Peer Destination Parameters dialog box to one of these values:

None Transactions in AUX_Q are not entirely safe because they are held in volatile memory. You can keep the server from using AUX_Q by setting the parameter to None, which forces the server to write every transaction for a destination to that destination's Hot Standby file.

Unlimited An unlimited number of transactions can be written to AUX_Q until either the Hot Standby timeout expires or the server sends all the transactions to the destination.

Maximum (1 to 9999) When AUX_Q reaches its limit, the contents are written to the Hot Standby file. The default for this parameter is 50.

How the DCS 300 Sets Application Status

When the DCS 300 is initialized or first starts up, all application channels listed in the configuration file are assumed to be *nonactive* or batch destinations. This means that until otherwise notified, the message handler automatically routes transactions for these applications to Hot Standby files.

Applications control their active and nonactive status by sending one of these system transactions:

Inter This system transaction places the application in an active state.

NoInter This system transaction places the application in a nonactive, Hot Standby state.

When an application is active, the server waits for an ACK transaction for the duration of the Hot Standby timeout. If an ACK is not received within the timeout period, the server automatically places the application in a nonactive, Hot Standby state.

During a server shutdown, the message handler saves the status (active or nonactive) and the last message number of each application with which it was communicating. Applications that acknowledged all transactions before shutdown are considered active by the server. The next time the server starts, active applications are immediately sent a DcmRsmTran system transaction while nonactive applications are sent nothing. If the status file does not exist when the message handler starts, it assumes that all configured applications are nonactive.

Note: *The term "nonactive" with respect to an application is not the same as "noninteractive" with respect to a device.*

Active Applications

An active application completes a handshake with the DCS 300 for each transaction it receives. The message handler ensures that data is secure by requiring an ACK transaction from the application receiving the data. The server can deliver only one transaction at a time to each application. Before the server delivers a second transaction to a destination, the remote application must take responsibility for the current transaction by sending an ACK transaction.

The server waits for the ACK transaction for the length of time specified in the Hot Standby timeout. While waiting, the message handler keeps a copy of the original transaction. During this waiting period, the message handler continues to read and process new transactions from the Receive channel. If any of the new transactions are for the application that has not acknowledged the last transaction, these new transactions are saved locally in AUX_Q. As soon as the ACK transaction is received, the stored copy of the delivered transaction is deleted and a new transaction is sent to the application. The message handler creates one AUX_Q for each application.

Note: *If an application sends a Inter system transaction instead of an acknowledgment to the message handler, the message handler retransmits the last transaction it sent to that application.*

Nonactive Applications

A nonactive application has failed to complete the handshake with the DCS 300 for a transaction. An application becomes nonactive in these two situations:

- If the Hot Standby timeout expires before the server received an ACK from the application, the server places the application in a nonactive state. Also, the server writes all subsequent transactions for the application in a Hot Standby file.
- If the number of transactions in the application's AUX_Q reaches its limit, the server places the application in a nonactive state. Also, the server writes the contents of AUX_Q and all new transactions for the application into the Hot Standby file.

Sending Hot Standby Messages

When the server receives a transaction for a nonactive application, it can send a user-defined response to the device that sent the transacaction. This user-defined response is the Hot Standby message. You can use the GUI to configure a Hot Standby message for each transaction ID. The Hot Standby message can serve as a positive response to a device by indicating that the transaction was saved on disk.

Note: *If the server does not recognize the transaction ID, the server sends a bad ID response to the source of the invalid transaction. You configure this bad transaction ID response in the System Parameters dialog box.*

Also, if the application receives a transaction is from a bar code reader that is operating in computer response required mode (CRRM), the reader remains locked until a response is received or the reader times out. The server should reply with the Hot Standby message when it cannot deliver a transaction to the application.

If the Hot Standby message field is empty, the server sends nothing to the device when it saves a transaction on disk. It becomes the application's responsibility to return a response to a device when it receives the transaction. In some cases, a response may not even be required, such as when the application is receiving status transactions from printers.

Because transactions can have multiple routes, the server appends a comma to the end of a Hot Standby message followed by the name of the destination where the Hot Standby response is being sent.

For example, you can define a transaction ID (TRXID1) that gets routed to three destinations (selftest, writeit, and batchit) and has the Hot Standby message, "Data saved on disk." When the server receives the TRXID1 transaction from a device, the message handler sends a copy of the transaction to each of the defined destinations and starts a Hot Standby timer for each one. If writeit and batchit do not acknowledge the transaction before they go nonactive, the message handler sends these strings to the device that was the source the transaction:

```
Data saved on disk, writeit
Data saved on disk, batchit
```

Changing From Nonactive to Active Status

When an application is nonactive, only two events allow it to become active:

- The application sends an ACK transaction for the most recently delivered transaction. In this case, the next transaction waiting is sent.
- The application sends a Inter system transaction. In this case, if the last transaction sent to the application was not acknowledged, sending Inter causes the transaction to be retransmitted.

Active Recovery Mode

Before entering a fully active state, the application goes through a recovery period, called Active Recovery mode. The DCS 300 takes transactions from the application's Hot Standby file and sends them in chronological (FIFO) order to the application. The application must acknowledge each transaction just as if it were active. From the application's point of view, it is an active application. To determine if the application is in Active Recovery mode, examine the batch flag in the transaction header. The batch flag is set to B on all transactions stored in the Hot Standby file prior to being forwarded to the application channel.

New transactions sent to an application in an Active Recovery mode are still sent to the Hot Standby file. From the device's point of view, the application is in Hot Standby mode. If the application is designed correctly for the data collection system, it should eventually be able to take delivery of all transactions in the Hot Standby file and resume interactivity with the device. At this point, the new transactions are no longer sent to the Hot Standby file. They are stored in AUX_Q until the application acknowledges or confirms responsibility for the transaction. After the acknowledgment or confirmation, the application is then active.

Note: *Data in an ACK transaction is ignored and not sent to the originator of the transaction if the transaction came from the Hot Standby file.*

2

Setting Up the DCS 300

This chapter explains how to set up the hardware for your DCS 300, configure the system parameters, and perform basic maintenance on your files.

Chapter Checklist

Done?	Task	Page
❑	Plug in the power cord.	2-4
❑	Plug in the keyboard.	2-5
❑	Plug in the mouse.	2-6
❑	Connect the monitor.	2-7
❑	Connect the uninterruptable power supply.	2-8
❑	Connect the modem.	2-10
❑	Set the system parameters.	2-12
❑	Understand the configuration files and how to restore your default configuration.	2-14
❑	Understand how to back up and restore the system and user files on your DCS 300.	2-15
❑	Understand how to start data collection, stop data collection, and shut down the DCS 300.	2-20

If you already understand and have performed these tasks, connect the server to your Intermec data collection network as described in these chapters:

- Chapter 3, “Connecting to the Intermec RF Network”
- Chapter 4, “Connecting to the 9180 and the Intermec CrossBar Network”

Plugging In the Power Cord

You need to attach the power cord before you can run the DCS 300. However, you may want to plug the power cord into a surge protector or an uninterruptable power supply (UPS). Intermec requires that you use a surge protector in locations that use 115 VAC.

Intermec recommends that you use a UPS in locations that have wide variations in AC power. For help, see "Connecting an Uninterruptable Power Supply" later in this chapter.

Warning
Before connecting the power cord, make sure that the server power switch is off. Failure to comply could result in injury due to electrical shock.

Avertissement
Avant de faire la connexion de la source de courant, assurez-vous que le commutateur soit "Off." Faute de quoi vous risquez une blessure comme un choc électrique.

Equipment

- Power cord, 110V U.S. cord (standard)

  Or,

  Power cord, 240V (Intermec Part No. 586266)
  Power cord, 250V (Intermec Part No. 586267)
- Surge protector

To connect the power cord

1. Locate the AC in port on the rear panel of the server.
2. Insert the power cord's 3-pin connector into the AC in port.
3. Intermec recommends that you use a surge protector. Plug the surge protector into the AC power outlet.
4. Plug the power cord into an AC power outlet or surge protector.

Plugging In the Keyboard

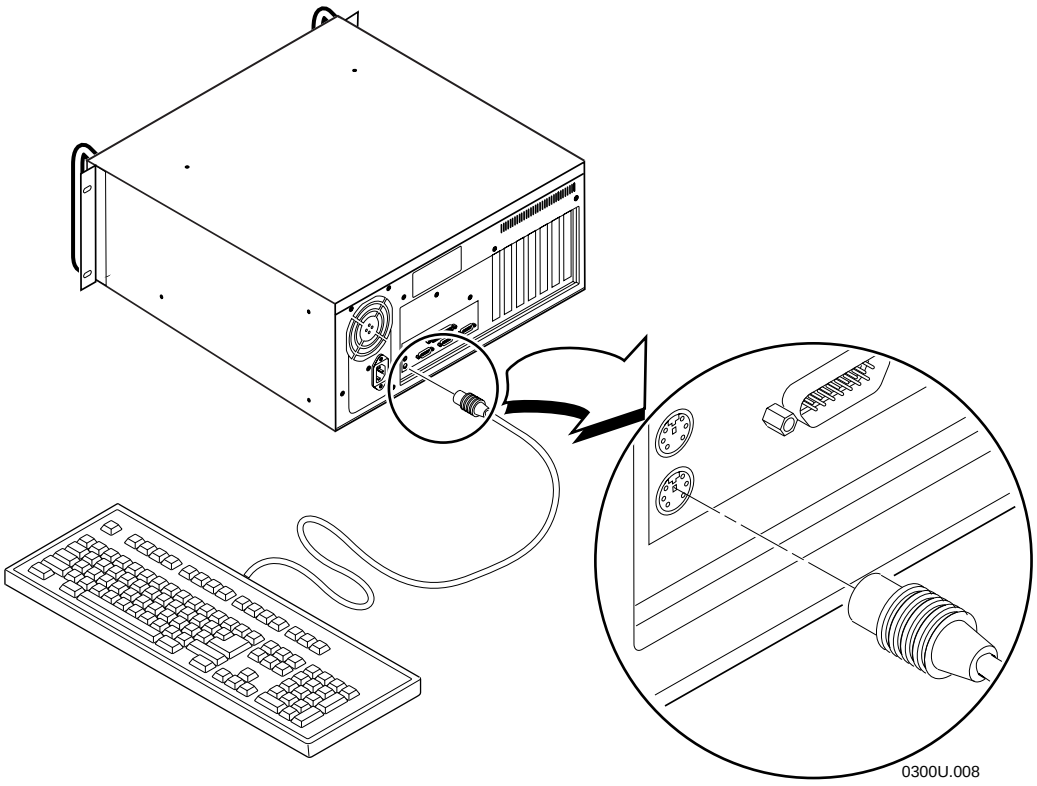
You need to use the keyboard to enter information when using the GUI to configure the DCS 300.

Equipment

- Keyboard (standard)

To plug in the keyboard

1. Locate the keyboard port on the rear panel of the server.
2. Insert the keyboard connector into the keyboard port.



Plugging In the Mouse

The mouse makes it easier for you to move around in the GUI when configuring the DCS 300.

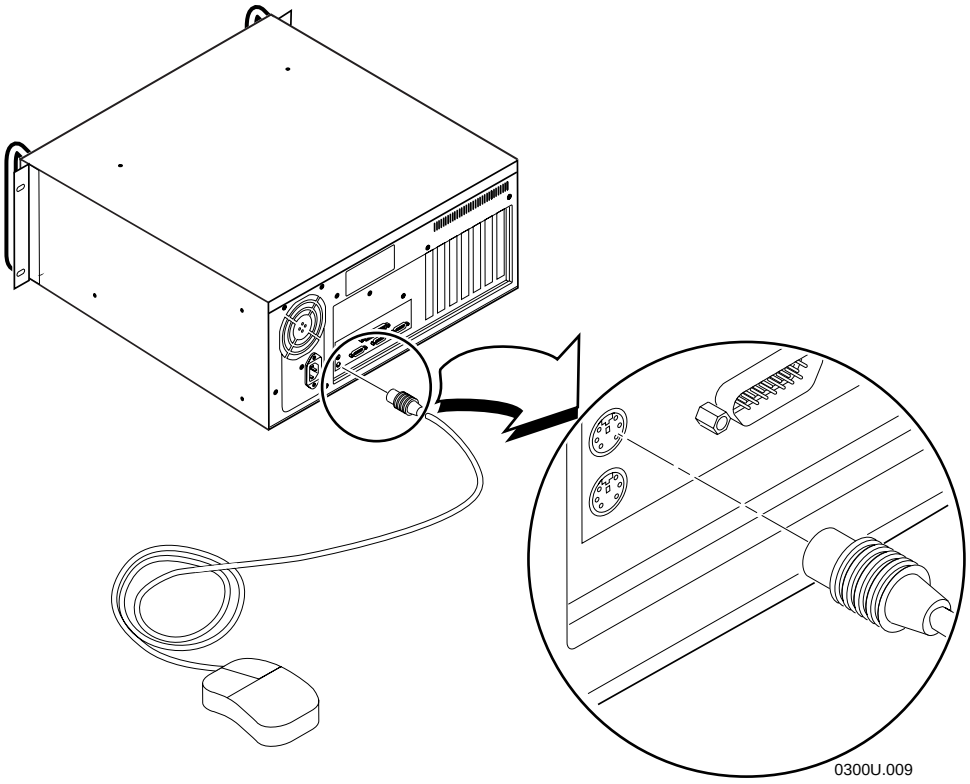
Note: *You must have the mouse plugged into the server whenever you boot the server.*

Equipment

- Mouse (standard)

To plug in the mouse

1. Locate the mouse port on the rear panel of the server.
2. Insert the mouse connector into the mouse port.



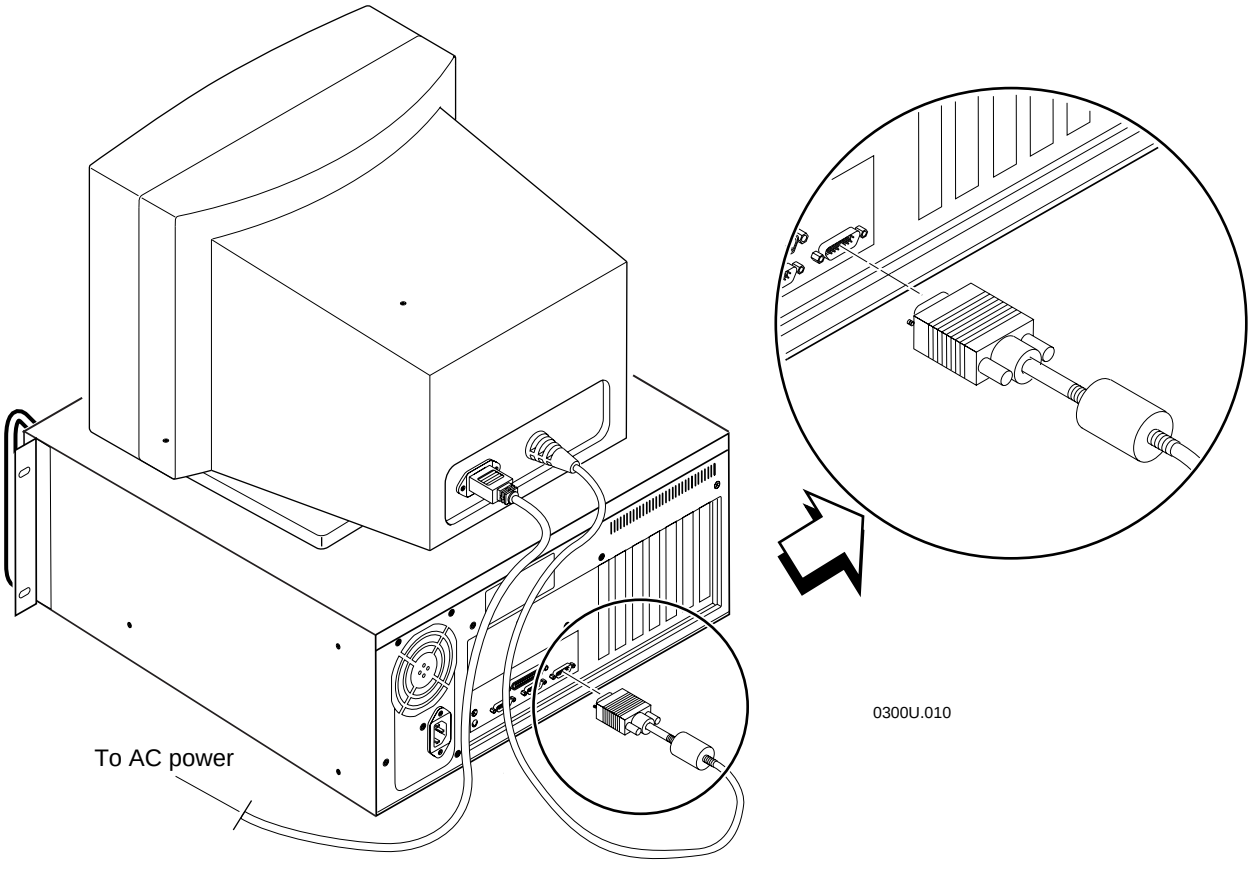
Connecting the Monitor

Equipment

- Monitor with cable and power cord (not provided)

To connect the monitor

1. Locate the video port on the rear panel of the server.
2. Insert one end of the monitor cable into the video port.
3. Insert one end of the power cord into the monitor and the other end into an AC power outlet.



Connecting an Uninterruptable Power Supply

Intermec strongly recommends that you connect an uninterruptable power supply (UPS) to your DCS 300. In case of a power failure, the UPS provides enough backup power to allow the server to properly shut down and minimize the loss of data.

If you experience a power failure after installing a UPS, these events will occur:

- If power returns within 45 seconds, no error message is logged and no message appears on the monitor.
- If power does not return within 45 seconds, an error message is logged and this message appears on the monitor.

  ```
  Power failure. UPS is running on battery power. Stopping data
  collection to preserve data integrity. DCS 300 shutdown will
  occur in approx 5 minutes.
  ```

  When data collection is stopped, the server tries to shut down. Five minutes after the error message is logged, the UPS cuts off power to the server.

You can configure the server to automatically restart data collection when power returns. For help, see "Setting the System Parameters" later in this chapter.

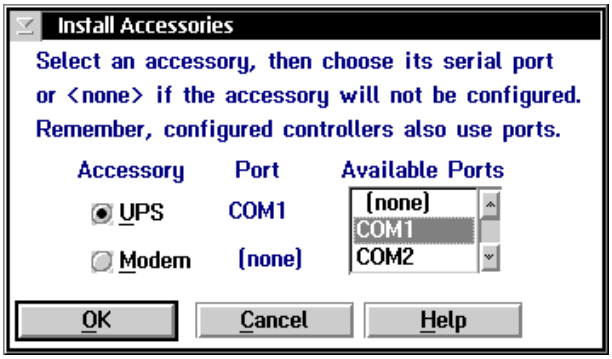
Equipment

- Uninterruptable power supply, U.S. and Canada (Intermec Part No. 589082). Uninterruptable power supply, International (Intermec Part No. 589079)
- Cable for auto-restoration (Intermec Part No. 589157)

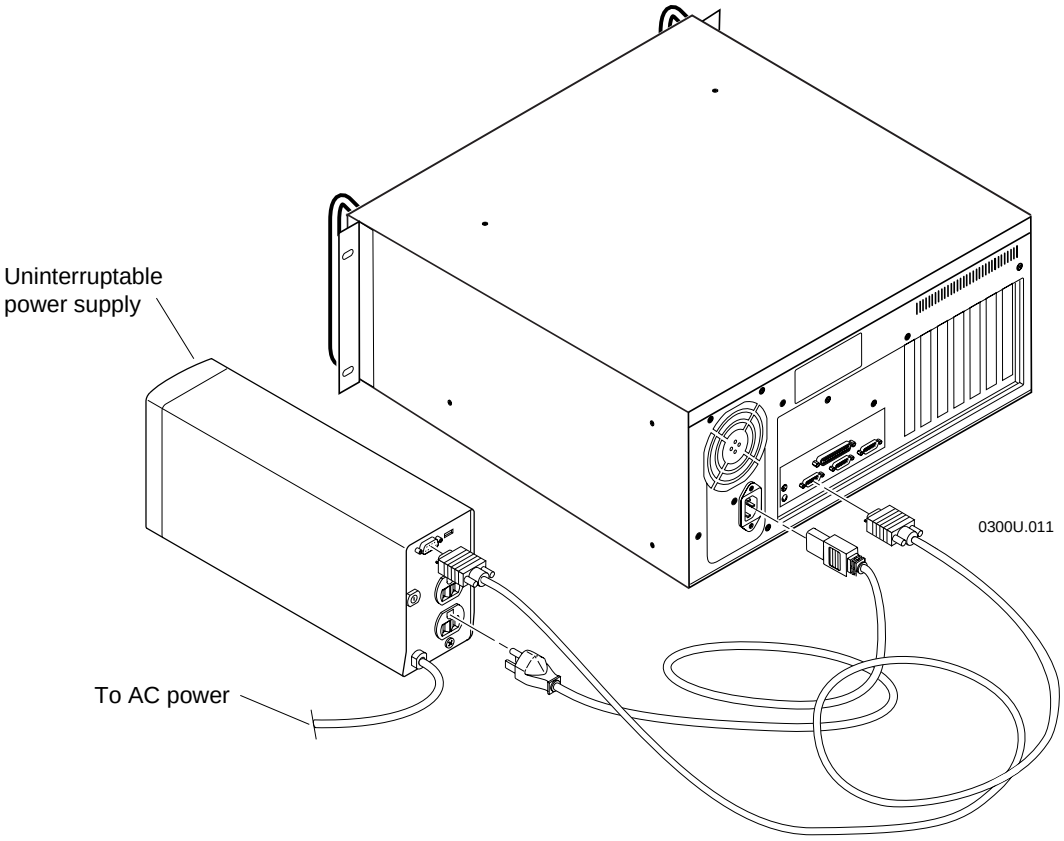
To connect a UPS

1. Make sure the power is off. The power LED should be off.
2. Insert the server power cord 3-pin connector into the AC in port.
3. Plug the other end of the power cord into the UPS.
4. (Optional) Intermec recommends that you use a surge protector. Plug the power cord of the UPS into the surge protector or an AC power outlet.
5. Insert one end of the serial cable into the serial port on the UPS.
6. Insert the other end of the serial cable into a COM port on the server.
7. Press the power button on the server. The power LED turns on. The main menu appears.
8. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.

9. In the System Maintenance list box, choose Install Accessories and then choose Start. The Install Accessories dialog box appears.



10. Choose UPS.
11. In the Available Ports list box, select the serial port on the server that you used to connect to the UPS.
12. Choose OK to save your changes. You return to the System Maintenance dialog box.
13. Choose Close to return to the main menu.



Connecting a Modem

You may want to connect your DCS 300 to a modem. If you have remote console support enabled on your server, you may want to use a modem to let you access the server GUI using a PC with a modem.

Note: *You can also use the remote console support feature through a LAN or a WAN connection.*

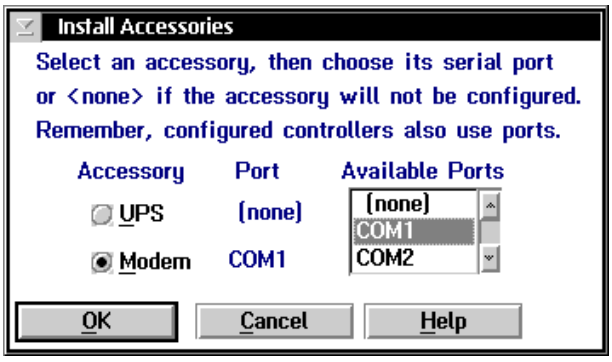
Equipment

- Modem with telephone cable and power cord, U.S. and Canada (Intermec Part No. 590887)
- Serial cable to connect the modem to the DCS 300 (Intermec Part No. 589182)

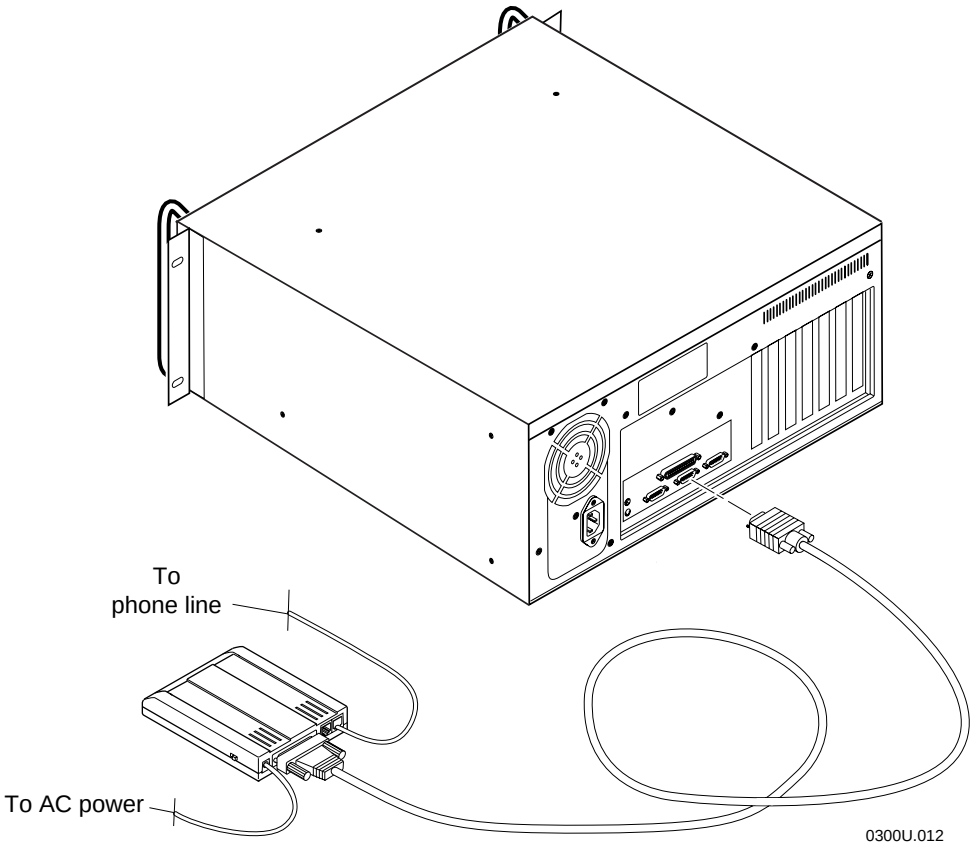
To attach a modem

1. Make sure the power is off. The power LED should be off.
2. Plug one end of the modem power cord into the modem and the other end into the AC power outlet.
3. Plug one end of the telephone cable into the modem and the other end into an RJ-11 telephone jack.
4. Insert one end of the serial cable into the serial port on the modem.
5. Insert the other end of the serial cable into a COM port on the server.
6. Press the power button on the server. The power LED turns on. The main menu appears.
7. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
8. In the System Maintenance list box, select Install Accessories and then choose Start. The Install Accessories dialog box appears.

Install Accessories Dialog Box



9. Choose Modem.
10. In the Available Ports list box, select the serial port on the server that you used to connect to the modem.
11. Choose OK to save your changes. You return to the System Maintenance dialog box.
12. Choose Close to return to the main menu.

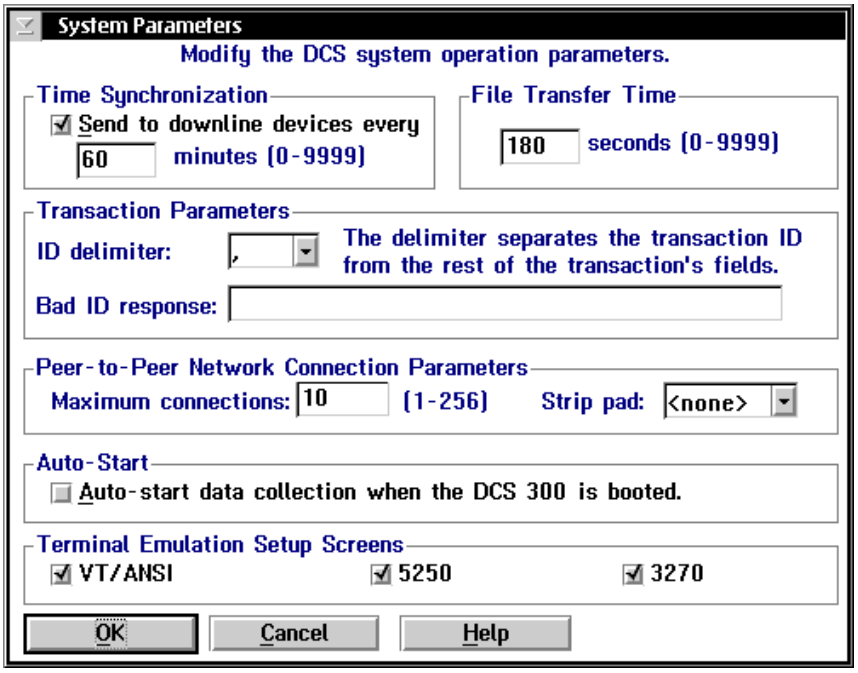


Setting the System Parameters

When you set system parameters, you are defining the operating parameters for the DCS 300.

To set the system parameters

- From the main menu sidebar buttons, choose System Parameters. The System Parameters dialog box appears.



Field	Description	Value	Default
Send to downline devices every...	This check box determines if the server sends its time to all Intermec controllers. ***Note:*** *The time broadcast is not necessarily sent to the devices that are connected to the Intermec controllers. However, when you configure a controller, you can configure it to broadcast the time to its devices.*	Check, Clear	Check
...minutes	This field specifies how often in minutes the server sends the time synchronization message.	0 to 9999	60
File Transfer Time	This box specifies how long in seconds the server waits for a response from the device when it is downloading files before it times out.	0 to 9999	180
ID delimiter	The character that the devices use to separate the transaction ID from the transaction fields.	Predefined	, (comma)
Bad ID response (Optional)	The message that the server sends to the source of the transaction if the server does not recognize the transaction ID. Use this field if you want to make sure that there is always a response for a failed delivery of a transaction.	1 to 40 alphanumeric and special characters	None
Maximum connections (Peer-to-peer)	A tuning value that defines the maximum number of connections for each NetComm process.	1 to 256	10
Strip pad (Peer-to-peer, APPC only)	The pad character, which is used by fixed-length transactions from a host application, that you want the server to remove before sending the transaction.	Predefined	None
Auto-Start	This check box determines if the server starts data collection when it is booted.	Check, Clear	Clear
Terminal Emulation Setup Screens (Optional)	This box lets you customize which terminal emulation buttons appear in the main menu.	VT/ANSI, 5250, 3270	All

About the Configuration Files

The DCS 300 uses three configuration files:

Default This configuration is the factory default configuration. If you want to restore the default configuration, for example you may want to move the server to a new system, select this option. For help, see "Restoring Default Configuration" in the next section.

Current When you choose Save Configuration, the server updates the current configuration file. The server does not change the active configuration file. Having separate files for the current and active configurations lets you make changes while the server is running without interrupting data collection.

Active When you choose Save and Activate, the server copies the current configuration file to the active configuration file. The active configuration file is the file that the server uses when you choose Start Data Collection.

Restoring Default Configuration

This procedure restores the factory default configuration of the server. It stops data collection, discards any unsaved and unactivated changes, and reboots the server. If you have used the Install Accessories dialog box to connect a modem or UPS or if you have upgraded your hardware, terminal license, screen mapping license, or remote console, then your new settings become the factory default configuration.

If you want to load your backed up system files or run-time configuration, see "Restoring Your System Files and Run-Time Configuration" or "Restoring Your User Files" later in this chapter.

To restore the default configuration

1. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
2. In the System Maintenance list box, select Reset to Factory Defaults and then choose Start. The Reset to Factory Defaults message box appears.
3. Choose Reset DCS 300 to reset the factory defaults and return to the main menu.
4. Choose Save and Activate to make the default configuration the active configuration.
5. Choose Shutdown DCS 300 to shut down the server.
6. Press **Ctrl-Alt-Del** to reboot the server.

Backing Up the DCS 300 Configuration

Once you have configured your Intermec hardware, have set up your host communications, and have set up your host environment parameters, you can start data collection on your DCS 300.

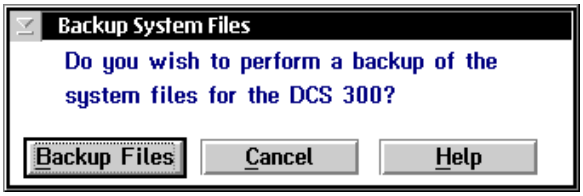
Intermec recommends that you back up your system files and your run-time configuration before you start data collection.

Backing Up Your System Files and Run-Time Configuration

When you open the DCS 300 package, unpack the blank, formatted, 3.5-inch disk. Use this disk to back up your system files and run-time configuration. If your server loses its configuration, you can use these files to restore the server.

To back up the configuration

1. Insert the 3.5-inch disk into the server disk drive.
2. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
3. In the System Maintenance list box, select Backup System Files and then choose Start. The Backup System Files message box appears.



4. Choose Backup Files. The server backs up the system files and run-time configuration.
5. Remove your disk from the disk drive, label it, and put it in a safe place.

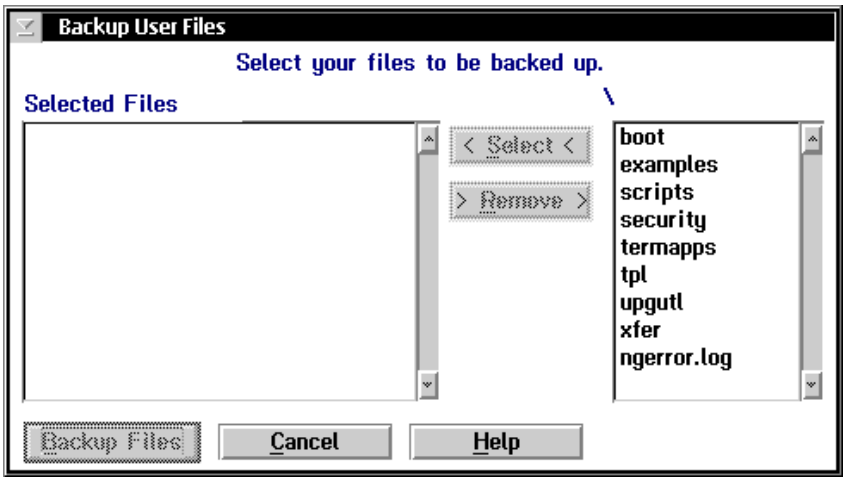
Backing Up Your User Files

You must back up any user files so that you can restore them if your DCS 300 loses its configuration. For example, if you are using screen mapping, you may want to back up your script (.SCR) files. You may also want to back up the NGERROR.LOG file, which contains error messages.

Note: *When backing up your user files, you must use a separate 3.5-inch disk from the one you used to back up your run-time configuration.*

To back up your user files

1. Insert a 3.5-inch disk into the server disk drive.
2. From the main menu sidebar buttons, choose File Handling. The File Handling dialog box appears.
3. In the File Handling list box, select Backup User Files and then choose Start. The Backup User Files dialog box appears.



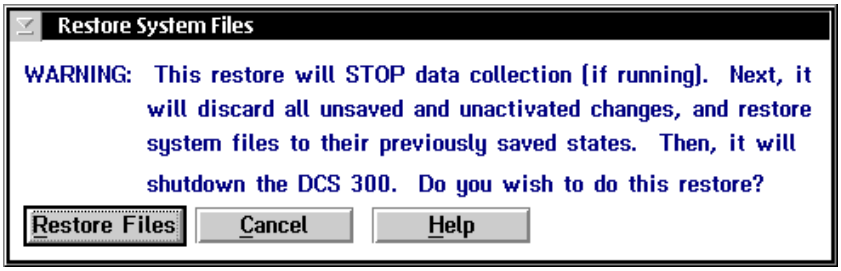
4. In the root directory list box (\), add all the files that you want to back up to the Selected Files list box.
   a. Select the file name. Script files are in the subdirectory SCRIPTS. Template files are in the subdirectory TPL.
   b. Choose Select. The file name appears in the Selected Files list box.
5. In the Selected Files list box, remove any files that you do not want to back up.
   a. Select the file name.
   b. Choose Remove. The file name is removed from the Selected Files list box.
6. Choose Backup Files. The server backs up the user files you selected.
7. Remove your disk from the disk drive, label it, and put it in a safe place.

Restoring the DCS 300 Configuration

If your DCS 300 loses its configuration, you can recover the system files and run-time configuration.

Restoring Your System Files and Run-Time Configuration

1. Insert the 3.5-inch disk that contains the system files and run-time configuration backup into the server disk drive.
2. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
3. In the System Maintenance list box, select Restore System Files and then choose Start. The Restore System Files message box appears.



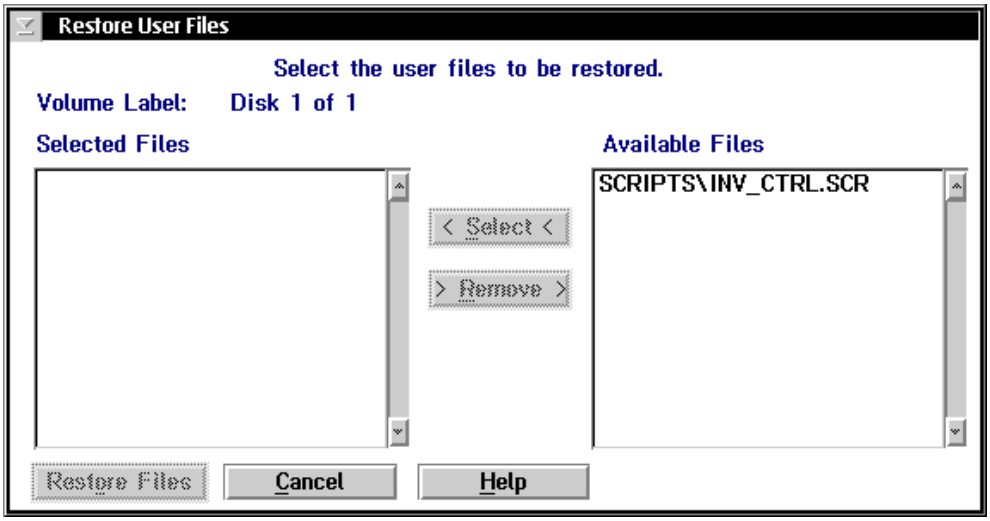
4. Choose Restore Files. The server restores the system files and run-time configuration and then shuts down.
5. Remove your disk from the disk drive and put it in a safe place.
6. Press **Ctrl-Alt-Del** to reboot the server.

Restoring Your User Files

You can also use this feature to transfer files, such as validation files or applications, from a floppy disk to the server.

To restore your user files

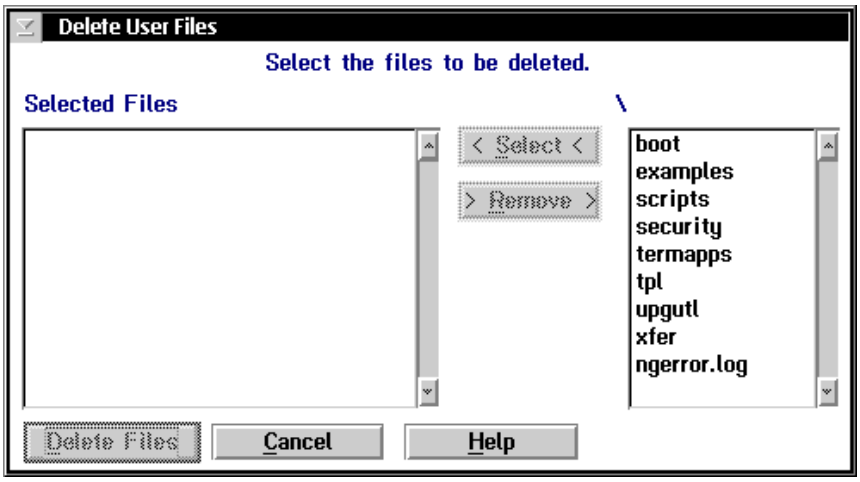
1. Insert the 3.5-inch disk that contains the backup of your user files into the server disk drive.
2. From the main menu sidebar buttons, choose File Handling. The File Handling dialog box appears.
3. In the File Handling list box, select Restore User Files and then choose Start. A message box appears with instructions to insert the disk in the drive of the server.
4. Choose OK. The Restore User Files dialog box appears. The files on the floppy disk appear in the Available Files list box.



5. In the Available Files list box, add all the files that you want to restore to the Selected Files list box.
   a. Select the file name.
   b. Choose Select. The file name appears in the Selected Files list box.
6. In the Selected Files list box, remove any of the files that you do not want to restore.
   a. Select the file name.
   b. Choose Remove. The file name is removed from the Selected Files list box.
7. Choose Restore Files. The server restores the files you selected.
8. Remove your disk from the disk drive and put it in a safe place.

Deleting User Files

1. From the main menu sidebar buttons, choose File Handling. The File Handling dialog box appears.
2. In the File Handling list box, select Delete User Files and then choose Start. The Delete User Files dialog box appears.



3. In the root directory list box (\), add all the files that you want to delete to the Selected Files list box.
   a. Select the file name.
   b. Choose Select. The file name appears in the Selected Files list box.
4. In the Selected Files list box, remove any the files that you do not want to delete.
   a. Select the file name.
   b. Choose Remove. The file name is removed from the Selected Files list box.
5. Choose Delete Files. A message box appears confirming that you want to delete the files.
6. Choose Delete. The server deletes the user files you selected.

Using the DCS 300

To use the DCS 300, you need to know how to start and stop data collection and shut down the server.

Caution
Always choose Shutdown DCS 300 before rebooting or turning off the server. If you do not shut down the server properly, you may lose data or damage files on the server.

Conseil
Choisissez toujours le bouton Shutdown DCS 300 dans l'encadré avant de réamorcer ou de fermer l'unité de contrôle. Si vous ne fermez pas correctement l'unité de contrôle, vous risquez de perdre des données ou d'endommager les fichiers sur l'unité de contrôle.

Starting Data Collection

1. From the main menu sidebar buttons, choose Save and Activate. A message box appears confirming that you want to save your changes and activate the configuration.
2. Choose Activate. A message box may appear informing you that the server needs to reboot and that you need to choose OK. Or, a message box may appear informing you that your activate is successful.
3. From the main menu sidebar buttons, choose Start Data Collection. The Start Data Collection message box appears.
4. Choose Start to start data collection. The title bar shows "Data Collection: Started."

Stopping Data Collection

You may need to stop data collection on the DCS 300 to update its configuration file. When you stop data collection, all data collection activities are stopped, but any external Intermec controllers continue polling and buffering data. Devices using programs that require a response directly from a destination (interactive mode) also stop until the server is started again.

To stop data collection

1. From the main menu sidebar buttons, choose Stop Data Collection. The Stop Data Collection message box appears.
2. Choose Stop to stop data collection. The title bar shows "Data Collection: Stopped."

Shutting Down the DCS 300

You may need to power off the DCS 300 for maintenance or relocation. The server needs to perform a series of shutdown activities, which may take up to five minutes to ensure that no system files or data are lost.

To turn off the DCS 300

1. From the main menu sidebar buttons, choose Shutdown DCS 300. The Shutdown DCS 300 message box appears.
2. Check or clear the Save and activate changes check box depending on if you want to save and activate any changes you have made to the configuration.

   Note: *If you have saved your changes without activating them (only [Activate] appears in the title bar) this check box will be grayed. The server will automatically activate your changes before it shuts down.*

3. Choose Shutdown to shut down the server. The server needs to perform a series of shutdown activities, which may take up to five minutes.

A message box appears letting you know when you can safely turn off the server.

Accessing a Command Prompt

While maintaining or configuring the DCS 300, you may find your task is easier by accessing a command prompt.

To access a command prompt

1. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
2. In the System Maintenance list box, select DCS 300 Command Prompt and then choose Start. The Command Prompt Password dialog box appears.

3. In the Password field, type:

   `INTERMEC`

4. Choose OK. The DCS 300 Command Prompt window appears.

To close the Command Prompt window

1. Choose the box in the upper left corner of the window. A drop-down menu appears.
2. Choose Close to return to the main menu.

3

Connecting to an Ethernet/Token Ring Network

This chapter describes how to install the DCS 300 in your Ethernet or token ring network and how to configure the network adapter card.

Chapter Checklist

Done?	Task	Page
❑	Install the server in the Ethernet network.	3-4
❑	Install the server in the token ring network.	3-5
❑	Use the GUI to configure each Ethernet and token ring card for TCP/IP.	3-6
	Or,	
❑	Use the GUI to configure each Ethernet and token ring card for IEEE 802.2.	3-12
❑	Save your run-time configuration.	3-13

If you already understand and have performed these tasks, either connect the DCS 300 to another host or set up the host environment as described in these chapters:

- Chapter 4, “Connecting to a Coaxial/Twinaxial Network”
- Chapter 5, “Connecting to an SDLC Network”
- Chapter 6, “Connecting to the Intermec RF Network”
- Chapter 7, “Connecting to the 9180 and the Intermec CrossBar Network”

Installing the DCS 300 in an Ethernet Network

There are two types of Ethernet network adapter cards you can have in your DCS 300: a 10 Mbps card or a 10/100 Mbps card. The parameters you set are the same for both cards. For information about upgrading to a 10/100 Mbps card (Intermec Part No. 066413), contact your local Intermec representative.

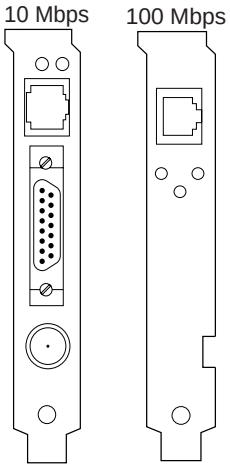
Before you can configure the DCS 300, you need to install it in your network.

Equipment

- An Ethernet connection where you can connect the server.
- A cable to connect the server to the connection. You can use any of these types of cables: UTP for 10BaseT, RG-58 coax for 10Base2, 50-ohm coax for 10Base5.

Note: *The default configuration for the Ethernet card is 10BaseT or 100BaseTX. Contact your local Intermec representative if you need to use 10Base2 or 10Base5.*

To install the server



0300U.019 0300U.020

1. Locate the slot that contains the Ethernet card(s) on the rear panel of your server. Refer to the figures on the left.
2. Insert one end of the cable into the appropriate Ethernet port on the card and the other end into the Ethernet connection.

Note: *If you are using 10Base2, make sure that you connect the cable to both the port and the Ethernet connection before turning on the server.*

Installing the DCS 300 in a Token Ring Network

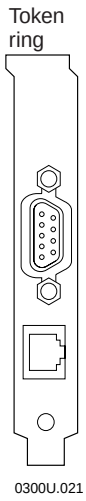
Before you can configure the DCS 300, you need to install it in your network.

Equipment

- A token ring connection where you can connect the server.
- A cable to connect the server to the connection. Your token ring card comes with an RJ-45 to STP cable.

Note: *The default ring speed for the token ring card is 16 Mbps. Contact your local Intermec representative if you need to set the ring speed to 4 Mbps.*

To install the server



0300U.021

1. Locate the slot that contains the token ring card on the rear panel of your server. The connector on the card looks like the figure on the left.
2. Insert one end of the cable in the token ring port on the card and the other end in the token ring connection.

Configuring the Network Adapter Card for TCP/IP

After you install the DCS 300, you need to turn it on and configure its network adapter cards. Ethernet and token ring support both TCP/IP and IEEE 802.2 protocols.

To configure the card for TCP/IP, either use a Dynamic Host Configuration Protocol (DHCP) server to provide the server TCP/IP information or enter the TCP/IP configuration manually. If you do not enter an IP address or subnet mask and you do not check the Use DHCP check box, TCP/IP communications are disabled.

Use a DHCP server to provide the server's IP information You can configure the DCS 300 to be a DHCP client in a network that uses a DHCP server. The DHCP server can provide the DCS 300 with an IP address assignment and other basic IP configuration characteristics, such as the subnet mask, the router IP address, and the DNS server address.

Note: *The DCS 300 supports only one network adapter card that is using DHCP.*

If you have a backup DCS 300 that is also configured as a DHCP client, you do not need to enter its IP address in each of your UDP Plus devices when it comes online. If you leave the backup DCS 300 online, you can perform pseudo load-balancing on your UDP Plus network. You need to use these bar codes to enable DHCP on each UDP Plus device

Enable DHCP

$+NI0

Disable DHCP

$+NI1

Note: *To use DHCP across routers in your network, the routers must have the DHCP relay agent configured and enabled. For help, see your router user's manual.*

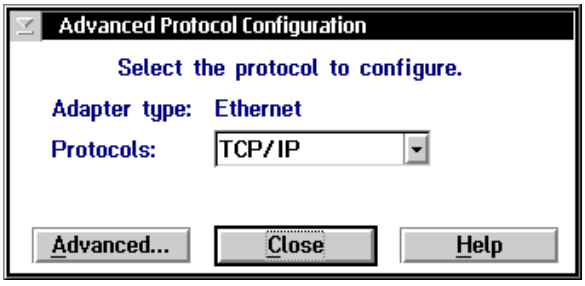
Enter the server's IP information manually From your network administrator, obtain a valid IP v4 address for each Ethernet or token ring card. You may also need to know the server's local host name and the subnet mask. If you have two or more cards communicating using TCP/IP, each card must be on a different subnet.

If you need to set up routing tables for the TCP/IP configuration, you also need the IP addresses of the route destinations and of the routers.

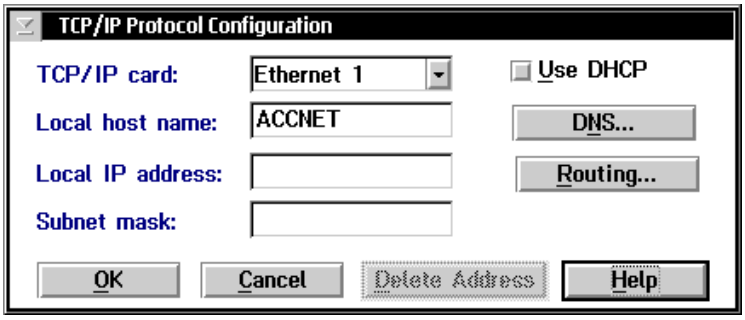
To configure the network adapter card

1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Local Network Adapter. Five buttons for different network adapter card types appear.
3. Choose the type of network adapter card (Ethernet or token ring) that you are configuring. The Advanced Protocol Configuration dialog box appears.

Advanced Protocol Configuration Dialog Box



4. In the Protocols field, click the down arrow on the right side of the field. Select TCP/IP.
5. Choose Advanced. The TCP/IP Protocol Configuration dialog box appears.



Field	Description	Value	Default
TCP/IP card	The card that you are configuring. ***Note:*** *If you have more than one Ethernet card, Ethernet 1 is further left than Ethernet 2 as you face the front panel.*	Ethernet 1 Ethernet 2 Token Ring 1	Ethernet 1
Use DHCP	This check box enables this network adapter card to be administered by a DHCP server.	Check, Clear	Clear
Local host name (Optional)	A meaningful name that identifies the server (host) to the network.	1 to 12 alphanumeric characters	ACCNET
Local IP address	A unique IP address that identifies the card in the server (host) to the network. This IP address must be a valid IP v4 address.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	None
Subnet mask	The mask that is used in the IP protocol layer to separate the subnet address from the local IP address.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	Calculated based on IP address

Using DNS

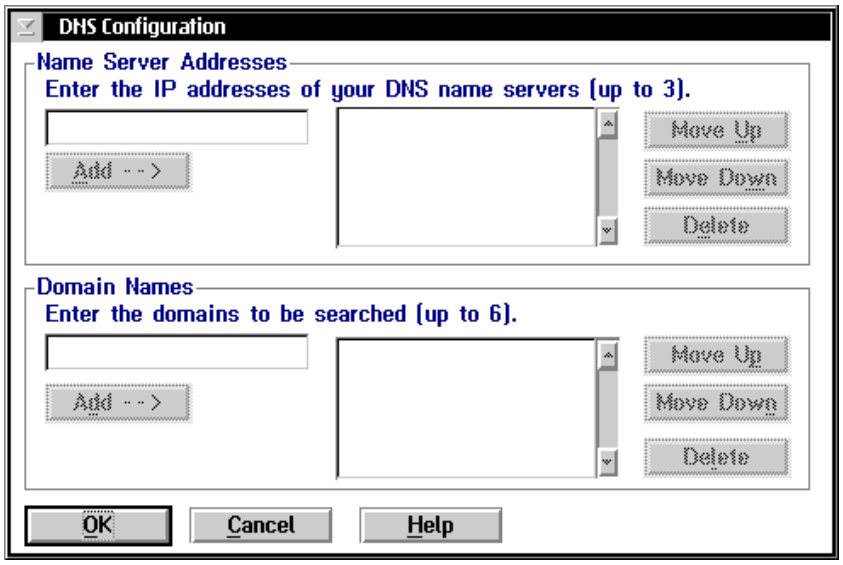
The DCS 300 supports the use of Domain Name System (DNS) servers in your network. DNS lets you configure single or multiple name servers, which will resolve name/IP address conversions of hosts and devices. The DCS 300 automatically obtains the IP addresses from the DNS server, along with any changes. For example, if you use a DNS server, you do not need to configure the DCS 300 with the IP addresses for the TCP/IP hosts. You only need to enter the host names. However, if you manually enter an IP address, this address takes precedence over an address supplied by the DNS server.

In a DHCP environment, the IP address changes frequently. The host may obtain a new IP address every time it is restarted and reconnects to the network. DNS servers let the DCS 300 locate and connect to TCP/IP hosts that are administered by a DHCP server. The DCS 300 locates the host by using the name to look up the host's current IP address, as registered in the DNS server.

Note: *Any changes to the DNS Configuration dialog box become active when you choose OK.*

To use DNS

- From the TCP/IP Protocol Configuration dialog box, choose DNS. The DNS Configuration dialog box appears.



Field	Description	Value	Default
Name Server Addresses	List of IP addresses of DNS servers that are used to resolve IP addresses. You can enter up to three IP addresses. The first IP address in the list is the first DNS server you want to use to resolve the IP address. If the first DNS server does not respond, then the DCS 300 uses the next IP address. However, if the DNS server responds, even if the response is a "not resolved" response, the search stops.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	None
Domain Names	List of domains that are searched when an abbreviated IP name is entered. You can enter up to six domain names. If the host or device name is not found in the domain, the DCS 300 searches the next one. The DCS 300 appends the complete domain name before attempting to use the DNS server to resolve the IP address. ***Note:*** *If the host or device name has any dotted notation, such as intermec.com, this list is not used.*	256 alphanumeric characters, dash	None

Clearing the IP Address and Subnet Mask

When you configure a card for TCP/IP and you do not use DHCP, you must enter the IP address and subnet mask. The Delete Address button lets you clear the Local IP address and Subnet mask fields.

When you choose the Delete Address button, a message box appears warning you that if you delete the IP address, routes and hosts that rely on this address may become invalid. If you have a UDP Plus network defined and you have only one card defined for TCP/IP, you must delete the UDP Plus network before you can clear the IP address and subnet mask.

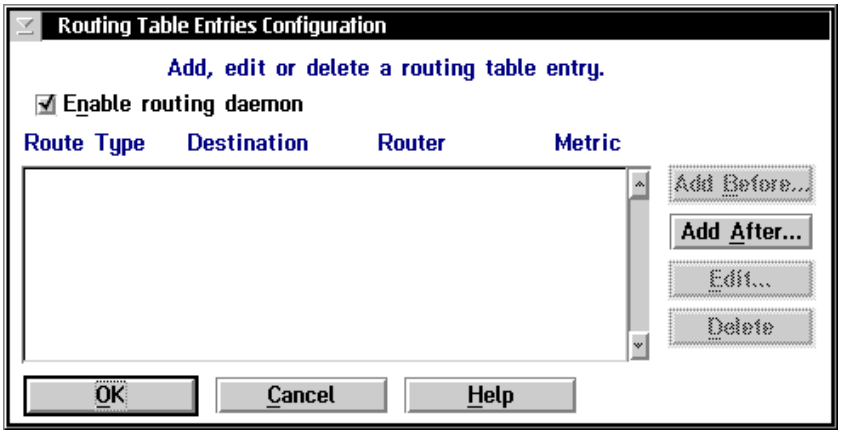
Using the Routing Daemon

The routing daemon tells the server how to route IP packets in an IP network. Generally, the routing daemon is sufficient for standard network configuration, but you may also configure explicit routes. Obtain these routes from your network administrator.

If you cannot connect with a TCP/IP host in your network, you may have a routing problem. Configuring an explicit route may resolve this problem.

To enable or disable the routing daemon

1. From the TCP/IP Protocol Configuration dialog box, choose Routing. The Routing Table Entries Configuration dialog box appears.



2. To enable the routing daemon, check the check box for Enable routing daemon.

   Or, to disable the routing daemon, clear the check box for Enable routing daemon and configure explicit routes. For help, see "Configuring Routing Tables" later in this chapter.

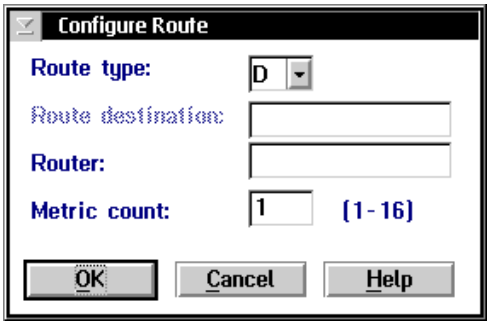
3. Choose OK to save your changes and return to the TCP/IP Protocol Configuration dialog box.

Configuring Routing Tables

There are four types of routes that you can configure: default, network, subnet, and host. The default route specifies a route that can be used as a destination for an IP packet if a route for the IP packet is not specified. Network routes define a network to add to the system. Subnet routes define a subnet to add to the system. Host routes define a specific host destination to add to the system.

To configure a route

- From the Routing Table Entries Configuration dialog box, choose Add Before or Add After. The Configure Route dialog box appears.



Field	Description	Value	Default
Route type	The type of route you are configuring for a destination.	D=default N=network S=subnet H=host	D
Route destination (N, S, H route types only)	The IP address of the destination of the route you are configuring.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	None
Router	The IP address of the router for the destination you are configuring.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	None
Metric count	The number of hops it takes to get to the destination.	1 to 16	1

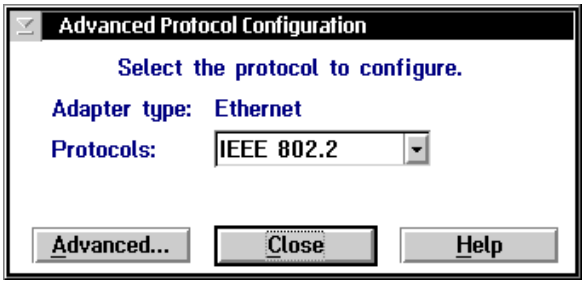
Configuring the Network Adapter Card for IEEE 802.2

After you install the DCS 300, you need to turn it on and configure its network adapter cards. Ethernet and token ring support both TCP/IP and IEEE 802.2 protocols.

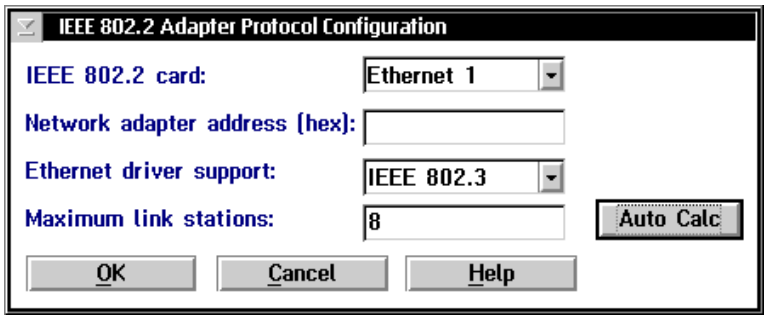
To configure the card for IEEE 802.2, you need to know the network adapter address, Ethernet driver support, and the maximum number of link stations. This protocol is used for IBM connectivity. It coexists with TCP/IP in the network adapter card.

To configure the network adapter card

1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Local Network Adapter. Five buttons for different network adapter card types appear.
3. Choose the type of network adapter card (Ethernet or token ring) that you are configuring. The Advanced Protocol Configuration dialog box appears.



4. In the Protocols field, click the down arrow on the right side of the field. Select IEEE 802.2.
5. Choose Advanced. The IEEE 802.2 Adapter Protocol Configuration dialog box appears.



Field	Description	Value	Default
IEEE 802.2 card	The Ethernet card that you are configuring.	Ethernet 1 Ethernet 2 Token Ring 1	Ethernet 1 Token Ring 1
Network adapter address (Optional)	The locally administered MAC address in IEEE format (hex) that identifies the card.	020000000000 through FEFFFFFFFFFF	The MAC address that is on the card.
Ethernet driver support	The Ethernet frame type you are using.	IEEE 802.3 or Ethernet DIX (Ethernet II)	IEEE 802.3
Maximum link stations	The maximum number of link stations that can exist for all SAPs concurrently. Or, choose the Auto Calc button if you want the server to determine the optimal values for this field based on how it is configured.	Based on how the server is configured.	8

Saving Your Run-Time Configuration

When you finish configuring your network adapter card, you should save your changes.

To save your run-time configuration

- From the main menu sidebar buttons, choose Save Configuration.

4

Connecting to a Coaxial/Twinaxial Network

This chapter describes how to connect the DCS 300 to your host using a coaxial or twinaxial connection and it also explains how to configure the network adapter card.

Chapter Checklist

Done?	Task	Page
❑	Install the server.	4-4
❑	Use the GUI to configure the coaxial card for the coaxial network.	4-4
	Or,	
	Use the GUI to configure the twinaxial card for the twinaxial network.	4-5

If you already understand and have performed these tasks, connect the DCS 300 to another host or set up the host environment as described in these chapters:

- Chapter 3, “Connecting to an Ethernet/Token Ring Network”
- Chapter 5, “Connecting to an SDLC Network”
- Chapter 6, “Connecting to the Intermec RF Network”
- Chapter 7, “Connecting to the 9180 and the Intermec CrossBar Network”

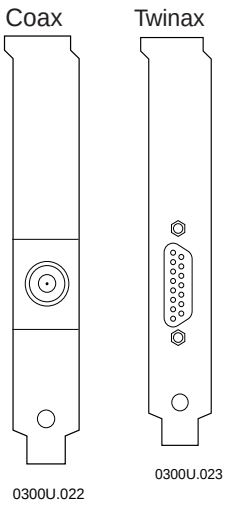
Installing the DCS 300

Before you can configure the DCS 300, you need to install it in your network.

Equipment

- A coaxial or twinaxial connection where you can connect the server.
- A cable to connect the server to the connection. You can use a RG-58 coaxial cable, or for a twinaxial connection you can use 15 conductor IBM custom cable.

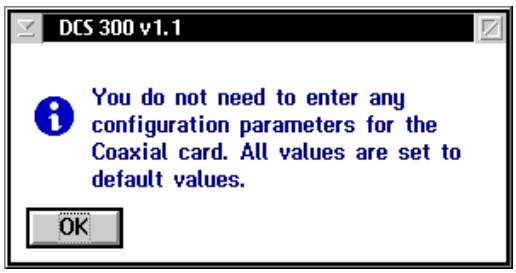
To install the server



1. Locate the slot that contains the coaxial or twinaxial card on the rear panel of your server. The twinaxial or coaxial card is the card that is furthest right when you are facing the front panel. Refer to the figure on the left.
2. Insert one end of the cable in the port and the other end in the coaxial or twinaxial connection.

Configuring the Coaxial Adapter Card

If you have a coaxial network adapter card in the DCS 300, you do not need to enter any configuration parameters. You can choose the type of communication you are using, Local Network Adapter, and then Coaxial. This message box appears:



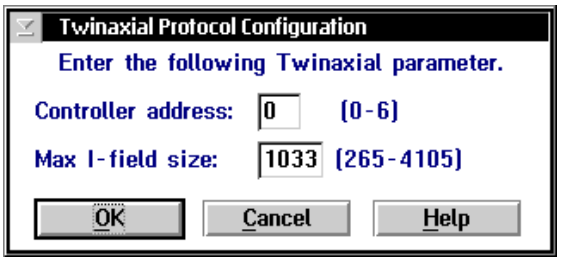
Configuring the Twinaxial Adapter Card

After you install the DCS 300, you need to turn it on and configure its network adapter cards.

Before you configure the network adapter card, obtain the server address and the maximum I-field size from your network administrator.

To configure the network adapter card

1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Local Network Adapter. Five buttons for different network adapter card types appear.
3. Choose Twinaxial. The Twinaxial Protocol Configuration dialog box appears.



Field	Description	Value	Default
Controller address	The address of the host twinaxial connection. This value must be unique for each twinaxial device connected to the host on this line.	0 to 6	0
Max I-field size	The maximum frame size that is used in this connection mode.	265 to 4105	1033

Saving Your Run-Time Configuration

When you finish configuring your network adapter card, you should save your changes.

To save your run-time configuration

- From the main menu sidebar buttons, choose Save Configuration.

5

Connecting to an SDLC Network

This chapter describes how to install the DCS 300 in your SDLC network and configure the network adapter card.

Chapter Checklist

Done?	Task	Page
❑	Install the server.	5-4
❑	Use the GUI to configure the SDLC card for the SDLC network.	5-5

If you already understand and have performed these tasks, connect the DCS 300 to another host or set up the host environment as described in these chapters:

- Chapter 3, “Connecting to an Ethernet/Token Ring Network”
- Chapter 4, “Connecting to a Coaxial/Twinaxial Network”
- Chapter 6, “Connecting to the Intermec RF Network”
- Chapter 7, “Connecting to the 9180 and the Intermec CrossBar Network”

Installing the DCS 300

Before you can configure the DCS 300, you need to install it in your network.

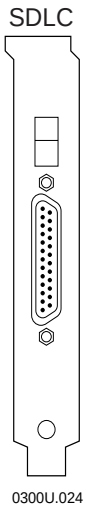
Equipment

- An SDLC connection where you connect the server.
- An SDLC cable to connect the server to the connection. You can use a 25 conductor IBM custom cable.

Note: *The SDLC card uses COM1. If you need more than one available serial port, you can purchase an Intermec serial I/O board.*

Note: *The default configuration for the SDLC card is V.35. Contact your local Intermec representative if you need to use RS-232 communications.*

To install the server



0300U.024

1. Locate the slot that contains the SDLC card on the rear panel of your server. The SDLC card is the card that is furthest right when you are facing the front panel. The connector on the card looks like the figure on the left.
2. Insert one end of the cable in the port on the card and the other end in the connection.

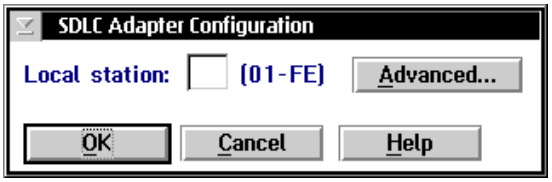
Configuring the Network Adapter Card

After you install the DCS 300, you need to turn it on and configure its network adapter cards. The SDLC card can use an internal or external clock at speeds up to 1 Mbps.

Before you configure the network adapter card, obtain the local station address from your network administrator. You may also need to know the line type, line mode, NRZI, link station role, and maximum I-field size.

To configure an SDLC network adapter card

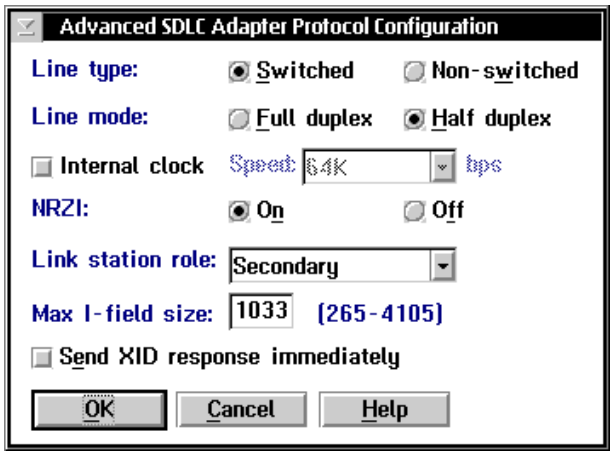
1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Local Network Adapter. Five buttons for different network adapter card types appear.
3. Choose SDLC. The SDLC Adapter Configuration dialog box appears.



4. In the Local station field, enter the address (in hex) that identifies the server station. The address can be from 01 to FE. The default is 01.
5. Configure any advanced SDLC parameters. For helps, see “Configuring Advanced SDLC Parameters” in the next section.
6. Choose OK to return to the SDLC Adapter Configuration dialog box.
7. Choose OK to return to the main menu.

Configuring Advanced SDLC Parameters

- From the SDLC Adapter Configuration dialog box, choose Advanced. The Advanced SDLC Adapter Protocol Configuration dialog box appears.



Field	Description	Value	Default
Line type	The type of telecommunications link that the server is using. Switched lines are the dialed type. Non-switched lines are the leased type.	Switched, Non-switched	Switched
Line mode	The type of cable you are using to connect the server to your host.	Full duplex, Half duplex	Half duplex
Internal clock	This check box determines if you are using an internal or external clock.	Check, Clear	Clear
Speed	The speed (in bps) of the internal clock.	4800, 9600, 19.2K, 38.4K, 56K, 64K, 128K, 192K, 256K, 384K, 560K, 840K, 960K, 1M	64K
NRZI (Non-Return-to-Zero Inverted)	The data encoding for modems that are sensitive to certain bit patterns.	On, Off	On

Field	Description	Value	Default
Link station role	This field sets the role of the server to be the primary workstation or the secondary workstation to the host. If you are configuring 3270 terminal emulation or you are communicating with a mainframe, this field is typically Secondary. Choose Negotiable if you want the server and host to negotiate their roles when they connect.	Primary, Negotiable, Secondary	Secondary
Max I-field size	The maximum frame size that is used in this connection mode.	265 to 4105	1033
Send XID response immediately	This check box determines if the server sends the XID response without waiting for the host to send the XID request. This XID is also the Node ID.	Check, Clear	Clear

Saving Your Run-Time Configuration

When you finish configuring your network adapter card, you should save your changes.

To save your run-time configuration

- From the main menu sidebar buttons, choose Save Configuration.

6

Connecting to the Intermec RF Network

This chapter explains how to connect the DCS 300 to the 900 MHz RF network using RF cards and BRUs. It also explains how to connect the server to the 2.4 GHz RF network using access points, JANUS devices, and TRAKKER Antares terminals. It also explains how to connect the server to the WTP network using access points and WTP devices.

Chapter Checklist

Done?	Task	Page
❑	Connect the server to your Intermec 900 MHz RF network.	6-4
❑	Connect the server to your Ethernet or token ring network.	3-4
❑	Configure the RF cards in the server to communicate with the BRUs.	6-6
❑	Set the time parameters for the 900 MHz RF network.	6-10
❑	Configure your 2.4 GHz RF network (UDP Plus network).	6-19
❑	Set the time parameters for the UDP Plus network.	6-23
❑	Configure your WTP network.	6-34
❑	Edit the JANUS 900 MHz RF device parameters.	6-16
❑	Edit the UDP Plus device parameters.	6-30
❑	Edit the WTP device parameters.	6-42

If you already understand and have performed these tasks, connect the DCS 300 to your CrossBar network or host environment as described in these chapters:

- Chapter 7, “Connecting to the 9180 and the Intermec CrossBar Network”
- Chapter 8, “Using Terminal Emulation”
- Chapter 9, “Using Peer-to-Peer Applications”
- Chapter 10, “Using Terminal Sessions”

Connecting the DCS 300 to the 900 MHz RF Network

The DCS 300 can communicate with Intermec's 900 MHz RF network. To communicate with this network, the server contains RF cards (up to two) that connect by an RS-485 cable to 9181 Base Radio Units (BRUs). The BRUs transmit information from the server to Intermec RF devices and receive signals from them. The illustration on the next page shows an example of a DCS 300 connected to the Intermec 900 MHz RF network.

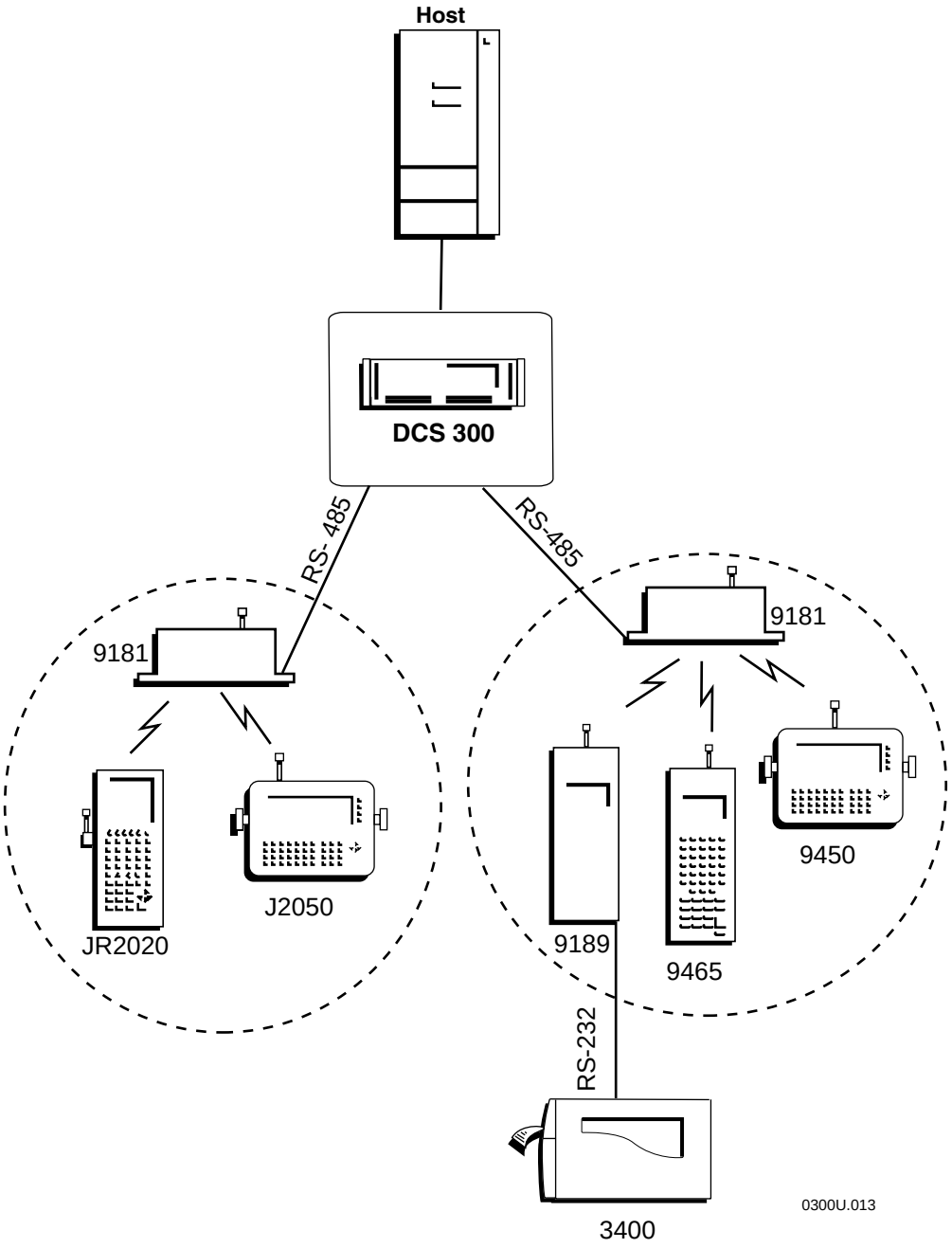
Each RF card supports either 2-port or 4-port options so you can connect up to seven BRUs in one data collection network.

Note: *If you are using the 9180 Network Controller to communicate with the 9181 BRU, you need to configure these BRUs using the 9180 controller's configuration menu. Refer to your 9180 user's manual.*

To connect the server and the BRU, you need to know if you have 2-port or 4-port RF cards in the server. Cables must be ordered separately.

- If you have a 2-port card, you need an Intermec cable kit (Intermec Part No. 055003) or equivalent. You also need a Belden 89688 cable (Intermec Part No. 583326) or equivalent.
- If you have a 4-port card, Intermec provides you with a 4-port interface cable. Insert one end of the cable into the port on the RF card. Use Intermec cable kit (Intermec Part No. 055003) or equivalent to connect to one of the DNLN ports on the other end of the cable. You also need a Belden 89688 cable (Intermec Part No. 583326) or equivalent.

Example: The DCS 300 Connected to the Intermec 900 MHz RF Network

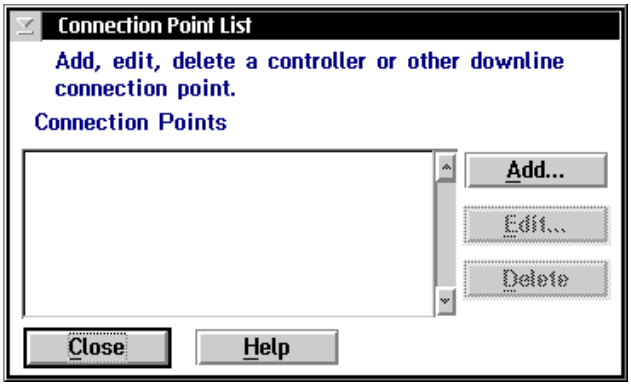


Configuring RF Cards

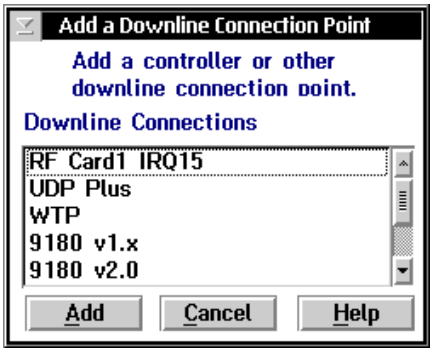
You must configure the communications parameters, enable the BRUs, set the Hot Standby timeout, and set any special time parameters for the RF cards. Each RF card must have a unique RFNC address and a unique network ID.

To configure the RF card

1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Downline Network. Two buttons, Connection Points and Downline Devices, appear.
3. Choose Connection Points. The Connection Point List dialog box appears.



4. Choose Add, Edit, or Delete. If you choose Add, the Add a Downline Connection Point dialog box appears.



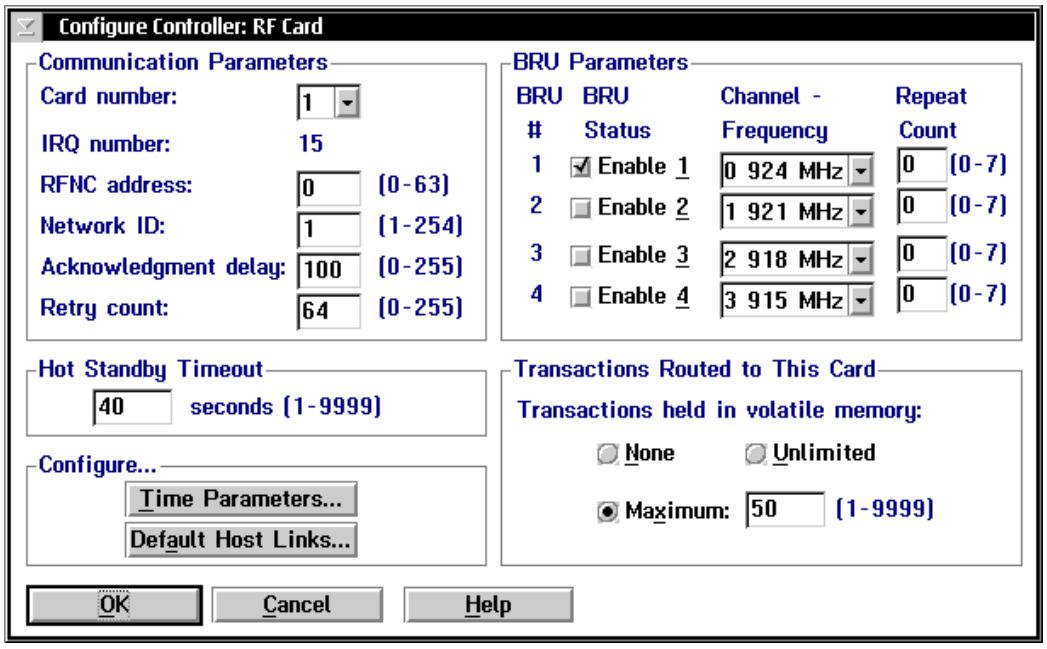
5. Choose the RF Card that you want to add and then choose Add. The Configure Controller: RF Card dialog box appears.
6. Configure the RF card. For help, see “Adding an RF Card” in the next section.
7. Set any time parameters for the RF card. For help, see “Setting the Time Parameters” later in this chapter.
8. Define a default host for each type of host that the RF card devices will communicate with through the RF card. For help, see “Defining Default Hosts” later in this chapter.
9. Choose OK. The RF Card Devices dialog box appears. For help, see “Defining the RF Card Devices” later in this chapter.
10. Choose Close to return to the Connection Point List dialog box.
11. Choose Close to return to the main menu.
12. Enable all the RF devices that you want to communicate with the server. For help, see “Enabling the RF Card Devices” later in this chapter.

Adding an RF Card

After you finish configuring the RF card and you choose OK, the RF Card Devices dialog box appears. For help, see "Defining the RF Card Devices" later in this chapter.

To add an RF card

- From the Add a Downline Connection Point dialog box, choose RF Card and then choose Add. The Configure Controller: RF Card dialog box appears.



Field	Description	Value	Default
Card number	The RF card that you want to configure.	1, 2	1
RFNC address	The unique radio frequency network address of the RF card. Devices use this address to communicate with the BRUs attached to this card.	0 to 63	0. If 0 is being used, the next available value is used.
Network ID	The unique network ID of the RF card. Devices use this ID during a channel search to locate the RF card's RFNC address.	1 to 254	1. If 1 is being used, the next available value is used.
Acknowledgment delay	The maximum amount of time in milliseconds that the RF card waits before it determines that the device did not receive a message.	0 to 255	100

Field	Description	Value	Default
Retry count	The number of times the RF card tries to transmit to a device.	0 to 255	64
BRU Status	This check box determines which BRUs are connected to the RF card.	Check, Clear	First BRU is checked, all others cleared.
Channel - Frequency	The channel and frequency on which the BRU is communicating.	0 to 6	0. If 0 is being used, the next available value is used.
Repeat count	The number of repeaters that a message is allowed to pass through for this BRU. ***Note:*** *Intermec recommends that a message does not pass through more than three repeaters.*	0 to 7	0
Hot Standby Timeout	The number of seconds the server waits to receive an acknowledgment after delivering a transaction to an RF device. If it does not receive an acknowledgment, the server writes the transactions for the RF device to a Hot Standby file. The RF device receives its transactions from this file when it comes back online.	1 to 9999	40
Transactions held in volatile memory	The number of transactions the server keeps in volatile RAM before it begins to write them to a Hot Standby file. Choose None if you want transactions always written to the file. Choose Unlimited if you do not want transactions written to the file unless the time you set for the Hot Standby timeout expires. Choose Maximum and enter a maximum number of transactions. When the server has this number of transactions in RAM, it writes them to a file.	None, Unlimited, Maximum	Maximum 50

Setting the Time Parameters

You can configure these time parameters between the BRUs and their devices.

Broadcast Parameters These optional parameters let the server broadcast a time, with a short string, at certain intervals to all RF devices. These parameters synchronize the RF devices with the server.

Append Parameters These optional parameters configure the BRUs to stamp the date and time to incoming data. The timestamp is in the format:

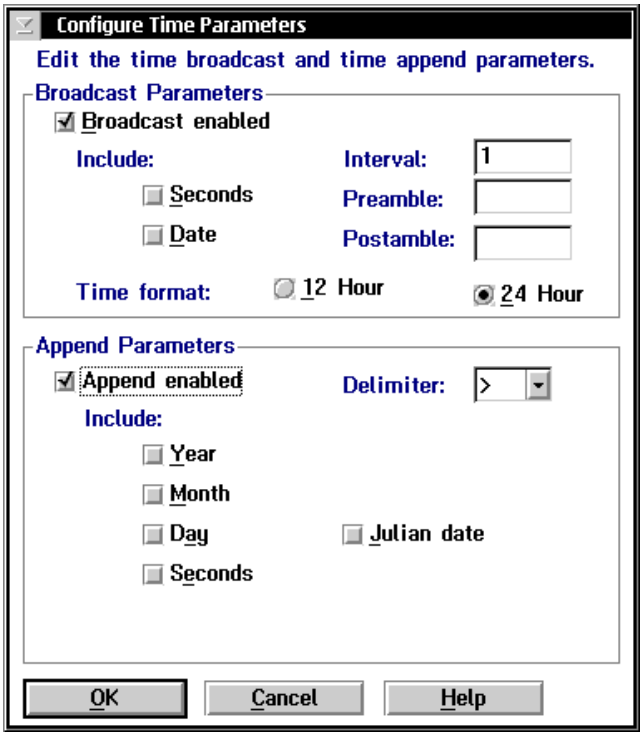
delimiterYYYY:MM:DD:HH:MM:SS

If you enable this feature, all messages have a timestamp with the hour and minute. You can also append the year, month, day, and seconds. Make sure that when you append the date and time to the incoming data, the maximum transaction data length will not exceed 1024 bytes. If the date and time that is appended is longer than the maximum transaction data length, the time append will be truncated. This feature will not operate when running terminal emulation or using the direct TCP/IP socket interface.

Note: *Do not enable time append on both the RF card and the RF device. If it is enabled on both, two timestamps are appended to incoming data.*

To set the time parameters

- From the Configure Controller: RF card dialog box, choose Time Parameters. The Configure Time Parameters dialog box appears.



Field	Description	Value	Default
Broadcast enabled	This check box determines if the BRUs send a time broadcast to all devices communicating with them.	Check, Clear	Clear
Include Seconds	This check box adds seconds to the time. ***Note:*** *If you are using JANUS devices to communicate with the BRUs, you must check this check box.*	Check, Clear	Clear
Include Date	This check box adds the date to the time.	Check, Clear	Clear
Time format	These option buttons choose the time format.	12 hour, 24 hour	12 hour
Interval	This field specifies how often in minutes the server broadcasts the time. If you set this field to 0, no broadcast is made.	0 to 99	1
Preamble	This field lets you add a short message to the beginning of the time.	1 to 5 alphanumeric characters	None
Postamble	This field lets you add a short message to the end of the time.	1 to 5 alphanumeric characters	None
Append enabled	This check box determines if a timestamp is added to messages from devices.	Check, Clear	Clear
Include Year	This check box adds the 4-digit year to the time.	Check, Clear	Clear
Include Month	This check box adds the 2-digit month to the time.	Check, Clear	Clear
Include Day	This check box adds the 2-digit day to the time.	Check, Clear	Check
Include Seconds	This check box adds the 2-digit seconds to the time.	Check, Clear	Clear
Delimiter	This character separates the data from the appended date and time.	1 alphanumeric or special character	>
Julian date	This check box determines if the date is in a 3-digit Julian format.	Check, Clear	Clear

Defining Default Hosts

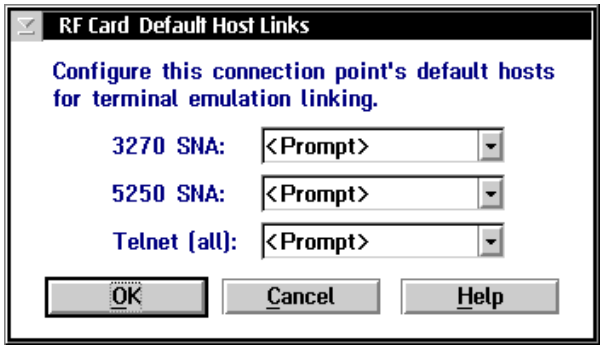
You can define a default method for the RF card devices to get a host name when they are communicating with different types of hosts. You can configure the RF card devices to

- explicitly link with a specific host. Click the down arrow on the right side of the field and choose a host that you have configured.
- prompt the user to enter a host name. Click the down arrow on the right side of the field and choose <Prompt>.
- not communicate with a host. Click the down arrow on the right side of the field and choose <none>.

To configure a specific device to communicate in a different way to a host, see "Configuring TE Links" in Chapter 8.

To configure your link

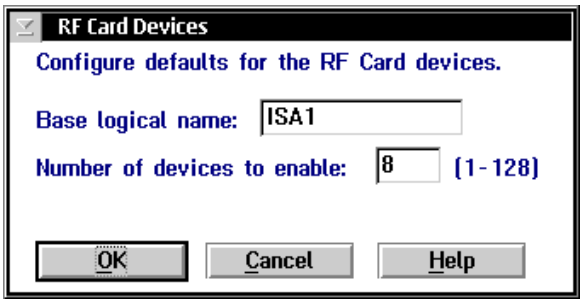
- From the Configure Controller: RF card dialog box, choose Default Host Links. The RF Card Default Host Links dialog box appears.



Field	Description	Value	Default
3270 SNA	The method that the RF card devices will use to get a host name when they communicate with 3270 SNA hosts.	None, Prompt, pre-defined list	Prompt
5250 SNA	The method that the RF card devices will use to get a host name when they communicate with 5250 SNA hosts.	None, Prompt, pre-defined list	Prompt
Telnet (all)	The method that the RF card devices will use to get a host name when they communicate with Telnet hosts.	None, Prompt, pre-defined list	Prompt

Defining the RF Card Devices

When you choose OK in the Configure Controller: RF Card dialog box, this dialog box appears.



Field	Description	Value	Default
Base logical name	The base name that the server uses to create a unique logical name for each device. The server appends a sequential 3-digit number to this name for each device.	1 to 13 alphanumeric characters	ISA1
Number of devices to enable	The number of logical names that you want to enable to communicate with the server.	1 to 128	8

Enabling the RF Card Devices

When you configured the RF card, you enabled a fixed number of RF card devices to communicate with the DCS 300. You can enable up to 128 RF card devices. Use the Device List dialog box to enable or disable addresses and logical names for devices that you want to communicate with the server.

Note: *Do not enable devices that you are not using. If you try to send data to a nonexistent enabled device, your system performance will degrade.*

You can edit each device to change its logical name, device type, transaction IDs, and delivery responses.

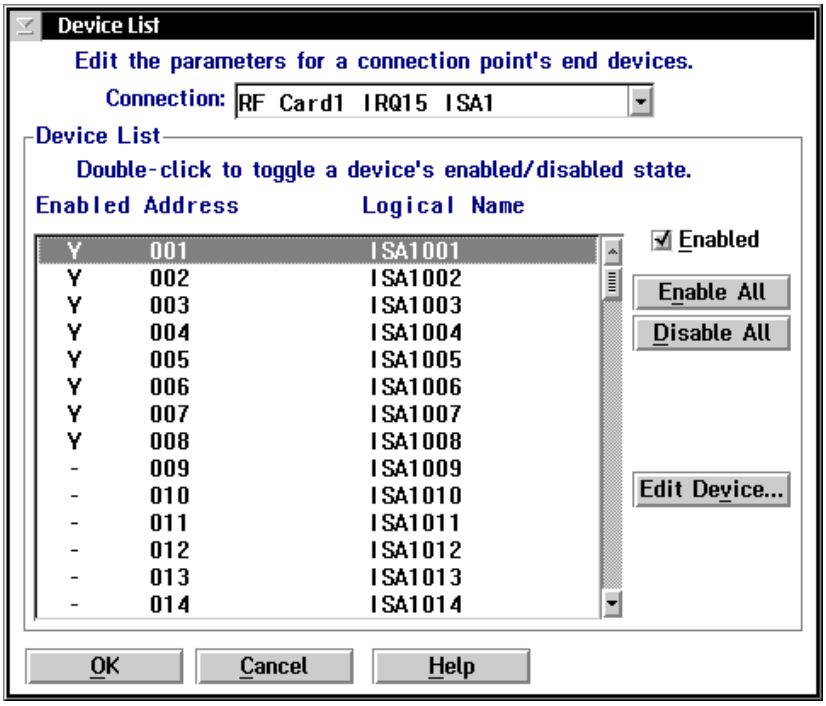
Your server is licensed to communicate with a fixed number of devices (1-8, 1-24, 1-64, 1-254). The server does not keep track of the number of devices you enable. You can enable all 254 devices. As each device sends messages to the server, the server logs its logical name. When the server logs the maximum number of logical names that your terminal license allows, it will not accept messages from any new logical names. When you stop data collection on the server, the terminal license count number is reset. If you need to purchase an upgrade to your terminal license, contact your local Intermec representative.

Note: *Each BRU only supports 32 devices. There fore, the maximum number of devices you can enable is 224 (7 BRUs x 32 devices). However, Intermec recommends that you do not enable more than 128 devices for maximum throughput.*

To enable the RF card devices

1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Downline Network. Two buttons, Connection Points and Downline Devices, appear.
3. Choose Downline Devices. The Device List dialog box appears.

Device List Dialog Box



4. In the Connection field, click the down arrow on the right side of the field. A list of the connection points that you have configured appears. Select the RF card for which you want to enable devices.
5. To enable all 128 devices, choose Enable All.

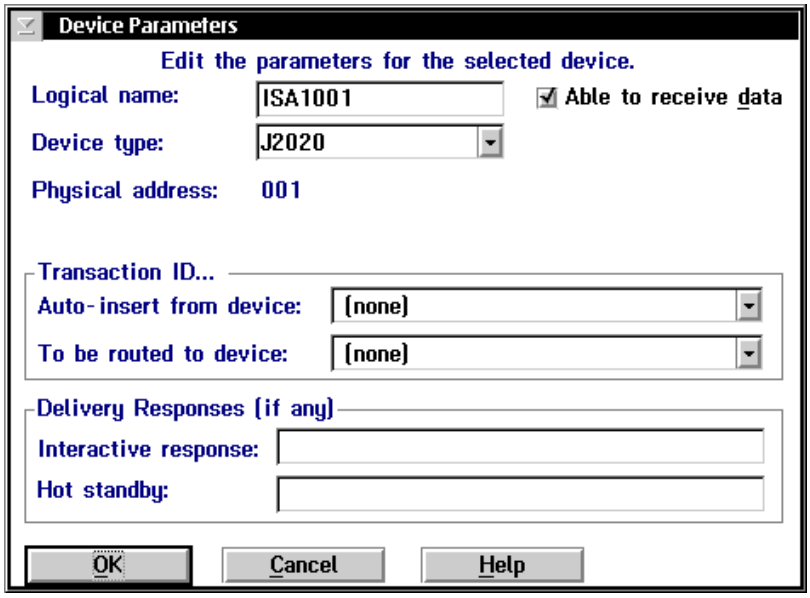
   Or, to enable specific devices, select the device you want to enable and make sure there is a check in the Enabled check box.
6. To disable all 128 devices, choose Disable All.

   Or, to disable specific devices, select the device you want to disable and make sure there is no check in the Enabled check box.
7. Select a terminal whose individual parameters you want to edit and then choose Edit Device. For help, see “Editing an RF Card Device” in the next section.
8. Choose OK to save your changes and return to the main menu.

Editing an RF Card Device

- From the Device List dialog box, choose Edit Device. The Device Parameters dialog box appears.

  Note: *If you are using terminal emulation, do not configure transaction IDs or delivery responses.*



Field	Description	Value	Default
Logical name	The logical name of the device.	1 to 16 alphanumeric characters	ISA1XXX
Able to receive data	This check box determines if this device can receive data from the network.	Check, Clear	Check
Device type	This list box contains the current Intermec devices that are supported.	Predefined list	J2020
Auto-insert from device	This field provides a transaction ID for this device if it cannot put a transaction ID in its transactions. ***Note:*** *All transactions from this terminal will be routed using this transaction ID.*	Predefined list	None
To be routed to device	This field contains a transaction ID that will always be routed to this device.	Predefined list	None
Interactive response (Optional)	The message that is sent to the source of the transaction if the transaction is delivered successfully to this device in Interactive mode.	1 to 39 characters	None
Hot standby (Optional)	The message that is sent to the source of the transaction if the transaction for this device is written to a Hot Standby file.	1 to 40 characters	None

Connecting the DCS 300 to the UDP Plus Network

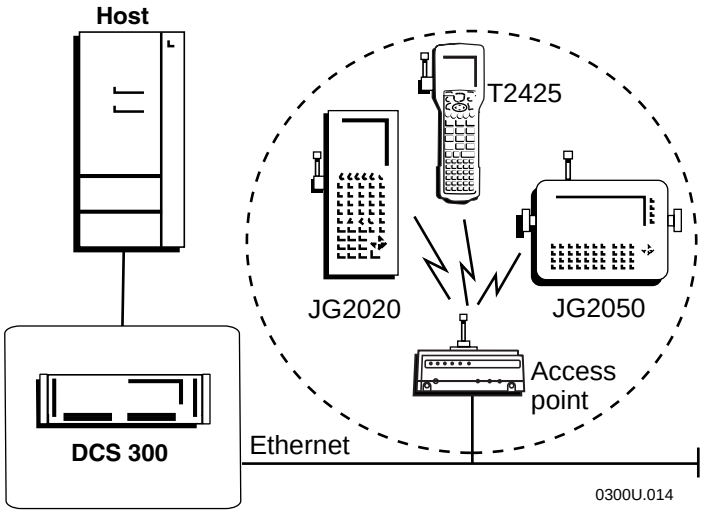
The DCS 300 supports communications with Intermec's UDP Plus network (2.4 GHz RF network) through access points that are connected to the Ethernet or token ring network. You can run standard TCP/IP applications, such as FTP, with the server. The illustration on the next page shows an example of a DCS 300 connected to the UDP Plus network.

You can also use the server to route any IP traffic from one subnet to the server. For example, if the server is connected to a twinaxial host, it can pass IP traffic from an Ethernet network to the host and back.

Refer to the figure on the next page. The UDP Plus network consists of access points communicating with various JANUS devices and TRAKKER Antares terminals.

- Access points act as bridges between the Ethernet or token ring network and Intermec's UDP Plus network. All terminals communicating in this network must have the same domain and security ID.
- TRAKKER Antares terminals, such as the T2425, are terminals with network support. The server supports these terminals using Intermec's UDP Plus network. Follow the instructions "Configuring a UDP Plus Network" later in this chapter.
- JANUS UDP Plus devices, such as the JG2020, are hand-held data collection computers with network support. The server communicates with these terminals using UDP Plus. The JANUS devices support both Novell NetWare Client for DOS and Novell LAN Workplace for DOS. Intermec recommends that you use LAN Workplace to provide the TCP/IP protocol stack.

Example: The DCS 300 Connected to the Intermec UDP Plus Network

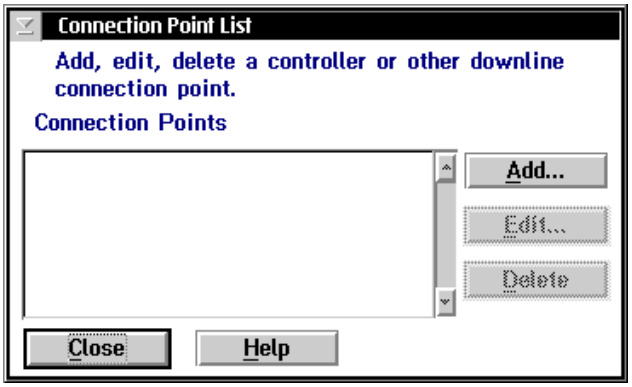


Configuring a UDP Plus Network

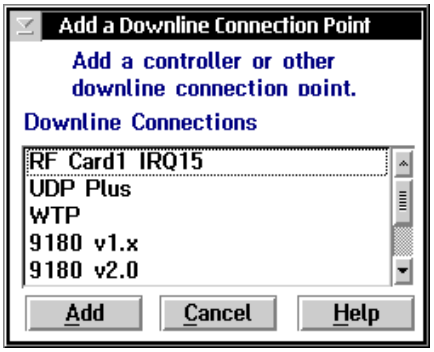
You must configure a UDP Plus network if you want the DCS 300 to communicate with TRAKKER Antares terminals and JANUS UDP Plus devices.

To configure a UDP Plus network

1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Downline Network. Two buttons, Connection Points and Downline Devices, appear.
3. Choose Connection Points. The Connection Point List dialog box appears.



4. Choose Add, Edit, or Delete. If you choose Add, the Add a Downline Connection Point dialog box appears.



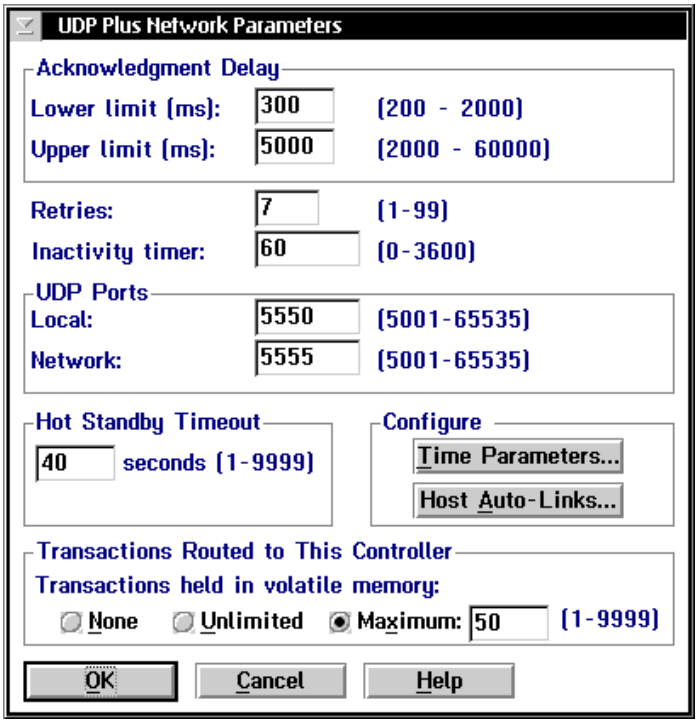
5. Choose UDP Plus and then choose Add. The UDP Plus Network Parameters dialog box appears.
6. Configure the UDP Plus network. For help, see "Adding a UDP Plus Network" in the next section.
7. Set any time parameters for the UDP Plus network. For help, see "Setting the Time Parameters" later in this chapter.
8. Define a default host for each type of host that the UDP Plus devices will communicate with. For help, see "Defining Default Hosts" later in this chapter.
9. Choose OK. The UDP Plus Devices dialog box appears. For help, see "Setting Up the UDP Plus Devices" later in this chapter.
10. Choose OK to return to the Connection Point List dialog box.
11. Choose Close to return to the main menu.
12. Enable all the UDP Plus devices that you want to communicate with the server. For help, see "Enabling the UDP Plus Devices" later in this chapter.

Adding a UDP Plus Network

After you finish configuring the UDP Plus network and you choose OK, the UDP Plus Devices dialog box appears. For help, see “Setting Up the UDP Plus Devices” later in this chapter.

To add a UDP Plus network

- From the Add a Downline Connection Point dialog box, choose UDP Plus and then choose Add. The UDP Plus Network Parameters dialog box appears.



Field	Description	Value	Default
Lower limit	The minimum time in milliseconds the server waits for an acknowledgment from the device before resending a transaction.	200 to 2000	300
Upper limit	The maximum time in milliseconds the server waits for an acknowledgment from the device before resending a transaction.	2000 to 60000	5000
Retries	The number of times the server tries to transmit to a device before it sets the device to "not responding."	1 to 99	7
Inactivity timer	The amount of time in minutes the terminal can be "not responding" before it is set to "disconnected."	0 to 3600	60
Local	The UDP port through which the server communicates with itself. This port must be different from the network port.	5001 to 65535	5550
Network	The UDP port that UDP Plus uses for communication. This port must match the network port that is configured on the terminal.	5001 to 65535	5555
Hot Standby Timeout	The number of seconds the server waits to receive an acknowledgment after delivering a transaction to a device. If it does not receive an acknowledgment, the server writes the transactions for the device to a Hot Standby file. The device receives its transactions from the Hot Standby file when it comes back online.	1 to 9999	40
Transactions held in volatile memory	The number of transactions the server keeps in volatile RAM before it begins to write them to a Hot Standby file. Choose None if you want transactions always written to the file. Choose Unlimited if you do not want transactions written to the file unless the time you set for the Hot Standby timeout expires. Choose Maximum and enter a maximum number of transactions. When the server has this number of transactions in RAM, it writes them to a file.	None, Unlimited, Maximum	Maximum 50

Setting the Time Parameters

You can configure these time parameters between the server and the UDP Plus terminals.

Broadcast Parameters These optional parameters allow the server to broadcast a time at certain intervals to all UDP Plus terminals. These parameters synchronize the terminals with the server.

Append Parameters These optional parameters configure the server to stamp the date and time to incoming data. The timestamp is in the format:

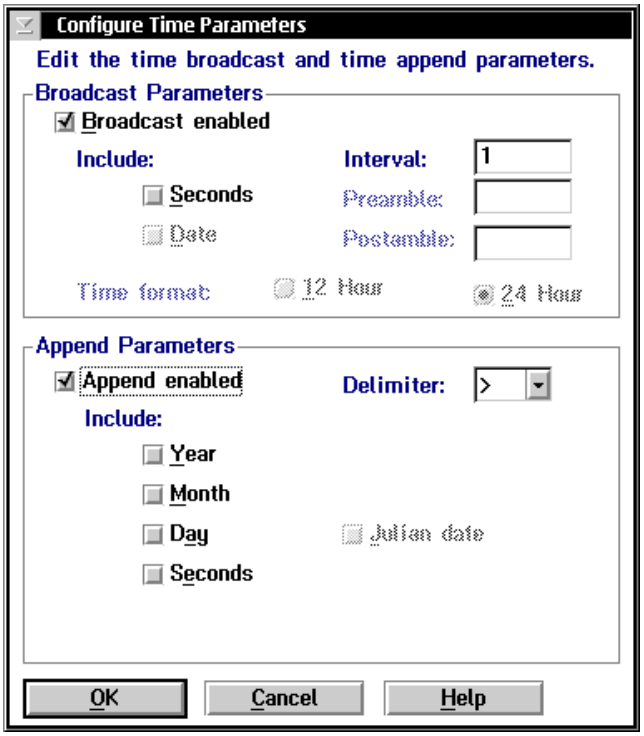
delimiterYYYY:MM:DD:HH:MM:SS

If you enable this feature, all messages have a timestamp with the hour and minute. You can also append the year, month, day, and seconds. Make sure that when you append the date and time to the incoming data, the maximum transaction data length will not exceed 1024 bytes. If the date and time that is appended is longer than the maximum transaction data length, the time append will be truncated. You cannot use this feature when running terminal emulation.

Note: *Do not enable time append on both the UDP Plus network and the terminal. If it is enabled on both, two timestamps are appended to incoming data.*

To set the time parameters

- From the UDP Plus Network Parameters dialog box, choose Time Parameters. The Configure Time Parameters dialog box appears.



Field	Description	Value	Default
Broadcast enabled	This check box determines if the server sends a time broadcast to all terminals in the UDP Plus network.	Check, Clear	Clear
Interval	This field specifies how often in minutes the server broadcasts the time. If you set this field to 0, no broadcast is made.	0 to 99	1
Append enabled	This check box determines if a timestamp is added to messages from terminals.	Check, Clear	Clear
Include Year	This check box adds a 4-digit year to the time.	Check, Clear	Clear
Include Month	This check box adds a 2-digit month to the time.	Check, Clear	Clear
Include Day	This check box adds a 2-digit day to the time.	Check, Clear	Check
Include Seconds	This check box adds a 2-digit seconds to the time.	Check, Clear	Clear
Delimiter	This character separates the data from the appended date and time.	1 alphanumeric or special character	>
Julian date	This check box determines if the date for the time is in a 3-digit Julian format.	Check, Clear	Clear

Defining Default Hosts

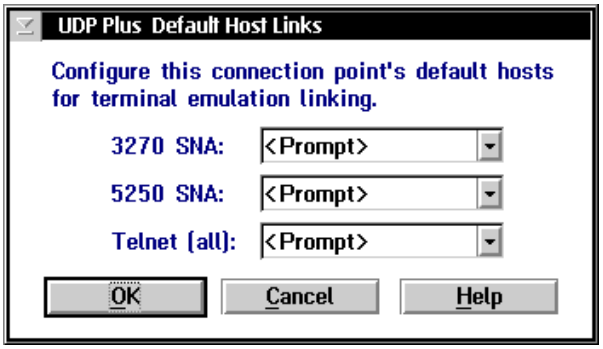
You can define a default method for the UDP Plus devices to get a host name when they are communicating with different types of hosts. You can configure the UDP Plus devices to

- explicitly link with a specific host. Click the down arrow on the right side of the field and choose a host that you have configured.
- prompt the user to enter a host name. Click the down arrow on the right side of the field and choose <Prompt>.
- not communicate with a host. Click the down arrow on the right side of the field and choose <none>.

To configure a specific device to communicate in a different way to a host, see "Configuring TE Links" in Chapter 8.

To configure your link

- From the UDP Plus Network Parameters dialog box, choose Default Host Links. The UDP Plus Default Host Links dialog box appears.



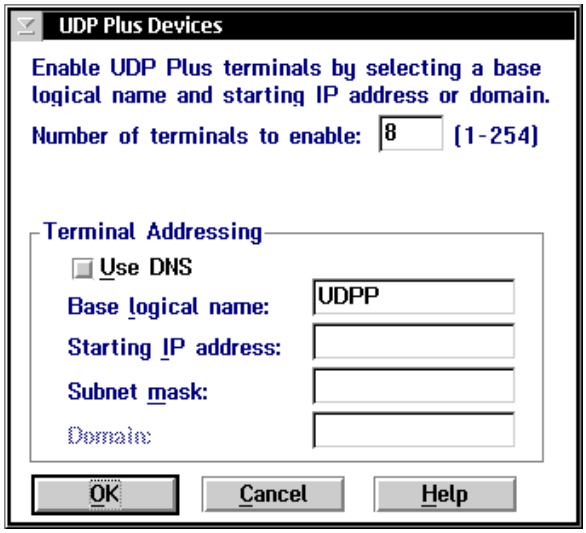
Field	Description	Value	Default
3270 SNA	The method that the UDP Plus devices will use to get a host name when they communicate with 3270 SNA hosts.	None, Prompt, pre-defined list	Prompt
5250 SNA	The method that the UDP Plus devices will use to get a host name when they communicate with 5250 SNA hosts.	None, Prompt, pre-defined list	Prompt
Telnet (all)	The method that the UDP Plus devices will use to get a host name when they communicate with Telnet hosts.	None, Prompt, pre-defined list	Prompt

Setting Up the UDP Plus Devices

When you choose OK in the UDP Plus Network parameters dialog box, the UDP Plus Devices dialog box appears. The DCS 300 must know the IP address for every UDP Plus terminal that it may communicate with. You can either use the DCS 300 to generate logical names for each terminal and use a DNS server to resolve the IP addresses or you can enter each terminal's IP address.

Use a DNS server If you use a DNS server, you do not need to enter the terminal's IP address on the DCS 300. You only need to enter the number of terminals to enable, a base logical name, and the domain. The DCS 300 generates the logical names for the terminals and the DNS server resolves the IP addresses. However, you still need to enter the terminal's IP address on the terminal.

Enter each terminal's IP address manually If you do not use a DNS server, you need to enter the terminal's IP address on the DCS 300. However, the server can help you generate logical names and IP addresses for the terminals. You need to enter the number of terminals to enable, a starting IP address, and a subnet mask. The server generates an appropriate number of sequential logical names and IP addresses. Make sure that each IP address that the server generates for a terminal matches an IP address on a terminal.



Field	Description	Value	Default
Number of terminals to enable	The number of logical names that you want to enable to communicate with the server. The server also generates this number of IP addresses.	1 to 254	8
Use DNS	This check box determines if the server uses a DNS server to translate the logical name to an IP address. ***Note:*** *Before you check this check box, you must first configure a DNS server in the DNS Configuration dialog box.*	Check, Clear	Clear
Base logical name	The base name that the server uses to create a unique logical name for each terminal. The server appends a sequential 3-digit number to this name for each terminal.	1 to 13 alphanumeric characters	UDPP
Starting IP address	The starting IP address that the server uses to assign IP addresses to each terminal. The IP address must be a valid IP v4 address.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	None
Subnet mask	The subnet mask that the server uses to validate the IP addresses. The server verifies that they do not cross a subnet boundary.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	Based on starting IP address
Domain	The name of the domain that all of the terminals are in. ***Note:*** *If you check the Use DNS check box and you do not enter a domain, the server searches the domains that are listed in the DNS Configuration dialog box.*	None	None

Enabling the UDP Plus Devices

When you configured the UDP Plus network, you enabled a fixed number of UDP Plus terminals to communicate with the DCS 300. You can enable up to 254 UDP Plus terminals. Use the Device List dialog box to enable or disable IP addresses and logical names for terminals that you want to communicate with the server.

Note: *Do not enable devices that you are not using. If you try to send data to a nonexistent enabled device, your system performance will degrade.*

You can edit each terminal to change its logical name, IP address, device type, transaction IDs, and delivery responses. You can also use DNS to determine the device's IP address or to edit an IP address.

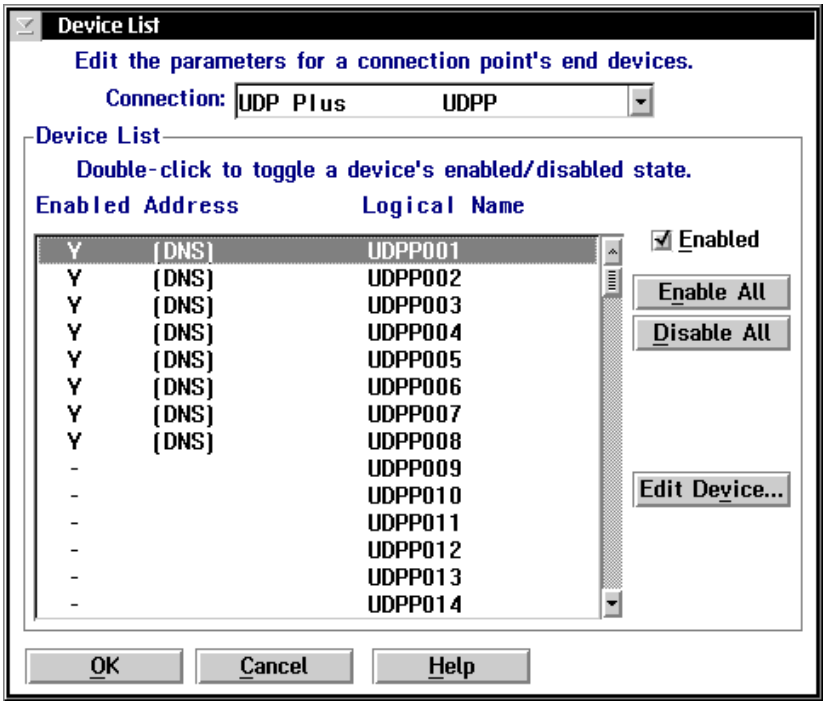
Your server is licensed to communicate with a fixed number of terminals (1-8, 1-24, 1-64, 1-254). The server does not keep track of the number of terminals you enable. You can enable all 254 terminals. As each terminal sends messages to the server, the server logs its logical name. When the server logs the maximum number of logical names that your terminal license allows, it will not accept messages from any new logical names. When you stop data collection on the server, the terminal license count number is reset.

If you need to purchase an upgrade to your terminal license, contact your local Intermec representative.

To enable the UDP Plus devices

1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Downline Network. Two buttons, Connection Points and Downline Devices, appear.
3. Choose Downline Devices. The Device List dialog box appears.

Device List Dialog Box



4. In the Connection field, click the down arrow on the right side of the field. A list of the connection points that you have configured appears. Select UDP Plus.
5. To enable all 254 devices, choose Enable All.

   Or, to enable specific terminals, select the terminal you want to enable and make sure there is a check in the Enabled check box.

   Note: *Each terminal must use DNS or have a valid IP v4 address before you can enable it.*

6. To disable all 254 terminals, choose Disable All.

   Or, to disable specific terminals, select the terminal you want to disable and make sure there is no check in the Enabled check box.
7. Select a terminal whose individual parameters you want to edit and choose Edit Device. Follow the next procedure, “Editing a UDP Plus Device.”
8. Choose OK to save your changes and return to the main menu.

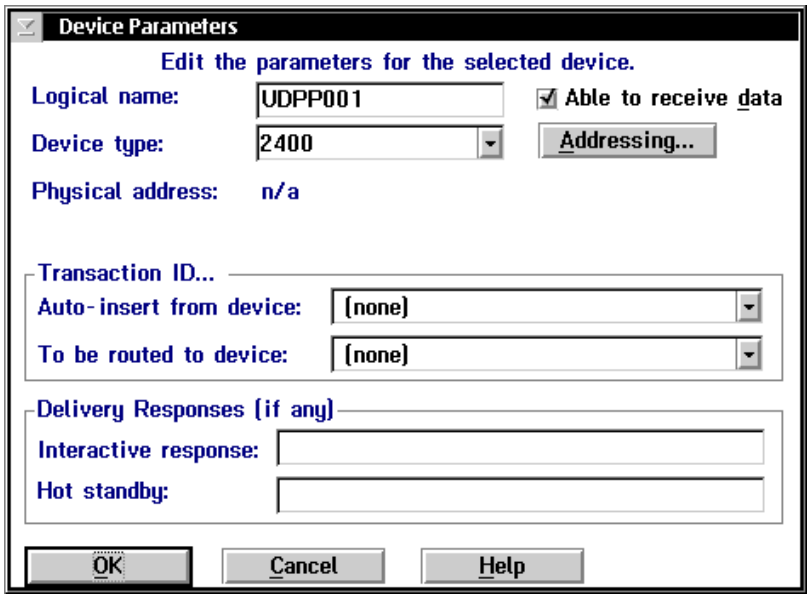
Editing a UDP Plus Device

This dialog box lets you edit many parameters for your UDP Plus terminal. If you need to edit or resolve the IP address of the terminal, see "Determining a UDP Plus Device's IP Address" or "Editing a UDP Plus Device's IP Address" later in this chapter.

To edit a UDP Plus device

- From the Device List dialog box, choose Edit Device. The Device Parameters dialog box appears.

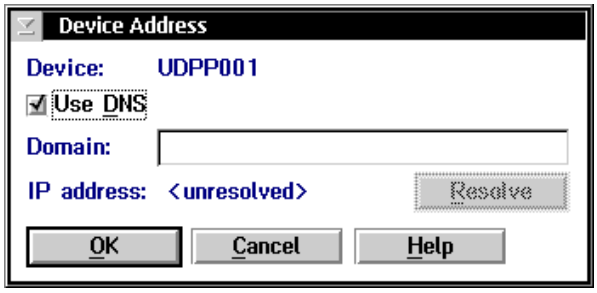
  Note: *If you are using terminal emulation, do not configure transaction IDs or delivery responses.*



Field	Description	Value	Default
Logical name	The logical name of the terminal. This name is created from the base logical name plus a 3-digit number.	1 to 16 alphanumeric characters	UDPPXXX
Able to receive data	This check box determines if this terminal can receive data from the network.	Check, Clear	Check
Device type	This list box contains all the current Intermec terminals supported.	Predefined list	2400
Auto-insert from device	This field provides a transaction ID for this terminal if it cannot put a transaction ID in its transactions. ***Note:*** *All transactions from this terminal are routed using this transaction ID.*	Predefined list	None
To be routed to device	This field contains a transaction ID that will always be routed to this terminal.	Predefined list	None
Interactive response (Optional)	The message that is sent to the source of the transaction if the transaction is delivered successfully to this terminal.	1 to 39 characters	None
Hot standby (Optional)	The message that is sent to the source of the transaction if the transaction for this terminal is written to a Hot Standby file.	1 to 40 characters	None

Determining a UDP Plus Device's IP Address

If you are using a DNS server and you want to know the IP address of a terminal, then from the Device Parameters dialog box, choose Addressing. The Device Address dialog box appears.

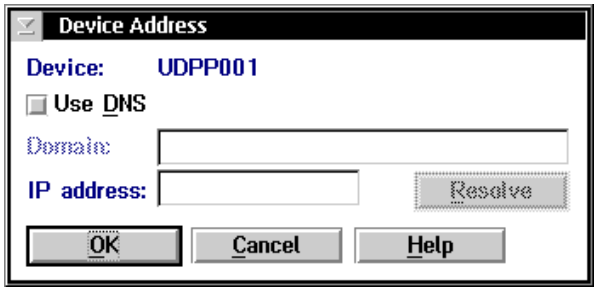


To determine a terminal's IP address

1. (Optional) In the Domain field, enter the specific domain that contains the terminal.
2. Choose Resolve to look up the terminal's IP address on the DNS server using the logical name. If you did not enter a domain, the server searches the list of domains that are configured in the DNS Configuration dialog box.

Editing a UDP Plus Device's IP Address

If you are not using a DNS server and you want to edit the IP address of a terminal, from the Device Parameters dialog box, choose Addressing. The Device Address dialog box appears.



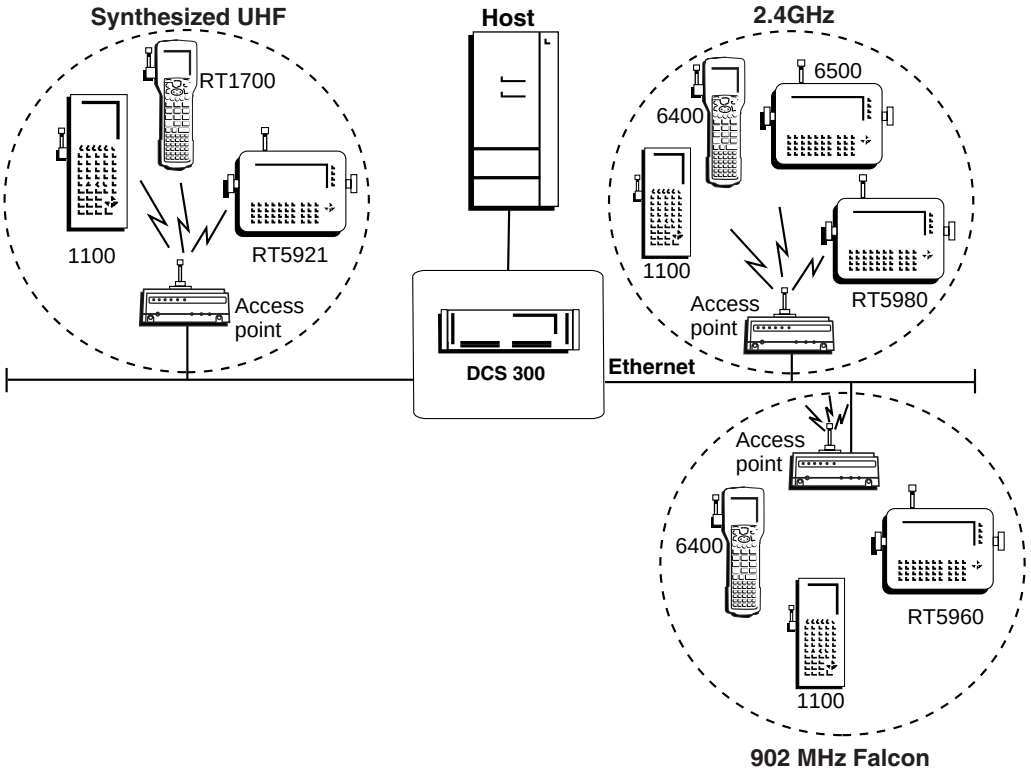
To edit a terminal's IP address

1. Clear the Use DNS check box.
2. In the IP address field, enter a new IP address for the terminal.

Connecting the DCS 300 to the WTP Network

The DCS 300 supports communications with WTP devices through access points that are connected to the Ethernet or token ring network. Access points act as bridges between the Ethernet or token ring network and WTP network. The illustration below shows an example of the DCS 300 connected to the WTP network.

Example: The DCS 300 Connected to the WTP Network

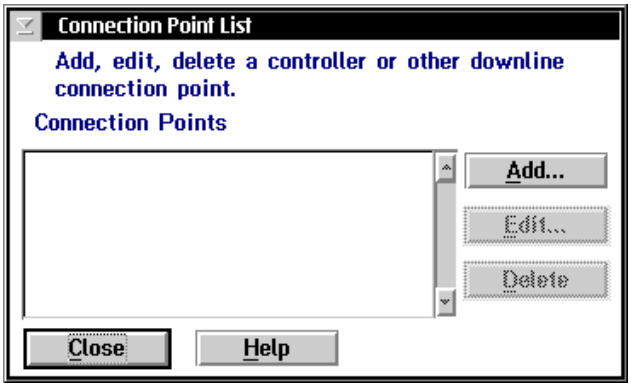


Configuring a WTP Network

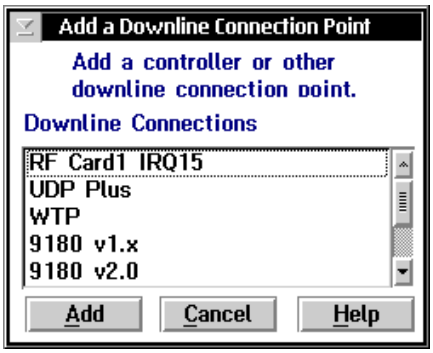
You must configure a WTP network if you want the DCS 300 to communicate with WTP devices.

To configure a WTP network

1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Downline Network. Two buttons, Connection Points and Downline Devices, appear.
3. Choose Connection Points. The Connection Point List dialog box appears.



4. Choose Add, Edit, or Delete. If you choose Add, the Add a Downline Connection Point dialog box appears.



5. Choose WTP and then choose Add. The WTP Parameters dialog box appears.
6. Configure the WTP network. For help, see “Adding a WTP Network” in the next section.
7. Define how the WTP devices will communicate with each of the different types of hosts. For help, see “Auto-Linking to Hosts” later in this chapter.
8. Choose OK. The WTP Devices dialog box appears. For help, see “Setting Up the WTP Devices” later in this chapter.
9. Choose OK. The RF Hosts Created for WTP dialog box appears. For help, see “About the RF Hosts Created for WTP” later in this chapter.
10. Choose OK to close the RF Hosts Created for WTP dialog box and return to the Connection Point List dialog box.
11. Choose Close to return to the main menu.
12. Enable all the WTP devices that you want to communicate with the server. For help, see “Enabling the WTP Devices” later in this chapter.

Adding a WTP Network

You can define a default method for the WTP devices to get a host name when they are communicating with different types of hosts. You can configure the WTP devices to

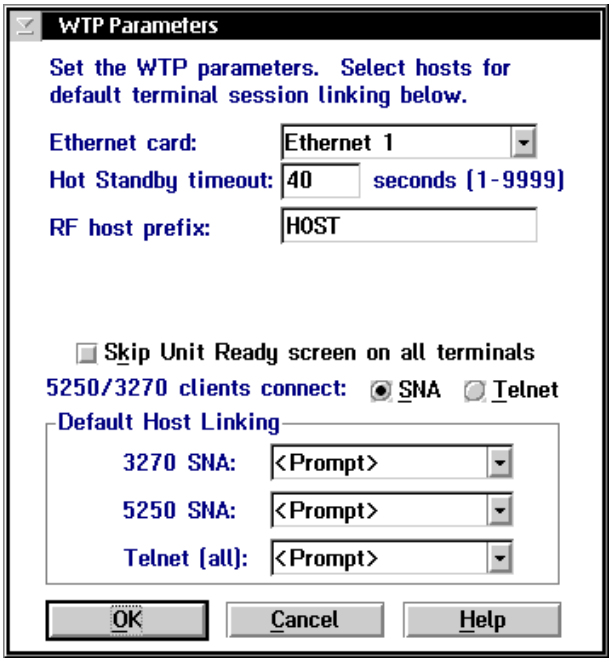
- explicitly link with a specific host. Click the down arrow on the right side of the field and choose a host that you have configured.
- prompt the user to enter a host name. Click the down arrow on the right side of the field and choose <Prompt>.
- not communicate with a host. Click the down arrow on the right side of the field and choose <none>.

To configure a specific device to communicate in a different way to a host, see "Configuring TE Links" in Chapter 8.

After you finish adding the WTP network and you choose OK, the WTP Devices dialog box appears. For help, see "Setting Up the WTP Devices" in the next section.

To add a WTP network

- From the Add a Downline Connection Point dialog box, choose WTP and then choose Add. The WTP Parameters dialog box appears.

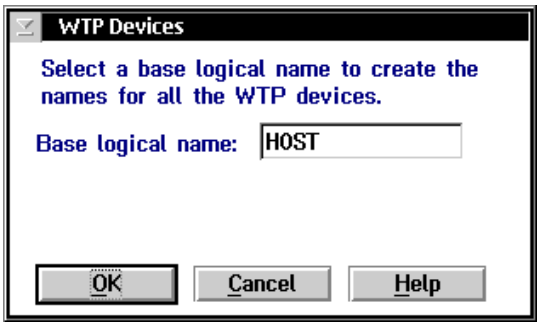


Field	Description	Value	Default
Ethernet card	The Ethernet card that you want to communicate with the WTP network.	Ethernet 1, Ethernet 2,	Ethernet 1
Hot Standby timeout	The number of seconds the server waits to receive an acknowledgment after delivering a transaction to a device. If it does not receive an acknowledgment, the server writes the transactions for the device to a Hot Standby file. The device receives its transactions from the Hot Standby file when it comes back online.	1 to 9999	40
RF host prefix	A name for the server that the server uses to generate the host instances to support the WTP network.	4 to 13 alphanumeric characters	HOST
Skip Unit Ready screen on all terminals	Determines if the WTP devices display their initialization information (Unit Ready) on the screen when they connect to the server.	Check, Clear	Clear
5250/3270 clients connect	Determines which emulation type the server will use to communicate with the host when it receives a transaction from the WTP network. ***Note:*** *WTP devices must communicate with the server using Telnet. The server will convert the transaction to the appropriate format for the host type.*	SNA, Telnet	SNA
3270 SNA	The host that a WTP device connects to if the device is not explicitly linked to a host and it is running a 3270 application.	None, Predefined list, Prompt	<Prompt>
5250 SNA	The host that a WTP device connects to if the device is not explicitly linked to a host and it is running a 5250 application.	None, Predefined list, Prompt	<Prompt>
Telnet	The host that a WTP device connects to if the device is not explicitly linked to a host and it is running a Telnet application.	None, Predefined list, Prompt	<Prompt>

Setting Up the WTP Devices

When you choose OK in the WTP Parameters dialog box, the WTP Devices dialog box appears. This dialog box generates logical names for each device.

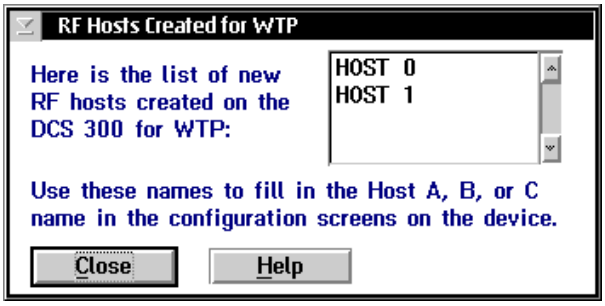
After you finish configuring the WTP devices and you choose OK, the RF Hosts Created for WTP dialog box appears. For help, see "About the RF Hosts Created for the WTP Network" in the next section.



Field	Description	Value	Default
Base logical name	The base name that the server uses to create a unique logical name for each device. The server appends a sequential 3-digit number to this name for each device.	1 to 13 alphanumeric characters	HOST

About the RF Hosts Created for the WTP Network

If you are adding a WTP network, when you choose OK in the WTP Devices dialog box, the RF Hosts Created for WTP dialog box appears. This dialog box shows you the RF host instances that the DCS 300 has created to support your terminal license. If your terminal license is a Level 3 or a Level 4, you must assign each device to the RF host instance that you want it to communicate with. Each RF host instance supports up to 127 terminal sessions.



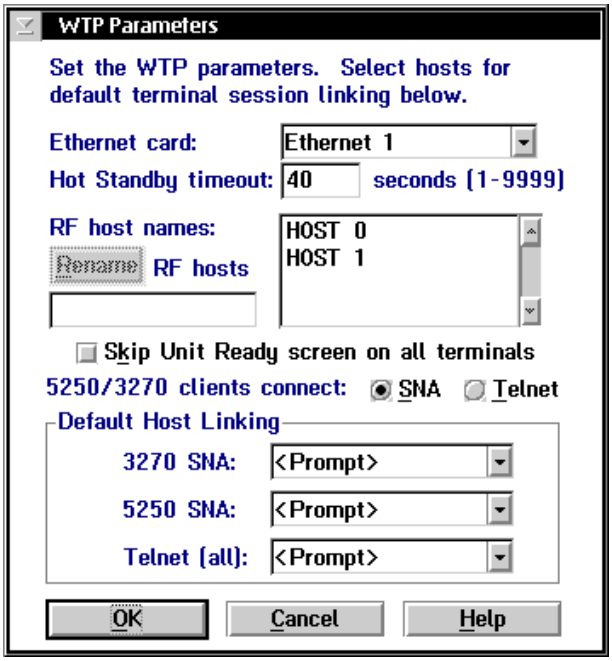
Editing the WTP Network

When you edit the WTP network, the WTP Parameters dialog box looks slightly different than when you added the network.

Rename RF Hosts This button lets you rename the RF host. Enter the new name in the field and then choose Rename. Note that each WTP device is configured with the RF host instance that it is using to communicate with the DCS 300. If you change the RF host name, you must reconfigure each device with the new name.

To edit the WTP network

- From the Connection Point List dialog box, choose WTP and then choose Edit. The WTP Parameters dialog box appears.



Enabling the WTP Devices

You do not need to enable each WTP device that you want to communicate with the DCS 300. The device list contains the logical names of all 254 WTP devices. The MAC address of the device only appears when a device connects with the server. You can edit each terminal to change its logical name, device type, MAC address, number of terminal sessions, transaction IDs, and delivery responses.

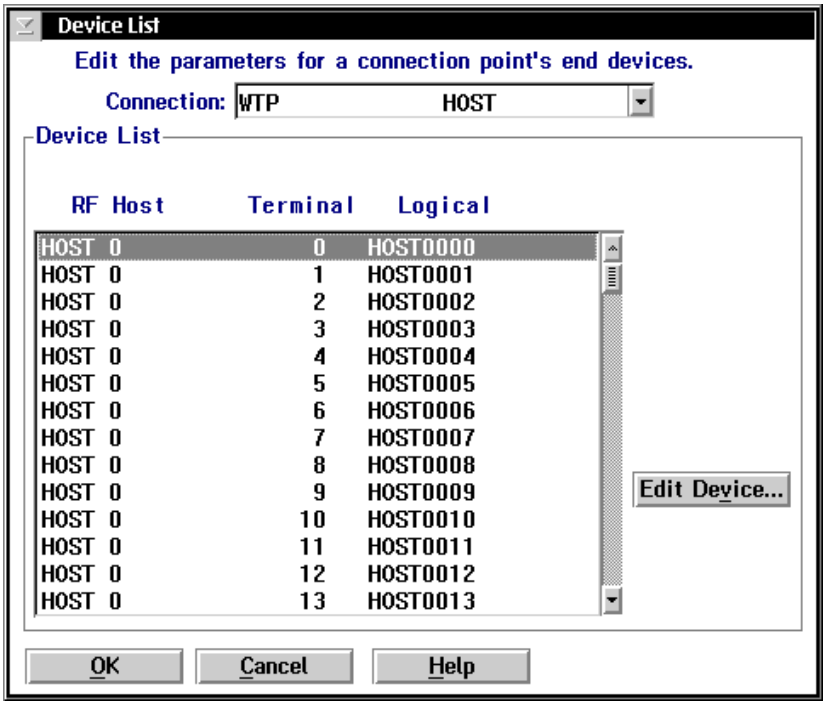
Your server is licensed to communicate with a fixed number of devices (1-8, 1-24, 1-64, 1-254). As each device sends messages to the server, the server logs its logical name. When the server logs the maximum number of logical names that your terminal license allows, it will not accept messages from any new logical names. When you stop data collection on the server, the terminal license count number is reset.

If you need to purchase an upgrade to your terminal license, contact your local Intermec representative.

To identify the WTP devices

1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Downline Network. Two buttons, Connection Points and Downline Devices, appear.
3. Choose Downline Devices. The Device List dialog box appears.

Device List Dialog Box

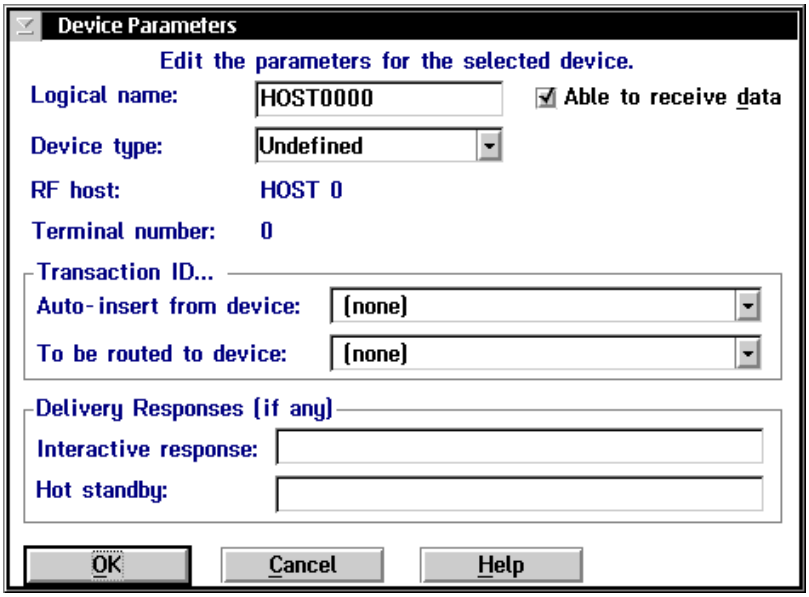


4. In the Connection field, click the down arrow on the right side of the field. A list of the connection points that you have configured appears. Select WTP.
5. Select a terminal whose individual parameters you want to edit and choose Edit Device. Follow the next procedure, “Editing a WTP Device.”
6. Choose OK to save your changes and return to the main menu.

Editing a WTP Device

- From the Device List dialog box, choose Edit Device. The Device Parameters dialog box appears.

  Note: *If you are using terminal emulation, do not configure transaction IDs or delivery responses.*



Field	Description	Value	Default
Logical name	The logical name of the device. This name is created from the base logical name plus a 3-digit number.	1 to 16 alphanumeric characters	HOST000
Able to receive data	This check box determines if this device can receive data from the network.	Check, Clear	Check
Device type	This list box contains all the current Intermec devices supported.	Predefined list	Undefined
Auto-insert from device	This field provides a transaction ID for this device if it cannot put a transaction ID in its transactions. ***Note:*** *All transactions from this terminal are routed using this transaction ID.*	Predefined list	None
To be routed to device	This field contains a transaction ID that will always be routed to this device.	Predefined list	None
Interactive response (Optional)	The message that is sent to the source of the transaction if the transaction is delivered successfully to this device.	1 to 39 characters	None
Hot standby (Optional)	The message that is sent to the source of the transaction if the transaction for this device is written to a Hot Standby file.	1 to 40 characters	None

Saving Your Run-Time Configuration

When you finish configuring your downline network, you should save your changes.

To save your run-time configuration

- From the main menu sidebar buttons, choose Save Configuration.

7

Connecting to the 9180 and the Intermec CrossBar Network

This chapter describes how to configure the DCS 300 to communicate with the 9180 Network Controller, other controllers in Intermec's CrossBar network, and the CrossBar devices.

Chapter Checklist

Done?	Task	Page
❑	Install all your Intermec controllers.	None
❑	Identify all the controllers on the DCS 300.	7-4
❑	Configure each controller connected to the DCS 300.	7-6
❑	Set the time parameters for each controller.	7-15
❑	Identify all the CrossBar devices connected to controllers.	7-20
❑	Edit the CrossBar devices.	7-22

Note: *In order for the 9181 Base Radio Units (BRUs) to communicate with a 9180 Network Controller that is connected to the DCS 300, you need to configure these BRUs using the 9180 configuration menu. Refer to your 9180 user's manual.*

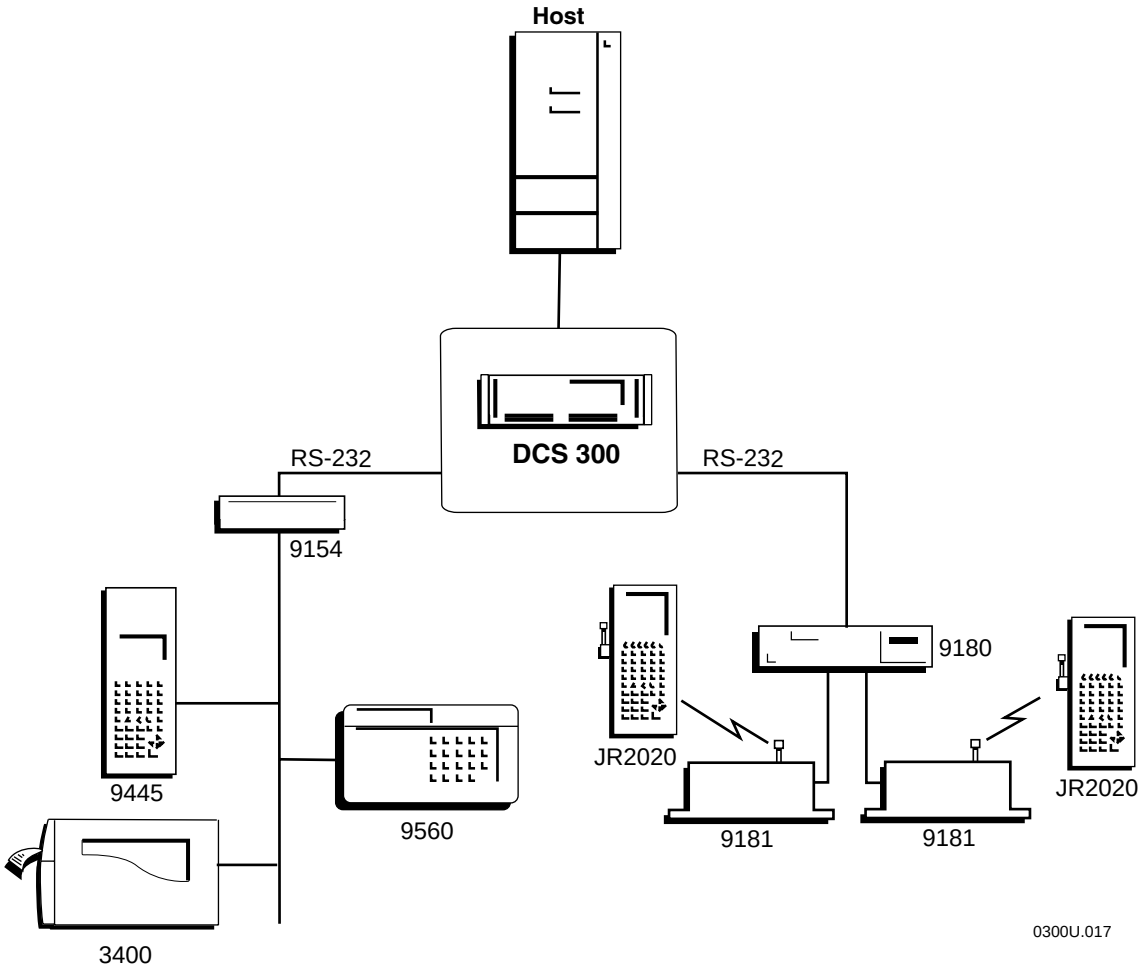
If you already understand these sections and have already performed these tasks, connect the DCS 300 to your Intermec RF network or host environment as described in these chapters:

- Chapter 6, "Connecting to the Intermec RF Network"
- Chapter 8, "Using Terminal Emulation"
- Chapter 9, "Using Peer-to-Peer Applications"
- Chapter 10, "Using Terminal Sessions"

Configuring an Intermec Controller

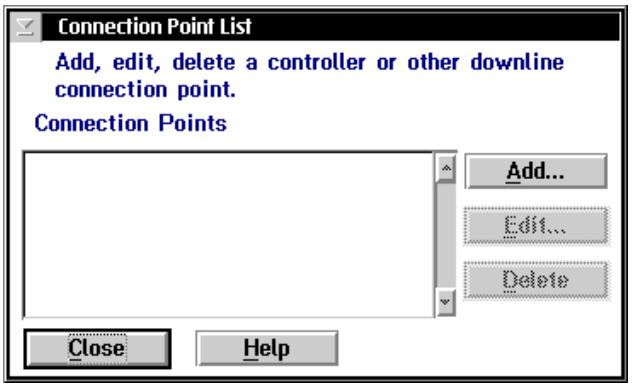
An Intermec controller is a 9180 Network Controller, 9161 Port Concentrator, or a 9154 Multi-Drop Line Controller that is connected to the DCS 300 through a serial port. The following illustration is an example of a DCS 300 connected to a 9180 and a CrossBar network.

Example: The DCS 300 Connected to a 9180 and CrossBar Network

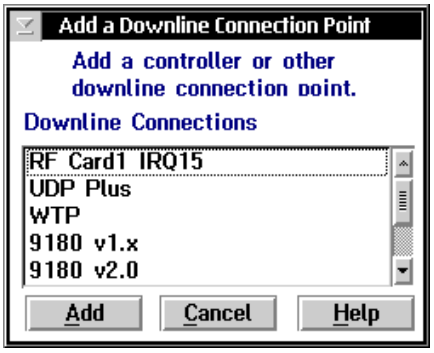


To configure the server to work with an Intermec controller

1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Downline Network. Two buttons, Connection Points and Downline Devices, appear.
3. Choose Connection Points. The Connection Point List dialog box appears.



4. Choose Add, Edit, or Delete. If you choose Add, the Add a Downline Connection Point dialog box appears.



5. Choose the controller that you want to add and then choose Add. The setup dialog box for the controller appears.
6. Configure the controller. For help, see “About the Controller Parameters” in the next section and then see the appropriate section for your controller.
7. Set any time parameters for the controller. For help, see “Setting the Time Parameters” later in this chapter.

8. (9180 v2.0 only) Define a default host for each type of host that the 9180 devices will communicate with through the 9180 controller. For help, see "Defining Default Hosts" later in this chapter.
9. Choose OK to save your changes and return to the Connection Point List dialog box. Choose Close to return to the main menu.

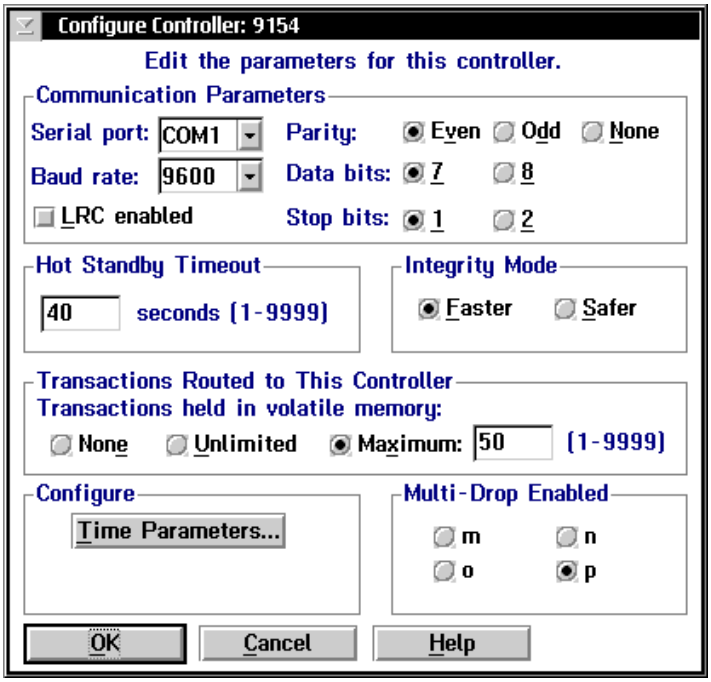
About the Controller Parameters

When you configure an Intermec controller, you may need to configure the communication parameters, set the hot standby timeout, define the integrity mode, set time parameters, and enable the correct Multi-Drop port. You must make sure that any communication parameters that you define for the serial port on the server are the same as the parameters set for the serial port on the Intermec controller.

Time Parameters These optional parameters let you set time broadcast and time append parameters for the Intermec controller. These time parameters synchronize the Intermec controllers with their devices. In the System Parameters dialog box, you can set a time synchronization parameter that synchronizes the time on the server with its Intermec controllers. For more help, see "Setting the Time Parameters" later in this chapter.

Adding a 9154 Controller

- From the Add a Downline Connection Point dialog box, choose 9154 and then choose Add. The Configure Controller: 9154 dialog box appears.

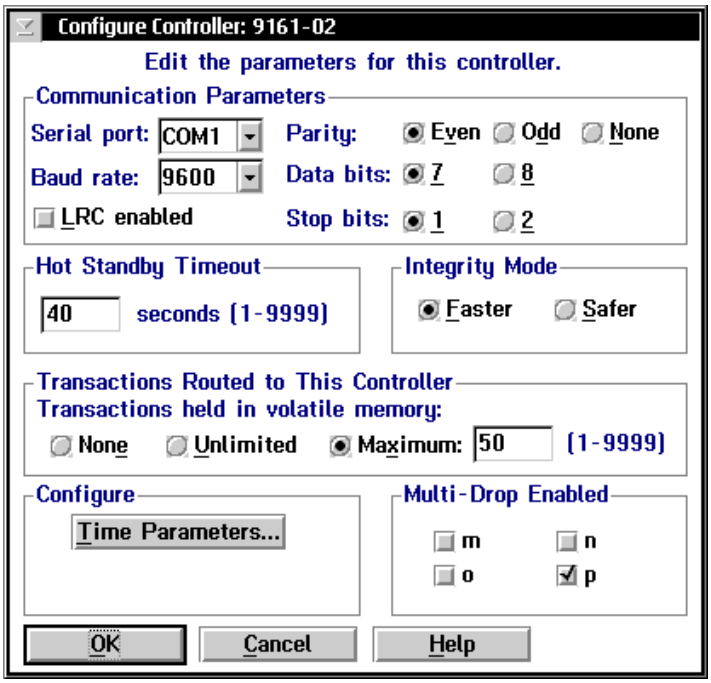


Field	Description	Value	Default
Serial port	The communications port to which the 9154 controller is connected.	COM1, COM2	COM1
Baud rate	The baud rate at which the serial port communicates.	Predefined	9600
LRC enabled	This check box determines if the longitudinal redundancy check character is appended to data transmitted by a device.	Check, Clear	Clear
Parity	The type of self-checking you want to use when sending data.	Even, Odd, None	Even
Data bits	The number of bits to use for setting communications protocol.	7, 8	7
Stop bits	The number of bits to use for setting communications protocol.	1, 2	1
Hot Standby Timeout	The number of seconds the server waits after delivering a transaction to the 9154 controller to receive an acknowledgment for the transaction. If it does not receive an acknowledgment, the server writes all transactions for the 9154 to a Hot Standby file. The 9154 receives its transactions from this file either when it sends an acknowledgment to the most recently delivered transaction or when it sends a system transaction. Before the 9154 becomes interactive again, it receives all the transactions, from oldest to newest, that are in its Hot Standby file.	1 to 9999	40
Integrity mode	This mode determines the amount of transaction verification that the server performs. In Faster mode, the server acknowledges the transaction as soon as it receives the transaction from 9154 controller. In Safer mode, the server acknowledges the transaction only after it is stored in a Hot Standby file. Transaction throughput is slower because the server cannot accept another transaction from the 9154 until it verifies the previous one.	Faster, Safer	Faster

Field	Description	Value	Default
Transactions held in volatile memory	The number of transactions the server keeps in volatile RAM before it begins to write them to a Hot Standby file. Choose None if you want the transaction always written to the file. Choose Unlimited if you do not want the transaction written to the file unless the time you set for the Hot Standby timeout expires. Choose Maximum and enter a maximum number of transactions. When the server has this number of transactions in RAM, it writes them to a file.	None, Unlimited, Maximum	Maximum 50
Multi-Drop Enabled	The Multi-Drop line that the 9154 controller uses.	m, n, o, p	p

Adding a 9161 Controller

- From the Add a Downline Connection Point dialog box, choose 9161-01 or 9161-02 and then choose Add. The Configure Controller: 9161 dialog box appears.

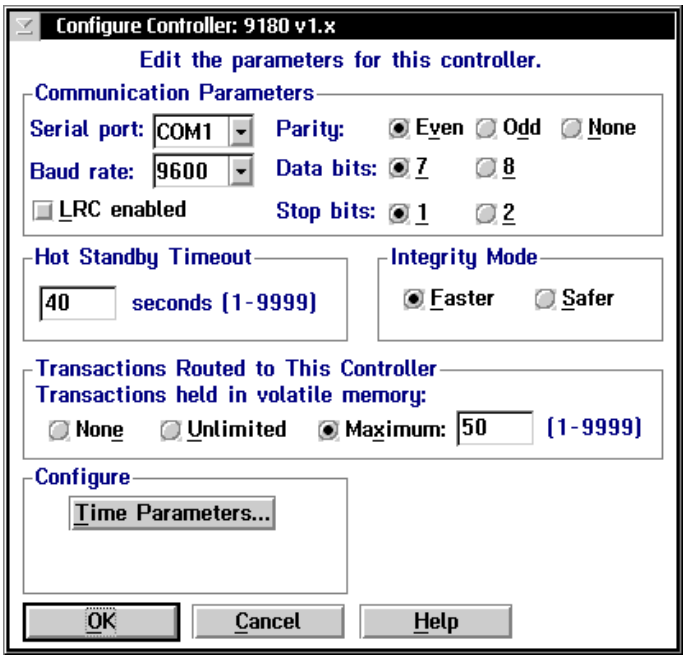


Field	Description	Value	Default
Serial port	The communications port to which the 9161 controller is connected.	COM1, COM2	COM1
Baud rate	The baud rate at which the serial port communicates.	Predefined	9600
LRC enabled	This check box determines if the longitudinal redundancy check character is appended to data transmitted by a device.	Check, Clear	Clear
Parity	The type of self-checking to use when sending data.	Even, Odd, None	Even
Data bits	The number of bits to use for setting communications protocol.	7, 8	7
Stop bits	The number of bits to use for setting communications protocol.	1, 2	1

Field	Description	Value	Default
Hot Standby Timeout	The number of seconds the server waits after delivering a transaction to the 9161 controller to receive an acknowledgment for the transaction. If it does not receive an acknowledgment, the server writes all transactions for the 9161 to a Hot Standby file. The 9161 receives its transactions from this file either when it sends an acknowledgment to the most recently delivered transaction or when it sends a system transaction. Before the 9161 becomes interactive again, it receives all the transactions, from oldest to newest, that are in its Hot Standby file.	1 to 9999	40
Integrity mode	This mode determines the amount of transaction verification the server performs. In Faster mode, the server acknowledges the transaction as soon as it receives the transaction from 9161 controller. In Safer mode, the server acknowledges the transaction only after it is stored in a Hot Standby file. Transaction throughput is slower because the server cannot accept another transaction from the 9161 until it verifies the previous one.	Faster, Safer	Faster
Transactions held in volatile memory	The number of transactions the server keeps in volatile RAM before it begins to write them to a Hot Standby file. Choose None if you want the transaction always written to the file. Choose Unlimited if you do not want the transaction written to the file unless the time you set for the Hot Standby timeout expires. Choose Maximum and enter a maximum number of transactions. When the server has this number of transactions in RAM, it writes them to a file.	None, Unlimited, Maximum	Maximum 50
Multi-Drop Enabled	The Multi-Drop lines (up to four) that the 9161-02 controller supports. The 9161-01 controller does not support this feature.	m, n, o, p	p

Adding a 9180 v1.x Controller

- From the Add a Downline Connection Point dialog box, choose 9180 v1.x and then choose Add. The Configure Controller: 9180 v1.x dialog box appears.

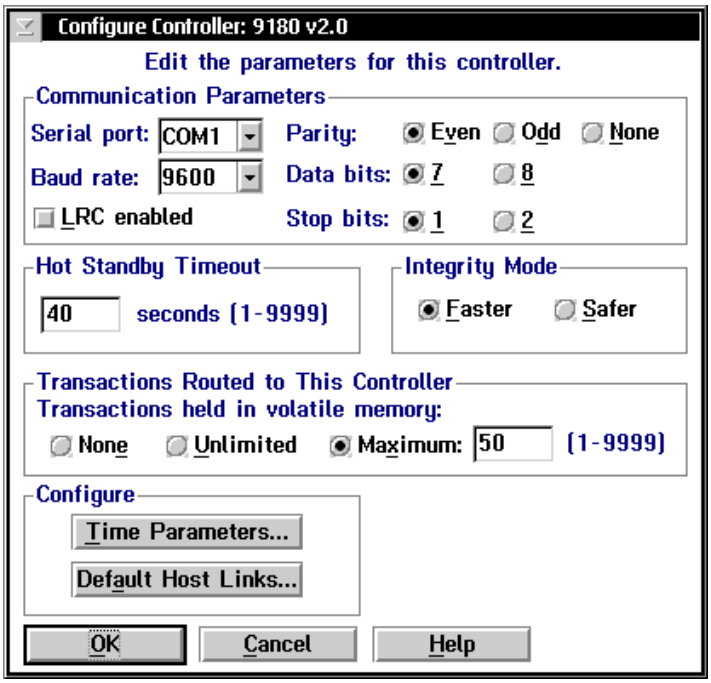


Field	Description	Value	Default
Serial port	The communications port to which the 9180 controller is connected.	COM1, COM2	COM1
Baud rate	The baud rate at which the serial port communicates.	Predefined	9600
LRC enabled	This check box determines if the longitudinal redundancy check character is appended to data transmitted by a device.	Check, Clear	Clear
Parity	The type of self-checking you want to use when sending data.	Even, Odd, None	Even
Data bits	The number of bits to use for setting communications protocol.	7, 8	7
Stop bits	The number of bits to use for setting communications protocol.	1, 2	1

Field	Description	Value	Default
Hot Standby Timeout	The number of seconds the server waits after delivering a transaction to the 9180 controller to receive an acknowledgment for the transaction. If it does not receive an acknowledgment, the server writes all transactions for the 9180 to a Hot Standby file. The 9180 receives its transactions from this file either when it sends an acknowledgment to the most recently delivered transaction or when it sends a system transaction. Before the 9180 becomes interactive again, it receives all the transactions, from oldest to newest, that are in its Hot Standby file.	1 to 9999	40
Integrity mode	This mode determines the amount of transaction verification the server performs. In Faster mode, the server acknowledges the transaction as soon as it receives the transaction from 9180 controller. In Safer mode, the server acknowledges the transaction only after it is stored in a Hot Standby file. Transaction throughput is slower because the server cannot accept another transaction from the 9180 until it verifies the previous one.	Faster, Safer	Faster
Transactions held in volatile memory	The number of transactions the server keeps in volatile RAM before it begins to write them to a Hot Standby file. Choose None if you want the transaction always written to the file. Choose Unlimited if you do not want the transaction written to the file unless the time you set for the Hot Standby timeout expires. Choose Maximum and enter a maximum number of transactions. When the server has this number of transactions in RAM, it writes them to a file.	None, Unlimited, Maximum	Maximum 50

Adding a 9180 v2.0 Controller

- From the Add a Downline Connection Point dialog box, choose 9180 v2.0 and then choose Add. The Configure Controller: 9180 v2.0 dialog box appears.



Field	Description	Value	Default
Serial port	The communications port to which the 9180 controller is connected.	COM1, COM2	COM1
Baud rate	The baud rate at which the serial port communicates.	Predefined	9600
LRC enabled	This check box determines if the longitudinal redundancy check character is appended to data transmitted by a device.	Check, Clear	Clear
Parity	The type of self-checking you want to use when sending data.	Even, Odd, None	Even
Data bits	The number of bits to use for setting communications protocol.	7, 8	7
Stop bits	The number of bits to use for setting communications protocol.	1, 2	1

Field	Description	Value	Default
Hot Standby Timeout	The number of seconds the server waits after delivering a transaction to the 9180 controller to receive an acknowledgment for the transaction. If it does not receive an acknowledgment, the server writes all transactions for the 9180 to a Hot Standby file. The 9180 receives its transactions from this file either when it sends an acknowledgment to the most recently delivered transaction or when it sends a system transaction. Before the 9180 becomes interactive again, it receives all the transactions, from oldest to newest, that are in its Hot Standby file.	1 to 9999	40
Integrity mode	This mode determines the amount of transaction verification the server performs. In Faster mode, the server acknowledges the transaction as soon as it receives the transaction from 9180 controller. In Safer mode, the server acknowledges the transaction only after it is stored in a Hot Standby file. Transaction throughput is slower because the server cannot accept another transaction from the 9180 until it verifies the previous one.	Faster, Safer	Faster
Transactions held in volatile memory	The number of transactions the server keeps in volatile RAM before it begins to write them to a Hot Standby file. Choose None if you want the transaction always written to the file. Choose Unlimited if you do not want the transaction written to the file unless the time you set for the Hot Standby timeout expires. Choose Maximum and enter a maximum number of transactions. When the server has this number of transactions in RAM, it writes them to a file.	None, Unlimited, Maximum	Maximum 50

Setting the Time Parameters

Use this dialog box to configure the time broadcast and time append parameters. If the Intermec controller does not support one of the parameters, it is grayed out.

Broadcast Parameters These optional parameters broadcast a time, with a short string, at certain intervals from the Intermec controller to all devices connected to it. These parameters synchronize the devices with the controller.

Note: *Using 0 to disable time broadcast is not supported on the 9180 controller.*

Append Parameters These optional parameters configure the Intermec controllers to stamp the time at certain intervals to incoming data. The timestamp is in the format:

```
HH:MM:SS
```

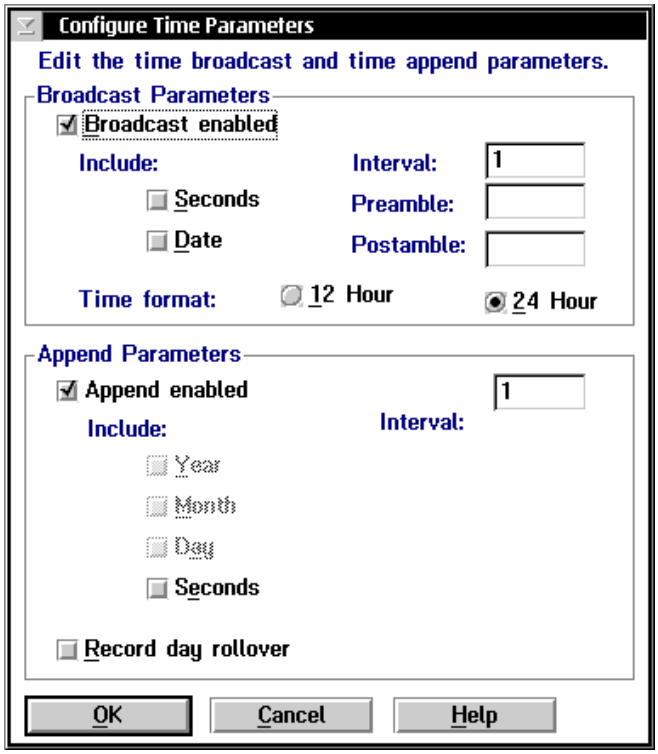
If you want all messages to have a timestamp with the hour and minute, enable this feature and set the interval to 0. Depending on your controller, you can also append the seconds. If no data is available within the interval, the controller waits until it receives data and then appends the time before sending it to the host. This feature will not operate when running terminal emulation or using the direct TCP/IP socket interface.

Note: *Do not enable time append on both the Intermec controller and the device itself. If it is enabled on both, two timestamps are appended to incoming data.*

Note: *If you are configuring a 9161 controller, you need to set the internal DIP switches to enable the time append feature. You can use this dialog box to set the interval of the time append.*

To set the time parameters

- From any Configure Controller dialog box, choose Time Parameters. The Configure Time Parameters dialog box appears.



Field	Description	Value	Default
Broadcast enabled	This check box determines if the Intermec controller broadcasts time to its devices.	Check, Clear	Clear
Include Seconds (9180 only)	This check box adds seconds to the time.	Check, Clear	Clear
Include Date (9154/9180 only)	This check box adds the date to the time.	Check, Clear	Clear
Interval	This field specifies how often the controller broadcasts the time. If you set this field to 0, no time broadcast is made.	0 to 99 minutes	1
Preamble (9154/9180 only)	This field lets you add a short message to the beginning of the time.	1 to 5 alphanumeric characters	None
Postamble (9154/9180 only)	This field lets you add a short message to the end of the time.	1 to 5 alphanumeric characters	None
Time format (9154/9180 only)	These option buttons choose the time broadcast format.	12 hour, 24 hour	12 hour
Append enabled	This check box determines if a timestamp is added to messages from devices. ***Note:*** *Intermec recommends that you use the time append feature. If you do not, you may see a "protocol error occurred" message in the error log.*	Check, Clear	Clear
Include Seconds (9180 only)	This check box adds a 2-digit seconds to the time.	Check, Clear	Clear
Record day rollover (9154/9180 only)	This check box adds a timestamp in the buffer of the host at midnight.	Check, Clear	Clear
Interval	This field specifies how often in minutes the controller appends the timestamp. If you set this field to 0, every message from a device will have a timestamp.	0 to 99	1

Defining Default Hosts (9180 v2.0)

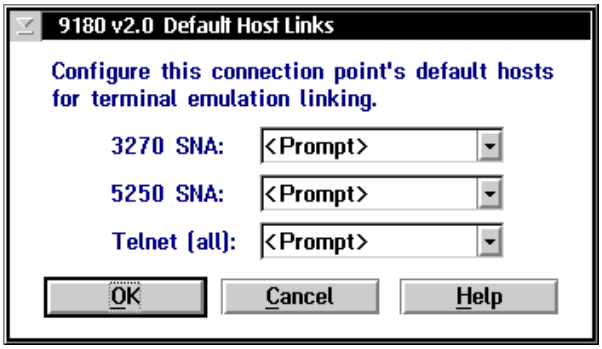
You can configure a default host for each of the types of hosts the 9180 devices will communicate with through the 9180 v2.0 controller. You can configure the devices to

- explicitly link with a specific host. Click the down arrow on the right side of the field and choose a host that you have configured.
- prompt the user to enter a host name. Click the down arrow on the right side of the field and choose <Prompt>.
- not communicate with a host. Click the down arrow on the right side of the field and choose <none>.

To configure a specific device to communicate in a different way to a host, see "Configuring TE Links" in Chapter 8.

To configure your link

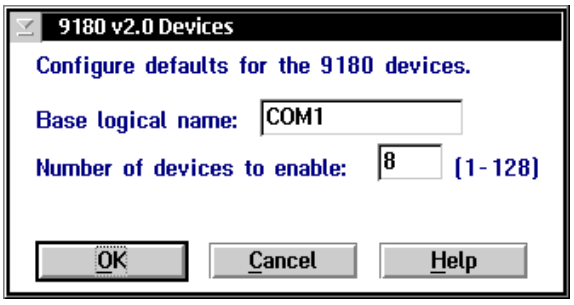
- From the Configure Controller: 9180 v2.0 dialog box, choose Default Host Links. The 9180 v2.0 Default Host Links dialog box appears.



Field	Description	Value	Default
3270 SNA	The method that the RF card devices will use to get a host name when they communicate with 3270 SNA hosts.	None, Prompt, pre-defined list	Prompt
5250 SNA	The method that the RF card devices will use to get a host name when they communicate with 5250 SNA hosts.	None, Prompt, pre-defined list	Prompt
Telnet (all)	The method that the RF card devices will use to get a host name when they communicate with Telnet hosts.	None, Prompt, pre-defined list	Prompt

Defining the 9180 v2.0 Devices

When you choose OK in the Configure Controller: 9180 v2.0 dialog box, this dialog box appears.



Field	Description	Value	Default
Base logical name	The base name that the server uses to create a unique logical name for each device. The server appends a sequential 3-digit number to this name for each device.	1 to 13 alphanumeric characters	COM1
Number of terminals to enable	The number of logical names that you want the server to generate.	1 to 128	8

Identifying the CrossBar Devices

The DCS 300 needs to know the addresses of all the devices that use it to communicate with the host. This section explains how to configure the server for the CrossBar devices.

The device list is automatically populated with device addresses as you configure the Intermec controllers. The first eight addresses are enabled and are configured as J2020s. You need to change the device type for these addresses and enable the addresses of the other devices that you want to communicate with the host. You can also edit the individual parameters for each address.

Note: *Do not enable devices that you are not using. If you try to send data to a nonexistent but enabled device, your system performance will degrade.*

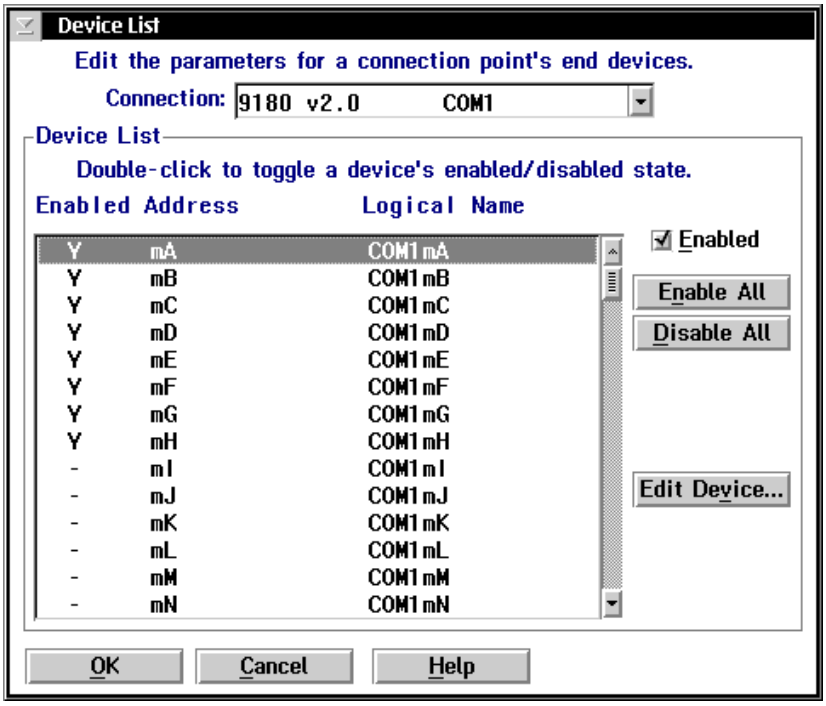
Your server has a terminal license that allows it to communicate with a limited number of device addresses (1-8, 1-24, 1-64, 1-128). The server does not keep track of the number of devices you enable. You can enable all 128 devices. As each device sends messages to the server, the server logs its address. When the server logs the maximum number of addresses that your terminal license allows, it will not accept messages from any new addresses.

If you need to upgrade your terminal license, contact your local Intermec representative.

To identify CrossBar devices

1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Downline Network. Two buttons, Connection Points and Downline Devices, appear.
3. Choose Downline Devices. The Device List dialog box appears.
4. In the Connection field, click the down arrow on the right side of the field. A list of the controllers that are configured appears.

Device List Dialog Box



5. Select the controller whose downline devices you want to configure. The Device List displays the status, address, and logical name of all 128 devices.
6. To enable all 128 devices, choose Enable All.

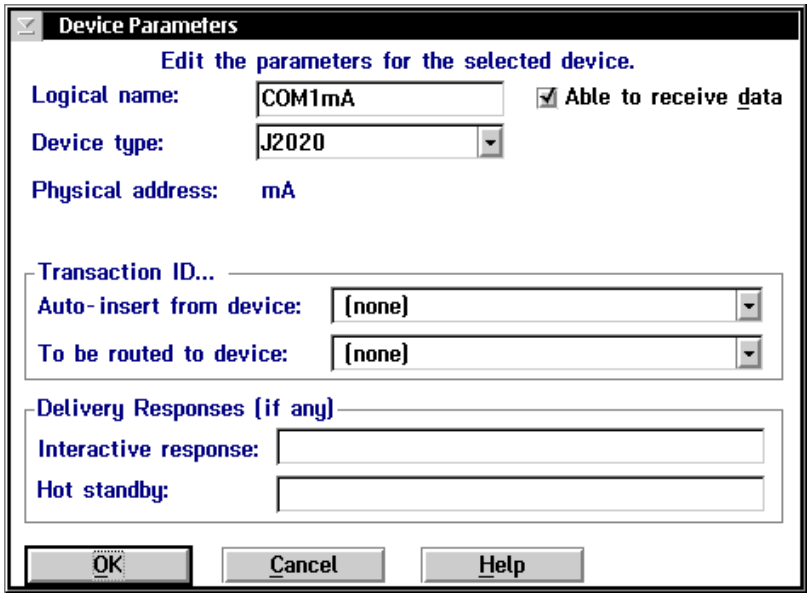
   Or, to enable specific devices, select the device you want to enable and make sure there is a check in the Enabled check box.
7. To disable all 128 devices, choose Disable All.

   Or, to disable specific devices, select the device you want to disable and make sure there is no check in the Enabled check box.
8. Select a device whose individual parameters you want to edit and then choose Edit Device. For help, see “Editing a CrossBar Device” in the next section.
9. Choose OK to save your changes and return to the main menu.

Editing a CrossBar Device

- From the Device List dialog box, choose Edit Device. The Device Parameters dialog box appears.

  Note: *If you are using VT or ANSI terminal emulation, do not configure transaction IDs or delivery responses.*



Field	Description	Value	Default
Logical name	The logical name of this device.	1 to 16 alphanumeric characters	Intermec standard
Able to receive data	This check box determines if this device can receive data from the network.	Check, Clear	If the device has a screen, it is checked, else it is cleared.
Device type	This list box contains all the current Intermec devices supported by the server.	Predefined	J2020
Physical address	This read-only field displays the physical address of the device.	Read-only	Predefined

Field	Description	Value	Default
Auto-insert from device	This field adds a transaction ID to devices that cannot put a transaction ID in the transactions they send. ***Note:*** *All transactions from this terminal will be routed using this transaction ID.*	Predefined list	None
To be routed to device	This field contains the transaction ID that will always be routed to this device.	Predefined list	None
Interactive response (Optional)	The message that is sent to the source of the transaction if the transaction for this device is delivered successfully in Interactive mode.	1 to 39 characters	None
Hot standby (Optional)	The message that is sent to the source of the transaction if the transaction for this device is not delivered.	1 to 40 characters	None

Saving Your Run-Time Configuration

When you finish configuring your downline network, you should save your changes.

To save your run-time configuration

- From the main menu sidebar buttons, choose Save Configuration.

8

Using Terminal Emulation

Now that you have configured the DCS 300 to communicate with your LAN and you have configured it to communicate with your Intermec RF network, you are ready to tie the entire data collection network together using a terminal emulation application.

This chapter describes how to configure your server for using VT, ANSI, 5250, and 3270 terminal emulation (TE) with your JANUS devices, TRAKKER Antares terminals, and WTP devices.

Chapter Checklist

Done?	Task	Page
❑	Understand how TE runs on the host, server, and devices.	8-4
❑	For VT, ANSI, TN5250, or TN3270 TE, identify all the Telnet hosts on the network.	8-7
❑	For 5250 TE, identify all the IBM SNA hosts on the network.	8-10
❑	For 3270 TE, identify all the IBM SNA hosts on the network.	8-18
❑	Configure any TE links.	8-23
❑	Save and activate the configuration.	8-25
❑	Configure your JANUS devices for TE.	8-26
❑	To run VT and ANSI TE on your JANUS devices, download the TE files.	8-26
❑	Configure your TRAKKER Antares terminals for TE.	8-31
❑	Configure your WTP devices for TE.	8-34
❑	Set security for accessing the TE Configuration menu.	8-35

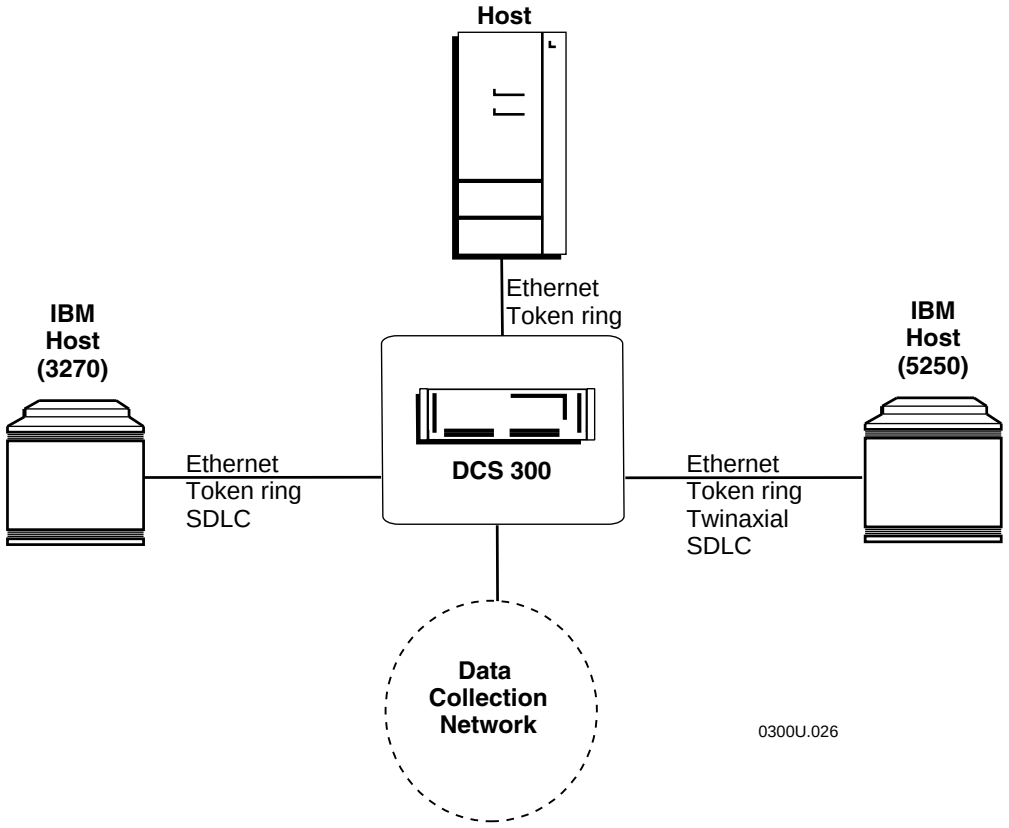
Note: *If your JANUS 2.4 GHz RF devices or your TRAKKER Antares terminals are running TCP/IP, you do not need a DCS 300 to run VT or ANSI TE, TN5250, or TN3270.*

Note: *You can also use the DCS 300 as an IP bridge to send transactions to a TCP/IP host on your token ring network.*

When you understand these sections and perform these tasks, you can start using the server.

About Terminal Emulation

Terminal emulation (TE) allows devices to communicate through the DCS 300 as if they were directly connected to the host. The server sends data to the device in a screen format that emulates the host session. Vehicle-mount computers and vehicle-mount terminals automatically see the entire screen. Other readers and terminals have viewporting abilities; that is, you can use commands to move the smaller device screen around to see a much larger terminal screen.



The next table provides a summary of what TE applications you can run on which networks.

Host Connectivity Table

	Ethernet	Token Ring	Coaxial	Twinaxial	SDLC
VT and ANSI	Yes	Yes	No	No	No
5250	Yes	Yes	No	Yes	Yes
3270	Yes	Yes	No	No	Yes
TN5250	Yes	Yes	No	No	No
TN3270	Yes	Yes	No	No	No

Using the server, you can run VT/ANSI TE on JANUS UDP Plus devices, TRAKKER Antares terminals, and WTP devices. The UNIX or other TCP/IP host must support Telnet.

Note: *WTP devices do not run VT100, VT320, or ANSI TE.*

You can also run TN5250 or TN3270 on JANUS UDP Plus devices, TRAKKER Antares terminals, and WTP devices. Your IBM host must support Telnet. When you send data from the device, the server routes it to the Telnet session on the host. You can also run IBM SNA 5250 TE or IBM SNA 3270 TE on JANUS UDP Plus devices, TRAKKER Antares terminals, and WTP devices that are communicating with an IBM AS/400 or other IBM SNA host.

Your server is licensed to communicate with a fixed number of devices (1-8, 1-24, 1-64, 1-254). When a device first sends a message through the server, the server logs its logical name. When the server logs the maximum number of logical names that your device license allows, it will not accept messages from any new addresses. If you need to purchase an upgrade to your terminal license, contact your local Intermec representative.

JANUS TE Applications

For JANUS devices that run VT or ANSI TE, the server provides the JANUS TE application.

For JANUS 900 MHz RF devices (1MB) that run 5250 or 3270 TE, your devices are preloaded with a JANUS TE application. However, this application is also loaded on the server, if you need to download it to your device. Your device must be running firmware v3.01 or later.

Note: *If you are replacing a 9185 controller with a DCS 300, you must download the new JANUS TE application to all your JANUS devices.*

TRAKKER Antares TE Applications

TRAKKER Antares terminals can run VT, ANSI, 5250, or 3270 TE. Your devices are preloaded with the TRAKKER Antares TE application. However, this application is also loaded on the server, if you need to download it to your device. For help, see "Using the DCS 300 to Transfer Files" in Appendix B.

WTP TE Applications

WTP devices can run VT, 5250, or 3270 TE. Your devices are preloaded with the TE application.

Note: *WTP devices must be running TE client v5.33 or higher to communicate with the DCS 300.*

Configuring Telnet Hosts

When you set up your data collection network to run Telnet TE, you need to configure the DCS 300 and the devices. Telnet TE includes VT100, VT220, VT320, ANSI, TN5250, and TN3270.

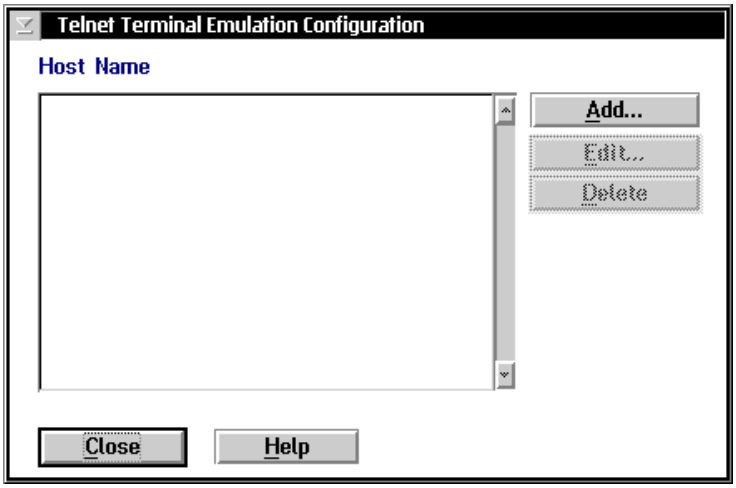
Note: *For VT, ANSI, TN5250, and TN3270 TE, your network administrator does not need to configure anything on the host.*

To run Telnet TE between JANUS devices, TRAKKER Antares terminals, and WTP devices and the host, you need to identify all the TCP/IP hosts and use DNS or manually enter their IP addresses. Before you proceed, make sure you have performed these tasks:

- Installed the DCS 300.
- Configured the network adapter cards.
- Installed and configured the connection points.

To configure a Telnet host

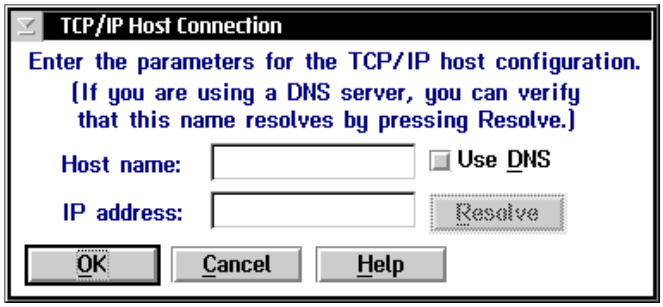
1. From the main menu, choose Terminal Emulation.
2. Choose Telnet Host. The Telnet Terminal Emulation Configuration dialog box appears.



3. Choose Add, Edit, or Delete. If you choose Add, the TCP/IP Host Connection dialog box appears.

   Note: *You cannot delete a host if it is linked to a device or a terminal session.*

TCP/IP Host Connection Dialog Box



Field	Description	Value	Default
Host name	The name that logically identifies the TCP/IP host to the network.	1 to 256 alphanumeric characters	None
Use DNS	This check box determines if you use a DNS server to resolve the IP address of this host. ***Note:*** *Before you check this check box, you must first configure a DNS server in the DNS Configuration dialog box.*	Check, Clear	Clear
IP address	The address that identifies the TCP/IP host to the network. This IP address must be a valid IP v4 address.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	None

To determine the host IP address using DNS

1. In the Host name field, enter the abbreviated or long host name. If you enter the abbreviated name, the server searches the domain names in the DNS Configuration dialog box to determine the long host name.
2. Check the Use DNS check box.
3. (Optional) Choose Resolve. The server searches the name server addresses in the DNS Configuration dialog box for the long host name and resolves the IP address.
4. Choose OK to save your changes and return to the Telnet Terminal Emulation Configuration dialog box.

To configure the host IP address manually

1. In the Host name field, enter the host name.
2. Make sure the Use DNS check box is cleared.
3. In the IP address field, enter the host IP address.
4. Choose OK to save your changes and return to the Telnet Terminal Emulation Configuration dialog box.

Configuring 5250 SNA Hosts

When you set up your data collection network to run 5250 SNA TE, you must configure the host, the DCS 300, and the devices.

Note: *To set up TN5250 terminal emulation, see "Configuring Telnet Hosts" earlier in this chapter.*

Configuring the Host

For 5250 TE, your network administrator needs to define the DCS 300 on the host unless you have auto-create controller turned on.

Configuring the DCS 300

To run 5250 TE between JANUS devices, TRAKKER Antares terminals, and WTP devices and the host, you must identify all the IBM SNA hosts. Before you proceed, make sure you have performed these tasks:

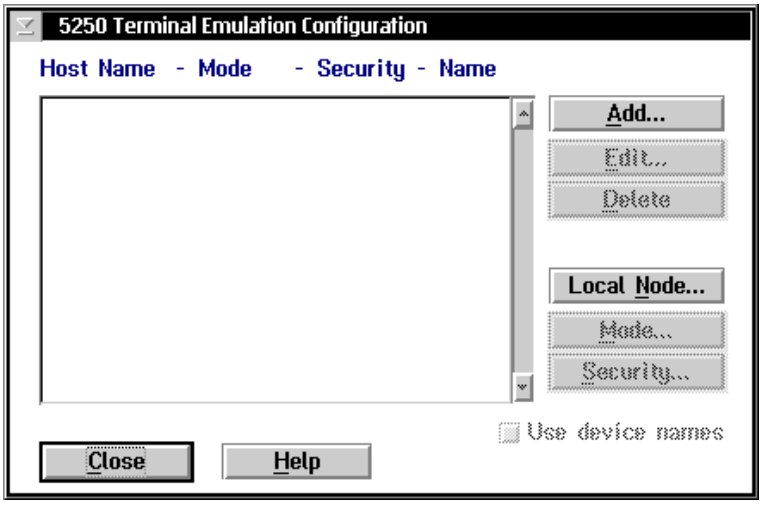
- Installed the DCS 300.
- Configured the network adapter cards.
- Installed and configured the connection points.

Use device names This check box determines if the selected host in the Host Name list box uses the device name when establishing terminal sessions. The device names are the logical names that you assigned when you identified these devices with the terminal session number (1 or 2) appended to the name. For help, see "Defining the RF Network," "Setting Up the UDP Plus Devices," and "Setting Up the WTP Devices" in Chapter 6.

To configure the DCS 300

1. From the main menu, choose Terminal Emulation.
2. Choose 5250 SNA Host. The 5250 Terminal Emulation Configuration dialog box appears.

5250 Terminal Emulation Configuration Dialog Box



3. Choose Add, Edit, or Delete. If you choose Add, the Host Connection Configuration dialog box appears. For help, see "Adding an IBM SNA Host" in the next section.

   Note: *You cannot delete a host if it is linked to a device or a terminal session.*

4. Choose Local Node to configure the SNA local node. For help, see "Configuring the SNA Local Node" later in this chapter.
5. Choose Mode to configure the IBM mode. For help, see "Selecting an IBM Mode" later in this chapter.
6. Configure the security. For help, see "Setting a User ID and Password" later in this chapter.
7. Check or clear the Use device names check box.

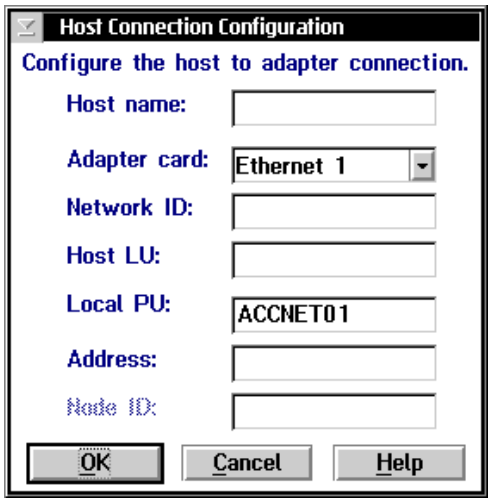
   Note: *You must configure all the devices that communicate with the AS/400 host as virtual devices of the type 3197.*

Adding an IBM SNA Host

You must identify any hosts you want the DCS 300 to communicate with for the terminal sessions. When you add a host, you set up a link to a specific host and this information is available throughout the system. Once you create a host connection, you may use it for any SNA configurations. Only one host connection is allowed for twinaxial and SDLC network adapter cards. The server maintains separate lists for 3270 hosts and 5250 hosts. If you create a host when defining a 5250 terminal session, you cannot use this host for a 3270 terminal session.

To add an IBM SNA host

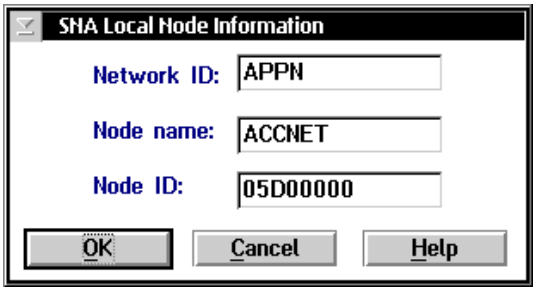
- From the 5250 Terminal Emulation Configuration dialog box, choose Add. The Host Connection Configuration dialog box appears.



Field	Description	Value	Default
Host name	A unique name for the SNA host. Use this internal name to make the host LU name easier to identify.	1 to 8 alphanumeric characters	None
Adapter card	The network adapter card you are using to connect to the host.	Ethernet, token ring, twinaxial, SDLC	Ethernet 1
Network ID	Identifies the network ID on which the host resides. This ID must match the network ID configured on the host.	1 to 8 alphanumeric characters	DCS 300 network ID from the local SNA node definition
Host LU	The LU name that identifies the host. This parameter must match the control point (CP) name or node name of the host.	1 to 8 alphanumeric and special characters	Host name
Local PU (Ethernet or token ring only)	A unique PU name for the host that allows the terminals to communicate with more than one host using the same upline adapter card. For each host configuration for the upline adapter card, you assign a unique host name and a unique local PU. Since you are using the same adapter card, all other fields in this dialog box are the same. To connect to different hosts, change the host name on your terminal.	8 uppercase alphanumeric or special characters The first character must be an alpha character.	SNA node name + 2-digit suffix, starting with 01
Address (Ethernet or token ring only)	The LAN adapter address of the host. For help, see “Converting Ethernet Addresses to Token Ring MAC Format” in Appendix B.	Token ring MAC address format	None

Configuring the SNA Local Node

- From the 5250 Terminal Emulation Configuration dialog box, choose Local Node. The SNA Local Node Information dialog box appears.



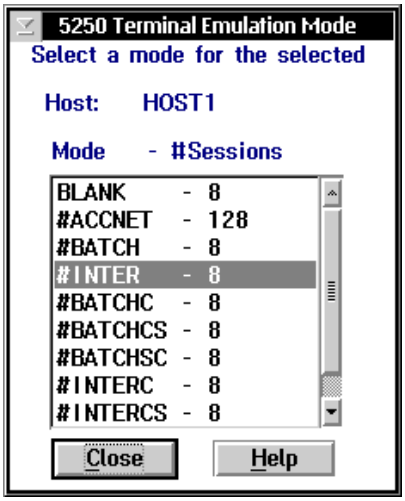
Field	Description	Value	Default
Network ID	The unique name of the SNA network. This ID is used for problem notification.	1 to 8 alphanumeric characters	APPN
Node name	The name that other nodes use to address the server. This name is also the default LU and must be unique to the SNA network.	1 to 8 alphanumeric and special characters	ACCNET
Node ID	Specifies the last eight characters in the XID used for establishing a host connection. On the host this value is IDBLK+IDNUM. When establishing a connection, the host or server with the higher Node ID number is the primary workstation.	8 hexadecimal characters	05D00000

Selecting an IBM Mode

The IBM mode defines the terminal session characteristics between the DCS 300 and the SNA host. The default mode, #INTER, allows only eight sessions. If you need more than eight sessions, select a new IBM mode. Use the #ACCNET mode for systems that need a larger session limit (up to 128). This mode, unlike the other ones in the predefined list, is not a default mode and your network administrator will have to create it on the host. For help on defining #ACCNET on the host, see the *DCS 300 Technical Reference Manual*.

To select an IBM mode

1. From the 5250 Terminal Emulation Configuration dialog box, select the host whose mode you want to set.
2. Choose Mode. The 5250 Terminal Emulation Mode dialog box appears.



3. In the list box, select the mode that you want to use.
4. Choose Close to close the dialog box and return to the 5250 Terminal Emulation Configuration dialog box.

Setting and Removing the User ID and Password

Your host may implement security at the session level. This type of security requires the server to log in before it can communicate with the host. Setting a user ID and password in this procedure will not automatically log the user into the host.

To set a user ID and password

1. From the 5250 Terminal Emulation Configuration dialog box, select the host whose security you want to set.
2. Choose Security. The 5250 Terminal Emulation Security dialog box appears.

Field	Description	Value	Default
Host user ID	The user ID that lets the server access the host.	1 to 10 alphanumeric characters.	None
Password	The password that goes with the user ID.	1 to 10 alphanumeric characters	None

To remove a user ID and password

1. From the 5250 Terminal Emulation Configuration dialog box, select the host that has a user ID and password that you want to remove.
2. Choose Security. The 5250 Terminal Emulation Security dialog box appears.
3. Choose Remove. The host user ID and password are removed. You return to the 5250 Terminal Emulation Configuration dialog box.

Performing a Double Pass-Through on an IBM AS/400 Host

Note: *To use this feature with 5250 TE, your AS/400 must be v2.3 or higher.*

When using 5250 TE, you may want to perform a double pass-through to log into a remote IBM AS/400 host. A double pass-through lets you log into one AS/400 and then access another AS/400 through the first one.

To perform a double pass-through

1. On your terminal, log into the AS/400 that you want to use for the pass-through.
2. At the command line on your terminal, type:

   `strpasthr` *`hostname`*

   where *hostname* is the name of the AS/400 you want to access. This host does not need to be defined on the server.

You are connected to the remote AS/400 through the original AS/400 you logged into.

To exit the remote IBM AS/400 host

- At the command line on your terminal, type:

  `endpasthr`

You are connected to the original AS/400.

Configuring 3270 SNA Hosts

When you set up your data collection network to run 3270 SNA TE, you must configure the host, the DCS 300, and devices.

Note: *To set up TN3270 terminal emulation, see "Setting Up Telnet Hosts" earlier in this chapter.*

Configuring the Host

For 3270 TE, your network administrator needs to set up the host to see the DCS 300 as an IBM model 3174 terminal controller. Your network administrator also must provide all the NAUs (host field: LOCADDR) that are set up on the host for the devices to use.

SDLC connections can be direct or through a modem. If you are connecting to the host using SDLC, you also need to know these parameters:

- the non-switched or switched SDLC station address (host field: ADDR)
- the node ID (host field: IDBLK+IDNUM)

Configuring the DCS 300

To run 3270 TE between JANUS devices, TRAKKER Antares terminals, WTP devices, and the host, you must identify all the IBM SNA hosts. You also must configure the SNA local node and NAUs. There are three ways to set up NAUs for the terminals.

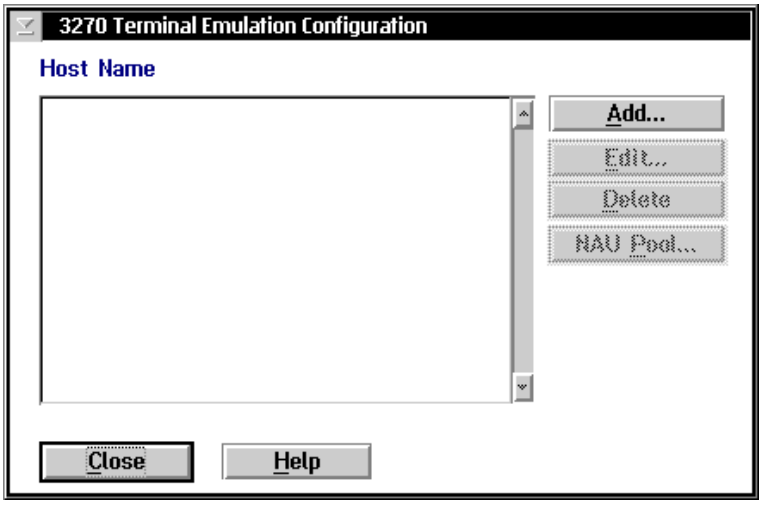
1. Fill the NAU pool for each of the hosts, but do not explicitly link any terminals to hosts. Terminals can dynamically connect with any host that has available NAUs. Terminals must be configured with a host name or the server must be configured with a default host name. For help, see "Filling the NAU Pool" later in this chapter or for help, see "Auto-Linking to Hosts" in Chapter 6.
2. Do not fill the NAU pool for any of the hosts. When you explicitly link terminal sessions to hosts, the server automatically generates NAUs starting at 002.
3. Fill the NAU pool for each of the hosts and explicitly link some terminals with hosts and NAUs. You cannot link the NAUs in the pool. For help, see "Filling the NAU Pool" and "Configuring TE Links" later in this chapter.

Before you proceed, make sure you have performed these tasks:

- Installed the DCS 300.
- Configured the network adapter cards.
- Installed and configured the connection points.

To configure the DCS 300

1. From the main menu, choose Terminal Emulation.
2. Choose 3270 SNA Host. The 3270 Terminal Emulation Configuration dialog box appears.



3. Choose Add, Edit, or Delete. If you choose Add, the Host Connection Configuration dialog box appears. For help, see "Adding an IBM SNA Host" in the next section.

   Note: *You cannot delete a host if it is linked to a device or a terminal session.*

4. (Optional) Fill the NAU pool for the hosts. For help, see "Filling the NAU Pool" later in this chapter.

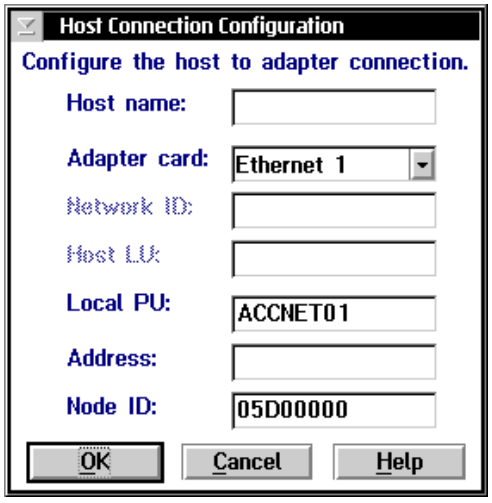
Adding an IBM SNA Host

You need to identify any hosts you want the DCS 300 to communicate with for your terminal sessions. When you add a host, you set up a link to a specific host and this information is available throughout the system. Once you create a host connection, you may use it for any SNA configurations. Only one host connection is allowed for SDLC network adapter cards.

The server maintains separate lists for 3270 hosts and 5250 hosts. If you create a host when defining a 5250 terminal session, you cannot use this host when defining a 3270 terminal session.

To add an IBM SNA host

- From the 3270 Terminal Emulation Configuration dialog box, choose Add. The Host Connection Configuration dialog box appears.



Field	Description	Value	Default
Host name	A unique name that identifies this SNA host. You can use this internal name to make the host LU name more meaningful.	1 to 8 alphanumeric characters	None
Adapter card	The network adapter card you are using to connect to the host.	Ethernet, Token Ring, SDLC	Ethernet 1
Local PU (Ethernet and token ring only)	A unique PU name for the host that allows the terminals to communicate with more than one host using the same upline adapter card. For each host configuration for the upline adapter card, you assign a unique host name and a unique local PU. Because you are using the same adapter card, all other fields in this dialog box are the same. To connect to different hosts, change the host name on your terminal.	8 uppercase alphanumeric or special characters The first character must be an alpha character.	SNA node name + 2-digit suffix, starting with 01
Address (Ethernet or token ring only)	The LAN adapter address of the host. For help, see "Converting Ethernet Addresses to Token Ring MAC Format" in Appendix B.	Token ring MAC address format	None
Node ID	Specifies the last eight characters in the host XID that are used for establishing a connection with the server. ***Note:*** *When establishing a connection, the host or server with the higher Node ID number is the primary workstation.*	8 hexadecimal characters	05D00000

Filling the NAU Pool

To edit the NAU pool and link terminals to hosts, see "Configuring TE Links" in the next section.

1. From the 3270 Terminal Emulation Configuration dialog box, choose NAU Pool. The 3270 NAU Pool dialog box appears.

2. Add all the NAUs to the NAU pool.
   a. In the New NAU field, type in the NAU.
   b. Choose Add. The NAU is added to the Unlinked NAUs pool.
3. Remove any NAUs that you do not want to use.
   a. In the Unlinked NAUs pool, select the NAU to remove.
   b. Choose Delete. The NAU is removed from the pool.
4. Choose Close to return to the 3270 Terminal Emulation Configuration dialog box.

Configuring TE Links

When you configured the connection points, you also decided how you wanted the devices to communicate with the different types of hosts. The Terminal Emulation Links dialog box lets you change these links for individual terminal sessions. There are four choices:

Link to Host The terminal session of the device is explicitly linked to a host. That is, even if a host name is specified on the device, the device can only communicate with the host to which it is linked on the server.

Default/Supplied The device will be configured with the host name. If the device is not configured with a host name, the server uses whatever method that you specified when you configured the connection point. For help, see Chapter 3, "Connecting to the Intermec RF Network."

Prompt for Host When the terminal session of the device is started, it will prompt the user to enter a host name.

Disable Session When the terminal session of the device is started, it will not be able to connect to a host. The terminal session is disabled.

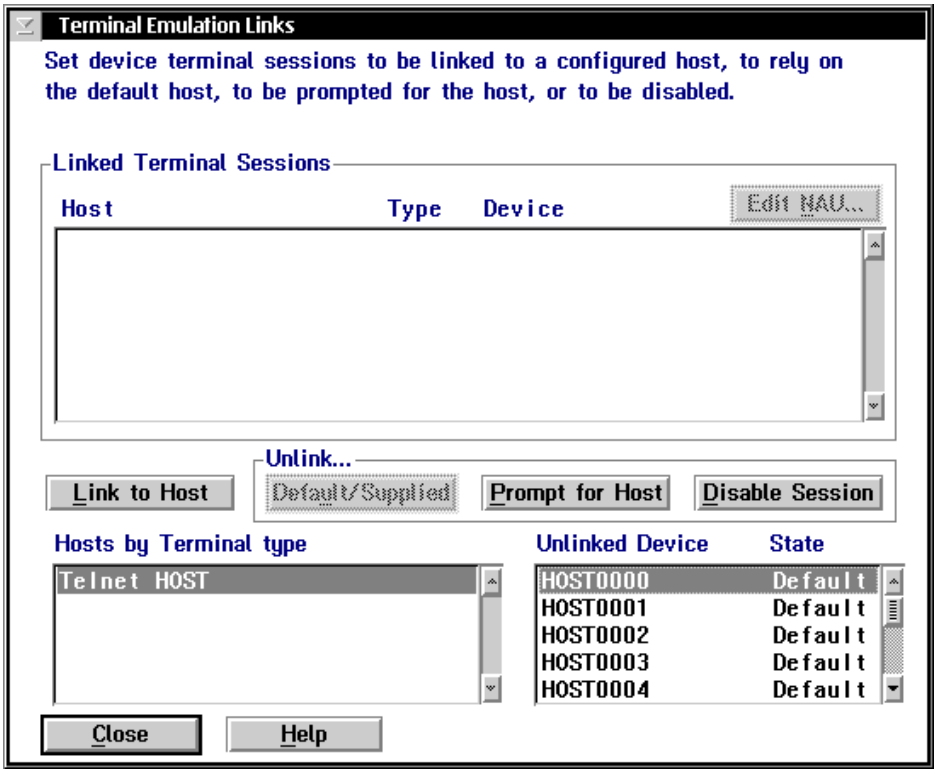
Note: *In the Terminal Emulation Links dialog box, the session number does not necessarily correspond to the session number on the server. Verify that the terminal number that appears in the Session Address List matches the terminal number that is configured on the terminal.*

The Terminal Emulation Links dialog box also lets you edit the NAUs for 3270 terminal emulation.

To configure TE links

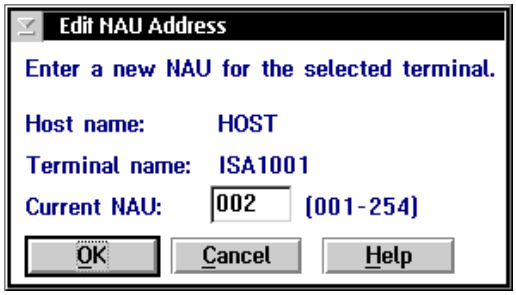
1. From the main menu, choose TE Links. The Terminal Emulation Links dialog box appears.

Terminal Emulation Links Dialog Box



3. Link any terminal sessions of the devices to hosts.
   a. In the Hosts by Terminal Type list box, select the host that you want to link to the device.
   b. In the Unlinked Device - Session - State list box, select the terminal session that you want to link to the host.
   c. Choose Link to Host. The terminal session is removed from the Unlinked Device - Session - State list box and it is added to the Link Terminal Sessions box.
4. Select any terminal sessions that you want to prompt the user for a host.
   a. In the Unlinked Device - Session - State list box or in the Link Terminal Sessions box, select the terminal session that you want to prompt the user for a host.
   b. Choose Prompt for Host. If you chose a terminal session from the Link Terminal Sessions box, it is now removed from the box and unlinked from the host. The State column is Prompt.

5. Disable any terminal sessions that you do not want to connect to a host.
   a. In the Unlinked Device - Session - State list box or in the Link Terminal Sessions box, select the terminal session that you want to disable.
   b. Choose Disable Session. If you chose a terminal session from the Link Terminal Sessions box, it is now removed from the box and unlinked from the host. The State column is Disabled.
6. (3270 SNA hosts only) Edit any NAUs that the server assigned when you explicitly linked the terminal session to a host.
   a. In the Link Terminal Sessions box, select the NAU that you want to change.
   b. Choose Edit NAU. The Edit NAU Address dialog box appears.



   c. In the Current NAU field, enter a new NAU for the device.
   d. Choose OK to return to the 3270 Terminal Emulation Configuration dialog box.

Saving and Activating Your Run-Time Configuration

If you are done configuring the DCS 300, save and activate your run-time configuration. When the activate is complete, a message box appears if you need to reboot the server.

To save and activate your run-time configuration

1. From the main menu sidebar buttons, choose Save and Activate. The Activate Configuration message box appears.
2. Choose Activate. The server saves your run-time configuration to disk and it becomes your active configuration.

If you are ready to start data collection, from the main menu sidebar buttons, choose Start Data Collection.

Configuring Your JANUS Devices

With the DCS 300 and your JANUS 900 MHz RF devices (1MB) or your JANUS UDP Plus devices (4MB), you can run:

- VT or ANSI terminal emulation (TE) to a TCP/IP host.
- 5250 or 3270 TE to an IBM SNA host.
- TN5250 or TN3270 TE to an IBM host that supports Telnet.

For help configuring your JANUS devices, see the *JANUS 900 MHz Radio Frequency Quick Reference Guide* and the *JANUS 2.4 GHz Radio Frequency Quick Reference Guide*.

Configuring for 900 MHz RF Communications

You need to configure each JANUS 900 MHz RF device for 900 MHz RF communications. Run the Interactive Configuration application (IC.EXE) on each device to set the parameters for the environment it will be used in. For help using IC.EXE, refer to your JANUS user's manual.

Configuring for UDP Plus Communications

You need to configure each JANUS UDP Plus device for UDP Plus communications. Run the JANUS 2.4 GHz Installation Utility to configure each device and install the network software. For help, see the *JANUS 2.4 GHz Installation Utility User's Manual*.

Note: *All access points and JANUS devices in the same roaming subnetwork must have the same domain and security ID.*

Downloading the JANUS TE Application

To run 5250 or 3270 TE, you do not need to load any files on your JANUS device. Your JANUS device was shipped from Intermec with the TE files already loaded. However, if you lose these TE files, or change the JANUS TE application, you may want to download the .CFG file, the .MAP file, and the application. To run VT or ANSI TE, you must download the TE.CFG file and the TE application from the DCS 300 to each JANUS device. When you download the JANUS TE application, the files must be on the E drive.

On the DCS 300, these files are in the \USERDATA\TERMAPPS\TE\ADD_FILE directory:

TE.CFG This file contains the configuration information that each JANUS device needs to run VT or ANSI TE. You define the configuration on the JANUS device using the Terminal, Communications, and Viewport screens in the TE Configuration menu.

TE5250.CFG This file contains the configuration information that each JANUS device needs to run 5250 TE.

TE3270.CFG This file contains the configuration information that each JANUS device needs to run 3270 TE.

JAN5250.MAP This key mapping file is used with 5250 TE. This file is read only.

JAN3270.MAP This key mapping file is used with 3270 TE. This file is read only.

On the DCS 300, these files are in the \USERDATA\TERMAPPS\TE\JANUS900 directory:

TNVT900.EXE This executable file runs VT/ANSI terminal emulation. You can only use this file if your JANUS 900 MHz RF device uses firmware v3.01 or higher.

J95250.EXE This executable file runs 5250 TE. You can only use this file if your JANUS 900 MHz RF device uses firmware v3.01 or higher.

J93270.EXE This executable file runs 3270 TE. You can only use this file if your JANUS 900 MHz RF device uses firmware v3.01 or higher.

On the DCS 300, these files are in the \USERDATA\TERMAPPS\TE\JANUSUDP directory:

UDPPVT.EXE This executable file runs VT/ANSI terminal emulation. You can only use this file if your JANUS 2.4 GHz RF device uses UDP Plus and firmware v4.01 or higher. To run 5250 or 3270 TE, you should not need to download the .CFG file and the JANUS TE application from the server.

UDPP5250.EXE This executable file runs 5250 terminal emulation. You can only use this file if your JANUS 2.4 GHz RF device uses UDP Plus and firmware v4.01 or higher.

UDPP3270.EXE This executable file runs 3270 terminal emulation. You can only use this file if your JANUS 2.4 GHz RF device uses UDP Plus and firmware v4.01 or higher.

Depending on the type of communications your JANUS devices are using and which firmware version is loaded, you can download the application to your JANUS devices using one of these methods:

- If your JANUS 900 MHz RF device has firmware v3.01 or later, use the download server feature. For help, see "Using the DCS 300 to Transfer Files" in Appendix B.

  Note: *Your JANUS devices must have FTA.EXE and FTA.INI loaded on drive C. Copy these files from Application companion disk 3. For help, see your JANUS user's manual.*

  Note: *Your JANUS devices must be running a BFT-ready PSK application.*

- If your JANUS 2.4 GHz RF device is using UDP Plus, use the download server or FTP. To use FTP, you must have an FTP client loaded on your JANUS device.

To use FTP to load the JANUS TE application

Note: *FTP commands are case-sensitive. You must type all commands in lowercase.*

1. Make sure that the JANUS device is at a writable DOS prompt. Type F T P space *IPaddress*

   where *IPaddress* is the IP address of the DCS 300 and press enter.

2. In the login name field, type A N O N Y M O U S and press enter.

3. Type C D space `path`

   where *path* is the location of the JANUS TE application on the DCS 300 and press enter.

4. Type B I N and press enter.

5. Type G E T space *filename*.cfg and press enter.

   where *filename*.CFG is the name of the file that contains the configuration information that each JANUS device needs to run TE.

6. Type G E T space *filename*.exe and press enter.

   where *filename*.EXE is the name of the executable file of the JANUS TE application.

7. When the terminal template application has finished loading on the JANUS device, type Q U I T and press enter.

About the Auto-Login Feature

When the terminal session is started, the terminal screen displays the host login prompt. If you are using the auto-login feature, then once you log into a host, the terminal runs the auto-login script file and saves your login information in memory. If you lose a connection to the host, you will automatically be logged into the subsequent TE session. However, if you use a hot key sequence to end the TE session or if you must reboot the device, you must log in again.

For help creating the auto-login script file, see your JANUS Terminal Emulation Quick Reference Guide. After you create your auto-login script file (AUTOLOG.SCR), you must download it to the same directory as the TE application on your JANUS device.

On the DCS 300, a sample AUTOLOG.SCR is in the \USERDATA\TERMAPPS\TE\ADD_FILE directory.

To use the auto-login feature

- For VT/ANSI, press Ctrl F4 .
- For 5250 or 3270, press Alt F6 .
- Or, you can scan:

  Auto-Login Restart

  %ALRS

To logoff from the host and use the auto-login feature

VT/ANSI At the TE prompt, type EXIT. You return to a DOS prompt. If the auto-login script file is in the current directory, you return to the first screen after the login screen. Or, press Ctrl F6 to go immediately to a DOS prompt.

5250/3270 Enter the appropriate command to logoff from the host screen. You return to the login screen. If the auto-login script file is in the current directory, you return to the first screen after the login screen. To return to the DOS prompt, follow the next procedure to exit TE.

To exit TE and delete the auto-login information

1. Access the TE Configuration menu.

   VT/ANSI On the JANUS device, press Ctrl F3 .

   5250 or **3270** On the JANUS device, press Alt X .

2. Select the Exit TE command and press enter ↵ . The next time you start a TE session on the JANUS device, you will need to log in again.

This method prevents another user from using your login.

Displaying International Characters

You can configure your JANUS devices to display single-byte international characters. That is, the device displays screen data using various character sets while running terminal emulation. This feature maps SBCS code pages for various Latin-based languages to SBCS code page 850, a multilingual code page for Latin-based languages.

On the DCS 300, you can find the .MAP files in the \USERDATA\TERMAPPS\TE\INTERNAT directory.

To use international character sets

1. On the server, rename the desired code page table .MAP file to DISPTBLS.MAP. Refer to the table below.
2. Download the new DISPTBLS.MAP file to your device. For help, see "Using the DCS 300 to Transfer Files" in Appendix B.
3. Modify the AUTOEXEC.BAT and CONFIG.SYS files on your device to display the international characters. For help, see your JANUS Terminal Emulation Quick Reference Guide.

Country	Code Page Table	Other Countries
U.S. English	037-850.MAP	Canada
France	297-850.MAP	
Germany	273-850.MAP	
Italy	280-850.MAP	
Norway	277-850.MAP	Denmark
Portugal	500-850.MAP	Belgium, Brazil, Switzerland
Spain	284-850.MAP	
Sweden	278-850.MAP	Finland

Note: *To create a custom translation table for non-IBM hosts running VT/ANSI TE, copy ISO1-850.MAP for UNIX hosts or DEC-850.MAP for DEC/VAX hosts and rename the file to DISPTBLS.MAP.*

Configuring Your TRAKKER Antares Terminals

With the DCS 300 and your TRAKKER Antares terminals, you can run:

- VT or ANSI terminal emulation (TE) to a TCP/IP host.
- 5250 or 3270 TE to an IBM SNA host.
- TN5250 or TN3270 TE to an IBM host that supports Telnet.

For help configuring your TRAKKER Antares terminals, see your *TRAKKER Antares Terminal Emulation User's Guide.*

Configuring for Communications

You must configure each TRAKKER Antares terminal to communicate with the DCS 300. Use the TRAKKER Antares 2400 Menu System to set the parameters for the environment that each terminal will be used in. For help, see your TRAKKER Antares terminal user's manual.

Note: *All access points and TRAKKER Antares terminals in the same roaming subnetwork must have the same domain and security ID.*

Downloading the TRAKKER Antares TE Application

The TRAKKER Antares TE application was preloaded when you ordered your terminal. However, this application is also loaded on your DCS 300 should you lose your TE files or if you want to change your TE application. When you download the TRAKKER Antares TE application, the files are automatically put in the C drive.

There are two ways that you can download the TRAKKER Antares applications:

- Use the Firmware Upgrade Utility. For help, see "Using the DCS 300 to Upgrade TRAKKER Antares Terminals" in Appendix D.
- Use the download server feature. For help, see "Using the DCS 300 to Transfer Files" in Appendix B.

To run VT or ANSI TE, download the .CFG file from the server to each terminal. On the server, the .CFG file and the map files are in the \USERDATA\TERMAPPS\TE\ADD_FILE directory:

TEANT.CFG This file contains the configuration information that each terminal needs to run VT or ANSI TE. You define the configuration using the TE Configuration menu.

POLX5250.MAP This key mapping file is used with 5250 TE. This file is read only.

POLX3270.MAP This key mapping file is used with 3270 TE. This file is read only.

To run any TE, download the TRAKKER Antares TE application from the server to each terminal. On the server, these files are in the \USERDATA\TERMAPPS\TE\POLUDPP directory:

VTXXX_D.BIN This executable file runs VT/ANSI TE on the terminal.

PLX3270.BIN This executable file runs 3270 TE on the terminal.

PLX5250.BIN This executable file runs 5250 TE on the terminal.

About the Auto-Login Feature

When the terminal session is started, the terminal screen displays the host login prompt. If you are using the auto-login feature, after you log into a host, the terminal runs the auto-login script file and saves your login information in memory. If you lose a connection to the host, you will automatically be logged into the subsequent TE session. However, if you use a hot key sequence to end the TE session or if you need to reboot the terminal, you will need to login again.

On the server, you can find an example auto-login script file in the \USERDATA\TERMAPPS\TE\ADD_FILE directory.

For more help on creating the auto-login script file, see the *TRAKKER Antares Terminal Emulation User's Guide*. After you create the auto-login script file (AUTOLOG.SCR), you need to download it to your terminal. For help, see "Using the DCS 300 to Transfer Files" in Appendix B.

Displaying International Characters

You can configure your TRAKKER Antares terminals to display single-byte international characters. That is, the terminal displays screen data using various character sets while running terminal emulation. This feature maps SBCS code pages for various Latin-based languages to SBCS code page 850, a multilingual code page for Latin-based languages.

On the DCS 300, you can find the .MAP files in the \USERDATA\TERMAPPS\TE\INTERNAT directory.

To use international character sets

1. On the server, rename the desired code page table .MAP file to DISPTBLS.MAP. Refer to the table on the next page.
2. Download the new DISPTBLS.MAP file to your device. For help, see "Using the DCS 300 to Transfer Files" in Appendix B.

Country	Code Page Table	Other Countries
U.S. English	037-850.MAP	Canada
France	297-850.MAP	
Germany	273-850.MAP	
Italy	280-850.MAP	
Norway	277-850.MAP	Denmark
Portugal	500-850.MAP	Belgium, Brazil, Switzerland
Spain	284-850.MAP	
Sweden	278-850.MAP	Finland

Note: *To create a custom translation table for non-IBM hosts running VT/ANSI TE, copy ISO1-850.MAP for UNIX hosts or DEC-850.MAP for DEC/VAX hosts and rename the file to DISPTBLS.MAP.*

Configuring Your WTP Devices

With the DCS 300 and your WTP devices, you can run:

- VT terminal emulation (TE) to a TCP/IP host.
- 5250 or 3270 TE to an IBM SNA host.
- TN5250 or TN3270 TE to an IBM host that supports Telnet.

For help configuring your WTP devices, see your device's user's manual.

Displaying International Characters

You may want to use an international character set with your WTP devices. This feature lets these terminals display screen data using this character set while running terminal emulation. You can also configure your devices to display single-byte or double-byte international characters.

For help, configuring your WTP devices to display international characters, see your device's user's manual.

Setting Security for the TE Configuration Menu

You can set a password to control access to the terminal emulation configuration menu on JANUS devices and TRAKKER Antares terminals. When you first configure your devices, no passwords are enabled. If you set a password on a device, when you use the hot key sequence to access the TE Configuration menu, the Verify TE Password screen appears. You must enter the correct password before the TE Configuration menu appears.

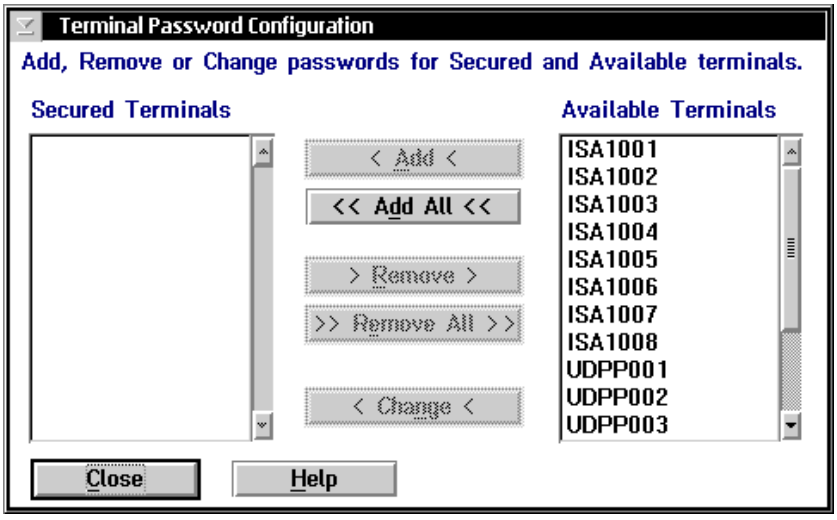
You can temporarily change the password on the device. The device stores the new encrypted password in a TE.SEC file. However, each time you start the TE application, the device requests the password that is stored on the DCS 300. Therefore, if you want to permanently change the password, you must change it from the server.

For help setting the password on JANUS 900 MHz RF devices, see the *JANUS 900 MHz Terminal Emulation Quick Reference Guide*. For help setting a password on JANUS 2.4 GHz RF devices, see your *JANUS 2.4 GHz Installation Utility User's Manual*. For help setting a password on TRAKKER Antares terminals, see the *TRAKKER Antares Terminal Emulation User's Guide*.

Note: *Currently, this feature is not supported on WTP devices.*

To set security for the TE Configuration menu

1. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
2. Choose Terminal Password Configuration and then choose Start. The Terminal Password Configuration dialog box appears.



3. To set a password on a terminal, select the terminal from the Available Terminals list box and choose Add.

   Tip: *You can press and hold the* ***Shift*** *key and then select multiple terminals.*

   To set the same password on all the terminals at the same time, choose Add All.

   The Terminal Password dialog box appears.

4. In the Password field, enter the password to access the TE Configuration menu. The password can be up to ten alphanumeric characters.
5. Choose Add. The terminal or terminals you selected appear in the Secured Terminals list box.
6. Choose Close to close the dialog box and return to the System Maintenance dialog box.
7. Choose Close to return the main menu.

To change the security for the TE Configuration menu

1. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
2. Choose Terminal Password Configuration and then choose Start. The Terminal Password Configuration dialog box appears.
3. To change a password on a terminal, select the terminal or group of terminals from the Secured Terminals list box and choose Change. The Terminal Password dialog box appears.
4. In the Password field, enter a new password to access the TE Configuration menu.
5. Choose Change. The password is changed.
6. Choose Close to close the dialog box and return to the System Maintenance dialog box.
7. Choose Close to return the main menu.

To disable security for the TE Configuration menu

1. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
2. Choose Terminal Password Configuration and then choose Start. The Terminal Password Configuration dialog box appears.
3. To remove the password from a terminal, select the terminal or group of terminals from the Secured Terminals list box and choose Remove. The terminal is removed from the Secured Terminals list box.

   To remove the password from all the terminals at the same time, choose Remove All. All the terminals are removed from the Secured Terminals list box and appear in the Available Terminals list box.
4. Choose Close to close the dialog box and return to the System Maintenance dialog box.
5. Choose Close to return the main menu.

To verify that security is set

1. From the main menu sidebar buttons, choose System Reporting. The System Reporting dialog box appears.
2. Choose View Runtime Configuration and then choose Start. The View Runtime Configuration Options dialog box appears.
3. Make sure that the Intermec controllers/Devices check box is checked and choose Run View. The Runtime Configuration dialog box appears.
4. Scroll through the file until you see a list of the devices that are enabled. If Password Protected is Yes, then security is set.
5. Choose Close to close the Runtime Configuration dialog box and return to the View Runtime Configuration Options dialog box.
6. Choose Cancel to return to the System Reporting dialog box.
7. Choose Close to return to the main menu.

9

Using Peer-to-Peer Applications

Now that you have configured the DCS 300 to communicate with your LAN and you have configured your server to communicate with your Intermec network, you are ready to tie the entire data collection network together using an application.

This chapter explains how to configure your server for using peer-to-peer applications and it provides guidelines on how to write TCP/IP or APPC applications so that they can communicate with the server. This chapter also provides guidelines on how to write applications that communicate using a direct TCP/IP socket interface.

Chapter Checklist

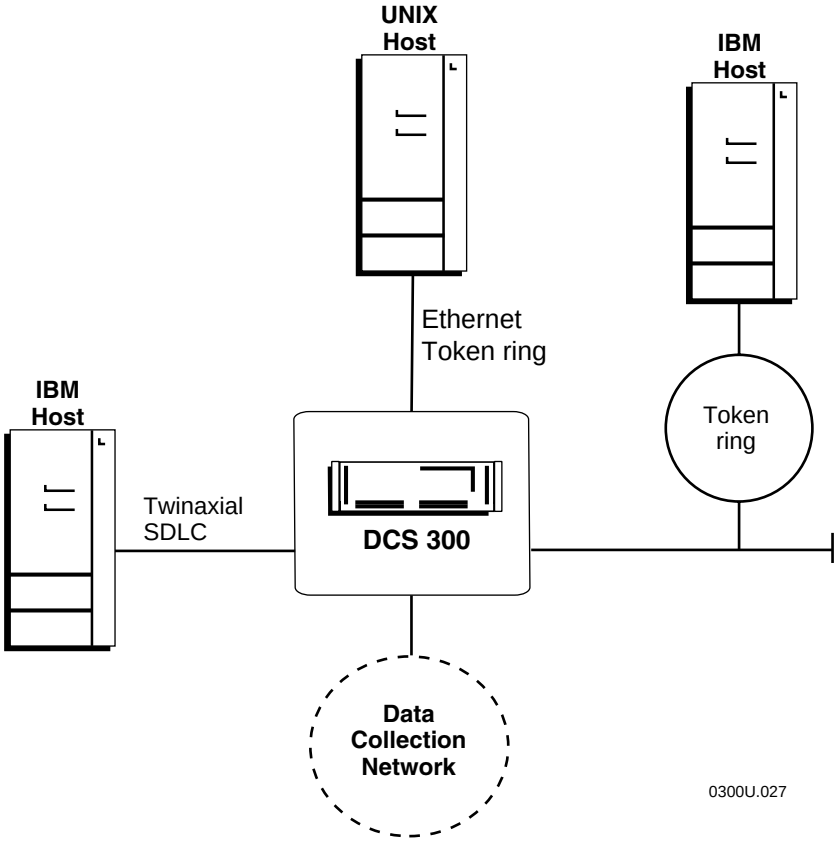
Done?	Task	Page
❑	Configure the host for peer-to-peer applications.	9-5
❑	Identify the peer-to-peer links.	9-6
❑	Identify any transaction IDs that are routed to the peer-to-peer links.	9-10
❑	Save and activate the configuration.	9-11
❑	Understand how TCP/IP applications communicate with the server.	9-12
	Or,	
	Understand how to use the direct TCP/IP socket interface.	9-18
	Understand how APPC applications communicate with the server.	9-23

When you understand these sections and perform these tasks, you can start using the server.

About Peer-to-Peer Applications

The DCS 300 runs an applications programming interface (API) that makes communicating with remote applications easier. Applications communicate with the server through network communications processes called NetComms. NetComms are responsible for safely routing data from remote applications across a network to the server and back.

After you configure the server, you need to create or modify your TCP/IP and APPC applications so that they communicate with the server. If you need more information, see the *DCS 300 Technical Reference Manual*.



Configuring the Host for Peer-to-Peer Applications

For peer-to-peer applications, your network administrator needs to set up certain parameters on the host for TCP/IP or APPC applications.

TCP/IP Applications

IP address The IP address is the address that is assigned to the Ethernet card or token ring card in the DCS 300. The IP address has the format xxx.xxx.xxx.xxx where xxx is a number from 0 to 255.

TCP/IP NetComm send port (4400) This number identifies the port number through which the host makes send connections to the DCS 300.

TCP/IP NetComm receive port (4401) This number identifies the port number through which the host makes receive connections to the DCS 300.

APPC Applications

LU name The DCS 300's logical unit name is the partner LU name that your application references when allocating an APPC conversation. The default is ACCNET.

Network ID The network ID is the SNA network ID that was specified when you configured the DCS 300. The default is APPN.

MAC address The Ethernet or token ring address. You can verify the default value using the View Runtime Configuration feature. For help, see "Viewing the Run-Time Configuration" in Appendix A.

Send transaction program This program is the DCS 300's transaction program name for the send connection. The default is RECEIVE.

Receive transaction program This program is the application's transaction program name for its receive connection to the DCS 300. The default is SEND.

Mode name The mode name describes the class of service and other session characteristics that you may want to alter or create to suit your network design. The default is #INTER. For help on setting up #ACCNET mode on your host, see the *DCS 300 Technical Reference Manual*.

Setting Up Peer-to-Peer Links

To run TCP/IP or APPC applications in your data collection network, you must identify all the application names in the DCS 300. The server puts these names in a peer-to-peer destination list. Every time an application connects to the server, it informs the server of its name. The server dynamically associates the application as one of the destinations in its peer-to-peer destination list and forwards the appropriate transactions to it. The server routes transactions to applications or other peer-to-peer destinations by one of two ways:

- The server recognizes the transaction ID and routes the transaction to all destinations in the peer-to-peer destination list that are associated with this transaction ID.
- The application is the destination in the transaction header.

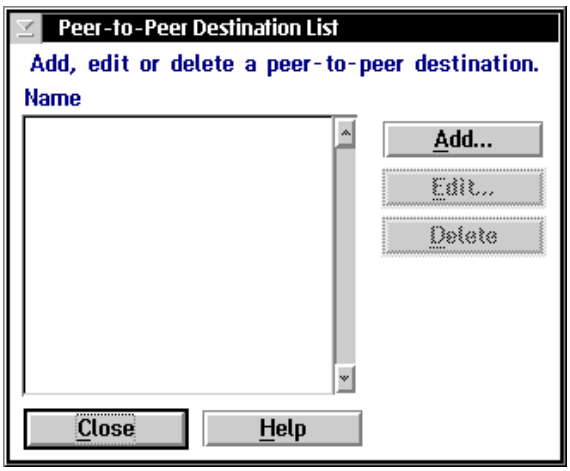
This section describes how to set up the peer-to-peer destination list for your host applications and your devices.

Before you proceed, make sure you have already performed these tasks:

- Installed the DCS 300.
- Installed and configured the connection points and downline devices.
- Configured the network adapter cards.

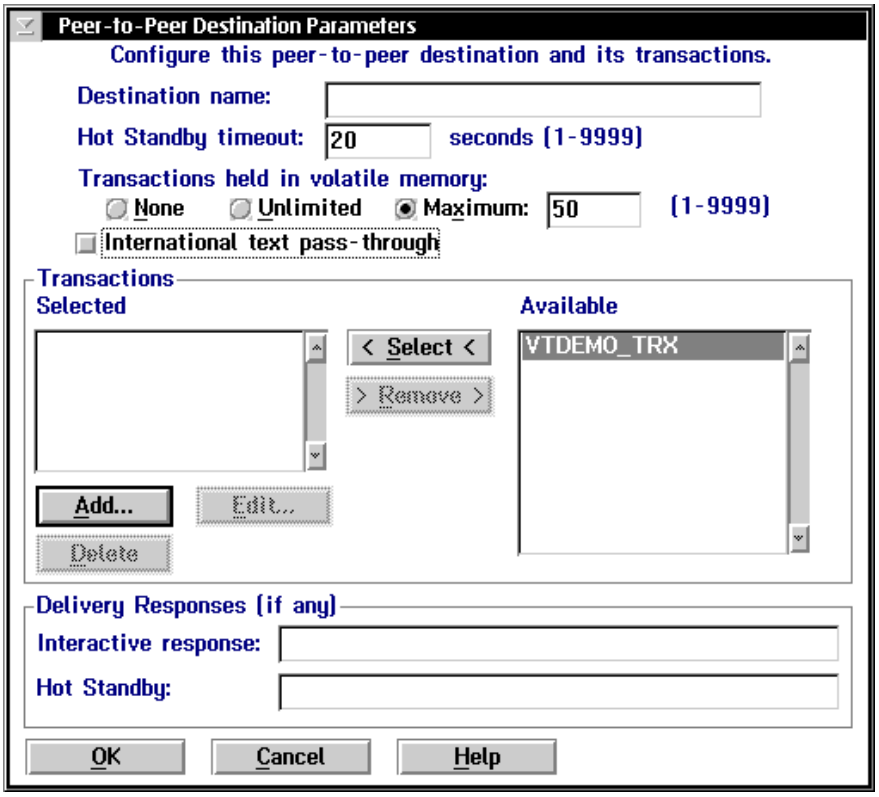
To set up peer-to-peer destination list

1. From the main menu, choose Peer-to-Peer and then choose Host Connection. The Peer-to-Peer Destination List dialog box appears.



2. Choose Add, Edit, or Delete destinations. If you choose Add, the Peer-to-Peer Destination Parameters dialog box appears.

Peer-to-Peer Destination Parameters Dialog Box



Field	Description	Value	Default
Destination name	The meaningful name that identifies the destination (application).	1 to 16 alphanumeric characters	None
Hot Standby timeout	The number of seconds the server waits for a response from this destination before it places transactions going to this destination in a Hot Standby file.	1 to 9999	20
Transactions held in volatile memory	The number of transactions the server keeps in RAM before it writes the transactions to a Hot Standby file. Choose None if you want the transaction always written to the file. This setting is the safest setting and it is also the slowest. Choose Unlimited if you do not want the transaction written to the file unless the time you set for the Hot Standby timeout expires. This setting is the fastest. Choose Maximum and enter the maximum number of transactions the server stores in RAM before it writes them to a file.	None, Unlimited, Maximum	50
International text pass-through	This check box determines how much of the transaction is converted. If you check this check box, the server converts only the transaction header. If you clear this check box to use limited EBCDIC mapping, the server converts the entire transaction. For help, see "Using International Text Pass-Through" in the next section.	Check, Clear	Clear
Selected	This list box contains the transactions that are routed to this destination.	Predefined	None
Available	This list box contains the transactions that are available to add to the Selected list box.	Predefined	None
Interactive response (optional)	This message is sent to the source of the transaction when the transaction for this destination is delivered successfully in Interactive mode.	1 to 39 characters	None
Hot standby (optional)	This message is sent to the source of the transaction when the transaction for this destination is written to a Hot Standby file.	1 to 39 characters	None

Using International Text Pass-Through

International text pass-through allows data streams representing characters encoded in various encoding schemes to pass without conversion between various hosts and devices through the DCS 300. The data streams appear to the server as arbitrary streams of bytes passed between the hosts and devices. The hosts and devices are responsible for any necessary conversion of the characters. The server is responsible for configuring connections between the hosts and devices, establishing sessions, and routing transactions.

International text pass-through provides uniform pass-through support for the character encoding schemes used by the hosts and devices.

Host	Character Encoding Scheme
IBM	EBCDIC SBCS, DBCS
Unix	SBCS, DBCS, EUC
Windows NT	Unicode
JANUS devices	SBCS, DBCS
TRAKKER Antares terminals	SBCS, DBCS

Before you use this feature, note the following:

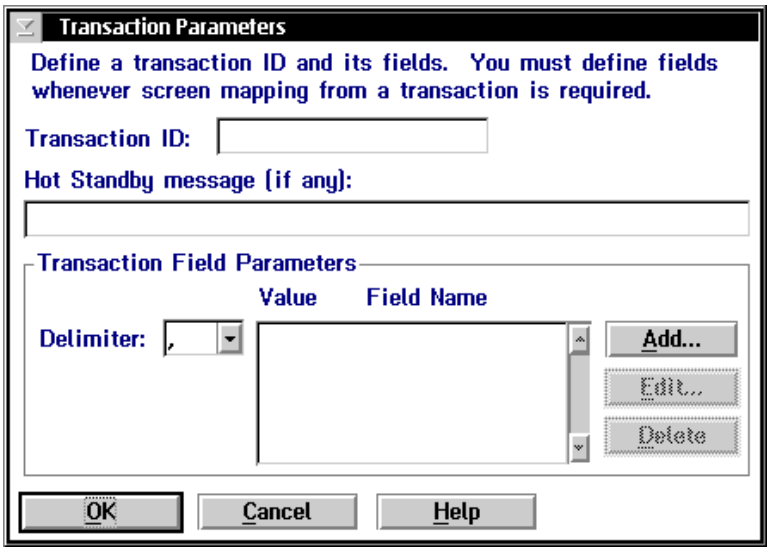
- The DCS 300 attaches a transaction header to messages that it receives from hosts and it attaches a transaction ID to route messages to and from devices. The characters in the transaction header and the transaction ID are limited by what you can type on the DCS 300. The characters for the transaction data can be an arbitrary sequence of bytes representing text in any character encoding scheme.
- Configuration text that is passed between the DCS 300 and devices must use the ASCII character set.
- The DCS 300 still supports limited mapping from EBCDIC code page 037 to PC code page 437. If the DCS 300 cannot look up the source of the transaction in the peer-to-peer destination list, the DCS 300 assumes that EBCDIC mapping is enabled and international text pass-through is disabled. However, if you check the international text pass-through check box, you disable this EBCDIC mapping.
- Mapping from arbitrary EBCDIC code pages to arbitrary PC code pages for the transaction data originating from an APPC peer-to-peer applications is not supported.
- No conversions are necessary if you enable the time append feature.
- The DCS 300 does not support sort order, date, item, and currency.

Adding a Transaction

You need to define all transaction IDs that you want the DCS 300 to route to the destinations.

To add a transaction

- From the Peer-to-Peer Destination Parameters dialog box, choose Add. The Transaction Parameters dialog box appears.



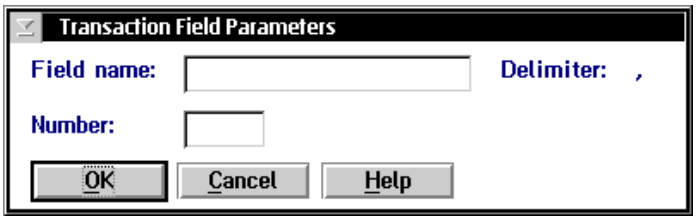
Field	Description	Value	Default
Transaction ID	The unique ID of the transaction.	1 to 20 alphanumeric characters	None
Hot Standby message (Optional)	The message that is sent to the source of the transaction when the server places the transaction in a Hot Standby file.	1 to 40 characters	None
Delimiter	The character that separates the fields in the transaction. The delimiter must be the same throughout the network.	1 alphanumeric or special character	, (comma)

Adding a Transaction Field

You need to add transaction fields if you are using these transactions for screen mapping.

To add a transaction field

- From the Transaction Parameters dialog box, choose Add. The Transaction Field Parameters dialog box appears.



Field	Description	Value	Default
Field name	The unique name for the transaction field.	1 to 16 alphanumeric characters	None
Number	The order or position of the field in the transaction. Fields start at 1.	1 to 999	None

Saving and Activating Your Run-Time Configuration

When you finish configuring peer-to-peer applications, you should save your changes. If you are done configuring the DCS 300, save and activate your run-time configuration. When the save and activate are complete, a message box appears if you need to reboot the server.

To save and activate your run-time configuration

1. From the main menu sidebar buttons, choose Save and Activate. The Activate Configuration message box appears.
2. Choose Activate. The server saves your run-time configuration to disk and it becomes your active configuration.

If you are ready to start data collection, from the main menu sidebar buttons, choose Start Data Collection.

Communicating With TCP/IP Applications

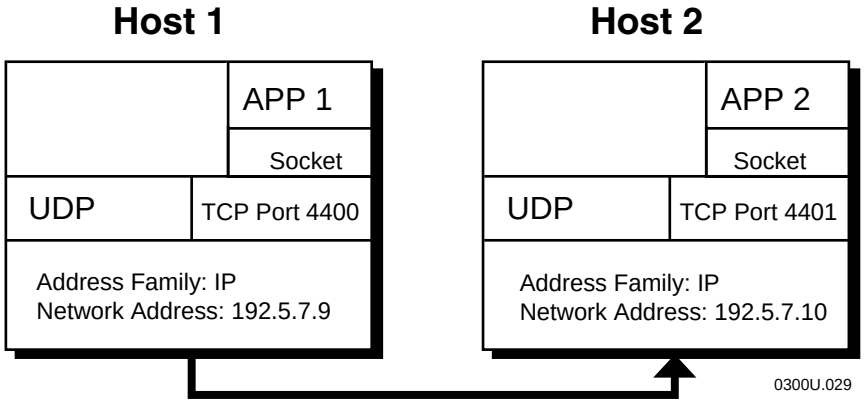
The DCS 300 communicates with remote applications using TCP/IP sockets. TCP provides a method for creating connection-oriented, error-free, full-duplex, byte-stream communications between two processes. IP provides a method for transmitting blocks of data, called IP datagrams, between hosts. Together, TCP and IP offer reliable, easy-to-use communications.

The server NetComms use the TCP/IP socket API to provide a standard interface to TCP/IP Transport and Internet layers. The API supports the "streams" socket-type interface, which is a reliable, connection-oriented service. When data is sent, the transmission of the data packet is guaranteed and it is received in the same order as it was sent. Built-in flow control avoids data overruns. No boundaries are imposed on the data; it is considered to be a byte stream.

The NetComms are server applications that issue passive open commands to accept connections from remote applications. The server mode send and receive NetComms are each started as a single process that receives requests from remote applications for both send and receive server connections respectively.

Each NetComm can handle a maximum number of connections before spawning off an identical process to handle any new connections. You set the maximum number of connections in the Max connections field in the System Parameters dialog box.

This figure shows a typical client/server configuration using sockets. Server 1 runs on Host 1 and Client 1 runs on Host 2. Server 1 listens on a socket that uses IP. Each socket is identified by a socket address, which is a data structure that specifies the address family, network address, and port number.



Address family Also called the protocol family. The address family determines the communications protocol used to deliver the transaction and the structure of the addresses used to represent the end point of the communication.

Network address Along with the communications protocol, the network address value uniquely identifies a host on one or more interconnected networks.

Port number This value specifies a communication end point within the host. The port numbers are 4400 for the send connection and 4401 for the receive connection.

For an application to become interactive with the server, it must have a send and a receive connection.

- The send connection sends data to the server.
- The receive connection receives data from the server.

The server supports only requester (client) connections. The remote application initiates both sockets.

For help, see the *DCS 300 Technical Reference Manual*.

How the DCS 300 Communicates With Applications

To use the NetComms, you must first configure the DCS 300 for TCP/IP communications. For help, see "Configuring the Network Adapter Card for TCP/IP" in Chapter 3.

Applications acknowledge the server directly by placing data in an ACK transaction and by using the Inter system transaction to control their interactivity with the server.

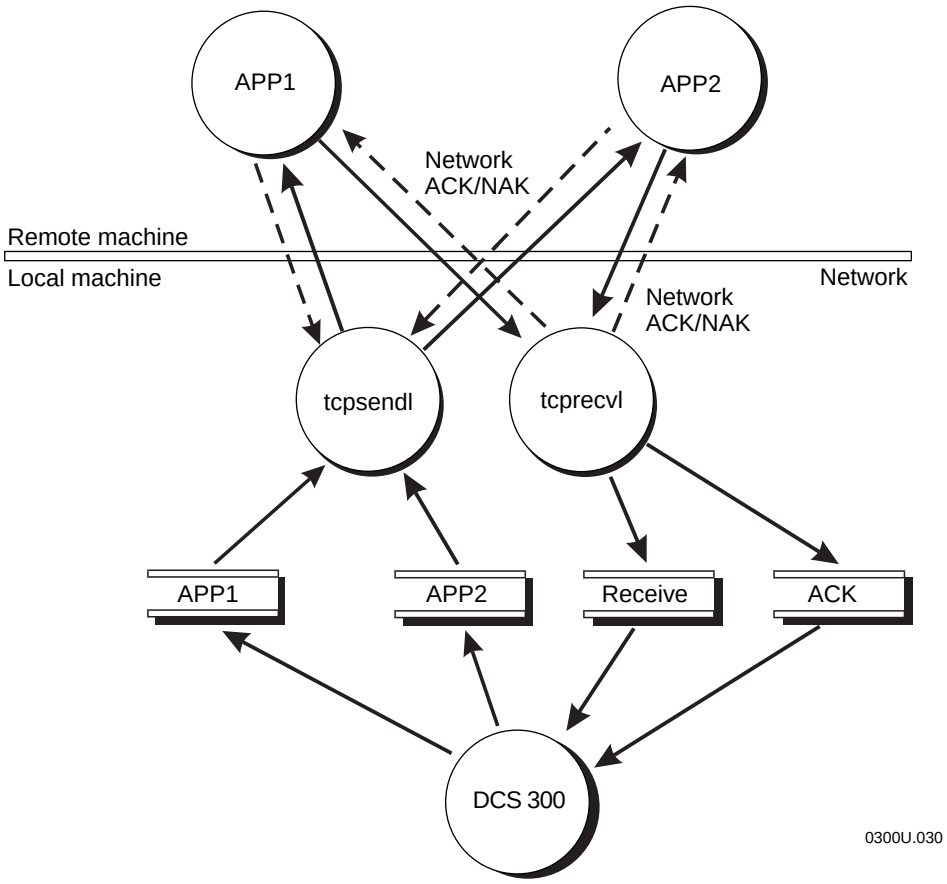
- The server send NetComm is responsible for creating the application IPC channel and forwarding any data in that channel to the application.
- The server receive NetComm is responsible for opening the Receive (input) channels of the message handler and for sending data that is received from the application through the network connection to the message handler.

When the server is turned on, it detects when TCP/IP is being used and it starts the appropriate NetComms.

If you use the wrong syntax or do not supply all the required startup arguments, an error message appears in the error log.

The following figure shows the NetComms communicating directly with applications. NetComms use IPC channels to exchange data with other server components and they use sockets to exchange data with a TCP/IP application.

Server NetComms Communicating With Applications



Understanding Transaction Routing in a TCP/IP Network

The applications you create to interact with the DCS 300 function as remote applications.

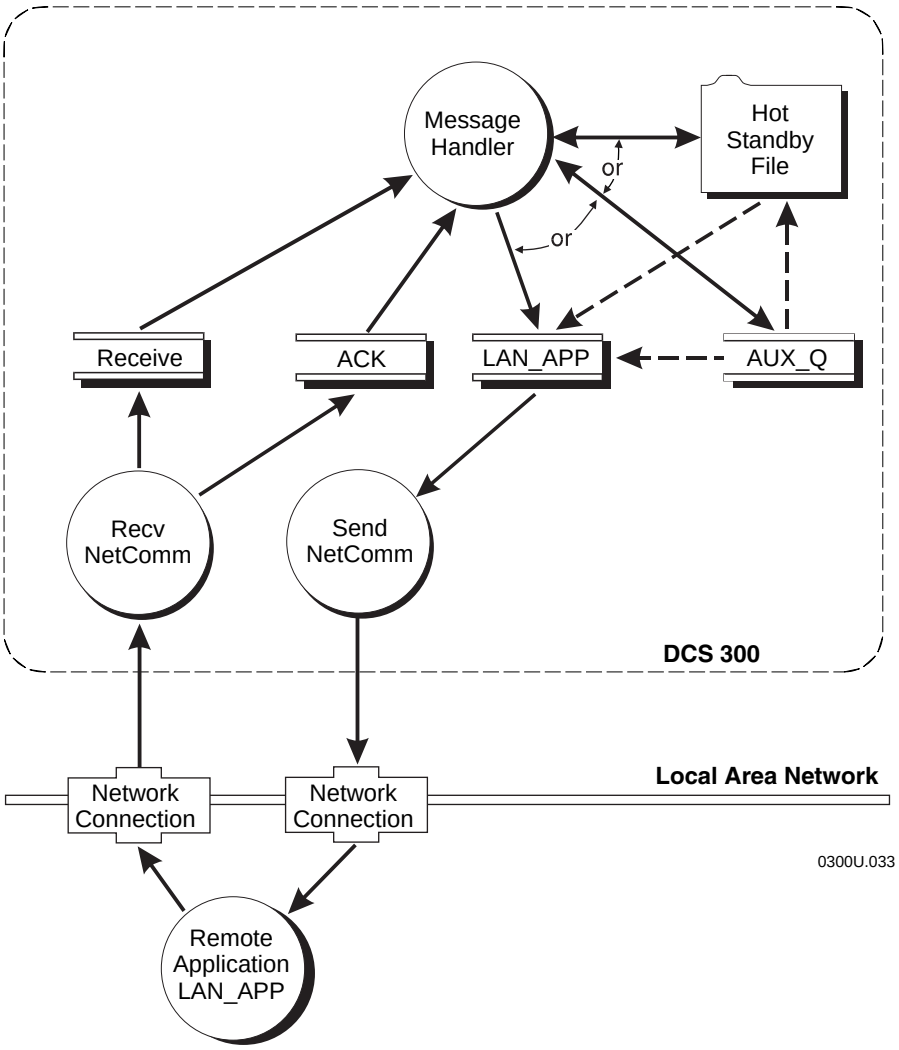
When your application receives a message from the server, your application must perform these steps:

1. The application acknowledges the send NetComm with the NetACK.
2. The application acknowledges the message handler, as follows:
    - The application creates the ACK transaction by swapping the message's source and destination. The transaction can contain data.
    - The application sets the fNetACK flag to A.
    - The application writes the ACK transaction to the receive NetComm. Because the fNetACK flag is set to A, the receive NetComm routes the transaction to the ACK channel, which sends the transaction to the message handler.

When your application sends unsolicited data to the server, your application must perform these steps:

1. The application builds the transaction and provides either a destination or a transaction ID.
2. The application clears the fNetACK flag.
3. The application sends the transaction to the receive NetComm. Because the fNetACK flag is clear, the receive NetComm routes the transaction to the Receive channel, which sends the transaction to the message handler.

Programming Interface for Applications to the Server



Your applications will use TCP sockets to communicate with the server across a TCP/IP network. The server sets up two channels:

Receive channel The low priority Receive channel handles unsolicited transactions from devices and applications, and handles system transactions from applications.

ACK channel The high priority ACK channel handles acknowledgment (ACK) transactions from applications and devices.

The server creates one auxiliary channel (AUX_Q) for each known application. Transactions that are held in AUX_Q have not been saved on disk. If you have a lot of unprotected power failures, you can reduce the risk of data loss by using the GUI to set the Transactions held in volatile memory parameter, as follows:

- If you set the parameter to a small number, only that many transactions can be lost during a power failure.
- If you set the parameter to 0, no transactions are held in volatile memory. Instead, all transactions that would have been written to AUX_Q are instead written to a Hot Standby file.

When you configure the server, you must pick a realistic value for the Hot Standby timeout so that the server does not hold too many transactions in the auxiliary channels. Once an application goes into Hot Standby mode, performance and throughput decrease because the transactions for the application are stored on disk.

It is also important for your application to remain active with respect to the server. When an application is inactive, the last transaction sent to the server is stored in a Hot Standby file along with any subsequent transactions. When the application becomes active, the transactions are delivered, first in first out (FIFO), from the Hot Standby file.

Communicating Through the Direct TCP/IP Socket Interface

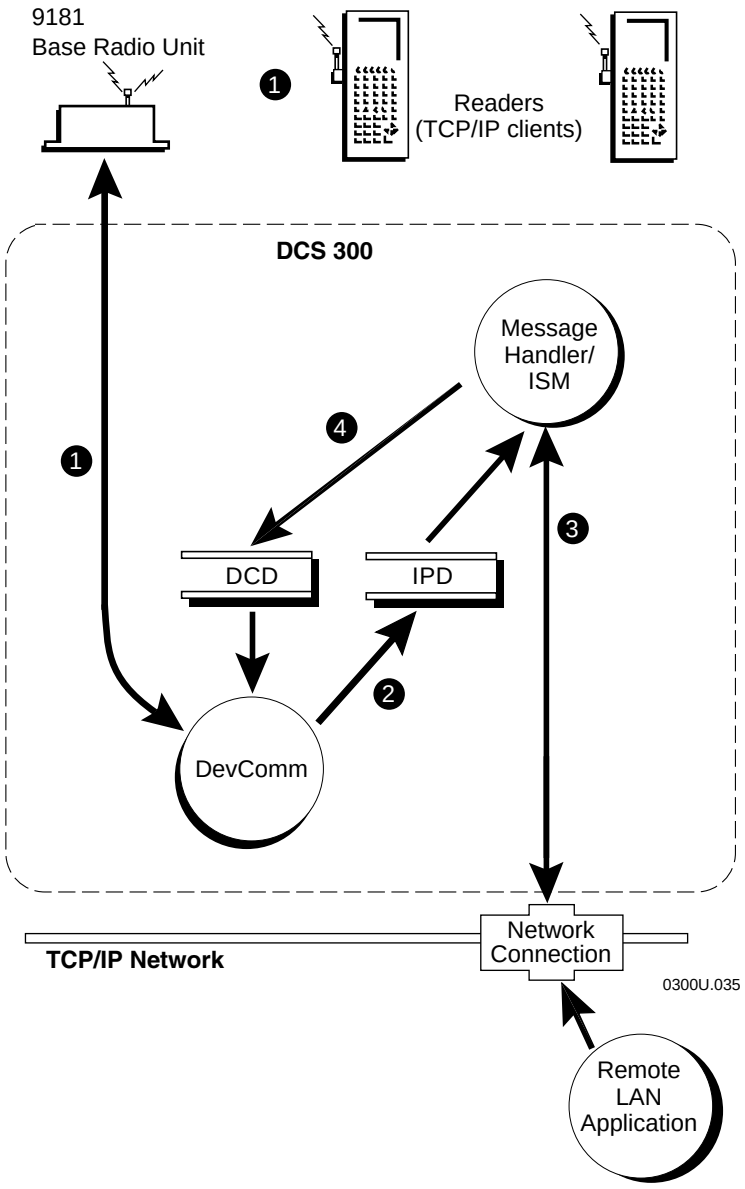
The direct TCP/IP socket interface allows non-TCP/IP capable devices, such as JANUS 900 MHz RF devices and TRAKKER Antares terminals, to establish a TCP/IP socket connection to the host through the DCS 300. For more information on using the direct TCP/IP socket interface, see the *DCS 300 Technical Reference Manual*.

Note: *The direct TCP/IP socket interface does not support JANUS 2.4 GHz RF devices, since these devices already allow you to load a TCP/IP stack.*

To use the direct TCP/IP socket interface, the clients must use a special transaction ID ($IPT). The server recognizes this special transaction ID and starts these steps:

1. A TCP/IP client, such as a JANUS device, sends a transaction with the special transaction ID, $IPT.
2. The server DevComm recognizes the special transaction ID and routes it directly to a message handler queue (IPD).
3. The queue sends the transaction to the correct message handler IP Session Manager (ISM) thread. The ISM thread routes the transaction data to the socket that the client opened earlier.
4. The ISM thread reads data sent by the host through the socket and forwards the data to the client.

Direct TCP/IP Socket Interface



Direct TCP/IP API vs. NetComm API

By using the direct TCP/IP API, you no longer need to write applications that communicate with the peer-to-peer interface of the DCS 300. You write your client application to communicate with an existing TCP/IP server application. The server application does not even know the DCS 300 exists. All TCP/IP server applications that passively wait for connections can use the direct TCP/IP API without modifications. This way of exchanging data is more dynamic than the NetComm API.

The NetComm API requires that the application that is running on the host use the 96-byte header and the application must acknowledge all transactions and messages to the message handler. However, this API still provides a more reliable way of exchanging data. If the host goes offline, your users can continue to work, since the transactions are saved in a Hot Standby file. The transactions in each Hot Standby file are sent to the application (destination) when the host connection is re-established. When a direct TCP/IP API socket connection goes down, there is no data redundancy and the client or server application must re-establish the connection and retransmit the last transaction.

With the direct TCP/IP API, only the client can initiate the connection. Your host application must be a server application. Also, your host application must be able to handle connections from many devices at different times. By using the NetComm API with a single socket pair connection, the host application can communicate with as many devices as it needs to. The application receives data using transactions from many devices. Also, a device can easily send data to multiple destinations based on the type of transaction it generates.

With the direct TCP/IP API, each client can run multiple TCP/IP sessions; therefore, each client can have multiple socket connections. There is a one-to-one relationship between the session and the socket to the host. Each session has a unique identifier that the server TCP ISM (IP Session Manager) uses to manage these connections.

About the $IPT Transaction ID

$IPT is a special transaction ID that contains the protocol that allows JANUS RF devices and TRAKKER Antares terminals to communicate with the DCS 300 using the direct TCP/IP socket interface. Every transaction from a device needs $IPT as the transaction ID, which allows the server DevComm to route the data to the proper queue. When a device receives a transaction from the server, the transaction does not contain $IPT, but the protocol is the same.

$IPT offers these features:

- Client requests permission to open a socket. The client sends a data packet that contains the OPEN command, session ID, port number, host name, and maximum packet size to the server.
- Client receives a packet from the server that acknowledges the request.
  - Client receives an OPEN_NAK (negative acknowledgment) packet from the server, which indicates the request to open a socket has failed.
  - Client receives an OPEN_ACK (acknowledgment) packet from the server, which indicates the request to open a socket has succeeded.
- Client sends and receives data to and from the host through the server. The data packet contains the DATA command, the session ID, and the data.
- Client requests permission to close the socket or it receives a CLOSE packet from the server indicating that the connection is closed.

About the Host Application Requirements

The DCS 300 to host interface does not require any modifications. Host applications must be written using the standard TCP/IP socket interface. Also, host applications must be server applications; that is, they open a socket and wait for a client connection to arrive at the socket.

Using International Text Pass-Through

International text pass-through allows data streams representing characters encoded in various encoding schemes to pass through the DCS 300 without conversion between various hosts and devices. The data streams appear to the server as arbitrary streams of bytes passed between the hosts and devices. The hosts and devices are responsible for any necessary conversion of the characters. The server is responsible for configuring connections between the hosts and devices, establishing sessions, and routing transactions.

International text pass-through provides uniform pass-through support for the character encoding schemes used by the hosts and devices.

Host	Character Encoding Scheme
IBM	EBCDIC SBCS, DBCS
Unix	SBCS, DBCS, EUC
Windows NT	Unicode
JANUS devices	SBCS, DBCS
TRAKKER Antares terminals	SBCS, DBCS

Before you use this feature, note the following:

- The DCS 300 attaches a transaction header to messages that it receives from hosts and it attaches a transaction ID to route messages to and from devices. The text for the transaction header and the transaction ID are limited to what you can enter on the DCS 300. The text for the transaction data can be an arbitrary sequence of bytes representing text in any character encoding scheme.
- Configuration text that is passed between the DCS 300 and devices must use the ASCII character set.
- The DCS 300 supports limited mapping from EBCDIC code page 037 to PC code page 437. If the DCS 300 cannot look up the source of the transaction in the peer-to-peer destination list, the DCS 300 acts as if EBCDIC mapping is enabled and international text pass-through is disabled. However, if you check the international text pass-through check box, you disable this EBCDIC mapping.
- Mapping from arbitrary EBCDIC code pages to arbitrary PC code pages for the transaction data originating from an APPC peer-to-peer application is not supported.
- No conversions are necessary if you enable the time append feature.
- The DCS 300 does not support sort order, date, item, and currency.

Communicating With APPC Applications

You can use APPC applications to communicate between the DCS 300 and any other device on an SNA network. Before you write APPC applications, you should have some familiarity with APPC/LU 6.2 because APPC applications use APPC/LU 6.2 verbs to communicate with the server.

APPC applications, acting as remote requester applications, initiate the connection to the server. The server waits for the connection to be initiated. The remote applications can be receive, send, interactive, or batch applications.

Receive applications Receive applications only receive data. A receive application must act as a receive requester. It must send the server a valid application name when it connects. The application name must be identical to the name configured for it in the server.

Send applications Send applications only send data. A send application must act as a send requester. It can send transactions to the server without being configured in the server because the server will never send anything to it. The source application ID field in the transaction header is always blank.

Note: *The server's APPC receive NetComms only receive data in a maximum of 1120 byte chunks (96 bytes transaction header + 1024 bytes data). If more than 1120 bytes are received, an error is reported.*

Interactive applications A typical interactive application consists of the application, a send connect, and a receive connect.

Batch applications Batch applications are requester applications that receive batched data from the server. This data is collected while the application is not active and is stored in the Hot Standby file. The batch NetComm takes the Hot Standby file and sends the data upline faster than the normal interactive retrieval of data. Batch applications are ideal for applications that collect data only periodically and do not need to remain interactive. Batch applications are never interactive; they merely collect data.

APPC Verbs

APPC/LU 6.2 verbs allow the DCS 300 to communicate over an SNA network to other devices supporting APPC/LU 6.2. The server uses APPC to route the data between remote applications and itself. In an SNA network there are two parts to communications: the server and the host. The server takes care of communications on its side, but you must make sure you build the APPC verbs into your applications to handle communications on the host side. Intermec recommends that you have some familiarity with the APPC/LU 6.2 protocol.

These are the primary verbs that you can use to communicate with the server. For a description of their functions, see the *DCS 300 Technical Reference Manual*.

MC_ALLOCATE	MC_SEND_DATA	MC_SEND_ERROR
MC_CONFIRM	CONFIRM	CONFIRM
MC_CONFIRMED	FLUSH	FLUSH
MC_DEALLOCATE	DEALLOCATE	ABEND
MC_RECEIVE_AND_WAIT	NONE	RECEIVE_ALLOCATE
MC_REQUEST_TO_SEND		

IMS Applications

Older IMS applications, before version 4.0, do not support the MC_CONFIRMED or MC_SEND_ERROR verbs. Since IMS applications do not support these verbs, applications must send an acknowledge transaction back to partner programs by setting the acknowledge flag in the server's transaction header to "A."

NetComm Pairs

This table shows how your application links with a server NetComm. The NetComms are created when you configure your remote application on the server.

NetComm	Remote Application
Send Server	Host Receive Requester
Receive Server	Host Send Requester
Batch File Transfer	Host Batch File Transfer
IMS Send Server	IMS Host Receive Requester (before version 4.0)
IMS Receive Server	IMS Host Send Requester (before version 4.0)

To see the verb flow diagrams, see the *DCS 300 Technical Reference Manual*.

10

Using Terminal Sessions

Now that you have configured the DCS 300 to communicate with your LAN and you have configured your server to communicate with your Intermec network, you are ready to tie the entire data collection network together using an application.

This chapter explains how to set up VT, ANSI, 5250, or 3270 terminal sessions on your server. You can use these terminal sessions for running screen mapping as explained in Chapter 11, "Using Screen Mapping."

Chapter Checklist

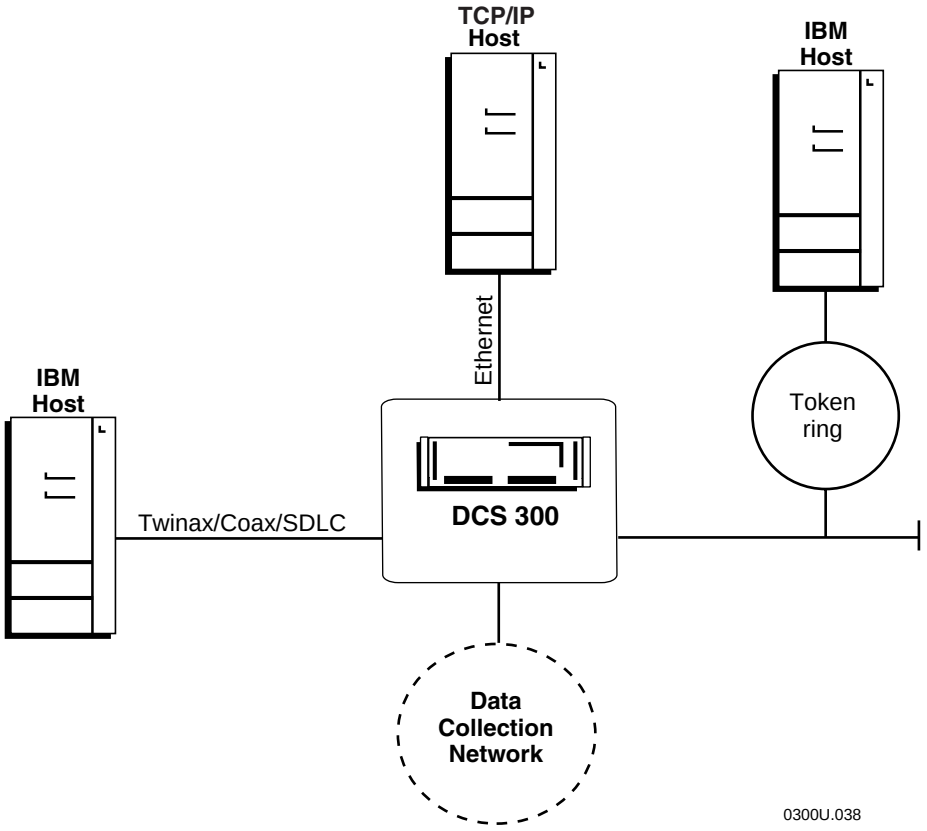
Done?	Task	Page
❑	Configure the host for terminal sessions	10-5
❑	Configure the VT terminal sessions on the DCS 300.	10-6
	Or,	
❑	Configure the 5250 terminal sessions on the DCS 300.	10-13
	Or,	
❑	Configure the 3270 terminal sessions on the DCS 300.	10-18
❑	Save and activate the configuration.	10-21
❑	Start a terminal session.	10-22
❑	(Optional) Map terminal keyboards to the DCS 300 keyboard	10-23

When you understand these sections and perform these tasks, you can start using the server.

About Terminal Sessions

You can establish VT, ANSI, 5250, or 3270 terminal sessions between the DCS 300 and your host. Use these sessions on the server to access your host directly from the server. By accessing your host, you can verify your host connection and you can start remote applications.

You can also use these sessions as screen mapping sessions. For help, see Chapter 11, "Using Screen Mapping."



Configuring the Host for Terminal Sessions

For VT, ANSI, 5250 or 3270 terminal sessions, there are relationships between emulation modes and network adapter cards. This section outlines the network administrator tasks for the special relationships between emulation modes and cards. This table lists the emulation modes and the network adapter cards they support.

Emulation Mode	Ethernet	Token Ring	Coaxial	Twinaxial	SDLC
VT100/220/320	Yes	Yes	No	No	No
ANSI	Yes	Yes	No	No	No
5250	Yes	Yes	No	Yes	Yes
3270	Yes	Yes	Yes	No	Yes

Setting Up 5250 Terminal Sessions Using SDLC

If you are setting up 5250 terminal sessions over an SDLC link, your network administrator can manually create the controller on the host or set up the AS/400 so that it will automatically create a controller. Your network administrator can also automatically or manually create a device that goes with the controller. When configuring the SDLC adapter card, you need to know these parameters:

- the station address
- whether the attached line is a switched (dialed) or non-switched (leased) line
- the maximum frame size

Setting Up 3270 Terminal Sessions Using Ethernet

If you are setting up 3270 terminal sessions over an Ethernet network, your network administrator needs to create a controller remote workstation and then a device to go with the controller on the host. The device definition provides the local location address (NAU) for the DCS 300. You need to know this parameter when configuring the DCS 300.

Setting Up 3270 Terminal Sessions Using SDLC

If you are setting up 3270 terminal sessions over an SDLC link, your network administrator needs to create a controller and then a display on the host. When configuring the SDLC adapter card, you need to know these parameters:

- the station address (2-digit hexadecimal number)
- the attached non-switched line, which is the line that is connected directly to the DCS 300
- the maximum frame (I) size
- the local location address (NAU) for the DCS 300, which is the display that your network administrator creates

Creating Terminal Sessions

This section explains how to define the communications parameters for the VT, ANSI, 3270, and 5250 terminal sessions between the DCS 300 and your host. You can use these sessions to access the host from the server or you can use them for screen mapping sessions.

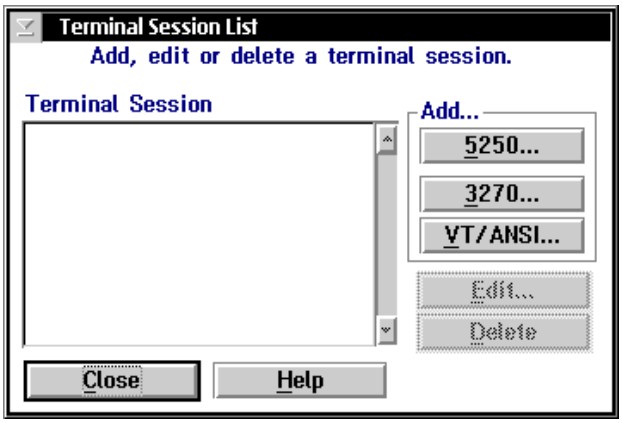
One terminal session on the server can communicate with one terminal emulator session running on the host. However, the terminal session on the server can receive transactions from multiple devices.

Before you proceed, make sure you have performed these tasks:

- Install the DCS 300.
- Install and configure the connection points and downline devices.
- Configure the network adapter cards.

To create a terminal session

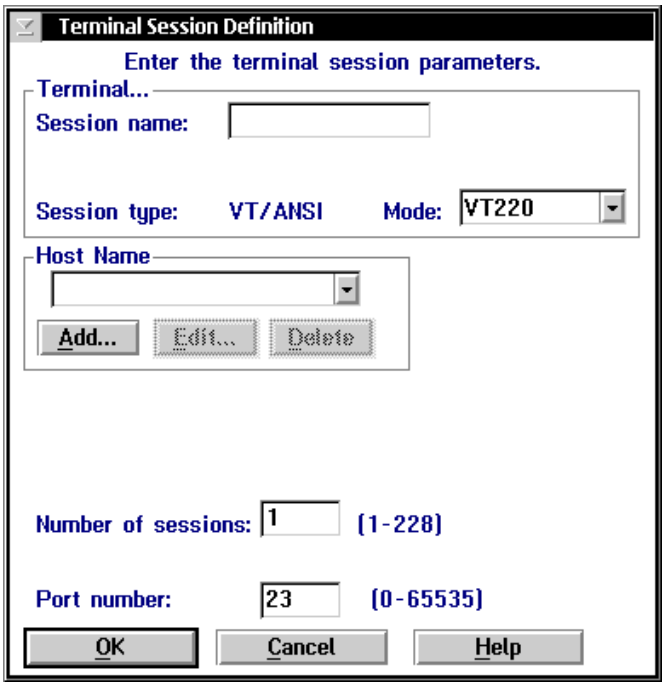
1. From the main menu, choose Terminal Session.
2. Choose Host Connection. The Terminal Session List dialog box appears.



3. Add, edit, or delete terminal sessions. For help, see “Adding a VT/ANSI Terminal Session,” “Adding a 5250 Terminal Session, ” or “Adding a 3270 Terminal Session” later in this chapter.
4. Choose Close to close the dialog box and return to the main menu.

Adding a VT/ANSI Terminal Session

- From the Terminal Session List dialog box, choose VT/ANSI. The Terminal Session Definition dialog box appears.



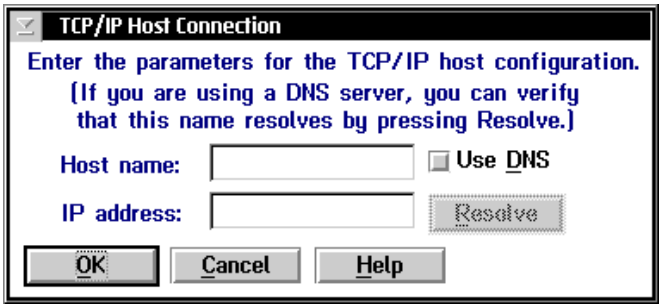
Field	Description	Value	Default
Session name	A meaningful name for this terminal session.	1 to 8 alphanumeric characters	None
Mode	The type of terminal mode that you want to use for this terminal session.	VT100, VT220, VT320, ANSI	VT220
Host Name	The name of the TCP/IP host to which the terminal session connects. For help adding a host, see "Adding a TCP/IP Host" in the next section.	Predefined	None
Number of sessions	The number of terminal sessions that you want to run on the server.	1 to 228	1
Port number	The port number that this session uses to communicate with the telnet daemon on the host. ***Note:*** *Telnet uses port number 23.*	0 to 65535	23

Adding a TCP/IP Host

To communicate with TCP/IP hosts, the DCS 300 needs to know their IP addresses. You can either use DNS to resolve these IP addresses or you can enter them in manually.

To add a TCP/IP host

- From the Terminal Session Definition dialog box, choose Add. The TCP/IP Host Connection dialog box appears.



Field	Description	Value	Default
Host name	The name that logically identifies the TCP/IP host to the network.	1 to 256 alphanumeric characters	None
Use DNS	This check box determines if you use a DNS server to resolve the IP address of this host. ***Note:*** *Before you check this check box, you must first configure a DNS server in the DNS Configuration dialog box.*	Check, Clear	Clear
IP address	The address that identifies the TCP/IP host to the network. This IP address must be a valid IP v4 address.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	None

To determine the host IP address using DNS

1. In the Host name field, enter the abbreviated or long host name. If you enter the abbreviated name, the server searches the domain names in the DNS Configuration dialog box to determine the long host name.
2. Check the Use DNS check box.
3. (Optional) Choose Resolve. The server searches for the host name in the domains that are listed in the DNS Configuration dialog box and resolves the IP address.
4. Choose OK to save your changes and return to the Terminal Session Definition dialog box.

To configure the host IP address manually

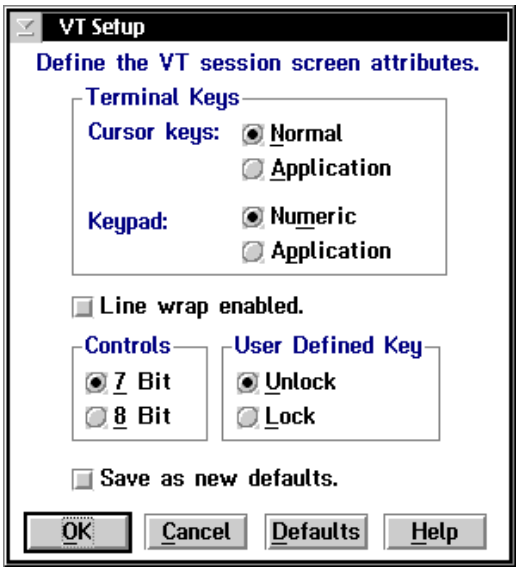
1. In the Host name field, enter the host name.
2. Make sure the Use DNS check box is cleared.
3. In the IP address field, enter the host's IP address.
4. Choose OK to save your changes and return to the Terminal Session Definition dialog box.

Customizing the VT Terminal Setup

When you add a new VT or ANSI terminal session and then you choose OK, a message box appears asking if you want to use the Default or Custom VT terminal setup. If you choose Default, you return to the Terminal Session List dialog box.

If you choose Custom, the VT Setup dialog box appears. If you have already created a terminal session and you want to edit the fields in this dialog box, from the Terminal Session list box, select the terminal session and then choose Edit. The Terminal Session Definition dialog box appears. Choose the Edit button that appears above the Terminal mode field. The VT Setup dialog box appears.

Note: *If you are defining VT100 terminals, the option buttons in the Controls box and the User-Defined Key box are grayed out.*



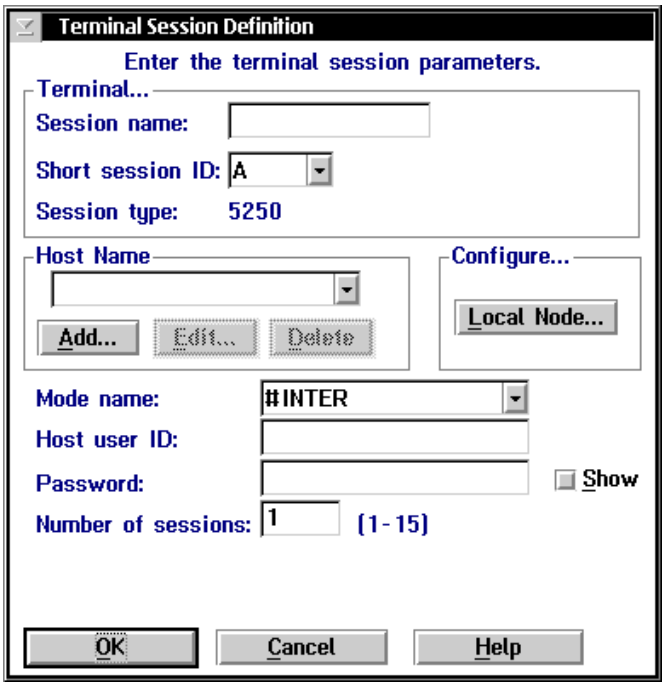
Field	Description	Value	Default
Cursor keys	Determines whether the arrow keys on the terminal control cursor movement (normal) or they send their application control functions (application).	Normal, Application	Normal
Keypad	Determines whether the number keys on the terminal send their keycap characters (numeric) or they send their programming functions (application).	Numeric, Application	Numeric
Line wrap enabled	This check box determines if text automatically wraps to the next line when it reaches the right margin. If this check box is clear, when the cursor reaches the right margin, the terminal displays each new character in the last column of the line. Each new character overwrites the previous character.	Check, Clear	Clear
Controls	Defines the type of control characters that your terminal uses. Choose 7-bit if you want the terminal to use all the VT320 features. Choose 8-bit if you want the terminal to support 8-bit graphic display characters and 7-bit control characters. Choose 8-bit for all VT220 applications.	7 bit, 8 bit	7 bit
User-Defined Key	Determines whether or not the host can change the user-defined keys. Choose Unlock if you want the host to be able to add or to change the user-defined key definitions.	Unlock, Lock	Unlock
Save as new defaults	This check box determines if the current parameter settings are used as the default parameter settings.	Check, Clear	Clear

Adding a 5250 Terminal Session

Use this dialog box to configure 5250 terminal sessions between your DCS 300 and your host. You also need to define terminal sessions that you can use for screen mapping sessions. You need to identify the server to the SNA network. For help, see "Configuring the SNA Local Node" later in this chapter.

To add a 5250 terminal session

- From the Terminal Session List dialog box, choose 5250. The Terminal Session Definition dialog box appears.



Note: *If you set a password and you choose OK and leave this dialog box, the Show check box does not appear if you edit this session. To change your password, delete all the asterisks in the Password field. The Show check box reappears. Enter a new host user ID and password.*

Field	Description	Value	Default
Session name	A meaningful long session ID that identifies this terminal session.	1 to 8 alphanumeric characters	None
Short session ID	The alpha identifier for this terminal session.	1 alpha character	A or the next available alpha character
Host Name	The name of the host to which the terminal session connects. For help adding a host, see "Adding an IBM SNA Host" in the next section. If you delete a terminal session, the host name associated with that session still exists.	Predefined	None
Mode name	This name describes the class of service and other session characteristics that you may want for your network. Use the #ACCNET mode for systems that need a larger session limit (up to 128). This mode, unlike the other ones in the predefined list, is not a default mode and your network administrator will have to create it on the host. For more help on #ACCNET, see the *DCS 300 Technical Reference Manual*.	Predefined	#INTER
Host user ID	The user ID that lets you log into the host.	1 to 10 alphanumeric characters, first character is alpha	None
Password	The password that goes with the user ID that lets you log into the host.	1 to 10 alphanumeric and special characters, first character is alpha	None
Show	This check box determines if your password appears in the Password field. If you clear the Show check box, asterisks appear instead of the keys you are typing. If you check the Show check box, the keys you are typing appear in the field.	Check, Clear	Clear
Number of sessions	The number of terminal sessions you want to configure to this host.	Non-coax - 1 to 15 Coax - N/A	1

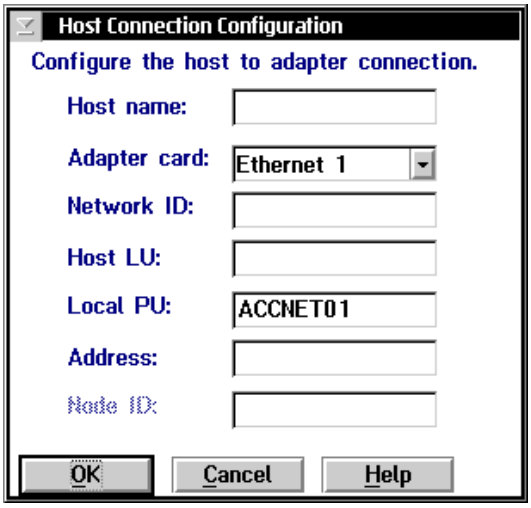
Adding an IBM SNA Host

You need to identify any hosts you want the DCS 300 to communicate with for your terminal sessions. When you add a host, you set up a link to a specific host and this information is available throughout the system. Once you create a host connection, you may use it for any SNA configurations. If you delete a terminal session, the host name associated with that session still exists. Only one host connection is allowed for coaxial, twinaxial, and SDLC network adapter cards.

The server maintains separate lists for 3270 hosts and 5250 hosts. If you create a host when defining a 5250 terminal session, you cannot use this host when defining a 3270 terminal session.

To add an IBM SNA host

- From the Terminal Session Definition dialog box, choose Add. The Host Connection Configuration dialog box appears.



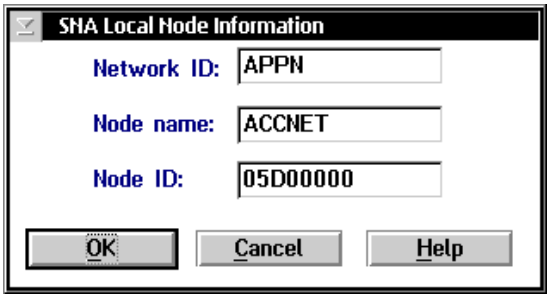
Field	Description	Value	Default
Host name (Optional)	A name that identifies this SNA host. You use this internal name to make the host LU name more meaningful.	1 to 8 alphanumeric characters	None
Adapter card	The network adapter card you are using to connect to the host.	Ethernet, token ring, twinaxial, SDLC	Ethernet 1
Network ID	Identifies the network ID on which the host resides. This ID must match the network ID configured on the host.	1 to 8 alphanumeric characters	DCS 300 network ID from the local SNA node definition
Host LU	The LU name that identifies the host. This parameter must match the control point (CP) name or node name of the host. This name is known throughout the SNA network.	1 to 8 alphanumeric and special characters	Host name
Local PU (TE only)	A unique PU name for the host that allows the terminals, when running TE, to communicate with more than one host using the same upline adapter card.	8 uppercase alphanumeric or special characters The first character must be an alpha character.	SNA node name + 2-digit suffix, starting with 01
Address (Ethernet or token ring only)	The LAN adapter address of the host. For help, see "Converting Ethernet Addresses to Token Ring MAC Format" in Appendix B.	Token ring MAC address format	None

Configuring the SNA Local Node

These parameters identify the DCS 300 to the SNA network. Once configured, these parameters apply system-wide for all SNA connection types and you do not need set them again.

To configure the SNA local node

- From the Terminal Session Definition dialog box, choose Local Node. The SNA Local Node Information dialog box appears.



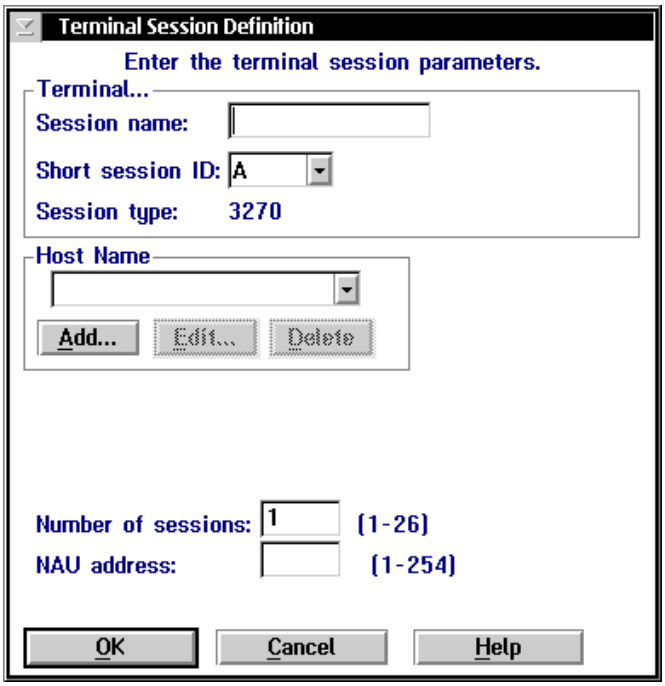
Field	Description	Value	Default
Network ID	The unique name of the SNA network. This ID is used for problem notification.	1 to 8 alphanumeric characters	APPN
Node name	The name that other nodes use to address the server. This name is also the default LU and must be unique to the SNA network.	1 to 8 alphanumeric and special characters	ACCNET
Node ID	Specifies the last eight characters in the host XID that are used for establishing a connection with the server. ***Note:*** *When establishing a connection, the host or server with the higher Node ID number is the primary workstation.*	8 hexadecimal characters	05D00000

Adding a 3270 Terminal Session

Use this dialog box to configure terminal sessions between your DCS 300 and your host. You also need to define terminal sessions that you can use for screen mapping sessions. You need to identify the SNA local node. For help, see "Configuring the SNA Local Node" earlier in this chapter.

To add a 3270 terminal session

- From the Terminal Session List dialog box, choose 3270. The Terminal Session Definition dialog box appears.

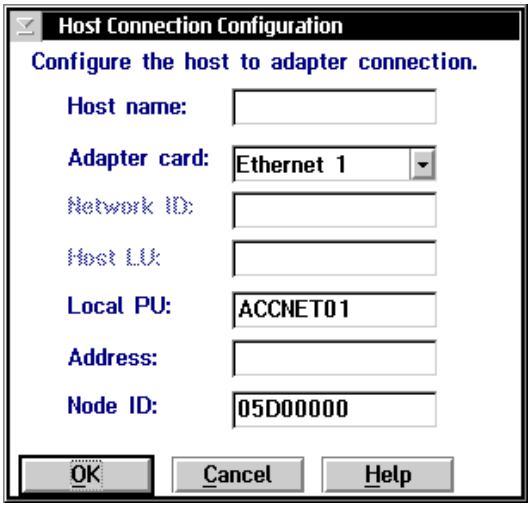


Field	Description	Value	Default
Session name	A meaningful long session ID that identifies this terminal session.	1 to 8 alphanumeric characters	None
Short session ID	The alpha identifier for this terminal session.	1 alpha character	A or the next available alpha character
Host Name	The name of the host to which the terminal session connects. For help adding a host, see "Adding an IBM SNA Host" in the next section.	Predefined	None
Number of sessions	The number of terminal sessions you want to configure to this host.	Non-coax - 1 to 26 Coax - 1 to 4	1
NAU address	The network addressable unit (NAU) that is specified for the workstation LU name.	001 to 254	None

Adding an IBM SNA Host

You need to identify any hosts you want the DCS 300 to communicate with for your terminal sessions. When you add a host, you set up a link to a specific host and this information is available throughout the system. Once you create a host connection, you may use it for any SNA configurations. If you delete a terminal session, the host name associated with that session still exists. Only one host connection is allowed for coaxial, twinaxial, and SDLC network adapter cards.

The server maintains separate lists for 3270 hosts and 5250 hosts. If you create a host when defining a 5250 terminal session, you cannot use this host when defining a 3270 terminal session.



Field	Description	Value	Default
Host name (Optional)	A name that identifies this SNA host. You use this internal name to make the host LU name more meaningful.	1 to 8 alphanumeric characters	None
Adapter card	The network adapter card you are using to connect to the host.	Ethernet, Token Ring, Coaxial, SDLC	Ethernet 1
Local PU (TE only)	A unique PU name for the host that allows the terminals, when running TE, to communicate with more than one host using the same upline adapter card.	8 uppercase alphanumeric or special characters The first character must be an alpha character.	SNA node name + 2-digit suffix, starting with 01
Address (Ethernet or token ring only)	The LAN adapter address of the host. For help, see "Converting Ethernet Addresses to Token Ring MAC Format" in Appendix B.	Token ring MAC address format	None
Node ID	Specifies the last eight characters in the host XID that are used for establishing a connection with the server. The Node ID is the same as the XID. ***Note:*** *When establishing a connection, the host or server with the higher Node ID number is the primary workstation.*	8 hexadecimal characters	05D00000

Saving and Activating Your Run-Time Configuration

When you are done configuring your terminal sessions, you should save your changes. If you are done configuring the server, activate your run-time configuration. When the activate is complete, a message box appears if you need to reboot the server.

To save and activate your run-time configuration

1. From the main menu sidebar buttons, choose Save and Activate. The Activate Configuration message box appears.
2. Choose Activate. The server saves your runtime configuration to disk and it becomes your active configuration.

If you are ready to start data collection, from the main menu sidebar buttons, choose Start Data Collection.

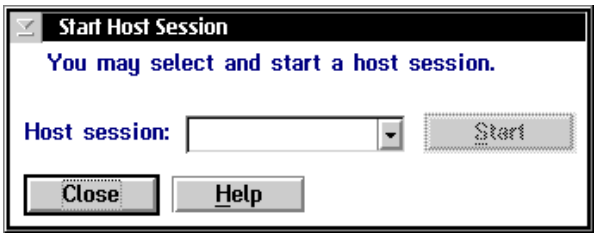
Starting a Host Session

You can start host sessions between the DCS 300 and your host. Use the session on the server to access your host directly from the server. By accessing your host, you can verify your host connection and you can start remote applications.

If you have purchased screen mapping, you can use these sessions to retrieve information about host screen fields and regions. When configuring screen mapping sessions, you tie a host session to a script file. For help, see Chapter 11, "Using Screen Mapping."

To start a host session

1. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
2. In the System Maintenance list box, select Start Host Session and then choose Start. The Start Host Session dialog box appears.



3. In the Host session field, click the down arrow on the right side of the field. A list of the terminal sessions you have configured appears. Select the session you want to start.
4. Choose Start. The host session starts and the host window appears.
5. Choose Close to close the dialog box and return to the System Maintenance dialog box.
6. Choose Close to return to the main menu.

Mapping Terminal Keyboards to the DCS 300 Keyboard

Use these diagrams to help you map terminal emulation keys that you find on a standard terminal emulation keyboard to the DCS 300 keyboard.

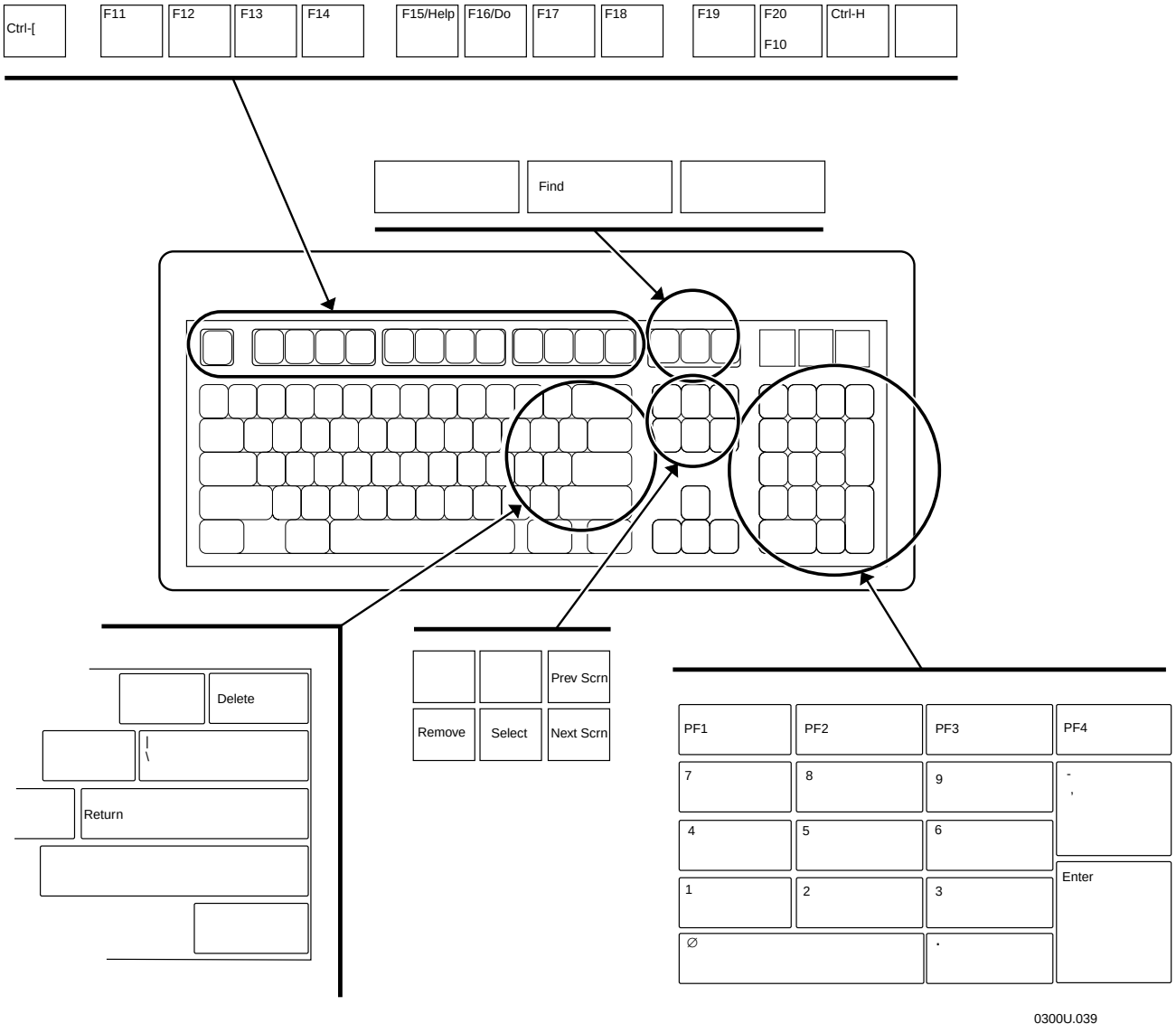
To use the diagrams

1. Locate the keyboard diagram for your application.
2. On the keyboard diagram, locate the function you want to perform and note its position on the key.
3. Using the key combination legend below the diagram, find the function's position on the key (column and row).
4. Press and hold the key from the legend and then press the key that performs the action.

For example, you are running VT/ANSI terminal emulation and you want to type bar (|). Press and hold the **Shift** key while pressing the **backslash** (\) key.

For example, you are running 3270 terminal emulation and you want to perform an undo. Undo is a function of the **BckSpc** key and it is printed on the key in the first column and the third row. In the legend, this location corresponds to the **Alt** key. Press and hold **Alt** and then press **BckSpc**.

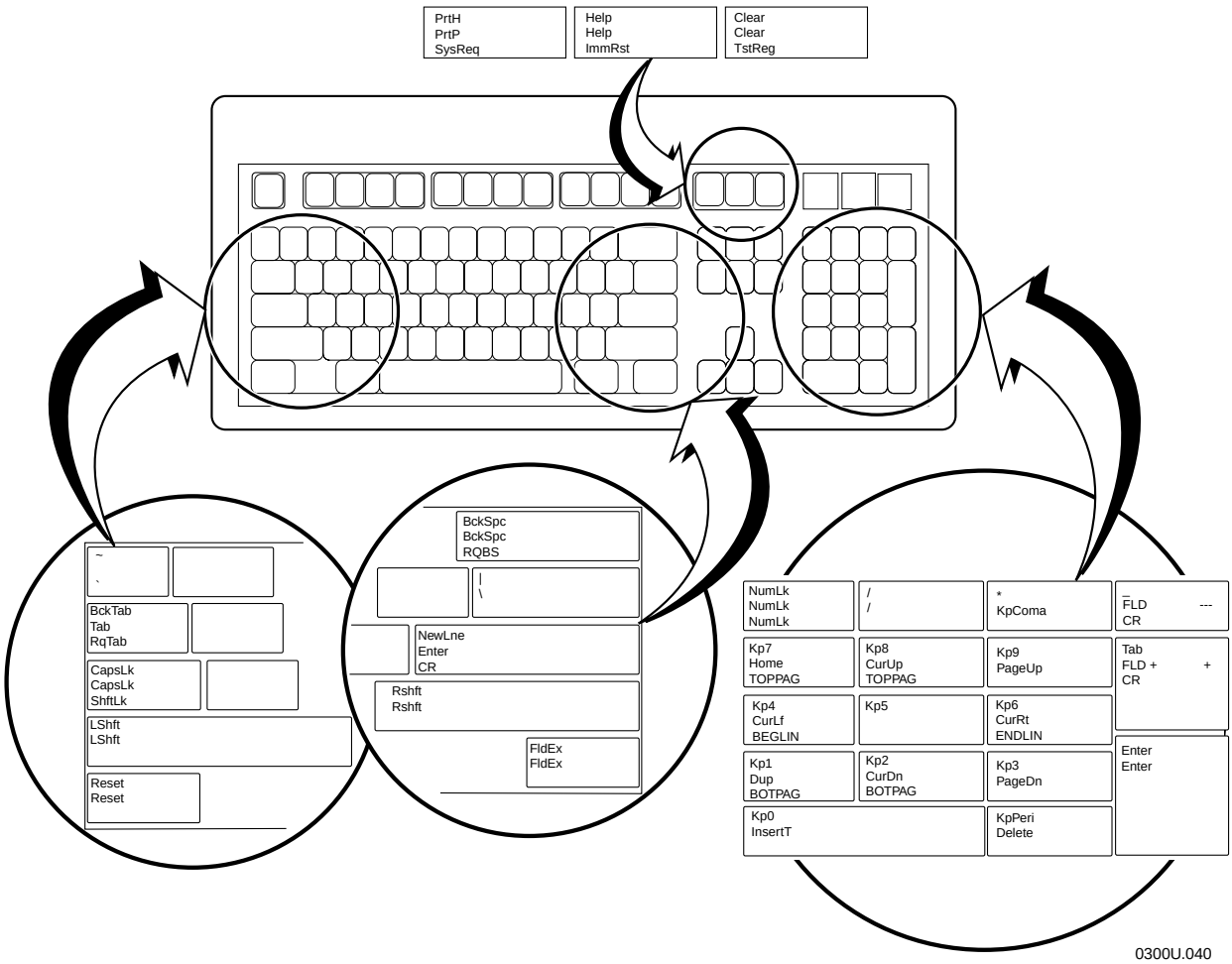
VT/ANSI Terminal Keyboard



Key Combination Legend

Shift
Base

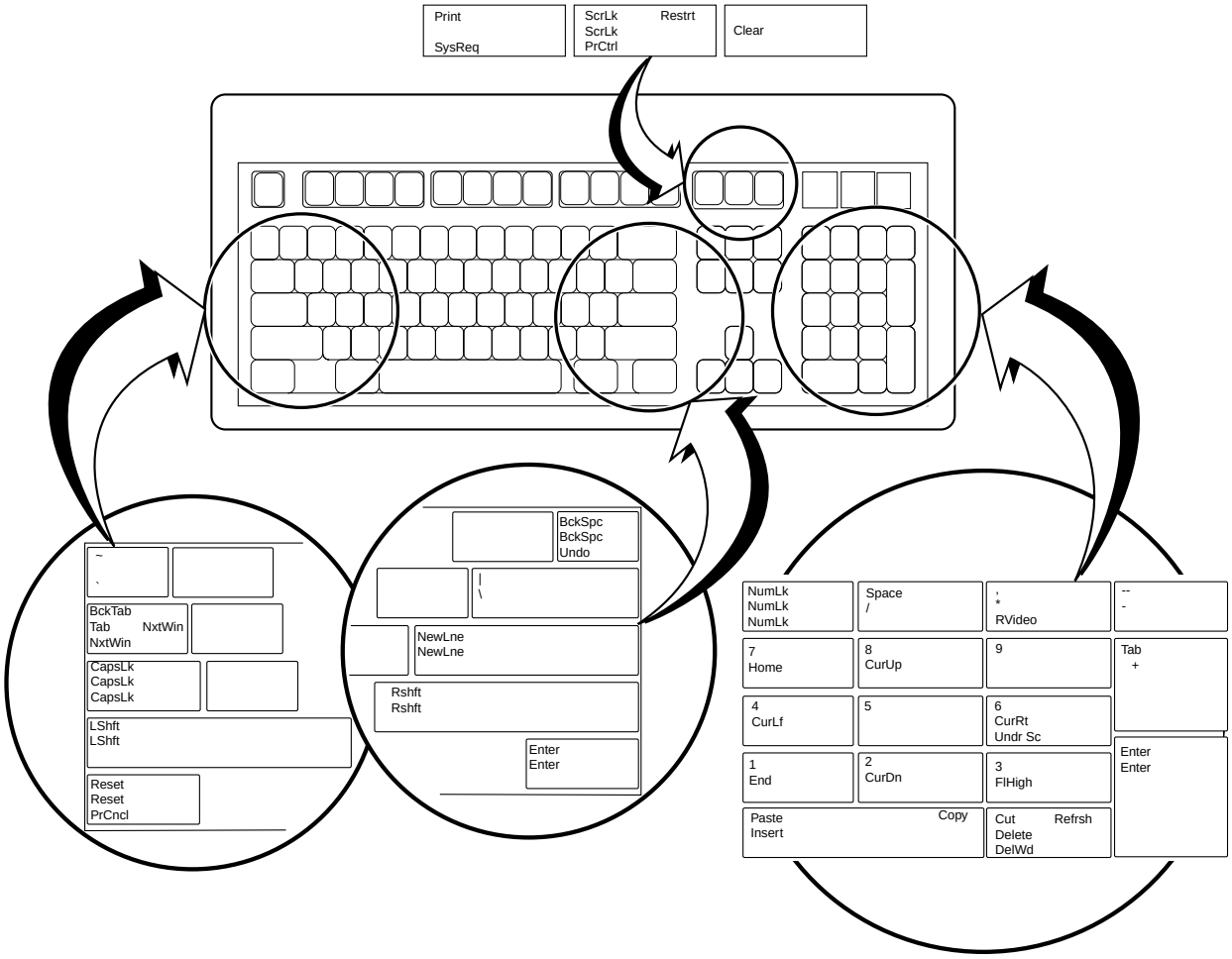
5250 Terminal Keyboard



Key Combination Legend

Shift	Ctrl
Base	AltGr
Alt	

3270 Terminal Keyboard



0300U.042

Key Combination Legend

Shift	Ctrl
Base	AltGr
Alt	Alt+Shift

11

Using Screen Mapping

Now that you have configured the DCS 300 to communicate with your LAN and you have configured your server to communicate with your Intermec network, you are ready to tie the entire data collection network together using screen mapping. Before you can run screen mapping, you need to have defined your terminal sessions in Chapter 10, "Using Terminal Sessions."

This chapter explains how to create script files for screen mapping. It also explains how to define screen mapping sessions that match a terminal session with a script file. You must use another program to create the application that runs on your devices.

Chapter Checklist

Done?	Task	Page
❑	Create a new or open an existing script file.	11-17
❑	Set global options for the current script.	11-22
❑	Create standard sequences for starting and ending screen mapping sessions.	11-26
❑	Define all transactions that the current script uses.	11-32
❑	Select a current transaction.	11-32
❑	Define all the host screens that receive data from the current transaction.	11-33
❑	Select a current host screen.	11-33
❑	Define all host screen fields, regions, and messages for the current host screen.	11-36
❑	Repeat the preceding two steps until you have defined all host screen fields, regions, and messages for all host screens that receive the data from the current transaction.	
❑	Repeat the preceding six steps until you have defined all transactions.	
❑	Determine the order of events.	11-54
❑	Define user blocks.	11-61

Chapter Checklist (continued)

Done?	Task	Page
❑	View and check the script.	11-64
❑	Map the transaction fields to the host screen fields.	11-74
❑	Save the configuration.	11-76

When you understand these sections and perform these tasks, you can start using the server.

About Screen Mapping

Screen mapping lets you map transaction fields from a JANUS device, a TRAKKER Antares terminal, or a 6400 to different host screen fields in a host application.

On the DCS 300, you use the Script Builder Tool to create a script file that the server uses to map transaction fields from the devices to host screen fields. You can also use the Script Builder Tool to create logon and logoff sequences in host screens, handle regions (such as error messages) on host screens, and send messages back to the source of the transaction, such as a terminal.

On the DCS 300, you also must create screen mapping sessions that define specific transactions to be sent to a specific host terminal session using a specific script file. Screen mapping sessions allow multiple terminal sessions on the server to simultaneously communicate with multiple terminal emulator sessions running on different hosts.

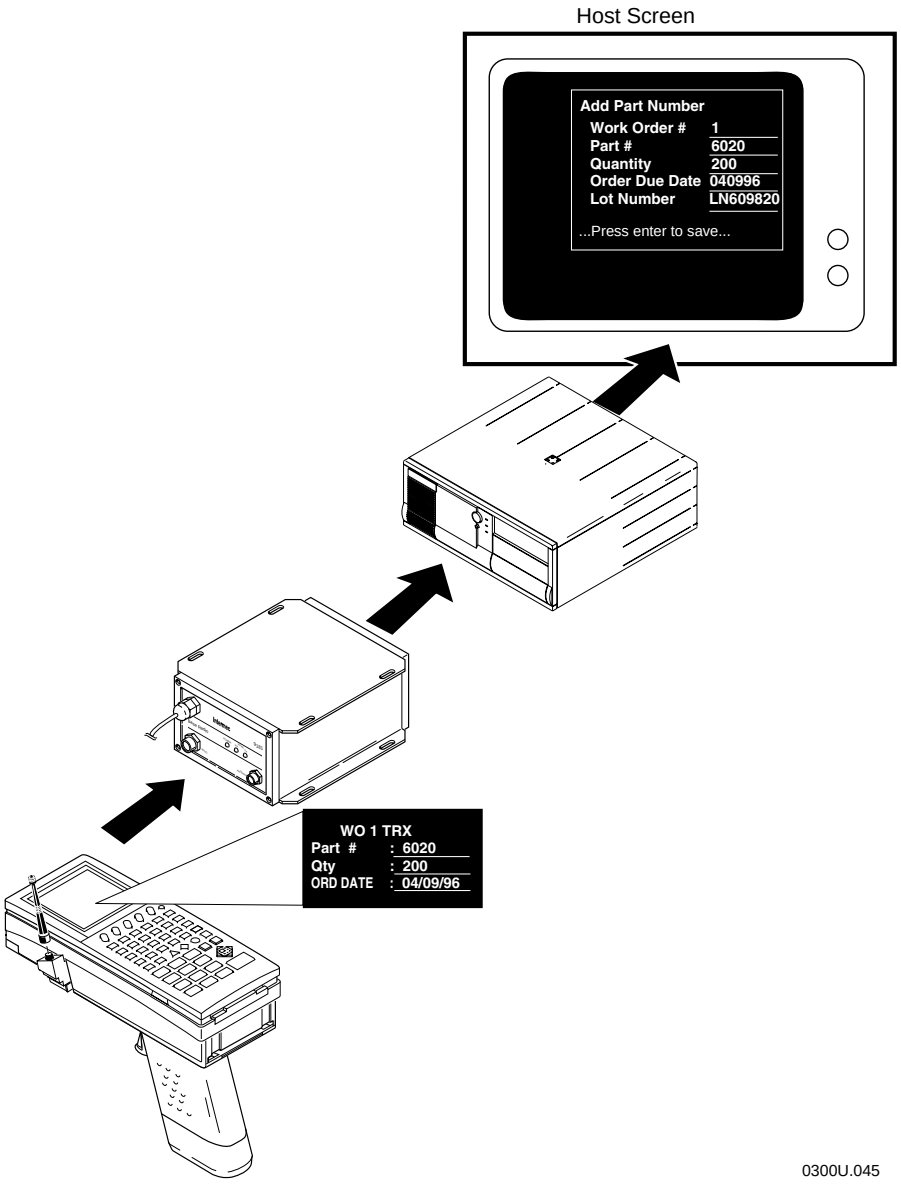
To create an application that runs on your devices:

- For TRAKKER Antares terminals, you can use the C programming language. Intermec recommends that you use EZBuilder, which is a fast, easy-to-use development tool that creates applications. You can use it to create menus, screens, data fields, labels, transactions, and other processing functions. For more information, contact your local Intermec respresentative.
- For JANUS devices and WTP devices, you can use C++ or any other standard programming language.

Note: *Transactions sent by TRAKKER Antares terminals and JANUS devices and running in the Intermec 2.4 GHz RF network have a maximum length of 1024 characters, including delimiters. Transactions sent by JANUS devices running in the Intermec 900 MHz RF network have a maximum length of 254 characters, including delimiters.*

This figure shows data originating from a JR2020 being sent through a BRU to the server to a host application running in a terminal emulator.

Typical Screen Mapping Application



About Script Files

Script files contain the logic for mapping the transaction data that is exchanged between devices and a host. Using script files, the DCS 300 maps transaction fields into host screens. Intermec has designed the Script Builder Tool as a GUI tool that lets you easily create, edit, and check script files.

Intermec recommends that you use the Script Builder Tool to create your scripts and define user blocks to customize it. If you manually create a script, you cannot open and edit this script using the Script Builder Tool. For help manually creating a script, see the *DCS 300 Technical Reference Manual*.

Preparing to Use the Script Builder Tool

Before you start using the Script Builder Tool, you should identify the tasks that you want the script to perform. You must know

- the transactions that the script will process. You should also design one terminal screen for each transaction.
- the starting point (host screen) for all transactions.

  If the script is going to handle only one transaction, the main host screen is the screen that contains the host screen field that will receive the first transaction field mapping.

  If the script is going to handle multiple transactions, the main host screen is the screen that contains the different options, such as a menu, where you can choose different options that send different transactions.
- the host screens and host screen fields that will receive transaction data, such as data entry screens.
- the host screens and host screen fields that will output data, such as inquiry result screens.

Single Transaction Script Files vs. Multiple Transaction Script Files

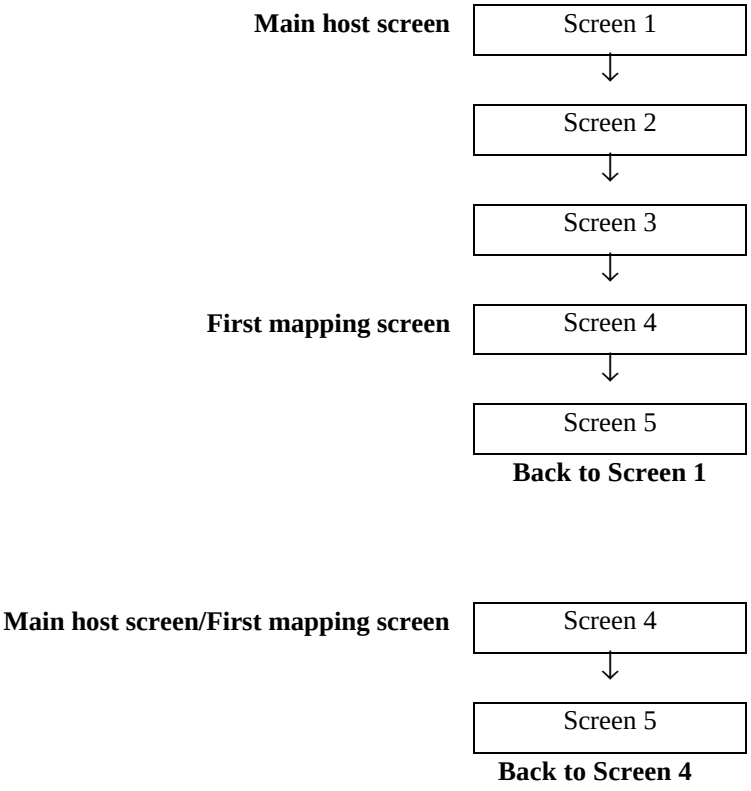
You can build a script file that contains only one transaction or you can build a script file that contains many transactions, as long as they all branch from one host screen. A single transaction script file is the easiest to build. However, if you have too many single transaction script files running at the same time, you can use up system resources and the server performance may slow down. Each script file requires a dedicated screen mapping session to run.

A multiple transaction script file lets you process many transactions (one at a time) using one screen mapping session. You should group transactions that are logically related. If you watch the host terminal session while a script file is running, you will notice that when the script file maps the transaction, it always starts from the main host screen. It returns to the main host screen after it maps the last transaction field. You need to consider how much time it takes to get from the main host screen to the first host screen that receives the first transaction field mapping.

Each type of script file has advantages and disadvantages. Generally, it is better to use a multiple transaction script file as long as you carefully group transactions to minimize overhead.

The next illustration shows how using a single transaction script file can reduce overhead on the system. The first part of illustration shows a multiple transaction script file. The transaction starts from the main host screen (Screen 1) and goes through three screens before the first mapping of a transaction field to a host screen field occurs. The second part of the illustration shows a single transaction script file. The main host screen is the screen where the first mapping occurs.

Multiple Transaction Script vs. Single Transaction Script Example



Identifying Key Elements for the Script File

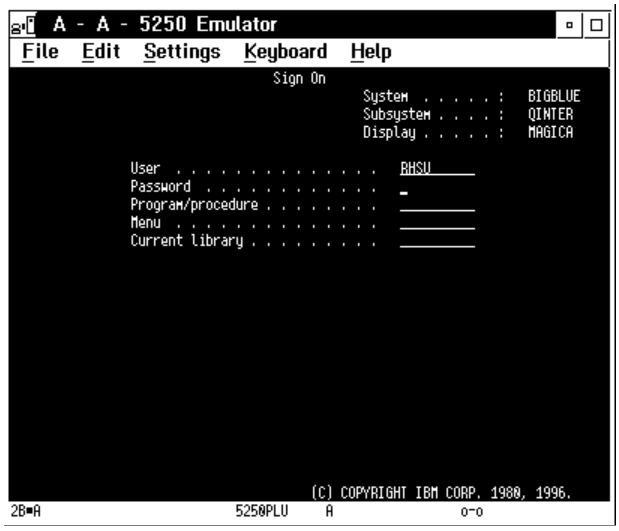
Before you create your screen mapping application, you need to be able to identify key elements, such as the main host screen, transactions, and host screen fields, for the script file. You also need to decide if your tasks will use single transaction script files or multiple transaction script files. Use these examples to help you determine how to structure your script file.

Example 1 - Single Transaction Script File

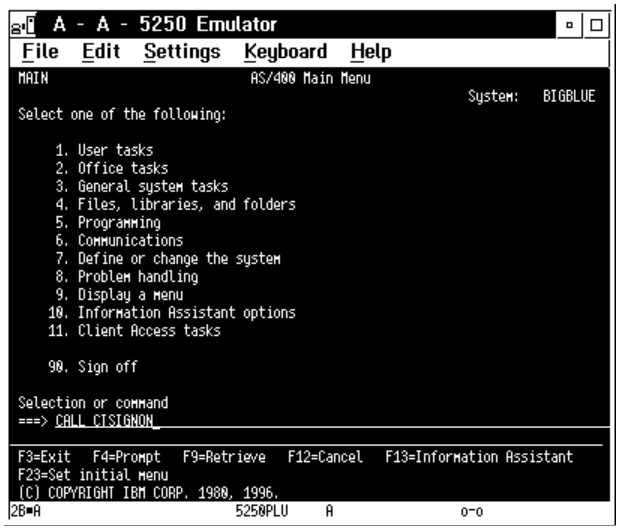
In this example, the script file will log on to the AS/400 and invoke an MRP application called Data 3 Systems to add a work order. This task will be performed using one transaction.

To complete the work order add transaction, a user will need to enter the work order part number in Screen 4, and the quantity and order due date in Screen 5. These fields will require the script file to map transaction data to them. Since this is a single transaction script file, the main host screen is the first screen (Screen 4) that has transaction data mapped to it.

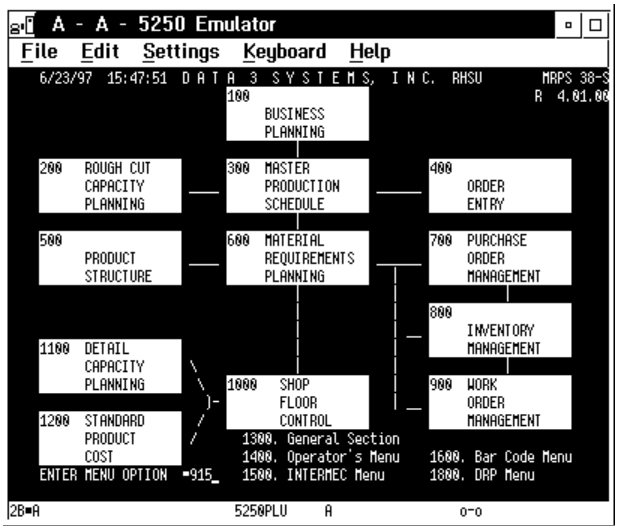
Screen 1



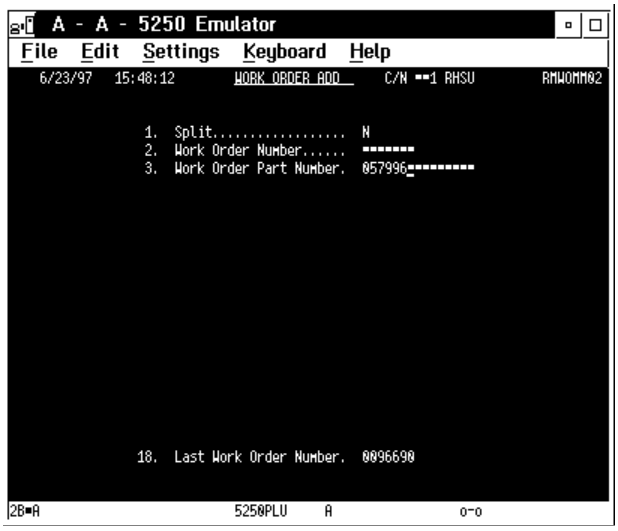
Screen 2



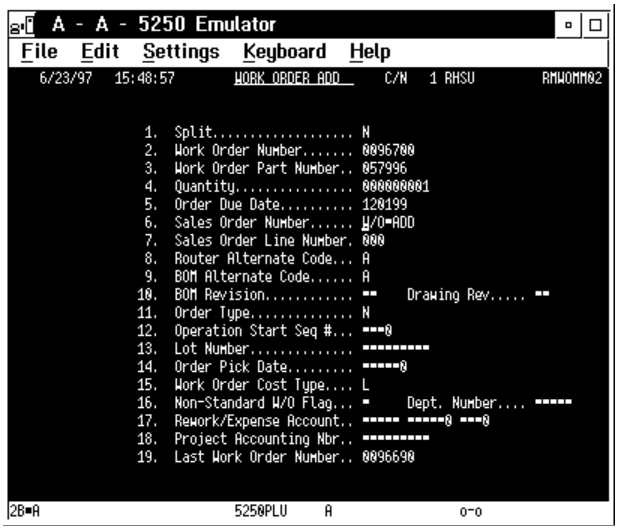
Screen 3



Screen 4 (Main Host Screen)



Screen 5



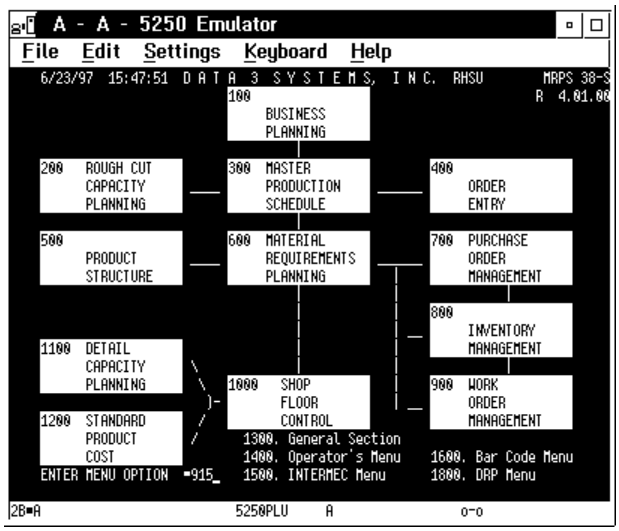
Example 2 - Multiple Transaction Script File

This example adds another transaction to Example 1. Besides the work order add transaction, the script file processes a work order quantity inquiry transaction. The result of the query is sent back to the application that is running on the terminal.

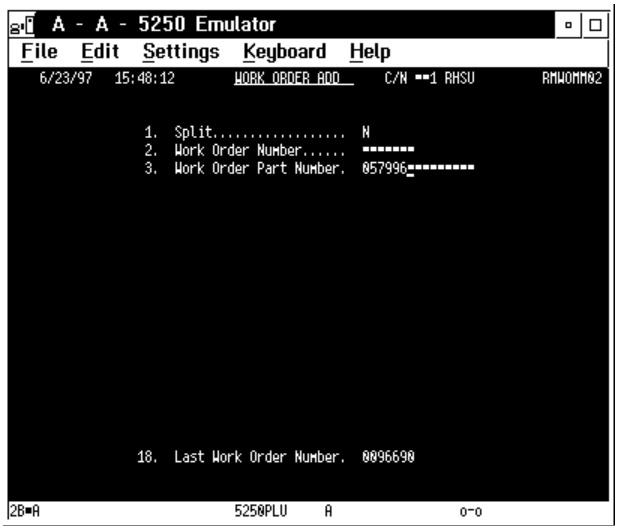
These screens show two transaction paths branching from Screen 3. If you enter 915 in the Enter Menu Option field of Screen 3, you will go to Screen 4 to process the work order add transaction. However, if you enter 910, you will go to Screen 6 to process the work order quantity inquiry transaction. Screen 3 is the central starting point for both transactions and therefore, it is the main host screen.

The work order quantity inquiry transaction requires you to enter the work order in Screen 6 to start the inquiry. Therefore, the Work Order field will require the script file to map transaction data to it. Screen 7 shows the result of the inquiry. The number in the Order Qty field will be sent back to the terminal application. Therefore, the Order Qty field is an output region. The query result will be sent back to the terminal using a transaction message. To learn how to define a transaction message, see "Adding a Message" later in this chapter.

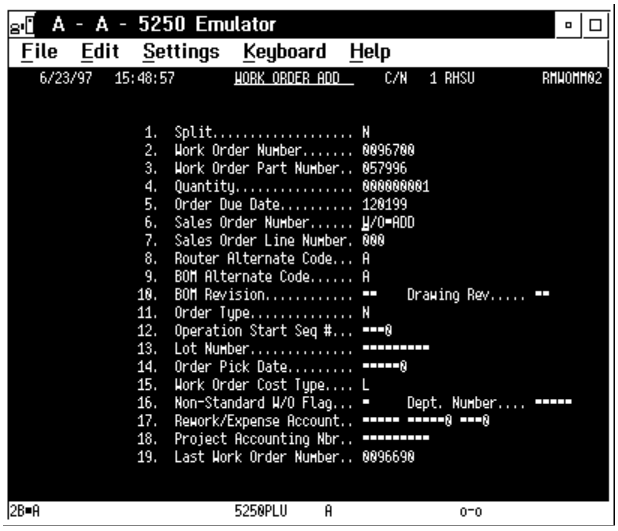
Screen 3 (Main Host Screen)



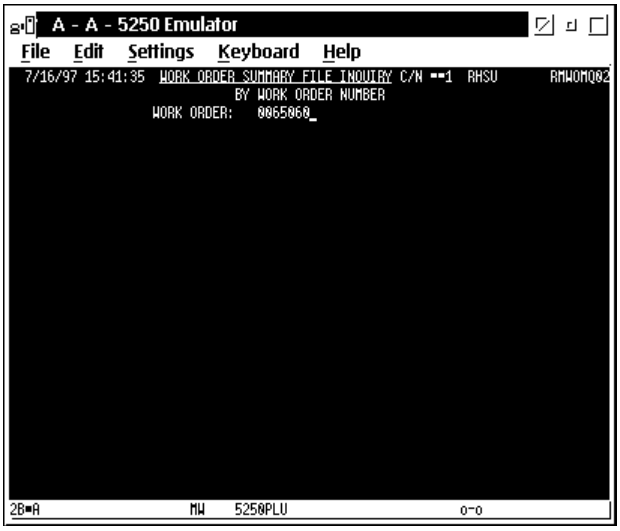
Screen 4 (Menu Option 915)



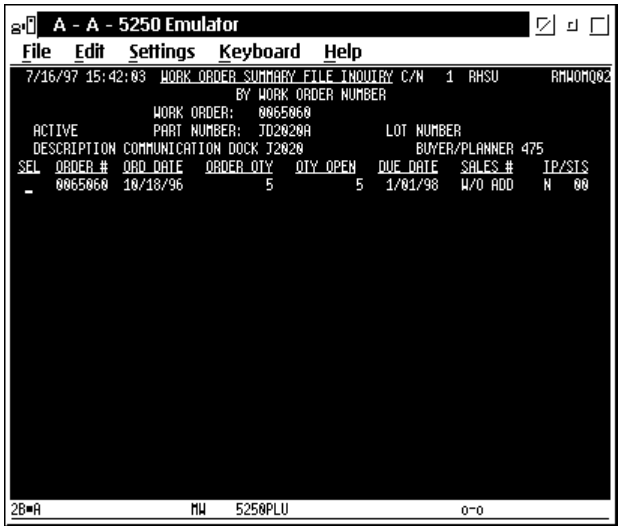
Screen 5



Screen 6 (Menu Option 910)



Screen 7

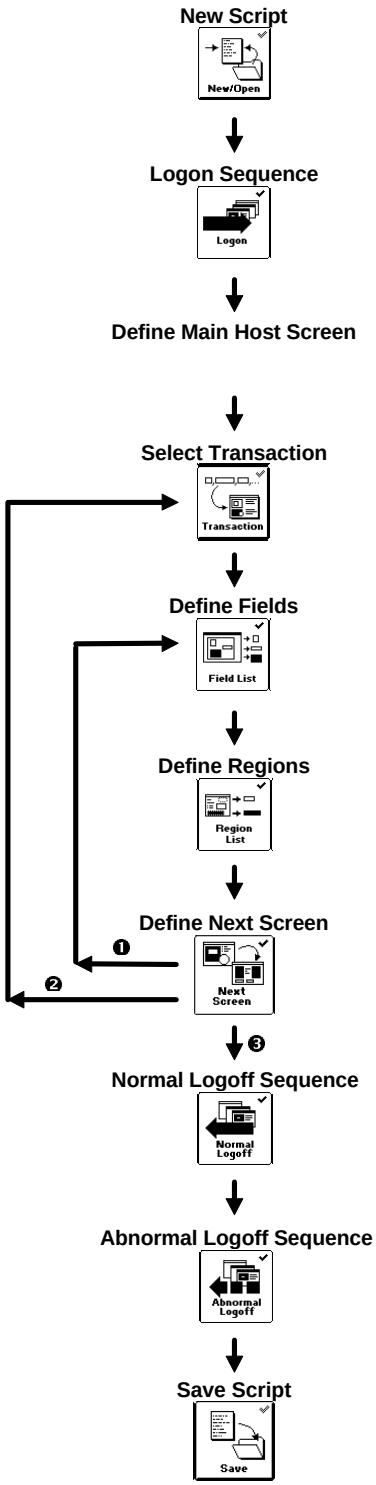


Understanding How the Script Builder Tool Flows

Use this table and the flow chart on the next page to help you understand how to use the Script Builder Tool.

Step	Button Names	Description
1	New/Open	Start data collection on the server. Choose Script and then New/Open to create a new script file and select a temporary host session for capturing keystrokes.
2	Logon	Choose Host Access and then Logon. Capture the keystrokes that take the user from the logon screen to the main host screen. Define the main host screen. This host screen becomes the current screen.
3	Transaction	Choose Transaction. Select a current transaction by either adding a new transaction or selecting an existing transaction and choosing Current.
4	Field List	Choose Screen and then Field List. Define the host screen fields (input fields) that are used on the current screen. The script maps transaction fields to these fields.
5	Region List	Choose Screen and then Region List. Define the regions for the current screen. Regions can handle errors on the host screen and they can output data.
6	Next Screen	Choose Screen and then Next Screen. Define the next host screen. This host screen becomes the current screen. Go to Step 4 (1 in the flow chart) to define fields and regions for the current screen. Go to Step 3 (2 in the flow chart) to choose a new current transaction. Go to Step 7 (3 in the flow chart) when you have finished adding all the transactions. The last screen should be the main host screen.
7	Normal Logoff	Choose Host Access and then Normal Logoff. Capture the keystrokes that take the user from the main host screen to the logoff screen.
8	Abnormal Logoff (Optional)	Choose Host Access and then Abnormal Logoff. Capture the keystrokes that take the user from any screen to the logoff screen.
9	Save	Choose Script and then Save. Save the script file. You should save the script file periodically while you work.

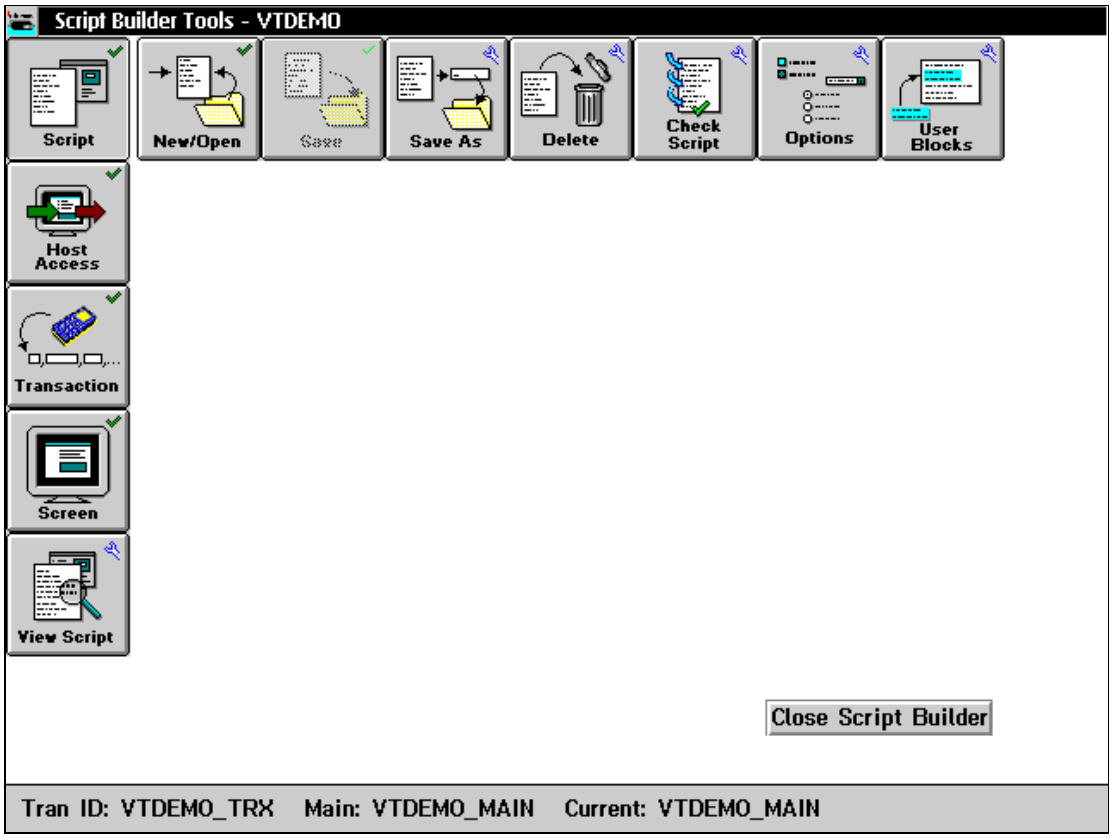
Script Builder Tool Flow Chart



Using the Script Builder Tool

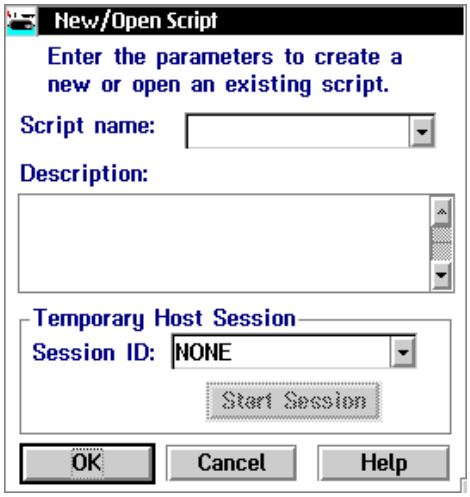
To use screen mapping, you need to create a script file. If you want to capture keystrokes on the host screen for a logon, a normal logoff, and an abnormal logoff, you need to start a temporary host session. You also need to start a host session if you want to get host attributes from the host screen. From the main menu, choose Screen Mapping and then Script Builder. The Script Builder Tools window opens.

All of the toolbar buttons for the major script building tasks are considered primary or configuration buttons. These buttons contain a check mark in the upper right corner, such as the New/Open button. All buttons for secondary or maintenance tasks contain a blue wrench in the upper right corner, such as the View Script button.



Creating a New Script File

1. From the Script Builder Tools window, choose Script.
2. Choose New/Open. The New/Open Script dialog box appears.



Field	Description	Value	Default
Script name	The unique name of the script you are creating or opening.	1 to 8 alphanumeric characters	None
Description (Optional)	A paragraph of text that describes the script.	1 to 255 characters	None
Session ID (Optional)	The session ID that you want to use when creating this script. ***Note:*** *This temporary host session does not have to be the same host session as the run-time screen mapping session you associate with the script.*	Predefined	None

Opening an Existing Script File

You need to start a temporary host session to capture keystrokes for logon, logoff, and abnormal logoff sequences. You also need an active host session if you want to use the Get Field feature.

To open an existing script

1. From the Script Builder Tools window, choose Script.
2. Choose New/Open. The New/Open Script dialog box appears.
3. In the Script name field, click the down arrow on the right side of the field. A list of existing scripts appears. Choose a script.
4. (Optional) In the Session ID field, click the down arrow on the right side of the field. A list of session IDs appears. Choose a session ID.

   Note: *If you have started data collection on the server, you cannot choose any session that is currently being used.*

5. (Optional) Choose Start Session. The host window opens.
6. Choose OK to return to the Script Builder Tools window.

Saving the Script File

You should periodically save your script while you are working on it. When you choose OK in a dialog box, the changes are temporarily stored in RAM. Choose Save or Save As to store your changes to disk.

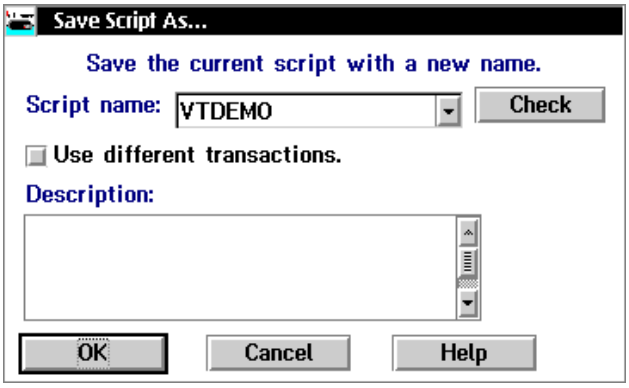
Note: *This toolbar button will not be available until you make changes to a new or existing script file.*

To save a script

1. From the Script Builder Tools window, choose Script.
2. Choose Save. The script is saved to disk.

Copying a Script File

1. Open the script file that you want to copy. For help, see “Opening an Existing Script File” earlier in this chapter.
2. From the Script Builder Tools window, choose Script.
3. Choose New/Open. The New/Open Script dialog box appears.
4. In the Script name field, click the down arrow on the right side of the field. A list of existing scripts appears. Choose a script to copy.
5. Choose Save As. The Save Script As dialog box appears.



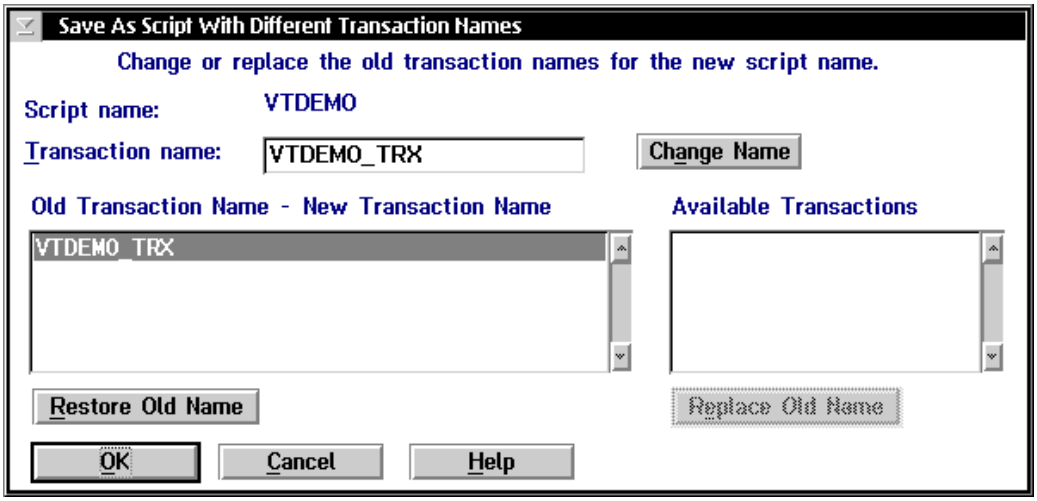
6. In the Script name field, enter a unique name for the new script.

   Or, click the down arrow on the right side of the field. A list of existing script names appears. Select one.
7. In the Description box, enter a new description for the script.
8. To assign new transactions to the new script, check the Use different transactions check box. The Save As Script With Different Transaction Names dialog box appears.

   Or, clear this check box if you want to assign new transactions later while you are editing the script.

   Note: *If the current script does not have any transactions assigned to it, the check box is grayed out.*

Save As Script With Different Transactions Dialog Box



9. In the Transaction name field, enter the name of the new transaction and choose Change Name. The old and new transaction names appear in the Old Transaction Name - New Transaction Name list box.

   Or, in the Available Transactions list box, select the transaction that you want to use. Choose Replace Old Name. The old and new transaction names appear in the Old Transaction Name - New Transaction Name list box.

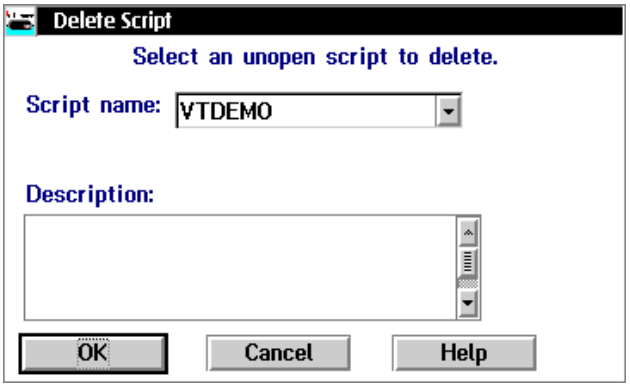
10. If you want to restore the old transaction name or if you want to choose another new transaction name, select the old transaction name from the Old Transaction Name - New Transaction Name list box and choose Restore Old Name.

11. Choose OK to save the script to disk and to return to the Script Builder Tools window.

Note: *If you choose a script name from the Script name drop-down list box in Step 3, a dialog box appears. This dialog box confirms that you want to write over the existing script. Choose Write.*

Deleting a Script File

1. From the Script Builder Tools window, choose Script.
2. Choose Delete. The Delete Script dialog box appears.



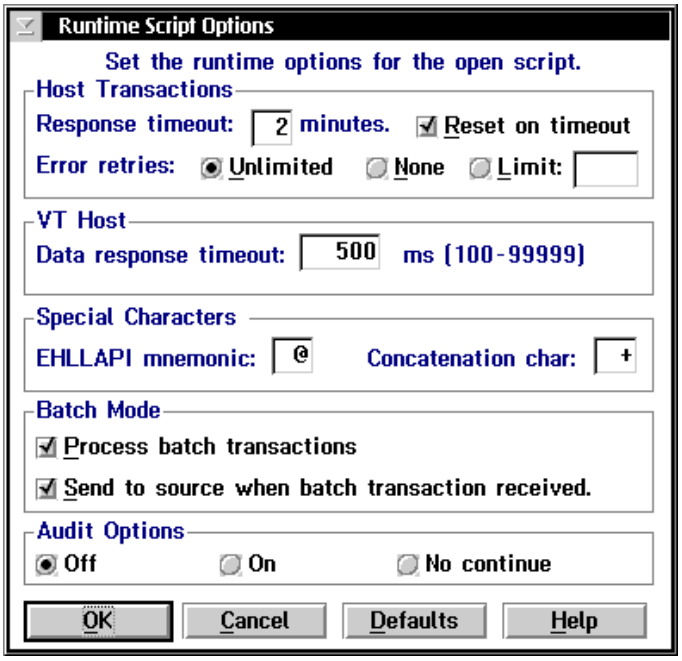
3. In the Script name field, click the down arrow on the right side of the field. A list of existing script files appears. Select the script you want to delete.
4. Choose OK to delete the script. A message box appears confirming that you want to delete the script.
5. Choose Delete. The script is deleted.

Setting Options for the Script File

Within the Script Builder Tools window, you can set certain script variables for the current script. Choose Defaults if you want to set this dialog box to default values.

To set options for the entire script

1. From the Script Builder Tools window, choose Script.
2. Choose Options. The Runtime Script Options dialog box appears.



Field	Description	Value	Default
Response timeout	Sets the number of minutes that the server waits for a "host busy" condition to clear.	1 to 9999	2
Reset on timeout	This check box determines if the server sends a Reset key to the host if the host is busy.	Check, Clear	Check

Field	Description	Value	Default
Error retries	These option buttons determine if the server retries the connection and how many times it retries the connection to the host application when an error occurs.	Unlimited, None, Limit	Unlimited
Data response timeout (VT/ANSI only)	The number of milliseconds of inactivity you want the server to wait before it assumes that the host is ready for more data.	100 to 99999	500
EHLLAPI mnemonic	EHLLAPI uses this character to represent special keys. This character must not occur in any keystroke of transaction data.	1 character	@
Concatenation char	The script uses this character to concatenate components of a message. This character must not occur in any static text of a message, such as a region label, or in any script keystroke name, such as CUR_POS. However, this character may appear in transaction data.	1 alphanumeric or special character	+
Process batch transactions	This check box determines if the controller processes batch transactions.	Check, Clear	Check
Send to source when batch transaction received	This check box determines if the server sends a message to the source of the transaction when the last transaction is received in batch mode. ***Note:*** *If the Process batch transactions check box is cleared, this check box is grayed out.*	Check, Clear	Check
Audit Options	Determines the level of auditing the server performs. If you enable auditing, when a non-fatal error occurs, the server writes the transaction and the explanatory transaction string to the audit file. • Choose Off if you do not want the controller to perform any script auditing. • Choose On if you want the controller to log non-fatal errors to the audit file and continue processing the script. • Choose No continue if you want the controller to log the error to the audit file and to stop processing the script.	Off, On, No continue	Off

About the Data Response Timeout (VT/ANSI)

In 3270 and 5250 screen mapping, the host application locks the terminal keypad while it is busy. When the keypad is unlocked, the host application is ready for the next action, such as another script command or keystroke. In VT/ANSI screen mapping, the terminals do not know when the host application is ready for the next action.

The Data response timeout field sets the amount of inactivity time the server waits before it assumes that the host is finished sending data. That is, the server listens on the TCP/IP socket and if there is no activity and the timeout period expires, the server performs the next action. However, there is no guarantee that the host is finished sending data.

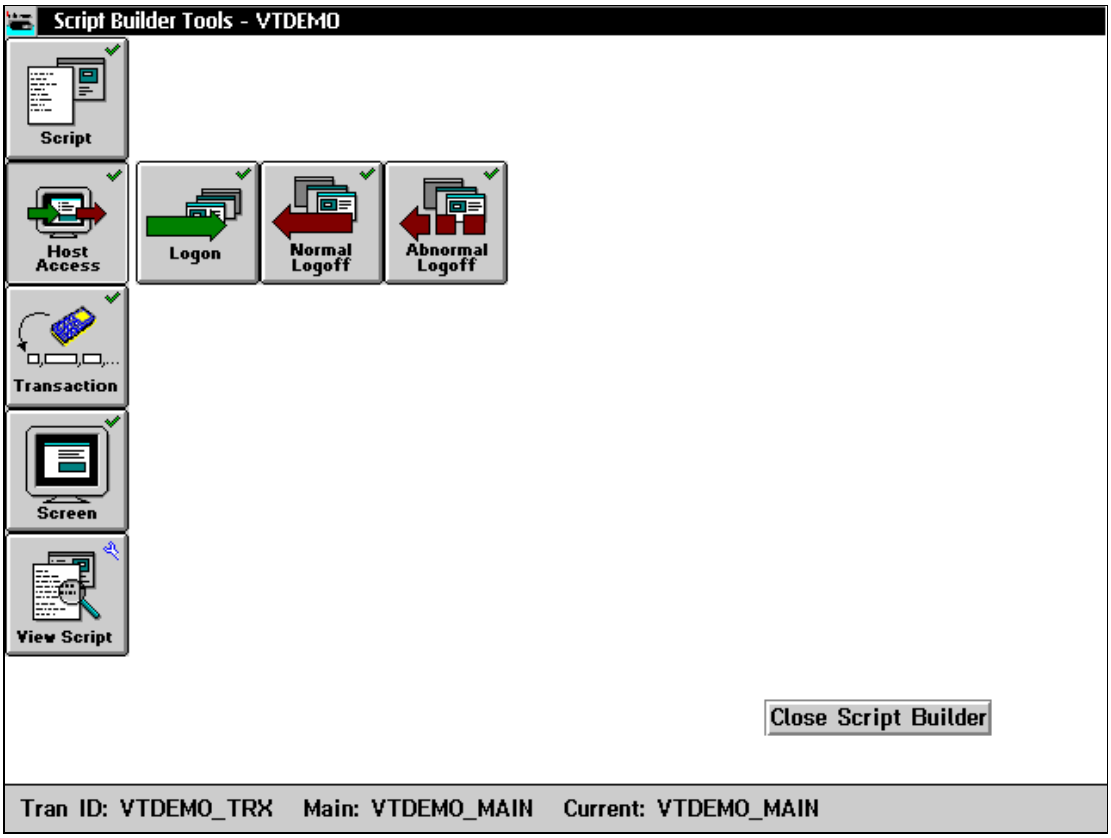
Note: *The server may not wait the entire timeout period if an action is performed successfully. For example, the PUT_TRANS_FIELD command waits until the cursor is at the field location or it may wait for the data response timeout to expire, whichever comes first.*

You set the data response timeout field when you set the script options. Use this field to tune the server to your network environment. If you set the data response timeout too long, it will affect server performance because your throughput will be slower. If you set the value too short, you may experience timing problems with your host.

Creating Host Access Sequences

For each script, you need to capture the keystrokes for a logon sequence, a normal logoff sequence and an abnormal logoff sequence. Logon sequences are keystrokes that take the script from the logon screen to the first host screen that receives all transactions for this script, such as the main host screen. Normal logoff sequences are keystrokes that exit the host application from the main host screen. Abnormal logoff sequences are keystrokes that exit the host application from any host screen. Abnormal logoffs usually occur when the server encounters a critical error.

Before you can capture keystrokes, you need to start a temporary host session. For help, see “Starting a Host Session” in Chapter 10.



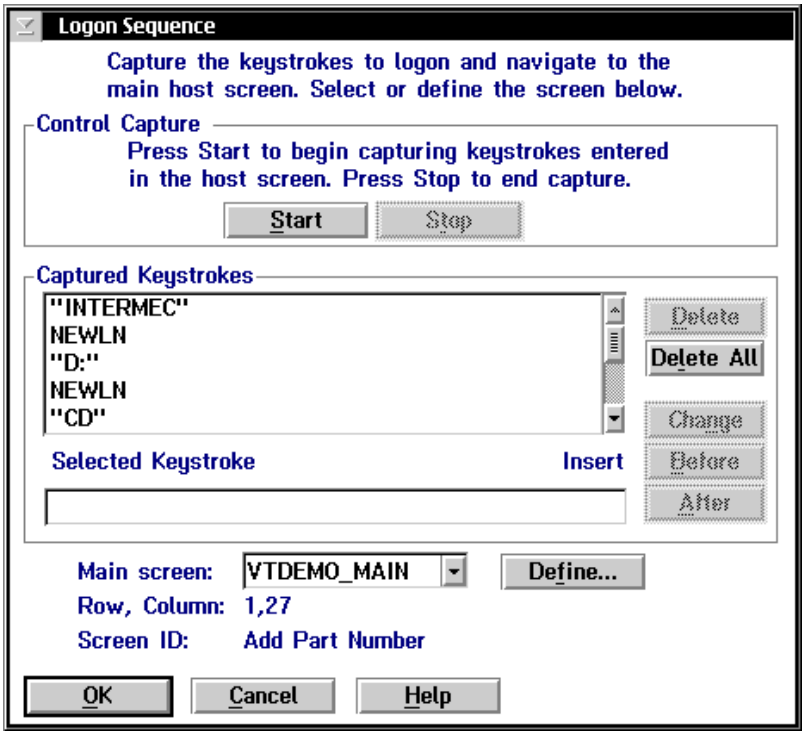
Creating a Logon Sequence

The logon sequence contains the keystrokes that get you from the login screen to the main host screen. The main host screen is the first host screen where every transaction in the script starts.

To create a logon

1. From the Script Builder Tools window, choose Host Access.
2. Choose Logon. The Logon Sequence dialog box appears.

   Note: *If you do not want to capture the logon keystrokes, you can type them into the Selected Keystrokes field. Go to Step 6.*



3. Choose Start.
4. In the host window, enter the keystrokes you want to use for your logon. The Script Builder Tool captures all the keystrokes that you type.
5. When you finish entering the keystrokes for the logon, choose Stop. The keystrokes you typed appear in the Captured Keystrokes box.
6. If necessary, edit the keystrokes. For help, see "Editing the Captured Keystrokes" later in this chapter.
7. In the Main screen field, click the down arrow on the right side of the field. A list of all the available host screens appears. Select a host screen to be the main screen.

   Or, choose Define to define a new host screen that you want to use as the main screen. For help, see "Adding a Host Screen" later in this chapter.
8. Choose OK to return to the Script Builder Tools window.

Example: Keystrokes Appearing in Logon Sequence

`"USERID"`	Enters the login name "USERID" in the User ID field.
`RTAB`	Tabs to the Password field.
`"PASSWORD"`	Enters the password "Password." This password goes with the login name.
`ENTER`	Presses **Enter** to enter the information from the login screen.
`ENTER`	Presses **Enter** to go to the main menu.

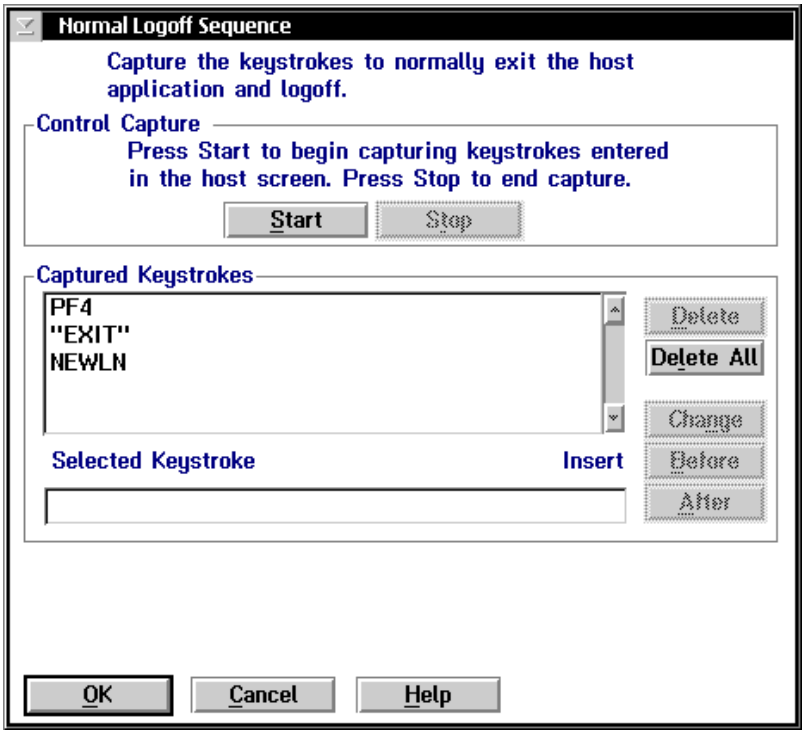
Creating a Normal Logoff Sequence

The normal logoff sequence contains keystrokes that exit you from the host application from the main host screen.

To create a normal logoff

1. From the Script Builder Tools window, choose Host Access.
2. Choose Normal Logoff. The Normal Logoff Sequence dialog box appears.

   Note: *If you do not want to capture the normal logoff keystrokes, you can type them into the Selected Keystrokes field. Go to Step 6.*



3. Choose Start.
4. In the host window, enter the keystrokes you want to use for your normal logoff. The Script Builder Tool captures all the keystrokes that you type.
5. When you finish entering the keystrokes for the normal logoff, choose Stop. The keystrokes you typed appear in the Captured Keystrokes box.
6. If necessary, edit the keystrokes. For help, see "Editing the Captured Keystrokes" later in this chapter.
7. Choose OK to return to the Script Builder Tools window.

Example: Keystrokes Appearing in Normal Logoff Sequence

`Home`	Presses **Home** to bring up a prompt.
`"signoff"`	Enters "signoff" at the prompt to leave the session.
`Enter`	Presses **Enter** to enter the command.

Creating an Abnormal Logoff Sequence

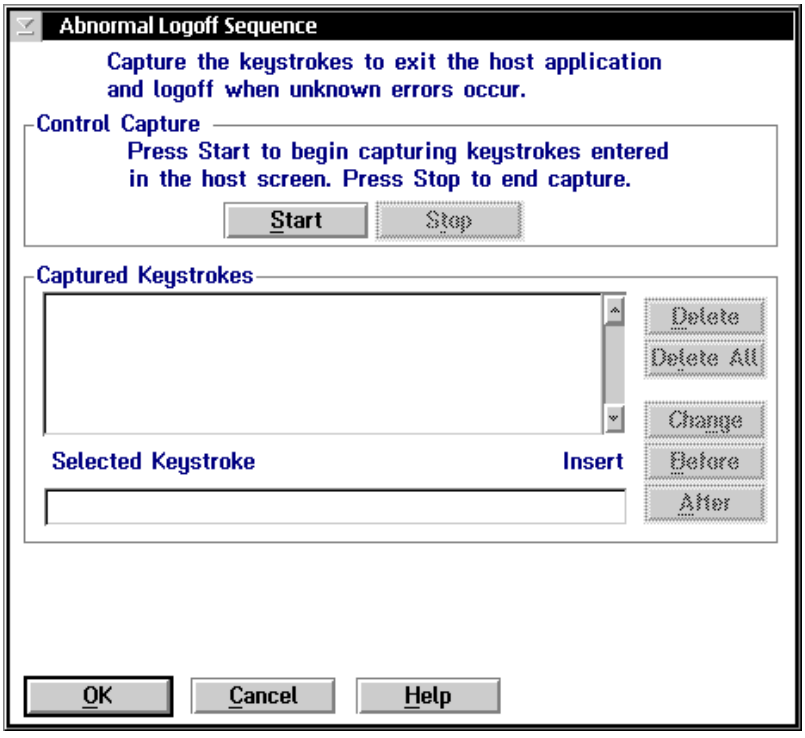
The abnormal logoff sequence contains keystrokes that exit you from the host application from any host screen. Abnormal logoffs usually occur when the server encounters a critical error.

Note: *Some host applications may not allow abnormal logoff sequences.*

To create an abnormal logoff

1. From the Script Builder Tools window, choose Host Access.
2. Choose Abnormal Logoff. The Abnormal Logoff Sequence dialog box appears.

   Note: *If you do not want to capture the abnormal logoff keystrokes, you can type them into the Selected Keystrokes field. Go to Step 6.*



3. Choose Start.
4. In the host window, enter the keystrokes you want to use for your abnormal logoff. The Script Builder Tool captures all the keystrokes that you type.
5. When you finish entering the keystrokes for the abnormal logoff, choose Stop. The keystrokes you typed appear in the Captured Keystrokes box.
6. If necessary, edit the keystrokes. For help, see "Editing the Captured Keystrokes" later in this chapter.
7. Choose OK to return to the Script Builder Tools window.

Editing the Captured Keystrokes

When you are done entering keystrokes for the host access sequence, choose Stop. The keystrokes that you typed appear in the Captured Keystrokes box. You can edit these keystrokes. Also, if you do not want to capture keystrokes, you can type them into the Selected Keystrokes field and then choose Before or After.

Deleting Lines in the Captured Keystrokes Box

You can either delete your keystrokes one line at a time, or you can delete all the keystrokes you have captured and start over again.

To delete one line

1. In the Captured Keystrokes box, select the line that contains the keystroke that you want to delete.
2. Choose Delete. The line is removed from the box.

To delete all of the lines

- Choose Delete All

Changing Lines in the Captured Keystrokes Box

1. In the Captured Keystrokes box, select the line that contains the keystroke that you want to change.
2. In the Selected Keystrokes box, enter the new keystroke.
3. Choose Change.

Inserting New Lines in the Captured Keystrokes Box

1. In the Captured Keystrokes box, select the line where you want to add a keystroke before it or after it.
2. In the Selected Keystrokes box, enter the new keystroke.
3. Choose Before to insert the new keystroke before the selected line.

   Choose After to insert the new keystroke after the selected line.

Selecting Transactions for the Script

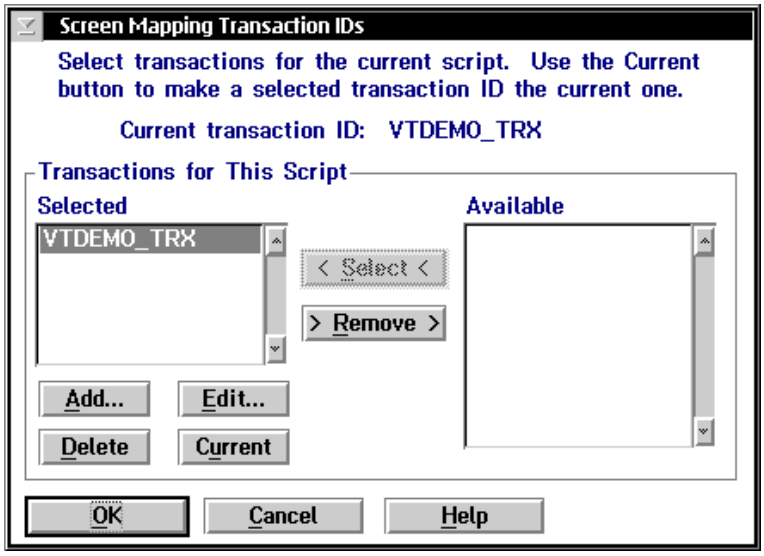
You need to define all the transactions you want this script to handle. For help, see "Adding a Transaction" in Chapter 9.

Note: *You can add a transaction without adding its transaction fields. When you define a host screen field and map it to a field in the new transaction, Script Builder automatically creates the transaction field.*

Using the Script Builder, you can map each transaction field to a host screen field. Therefore, you need to choose a current transaction before you can define any host screens, host screen fields, or regions for that transaction. In the Selected list box, select the transaction whose fields you want to map to host screen fields and then choose Current.

To select the transactions for the script

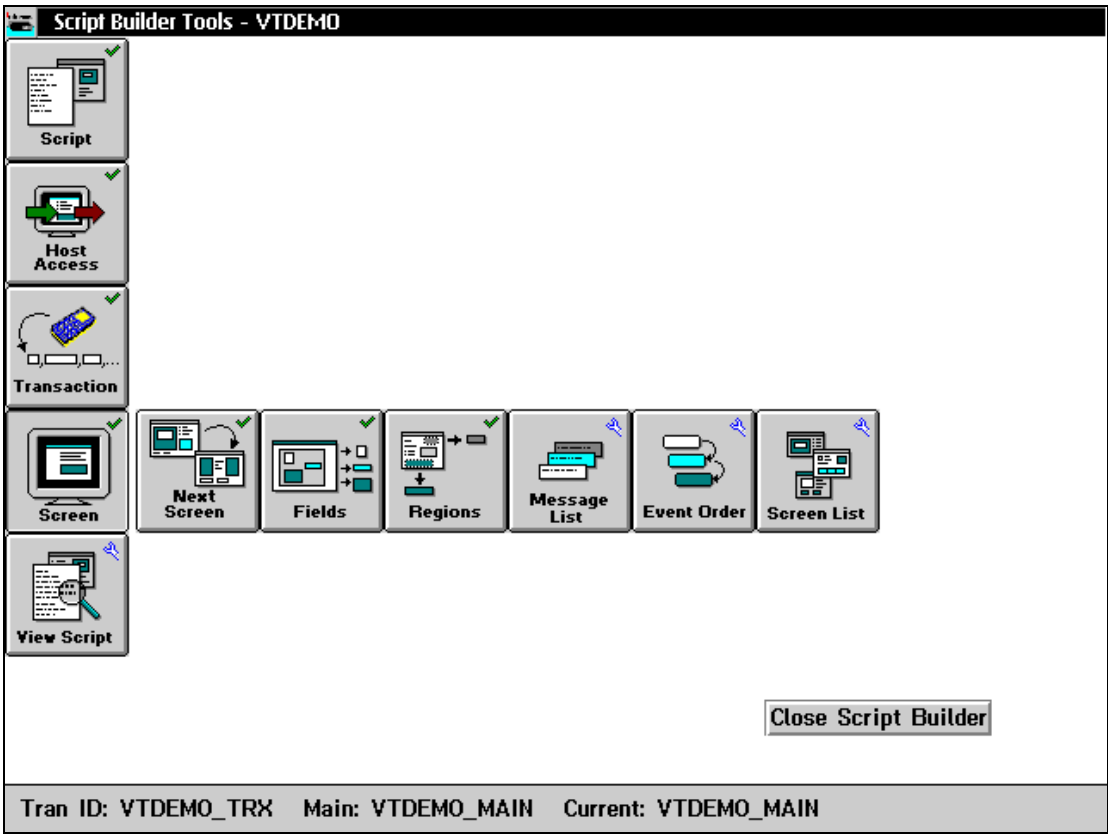
- From the Script Builder Tools window, choose Transaction. The Screen Mapping Transaction IDs dialog box appears.



Field	Description	Value	Default
Selected	This list box contains the transactions that this script handles.	None	None
Available	This list box contains all the transactions that are available to use with this script.	Predefined	None

Selecting Host Screens for the Current Transaction

You need to identify the host screens that receive transaction data from the current transaction. The current host screen is the host screen for which you are currently defining fields, regions, messages, and events. When you define the main host screen, it automatically becomes the current host screen. If you add more host screens, the main screen remains the current host screen until you go to the Maintain Screen List dialog box, select a screen and then choose Current.



Defining Next Screen Sequences for Host Screens

You need to define the sequence of host screens that the current transaction uses for mapping its fields.

In the Next Screen box, check the Yes check box if your transaction fields map to host screen fields on more than one host screen. After the Script Builder has performed all the screen events for the current host screen, it retrieves the next host screen.

The main host screen should always be the last screen in the sequence of host screens. Then, your host is always ready to receive data from the next transaction. If you do not define a next screen, the default next screen is the main host screen.

Note: *Before you can use the capture keystrokes feature, you must start a temporary host session. For help, see "Starting a Host Session" in Chapter 10.*

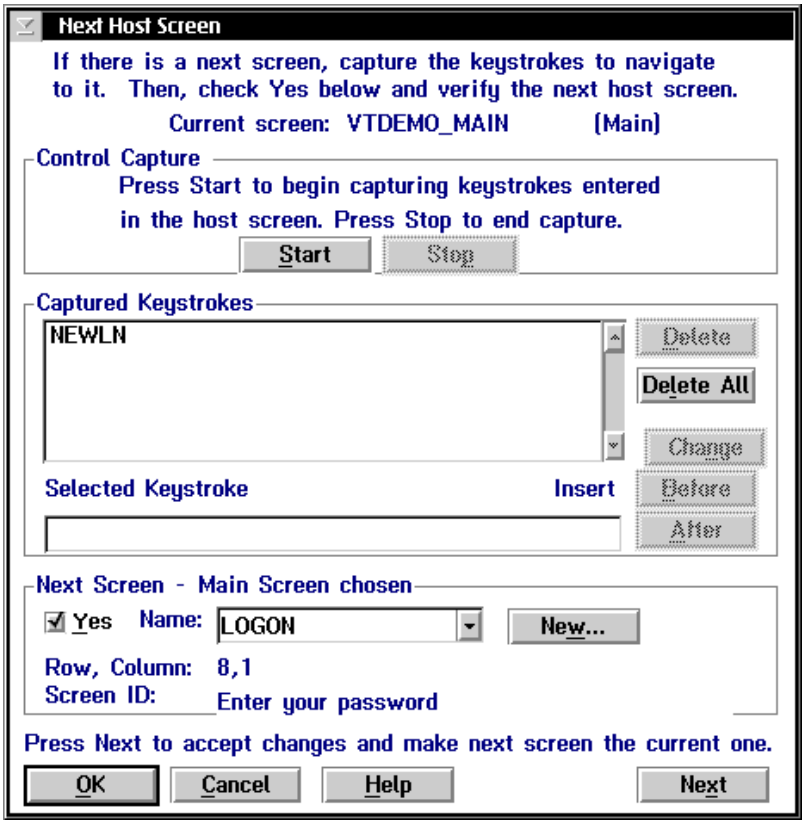
To define the next screen sequence

1. From the Script Builder Tools window, choose Screen.
2. Choose Next Screen. The Next Host Screen dialog box appears. This dialog box is shown on the next page.

   Note: *If you do not want to capture the keystrokes, you can type them into the Selected Keystrokes field. Go to Step 6.*

3. Choose Start.
4. In the host window, enter the keystrokes to bring up the next host screen. The Script Builder Tool captures all the keystrokes that you type and enters them into the Captured Keystrokes box.
5. When you finish entering the keystrokes, choose Stop. The keystrokes you typed appear in the Captured Keystrokes box.
6. If necessary, edit the keystrokes. For help, see "Editing the Captured Keystrokes" earlier in this chapter.

Next Host Screen Dialog Box



7. Check Yes in the Next Screen? box if you want to assign the next screen.

   To select an existing host screen for the next screen, click the down arrow on the right side of the field. A list of host screens appears. Select the host screen that you want to follow the Current screen.

   Or, to define a new host screen for the next screen, choose New. For help, see "Adding a Host Screen" later in this chapter.

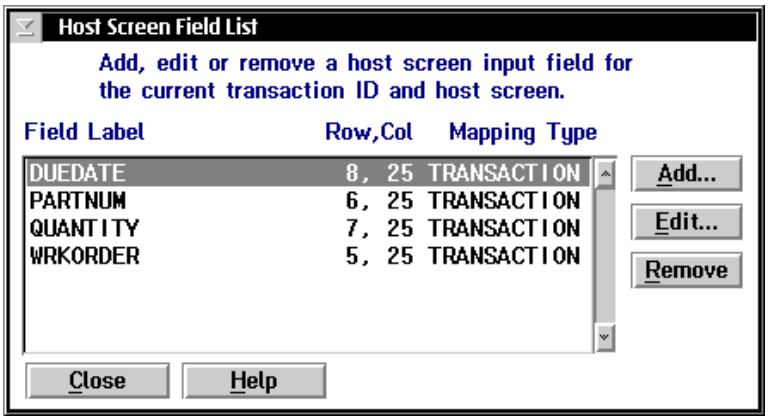
8. (Optional) Choose Next if you want to make the next screen the current host screen. The Script Builder displays the next screen information.
9. Repeat Steps 3 through 8 to define the entire next host screen sequence for the current transaction.
10. Choose OK to return to the Script Builder Tools window.

Selecting Host Screen Fields for the Current Host Screen

You must identify all the fields on the current host screen that receive transaction data.

To select host screen fields

1. From the Script Builder Tools window, choose Screen.
2. Choose Fields. The Host Screen Field List dialog box appears. This list box displays all of the fields that are defined for the current host screen, their location in the host screen, and whether they receive their data from a transaction field or a static string.



3. Add, edit, or remove fields for the current host screen. For help, see "Adding a Host Screen Field" later in this chapter.

   Note: *If you try to delete this host screen field and other transactions map fields to it, it is only removed from use with the current transaction.*

4. Choose Close to close the dialog box and return to the Script Builder Tools window.

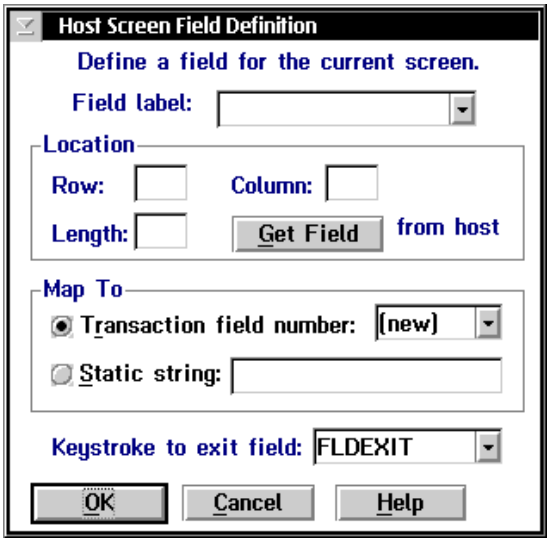
Adding a Host Screen Field

Different transactions may contain fields that map to the same host screen field. If you click the down arrow on the right side of the Field label field, you can choose from a list of defined host screen fields. If you choose one of these fields, the Location box is filled with row, column, and length attributes. You can keep the location information, but you must add the mapping type and keystroke to exit field.

Get Field button If you started a temporary host session for this script, you can use the Get Field feature to automatically detect the location of the field. On the host window, position your cursor on the first character of the field. Choose Get Field. The Row, Column, and Length fields are filled with values. For help, see "Getting Host Screen Field Attributes From a Host Screen" later in this chapter.

To add a host screen field

- From the Host Screen Field List dialog box, choose Add. The Host Screen Field Definition dialog box appears.



Field	Description	Value	Default
Field label	A unique name for the field.	1 to 20 alphanumeric characters	None
Row	The row position on the host screen of the first character of the field.	1 to 24	None
Column	The column position on the host screen of the first character of the field.	1 to 80	None
Length	The maximum number of characters this field accepts.	1 to 999	None
Transaction field number	The number of the transaction field whose data is mapped to the host screen field. Use this option if the data for the host screen field is mapped from a transaction field sent by a terminal. Select <new> to define a new transaction field number. Script Builder creates a new field with the host screen field label. You can edit this transaction field later. For help, see "Adding a Transaction Field" in Chapter 9.	Predefined	(new)
Static string	The string that is mapped to the host screen field. Use this option if the data for the host screen field comes from a static string.	1 to 119 characters	None
Keystroke to exit field	Determines the keystroke mnemonic that exits the input field after data is placed in it.	FLDEXIT, ENTER, RTAB, LTAB, (none)	FLDEXIT

Getting Host Screen Field Attributes From a Host Screen

In 5250 field-formatted host screens, there are two types of fields: protected and unprotected. Protected fields are fields that you cannot write over and are usually text on the host screen. Unprotected fields are usually input fields. To get host screen field attributes from a host screen field, you position the host cursor anywhere in an unprotected field and then choose Get Field. The Script Builder fills in the Location box with the beginning position of the field and its length. If the host cursor is in a protected field when you choose Get Field, an error message occurs.

3270 field-formatted host screens do not differentiate between protected and unprotected fields. To get host screen field attributes from a host screen field, you position the host cursor at the beginning position of a field and then choose Get Field. The Script Builder fills in the Location box with the beginning position of the field and its length.

VT/ANSI host screens are not field-formatted host screens. To get host screen field attributes from a host screen field, you must highlight the entire host screen input field before you choose Get Field. If nothing is selsected when you choose Get Field, an error message occurs.

To get host screen field attributes from a host screen

1. Start a temporary host session. For help, see “Starting a Host Session” in Chapter 10.
2. In the host window, open the host screen that contains the field that you need to define.
3. In the host window, place your cursor on the host screen field.

   Note: *In VT or ANSI host screens, you need to select the entire host screen field.*

4. In the Host Screen Field Definition dialog box, choose Get Field. The Location box is populated with the attributes of the field.
5. If necessary, edit the information in the fields.
6. Choose OK to save your changes and return to the Host Field List dialog box.
7. Repeat Steps 2 through 6 until you have defined all the host screen fields.

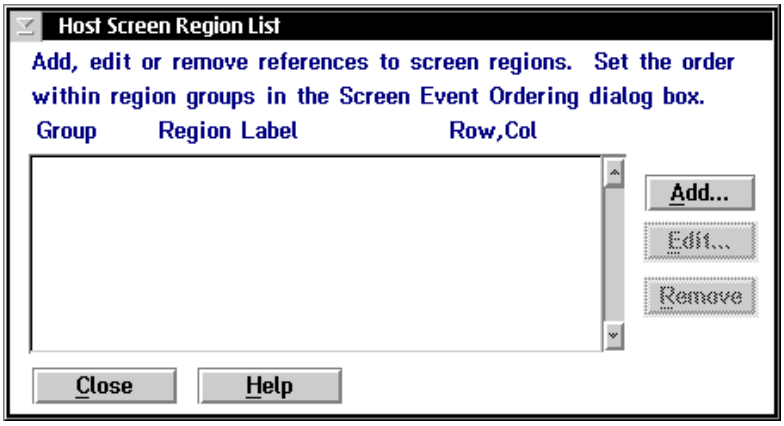
Selecting Regions for the Current Host Screen

Regions are areas on the host screen. You can define a region that the script file examines to determine whether or not a certain condition has been met or you can define a region from which the script file reads data. Specifically, you usually define a region to:

- catch an error message that appears on the host screen after a transaction field is mapped to a host screen field. You define the location information of the region. You also define actions that the script file takes when the region appears and when the region does not appear.
- read data from a certain host screen field. You define the location and the length of the region. To define the length, you choose the Match on Any String within *x* characters field. The script file sends any data that it finds in the location back to the application that is running on the terminal through a message.

To select a region

1. From the Script Builder Tools window, choose Screen.
2. Choose Regions. The Host Screen Region List dialog box appears. This list box displays the group the regions are in, the region labels, and their location in the host screen.



3. Add, edit, or remove regions for the current host screen. For help, see "Adding a Region" later in this chapter.

   Note: *If you try to delete this region and other transactions use this region, it is only removed from use with the current transaction.*

4. Choose Close to close the dialog box and return to the Script Builder Tools window.

Adding a Region

There are three types of actions that you can define when a region appears:

- Send a message to the source of the transaction.
- Capture keystrokes to clear the region.
- Determine what event happens when the region is done performing its actions. The default action is to continue processing screen events. You usually use this action when you read data from a host screen field.

  However, if you are defining a region to catch an error message that appears on the host screen, you should choose to go to a next screen and then select the main host screen. If you are at the main host screen, you should choose to cancel processing the screen event. When an error message occurs, you usually want to return to the main host screen and process the next transaction.

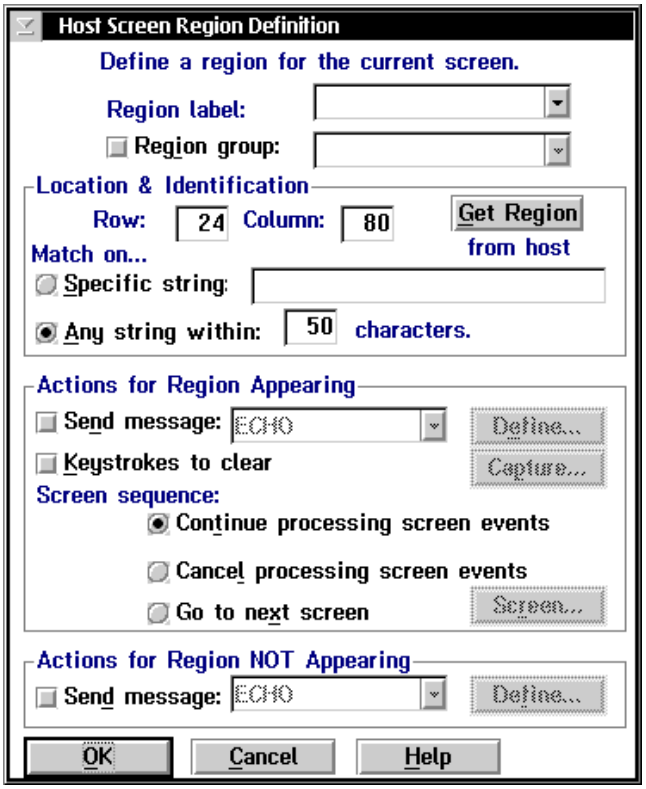
If a region does not appear, you can send a message to the source of the transaction.

Get Region button If you started a temporary host session for this script, use the Get Region feature to automatically select the location and contents of the region. On the host window, position your cursor on the first character of the region. Choose Get Region. The Row, Column, and Specific String fields are filled with values. For help, see "Getting a Region From a Host Screen" later in this chapter.

To add a region

- From the Host Screen Region List dialog box, choose Add. The Host Screen Region Definition dialog box appears.

Host Screen Region Definition Dialog Box



Field	Description	Value	Default
Region label	A name for the region that is unique within the current screen.	1 to 20 alphanumeric characters	None
Region group (Optional)	This check box determines if you want this region to be part of a group of regions that share the same action in the Actions for Region NOT appearing box. This action only occurs if none of the regions in the group appear.	1 to 8 alphanumeric characters	None
Row	The row position on the host screen of the first character of the region.	1 to 24	24
Column	The column position on the host screen of the first character of the region.	1 to 80	80
Match on	The method the server uses to identify the region.	Specific string, Any string within	Any string within

Field	Description	Value	Default
Specific string	Lets you define a specific string the server must identify at the specified row and column positions before it recognizes the region.	1 to 80 alphanumeric characters	None
Any string within	Specifies the length of a region from the specified row position. The server identifies the region if any string appears within this length.	1 to 999	50
Send message (Optional)	This check box determines if a message is sent to the source of the transaction when the region is recognized. Or, choose Define to create a new message. For help, see “Creating Screen and Region Messages” later in this chapter.	Check, Clear	Clear
Keystrokes to clear (Optional)	This check box lets you define a keystroke sequence that clears the region. Choose Capture to specify keystrokes to clear the region when it appears. For help defining the keystrokes, see “Capturing Keystrokes” later in this chapter.	Check, Clear	Clear
Screen sequence	Determines what event happens when the region is finished performing its actions.	Continue processing screen events, Cancel processing screen events, Go to next screen	Continue processing screen events
Continue processing screen events	This option button indicates that the script file remains on the host screen to continue processing any other defined screen events.	Check, Clear	Check
Cancel processing screen events	This option button indicates that the script file remains on the host screen, but does not process any other defined screen events.	Check, Clear	Clear
Go to next screen	This option button indicates that the script file goes to another host screen.	Check, Clear	Clear
Send message (Optional)	This check box determines if a message is sent to the source of the transaction if the region does not appear. Or, choose Define to create a new message. For help, see “Creating Screen and Region Messages” later in this chapter.	Check, Clear	Clear

Getting a Region From a Host Screen

In 5250 field-formatted host screens, there are two types of fields: protected and unprotected. Protected fields are fields that you cannot write over and are usually text on the host screen. Unprotected fields are usually input fields. To get region attributes from a host screen field, you position the host cursor anywhere in an unprotected field and then choose Get Region. The Script Builder fills in the Location box with the beginning position of the field, its contents, and its length. If the host cursor is in a protected field when you choose Get Region, the Script Builder fills in the Location box with the host cursor position, and it fills in the contents and length of the field from the host cursor position to the end of the field.

3270 field-formatted host screens do not differentiate between protected and unprotected fields. All fields are treated like protected fields. When you choose Get Region, the Script Builder fills in the Location box with the host cursor position, and it fills in the contents and length of the field from the host cursor position to the end of the field.

VT/ANSI host screens are not field-formatted host screens. To get region attributes, you must highlight the entire region before you choose Get Region. If nothing is selected when you choose Get Region, an error message occurs.

To get a region from a host screen

1. Start a temporary host session. For help, see "Starting a Host Session" in Chapter 10.
2. In the host window, open the host screen that contains the region that you need to define.
3. In the host window, place your cursor on the region.

   Note: *In VT or ANSI host screens, you need to select the entire region.*

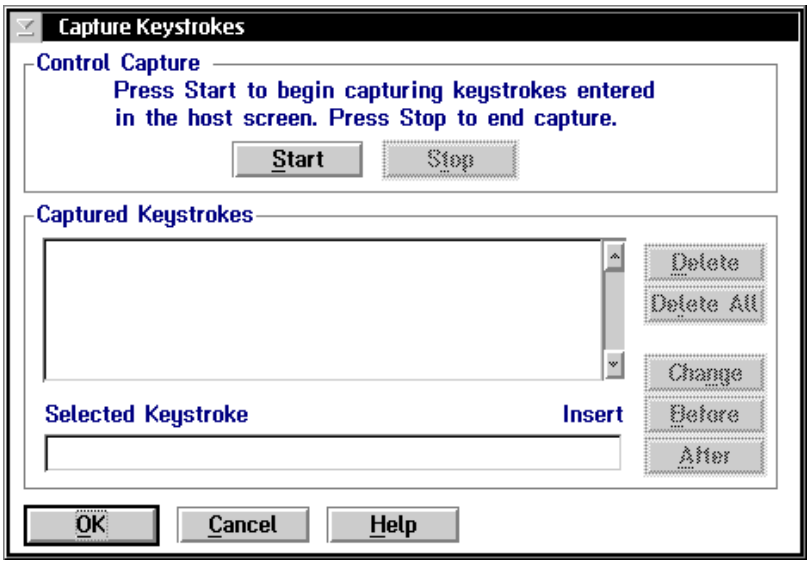
4. In the Host Screen Region Definition dialog box, choose Get Region. The Location & Identification box is populated with the attributes of the region.
5. If necessary, edit the information in the fields.
6. Choose OK to save your changes and return to the Host Region List dialog box.
7. Repeat Steps 2 through 6 until you have defined all the host regions.

Capturing Keystrokes

Before you can use the capture keystrokes feature, you must start a temporary host session. For help, see “Starting a Host Session” in Chapter 10.

To capture keystrokes

1. From the Host Screen Region Definition dialog box, check the Keystrokes to clear check box.
2. Choose Capture. The Capture Keystrokes dialog box appears.



Note: *If you do not want to capture the keystrokes, you can type them into the Selected Keystrokes field. Go to Step 6.*

3. Choose Start.
4. In the host window, enter the keystrokes to clear the region. The Script Builder Tool captures all the keystrokes that you type.
5. When you finish entering the keystrokes, choose Stop. The keystrokes you typed appear in the Captured Keystrokes box.
6. If necessary, edit the keystrokes. For help, see “Editing the Captured Keystrokes” earlier in this chapter.
7. Choose OK to return to the Script Builder Tools window.

Defining Next Host Screen Sequences for Regions

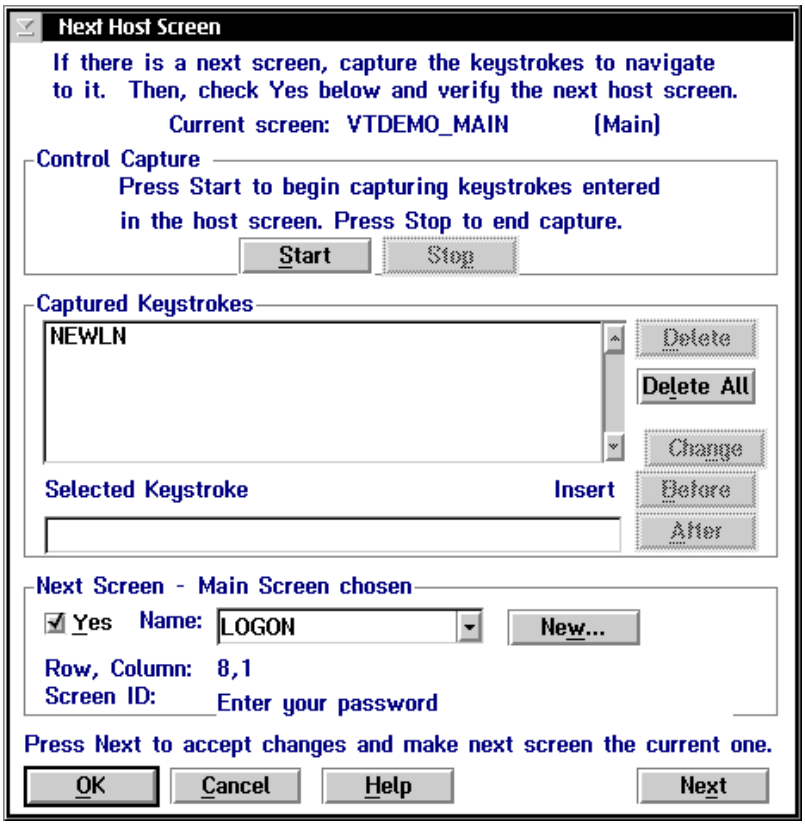
You may want the script file to go to a different host screen when it is finished performing all the actions for the region. If you are defining a host screen for the region to go to when it catches an error message, you usually want the script file to return to the main host screen.

Note: *Before you can use the capture keystrokes feature, you must start a temporary host session. For help, see "Starting a Host Session" in Chapter 10.*

To define the next screen sequence for a region appearing

1. From the Host Screen Region Definition dialog box, choose the Go to next screen option button.
2. Choose Screen. The Next Host Screen dialog box appears.

   Note: *If you do not want to capture the keystrokes, you can type them into the Selected Keystrokes field. Go to Step 6.*



3. Choose Start.
4. In the host window, enter the keystrokes to go to the next screen. The Script Builder Tool captures all the keystrokes that you type and enters them into the Captured Keystrokes box.
5. When you finish entering the keystrokes, choose Stop. The keystrokes you typed appear in the Captured Keystrokes box.
6. If necessary, edit the keystrokes. For help, see “Editing the Captured Keystrokes” earlier in this chapter.
7. In the Next Screen box, check the Yes check box and then click the down arrow on the right side of the Name field. A list of host screens appears. Select the host screen that you want to follow the Current screen.

   Or, to define a new host screen, choose New. For help, see “Adding a Host Screen” later in this chapter.
8. Choose OK to return to the Script Builder Tools window.

Creating Screen and Region Messages

There are two types of messages that you can send: screen messages and region messages. Messages are always sent to the source of the transaction. When you choose Screen and then Message List from the Script Builder Tools, the Screen Message List dialog box displays all the messages that are defined for the current host screen.

Sending screen messages is a screen event; sending region messages is not an event. If you define a screen message, it is sent to the source of the transaction while the script file is processing screen events. In the Screen Event Ordering dialog box, you can adjust the order of screen events.

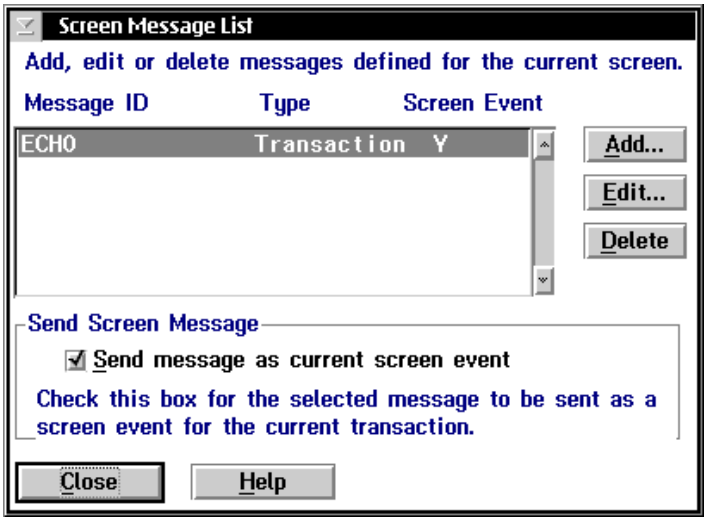
However, if you define a region message, it can be sent to the source of the transaction when a region appears or it can be sent when a region does not appear. Region messages do not appear in the Screen Event Ordering dialog box.

Both screen and region messages are text messages that may also include information from the current host screen.

Send message as current screen event check box If you check this check box, the message will be sent as a screen message. If you do clear this check box, the message will be defined as a region message. That is, it will only be sent if you select it when you are defining a region. By using this check box, you are only defining the characteristic of a message with the current transaction. Other transactions may use the same message differently.

To create messages

1. From the Script Builder Tools window, choose Screen.
2. Choose Message List. The Screen Message List dialog box appears.



3. Add, edit, or remove messages for the current host screen. For help, see “Adding a Message” later in this chapter.
4. To use a message as a screen message, select the message and check the Send message as current screen event check box.

   To use a message as a region message, do not check the Send message as current screen event check box. When you define the region where you want to use this message, select this message from the Send message drop-down list box.
5. Choose Close to return to the Script Builder Tools window.

Adding a Message

Use messages to carry information from the host application to the application that is running on the terminal. You can only define one message per transaction per script file to be sent back to the terminal. You can define two types of messages:

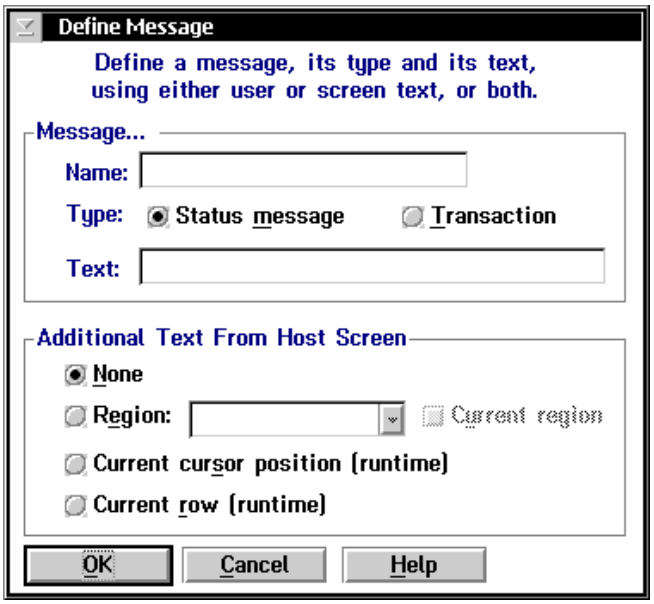
Status message This message appears in the status line of your terminal.

Transaction message This message contains its data in the format of a transaction. The transaction fields are mapped to the terminal screen fields according to the template.

Note: *To receive either type of message, you must check the Wait for response check box when you are defining your terminal screen. If you do not check this option, the terminal will not read the incoming message.*

To add a message

- From the Screen Message List dialog box, choose Add. The Define Message dialog box appears.



Field	Description	Value	Default
Name	A unique name for the message.	1 to 16 alphanumeric characters	None
Type	The type of message you want to send to the source of the transaction.	Status message, Transaction	Status message
Status message	Use this message type to define a text message in the Text field. This message will appear in the status line at the bottom of the terminal screen that originated the transaction.	Check, Clear	Check
Transaction	Use this message type to define a transaction in the Text field that will be mapped back to the terminal screen fields that originated the transaction.	Check, Clear	Clear
Text	For a status message, enter the string. For a transaction, enter the transaction data. You need to separate the transaction fields using the delimiter you set earlier when you defined your transactions. This delimiter is usually a comma (,).	1 to 120 characters	None
None	This option button indicates that nothing from the host screen is included in the message.	Check, Clear	Check
Region	This option button indicates that a region is included in the message. Choose the region to include with the message.	Check, Clear	Clear
Current region	This check box lets you choose the current region since it is not listed in the region list.	Check, Clear	Clear
Current cursor position	This option button indicates that the entire host screen field where the cursor is positioned at run-time is included in the message.	Check, Clear	Clear
Current row	This option button indicates that the entire row where the cursor is positioned at run-time is included in the message.	Check, Clear	Clear

About Message Types (Status vs. Transaction)

Screen and region messages can be sent to the source of the transaction as a status message or as a transaction. A status message is text that appears in the status line at the bottom of the terminal screen. However, some applications may expect to receive a transaction back. For example, when you define a terminal screen field as an output field, you need to map a transaction field to it. This transaction field can come from a transaction message.

Transaction Message Example

You want to know how many parts you have in stock for a part number. Your Part Query terminal screen has two fields: part number (an input field that maps to transaction field number 1) and quantity (an output field that maps to transaction field number 2). You also need to define a region (QTY_RESULT) on the Part Number Quantity host screen at the Quantity field.

Define a message, Quantity, and choose Transaction. In the Text field, enter:

```
1+",",+QTY_RESULT
```

where:

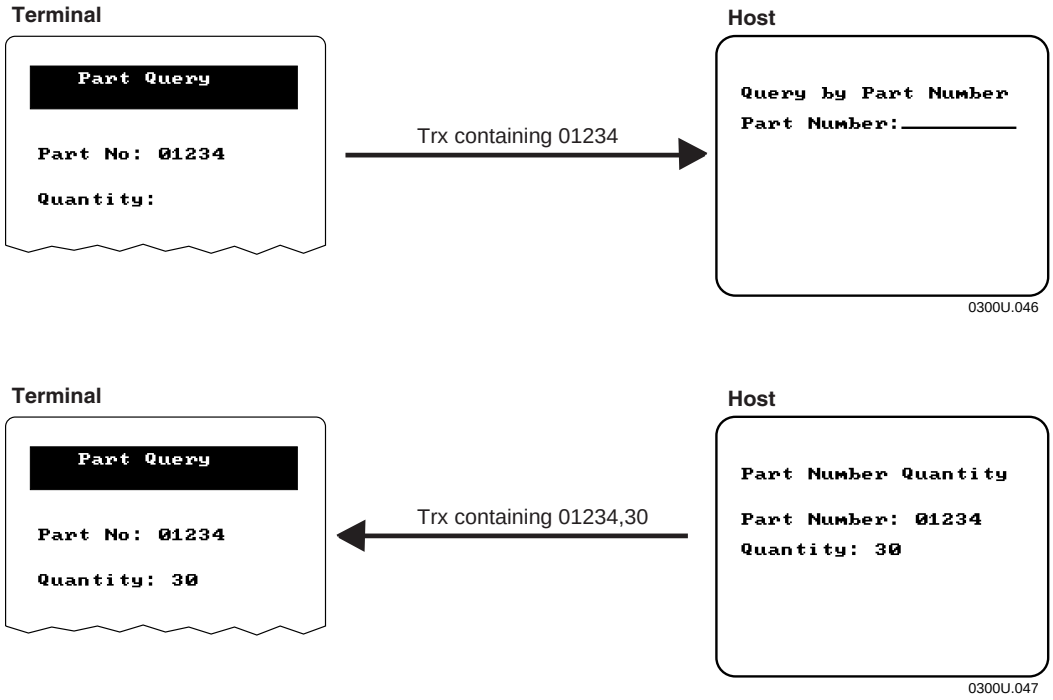
1 means that transaction field number 1 contains the same value as the original transaction field 1.

"," is the transaction field delimiter.

QTY_RESULT is the region that you defined. The contents of this region are sent back to the terminal screen as transaction field number 2.

At the terminal screen, enter the part number (01234) in the Part number field and send the transaction. When the script file receives the transaction, it performs actions to get to the host screen titled, Query by Part Number. The part number 01234 is entered and the Part Number Quantity screen appears and displays the value (30) you want in the Quantity field. Part number 01234 maps back to the Part number field in the terminal screen. The value of the quantity, 30, maps back to the Quantity field.

Transaction Message Example



Changing the Order of Screen Events

You can change the order of screen events and you can change the order of the regions within a region group. As each host screen appears, certain screen events can occur. These events include

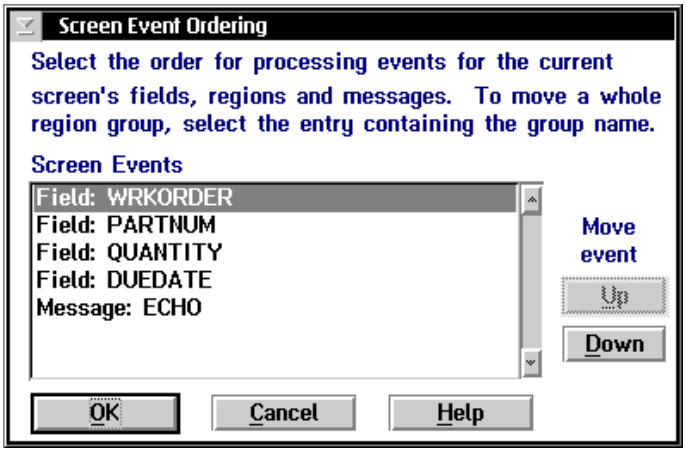
- mapping terminal (transaction) fields to host screen fields.
- handling regions in the host screen.
- sending screen messages.

The events listed below are not screen events and you cannot change the order in which they occur. They are:

- going to a next screen. Next screen allows the script to go to another host screen after finishing all the screen events.
- sending region messages. Region messages are sent to the source of the transaction when a region appears or does not appear in a host screen. The send message action is completed when processing a region event.

To change the order of screen events

1. From the Script Builder Tools window, choose Screen.
2. Choose Event Order. The Screen Event Ordering dialog box appears.



3. In the Screen Events list box, select the event you want to move. Events occur in order starting from the top.
4. Choose Up or Down to move the event to the appropriate place.
5. Choose OK to return to the Script Builder Tools window.

To change the order of regions within a region group

1. From the Script Builder Tools window, choose Screen.
2. Choose Event Order. The Screen Event Ordering dialog box appears.
3. In the Screen Events list box, select the region that you want to move.
4. Choose Up or Down to move the region to the appropriate place.
5. Choose OK to return to the Script Builder Tools window.

Note: *Regions that match on a specific string are checked before regions that match on any string. You may need to be aware of this feature if you have regions that overlap.*

Note: *Region actions (events) that occur within region groups are mutually exclusive. That is, when the script identifies a region and that region is in a region group, the script performs the actions that are defined for the region. It ignores all other actions that occur for other regions in the group.*

Maintaining the Host Screens

The Maintain Screen List dialog box lets you add any new host screens that you did not create when you defined the host screen sequences. You can also edit and delete host screens. For help, see "Adding a Host Screen" later in this chapter.

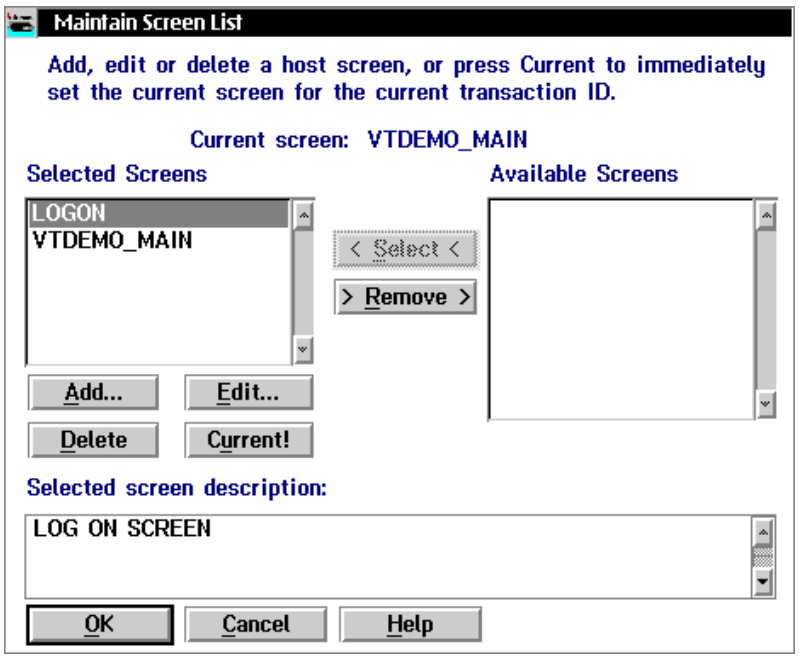
Note: *You may not be able to delete the host screen if other transactions send data to it. Instead, a message box appears.*

Note: *You cannot delete or remove the main host screen from the Selected Screens list box. To delete or remove the main host screen, you must edit the Logon Sequence dialog box and select a new main host screen.*

If you want to define host screen fields and regions for a different host screen, you can also select a new current host screen and choose Current! The description of the screen appears in the Selected Screen Description box.

To maintain the host screens

1. From the Script Builder Tools window, choose Screen.
2. Choose Screen List. The Maintain Screen List dialog box appears.



Field	Description	Value	Default
Selected Screens	This list box contains the host screens that receive transaction data from the current transaction.	None	None
Available Screens	This list box contains all the host screens that are available to use.	Predefined	None

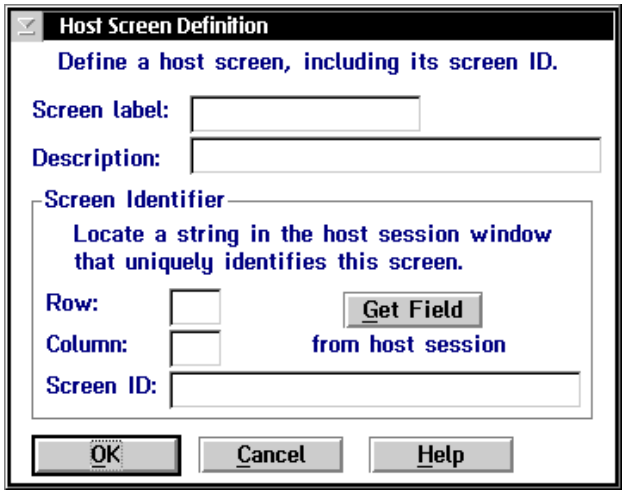
Adding a Host Screen

Each host screen definition corresponds to a different host screen. The screen identifier is any string on a host screen that makes the host screen unique.

Get Field button If you started a temporary host session for this script, you can use the Get Field feature to automatically select the location and contents of the screen identification. On the host window, position your cursor on the first character of the field. Choose Get Field. The Row, Column, and Screen ID fields are filled with values. For help, see "Getting the Screen Identifier From the Host Screen" later in this chapter.

To add a host screen

- In the Maintain Screen List dialog box, choose Add. The Host Screen Definition dialog box appears.



Field	Description	Value	Default
Screen label	A unique name for the screen	1 to 20 alphanumeric characters	None
Description (Optional)	A description for the screen.	1 to 255 characters	None
Row	The row position on the host screen of the first character of the screen identification string.	1 to 24	None
Column	The column position on the host screen of the first character of the screen identification string.	1 to 80	None
Screen ID	The identification string on the host screen that makes the screen unique.	1 to 80 alphanumeric characters and spaces	None

Getting the Screen Identifier From the Host Screen

In 5250 field-formatted host screens, there are two types of fields: protected and unprotected. Protected fields are fields that you cannot write over and are usually text on the host screen. Unprotected fields are usually input fields. To get the screen ID from a host screen field, you should use protected fields that contain static text. Position the host cursor anywhere in a protected field and then choose Get Field. The Script Builder fills in the Screen Identifier box with the current host cursor position, and it fills in the contents and length of the field from the host cursor position to the end of the field. If the host cursor is in an unprotected field when you choose Get Field, an error message occurs.

3270 field-formatted host screens do not differentiate between protected and unprotected fields. All fields are treated like protected fields. When you choose Get Field, the Script Builder fills in the Screen Identifier box with the host cursor position, and it fills in the contents and length of the field from the host cursor position to the end of the field.

VT/ANSI host screens are not field-formatted host screens. To get the screen ID from a host screen field, you must highlight the entire host screen field before you choose Get Field. If nothing is selected when you choose Get Field, an error message occurs.

To get the screen identifier from a host screen

1. Start a temporary host session. For help, see "Starting a Host Session" in Chapter 10.
2. In the host window, open the host screen that contains the field that you need to define.
3. In the host window, place your cursor on the screen identifier.

   Note: *In VT or ANSI host screens, you must select the entire screen identifier.*

4. In the Host Screen Definition dialog box, choose Get Field. The Screen Identifier box is populated with the attributes of the field.
5. If necessary, edit the information in the fields.
6. Choose OK to save your changes and return to the Host Screen List dialog box.
7. Repeat Steps 2 through 6 until you have defined all the host screens.

Defining User Blocks

In the Script Builder Tool, you cannot modify the script that has been automatically generated. However, you can add user blocks after any line in the script that has a plus (+) sign in the left margin. When you define user blocks, you can insert script comments or commands that the Script Builder cannot generate. For help, see the *DCS 300 Technical Reference Manual*.

Note: *If you open and then save your script file in any text editor, the Script Builder Tool will no longer recognize the file. However, you can still use your script file for screen mapping.*

When you open the User Block List dialog box, you may see these symbols to the left of lines in the script:

+ A plus sign indicates places where you can enter user blocks.

< The less than sign precedes existing user blocks.

> The greater than sign precedes both INPUT_FIELDS and REGIONS.

:: Two colons indicate a new screen description. This symbol should precede a screen label.

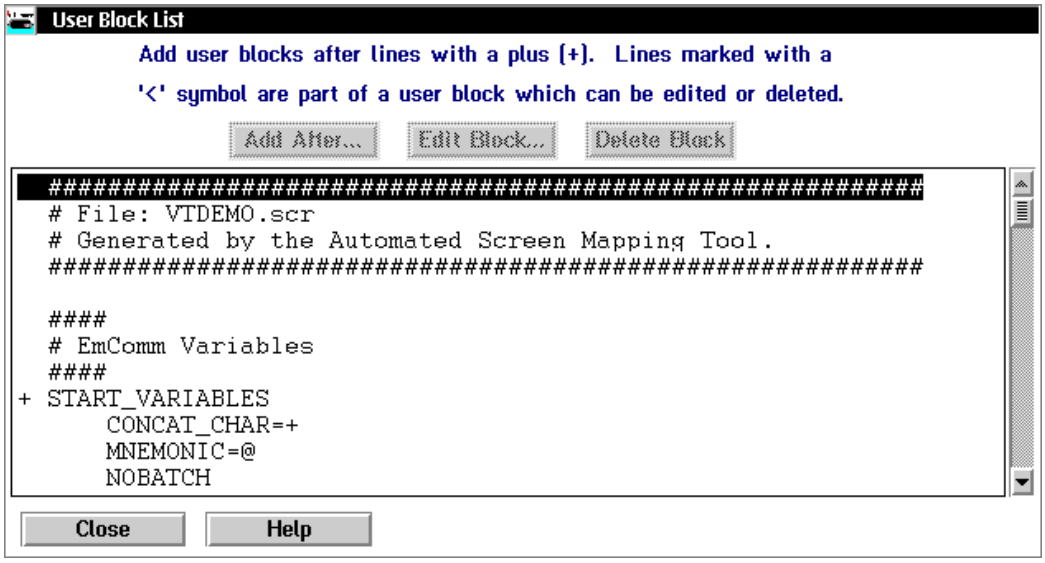
: A single colon precedes the label of a field or region.

The pound sign denotes comment lines.

To define a user block

1. From the Script Builder Tools window, choose Script.
2. Choose New/Open. The New/Open Script dialog box appears.
3. In the Script name field, click the down arrow on the right side of the field. A list of existing scripts appears. Choose the script to which you want to add user blocks.
4. Choose OK. The script opens.
5. Choose User Blocks. The User Block List dialog box appears.

User Block List Dialog Box



6. Add, edit, or delete user blocks. For help, see "Adding a User Block" later in this chapter.
7. Choose Close to return to the Script Builder Tools window.

Adding a User Block

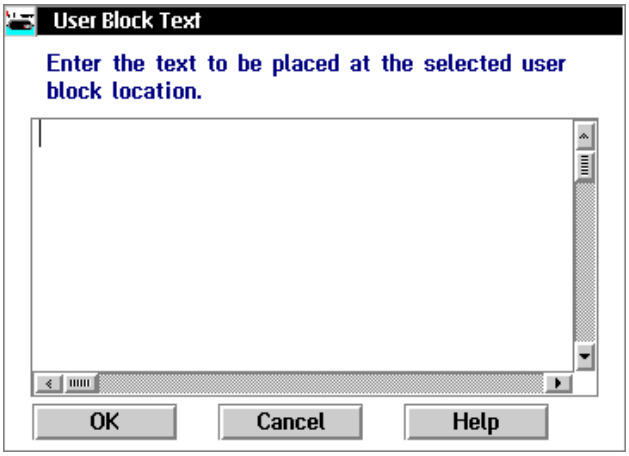
You can add user blocks after any line in the script that has a plus (+) sign in the left margin. Make sure you use the pound (#) character before any script comment.

Note: *Do not use the* ***Tab*** *key to add spaces before your user block. The* ***Tab*** *key will only shift the focus to the next control.*

The Script Builder Tool stores the user blocks in certain data structures so that it can reload them when the script file is closed and then reopened. If you delete a data structure, you may lose any user blocks that are associated with it. For example, you add a user block, BLOCK1, that contains a comment after a specific PUT_TRANS_FIELD command. If you delete the host screen field that generated the command, BLOCK1 is also deleted.

To add a user block

1. In the User Block List dialog box, select where you want to add the user block.
2. Choose Add After. The User Block Text dialog box appears.



3. Enter the comment or command.
4. Choose OK to return to the User Block List dialog box.

Viewing the Script

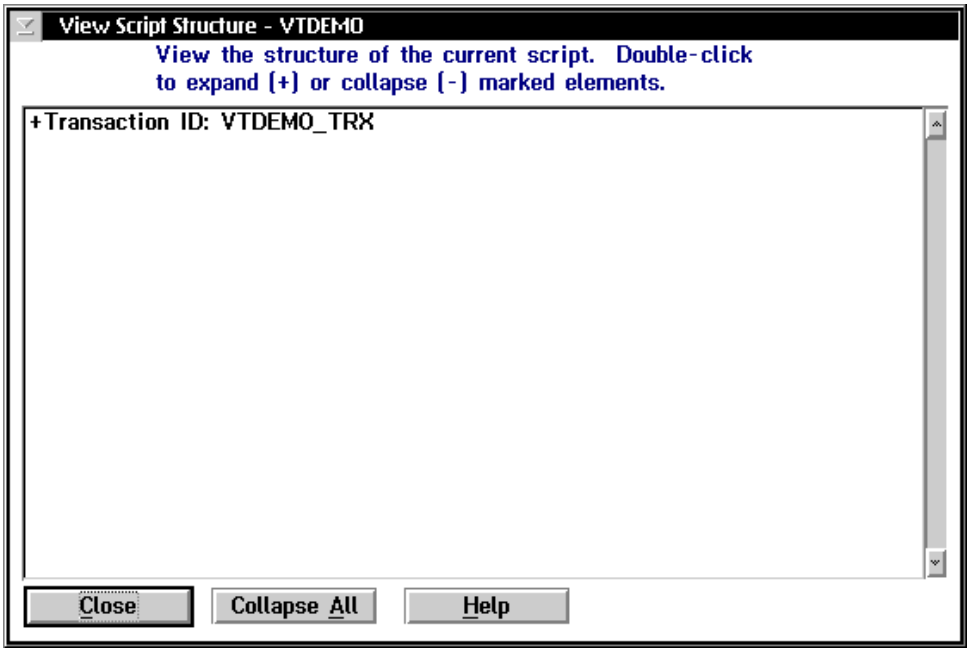
This feature provides you with a hierarchical view of the current script. Since the logic flow of the script is driven by transactions, the View Script feature displays the transactions as the top level in the script structure. You can expand the transaction level to see the host screens that receive data from the transaction. You may see these symbols in the script:

+ A plus sign indicates where you can expand the script.

- A minus sign indicates where you can collapse the script.

To view the script

1. From the Script Builder Tools window, choose View Script. The View Script Structure dialog box appears with the name of the script in the title bar.



2. Scroll through the script. A plus (+) on the left side of a line indicates that more information is underneath the heading that is collapsed.
3. Double-click on a line with a + on the left side to expand it.

   Or, double-click on a line with a minus (-) on the left side to collapse it.
4. Choose Collapse All to collapse all lines that are expanded.
5. Choose Close to return to the Script Builder Tools window.

Checking a Script File

When you finish editing the script file, you can use the script checker to check it for correct syntax. Intermec has also provided some general guidelines to help you check the logic of your script file. Always verify the script syntax before you verify the script logic.

Verifying the Script File Syntax

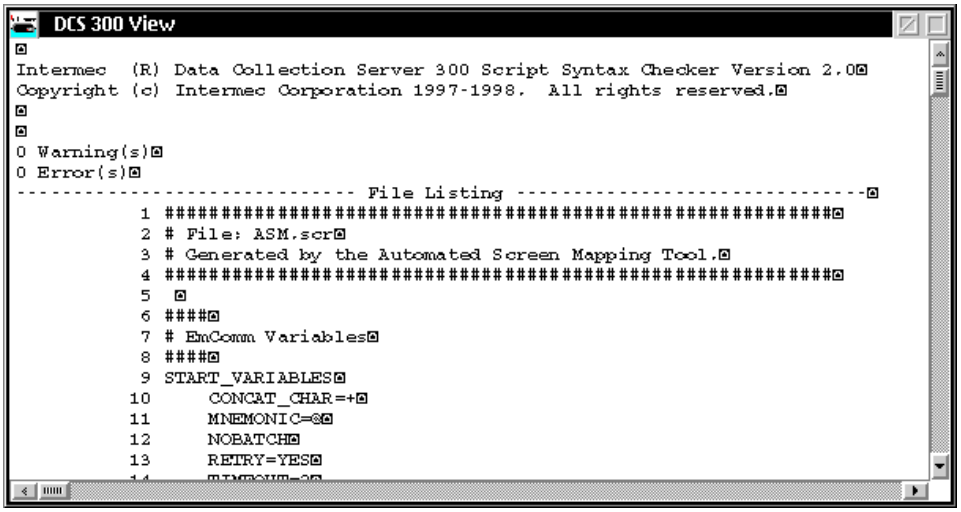
You can use the script checker to check your script file for correct syntax. However, the script checker cannot check the logic. For help checking the logic of your script file, see "Verifying the Script File Logic" in the next section.

Note: *You can also check your script file syntax in the Screen Mapping Session Definition dialog box.*

To check for correct syntax

1. From the Script Builder Tools window, choose Script.
2. Choose Check Script. The script checker checks the current script for syntax errors. The DCS 300 View Results window appears listing the errors that the script checker found. Refer to the example window below.
3. Note the error messages, if any. If you use the Script Builder Tool to create your script, you should not have any errors. You may see some warnings that you can ignore.
4. You may have errors in the user blocks. Edit the user blocks to correct the errors.
5. Repeat Steps 1 through 4 until the DCS 300 View Results window lists no more errors.

The top part of the DCS 300 View Results window displays the result of the script checker. You may see some errors and warnings. Your script file should still run with warnings, but you must resolve all errors.



Verifying the Script File Logic

To test the logic of the script file, you must set up a test environment and start data collection on the DCS 300. Then, you must use the Send Transaction feature to send every transaction to the script file and verify that the script file handles the transaction correctly.

When you test script files, you should provide many different sets of data and you should test as many scenarios as possible.

Note: *When testing VT script files, watch for timing problems.*

(Part 1) To verify the logic of a script file

1. Set up your test environment.

   Note: *If you already have started a host terminal session, make sure that the host terminal session is at the logon screen.*

   a. Add a screen mapping session for the script file. Select all the transactions that the script expects. Enable the Visible when data collection started? check box.

   b. Add a peer-to-peer destination. This destination will be the source of the transaction when you send transactions to the screen mapping session. It will also be the destination that receives output transactions from the screen mapping sessions.

2. From the main menu sidebar buttons, choose Save and Activate.
3. From the main menu sidebar, choose Start Data Collection.

Note: *If you stop data collection because the script fails, clear the Hot Standby file for the screen mapping session you are testing and make sure that the host terminal session is at the logon prompt before you restart data collection.*

Verify that

- the host terminal session opens.
- the logon sequence happens correctly.
- the main host screen appears and waits for a transaction.

Problem	Solution
The host terminal session does not appear.	Make sure that you checked the Visible when data collection started? check box in the Screen Mapping Session Definition dialog box. View the error log.
The main host screen does not appear.	Make sure that the keystrokes that you captured for the logon sequence are correct. For help, see "Creating a Logon Sequence" earlier in this chapter.
(VT only)	The logon sequence may have been sent before the sign on screen appears. Add logic to the script file so that it waits for the sign on screen before it sends the logon sequence. For example, see VTDEMO.SCR in the USERDATA\SCRIPTS directory on the server.

(Part 2) To verify the logic of a script file

1. Open testing and viewing tools.
    a. From the System Maintenance dialog box, open the Send Transaction dialog box.
    b. From the System Maintenance dialog box, open the Receive Transactions dialog box. In the Application List dialog box in the Application name field, enter the peer-to-peer destination name that you defined earlier. Choose Add.
    c. From the System Diagnostics dialog box, open the Trace Utility and configure a screen mapping trace.
    d. From the System Reporting dialog box, open the DCS 300 Status Monitor window (View Status Monitor command).
2. Test all successful transactions in the script file one at a time.
    a. In the Send Transaction dialog box in the Source ID field, enter the peer-to-peer destination name that you defined earlier.
    b. In the Transaction ID field, enter the transaction ID of the transaction you want to test.
    c. In the (D)ata or (S)ystem field, enter D.
    d. In the Data field, enter the data that the transaction needs to be successful. If the transaction contains data for multiple host screen fields, separate each field with a comma and make sure that the field order matches what you have defined in the script file.

Verify that

- the transaction data maps correctly to the host screen fields.
- if you use more than one host screen, when the transaction data is processed, you return to the main host screen.
- if you defined a message to send when the transaction is processed, the message appears in the Receive Transactions dialog box.
- (VT only) you do not have a timing problem. Send multiple transactions as fast as you can. If you send transactions faster than the response time of the host, the script file should wait for the host to be ready to receive data. The script file should always check to see if the host screen is ready before it maps data to it.

Problem	Solution
The script file is stuck in a host screen and cannot finish processing the transaction data.	Make sure that the keystrokes that you captured that move you from one host screen to the next screen are correct.
Nothing happens on the host screen	Make sure that you entered the correct transaction ID in the Send Transactions dialog box. Make sure that the transaction ID you entered is listed in the Selected list box in the Screen Mapping Session Definition dialog box. View the Status Monitor window.
(VT only)	View the Status Monitor window. If you see the statement, "EMCOMM ERROR - A bad position was specified - cannot write data," the script file does not handle timing properly. The error log also tells you what field caused the error. The script file should always check to see if the host screen is ready before mapping data to it.

(Part 3) To verify the logic of a script file

- Test all failed transactions in the script file, one at a time. You need to make sure that the script file handles error conditions caused by bad transaction data.
  a. For each transaction, note all the regions that you have defined.
  b. For each region, use the Send Transaction dialog box to send a transaction that causes erroneous data to appear.

Verify that

- the script file handles the error properly. Usually, the script file clears the error condition, sends a message to notify the source that the transaction has failed, and then returns to the main host screen to wait for the next transaction.

Problem	Solution
The script file is stuck in a host screen.	View the logic that you defined for the region. If you defined a message to send when the region appears, check the Receive Transactions dialog box to see if the message was received. If the message exists, the script has caught the region. Verify that the keystrokes you captured that move from one host screen to the next screen are correct.
The message received is not what you expect.	If you define a region for a specific error and you also define a region for general errors and their locations overlap, make sure that the script checks the specific error before the general error. Define both regions in the same group and then use the Screen Event Ordering dialog box to adjust the region order.
(VT only) The script file does not catch the region even though you can see it on the host screen.	Due to the timing problem that occurs when the script file is executed faster than the host response time, the script file might check the region before the host sends the error message to the terminal screen. In the script file, add a PAUSE statement before the IF_REGION so the script file will pause for a certain amount of time before it checks the region.

(Part 4) To verify the logic of a script file

- Debug the script.
  a. Add some LOG_ERROR statements to your script file.
  b. View the Status Monitor window.
  c. Check the error messages that appear as the script is running.

Conclusion

When you have verified the logic of the script file on the server, you can try downloading your application and then running it. Verify the application as much as possible before you use it with the script file. The most common errors occur when the application expects to receive a response after it sends a transaction. Make sure that the script file only sends one message per transaction to the terminal; otherwise, messages are queued in the Hot Standby file and your application will get out of sync messages.

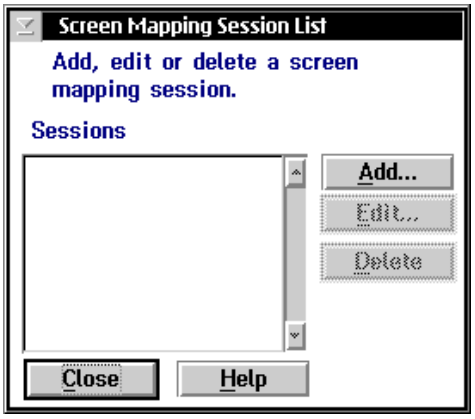
Setting Up Screen Mapping Sessions

When you define a screen mapping session, you define specific transactions to be sent to a specific host terminal session using a specific script file. Screen mapping sessions allow multiple terminal sessions on the server to simultaneously communicate with multiple terminal emulator sessions running on different hosts. Before you proceed, make sure you have performed these tasks:

- Defined each host terminal session you want to connect to a screen mapping session. One screen mapping session connects to one host terminal session.
- Named each script you want to use. Each script may use many transactions. To send transactions to a different host using the same script file, you define another screen mapping session that connects to the appropriate host session.
- Defined the transactions you want to route to each host terminal session using the script file.

To set up a screen mapping session

1. From the main menu, choose Screen Mapping.
2. Choose Sessions. The Screen Mapping Session List dialog box appears.



3. The Sessions list box lists all the sessions that are defined for screen mapping. From this dialog box you can add new sessions, or you can edit or delete existing sessions. For help, see “Adding a Screen Mapping Session” later in this chapter.
4. Choose Close to close the dialog box and return to the main menu.

Adding a Screen Mapping Session

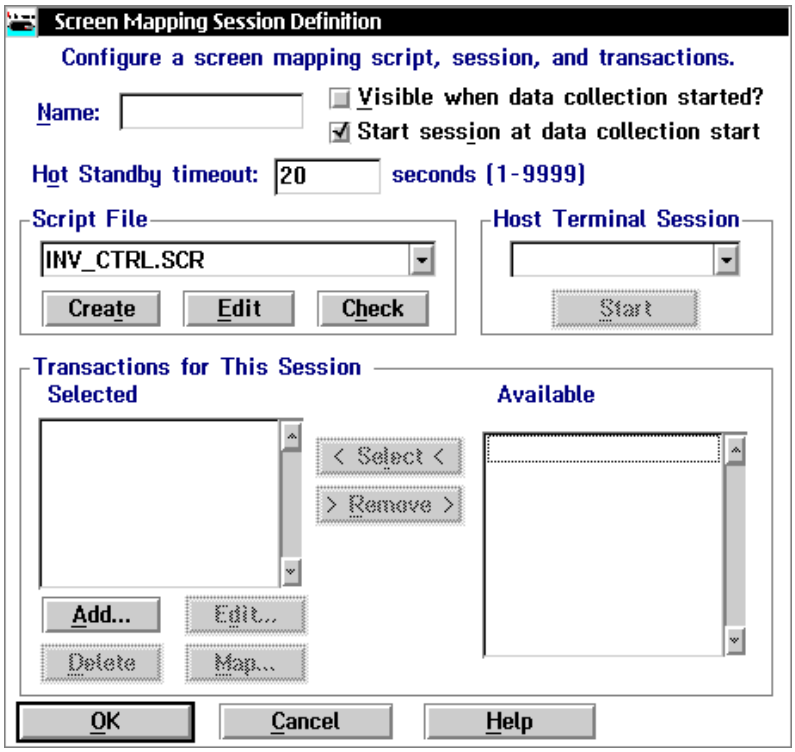
Intermec highly recommends that you use the Script Builder Tool for creating and editing script files. In the Screen Mapping Session Definition dialog box, if you choose Create or Edit and then you save your changes, the Script Builder Tool will not recognize the script file and you will not be able to open this script file using the Script Builder Tool.

Visible when data collection started? check box You may want to view the host terminal session when you develop and debug your screen mapping applications. However, you should not use this feature when you actually run your application because it will affect the server performance. If you check this check box, the host terminal session opens when you start data collection. Then, you can watch your host screen fields being filled in as they receive transactions from the server.

Start session at data collection start check box You may want to immediately run your screen mapping application when you choose Start Data Collection. If you check this check box, the server starts the screen mapping session and is ready to accept transactions from devices.

To add a screen mapping session

- From the Screen Mapping Session List dialog box, choose Add. The Screen Mapping Session Definition dialog box appears.



Field	Description	Value	Default
Name	A meaningful name that identifies this screen mapping session.	1 to 8 alphanumeric characters	None
Visible when data collection started?	This check box determines if the screen mapping application automatically opens the host terminal session when you start data collection.	Check, Clear	Clear
Start session at data collection start	This check box determines if the screen mapping application automatically starts when you start data collection.	Check, Clear	Check
Hot Standby timeout	The number of seconds the DCS 300 waits for a response from the data collection device before it places the device in Hot Standby mode.	1 to 9999	20
Script File	The name of the script file that this screen mapping session uses.	Predefined	None
Host Terminal Session	The long session ID of the terminal session that this screen mapping session uses.	Predefined	None
Selected	This list box contains the transactions that send data to the selected host terminal session using the selected script file. For help, see “Adding a Transaction” in Chapter 9.	None	None
Available	This list box contains all the available transactions that you can use.	Predefined	None

Mapping Transaction Fields

If your script does not contain explicit transaction mapping information, you need to map the transaction fields to the host screen fields. You only need to map the transaction fields if you are using the PUT_MAPPED_TRANS command in your script file.

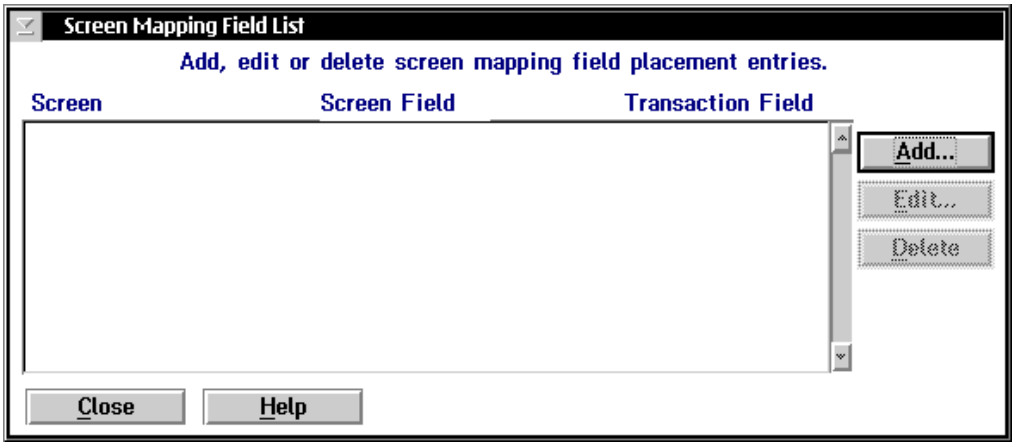
For VT screen mapping, when using the PUT_TRANS_FIELD command, the script executes an implied WAIT_FOR_LABEL_POS command for the field specified in the PUT_TRANS_FIELD. The WAIT_FOR_LABEL_POS command waits for the cursor to be at the field before the PUT_TRANS_FIELD command maps the field. Generally, the WAIT_FOR_LABEL_POS timeout period is the same as the VT_WAIT timeout period.

Note: *If you insert the WAIT_FOR_LABEL_POS command as a user block, you must specify the wait period.*

The Script Builder uses the PUT_TRANS_FIELD command, which explicitly maps a transaction field to a host screen field. If you use the Script Builder to generate your script files, you usually do not need to map transaction fields. **Intermec highly recommends that you use the Script Builder Tool to generate your script files.**

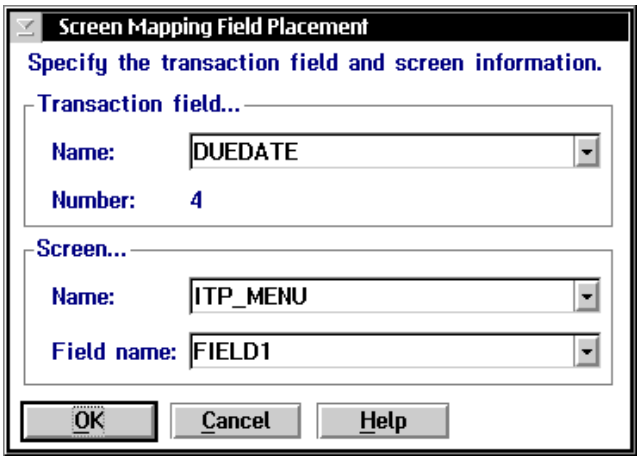
To map transaction fields to screen fields

1. From the Screen Mapping Session Definition dialog box, select the transaction whose fields you want to map to screen fields.
2. Choose Map. The Screen Mapping Field List dialog box appears.



3. Add, edit, or delete screen mapping fields from the list box. For help, see "Adding a Screen Mapping Field Placement Entry" later in this chapter.
4. Choose Close to close the dialog box and return to the Screen Mapping Session Definition dialog box.

Adding a Screen Mapping Field Placement Entry



1. From the Screen Mapping Field List dialog box, choose Add. The Screen Mapping Field Placement dialog box appears.
2. In the Transaction field box Name field, click the down arrow on the right side of the field. A list of the transaction fields for the transaction you selected appears. Select the transaction field you want to map.
3. In the Screen box Name field, click the down arrow on the right side of the field. A list of the screens that are defined in your script file appears. Select the screen that contains the field that you want to map to the transaction field.
4. In the Screen box Field name field, click the down arrow on the right side of the field. A list of the fields that are defined for that screen in your script file appears. Select the field name that you want to map to the transaction field.
5. Choose OK to save your changes and return to the Screen Mapping Field list dialog box.

Saving and Activating Your Run-Time Configuration

When you finish configuring screen mapping, you should save your changes. If you have finished configuring your server, activate your run-time configuration. When the activate is complete, a message box appears if you need to reboot the server.

To save and activate your run-time configuration

1. From the main menu sidebar buttons, choose Save and Activate. The Activate Configuration message box appears.
2. Choose Activate. The server saves your run-time configuration to disk and it becomes your active configuration.

If you are ready to start data collection, from the main menu sidebar buttons, choose Start Data Collection.

Script Builder Tool Limitations

Validation can be performed by the data collection device or the host application. The script cannot perform any validation.

The Script Builder Tool cannot generate these commands:

ACK_MESSAGE	IF_BATCH	SEARCH_SCREEN
AUDIT	IF_SEARCH	USER_INPUT
CAPTURE_POS	LOG_ERROR	WAIT_FOR_POS
FILL_FIELD	PAUSE	WAIT_FOR
IF_	PUT_MAPPED_TRANS	WAIT_FOR_LABEL_POS

If you need to use these commands, you can define a user block to insert these commands into the script. For help, see "Defining User Blocks" earlier in this chapter.

PUT_TRANS_FIELD The format of this command that the Script Builder Tool generates is:

```
PUT_TRANS_FIELD transactionfieldnumber fieldlabel
```

where:

transaction field number is the position of the field in the transaction.

field label is the name of the host screen field you want to map to the transaction field.

In the *DCS 300 Technical Reference Manual*, there are two optional parameters following the field label that let you map partial data to a host field. The Script Builder Tool does not support partial data mapping. These parameters are:

SEND_MESSAGE There are two types of messages: status and transaction.

For status messages, the format of this command that the Script Builder Tool generates is:

```
SEND_MESSAGE "TERM_MESSAGE," + userdefinedtext + [regionlabel |
CUR_POS | CUR_ROW] SRC
```

Status messages always starts with "TERM_MESSAGE," which is automatically generated. The destination is always fixed to SRC, the source of the transaction, which is assumed to be an Intermec terminal. The SRC can only receive the message if the Wait for response check box is checked in the Terminal Screen and Fields dialog box.

For transaction messages, the format of this command that is generated by Script Builder Tool is:

```
SEND_MESSAGE userdefinedtext + [regionlabel | CUR_POS | CUR_ROW]
SRC
```

The user-defined text contains data in the format of a transaction and again the destination is fixed to SRC. This type of message is delivered to the source of the transaction and the transaction data is mapped to the terminal screen according to the terminal template definition.

In the *DCS 300 Technical Reference Manual*, the SEND_MESSAGE command lets you specify a destination other than SRC. You can also have as many concatenations as you want, as long as the string does not exceed the maximum line length. If the Script Builder Tool generates the SEND_MESSAGE command, you are restricted to these formats.

CURRENT_SCREEN The Script Builder Tool generates this command and places it as the first line of every set of events for each transaction. The screen label for this command is the main screen, since every set of events for each transaction starts from processing the main screen events. You cannot control where this command appears in the script.

VT/ANSI Screen Mapping Limitations

VT/ANSI terminals have some limitations that affect how you can use screen mapping. However, if you are having problems because of a limitation, you can use the WAIT_FOR scripting command. For help, see the *DCS 300 Technical Reference Manual*.

- You cannot automatically position the host cursor to the host screen field in VT/ANSI screen mapping. However, you can program the script to wait until the cursor is at the field using the WAIT_FOR command. To move the host cursor to the desired host screen field, you add keystrokes, such as NEWLN, to the script. When you define a host screen field in Script Builder, you can define an exit keystroke that will be applied after field mapping. If the exit field keystroke will not move the host cursor to the next host screen field, you can define keystrokes using the user block feature. Make sure that you add these keystrokes before the PUT_TRANS_FIELD command for the next field.
- When the host VT/ANSI screen is in Scroll mode and the host is using pseudo field-formatted screens, the server does not know where to put the data on the host screen. You must use the script WAIT_FOR commands so the server knows when the host is done sending data.
- VT terminal sessions and the VT windows that are displayed on the DCS 300 screen cannot show blinking text. If the host application sends blinking text to a VT terminal session, the DCS 300 shows the text as white text on a dark red background. If it sends blinking text to a VT window, the DCS 300 shows the text as green text on a black background.

VT Keyboard Mapping and Script Keystroke Names

This table shows how VT keyboard keys map to the DCS 300 keyboard and to the script keystroke names. For a diagram of how the VT keyboard maps to the server keyboard, see Chapter 8, "Using Terminal Emulation."

VT Keyboard	Server Keyboard	Script Name
Enter (keypad)	Enter (keypad)	ENTER
, (keypad comma)	+ (keypad plus)	CLEAR
Not used	Not used	LTAB
Tab	Tab	RTAB
Delete	Backspace	DEL
Ctrl-H	Shift-Backspace	BACKSP
Insert	Insert	INS
- (keypad minus)	Shift-+ (keypad plus)	ERS_EOF
Cursor left	Cursor left	CUR_LFT
Return	Enter (keyboard)	NEWLN
Spacebar	Spacebar	SPACE
Not used	Not used	RESET
Cursor up	Cursor up	CUR_UP
Cursor down	Cursor down	CUR_DN
Cursor right	Cursor right	CUR_RT
Find	Home	HOME
PF1	Num Lock	PF1
PF2	/ (keypad forward slash)	PF2
PF3	* (keypad asterisk)	PF3
PF4	- (keypad minus)	PF4
Not used	Not used	PF5

VT Keyboard Map (continued)

VT Keyboard	Server Keyboard	Script Name
F6	F6	PF6
F7	F7	PF7
F8	F8	PF8
F9	F9	PF9
F10	Alt-F10	PF10
F11	Shift-F1	PF11
F12	Shift-F2	PF12
F13	Shift-F3	PF13
F14	Shift-F4	PF14
F15/Help	Shift-F5	PF15
F16/Do	Shift-F6	PF16
F17	Shift-F7	PF17
F18	Shift-F8	PF18
F19	Shift-F9	PF19
F20	Shift-F10	PF20
0 (keypad 0)	0 (keypad 0)	PF21
1 (keypad 1)	1 (keypad 1)	PF22
2 (keypad 2)	2 (keypad 2)	PF23
3 (keypad 3)	3 (keypad 3)	PF24
4 (keypad 4)	4 (keypad 4)	END
Prev Scrn	Page up	PAGEUP
Next Scrn	Page down	PAGEDN
Select	End	PA1
Remove	Delete	PA2
Ctrl-[	Esc	PA3
5 (keypad 5)	5 (keypad 5)	TEST
6 (keypad 6)	6 (keypad 6)	SYSREQ
7 (keypad 7)	7 (keypad 7)	ATTN
8 (keypad 8)	8 (keypad 8)	FLDPLUS
9 (keypad 9)	9 (keypad 9)	FLDMINUS
. (keypad decimal point)	. (keypad decimal point)	FLDEXIT

Keystrokes

A keystroke can be a mnemonic or a string. The table below lists the 3270 and 5250 keystroke mnemonics supported by the server.

Key	Mnemonic	Key	Mnemonic
Attention	ATTN	Home	HOME
Backspace	BACKSP	Insert	INS
Clear	CLEAR	Left Tab	LTAB
Cursor Down	CUR_DN	New Line	NEWLN
Cursor Left	CUR_LFT	No Keystroke	NONE
Cursor Right	CUR_RT	PA1, PA2, PA3	PA1, PA2, PA3
Cursor Up	CUR_UP	Page Down	PAGEDN
Delete	DEL	Page Up	PAGEUP
End	END	Reset	RESET
Enter	ENTER	Right Tab	RTAB
Erase EOF	ERS_EOF	Space	SPACE
Field Exit	FLDEXIT	System Request	SYSREQ
Function Keys F1 - F24	PF1 - PF24	Test	TEST

A

Troubleshooting

This appendix describes the troubleshooting tools that are provided in the System Reporting and System Diagnostics sidebar buttons.

General Troubleshooting

These problems are general system problems that may occur while you are using the DCS 300.

Problem	Solution
The Intermec controller is not communicating with the DCS 300.	Make sure that you have defined the correct configuration for the controller on the DCS 300. Make sure you are using the correct Intermec cable. Replace the cable. Replace the serial card.
The green LED on the Ethernet card is not lit and the card is not communicating with the network.	Make sure that your Ethernet cable is securely plugged into the card and into an Ethernet connection. The default configuration for the Ethernet card is 10BaseT. If you are using 10Base2 or 10Base5, contact your local Intermec representative. Replace the cable. Replace the card.
The green LED on the token ring card is not lit and the card is not communicating with the network.	Make sure that your token ring cable is plugged into the card and into a token ring connection. If you are connected to a 4-Mbit ring, you need to reconfigure the card. Contact your local Intermec representative.
The green LED on the RF card is not lit and the card is not communicating with the network.	Verify that the devices are configured properly and are attempting to communicate with the network. Verify that you have configured the RF card and started data collection. Make sure that all cables are securely plugged into their connections. Contact your local Intermec representative.

General Troubleshooting (continued)

Problem	Solution
The Intermec controllers are not communicating with the network.	Make sure the configuration for the controller in the DCS 300 GUI matches the configuration in the controller. Make sure that you are using the correct cables to connect your controller to your network. Contact your local Intermec representative.
Keystrokes are not displayed in a field.	Make sure your keyboard connector is securely seated in the keyboard port on the DCS 300. With the keyboard connected, shut down the DCS 300 and boot it. A keyboard echo failure has occurred. To release the keyboard, hold down the right-hand **Alt** key and press the right-hand **Ctrl** key. Replace the keyboard.
The mouse does not work.	Make sure that your mouse connector is securely seated in the mouse port on the DCS 300. When the DCS 300 experiences electrical fast transients, the mouse may not work for a short period of time. Wait a few seconds and try using it again. Replace the mouse.

Using the System Reporting Tools

Use these tools and features, which are available under the System Reporting sidebar button, to help you troubleshoot error conditions:

View runtime configuration Shows you the active (run-time) configuration. Use this feature to look at this configuration to determine what parameters you have defined. You can also save this file.

View Hot Standby files Shows the contents of any Hot Standby files that reside on the server. You can also erase all messages in a Hot Standby file.

View Status Monitor Shows the most recent error messages as they are being written to the error log file.

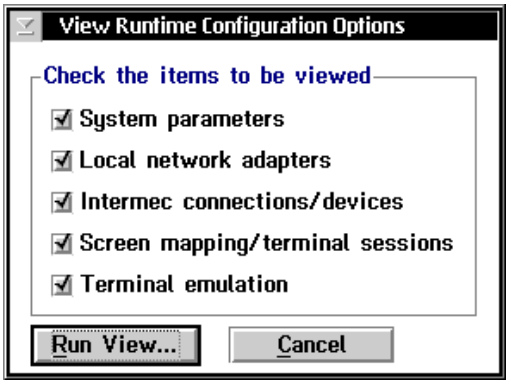
View error log Provides information about message boxes and the error log. This section also gives you ideas about how to troubleshoot problems.

Viewing the Run-Time Configuration

The DCS 300 produces a configuration file that you can view to verify the parameters that you have defined for the active configuration.

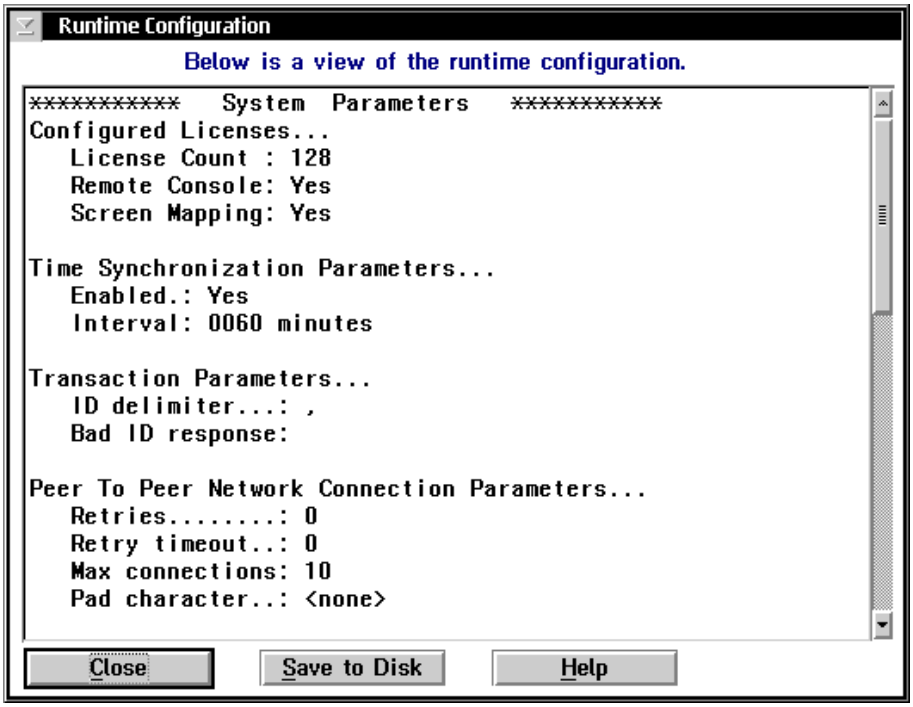
To view the configuration

1. From the main menu sidebar buttons, choose System Reporting. The System Reporting dialog box appears.
2. In the System Reporting list box select View Runtime Configuration(s) and then choose Start. The View Runtime Configuration Options dialog box appears.



3. Check the configuration items that you want to view.
4. Choose Run View. The Runtime Configuration dialog box appears.

Runtime Configuration Dialog Box



5. Use the vertical scroll bar on the right side of the dialog box to view your run-time configuration.
6. If you want to save the file to the server, choose Save to Disk.
7. Choose Close to close the dialog box and return to the System Reporting dialog box.

Viewing and Clearing the Hot Standby Files

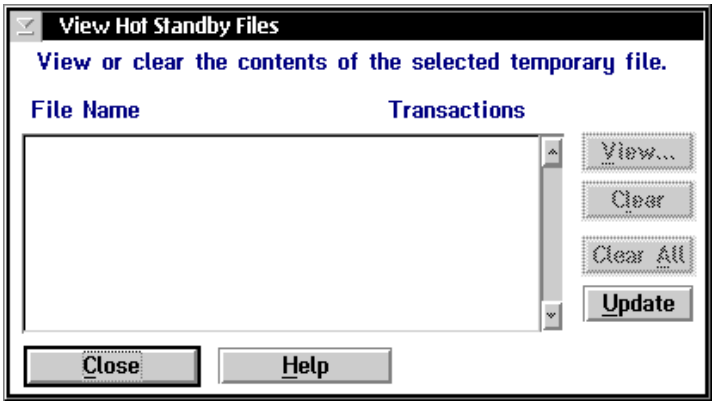
You can view the contents of the Hot Standby files that the DCS 300 creates when it places an application or device in Hot Standby mode. The server waits a certain period of time, which is set in the Hot Standby timeout, after delivering a transaction to an application or device to receive an acknowledgment for the transaction. If it does not receive an acknowledgment, the server writes all transactions for the application or device to a Hot Standby file. The application or device receives its transactions from the Hot Standby file when it either sends an acknowledgment to the most recently delivered transaction or when it sends a system transaction. Before the application or device becomes interactive, it receives all the transactions from oldest to newest that are in its Hot Standby file.

You can use the Clear and Clear All buttons to erase all the messages in one Hot Standby file or to erase all the messages in all the Hot Standby files. You cannot erase single messages in a Hot Standby file.

Clearing the Hot Standby files can interrupt data flow and you may lose transactions. For example, if you clear a Hot Standby file while transferring a file, the transfer stops, times out, and logs an error in the error file. Also, if you clear the Hot Standby file for an application while the application is connected to the controller, the application may need to send an Inter system transaction to resume communications.

To view a Hot Standby file

1. From the main menu sidebar buttons, choose System Reporting. The System Reporting dialog box appears.
2. In the System Reporting list box, select View Hot Standby Files and then choose Start. The View Hot Standby Files dialog box appears.



3. Choose Update to make sure that you have the most current list.
4. Select the File Name that represents the Hot Standby file that you want to view and then choose View. The Hot Standby file appears.

To clear one or more Hot Standby files

1. From the main menu sidebar buttons, choose System Reporting. The System Reporting dialog box appears.
2. In the System Reporting list box, select View Hot Standby Files and then choose Start. The View Hot Standby Files dialog box appears.
3. Choose Update to make sure that you have the most current list.
4. Select the File Name that represents the Hot Standby file that contains all the messages that you want to delete and then choose Clear.

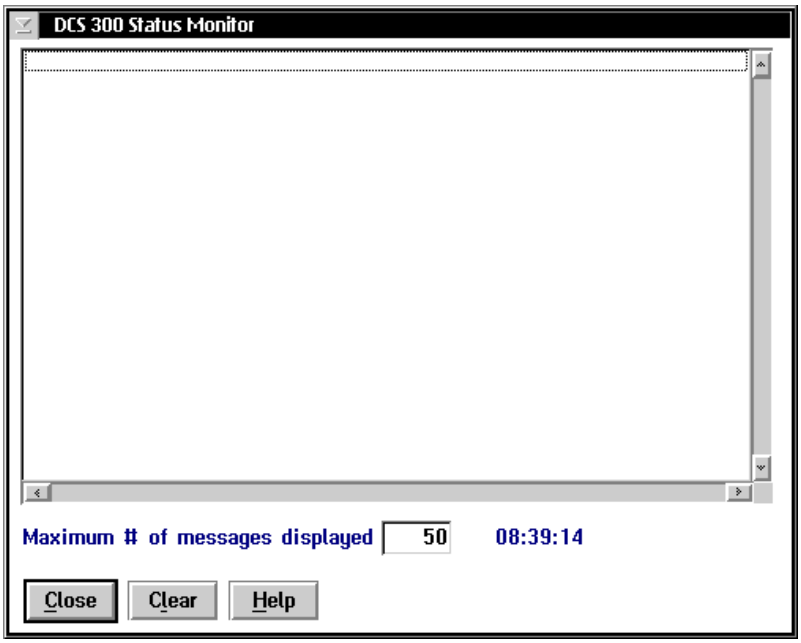
   Or, choose Clear All to delete all the error messages in all the Hot Standby files.

Viewing the Status Monitor

The DCS 300 Status Monitor provides a run-time view of the error messages. That is, it displays the most recent error messages as they are being written to the error log file. The clock in the lower right corner of the dialog box lets you verify the exact time when the error message occurred.

To view the error log

1. From the main menu sidebar buttons, choose System Reporting. The System Reporting dialog box appears.
2. In the System Reporting list box select View Status Monitor and then choose Start. The DCS 300 Status Monitor dialog box appears.



3. In the Maximum # of messages displayed field, enter the number of error messages you want to list in the status monitor (10-9999). The default is 50 messages. When the number of error messages reaches this number, the oldest message is deleted.

   Note: *Intermec recommends that you do not make this number too large since these error messages are stored in RAM.*

   For help viewing the error log, see "Viewing Error Messages" in the next section.
4. Choose Clear if you want to clear all the messages in the status monitor.
5. Choose Close to close the dialog box and return to the System Reporting dialog box.

Viewing Error Messages

There are two types of error messages that you may encounter when you are working on the DCS 300:

- message box error messages
- error log error messages

If you cannot troubleshoot and fix an error message:

1. Write down the entire text of the message that is in the message box.
2. If the error message says to view the error log, open the error log.
3. Contact your network administrator to help you solve the problem.
4. Contact Intermec Technical Support to help you solve the problem.

Message Box Error Messages

Message box error messages appear in message boxes on the DCS 300 screen. If your error message refers to the error log, then you must view the message in the error log. For help see "Error Log Error Messages" in the next section.

Error Log Error Messages

The error log, NGERROR.LOG, provides a static view of all the error messages. If new error messages are generated while you are viewing the error log, you will not see them until you open the error log the next time. If you want to view error messages as the DCS 300 is logging them, open the status monitor. For help, see "Viewing the Status Monitor" earlier in this section. When messages are logged to the error log, no message box appears on the screen.

The error log is limited to 700K and has two backup versions. When NGERROR.LOG reaches 700K, it is renamed to NGERLOG1.BAK. The next time the error log is full, NGERLOG1.BAK is renamed to NGERLOG2.BAK. Then, NGERROR.LOG becomes NGERLOG1.BAK. NGERLOG2.BAK is not backed up.

Error log error messages are divided into the following parts:

- The first line contains the date and time the message was generated and information about the message, including the source that generated it.

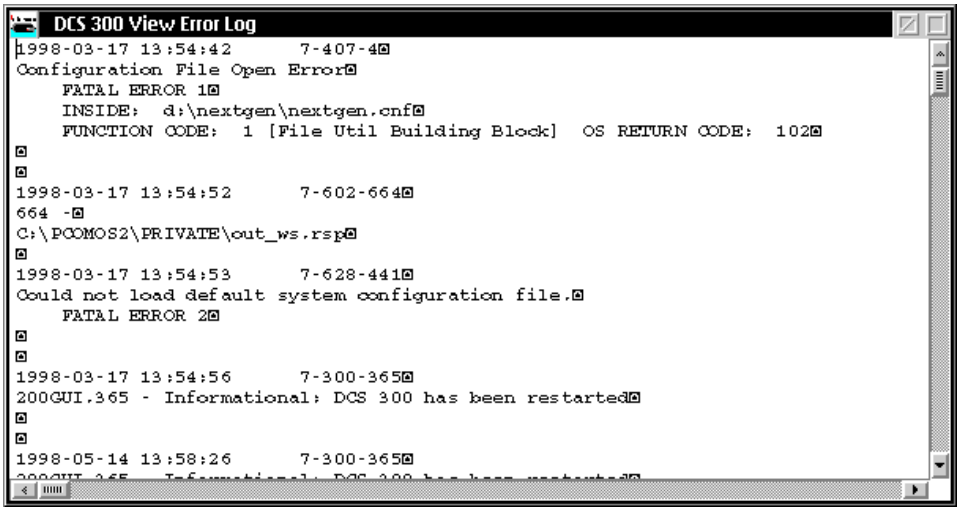
  The format *w-xxx-yyy* represents: *w* is the subsystem number (the server is system 7), *xxx* is the module number of the source code, and *yyy* is the specific message number.
- The second line contains the specific message.
- There may be other lines that contain arguments pertaining to the error.

Example

```
1996-08-25 11:28:55 7-952-248
EMCOMM ERROR - The transaction Id was not found in configuration
file
  FATAL ERROR 10
  INSIDE: TEST002
  FUNCTION CODE: 6 [Bad Data from Config File]
```

To view the error log

1. From the main menu sidebar buttons, choose System Reporting. The System Reporting dialog box appears.
2. In the System Reporting list box, select View Error Log and then choose Start. The DCS 300 View Error Log window appears.



3. Use the horizontal and vertical scroll bars to view the error messages.

Double-click on the box in the upper left corner to close the dialog box and return to the System Reporting dialog box.

Using the System Diagnostics Tools

Use these tools and features, which are available under the System Diagnostics sidebar button, to help you troubleshoot error conditions:

Message Log Formatter Lets you view the OS/2 message log file (OS2MLOG.DAT) that contains messages that are generated by the DCS 300.

SNA Subsystem Management Helps you troubleshoot the DCS 300 by showing you the current status of links, sessions, and transaction programs. You can change the status of many communication processes on the DCS 300 and watch the immediate effects of these changes.

Trace Utility Records the information processing through the server message handler queues during data collection. You can display the trace results and you can save the file.

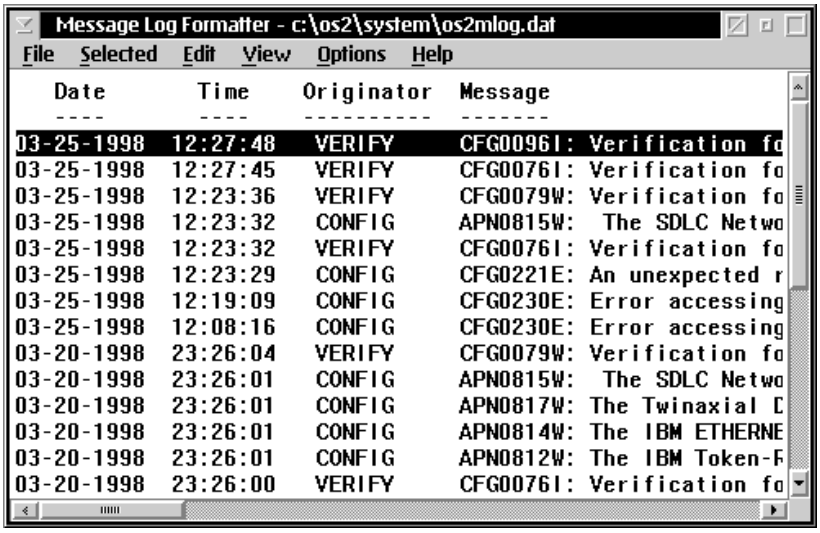
Using the Message Log Formatter

This system diagnostics tool lets you view the OS/2 message log file (OS2MLOG.DAT). Using this tool, you can also change the format of the messages and save the file.

Note: *If you choose File and then you choose Save As, the Message Log Formatter - Save As dialog box appears. In the Select output type box, choose Formatted text.*

To use the message log formatter

1. From the main menu sidebar buttons, choose System Diagnostics. The System Diagnostic Tools dialog box appears.
2. In the System Diagnostic Tools list box select Message Log Formatter and then choose Start. The Message Log Formatter window appears.



3. Use the horizontal and vertical scroll bars to view the error messages. For help using this tool, see the Help menu that is provided by IBM PComm.

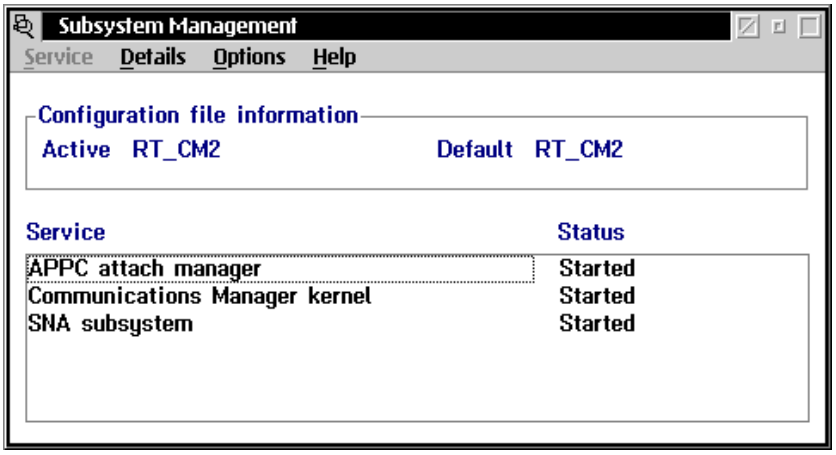
Double-click on the box in the upper left corner to close the dialog box and return to the System Diagnostic Tools dialog box.

Using SNA Subsystem Management

This system diagnostics tool shows you the current status of links, sessions, and transaction programs. You can change the status of many communication processes and watch the immediate effects of these changes on the DCS 300.

To use SNA subsystem management

1. From the main menu sidebar buttons, choose System Diagnostics. The System Diagnostic Tools dialog box appears.
2. In the System Diagnostic Tools list box select SNA System Management and then choose Start. The Subsystem Management window appears.



For help using this tool, see the Help menu that is provided by IBM PComm. Double-click on the box in the upper left corner to close the dialog box and return to the System Diagnostic Tools dialog box.

Using the Trace Utility

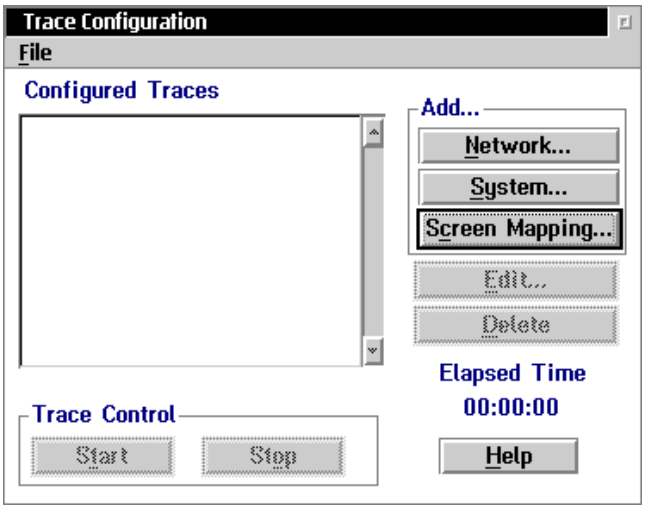
This system diagnostics tool provides you with ways to configure and run traces on the peer-to-peer network connections, downline device communications, and screen mapping sessions. The Trace utility combines features from IP trace and SNA trace applications that are provided with the IBM PComm product.

You add trace components one at a time. Each type of trace has a different set of trace options associated with it. You can monitor system traces in the Monitor Message Handler dialog box while they are running. To view the network trace or the screen mapping trace, you need to stop the trace and then use the File menu command. The server saves all of the traces in the D:\SYSDIAG\TRACEUTL\CURRENT directory.

Note: *Each time that you start a new trace, the utility discards the previous trace files.*

To start the Trace utility

1. Make sure that you have saved and activated your run-time configuration.
2. Make sure that you have started data collection.
3. From the main menu sidebar buttons, choose System Diagnostics. The System Diagnostic Tools dialog box appears.
4. In the System Diagnostic Tools list box select Trace utility and then choose Start. The Trace Configuration dialog box appears.



5. Add all the trace components to the Configured Traces list box. For help, see "Adding a Network Trace," "Adding a Screen Mapping Trace," and "Adding a System Trace" in the next sections.
6. In the Trace Control box, choose Start. A message box appears confirming that you want to start all the traces.

7. Choose Start. The Elapsed Time clock starts. If you added any system traces, the Monitor Message Handler Transactions dialog box appears.

To stop the Trace utility

- In the Trace Control box, choose Stop. The Elapsed Time clock stops.

To view a trace

1. From the Trace Configuration dialog box, in the Configured Traces list box, select the trace that you want to view.
2. In the menu bar, choose the File menu command and then choose View Trace Files. An edit window opens for each trace file that was generated. For help using these windows, see the Help menu that is provided by IBM.

To save a trace

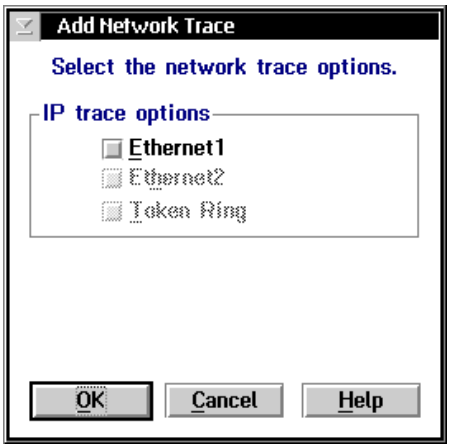
1. From the Trace Configuration dialog box, choose the File menu command.
2. Choose Backup Trace Files. A message box appears instructing you to insert a blank formatted disk in your disk drive.
3. Choose Backup. The trace files are backed up to the disk.

Adding a Network Trace

Network traces can be useful when troubleshooting IP traffic on the Ethernet or token ring network. The network trace is called IPTRACE.TXT.

To add a network trace

1. From the Trace Configuration dialog box, choose Network. The Add Network Trace dialog box appears.



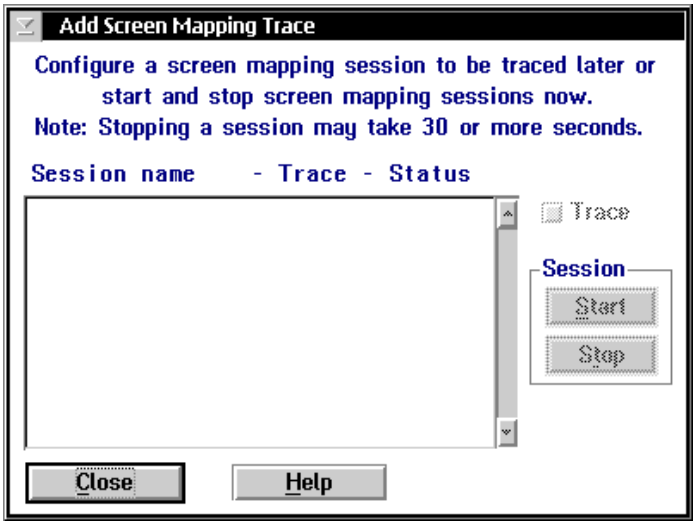
2. In the IP Trace Options box, check the appropriate network traces. You can only enable the traces if the network card is installed in the server.
3. Choose OK. The trace appears in the Configured Traces list box.

Adding a Screen Mapping Trace

Screen mapping traces are useful when troubleshooting the script files. The screen mapping trace file is called *script*.SM, where *script* is the name of the script file that you are tracing.

To add a screen mapping trace

1. From the Trace Configuration dialog box, choose Screen Mapping. The Add Screen Mapping Trace dialog box appears.



2. In the Session Name - Trace - Status list box, you can see all the screen mapping sessions that you have configured.
3. In the Session box, start any sessions that you need by selecting the session and then choosing Start.

   Note: *You may need to start a session even if you do not want to run a trace on it because the session that you are tracing may be dependent on it.*

4. Select the session that you want to trace by highlighting the session and checking the Trace check box.
5. Choose Close. The trace appears in the Configured Traces list box.

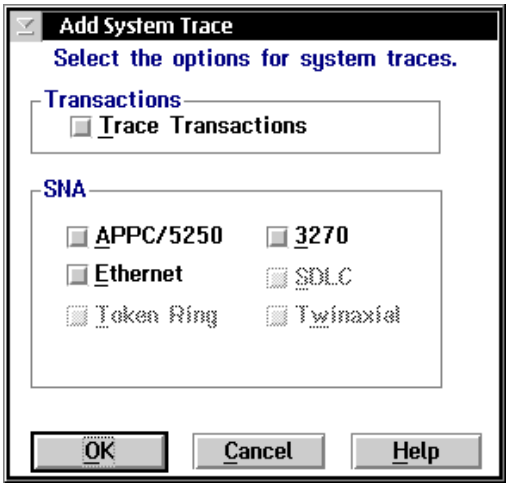
Adding a System Trace

System traces are useful in tracing transactions and SNA traffic on the system. While you are running a system trace, you can watch the traces in the Monitor Message Handler Transactions dialog box. For help, see "Understanding the Monitor Message Handler Transactions Dialog Box" later in this appendix.

The transaction trace file is called TRXTRACE.TXT and it contains up to 10,000 transactions in the order that the DCS 300 received the transactions. The SNA trace file is called SNATRACE.TXT.

To add a system trace

1. From the Trace Configuration dialog box, choose System. The Add System Trace dialog box appears.



2. In the Transactions box, check the Trace transactions check box if you want to record transactions.
3. In the SNA box, check the appropriate SNA traces.
4. Choose OK. The trace appears in the Configured Traces list box.

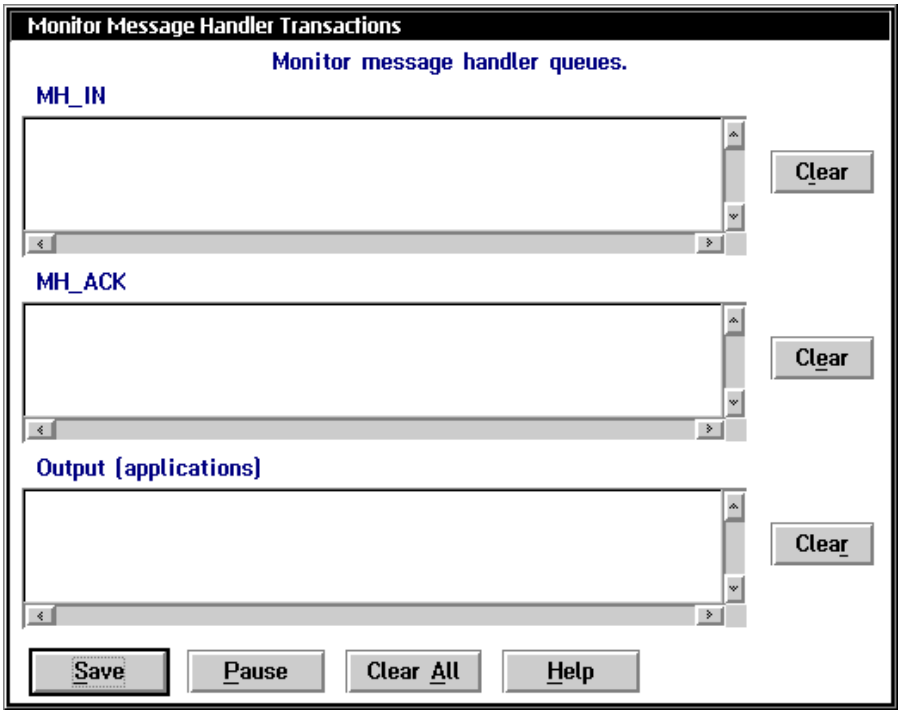
Understanding the Monitor Message Handler Transactions Dialog Box

When you start a system trace or a screen mapping trace, the Monitor Message Handler Transactions dialog box appears. As you send transactions from your devices to the hosts, you can view the traces.

MH_IN This box records the information that enters the message handler Receive (input) channel. Choose Clear to clear the information in the box.

MH_ACK This box records the information that enters the message handler ACK channel. Choose Clear to clear the information in the box.

Output (applications) This box records the information that the message handler sends to the applications and devices.



To pause the system trace

- Choose Pause.

To save the system trace

- Choose Save. The results are stored in the USERDATA\NGTRACE.DAT file.

To close the Monitor Message Handler Transactions dialog box

1. Move the Monitor Message Handler Transactions dialog box so that you uncover the Trace Configuration dialog box.
2. Choose Stop. The trace stops and the Monitor Message Handler Transactions dialog box closes.

B

Helpful Information

This appendix provides helpful information for using the DCS 300 to verify your network connections, to transfer files, and to configure the TRAKKER Antares terminals.

Specifications

Physical Specifications

Length: 39.2 cm (15.25 in.)

Height: 17.7 cm (6.97 in.)

Width: 48.3 cm (19.0 in.)

Weight: 12.35 kg (27.2 lb)

Electrical Specifications

100-120 VAC

200-240 VAC

47-63 Hz

250 Watts maximum

North American or International power via autoswitching

Environment Specifications

Operating: 10° to 50°C (50° to 122°F

Storage: -20° to +60°C (-4° to +140°F)

Humidity: 0 to 85% (non-condensing)

Other Specifications

Network Independent™

Radio Independent™

Application Independent™

Central Network Management

Automatic Restoration

Software Distribution

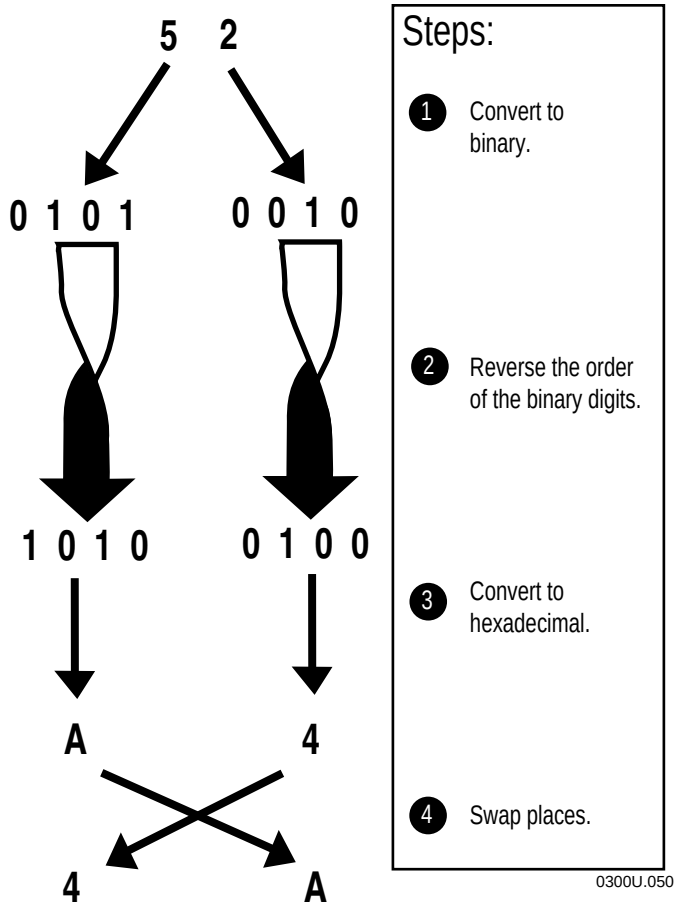
Accessories

Regulatory Approvals

CE Marked, UL Listed, CSA, TÜV-GS, NOM, C-Tic

Converting Ethernet Addresses to Token Ring MAC Format

When configuring the AS/400 host on the DCS 300, the LAN adapter address you specify depends on whether the controller and the host are on the same type of network. If the controller and AS/400 are on different types of networks, you must "byte-flip" the adapter card address.



As a shortcut, you can use this table to byte-flip addresses. The table shows what each hexadecimal digit, from 0 to F, becomes when you perform Steps 1 to 3 (from the previous figure). Then you must perform Step 4.

Byte Flipped Hexadecimal Equivalents

0	converts to	0
1	converts to	8
2	converts to	4
3	converts to	C
4	converts to	2
5	converts to	A
6	converts to	6
7	converts to	E
8	converts to	1
9	converts to	9
A	converts to	5
B	converts to	D
C	converts to	3
D	converts to	B
E	converts to	7
F	converts to	F

Using the DCS 300 to Verify Your Network Connections

You can use the DCS 300 to verify it is correctly connected to the downline devices and to your host. You need to start data collection before you can use the server to send or receive transactions.

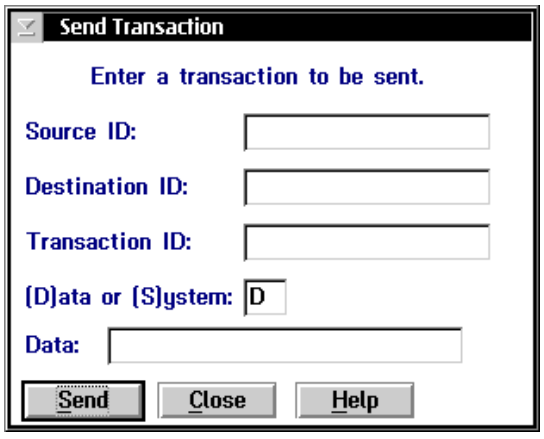
Sending Transactions

Once you configure the DCS 300, you may want to verify that you have a connection between the server and a device or you may want to verify you have a connection between the server and the host application. Use the Send Transaction feature to send a transaction from a source to a destination.

When sending a transaction to a device or an application (destination), make sure that your device or application is ready to accept the transaction. If it is not ready, the transaction is written to a Hot Standby file and you will need to clear the Hot Standby file before sending another transaction to the device or application. For help, see "Viewing and Clearing the Hot Standby Files" in Appendix A.

To verify your connection

1. Make sure that you have saved and activated your run-time configuration.
2. Make sure that you have started data collection.
3. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
4. Select Send Transaction and then choose Start. The Send Transaction dialog box appears.



Field	Description	Value	Default
Source ID (Optional)	This field can contain the name that you want to use as the source of the transaction.	1 to 16 alphanumeric characters	None
Destination ID (Optional)	This field can contain the name of the device that you want to use as the destination of the transaction.	1 to 16 alphanumeric characters	None
Transaction ID (Optional)	This field can contain the transaction ID of the transaction that you want to send to all devices that accept it.	1 to 20 alphanumeric characters	None
Data or System	This field identifies the transaction to be a data or a system transaction.	D, S	D
Data (Optional)	This field contains any data that you want to send with the transaction ID.	1 to 1024 alpha-numeric and special characters	None

Receiving Transactions

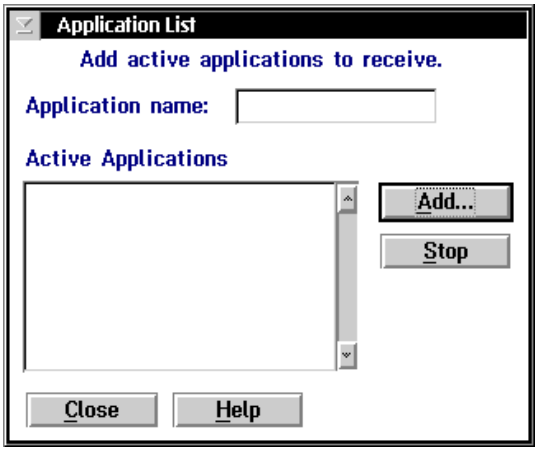
Once you have configured the DCS 300, you may want to test your configuration by sending transactions from a device to an application without starting the application on the host. Or, you may want to send transactions to a device.

The receive transactions feature can troubleshoot your connection to a destination. It lets the server emulate the destination, application, or device, without the destination being active. It also displays a list of transactions that the devices or applications sent to the destination.

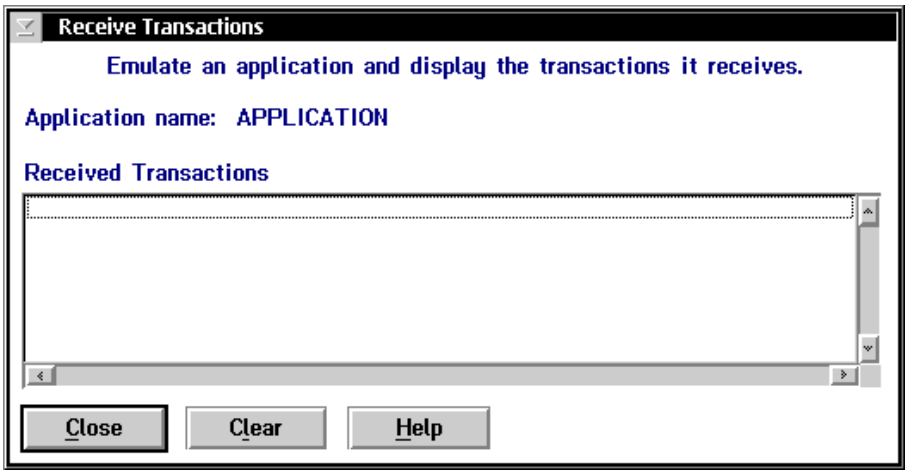
Note: *Any transactions routed to the destination are intercepted by the server emulator and then they are displayed in the Receive Transactions dialog box. If you want the destination to receive the transaction, close the Application List dialog box and send the transaction again.*

To start the emulator to receive transactions

1. From the main menu sidebar buttons, choose Start Data Collection. The Start Data Collection message box appears.
2. Choose Start.
3. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
4. In the System Maintenance list box, select Receive Transactions and then choose Start. The Application List dialog box appears.



5. In the Application name field, enter the name of a destination. The destination name (application or device) must be defined in the server.
6. Choose Add. The Receive Transactions dialog box appears and the server begins emulating and monitoring incoming transactions for the destination.



7. Send a transaction from the application or device. The transaction appears in the Received Transactions box.
8. Choose Clear to delete all the received transactions in the Received Transactions box.

Using the DCS 300 to Transfer Files

You can use the DCS 300 to send binary files, such as the reader program, to JANUS devices and TRAKKER Antares terminals. You can also send ASCII files, such as IRL files, templates, and validation files, to one or more devices in any network.

Note: *Currently, you cannot transfer files to WTP devices.*

Device	File Type	Transfer Method
JANUS 900 MHz RF device (v3.01 or later)	Binary	Binary file transfer (BFT)
JANUS 2.4 GHz RF device (v4.1 or later)	Binary	File transfer protocol (FTP)
TRAKKER Antares terminal	Binary	Terminal file transfer protocol (TFTP)
All devices	ASCII	ASCII

Note: *To transfer files using BFT, your JANUS devices must have FTA.EXE and FTA.INI loaded on the C drive and they must be running a BFT-ready PSK application. You can copy FTA.EXE and FTA.INI from Application companion disk 3.*

To transfer files, you need to perform these tasks:

1. Make sure all the devices are ready to receive the files and data. If the device is not ready, the transaction is written to a Hot Standby file.
2. Make sure the server contains the files and data you want to download. You can put files onto the server using the Restore User Files feature. For help, see "Restoring Your User Files" in Chapter 2.
3. Use the download server to create logical groups so that you can send the files and data to more than one device. For help, see "Adding a Group in the Download Server" later in this appendix.
4. Start data collection.
5. Using the download server feature or download server commands, download the files and data to the terminal or group. For help, see "Using the Download Server to Transfer Files" or "Using the Download Server Commands to Transfer Files" later in this appendix.

Limitations When Downloading IRL Programs

Problem When you download an IRL program from the DCS 300, the mnemonic representation of ASCII control characters (0-31) is converted into actual characters. Usually, you use these characters to create bar code printer labels or to create data that is based on the IRL program execution. When the server converts these characters, the device misinterprets the IRL program and compilation fails.

Solution Create the mnemonic representation of ASCII control characters with an extra leading < character. For example, <NUL> becomes <<NUL>. Then, the server will strip off the leading < character and then pass the correct mnemonic representation to the device.

Problem When you download an IRL program from the DCS 300, the mnemonic representation of five ASCII control characters do not download correctly.

Control Character	Hexadecimal Number
<LF>	0A
<CR>	0D
<SO>	0E
<DC2>	12
<SYN>	16

These characters have special meanings to the IRL interpreter on the device. The device translates the control character into its equivalent hexadecimal (hex) character and then uses the meaning of the hex character when it compiles the program. An error usually occurs.

Solution You can avoid this problem by

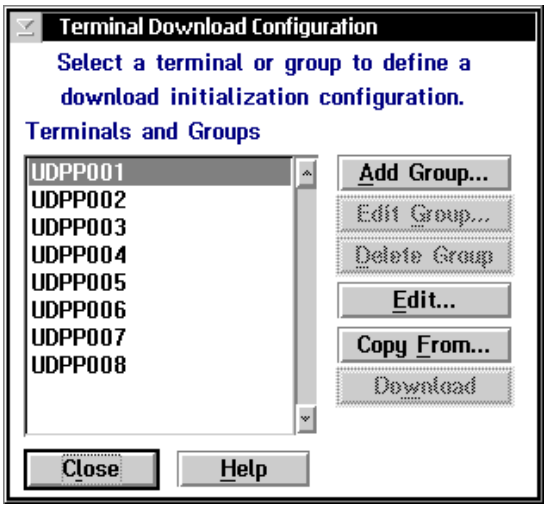
- using PC-IRL to download the IRL program. For help, see the *PC-IRL Reference Manual* (Part No. 049212).
- using the hex number for the control character. The device translates the hex number after it has parsed all the special characters. Use the previous table to translate the control character to its hex number.

Adding a Group in the Download Server

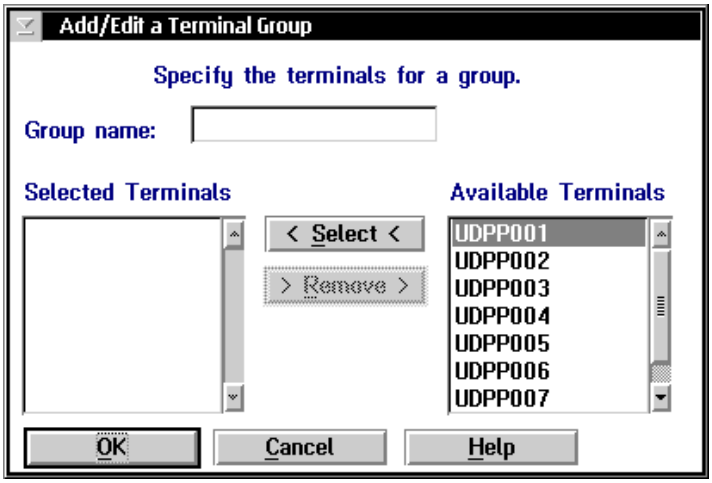
If you want to send files and data to more than one device at the same time, create a group in the download server. You can also edit or delete a group.

To add a group

1. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
2. In the System Maintenance list box, select Configure Download Server and then choose Start. The Terminal Download Configuration dialog box appears.



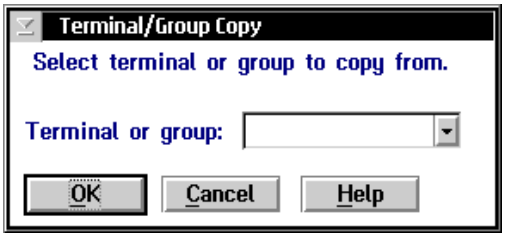
3. Choose Add Group. The Add/Edit a Terminal Group dialog box appears.



4. In the Group name field, enter a meaningful name for the group of terminals.
5. Add the terminals that you want in this group to the Selected Terminals list box.
   a. From the Available Terminals list box, select a terminal to add.
   b. Choose Select. The terminal appears in the Selected Terminals list box.
6. Remove the terminals that you do not want in this group.
   a. From the Selected Terminals list box, select a terminal to remove.
   b. Choose Remove. The terminal is removed from the Selected Terminals list box.
7. Choose OK to save your changes and return to the Terminal Download Configuration dialog box.

Copying Information Between Terminals or Groups

1. From the Terminal Download Configuration dialog box, select the terminal or group that you want to configure.
2. Choose Copy. The Terminal/Group Copy dialog box appears.

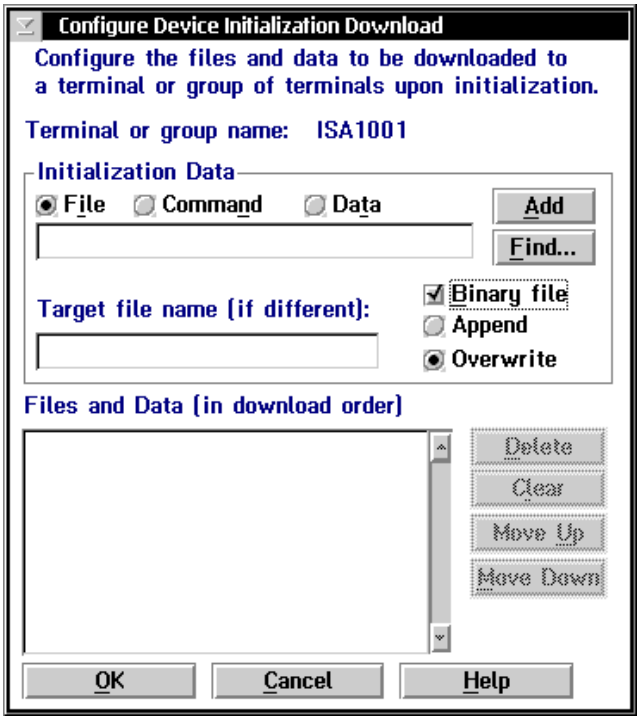


3. In the Terminal or group field, click the down arrow on the right side of the field. A list of terminals or groups that you have configured appears. Select a terminal or group whose configuration you want to copy.
4. Choose OK to copy the configuration, save your changes, and return to the Terminal Download Configuration dialog box.

Using the Download Server to Transfer Files

Note: *The 9154 controller does not support binary file transfer.*

1. From the Terminal Download Configuration dialog box in the Terminals and Groups list box, select a terminal or group to receive files or data.
2. Choose Edit. The Configure Device Initialization Download dialog box appears.



3. In the Initialization Data box, choose the type of initialization data to download.

   Binary file To send a binary file to a device, choose File. Enter the path and filename of the file on the server and choose Binary file. If the file already exists on one of the devices, decide if you want to Append the new file to the existing file, if you want to Overwrite the existing file, or if you want to do nothing but generate an error message.

   Note*: Do not choose Append if you are downloading an .EXE file or any other true binary file.*

   ASCII file To send an ASCII file, choose File.

   Data To send data, choose Data.

4. Enter the file name or data in the field in the Initialization Data box.
5. Choose Add. The file name or data appears in the Files and Data list box.
6. Repeat Steps 3 through 5 until you have entered all the files and data you want to download for this terminal or group. Files and data are downloaded in the order they appear in the Files and Data list box.
   - Choose Move Up or Move Down to change the order of the files and data.
   - Select a file name or data and choose Delete to delete a file name or data.
   - To start over, clear the entire Files and Data list box by choosing Clear.
7. Choose OK to save your changes and return to the Terminal Download Configuration dialog box.
8. Choose Download. The files and data configured for the terminal or group are downloaded to the terminal or group.

Using Download Server Commands to Transfer Files

This section explains some special commands that you can run on devices or use with the Send Transaction feature on the DCS 300. Using these download server commands, you can send files to devices or groups that are configured in the download server.

To send the commands from a device, you need to include these commands in an application that runs on the device.

To send these commands using the Send Transaction feature, you need to enter the commands as data. Then, open the Send Transactions dialog box and send the download server command from the server to a device or a group, or emulate a request by a device for a file.

To create the download server command

1. Configure the download server for the files and data that each device or group will receive. For help, see "Using the Download Server to Transfer Files" in the previous section. Do not choose the Download button.
2. Create your download server command.

   This table lists examples of commands you can use and the results of using the commands. This table assumes that all requests come from a device that has the address pA.

Command	Result
DEV=pA	The server sends all the files and data defined for device address pA to pA.
G=*group*	The server sends all the files and data defined for the group to all the devices in the group.
F=*filename*	The server sends the filename to pA. You can also specify the directory for the file.
D=*data*	The server sends the data specified in the command line to pA.
E=*errormessage*	The server sends the specified error message to pA if there is a problem with the request.

   You can use one line to send multiple download server commands by stringing the commands together with a comma and no spaces. For example, to send a validation file, WORKORDR.TXT to device addresses pA and pB and run the program, use this command:

```
$NGDNLD,DEV=pA,DEV=pB,F=WORKORDR.TXT,D=//
```

To send the download server command

1. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
2. In the System Maintenance list box, select Send Transaction and then choose Start. The Send Transaction dialog box appears.
3. If you want to emulate a request from a device, in the Source ID field enter the logical name of the device that you want to use as the source of the transaction.
4. In the Transaction ID field, enter $NGDNLD.
5. In the Data or System field, enter D.
6. In the Data field, enter the download server command.

   Note: *If you do not enter any data in the Data field, the server will send the source all the files and data that are configured for the source.*

7. Choose Send to send the transaction to the server. The server performs the download server command.

Using the DCS 300 to Configure TRAKKER Antares Terminals

You can use the DCS 300 to configure one or more TRAKKER Antares terminals by sending configuration commands using the download server.

Note: *You cannot retrieve configuration data from a terminal.*

For example, you may want to set the Beep Volume to very loud and turn on Keypad Caps Lock for all the terminals in one area. For a complete list of the configuration commands, see your TRAKKER Antares terminal user's manual.

To send configuration commands to a terminal, you need to perform these tasks:

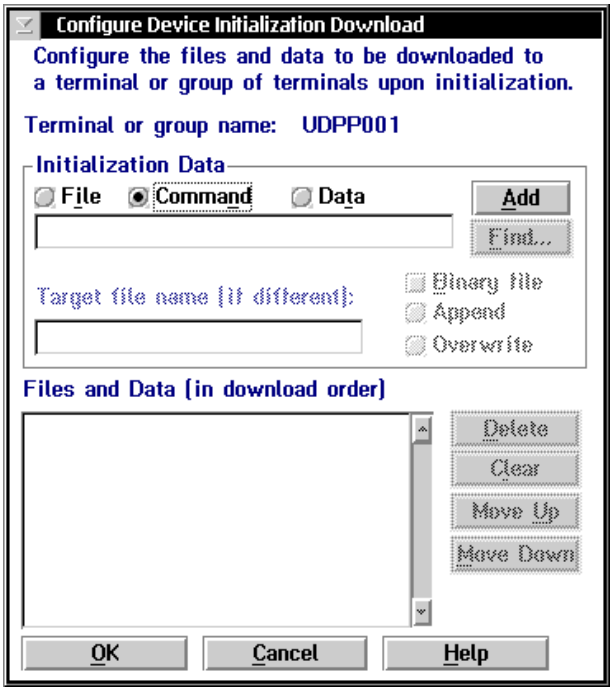
1. Make sure all of the terminals are ready to receive the commands. If a terminal is not ready, the transaction is written to a Hot Standby file.
2. Use the download server to create any logical groups. For help, see "Adding a Group in the Download Server" earlier in this appendix.
3. Start data collection.
4. Use the download server to download the configuration command to the terminal or group. For help, see "Using the Download Server to Transfer Files"earlier in this appendix.

Note: *You can continue running an application on the TRAKKER Antares terminal while configuring the terminal from the server.*

To use the download server to configure a terminal

1. From the Terminal Download Configuration dialog box in the Terminals and Groups list box, select a terminal or group to receive files or data.
2. Choose Edit. The Configure Device Initialization Download dialog box appears.

Configure Device Initialization Download Dialog Box



3. In the Initialization Data box, choose Command.
4. Enter the configuration command and choose Add. The command appears in the Files and Data box.

   For example, to set the Beep Volume to very loud, type: $+BV4
5. Repeat Steps 3 and 4 until you have entered all the commands you want to download for this terminal or group. Commands are downloaded in the order they appear in the Files and Data list box. You can then
   - choose Move Up or Move Down to change the order.
   - select a command and choose Delete to delete a command.
   - start over by clearing the entire list box by choosing Clear.
6. Choose OK to save your changes and return to the Terminal Download Configuration dialog box.
7. Choose Download. The server downloads the commands to the terminal or group.

When you remotely configure the terminal, the commands change the terminal's run-time configuration. The configuration changes are not saved in flash memory. You must send `.+1` as the last command or use the TRAKKER Antares 2400 Menu System to save the configuration in flash memory. For help, see your TRAKKER Antares terminal user's manual.

C

Using Remote Console

This appendix explains how to use the remote console option on your DCS 300. For help upgrading the DCS 300 to remote console, see "Upgrading to Remote Console" in Appendix D.

About Remote Console

The remote console option lets you access the server remotely using a LAN, a WAN, or a dial-up modem. Using third-party remote control software, NetOp from Danware Data A/S, you can

- access the DCS 300 GUI from a remote PC using the remote PC's mouse and keyboard.
- transfer files between a remote PC and the server.
- redirect printing from the DCS 300 to a printer that is connected to the remote PC (OS/2 guest software only).

NetOp is a family of remote control products that support multiple operating systems and various communication interfaces. The software consists of two components: the host and the guest. The host is a server program that is running on the DCS 300. The guest is a client program that you run on a remote PC. You must purchase one of these Intermec versions of the NetOp v5.3 PC Remote Control guest software:

- PC Remote Control software for Windows™ 95 and NT (Part No. 590480)
- PC Remote Control software for OS/2 (Part No. 590478)

Note: *The guest software contains special software that works with the DCS 300. You cannot purchase commercially-available NetOp PC Remote Control software.*

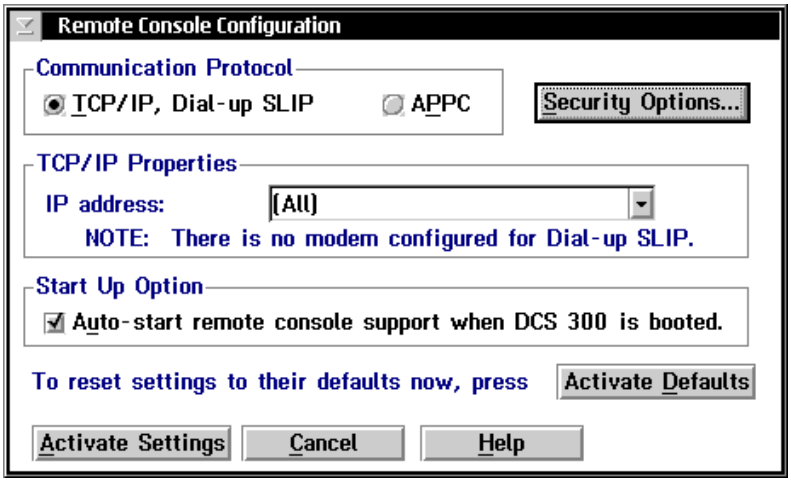
Configuring the NetOp Host (DCS 300)

The DCS 300 communication protocol settings must match the guest communication protocol settings; that is, they must match the communication settings on the remote PC. Use the Remote Console Configuration dialog box to configure the server. If you want to return to the default settings, choose Activate Defaults. When you choose Activate Settings, you can use the new configuration immediately.

If you are using dial-up SLIP, you must connect a modem to the DCS 300. For help, see "Connecting a Modem" in Chapter 2.

To configure the NetOp host for TCP/IP or dial-up SLIP

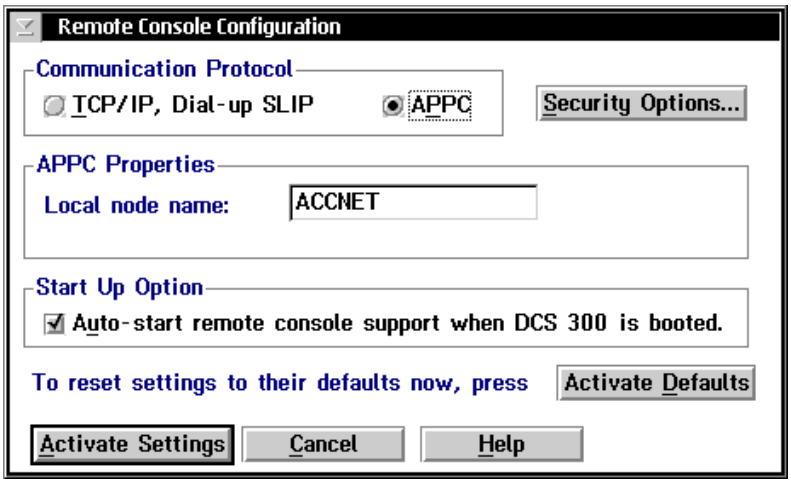
1. From the main menu, choose System Maintenance. The System Maintenance dialog box appears.
2. In the System Maintenance list box, select Remote Console Support and then choose Start. The Remote Console Configuration dialog box appears.



Field	Description	Value	Default
Communication Protocol	This box lets you specify which communication protocol you are using for remote connections.	TCP/IP and Dial-up SLIP, APPC	TCP/IP and Dial-up SLIP
TCP/IP Properties	The IP address field lets you choose which IP address you use to accept the connection. If you are using dial-up SLIP, choose 222.222.222.10. To accept connections for all available IP addresses, choose All.	xxx.xxx.xxx.xxx where xxx is a value between 0 and 255	First TCP/IP network adapter card
Start Up Option	This check box determines if the DCS 300 starts the NetOp host software when it is booted.	Check, Clear	Check

To configure the NetOp host for APPC

1. From the main menu, choose System Maintenance. The System Maintenance dialog box appears.
2. In the System Maintenance list box, select Remote Console Support and then choose Start. The Remote Console Configuration dialog box appears.



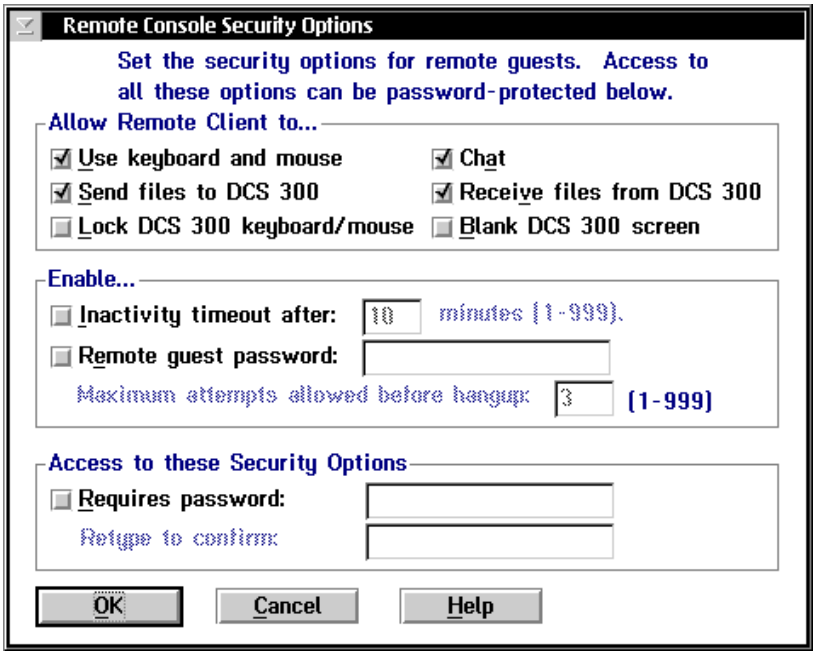
Field	Description	Value	Default
Communication Protocol	This box lets you specify which communication protocol you are using for remote connections.	TCP/IP and Dial-up SLIP, APPC	TCP/IP and Dial-up SLIP
APPC Properties	The Local node name field specifies the SNA local node name.	1 to 8 alphanumeric and special characters	ACCNET
Start Up Option	This check box determines if the DCS 300 starts the NetOp host software when it is booted.	Check, Clear	Check

Configuring Security

The NetOp host software includes security features to prevent unauthorized access to the DCS 300. You can also use the security options to limit the actions that the remote PC can perform.

To configure security

- In the Remote Console Configuration dialog box, choose Security Options. The Remote Console Security Options dialog box appears.



Field	Description	Value	Default
Use keyboard and mouse	This check box determines if the remote PC user can control the DCS 300 keyboard and mouse. If this check box is clear, the remote PC user can only look at the screen on the DCS 300.	Check, Clear	Check
Chat	This check box determines if the remote PC user can start a chat with the DCS 300 user.	Check, Clear	Check
Send files to DCS 300	This check box determines if the remote PC user can transfer files from the remote PC to the DCS 300.	Check, Clear	Check

Field	Description	Value	Default
Receive files from DCS 300	This check box determines if the remote PC user can transfer files from the DCS 300 to the remote PC.	Check, Clear	Check
Lock DCS 300 keyboard and mouse	This check box determines if the remote PC user can lock the DCS 300 keyboard and mouse during a session.	Check, Clear	Clear
Blank DCS 300 screen	This check box determines if the remote PC user can blank the DCS 300 screen during a session.	Check, Clear	Clear
Inactivity timeout after…	This check box determines if the server ends the NetOp connection if there is no activity between the remote PC and the server. ***Note:*** *Screen update is considered an activity.*	Check, Clear	Clear
…minutes	This field specifies how long the server waits before it ends the NetOp connection if there is no activity between the remote PC and the server.	1 to 999	10
Remote guest password	This check box determines if the remote PC user needs to enter a password after a NetOp connection is made.	Check, Clear	Clear
…password	This field contains the password the remote PC user must enter after a NetOp connection is made.	1 to 16 printable characters, except a semicolon (;)	None
Maximum attempts allowed before hangup	This field specifies the number of times the remote PC user can enter an incorrect password before the server ends the connection.	1 to 999	3
Requires password	This check box determines if you must enter a password to access this dialog box.	Check, Clear	Clear
…password	This field contains the password that you must enter to access this dialog box.	1 to 16 printable characters, except a semicolon (;)	None
Retype to confirm	You must retype the password that you entered in the Requires password field.	1 to 16 printable characters, except a semicolon (;)	None

Configuring the NetOp Guest (Remote PC)

For help installing the NetOp guest software, see the NetOp user's guide that shipped with your guest software.

Note: *The guest communication settings must match the host communication settings; that is, they must match the communication settings on the DCS 300.*

Using NetOp Guest for Windows

After you install the NetOp guest software on your remote PC, follow these tips to ensure that a connection is made.

Tips for using TCP/IP

1. Choose the Call a Host PC toolbar button. The Call Host dialog box appears.
2. In the Name field, enter the IP address of the DCS 300.
3. Choose Call.

Tips for using dial-up SLIP in Windows 95

1. In the Control Panel, use the Add/Remove program to install Dial-up Networking, if it is not already installed.
2. Select the Windows Setup tab to install SLIP support. Click the Have Disk button. The files are in the ADMIN\APPTOOLS\DSCRIPT directory on your Win95 CD.
3. Create a phonebook entry.
    a. In My Computer folder, double-click the Dial-Up Networking icon.
    b. In the Dial-up Networking folder, double-click the Make a New Connection icon to create a new Dial-up Networking connection.
    c. Enter a name for the connection and click Next.
    d. Enter the phone number you want to dial and click Next.
    e. Click Finish to create the connection. An icon with the name of the new connection will be created in the Dial-up Networking folder.
    f. Right click on the connection icon just created and select Properties.
    g. In the General tab, press the Server Type button.
    h. Select SLIP as the Type of Dial-up Server and uncheck the Log on to network check box.

4. In the TCP/IP Settings dialog box, type 222.222.222.20 as the IP address. Make sure the Use IP header compression check box is unchecked.
5. Make sure that the modem that is connected to the DCS 300 is configured.
6. After the modem connection is made, start the NetOp guest software.
7. Call the TCP/IP host using the name 222.222.222.10.

Tips for using dial-up SLIP in Windows NT

1. Install RAS (Remote Access Service) so that you can have dial-up networking support.
2. Create a phonebook entry.
   a. In My Computer folder, double-click the Dial-Up Networking icon.
   b. In the Dial-up Networking dialog box, click the New button to create a new phonebook entry.
   c. In the Basic tab, enter an entry name and the phone number you want to dial.
   d. In the Server tab, select SLIP as the Dial-up server type and press the TCP/IP Settings button.
   e. In the SLIP TCP/IP Settings dialog, you must specify "222.222.222.20" as the IP address.

   Note: *You should also uncheck the IP header compression option.*
3. Make sure that the modem that is connected to the DCS 300 is configured.
4. After the modem connection is made, start the NetOp guest software.
5. Call the TCP/IP host using the name 222.222.222.10.

Using NetOp Guest for OS/2

After you install the NetOp guest software on your remote PC, follow these tips to ensure that a connection is made.

Tips for using TCP/IP

1. From the Host menu, choose Add Host. The NetOp Guest - Add Host dialog box appears.
2. In the Host ID field, enter the IP address of the DCS 300.
3. Click Settings. The NetOp Guest - Edit Host dialog box appears.
4. In the Protocol list, select TCP/IP.
5. Close all dialog boxes and then choose the Call toolbar button.

Tips for using dial-up SLIP

1. Use the Network Dialer tool to make a SLIP connection to the DCS 300.
2. In the Login Info tab, choose SLIP as the connection type.
3. In the Connect Info tab, type 222.222.222.20 as the destination IP address.
4. Make sure that the modem that is connected to the DCS 300 is configured.
5. After the modem connection is made, start the NetOp guest software.
6. Call the TCP/IP host using the name, 222.222.222.10.

Tips for using APPC

1. Use Communication Manager Setup to create a configuration file that defines the partner LU, such as the DCS 300, that you want to control.
2. Start Communication Manager before you start the NetOp guest software. Communication Manager will use the configuration file that you defined in Step 1 as the default file.

D

Upgrading the DCS 300 and Devices

This appendix provides you with instructions on how to upgrade the DCS 300 and its licenses. It also explains how to use the server to upgrade the TRAKKER Antares terminals.

Upgrading the DCS 300 Software

Your DCS 300 upgrade CD contains one of these kinds of upgrades:

Background A background upgrade will not reboot the server. You can keep data collection running while you are upgrading the server. You can run a background upgrade from the hard drive.

Minor A minor upgrade will reboot the server. You must stop data collection before you can upgrade the server. You will not have to restore your system files or your run-time configuration. You can run a minor upgrade from the hard drive.

Major A major upgrade may change the hard drive partitions or it may update the operating system. This upgrade can only be done from the CD.

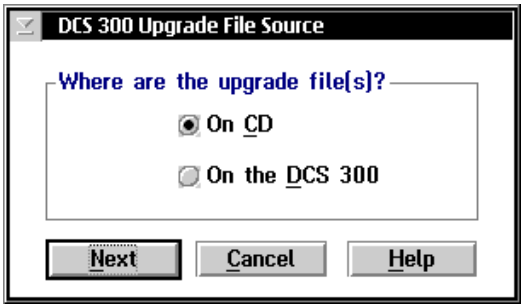
For background and minor upgrades, you can copy the files from the CD to the directory D:\UPGRADE.

To upgrade the DCS 300 software

1. Back up the system files, run-time configuration, and user files. For help, see "Backup Up the DCS 300 Configuration" in Chapter 2.

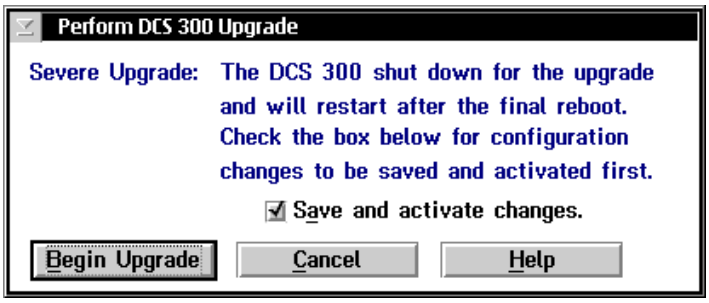
   Note: *When you finish performaing a major upgrade, the server automatically restores your system files, run-time configuration, and user files. However, if you decide to downgrade the server, you will need these backup disks to restore your configuration.*

2. From the main menu, choose System Maintenance. The System Maintenance dialog box appears.
3. In the System Maintenance list box, select DCS 300 Upgrade Utility and then choose Start. The DCS 300 Upgrade File Source dialog box appears.



4. Choose the location of the upgrade files. Major upgrades must be run from the CD.
5. If you are running the upgrade from the CD, insert the CD into the CD-ROM drive.
6. Choose Next. A message appears informing you that the server is comparing the upgrade files with the current installation. The DCS 300 Upgrade File Check dialog box lets you know if you can continue with the upgrade.

   If you cannot continue with the upgrade, correct the problem and start this procedure again.
7. Choose Next. The Perform DCS 300 Upgrade dialog box appears.



8. Choose Begin Upgrade. Background and minor upgrades may take from 30 seconds to two minutes. A major upgrade can take up to 30 minutes.

Upgrading Your Licenses

When you purchased your DCS 300, you selected a license that lets you run a specific number of devices in your network. If you need to run more devices than what is allowed by your license, you can purchase a new license that will let the server control as many as 254 devices. You can also purchase a license that lets you run screen mapping and remote console, if your original license did not include it. These sections provide more information about terminal, screen mapping, and remote console license.

Upgrading Your Terminal License

You purchase different terminal licenses depending on the number of terminals that you want to simultaneously communicate with the server.

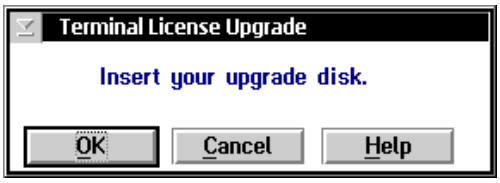
Level	Network Size (Number of Terminals)	Intermec Part No.
2	1-24	067543
3	1-64	067544
4	1-254	067545

You cannot skip a level when you are upgrading your terminal license. That is, if you want to go from a Level 1 to a Level 4, you must also purchase Levels 2 and 3 and upgrade your server to Levels 2 and 3.

The server maintains an internal count of the number of devices that connect to it. Every time a new device is sent data, the server increments its count. If the count reaches the maximum network size, the server will not accept data from, nor send transactions to, any new device. The transaction is not saved and an error message appears. Each time data collection is started on the server, the internal count is reset.

To install the license

1. From the main menu, choose System Maintenance. The System Maintenance dialog box appears.
2. In the System Maintenance list box, select Terminal License Upgrade and then choose Start. The Terminal License Upgrade message box appears.



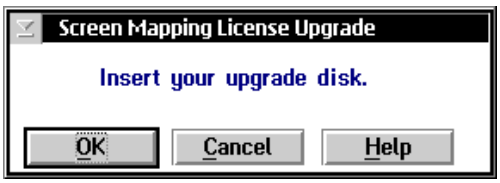
3. Insert the upgrade disk.
4. Choose OK to upgrade your terminal license. When the upgrade is complete, you return to the System Maintenance dialog box.

Upgrading to Screen Mapping

You can purchase screen mapping with remote console (Intermec Part No. 067190) or without remote console (Intermec Part No. 066370). Intermec has designed an automated Script Builder Tool that lets you create script files for your JANUS devices, TRAKKER Antares terminals, and the 6400. Remote console lets you manage the server remotely.

To install the license

1. From the main menu, choose System Maintenance. The System Maintenance dialog box appears.
2. In the System Maintenance list box, select Screen Mapping License Upgrade and then choose Start. The Screen Mapping License Upgrade message box appears.



3. Insert the upgrade disk.
4. Choose OK to load screen mapping. When the upgrade is complete, you return to the System Maintenance dialog box.

Upgrading to Remote Console

You can purchase remote console with screen mapping (Intermec Part No. 067190) or without screen mapping (Intermec Part No. 067188). Remote console lets you manage the server remotely. To run remote console, you also need to purchase the Intermec version of Danware's NetOp® PC Remote Control guest software:

- PC remote control software for Windows™ 95 and NT (Intermec Part No. 590480)
- PC remote control software for OS/2 (Intermec Part No. 590478)

Note: *This guest software contains special software that works with the DCS 300. You cannot use Danware's commercially-available software.*

To install the license

1. From the main menu, choose System Maintenance. The System Maintenance dialog box appears.
2. In the System Maintenance list box, select Remote Console License Upgrade and then choose Start. The Remote Console Upgrade message box appears instructing you to insert the upgrade disk.
3. Insert the upgrade disk. A message box appears confirming that you want to upgrade to remote console.
4. Choose Upgrade. When the upgrade is complete, you return to the System Maintenance dialog box.

For help running the remote console feature, see Appendix C, "Using Remote Console."

Using the DCS 300 to Upgrade TRAKKER Antares Terminals

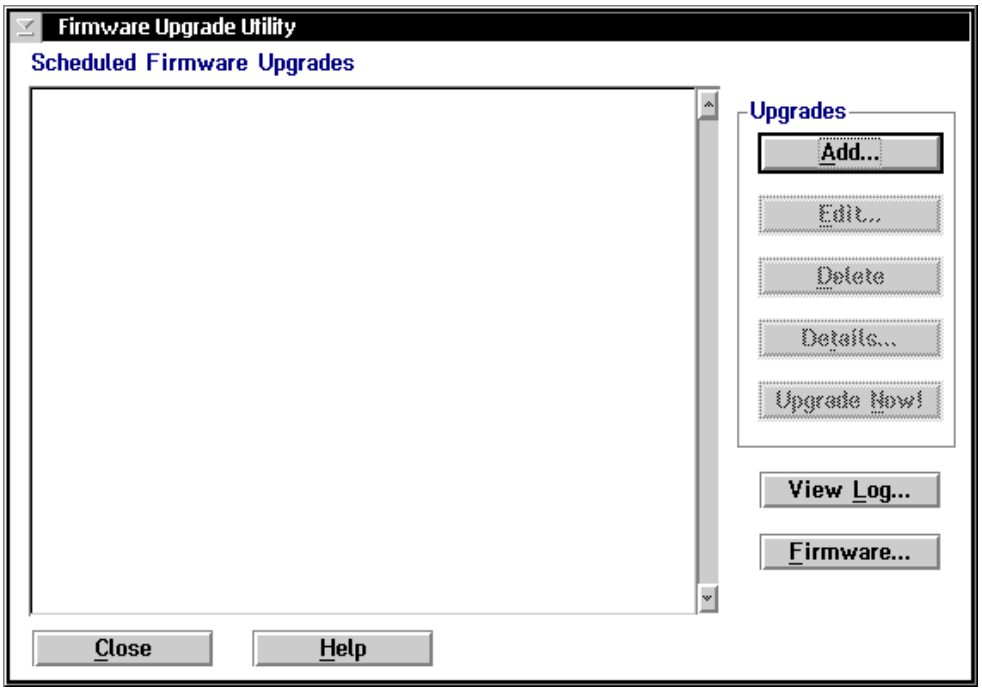
The Firmware Upgrade Utility lets you simultaneously upgrade the firmware on all the TRAKKER Antares terminals that the DCS 300 can communicate with. It detects which firmware each terminal is running and performs the correct upgrade procedure for that version. This utility also lets you install different applications on your terminals.

To upgrade your terminals, you schedule upgrade events. For example, you can upgrade the firmware on one terminal now and then later in the day, when no one is using the terminals, you can put a new application on all the terminals. When the events are done, you verify that the terminals were upgraded by viewing the terminal device status and the upgrade log.

Before you start scheduling upgrade events, you must know if the new firmware or new application is already on the server or if it is on a floppy disk. To see what firmware and applications are on your server, see "Managing System Firmware and Applications" later in this appendix.

To start the Firmware Upgrade Utility

1. From the main menu sidebar buttons, choose System Maintenance. The System Maintenance dialog box appears.
2. From the System Maintenance list, choose Firmware Upgrade Utility and then choose Start. The Firmware Upgrade Utility window appears.



In the Scheduled Firmware Upgrades box, you can view the state of all the scheduled upgrade events.

Column	Description	Example
1	The date on which the upgrade event is scheduled to occur.	1997/06/14
2	The time at which the upgrade event is scheduled to occur. Time is in 24-hour format.	01:44
3	The state of the scheduled upgrade event: **Pending** The utility is waiting until the scheduled date and time before starting the upgrade. **Upgrading** The utility is currently upgrading the devices. **Missed** The utility was unable to perform the upgrade. The event may have been scheduled in the past or data collection was not started on the server at the scheduled time of the upgrade event. **Complete** The utility successfully performed the upgrade. **Errors** The utility was unable to upgrade all the devices because one or more of the devices may have been unavailable at the scheduled time. The utility may have timed out or you may have stopped the upgrade on one of the devices.	Pending
4	The name of the upgrade event.	Upgrade Firmware to v2.0

Now, you need to add, edit, or delete upgrade events. For help adding upgrade events, see "Adding Upgrade Events" in the next section.

To exit the Firmware Upgrade Utility

1. From the Firmware Upgrade Utility window, choose Close. You return to the System Maintenance dialog box.
2. Choose Close. You return to the main menu.

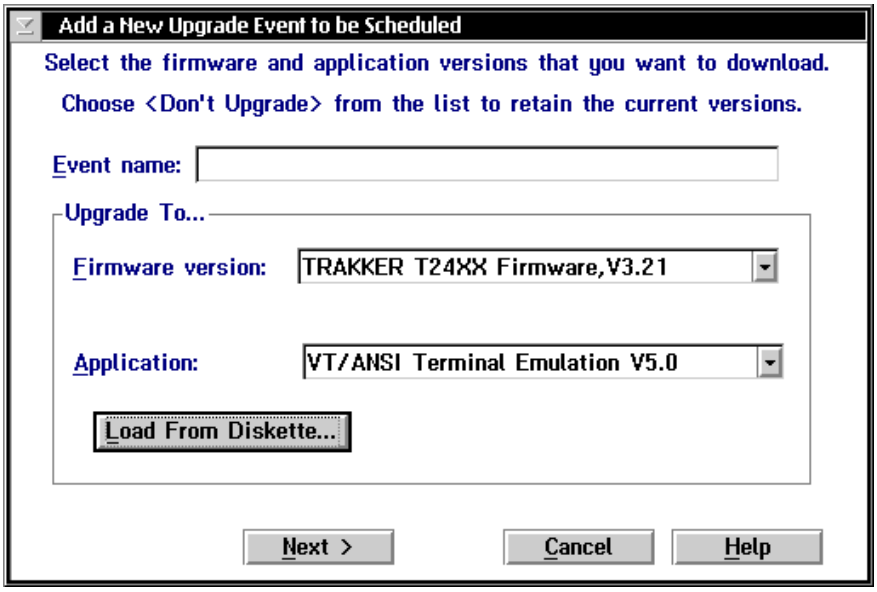
Adding Upgrade Events

The Firmware Upgrade Utility lets you schedule the upgrade events or you can start the upgrade event immediately.

Note: *You need to use three screens to schedule an upgrade event. You can choose Back to go to a previous screen. If you choose Cancel, you return to the main Firmware Upgrade Utility window.*

To add an upgrade event

1. From the Firmware Upgrade Utility window, choose Add. The Add a New Upgrade Event to be Scheduled dialog box appears.
2. In the Event name field, enter a meaningful name for the event you are scheduling. This name can have up to 40 alphanumeric or special characters or spaces.



3. In the Firmware version field, click the down arrow on the right side of the field. A list of firmware versions that you can download appears. Choose one.

   Or, load the firmware from a disk that was supplied to you by your local Intermec representative or a VAR. For help, see "Loading Firmware and Applications From a Disk" later in this appendix.

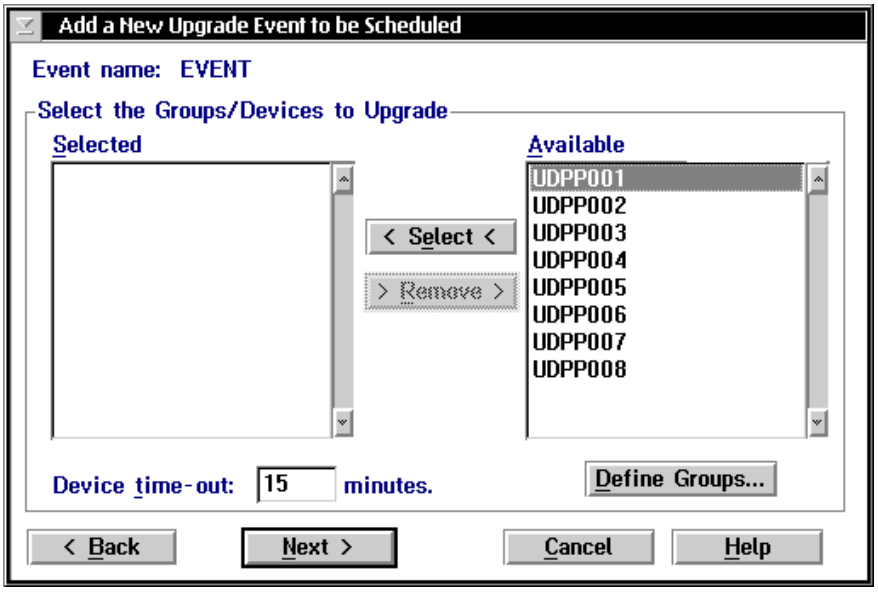
   Or, choose <Don't Upgrade> if you want to keep the current firmware version on your devices.

4. In the Application field, click the down arrow on the right side of the field. A list of applications that you can download appears. Choose one.

   Or, load the application from a disk that was supplied to you by your local Intermec representative or a VAR. For help, see "Loading Firmware and Applications From a Disk" later in this section.

   Or, choose <Don't Upgrade> if you want to keep the current application on your devices.

5. Choose Next.



6. Define logical groups of devices. All group names have a G on the right side of the name. For help, see "Defining a Group" later in this appendix.

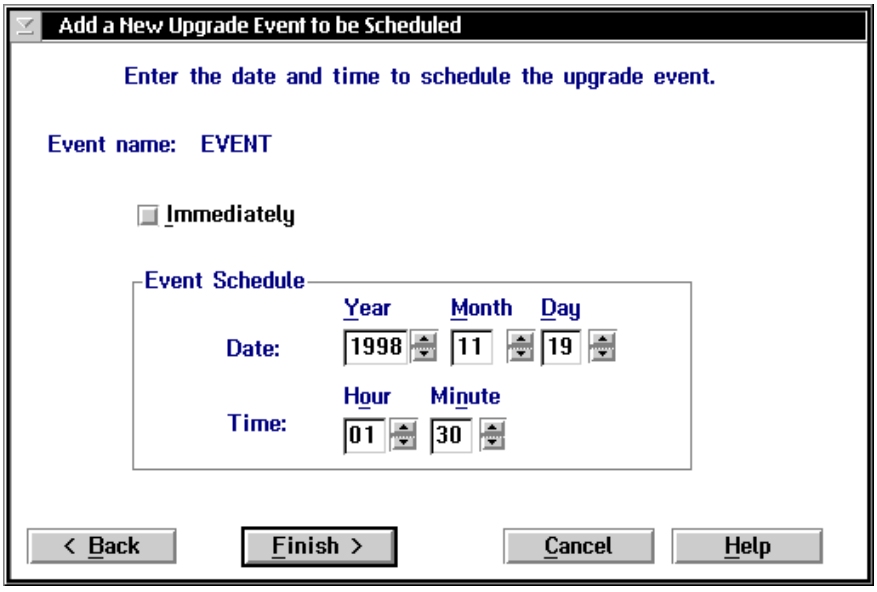
7. Select the groups and devices that you want to upgrade.

   Note: *You can select several sequential devices in the list box by holding down the* ***Shift*** *key and selecting two or more devices. You can select several individual items by holding down the* ***Ctrl*** *key and selecting each item.*

   a. In the Available list box, select the groups and devices that you want to upgrade.

   b. Choose Select.

8. Remove any groups and devices that you do not want to upgrade.
   a. In the Selected list box, select the groups and devices that you do not want to upgrade.
   b. Choose Remove.
9. In the Device time-out field, enter the number of minutes that the utility waits for the upgrade to complete on each device before it times out. If the upgrade on one of the devices does not finish before the time-out, an Error status appears next to the upgrade event name in the Firmware Upgrade utility window.
10. Choose Next.



11. In the Event Schedule box, enter the date and time that you want the upgrade event to take place. Or, use the spin buttons (up and down arrows) in the fields to select the correct Year, Month, Day, Hour, and Minute.

    Or, check the Immediately check box if you want the upgrade event to occur immediately after Step 12.
12. Choose Finish. You return to the Firmware Upgrade Utility window.

You are done scheduling the upgrade event. If you set a date and time for the upgrade event, a Pending status appears in the third column of the Firmware Upgrade Utility window. If you checked the Immediately check box, the utility starts upgrading the devices.

Note: *Before an upgrade event can happen, start data collection on the server.*

Loading Firmware and Applications From a Disk

If you are ready to start scheduling upgrade events and you have received new firmware or an application from Intermec or a VAR, you can load it on your DCS 300. Then you can continue scheduling an upgrade event.

If you are not ready to schedule an upgrade event, but you still want to load the new firmware or application, from the Firmware Upgrade Utility window, choose Firmware. Start at Step 3 in the next procedure.

To load firmware or an application on the server

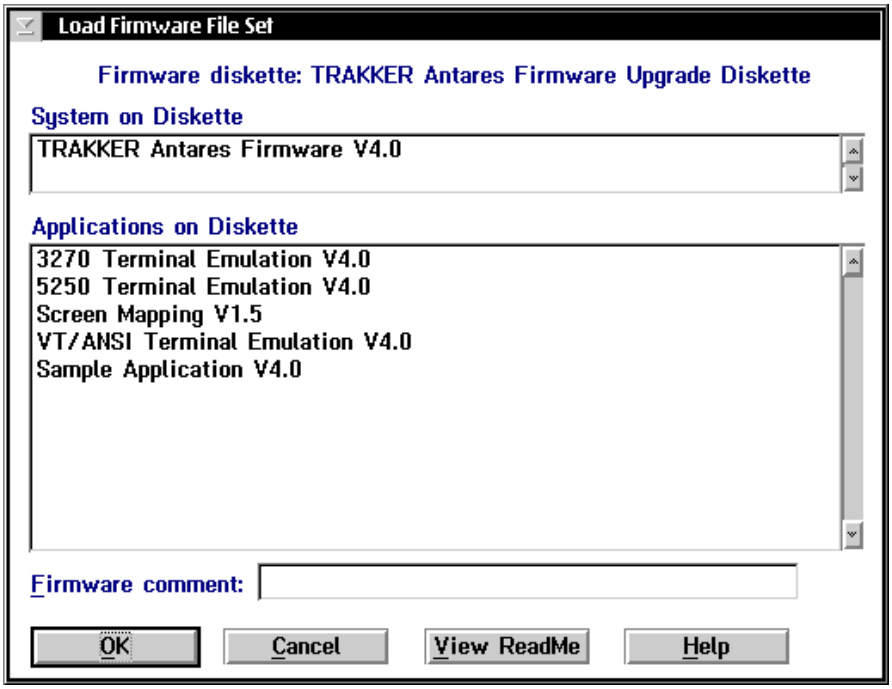
1. From the Firmware Upgrade Utility window, choose Add. The Add a New Upgrade Event to be Scheduled dialog box appears.
2. Choose Load From Diskette. This message box appears.

3. Insert the Firmware Upgrade disk in the disk drive of the server.
4. Choose OK. The Load Firmware File Set dialog box appears.

   In the System on Diskette box, you can see the firmware upgrade that is available on the disk.

   In the Applications on Diskette box, you can see the applications that are available on the disk.

Load Firmware File Set Dialog Box



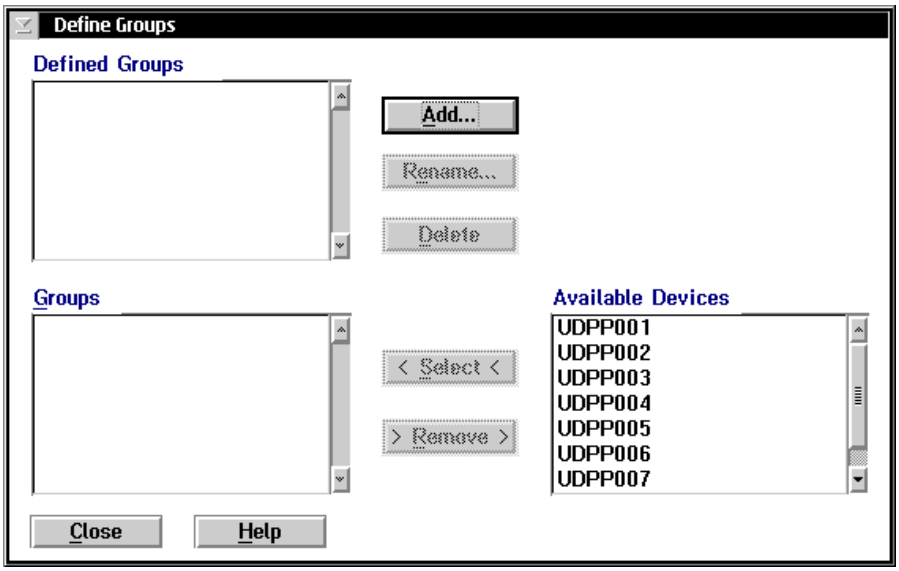
5. In the Firmware comment field, enter any comments you want to be stored with the firmware or application. These comments appear in the Firmware File Set Details message box. You can enter up to 40 alphanumeric characters, special characters, or spaces.
6. Choose View ReadMe if you want to read the README.TXT file on the disk. This file usually contains additional information about the firmware.
7. Choose OK to load the firmware and applications from the disk. When you choose OK, the utility copies the firmware and applications from the disk to the server. Several message boxes appear to show you the status of the loading process.
8. When the utility has copied the files to the server, a message box appears confirming that you have successfully loaded the firmware on the server.
9. Choose OK to return to the Firmware Upgrade Utility window.

Defining a Group

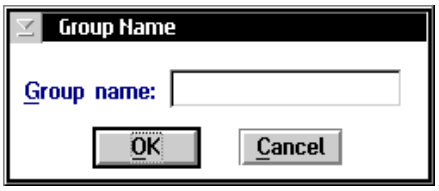
You can define groups so that you can more easily manage upgrading your devices. For example, you may want to upgrade the firmware on the dayshift terminals at night and upgrade the nightshift terminals during the day. You can assign a device to more than one group. The server upgrades all the devices in a group at the same time.

To define a group

1. From the second Add a New Upgrade Event to be Scheduled dialog box, choose Define Groups. The Define Groups dialog box appears.



2. Choose Add. The Group Name dialog box appears.



3. In the Group name field, enter a meaningful group name. This name can have up to 16 alphanumeric characters, special characters, or spaces.

4. Choose OK. You return to the Define Groups dialog box. The new group name appears in the Defined Groups list box and in the Groups list box.
5. Repeat Steps 2 through 4 until you have added all the groups to the Defined Groups list box. You can also rename and delete groups.
6. Add devices to each group. In the Groups list box, a plus (+) on the left side of the group name shows that the group is not expanded to show all the devices that are in it. If a minus (-) is next to the group name, the group has been expanded and all the devices in it are listed below it. You can double-click on a group name to expand or contract the group.

   Note: *You can select several sequential devices in the Available Devices list box by holding down the* ***Shift*** *key and selecting two or more devices. You can select several individual items by holding down the* ***Ctrl*** *key and selecting each item.*

   a. In the Groups list box, select the group that you want to edit.
   b. In the Available Devices list box, select the devices that you want to add to the group.
   c. Choose Select. The devices are added to the group.
7. Remove devices from each group.
   a. In the Groups list box, expand the group that you want to edit.
   b. Select the devices in the group that you want to remove.
   c. Choose Remove. The devices are removed from the group.
8. Choose Close to close the dialog box and return to the second Add a New Upgrade Event to be Scheduled dialog box.

Renaming a Group

1. From the second Add a New Upgrade Event to be Scheduled dialog box, choose Define Groups. The Define Groups dialog box appears.
2. In the Defined Groups list box, select the group that you want to rename.
3. Choose Rename. The Group Name dialog box appears.
4. In the Group name field, enter the new name for the group.
5. Choose OK. The new group name appears in the Defined Groups list box. Note that the name also changes in the Groups list box.

Performing the Upgrade

If you do not want to schedule an upgrade event or if you want to rerun a completed upgrade event, there are two ways you can perform an upgrade event immediately:

Note: *Before an upgrade event can happen, you must start data collection on the server.*

- In the third Add a New Upgrade Event to be Scheduled dialog box, check the Immediately check box. When you choose Finish, the utility starts upgrading the terminals.
- From the Firmware Upgrade Utility window, select an event and then choose Upgrade Now! This message box appears:

Choose Start to start the upgrade event.

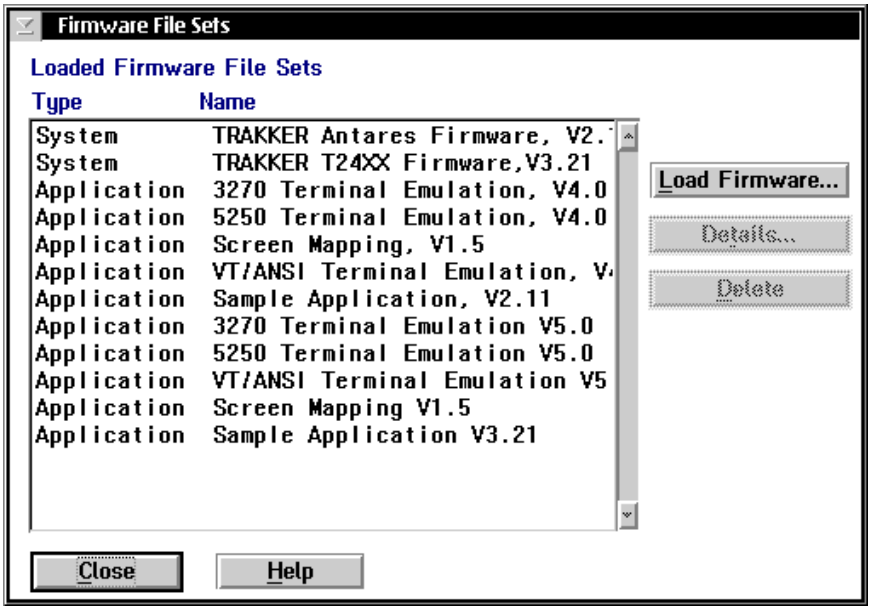
Managing System Firmware and Applications

You can view the firmware and applications that are loaded on your DCS 300. From the Firmware Files Set dialog box, you can also:

- load new firmware or an application from a disk.
- view details of the firmware or application that is loaded on the server.
- delete firmware or applications that are loaded on the server.

To view the firmware and applications

- From the Firmware Upgrade Utility window, choose Firmware. The Firmware File Sets dialog box appears. The Type column identifies the file as a system file (firmware) or an application.

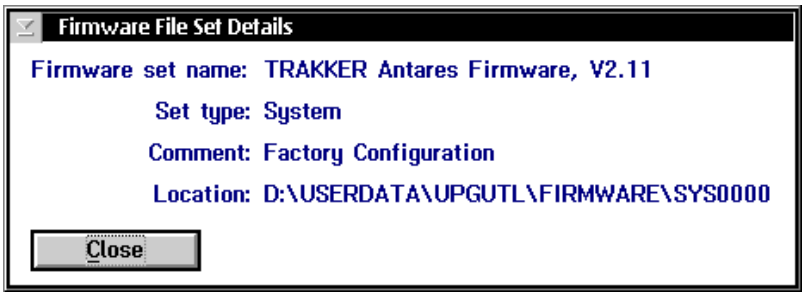


To load firmware or an application from a disk

- From the Firmware File Sets dialog box, choose Load Firmware. For help, see "Loading Firmware and Applications From a Disk" earlier in this appendix. Start at Step 3.

To view details of a firmware file or application

- From the Firmware File Sets dialog box, select a system file (firmware) or an application and then choose Details. This message box appears:



  Choose Close to close the message box and return to the Firmware File Sets message box.

To delete firmware and applications from the server

1. From the Firmware File Sets dialog box, select a system file (firmware) or an application to delete.
2. Choose Delete. A message box appears confirming that you want to delete the system file or application.
3. Choose Delete. The file is removed from the server.

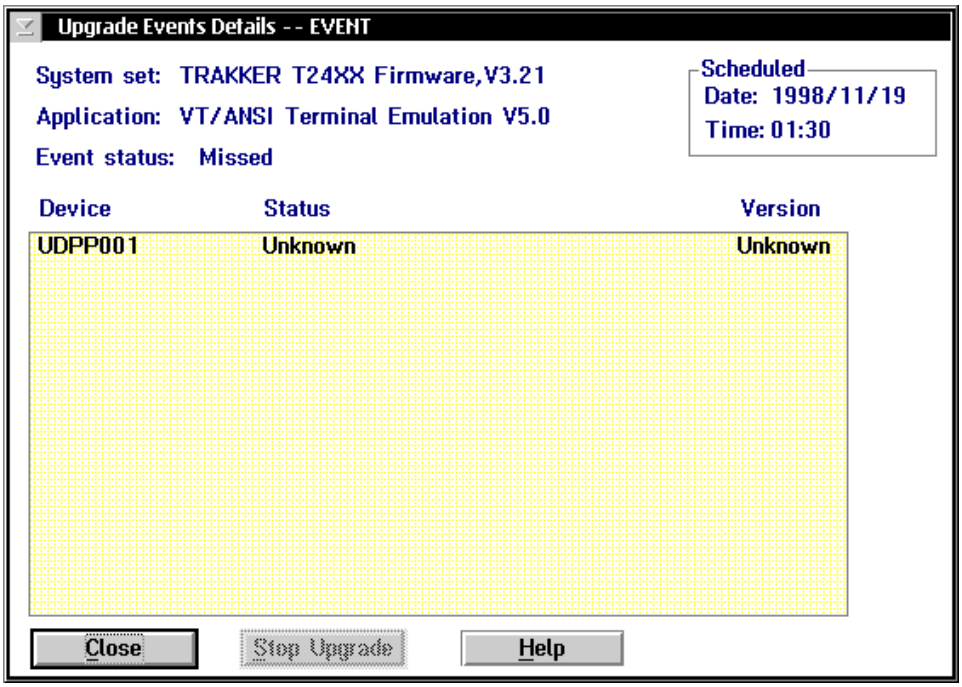
Viewing Upgrade Event Details

The Firmware Upgrade Utility window displays the scheduled upgrade events and their current status. You can view more details of an upgrade event and see the status of each device that is scheduled to be upgraded.

Stop Upgrade button If the status of upgrade on a terminal is Upgrading, you can stop the server thread that is handling/monitoring the upgrade. For example, if your terminal battery is too low, you can stop the upgrade, change the battery, and restart the upgrade of the terminal.

To view details of an upgrade event

1. From the Firmware Upgrade Utility window, select an event to view.
2. Choose Details. The Upgrade Events Details dialog box appears.



This dialog box shows the system file (firmware) and application that the event is using, the status of the event, and the scheduled date and time of the event. You can see all the devices that are scheduled to be upgraded, the status of the upgrade of a specific device, and which firmware version is currently on the device.

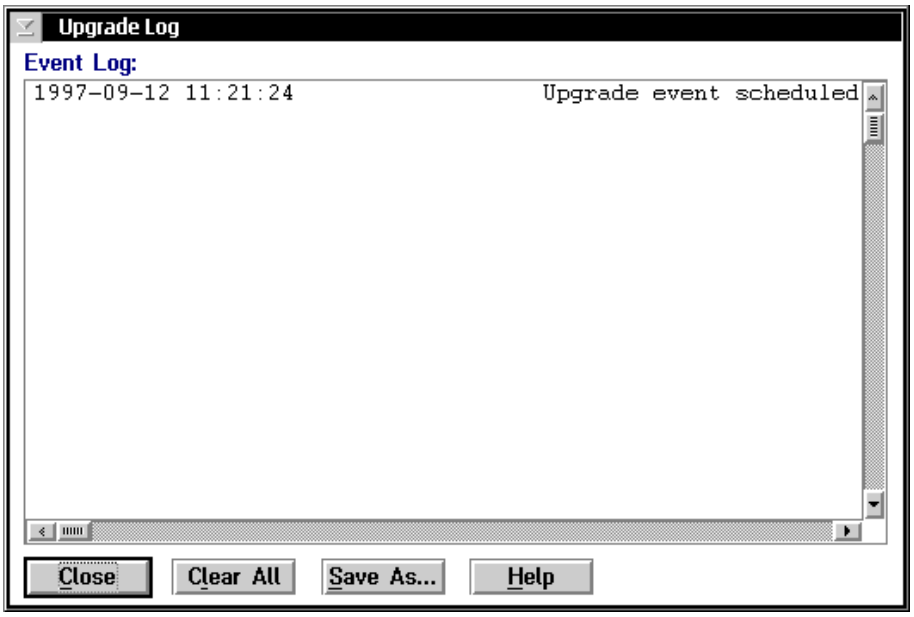
3. If necessary, you can select a device and choose Stop Upgrade to stop the upgrade of that device.
4. Choose Close to close the screen and return to the Firmware Upgrade Utility window.

Viewing the Event Log

The event log contains the history of all upgrade events. The log is sorted by date and time, with the most recent event listed first.

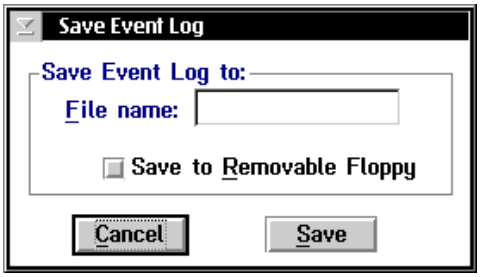
To view the event log

1. From the Firmware Upgrade Utility window, choose View Log. The Upgrade Log dialog box appears.



2. If you want to clear all the entries in the event log, choose Clear All. A message box appears confirming that you want to clear the log. Choose Clear.
3. If you want to save the contents of the event log to a file on a hard disk or a floppy disk, choose Save As. The Save Event Log dialog box appears.

Save Event Log Dialog Box



a. In the File name field, enter a meaningful file name for the event log.

b. If you want to save the file to a floppy disk, check the Save to Removable Floppy check box.

   If you want to save the file to the hard drive, clear the Save to Removable Floppy check box.

c. Choose Save. A message box appears confirming the location of the event log.

d. Choose OK. You return to the Upgrade Log dialog box.

4. Choose Close to close the dialog box and return to the Firmware Upgrade Utility window.

I

Index

Symbols and Numbers

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

System Manual Addendum

P/N 069283-002

DCS 300

Intermec

A UNOVA Company

Intermec Technologies Corporation
6001 36th Avenue West
P.O. Box 4280
Everett, WA 98203-9280

U.S. service and technical support: 1-800-755-5505
U.S. media supplies ordering information: 1-800-227-9947

Canadian service and technical support: 1-800-688-7043
Canadian media supplies ordering information: 1-800-268-6936

Outside U.S. and Canada: Contact your local Intermec service supplier.

Contents

About this Addendum

This addendum describes recent changes to the DCS 300 software v1.3 and v1.2. It also describes new features that were added to the DCS 300 software that are not explained in the *DCS 300 System Manual*.

Please review this addendum for information that you may need to use immediately and then store this addendum with your system manual for future reference. By adding this addendum, the part number of the *DCS 300 System Manual* is 067296-004.

Specific Changes to the DCS 300 System Manual

This section contains specific information about changes that you should make to your *DCS 300 System Manual*.

- Page 2-21

  When you are shutting down the DCS 300, you can choose the Restart button in the Shutdown DCS 300 message box to shut down and restart the server. This feature is useful if you know that you must reboot the server to activate your changes.

  Note: If you are using Remote Console, you must choose the Restart button. You cannot choose Shutdown and then press **Ctrl-Alt-Del**.

- Page 3-6

  These are the correct bar codes to enable DHCP on UDP Plus devices.

  Enable DHCP

  $+NI1

  Disable DHCP

  $+NI0

- Page 4-4

  The DCS 300 no longer supports a connection to a coaxial network.

- Page 6-40

  When you are enabling WTP devices, the MAC address of the device does not appear in the Device List dialog box.

- Pages 8-12 to 8-13, 8-20 to 8-21, 10-15 to 10-16, and 10-20 to 10-21

  When you are adding an IBM SNA host, the Address field no longer needs the address to be in token ring MAC address format. That is, if you are configuring an Ethernet host, enter the LAN adapter address in Ethernet format. However, if you are configuring a token ring host, enter the address in token ring MAC address format.

- Page 10-8

  For Telnet (formerly VT/ANSI) terminal sessions, the range for the Port number is from to 1 to 65535.

- Pages 11-40 to 11-44

  You can no longer use the Get Region button to get an error/status message from the bottom line (line 24 or line 25) in a host window. Instead, use the Location & Identification box in the Host Screen Region Definition dialog box to enter the information for the error/status message for which you want to define an action.

General Changes to the DCS 300 System Manual

This section contains general information about features that were removed or added to the DCS 300 software. The new features are further described later in this addendum.

Feature	Description
Fast Setup removed	You can no longer use Fast Setup button to configure the DCS 300. You must configure the DCS 300 using the Terminal Emulation, Terminal Session, Peer-to-Peer, or Screen Mapping buttons.
Coaxial network adapter card removed	You can no longer connect the DCS 300 to a coaxial network.
Data Collection Browser support added	The Data Collection Browser lets you run HTML applications on your data collection devices in your RF data collection network.
Auto Fallback feature added	The Auto Fallback feature lets Trakker Antares UDP Plus terminals and WTP devices switch from a DCS 300 that goes offline to a DCS 300 that is online with minimal system disruption.
TN3270 and TN5250 terminal sessions support added	You can use TN3270 and TN5250 terminal sessions to access your host directly from the DCS 300 or you can use them with screen mapping applications.
Norand Native mode support added	Norand Native mode is a raw data transport protocol that lets Norand devices communicate with the DCS 300 using a stream/sockets interface. The DCS 300 manages the IP socket connection. • Both Norand Native and Telnet hosts use an IP address; therefore, they can use the same host configuration dialog boxes. • Norand Native hosts communicate through ports. (By default, Telnet hosts communicate through port 23.) When a WTP device is linked to a Norand Native host, you must also specify the port number.

Understanding the Data Collection Browser

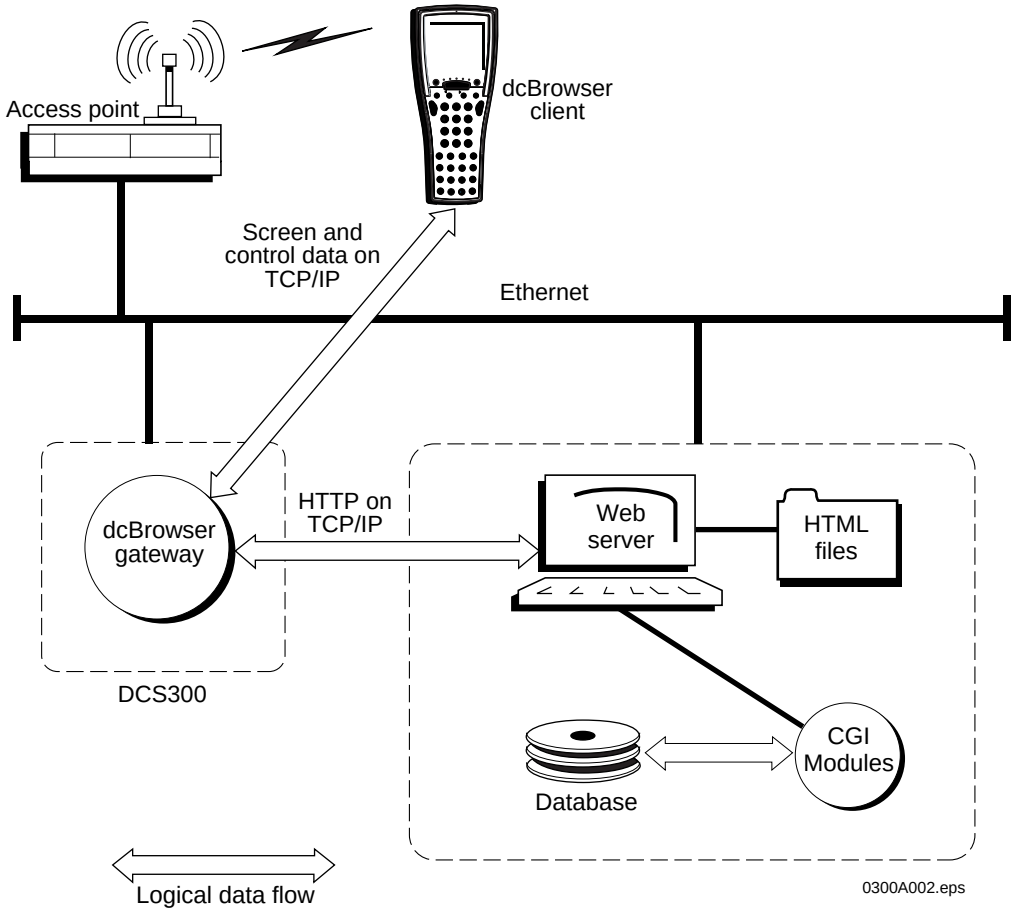
This version of the DCS 300 software provides support for the Data Collection Browser™ (dcBrowser™). You use the dcBrowser to run HTML applications on your data collection devices in your RF data collection network. The applications themselves reside on a Web server, which downloads Web pages to the devices. The dcBrowser consists of two parts: the dcBrowser client that resides on each device and the dcBrowser gateway that resides on the DCS 300.

This version of the dcBrowser supports only Trakker Antares hand-held terminals (2415, T2425, T455) and JANUS devices (JG2010, JG2020, JG2050) that are communicating using TCP/IP. You must install the DCS 300 in the Ethernet or token ring network and you must configure the network adapter card for TCP/IP. For help, see Chapter 3, "Connecting to an Ethernet/Token Ring Network" in the *DCS 300 System Manual*. Since these devices are not using UDP Plus, you do not need to follow the procedures enabling the devices on the DCS 300 and you do not need to start data collection.

How the dcBrowser works (Refer to the illustration on the next page.)

1. When a device is turned on, the dcBrowser client running on the device requests a Web page from the data collection network.
2. The dcBrowser gateway running on the DCS 300 identifies the Web home page for this device. The gateway requests this home page from the Web server.
3. The Web server sends the requested home page to the gateway.
4. The gateway interprets the HTML and filters all of the complex HTML data that is beyond the device's capability, such as comment tags and graphics. Then, the gateway sends the home page to the device.
5. Information from the device is sent to the gateway. The gateway forwards this data to the Web server. The Web server may send other Web pages to the device based on information that it receives via the gateway.

Understanding the dcBrowser



For more information, see the *Data Collection Browser User's Guide* (Part No. 070011). This user's guide is in PDF format and it ships on the dcBrowser client CD or you can download it from the Intermec Web site at www.intermec.com.

Using the Auto Fallback Feature

The Auto Fallback feature lets Trakker Antares UDP Plus terminals and WTP devices switch from a DCS 300 that goes offline to a DCS 300 that is online with minimal system disruption. This feature can also be useful in a DHCP environment where a server gets a new IP address every time it is booted.

When Trakker Antares UDP Plus terminals are communicating with access points and the DCS 300, the Connect icon is on. If the Connect icon blinks, the terminal is no longer communicating with the DCS 300. If you have implemented the Auto Fallback feature in your data collection network, simply press I/O twice on your terminal to obtain a new controller IP address. When the Connect icon is on, you can continue data collection.

Note: If your Connect icon blinks or turns off, you may be out of range of an access point, you may be about to go out of range of an access point, or the access point may have recently been turned off. Verify that you do not have an access point problem before you try to obtain a new controller IP address.

When WTP devices are no longer communicating with the DCS 300, you can no longer perform data collection. If you have implemented the Auto Fallback feature in your data collection network, reboot the device. The terminal session will try to connect to Host A and then Host B and then Host C. When it makes a connection, you can continue data collection.

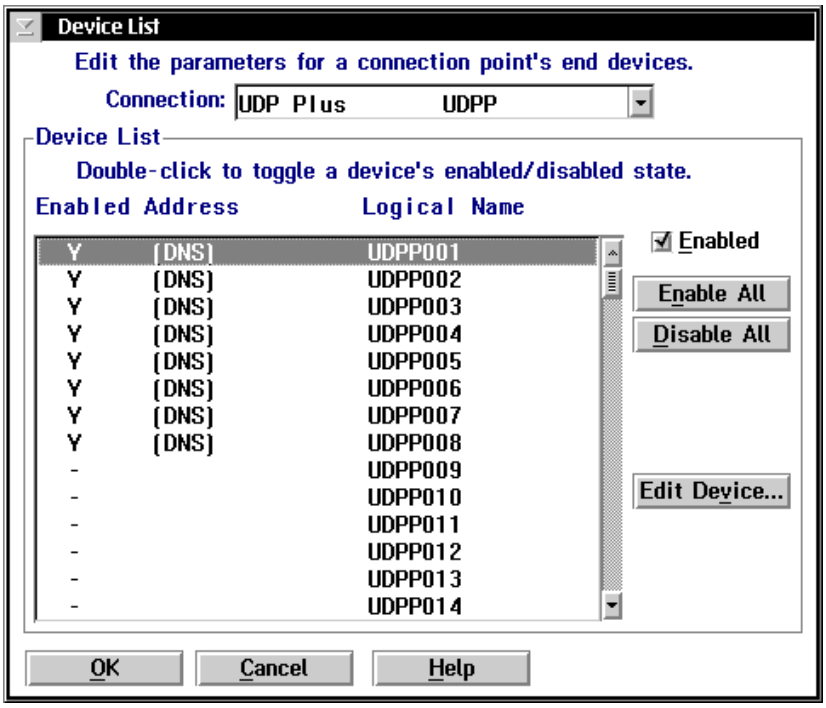
Configuring the DCS 300s

You must configure each DCS 300 that you want to be available to use with the Auto Fallback feature to accept connections from the terminal or terminals that you want to use with this feature.

To configure the DCS 300 to use the Auto Fallback feature

1. From the main menu, choose the type of communication you are using to connect the server to the host.
2. Choose Downline Network. Two buttons, Connection Points and Downline Devices, appear.
3. Choose Downline Devices. The Device List dialog box appears. This example shows how to configure the DCS 300 to accept Trakker Antares UDP Plus terminal connections.

Device List Dialog Box



4. In the Connection field, click the down arrow on the right side of the field. A list of the connection points that you have configured appears. Choose one.
5. Enable the terminals that you want to be able to communicate with this DCS 300.

   To enable all 254 devices, choose Enable All.

   Or, to enable specific terminals, select the terminal you want to enable and make sure there is a check in the Enabled check box.

Note: Each terminal must use DNS or have a valid IP v4 address before you can enable it.

6. Disable the terminals that you do not want to be able to communicate with this DCS 300.

   To disable all 254 terminals, choose Disable All.

   Or, to disable specific terminals, select the terminal you want to disable and make sure there is no check in the Enabled check box.
7. Choose OK to save your changes and return to the main menu.
8. Repeat this procedure for each DCS 300 that you want to be available to use with the Auto Fallback feature.

Configuring the Trakker Antares UDP Plus Terminals

The Trakker Antares UDP Plus terminals must be running firmware version 3.21 or later.

To configure the terminals to use the Auto Fallback feature

1. Configure the network parameters for the terminal, including the terminal IP address and the controller IP Address. The controller IP address can be any valid IP address. For help, see your terminal user's manual.
2. Scan this bar code:

   Enable DHCP

   $+NI1
3. Press ⓘ/ⓞ twice.

The terminal looks for a DCS 300 on the network. When it locates a DCS 300, it resets its controller IP address parameter to the IP address of the DCS 300 that it found.

Note: If the terminals are in a different subnetwork than the DCS 300, you must configure and enable the DHCP relay agent on the routers. For help, see your router user's manual.

Configuring the WTP Devices

The WTP devices must be running firmware version 5.33 or later. You must configure the network parameters for the device, including Host A, Host B, and Host C. For each of these hosts, you define the communications mode, the terminal number, and the RF host stack. The RF host is the DCS 300 to which you want the device to connect. When a device is booted, the terminal session tries to connect with Host A and then Host B and then Host C.

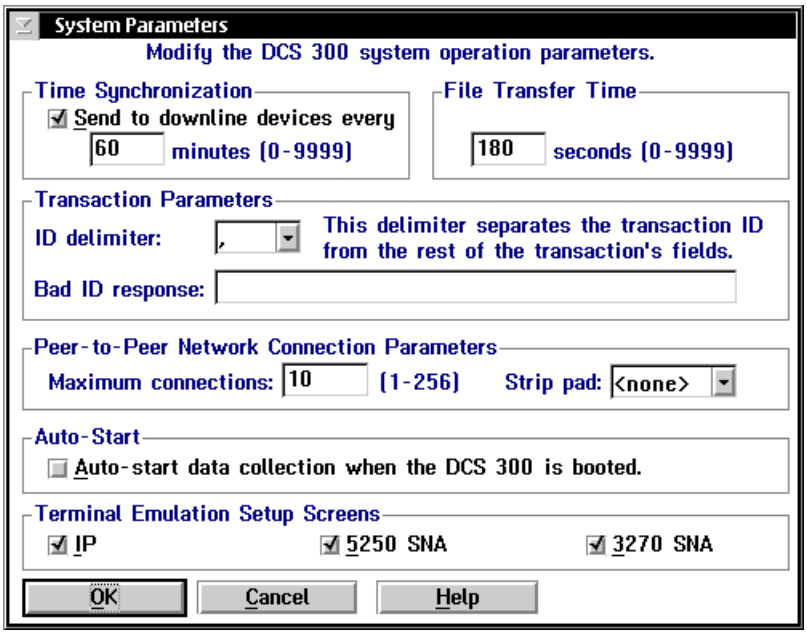
Setting the System Parameters

This section amends the information on page 2-12 and 2-13. In the Terminal Emulation Setup Screens box, VT/ANSI has been changed to IP.

When you set system parameters, you are defining the operating parameters for the DCS 300.

To set the system parameters

- From the main menu sidebar buttons, choose System Parameters. The System Parameters dialog box appears.



Field	Description	Value	Default
Terminal Emulation Setup Screens (Optional)	This box lets you customize which terminal emulation buttons appear in the main menu.	IP, 5250 SNA, 3270 SNA	Checked

Adding a WTP Network

This section amends the information on pages 6-36 and 6-37. In the Default Host Linking box, there is a new Native field.

You can define a default method for the WTP devices to get a host name when they are communicating with different types of hosts. You can configure all WTP devices to

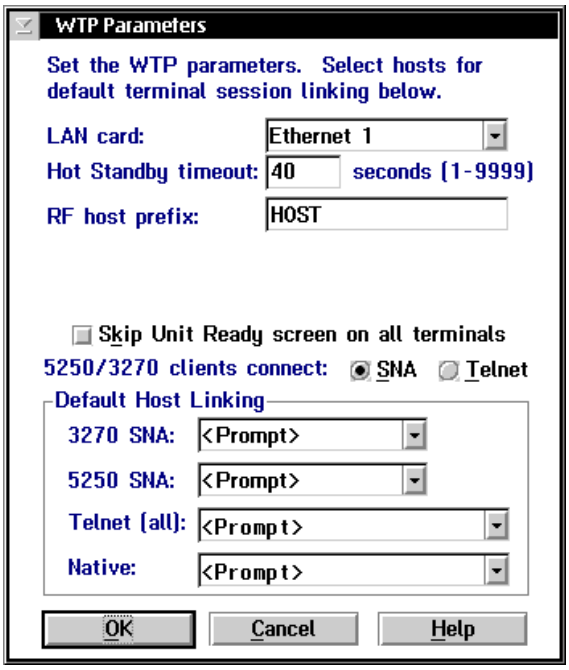
- explicitly link with a specific host. Click the down arrow on the right side of the field and choose a host that you have configured. For Telnet and Native hosts, you must choose the port name and host.
- prompt the user to enter a host name. Click the down arrow on the right side of the field and choose <Prompt>.
- not communicate with a host. Click the down arrow on the right side of the field and choose <none>. Since you cannot define a host on a WTP device if you choose <none>, the WTP device will not be able to connect to a host. You can still use the Terminal Emulation Links dialog box to explicitly link the WTP device to a host.

If you define an explicit link for a terminal in the Terminal Emulation Links dialog box, these settings override the setting in the Default Host Linking box.

To add a WTP network

1. From the main menu, choose the type of communications you are using to connect the server to the host.
2. Choose Downline Network. Two buttons, Connection Points and Downline Devices, appear.
3. Choose Connection Points. The Connection Point List dialog box appears.
4. Choose Add. The Add a Downline Connection Point dialog box appears.
5. Choose WTP and then choose Add. The WTP Parameters dialog box appears.

WTP Parameters Dialog Box



Field	Description	Value	Default
LAN card	The network adapter card that you are using to communicate with the WTP network.	Ethernet 1, Ethernet 2	Ethernet 1
Native	The port name and host that a WTP device connects to if the device is not explicitly linked to a host and it is running in Native mode.	None, Predefined list, Prompt	<Prompt>

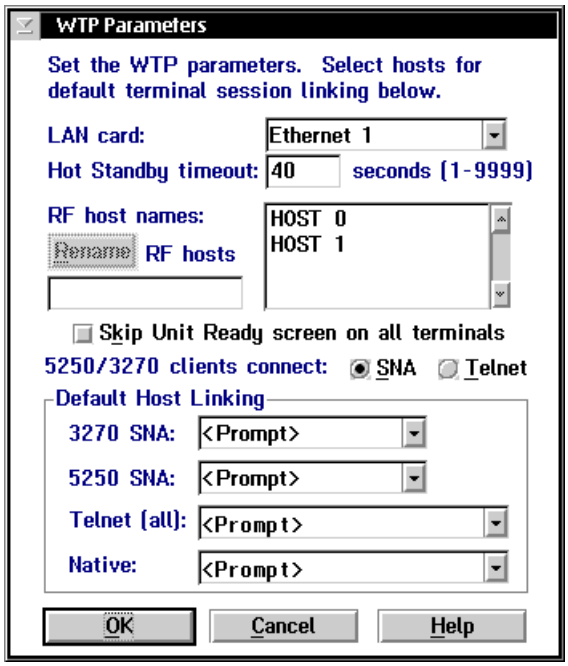
Editing the WTP Network

This section amends the information on page 6-39. In the Default Host Linking box, there is a new Native field.

When you edit the WTP network, the WTP Parameters dialog box looks slightly different than when you added the network.

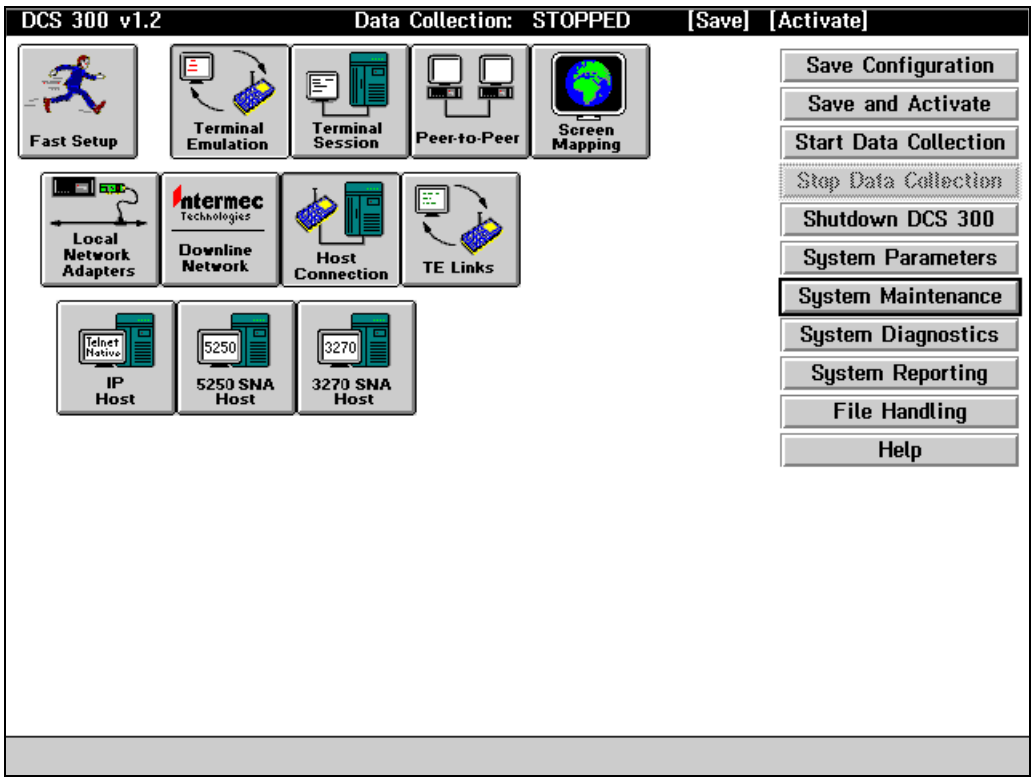
To edit the WTP network

1. From the main menu, choose the type of communications you are using to connect the server to the host.
2. Choose Downline Network. Two buttons, Connection Points and Downline Devices, appear.
3. Choose Connection Points. The Connection Point List dialog box appears.
4. Choose WTP and then choose Edit. The WTP Parameters dialog box appears.



Configuring IP Hosts

This section replaces “Configuring Telnet Hosts” on pages 8-7 and 8-8. If you choose Terminal Emulation and then Host Connection, a new IP Host button replaces the Telnet Host button.

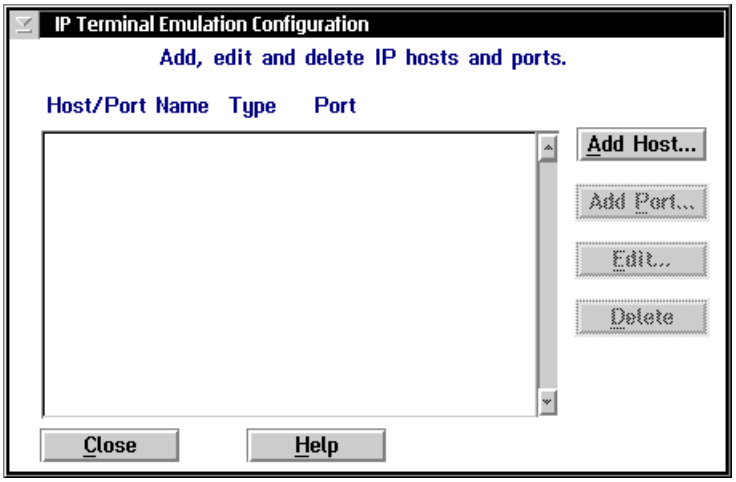


When you upgrade the DCS 300 to v1.2, any IP host that is either the default host for a downline network or is linked to a device has a port configured with a port name of Telnet and port number of 23. However, if the IP host was defined through the Terminal Session path or Screen Mapping path, it will appear in the IP Terminal Emulation Configuration dialog box, but it will not have any ports configured.

To configure an IP host

1. From the main menu, choose Terminal Emulation.
2. Choose Host Connection and then choose IP Host. The IP Terminal Emulation Configuration dialog box appears.

   The list box contains the host names that you have configured. Hosts that have ports are prefixed by a + (plus) sign or a - (minus) sign. Double-click on a host name with a + sign and the ports that have been configured for that host will appear underneath it. Double-click on a host name with a - sign and the ports for that host will disappear.



3. Choose Add Host, Add Port, Edit, or Delete. You must be able to select a host before you choose to add a port, edit a host, or delete a host. That is, you must have already added at least one host.

   If you choose Add Host, the TCP/IP Host Connection dialog box appears. For help, see “Configuring a Telnet Host” in Chapter 8 of the *DCS 300 System Manual*.

   If you choose Add Port, the Port Configuration dialog box appears. For help, see “Adding an IP Port” in the next section.

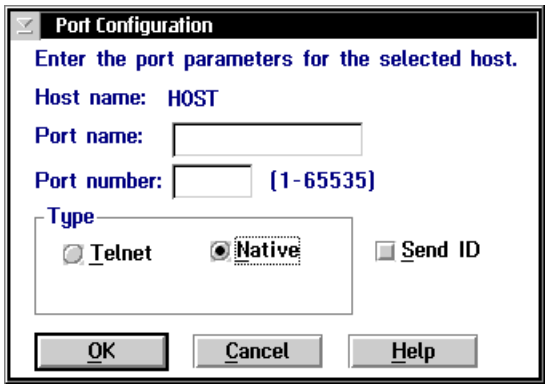
Adding an IP Port

This section is new. The Port Configuration dialog box is new.

Note: When you add an IP host, a default port (Telnet, port number 23) is automatically added.

To add an IP port

- From the IP Terminal Emulation Configuration dialog box, choose Add Port. The Port Configuration dialog box appears.



Field	Description	Value	Default
Port name	The name that identifies this port for this host. The name must be unique for this host.	1 to 8 alphanumeric characters	None
Port number	The number of the port that you are configuring for this host. The number must be unique for this host.	1 to 65535	None
Type	These option buttons identify the type of port that you are configuring.	Telnet, Native	Native
Send ID (Native only)	This check box determines if the terminal session name, RF host stack number, and the terminal number are sent to the host.	Check, Clear	Clear

Configuring TE Links

This section amends pages 8-23 and 8-24.

The Terminal Emulation Links dialog box lets you change links for individual terminal sessions. These explicit links override the host name that is defined on the terminal and the default host link that you defined when you configured the downline connection point. You can only link Native host ports to WTP devices.

The Linked Terminal Sessions box and the Unlinked Device/State box let you select multiple objects by

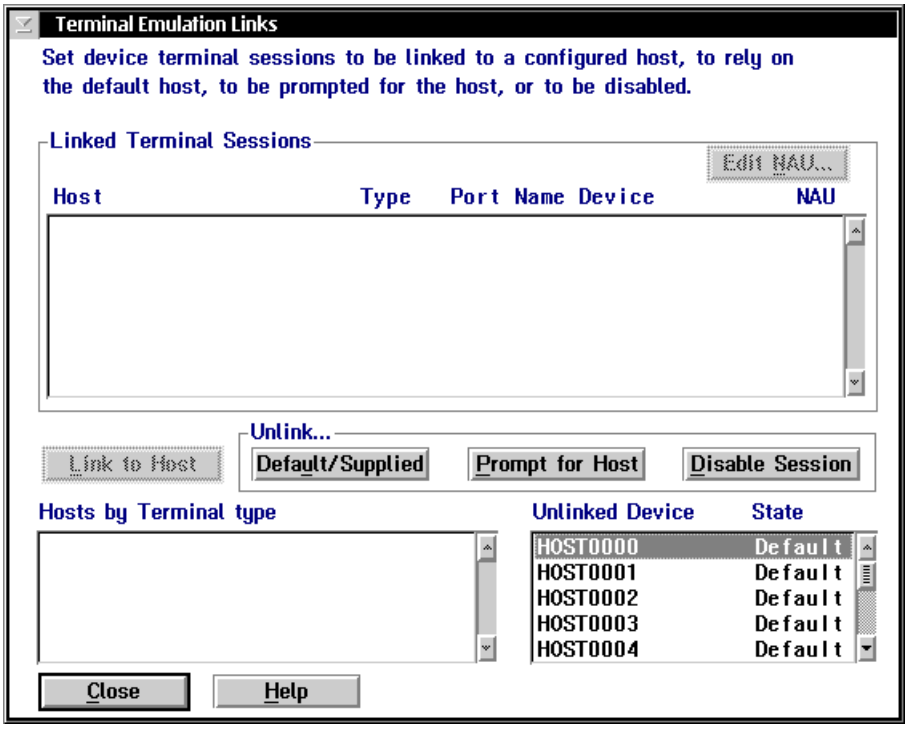
- clicking and dragging to select several sequential objects.
- selecting one object and then holding down the **Shift** key and selecting another object. You now have selected all sequential objects from the first clicked object to the last one.
- selecting one object and then holding down the **Ctrl** key and selecting another object. You now have selected two non-sequential objects.

Linked Terminal Sessions box This list box contains the terminal sessions and devices that are explicitly linked to a host. It contains a new column that identifies the port name of the Telnet or Native host.

Hosts by Terminal Type list box This list box contains the host types (5250, Native, etc.) that you have configured. Telnet hosts and Native hosts are prefixed by a + (plus) sign or a - (minus) sign. You can double-click on a host with a + sign and the ports that have been configured for that host will appear underneath it. You can double-click on a host with a - sign and the ports for that host will disappear.

Unlinked Device/State list box This list box contains a list of terminal sessions and devices that have not been linked to a host. You can select multiple terminal sessions and devices in this box and link them to a host or apply a state to them.

Terminal Emulation Links Dialog Box



Creating Terminal Sessions

This section amends page 10-7. The 5250, 3270, VT/ANSI buttons have been renamed to 5250 SNA, 3270 SNA, and Telnet.

You can use these sessions to access the host from the DCS 300 or you can use them for screen mapping sessions.

5250 SNA button This button lets you configure 5250 SNA terminal sessions.

3270 SNA button This button lets you configure 3270 SNA terminal sessions.

Telnet button This button lets you configure Telnet terminal sessions. In the Mode field, you can choose VT100, VT220, VT320, ANSI, TN3270, or TN5250.

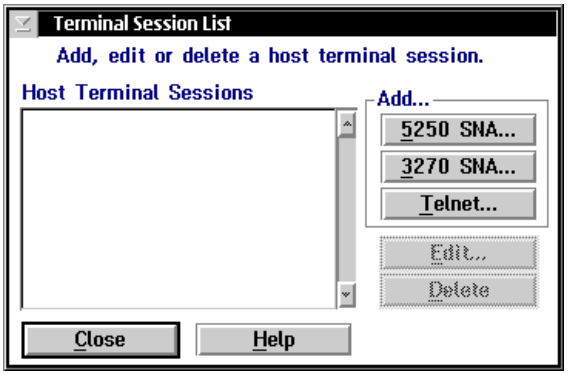
There is a limit to the number of terminal sessions that the DCS 300 can support. The total number of sessions is the sum of all of the terminal session types. You can have 100 VT100 sessions and 128 VT220 sessions, but you cannot have 228 VT100 sessions and 228 VT320 sessions.

Terminal Session Type	Total Number of Sessions
VT100, VT220, VT320, ANSI	228
TN3270, TN5250, 5250 SNA, 3270 SNA	26

Note: You can create a maximum of 15 5250 SNA terminal sessions.

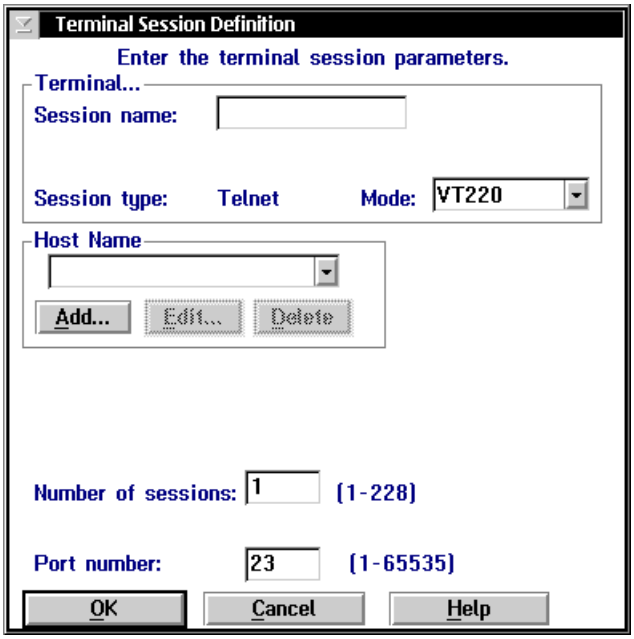
To create a terminal session

1. From the main menu, choose Terminal Sessions.
2. Choose Host Connection. The Terminal Session List dialog box appears.



3. Choose the type of terminal session you want to create. The Terminal Session Definition dialog box appears.

   This dialog box appears if you choose Telnet.



Field	Description	Value	Default
Mode	The type of terminal mode that you want to use for this terminal session.	VT100, VT220, VT320, ANSI, TN3270, TN5250	VT220

Note: If you edit a Telnet terminal session and you have set the mode to TN3270 or TN5250, you cannot change the mode. To change the mode, you must delete the terminal session and then create a new one with the new mode.

Communicating Through the Native Sockets Interface

You can configure the DCS 300 to support Norand Native communications between terminals running in Native mode and a custom host application. These terminals present a simple read/write interface to the custom host application. The 1100, 1700, 5055, 5900, 6400, and 6550 terminals that run in the Intermec 2.4 GHz RF network or the Falcon 900 MHz network support Native mode.

You may want to use Norand Native communications when you need to develop a custom host application and you cannot use standard terminal emulation. You can use Native syntax with the terminal Application Development Kit (ADK) to create client applications on the 6400 terminals. However, ADK applications are not supported on the 1100, 1700, 5055, 5900, and 6550 terminals. For more information on the ADK (Part No. 215-299-001), contact your local Intermec representative.

Setting Up the DCS 300

To set up the DCS 300 for Native communications, you must:

- Configure the DCS 300 for an Ethernet or token ring network. For help, see Chapter 3, "Connecting to an Ethernet/Token Ring Network" in the *DCS 300 System Manual*.
- Configure the IP hosts and add the ports for the host applications. For help, see "Configuring IP Hosts" in this addendum.
- Add a WTP network and define the Default Host Linking box, Native field. For help, see "Adding a WTP Network" in this addendum.
- Configure any TE links. For help, see "Configuring TE Links" in this addendum.

Setting Up the Terminals

For each terminal, you must use the menus to configure the radio network, Native communications, a terminal number, and the RF host stack number. Each terminal session must have a unique terminal number/RF host stack number combination.

To set up the terminals

1. In the Main Menu select (1) Setup Parms. Enter the password.
2. Configure the LAN ID and the other radio parameters. These parameters must be set the same for all terminals and access points.
3. Use the host setup screens to configure the terminal session for Native communications, the unit (terminal) number, and the RF host (DCS 300) stack number. You configure Host A, Host B, and Host C independently.
4. Press **Enter** repeatedly to exit the menus.

Example

This example walks you through the terminal screens to show you how to configure one of the terminal sessions for Host A, Native communications, terminal number 42, and the RF host stack number 0 (RF host name is MYHOST).

```
1)  Host A
2)  Host B
3)  Host C
```

```
1) Native
2) 3270
3) 5250
4) VT220
```

```
Enter Unit
Number:
42
```

```
Native
Unit #     42
Enter Host Name
MYHOST 0
```

About the Host Application Requirements

You may need to make some changes to your existing Norand Native host applications so they will work with the DCS 300.

New feature You can now send the terminal session name, the RF host stack number, and the terminal number to the host. In the Port Configuration dialog box, check the Send ID check box.

Unsupported command The DtE Terminal Echo-back Diagnostic command is not supported.

Converting to the DCS 300 From the 6950 EGS

If your host application was written to work with the 6950 EGS, it should also work with the DCS 300 as long as the host application separates packets using a line feed (LF) character. If you did not write your host application for the 6950 EGS using delimiters, you must add an LF after each command. After you add the LFs, your host application will still work with the 6950 EGS.

Converting to the DCS 300 From WNAS or Serial Controllers

If your host application was written to work with WNAS or Norand's serially connected controllers, you must modify the application before it will work with the DCS 300. These next two sections explain the changes you need to make to the Native syntax and the considerations you need to understand when using sockets.

Changes to the Native Syntax

If your host application was written to work with WNAS or Norand's serially connected controllers, you must make some changes to the Native syntax before it will work with the DCS 300. You can obtain a complete description of Native syntax in Section 3 of the Terminal Commands of the *Native Terminal Emulation Asynchronous Terminal Emulation Reference Guide* (Part No. 977-047-038).

Important: In the *Native Terminal Emulation Asynchronous Terminal Emulation Reference Guide,* you must use a line feed (LF) as the delimiter. You cannot use a carriage return (CR).

For your host application to work with the DCS 300, you must make these syntax changes to the terminal commands:

Write Display command (WtD…) You must remove the "Wt" portion of the command. Format the command as D*options*/*data* and write it to the socket. The socket number, not the terminal number, uniquely identifies each terminal to the application. The DCS 300 maintains the mapping between socket number and terminal number.

Set Terminal Control Parameters command (StD…) You must replace the "St" portion of the command with a lowercase "e." Format the command as eD*options*/*parameters*.

Reset command (G) You must format the command by sending a lowercase "g" as a null-terminated string.

Terminal Firmware Version command (DtV) You must format the command by sending a lowercase "v" as a null-terminated string.

Using Native Sockets

If your host application was written to work with WNAS or Norand's serially connected controllers, you must modify the application to use a socket interface instead of a serial port interface before it will work with the DCS 300.

Terminals that are running in Native mode establish terminal sessions on the DCS 300 through a sockets interface. To use this interface, you must understand stream/sockets programming fundamentals. An excellent reference book for sockets programming is *UNIX Network Programming* by W. Richard Stevens (ISBN 0-13-949876-1).

Note: Intermec does not provide application programming support for streams/sockets programming.

The DCS 300 initiates communications with the host application through the configured port. Individual terminal sessions are mapped to unique sockets. Each terminal power up results in the DCS 300 opening another socket on the port to initiate the session with the host. The DCS 300 keeps an internal table mapping terminal numbers to socket numbers. These sockets (sessions) remain open until the host application closes the session using the Reset command, or a terminal cycles power resulting in the DCS 300 closing the old session and a new session being initiated.

Sample Program

The nui_sock.c program is a sample C Language program that uses internet stream sockets to send Native syntax to a terminal via the DCS 300. This program uses a single user-assigned system port to communicate to multiple terminals, each connected via sockets under the control of the DCS 300. This program demonstrates the portability of Native applications from the WNAS or serial communications to the DCS 300.

In order for the terminals to connect, you must configure the DCS 300 and terminals. For help, see "Setting Up the DCS 300" and "Setting Up the Terminals" earlier in this addendum.

Note: On the DCS 300, when you configure the IP host and the port, do not check the Send ID check box in the Port Configuration dialog box. The nui_sock.c program does not expect the terminal ID.

To run this program, you need to supply an available port number as an argument on the command line. For example, at a UNIX prompt you would type:

`./nui_sock` *`portnumber`*

where *portnumber* is the port number that is configured for the IP host on the DCS 300.

Once everything is configured correctly and terminals are powered up, a unique connection (socket) is established between each terminal and the nui_sock program. The terminal will begin with a prompt that says, "Enter data now:" This program lets you enter data and then it echoes the data you entered.